F-Secure

Annual report 2025

Contents

F-Secure 2025 04

This is F-Secure 04

The year 2025 in numbers 05

President and CEO's review 06

Strategy 09

Board of Directors' Report 11

Key figures 21

Shares and Shareholders 25

Group Sustainability Report 27

Consolidated financial statements 112

Statement of comprehensive income 114

Statement of financial position 115

Statement of cash flows 116

Statement of changes in equity 117

Notes to the financial statements 117

F-Secure Corporation financial statements ... 148

Signatures of the Board of Directors' report and Financial statements 167

Information for shareholders 170

Auditor's report **171**

Assurance Report on the Sustainability Report **176**

Independent auditor's report on the ESEF financial statements **178**

Corporate Governance **180**

F-Secure Corporate Governance Statement 181

Board of Directors 31 December 2025 186

Leadership team 31 December 2025 195

Remuneration Report 206

This is F-Secure

We exist to make every digital moment more secure for everyone, as the world needs securing like never before.

The trust gap between consumers and their digital experiences is widening. As trust declines, its value rises, emerging as a critical driver of brand choice and long-term loyalty. This shift is increasingly important for digital service providers as they seek new, profitable revenue streams.

Consumers are no longer looking for protection alone. They want a deeper security experience that feels more like care, one that builds digital confidence and enables them to live their best digital lives: secure, empowered, and limited only by their own imagination.

We believe world-class protection begins with a deep understanding of human needs then wrapping technology around them. By multiplying our 37 years of security expertise with the power and scale of AI, F-Secure is uniquely positioned to continue innovating and leading the market with award-winning products and services.

Delivering Trust as a Service, we enable our partners to move beyond standalone security tools to deliver trusted digital experiences that strengthen customer relationships and unlock new growth opportunities. This consolidates our number one position with the world's largest communication service providers and our network of more than 200 partners, while advancing our ambition to become the most trusted and desirable brand in cybersecurity.

Headquartered in Helsinki, Finland, F-Secure operates globally from multiple locations and protects tens of millions of consumers through all its channels. F-Secure had revenue of EUR 145.7 million in 2025 and employed around 550 people. F-Secure shares are listed on the Nasdaq Helsinki Stock Exchange.

The year 2025 in numbers

Revenue **145.7** MEUR (-0.4%)	Subscribers **~30** million across channels	Number of Service Provider Partners **~200**
Adjusted EBITA **50.3** MEUR (34.5% margin)	Users in **~200** countries	Fellows **~550**
Earnings per share **0.13** EUR	Dividend per share* **0.04** EUR	**45** nationalities

*The Board proposal to the Annual General Meeting

Revenue by channel, %

- 18.4% Direct Channel
- 81.6% Partner Channel

Revenue by geography, %

- 31.2 % Rest of Europe
- 30.7 % Nordic Countries
- 30.4 % North America
- 7.7 % Rest of the world

President and CEO's review

In 2025, we continued to advance our strategy, focusing on innovation, operational excellence, and commercial performance to deliver the world's leading security experience for consumers and partners.

The year began with a renewed organization and operating model. Our customercentric sales and service teams are now fully operational, improving solution fit, execution quality and speed across partner onboarding, partner success operations, and lifecycle management. This shift is central to how we plan, build, and deliver solutions with - and for - our partners and end users.

Our Scam Intelligence & Impact Report 2025 delivers a clear message: scams are scaling faster than ever. Global consumer losses are estimated at over USD 400 billion, and younger adults (18–34 yrs) now face twice the scam risk compared to older generations. AI-driven scams have grown rapidly, and it is no longer enough to protect consumers from malware to keep them safe. Instead, we need to also identify signs and events that can lead to consumers being tricked, and subsequently either warn or stop the user from falling for the scam. Increasingly, humans are the weakest entry point as social engineering has become the most effective method for compromising victims. This environment reaffirms our strategic focus on comprehensive scam protection and humancentered security 1).

Persistence paid off with several major milestones on our strategic journey; We signed a strategic partnership with one of the world's largest communication service providers, targeting worldclass digital protection for more than 100 million customers. We entered finalstage negotiations with another leading CSP to embed our solutions at scale, with launch expected in Q2 2026. At the end of the year we agreed on a significant solution expansion with an existing Tier1 partner, introducing new Embedded

Security capabilities: Credit Monitoring, Financial Transaction Monitoring and Identity Fraud Insurance. This is a new solution domain for FSecure and deliveries for these strategic projects will commence in phases, strengthening our 2026 revenue.

These steps expand our addressable market, deepen our role in the CSP core value stack, and position us to capture significant subscriber growth along with higher Embedded Security ARPU through an expanding suite of protection capabilities.

Consumer sentiment remained neutral at best with global and local uncertainties. We see this environment not as a headwind, but as a call for sharper execution and innovation – strengths that position us strongly for the future. In 2025 our business execution faced delays as our Tier 1 partner deals took longer to materialize than indicated by them. Despite falling short of our 2025 growth expectations, we remain confident that our strategic partner agreements will start to generate meaningful revenue growth in 2026 and beyond.

F-Secure has always been committed to protecting people, but today's evolving threats - scams, social engineering, and mass deception - demand new capabilities. We are now applying AI across the company to boost innovation, productivity, and agility. Our evolution into an AI-native organization is exemplified by Horizon and Halo initiatives. Horizon is our new partner business platform, now in beta with first partners onboard and a public launch in February. Halo, a completely new scam protection focused product, is expected to enter beta in early Q2/26. We do not expect these products to have a significant impact on 2026 revenue, but we are building a strong foundation for scalable development in the coming years.

Nearly 80% of our software development work is either fully AI-generated or AI-assisted, cutting cycle times by more than half in 2025 alone.

Technology remains at the heart of our strategy. In the first half, we enhanced our Embedded Security portfolio with a host of new Scam Protection capabilities - spanning detection of imagebased scams, deepfake voice cues, and socialengineering signals. We also launched Scam Protection as a standalone module of Total, offering consumers greater flexibility and access in the face of rising online scams. Sales of our Embedded Security portfolio grew 4 % during the year, demonstrating resilience and productmarket fit despite partner timing effects.

Our innovation leadership received global recognition throughout the year. FSecure was named the leading cybersecurity partner for telcos by STL Partners' [2)], highlighting our technology, threat intelligence, and proven track record. We received the Most Innovative PoC Award at Fiber Connect [3)] for our joint proof of concept. We earned a Gold Medal from EcoVadis [4)], placing us in the top five percent of over 150,000 companies worldwide for sustainability performance - an independent benchmark for trustworthy and transparent ESG practices. We were honored with the AI Growth Initiative of the Year at the AI Gala 2025 [5)] for our Scam Image Scanner, an AIdriven capability protecting consumers from imagebased scams across social media, messaging apps, marketplaces, and online platforms. In addition, FSecure Internet Security earned AVComparatives' FakeShops Detection Certification for the second consecutive year, and we were proud to receive the KPN Cybersecurity Award 2025 in recognition of outstanding partnership and services.

Looking ahead, we will continue to execute our strategy to become the number one security experience company globally, with three priorities in 2026:

1. Strategic partner wins fuel growth
2. Unlock growth potential
3. Accelerate innovation and execution

We will maintain financial discipline, sharpen commercial execution, and continue investing in AI, threat intelligence, and partner experience to drive innovation, operational efficiencies and to convert our business pipeline into sustainable growth.

Finally, I want to extend my heartfelt thanks to all FSecure Fellows for your dedication and hard work throughout the year. Your passion and resilience are the driving force behind our progress. Together with our trusted customers and partners, we look forward to building on this momentum and embracing new opportunities in 2026.

Timo Laaksonen, CEO & President of F-Secure

“F-Secure has always been committed to protecting people, but today’s evolving threats - scams, social engineering, and mass deception - demand new capabilities.”

[1] F-Secure Scam Intelligence & Impact Report 2025: https://www.f-secure.com/en/partners/insights/scam-intelligence-and-impacts-report-2025?utm_source=linkedin&utm_medium=social&utm_campaign=Scam+Report+2025&utm_content=wave2
[2] STL Partners helps telcos, technology, and digital infrastructure companies to innovate, grow and stay ahead of the competition by providing actionable insights and practical guidance on emerging challenges and opportunities, with a focus on innovation and identifying new sources of growth. https://stlpartners.com
[3] https://fiberbroadband.org/2025/06/04/fiber-broadband-association-awards-connected-home-subscriber-experience-concepts-at-fiber-connect-2025/
[4] Ecovadis is a global standard for resilient, sustainable supply chains. Trusted data, actionable insights, continuous improvement. https://ecovadis.com
[5] https://www.f-secure.com/en/partners/newsroom/f-secure-wins-ai-growth-initiative-of-the-year-at-ai-gala-2025-for-scam-image-scanner

Strategy

OUR VISION Living your best digital life – trust for a world AI keeps rewriting

OUR MISSION To create security that feels like care, building consumer confidence and enabling trusted digital experiences

Strategic priorities for 2026

#1

Strategic Partner wins fuel growth

Tier 1 commitments and new deals a key growth engine

Fully productized, carrier-grade solution and service portfolio

#2

Unlock growth potential

Comprehensive scam protection offering drives ARPU and subscriber growth

Scale number of partners served with AI-native SaaS business platform (Horizon)

Deliver AI-powered and human-centered scam protection product (Halo)

#3

Accelerate innovation and execution

Launch innovative, research-based solutions in scam protection

Drive holistic data strategy for partner insights and customer engagement

Implement AI-native business processes and workflows

Financial targets

F-Secure medium term financial targets reflect the company's growth amibitions and strategic direction.

Growth

High single digit growth (CAGR) with additional significant upside from major Tier 1 deals.

Profitability

Adjusted EBITA margin approaching 40% as revenue reaches EUR 200 million.

Divident yield

Around or above 50% of net profit; which can be adjusted as long as the leverage is higher than the targeted level.

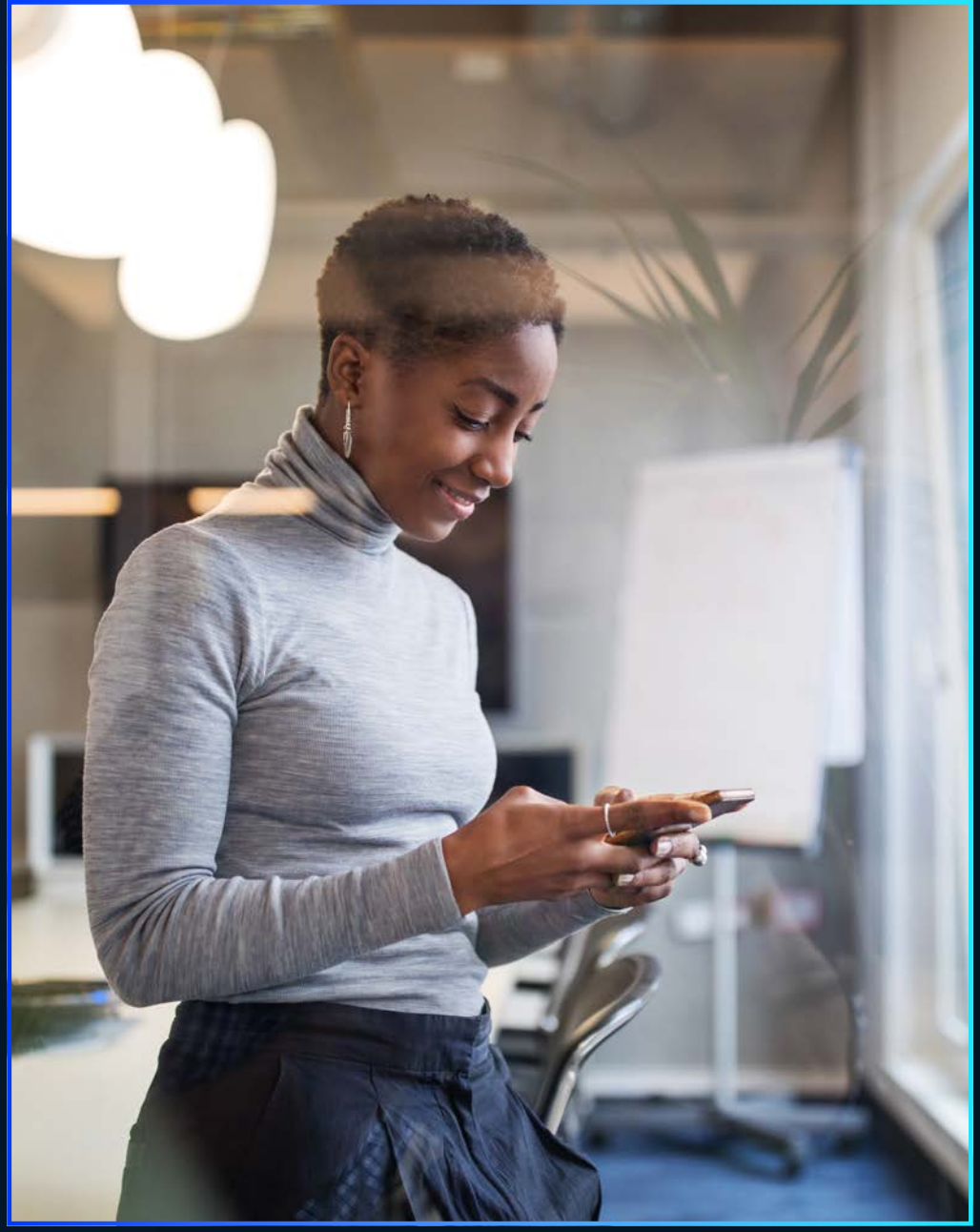
Leverage

Net debt / adjusted EBITDA ratio below 2.5x, excluding temporary impact from acquisitions.

Rule of 40

F-Secure Corporation follows the Rule of 40 metric as internal performance measurement and guiding principle, according to which the combined revenue growth rate and profitability margin should be equal to or greater than 40%.

Board of Directors' Report and Financial Statements



Board of Directors' report

F-Secure Corporation in 2025

F-Secure Corporation is a globally operating consumer cybersecurity company. F-Secure designs and offers a comprehensive range of award-winning consumer cybersecurity products and services that are AI-powered and human-centered. These products and services protect consumers' digital moments against scams, and are contextually relevant, resonate emotionally and proactively helpful.

F-Secure is the global leader in providing consumer cybersecurity through Communication Services Providers (CSPs) and has become undisputed leader among world's largest CSPs. Additionally, F-Secure partners with Service Providers such as banks and insurance companies, and sells services directly to consumers through its web store mobile and app stores. The company was reborn through the demerger of the consumer business from WithSecure Corporation in June 2022. In 2023, F-Secure strengthened its footprint in the US and among CSPs by the acquisition of Lookout Life, a US-based consumer mobile security business of Lookout Inc.

F-Secure's main product and service portfolios are:

Security Suite: F-Secure Total, which is an all-in-one consumer cybersecurity application that provides complete protection against scams as well as security, privacy and identity protection on all consumers' personal devices.

Embedded Security: Comprehensive portfolio of consumer cybersecurity capabilities available as Software Development Kits (SDKs) and cloud Application Programming Interfaces (APIs) that can be embedded into Service Provider's app or service. Embedded Security portfolio also includes F-Secure Sense, an SDK based solution that provides whole home protection embedded inside a Wi-Fi-router. Embedded Security typically has a lower gross margin than Security Suite due to lower pricing, and higher expected volumes. The partner is responsible for the implementation of the solution.

Services: F-Secure Security Business Platform based scalable expert and cloud-based services supporting both Security Suite and Embedded Security business such as delivery and integration, customer care, and partner success services that support F-Secure's Partner Business. Furthermore, during 2025, F-Secure piloted "Horizon," an AI-native self-service SaaS platform designed to scale the number of Service Providers the company can serve.

F-Secure operates globally in over 100 countries and has tens of millions of subscribers in all channels. F-Secure products are sold to consumers through approximately 200 CSPs, retailers, banks, insurance companies and directly through online and app stores.

F-Secure shares are listed on the main list of Nasdaq Helsinki.

Presentation of financial information

Figures in brackets refer to the corresponding period in the previous year, unless otherwise stated. Percentages and figures presented herein may include rounding differences and therefore may not add up precisely to the totals presented.

Financial performance

Revenue

F-Secure currency neutral growth was 0.6%. Reported revenue remained at previous year's level (-0.4%) and was EUR 145.7 million (EUR 146.3 million).

Deferred revenue decreased by 5.2% from December 2024, mainly due to normal seasonal variation in billings of some large partner contracts but also due to reduced engagement with retail partners.

Partner Channel

Currency neutral revenue in the Partner channel increased by 1.8%. Reported revenue increased by 0.6% and was EUR 119.0 million (EUR 118.2 million). Partner channel revenue in North America was weak due to US dollar fluctuations.

At comparable exchange rates, **Security Suite** revenue increased by 0.7%. Reported revenue decreased by -0.2% and was EUR 95.6 million (EUR 95.7 million). Total conversion continued well and average revenue per user (ARPU) increased. In the Nordics, activity was strong in Sweden and Finland. The DACH region[1)] continued to perform well except for Germany, where revenue declined significantly due to ongoing challenges faced by a key partner in its core business. Progress in North America was weak partly due to lower price levels of an existing customer and modest performance of customers with legacy products.

At comparable exchange rates, revenue from **Embedded Security** increased by 6.7%. Underlying business in Japan was good throughout the period, although in the fourth quarter it was weaker than in the previous quarters. First quarter revenue

[1)] Germany, Austria, and Switzerland.

was negatively impacted by one-time revenue recognition timing adjustment of EUR 0.3 million related to Japan. Growth was supported by good development in the US, where the majority of revenue is attributable to Embedded Security. Reported revenue increased by 4.0% and was EUR 23.4 million (EUR 22.5 million).

Direct Channel

Currency neutral revenue and reported revenue from Direct channel decreased by -4.5% and was EUR 26.8 million (EUR 28.0 million). The decline in revenue is especially due to weak performance in North America. Service renewal rates were high and ARPU development was healthy. However, the number of users declined throughout the year due to low level of paid customer acquisition investments as per current strategy.

F-Secure reports Partner channel revenue divided into its main product portfolios: Security Suite and Embedded Security. This reporting approach aims to increase transparency in the development of the company's product mix, as the portfolios have different levels of profitability.

Revenue by sales channel

EUR million	1-12/2025	1-12/2024	Change %	Currency neutral change %
Revenue from external customers				
Partner channel	119.0	118.2	0.6%	1.8%
Security Suite	95.6	95.7	-0.2%	0.7%
Embedded Security	23.4	22.5	4.0%	6.7%
Direct channel (E-commerce)	26.8	28.0	-4.5%	-4.5%
Total	**145.7**	**146.3**	**-0.4%**	**0.6%**

Revenue by geography

EUR million	1-12/2025	1-12/2024	Change %	Currency neutral change %
Revenue from external customers				
Nordic countries	44.8	42.0	6.5%	6.5%
Rest of Europe	45.4	48.1	-5.6%	-5.6%
North America	44.3	45.5	-2.6%	-0.1%
Rest of the world	11.3	10.6	6.0%	8.4%
Total	**145.7**	**146.3**	**-0.4%**	**0.6%**

Gross margin

Gross margin declined and totaled 123.4 million (EUR 126.0 million) or 84.7% of revenue (86.2%) due to lower-than-expected volumes as well as a higher proportion of the lower-margin Embedded business.

Operating expenses

Operating expenses excluding depreciation and amortization and items affecting comparability were EUR -72.3 million (EUR -73.3 million). Sales and marketing costs declined and were EUR -32.2 million (EUR -33.4 million). The decrease was driven by reduced engagement with retail partners resulting in lower marketing costs. Research and development (R&D) costs were EUR -24.7 million (EUR -25.4 million). R&D activity increased somewhat, but a higher

level of capitalization led to lower level of R&D expenses during the year. Administration costs were EUR -15.4 million (EUR -14.5 million). Administration costs increased due to a few one-off costs.

Depreciation and amortization excluding purchase price allocation (PPA) amortization increased due to the higher R&D capitalization during the last couple of years and totaled EUR -8.5 million (EUR -5.8 million). PPA amortizations related to the Lookout consumer security business acquisition totaled EUR -7.9 million (EUR -7.8 million).

Profitability

Adjusted EBITA amounted to EUR 50.3 million or 34.5% of revenue (EUR 52.2 million, 35.7%). EBIT was EUR 35.5 million and 24.4% of revenue (EUR 38.4 million, 26.3%), the decline was due to lower EBITA level and higher amortizations of capitalized R&D expenses. The comparison period included EUR -1.4 million of items affecting comparability attributable to restructuring and change negotiations.

Cash flow, financial position and financing

In January–December 2025, cash flow from operating activities before financial items and taxes amounted to EUR 54.0 million (EUR 53.9 million). Cash flow from operations was EUR 43.6 million (EUR 38.8 million). Despite the higher capitalization during the year, the cash conversion rate remained stable, being 79.1% (80.5%). Cash at the end of December 2025 stood at EUR 10.8 million (EUR 8.1 million).

At the end of December 2025, F-Secure net debt amounted to EUR 145.6 million (EUR 163.6 million) and the net debt to adjusted EBITDA ratio was 2.8x. All the Group's loan agreements include a quarterly measured financial covenant based on the ratio between net debt and EBITDA. The Group has met these covenant terms and conditions on the reporting date. The equity ratio was 21.5% (17.4%).

Total assets were EUR 261.1 million (EUR 270.6 million) at the end of December 2025.

As of 31 December 2025, current lease liabilities were EUR 1.7 million (EUR 0.7 million), and non-current lease liabilities were EUR 3.4 million (EUR 0.5 million). The lease liabilities relate to leases for office premises and cars. The increase in lease liabilities relates to the new lease agreement for headquarter office premises which was recorded in the balance sheet as a right-of-use asset (EUR 4.0 million) and lease liability in July 2025 when the lease term started.

In January–December 2025, capex was EUR 12.8 million (EUR 11.1 million) and was related to investments in technology and headquarter premises (EUR 0.7 million).

Acquisitions and financial arrangements

F-Secure hasn't made any acquisitions during the reporting period.

During the reporting period, in June 2025, F-Secure signed and withdrew a EUR 35 million loan with Nordic Investment Bank (NIB). The loan is the first step of refinancing the company's loan portfolio. The loan has a seven-year maturity, and the first two years of the loan are repayment-free. This extends the average maturity of the company's debt structure.

Financing package with Danske Bank A/S and OP Corporate Bank plc was extended in March 2025 and this loan matures in 2028. The financing package consists of two facilities, (i) a EUR 202 million amortizing term loan to finance the acquisition, and (ii) a EUR 20 million revolving loan facility to be used for general corporate purposes. During the reporting period, F-Secure has repaid EUR 45.0 million of the term loan in total: EUR 30.0 million of scheduled repayments and EUR 15.0 million of additional repayment. The revolving credit facility is undrawn at the reporting date.

Group structure and changes

F-Secure's subsidiary in Brazil, F-Secure do Brasil Tecnol. da Informãcao Ltda, was closed during 2025.

Loans, liabilities and guarantees from related parties

F-Secure Corporation's receivables from companies within the same group are presented in Note 12. Receivables of the parent company's financial statements. The company has not provided any other loans, liabilities, or guarantees to related parties.

Significant events during the financial year

F-Secure lowered full year 2025 revenue and adjusted EBITA outlook

On 8 July 2025, F-Secure lowered its outlook for the full year 2025 revenue and adjusted EBITA. From an operational perspective, the adoption of new security services by Tier 1 customers has progressed slower than expected. In addition, the closing of new Tier 1 deals, both with existing and new partners, has been delayed due to factors such as organizational changes, shifting priorities, limited resources, and evolving business cases.

More than 10 percent weakening of the U.S. dollar during the first half of the year has a strong

impact, resulting in a negative effect of more than EUR 3 million on full-year forecast compared to the level at the beginning of 2025.

The revised profitability guidance reflects the revenue decline outlined above. While cost control has remained disciplined, F-Secure's business model limits the ability to fully offset the lower revenue through cost reductions alone.

Despite these challenges, F-Secure maintains a strong opportunity pipeline and remains optimistic about future growth.

Updated outlook for 2025
Growth: F-Secure expects low single-digit currency-neutral revenue growth for 2025. Profitability: The group's adjusted EBITA margin is expected to be in the range of 32%–35% in 2025 (in 2024: 35.7%).

Previous outlook for 2025 was issued on 6 February 2025:
Growth: F-Secure expects mid-single digit revenue growth for 2025. Profitability: The group's adjusted EBITA is expected to be approximately on the same level as in 2024 (EUR 52.2 million).

Negotiations of a significant strategic partnership agreement with a leading Communications Service Provider

On 20 November, F-Secure announced that the company is negotiating a significant strategic partnership agreement with one of the world's leading Tier 1 Communications Service Providers (CSP). The ongoing negotiations relate to delivering F-Secure's embedded solutions to the customer. This agreement demonstrates F-Secure's capability to serve the world's leading CSP's with innovative, highly scalable cybersecurity services. The agreement under negotiation contains a minimum guaranteed revenue, starting from the service launch to customers. Negotiations are ongoing and the company will publish a release with additional details once the agreement has been signed. The launch is expected to take place in the second quarter of 2026.

Research and development

F-Secure Corporation research and development expenditure amounted to EUR 30.9 million (EUR 29.3 million) in 2025, representing 21.2% (20.0%) of revenue and 34.9% (33.1%) of all expenditures. Additionally, capitalized investments in technology were EUR 11.7 million (EUR 11.0 million).

In 2025, F-Secure's Technology function focused on scam protection, simplifying our product and systems landscape, improving delivery discipline, and strengthening the foundations for efficient growth and Tier 1 readiness. Our objective is clear: a technology base that supports consistent execution and a lower cost to serve, contributing to strong profitability over the long term. We also continued to invest in our distribution capabilities with partners. With the developments made in our standardized Software Development Kit (SDK) approach in 2025 we will scale to serve more Tier 1 partners in 2026. This "build once, deploy broadly" model is intended to scale reach while protecting unit economics.

A major theme throughout the year was advancing our "one platform, many segments" program. We continued to bring products onto a single, unified SaaS platform and SDKs that can support multiple customer segments. This reduces duplication, increases reliability, and allows us to direct more investment toward innovation. This remains in progress by design; as key technology cutovers complete during 2026.

Within our engineering work, we emphasized practical, AI-native efficiency. The use of assistive tools, internal data and model services, and repeatable methods helped targeted teams shorten delivery cycles and reduce rework. In teams adopting AI-assisted workflows, we saw around 30% improvement in cycle time; in selected new-build teams, time to initial capability improved by up to tenfold in pilots. We scaled these practices deliberately—prioritizing quality, security and service continuity. In parallel, we strengthened our internal data and automation foundations. This groundwork is not customer-facing or imminently visible on its own; its purpose is to enable a steady flow of product improvements in 2026 and beyond.

Our advances in scam protection were recognized with an AI award in 2025. We continued to deepen our understanding of online fraud through ongoing research and market assessment, including work on deepfake detection and cross-channel scams. These insights inform our product roadmap and partner discussions—supporting identity and account-protection features—and help us focus on areas that matter most to consumers and operators.

Looking ahead to 2026, our priorities are to complete the most important migrations, retire remaining legacy systems, and bring the gains from our internal foundations into visible product improvements. We will extend standardized partner integrations to additional operators and segments while maintaining a single platform and a single codebase. As capacity shifts from refactoring to new product work—particularly in the second half of 2026—we expect clearer operating leverage: lower structural costs, more predictable delivery, and a distribution model that scales efficiently across households and connected devices.

We are executing methodically, with a focus on cost discipline, service quality, predictable outcomes, and selected product innovation initiatives. The work we did in 2025 lays the groundwork for 2026 to harvest the benefits—supporting a simpler, faster, and more economical technology foundation aligned with long-term, stable profitability.

Personnel, management, board of directors and auditor and sustainability auditor of the company

At the end of December 2025, F-Secure had 549 (529) employees. The average number of personnel in 2025 was 526 (519). Wages and salaries were EUR 34.0 (36.1) million in 2025.

F-Secure's most important intangible resource is our personnel, which is critical for implementing our strategy. This includes i) our product and technology organizations, who ensure the competitiveness of our product portfolio and our ability to protect consumers' digital moments through research and innovation, ii) our sales, marketing, and services organizations, through which we can serve our partner segments and consumers. In addition, our business support organizations (e.g. corporate development, finance and people & culture) ensure our smooth daily operational activities.

In 2025, we built the foundation for F-Secure's AI-native future. We launched our AI Learning Academy, upskilling our entire organization in AI capabilities critical to our product innovation and partner service excellence. We fostered AI-experimentation and introduced AI-powered tools to enhance employee experience and team performance. Most significantly, we established the standards for high-performing teams across the organization, strengthening collaboration and accountability that accelerate our time-to-market and enhance our ability to protect consumers' digital moments. These changes position F-Secure as an agile, AI-first organization ready to lead in the evolving cybersecurity landscape.

Leadership team

During 2025 the following changes to F-Secure Leadership Team were announced:

- Toby White, Chief Technology Officer (CTO) and a member of the Leadership Team decided to leave F-Secure at the end of July, 2025.
- Santeri Kangas was appointed CTO and a member of the Leadership Team as of 1 October 2025.
- TL Viswanathan, F-Secure Chief Product Officer, served as interim CTO from August until 1 October 2025.
- Sari Somerkallio, CFO and a member of the Leadership Team, decided to leave the company on 30 April 2026.
- Robin Pulkkinen was appointed as Chief Financial Officer (CFO) and a member of the Leadership Team, and he will start in this position no later than June 2026.

After the review period, on 13 January 2026, company announced the appointment of a new Chief Strategy Officer (CSO). F-Secure's SVP, Corporate Development and a member of the Leadership Team, **Antero Norkio**, decided to leave the Company on 30 January 2026. **Jyrki Tulokas** was appointed CSO and a member of the Leadership Team of F-Secure Corporation, effective 2 February 2026.

At the end of December 2025, the composition of the Leadership Team was the following:

Timo Laaksonen	President & Chief Executive Officer
Santeri Kangas	Chief Technology Officer
Richard Larcombe	Chief Marketing Officer
Nina Lehto	Senior Vice President, Services
Antero Norkio	Senior Vice President, Corporate Development (until the end of January 2026)
Bruno Rodriguez	Chief Revenue Officer
Sari Somerkallio	Chief Financial Officer (until the end of April 2026)
Kaisa Tikka-Mustonen	Chief People Officer
TL Viswanathan	Chief Product Officer

The Board of Directors

Members of the Board of Directors of F-Secure are Pertti Ervi (Chair of the board), Alessandro Adriani, Roxana Diaconescu, Cornelia Schaurecker, Petra Teräsaho, Tommi Uitto and Rachit Mittal. Rachit Mittal belongs to the personnel of the F-Secure Corporation. One member of the Board of Directors is elected from among F-Secure personnel. An election is arranged annually for F-Secure personnel and each permanent employee, except the people belonging to the company's Leadership Team, is eligible to stand as a candidate. The representatives of the Board of Directors interview persons who have obtained the highest number of votes in the elections and choose a candidate from amongst them to be proposed for election as a member of the Board by the Annual General Meeting.

The term of office of members of the Board of Directors ends at the close of the annual general meeting of shareholders following their election.

Auditor and authorized sustainability auditor

The auditor and also authorized sustainability auditor of F-Secure Corporation is the Authorized Public Accountant PricewaterhouseCoopers Oy with Samuli Perälä, APA, as the auditor and authorized sustainability auditor with the principal responsibility.

Share-based incentive plans

F-Secure has share-based incentive plans for the key personnel of the company. The share-based long-term incentive plans include a Performance Share Plan (PSP), Performance Matching Share Plan (PMSP) and Restricted Share Plan (RSP) as a complementary share-based incentive plan for individually selected key employees in specific situations. Members of the Leadership Team and selected key employees can participate in either PSP or PMSP according to their choice, not both plans. The purpose of the share-based long-term incentive plans is to align shareholders' and management's interests, motivate and incentivize key individuals to focus on F-Secure's long-term success and targets and to commit key resources in the company.

In addition, F-Secure has an Employee Share Savings Plan (ESSP). The ESSP consists of annually commencing plan periods, each one comprising a 12-month savings period and a holding period following the savings period. The ESSP is offered to all F-Secure employees. The employees have an opportunity to save a proportion of their salaries and invest those savings in F-Secure shares. The savings are used for acquiring F-Secure shares quarterly after the publication of the respective interim reports. As a reward for the commitment, F-Secure grants the participating employees a gross award of one matching share for every two shares acquired with their savings. Continuity of employment and holding of acquired shares for the duration of the holding period are the prerequisites for receiving the award.

More information on the programs is provided in Note 19 Share-based payment transactions of the Financial Statements, as well as in the Remuneration Report, which is published separately from the Board of Directors report.

Shares and shareholders

Shares and share capital

At the end of December 2025, the registered share capital of F-Secure was 80,000 euros and the company had 174,707,070 fully paid shares. F-Secure has one share class and the company's shares are included in a book-entry system.

Information on the authorizations held by the Board of Directors in 2025 to issue shares and special rights entitling to shares, to transfer shares and repurchase own shares, is available in the section on the Annual General Meeting 2025.

Trading of shares

The closing price of the share at the end of December 2025 was EUR 1.93. In January–December 2025, the highest price paid was EUR 2.03 and the lowest EUR 1.59. In January–December 2025, the share's volume weighted average price was EUR 1.73. The share trading volume was EUR 80 million or 46 million shares. On 31 December 2025, the company's market capitalization was EUR 338 million.

Shareholders

The number of registered shareholders at the end of December 2025 was 35,317, including nominee registers. The proportion of nominee-registered and direct foreign shareholders was 9.52% of the company's shares at the end of the year. The list of the shareholders of F-Secure Corporation is based on the information given by Euroclear Finland Ltd.

Treasury shares

During or at the end of the financial year 2025, F-Secure did not hold any treasury shares.

Flagging notifications

During the financial year 2025, F-Secure has not received any flagging notification of change in holdings in accordance with Chapter 9, Section 10 of the Securities Market Act:

Short-term risks and uncertainties

Risks related to F-Secure's operating environment

Intensifying competition in the consumer security market could lead to a general decline in the price level and affect F-Secure's ability to maintain or increase its market share, and the intensifying competition could thus have an adverse effect on F-Secure's revenue, profitability, and market share.

F-Secure may not be able to keep up with rapid changes in customer demand, distribution channels, technologies such as AI and the evolution of consumer cybersecurity threats such as scams, which could have an adverse effect on F-Secure reputation, competitiveness, operational results and financial position.

Uncertainty about F-Secure's key markets, financial markets and general economic situation could have an adverse effect on F-Secure's business and growth opportunities and reduce the demand or increase the cost of the products and services offered

by F-Secure. Geopolitical instability has increased uncertainty in the world and the risk of unexpected disruptions of the world economy. For example, the war in Ukraine has caused some exceptional consequences to the cybersecurity landscape, such as highly visible governmental activities, as well as organized civilian response to the war efforts. In addition, there is a risk that F-Secure may be indirectly affected by escalating trade war (“tariffs”) that may increase inflation, reduce consumer purchasing power or otherwise negatively affect consumers and F-Secure's channel partners.

Risks related to F-Secure’s business operations and strategy

If F-Secure’s agreement with a significant business partner or Channel Partner is terminated or expires, or if F-Secure is unable to continue to work with a business partner or Channel Partner on acceptable terms, or if a channel partner fails to fulfill its obligations, this could significantly reduce F-Secure's revenues, increase its costs, hinder its operations and weaken its ability to provide services or solutions to its customers. In addition, some Channel Partners may be slow to adopt new solutions, which may delay F-Secure's revenue growth or increase maintenance-related costs.

The loss of key personnel and skilled employees, the possible delay in new hires or increase in personnel expenses could weaken F-Secure’s profitability and the standard of its services or solutions, hinder operations and prevent F-Secure from successfully developing and growing its business, including effective and differentiating innovation strategy.

Actual, possible, or perceived defects, disruptions or vulnerabilities in F-Secure products or services, including risks from usage of AI technologies, could lead to security breaches or cybersecurity attacks and errors. Such incidents may also result from errors or misuse by F-Secure employees or business partners. These issues could harm F-Secure or its customers' reputation, reduce sales, disrupt operations, tie up personnel resources, lead to contractual penalties or regulatory fines and increase other costs.

F-Secure channel partners may not always promote the latest version of our product offering, and end customers on various channels may be using older product versions ("legacy products"). Supporting these legacy products may increase F-Secure costs or adversely affect planned future product releases, their scope, availability and/or competitiveness, while migrating end-customers to the latest product versions may take time, require additional investments, and thus affect revenue growth.

F-Secure provides consumer cybersecurity solutions to some of the largest Service Providers in the world (“Tier 1 Channel Partners”) and aims to win new Tier 1 Channel Partner contracts. Tier 1 Channel Partners may require solutions that F-Secure is unable to develop, deliver and maintain at the expected level of profitability. These contracts may also expose F-Secure to Service Level Agreement claims (support penalties) or other similar and material contractual liabilities, such as related to a consumer data breach. F-Secure may be required to make upfront investments to develop and deliver these solutions, which may have a negative impact on F-Secure product roadmaps, company revenues and profitability.

F-Secure is in the process of transforming the company and its operating model with its growth strategy and taking advantage of AI capabilities in our offering and business processes. Changes in the company's strategic priorities, structure and processes may take time to become effective. Additionally, these strategic investments and changes may at least initially have a negative impact on the company's product roadmap and its operations. These combined can have a negative impact on the financial outlook of the company.

Risks related to the technology used by F-Secure, intellectual property rights and other regulations

Any malfunction in technologies, IT systems or network connections used by F-Secure or any security breaches could result in disruption of F-Secure's service offerings. F-Secure may fail to register, protect, manage, maintain and enforce its intellectual property rights, and F-Secure may be subject to intellectual property infringement claims, which may result in significant costs. Leakage of personal data collected by F-Secure may have a material adverse effect on F-Secure’s business and reputation and result in claims for damages as well as fines and orders imposed by the authorities. As is customary in the cybersecurity industry, F-Secure protection is a combination of its own IPR and third-party solutions. F-Secure continues to have a relationship with Lookout and WithSecure for certain protection capabilities after the Lookout Life acquisition and Withsecure demerger. The inability of third parties such as Lookout or WithSecure to provide these protection capabilities could have a material adverse effect on F-Secure’s business and its customers.

Risks related to F-Secure´s financial position and financing

The number of operations and locations outside the eurozone in different currencies exposes F-Secure to a risk related to currency fluctuations. Changes in the exchange rates between currencies could have an adverse effect on F-Secure’s revenue, results and

financial position. F-Secure is exposed to transaction risks caused by purchasing and selling products and goods in currencies that are not F-Secure's home currencies, in particular the US dollar. In addition, F-Secure is exposed to investment risks in its units abroad and translation risks that arise when investments in subsidiaries in different currencies are converted into F-Secure's operational currency, i.e., the euro. Furthermore, F-Secure financed the acquisition of Lookout's consumer security business with bank debt subject to leverage covenants. Failure to comply with the covenants would lead to early expiry of the debt. Changes in interest rates have an impact on interest costs.

Significant events after the review period

After the review period, on 13 January 2026, company announced the appointment of a new Chief Strategy Officer (CSO). F-Secure's SVP, Corporate Development and a member of the Leadership Team, **Antero Norkio**, decided to leave the Company on 30 January 2026. **Jyrki Tulokas** was appointed CSO and a member of the Leadership Team of F-Secure Corporation, effective 2 February 2026.

On 4 February 2026, F-Secure Board's Personnel and Nomination Committee gave proposals to the Annual General Meeting scheduled for 25 March 2026 for the composition and remuneration of the Board of Directors. The Board's Personnel and Nomination Committee proposes to that the Board of Directors consists of a total of seven (7) members and that the following persons be elected as members of the Board of Directors for a term expiring at the end of the Annual General Meeting 2027: Alessandro Adriani, Roxana Diaconescu, Pertti Ervi, Cornelia Schaurecker, Petra Teräsaho, Tommi Uitto are proposed to be re-elected as members. As F-Secure personnel member to-be-elected, the Personnel and Nomination Committee proposes Wilhelm Lamptey.

The Personnel and Nomination Committee proposes to the Annual General Meeting that the following annual remuneration be paid to the members of Board of Directors to be elected at the Annual General Meeting: EUR 80,000 annually for the Chair of the Board of Directors; EUR 38,000 annually for the external members of the Board of Directors; EUR 12,667 for members employed by F-Secure; EUR 10,000 additional remuneration for the Audit Committee Chair; EUR 4,000 additional remuneration for the Personnel and Nomination Committee Chair; EUR 2,000 additional remuneration for the members of Audit Committee as well as Personnel and Nomination Committee. The proposed annual fee and the fees for Committee work correspond to the current remuneration. In addition, The Personnel and Nomination Committee proposes that approximately 40 percent of the remuneration be paid as shares in the company repurchased from the market or as treasury shares held by the company.

Annual General Meeting 2025

The Annual General Meeting of F-Secure Corporation and organizational meeting of the Board of Directors was held on 1 April 2025. The Annual General Meeting adopted the annual accounts and the consolidated annual accounts for the financial year that ended on 31 December 2024, discharged the members of the Company's Board of Directors and the CEO from liability, and approved all proposals made to the Annual General Meeting by the Board of Directors. The Annual General Meeting also approved the 2024 remuneration report for governing bodies. The resolution is advisory according to the Finnish Companies Act.

The Annual General Meeting resolved that for the financial year that ended on 31 December 2024, a dividend of EUR 0.04 per share to be paid in two instalments of EUR 0.02 per share each.

More detailed information regarding the decisions and board composition can be found in the stock exchange release published 1 April 2025. Similarly, the minutes of the Annual General Meeting are available on the company's website at https://www.investors.f-secure.com/en/ investors/corporate_governance/governing_model/annual_general_meeting_2026

Outlook for 2026

Growth: F-Secure expects mid to high single-digit currency neutral revenue growth for 2026.

Profitability: The group's adjusted EBITA is expected to be EUR 44–50 million in 2026 (2025: EUR 50.3 million).

Background for the outlook:

- F-Secure expects the core consumer cybersecurity market to grow mid-single digit CAGR mid- to long-term[1]. F-Secure sees the potential to grow faster than the market, focusing on partner channel and its offering around Embedded security and Scam Protection. The growth may be moderated by uncertainties around consumer sentiment in certain markets and general economic volatility.
- Partner business and especially Embedded Security solutions are expected to drive F-Secure growth during 2026. Growth is expected to accelerate throughout the year as the most significant new Tier 1 services gradually start to generate revenue and support profitability.

[1] Industry analyst views such as Gartner and IDC, and F-Secure management estimates.

- Direct business revenue development is expected to be negative due to continued strategy of refraining from paid customer acquisition. Focus is on improving retention rate and ARPU.
- Gross margin is expected to be slightly lower than in 2025 (84.7%) due to growth of strategic partners with Embedded Security solutions, as these typically have a lower gross margin level than F-Secure Total business.
- F-Secure continues to develop its service, operations and production capabilities further to meet Tier 1 partner requirements. These efforts are reflected in the higher cost base. As business scales up we expect to leverage continued service level investments across a wider partner base, leading to positive Adjusted EBITA % development along with business growth.
- Capex level is expected to remain on a similar or slightly higher level as in 2025 related to both product development as well as technology infrastructure improvements.

Financial targets

F-Secure's medium-term financial targets and dividend policy reflect the company's growth ambitions and strategic direction.

- **Growth:** High single digit growth (CAGR) with additional significant upside from major Tier 1 deal
- **Profitability:** Adjusted EBITA margin approaching 40% as revenue reaches EUR 200 million
- **Dividend Yield:** Around or above 50% of net profit; which can be adjusted as long as leverage is higher than the targeted level
- **Leverage:** Net debt / adjusted EBITDA ratio below 2.5x, excluding temporary impact from acquisitions

F-Secure Corporation follows the Rule of 40 metric as internal performance measurement and guiding principle, according to which the combined revenue growth rate and profitability margin should be equal to or greater than 40%.

Corporate Sustainability Statement

F-Secure has prepared its Sustainability Statement in accordance with the EU Corporate Sustainability Reporting Directive (CSRD) and the related Finnish legislation. The statement is published with this Board of Directors' Report; (Sustainability statement 2025).

Annual General Meeting 2026

The Annual General Meeting 2026 is scheduled for Wednesday, 25 March 2026. The Board of Directors will convene the meeting with separate stock exchange release.

Board of Directors' proposal for the distribution of profit

According to the company's dividend policy, F-Secure aims to pay around or above 50% of net profit as dividend on an annual basis, which can be adjusted as long as leverage is higher than the targeted level (2.5x). On 31 December 2025 distributable funds of F-Secure Corporation were EUR 15.2 million. As the leverage (2.8x) is above the target level, the Board of Directors proposes to the Annual General Meeting 2026 that a dividend of EUR 0.04 per share to be paid. Earnings per share (EPS) for the period January–December 2025 was EUR 0.13, and the proposed dividend is 31.2% of the group January– December 2025 earnings. The dividend is proposed to be paid in two instalments.

No material changes have occurred in the company's financial position since the end of the financial year.

Key figures

EUR million	2025	2024	2023	2022	Carve-out 2021
Revenue	145.7	146.3	130.4	111.0	106.3
Revenue growth %	-0.4%	12.2%	17.4%	4.5%	6.1%
Adjusted EBITDA	51.9	53.5	45.7	44.5	47.4
% of revenue	35.6 %	36.6 %	35.0 %	40.1 %	44.6 %
EBITA	50.4	50.8	36.6	40.2	44.8
% of revenue	34.6%	34.7%	28.1%	36.2%	42.2%
Adjusted EBITA	50.3	52.2	44.6	43.9	47.2
% of revenue	34.5 %	35.7 %	34.2 %	39.6 %	44.4 %
EBIT	35.5	38.4	29.5	38.8	43.5
% of revenue	24.4 %	26.3 %	22.6 %	34.9 %	40.9 %
Profit before taxes	27.5	27.0	27.7	38.6	43.6
% of revenue	18.9 %	18.5 %	21.2 %	34.7 %	41.0 %
Result for the period	22.4	21.1	22.4	30.2	34.4
% of revenue	15.3 %	14.4 %	17.2 %	27.2 %	32.4 %
R&D costs	30.9	29.3	27.5	16.4	16.9
% of revenue	21.2 %	20.0 %	21.1 %	14.8 %	15.9 %
Capital expenditure	12.8	11.1	7.9[1]	4.6	1.7
% of revenue	8.8 %	7.6 %	6.1 %	4.2 %	1.6 %
Operating cash flow	43.6	38.8	30.1	36.4	36.1
Net debt (+)/Net cash (-)	145.6	163.6	177.4	-19.3	0.2
Equity ratio %	21.5 %	17.4 %	12.0 %	39.6 %	24.5%
Cash conversion	79.1 %	80.5 %	81.2 %	96.2 %	95.6%
Wages and salaries	34.0	36.1	33.3	20.8	16.1
Personnel on average	526	519	484	368[2]	245[3]
Personnel on Dec 31	549	529	524	376	248

1) Excluding acquisition

2) Average number of personnel for 2022 represents the average employees after demerger (July-December 2022).

3) For carve-out period the average number of personnel consists of direct personnel working in the Consumer Security Business.

The key figures are presented combining actuals and carve-out basis for 1-12/2022 and on an actuals basis for financial position at 31 December 2022. For period 2021 financial information is on carve-out basis.

F-Secure

Key ratios	2025	2024	2023	2022
Earnings / share (EUR)	0.13	0.12	0.13	0.17
Earnings / share diluted (EUR)	0.13	0.12	0.13	0.17
Shareholders' equity per share (EUR)	0.32	0.27	0.19	0.14
Dividend per share (EUR)	0.04[1)]	0.04	0.07	0.07[2)]
Dividend per earnings (%)	31.2 %	33.2 %	54.7 %	41.2 %
Effective dividends (%)	2.1 %	2.2 %	3.4 %	2.5 %
P/E ratio	15.1	22.9	27.7	16.4
Share price, lowest (EUR)	1.59	1.67	1.64	2.29
Share price, highest (EUR)	2.03	2.33	3.44	3.26
Share price, average (EUR)	1.73	1.95	2.35	2.68
Share price Dec 31	1.93	1.78	2.04	2.83
Market capitalization (MEUR)	337.9	311.6	355.5	494.0
Trading volume (millions)	79.9	44.8	39.0	15.8
Adjusted number of shares				
average during the period	174,682,268	174,673,165	174,647,528	174,526,944
average during the period, diluted	175,453,056	174,924,124	174,526,944	174,526,944
Dec 31	174,707,070	174,673,165	174,673,165	174,526,944
Dec 31, diluted	175,691,907	175,243,726	174,526,944	174,526,944

1) Board proposal for 2025

2) For 2022 dividend distribution was based on July-December 2022 net profit and 78% from July-December earnings.

Reconciliation between adjusted EBITDA, EBITDA, adjusted EBITA, EBITA and EBIT

EUR 1,000	2025	2024
Adjusted EBITDA	**51,907**	**53,480**
Adjustments to EBITDA		
Costs related to restructuring	75	-1,438
EBITDA	**51,982**	**52,042**
Depreciation and amortization	-16,443	-13,621
EBIT	**35,538**	**38,422**
Adjusted EBITA	**50,312**	**52,248**
Adjustments to EBITA		
Costs related to restructuring	75	-1,438
EBITA	**50,387**	**50,810**
Amortization	-6,930	-4,573
PPA amortization	-7,919	-7,816
EBIT	**35,538**	**38,422**

Calculation of key figures

Key figure	Definition	
Currency neutral revenue	((Current period revenue at constant rates - Prior period revenue)/Prior period revenue) x 100	
EBITDA	EBIT + Depreciation, amortisation and impairment	
EBITA	EBIT + Amortisation and impairment	
EBIT	Result before taxes and net financial items	
Adjusted EBITDA	EBITDA before items affecting comparability	
Adjusted EBITA	EBITA before items affecting comparability	
Items affecting comparability	Items affecting comparability are associated with restructuring, acquisition and cost related to listing	
Operating expenses	Sales and marketing, research and development, and administration expenses	
Capital expenditure	Corresponds to the Statement of Cash Flow line item Investments in intangible and tangible assets	
Operating cash flow	Corresponds to the Statement of Cash Flow line item Cash flow from operations	
Net debt (+) / Net cash (–)	Interest-bearing liabilities – Interest-bearing receivables – Cash and cash equivalents	
Equity ratio, %	Total equity / Total assets	× 100

Key figure	Definition	
Cash conversion, %	(Adjusted EBITDA – Capital expenditure –/+ Change in net working capital) / Adjusted EBITDA	× 100
Earnings per share, EUR	Profit attributable to equity holders of the company / Weighted average number of outstanding shares	
Earnings per share, excluding PPA, EUR	(Profit attributable to equity holders of the company + PPA amortization adjusted by tax impact) / Weighted average number of outstanding shares	
Shareholders' equity per share, EUR	Equity attributable to equity holders of the company / Number of outstanding shares at the end of period	
P/E ratio	Closing price of the share (at period end) / Earnings per share (annualized)	
Gearing, %	(Interest-bearing liabilities – cash and bank) / Total equity	× 100

Shares and Shareholders

Shares and share ownership distribution, 31 Dec 2025

Shares	Number of shareholders	% of shareholders	Total shares	% of shares
1-100	10,738	30.40%	462,291	0.26%
101-1 000	18,019	51.02%	7,068,256	4.05%
1001-50 000	6,462	18.30%	25,453,859	14.57%
50 001-100 000	43	0.12%	3,039,620	1.74%
100 001-	55	0.16%	138,683,044	79.38%
Total	**35,317**	**100.00%**	**174,707,070**	**100.00%**

Shareholders by category, 31 Dec 2025	Total shares	% of shares
Private individuals	92,523,560	52.96%
Pension & Insurance companies	29,710,678	17.01%
Fund companies	24,399,385	13.97%
Companies	9,814,336	5.62%
Foundations	1,553,806	0.89%
Nominee registered	16,040,801	9.18%
Others	664,504	0.38%
Total	**174,707,070**	**100.00%**
Own shares F-Secure Corporation		
Total	**174,707,070**	**100.00%**

Largest shareholders and administrative register

Owner	Shares	% of shares	% of votes
Risto Siilasmaa	60,035,288	34.36%	34.36%
Nordea Nordic Small Cap Fund	11,584,976	6.63%	6.63%
Ilmarinen Mutual Pension Insurance Company	6,273,663	3.59%	3.59%
Varma Mutual Pension Insurance Company	3,970,660	2.27%	2.27%
The State Pension Fund of Finland	3,900,000	2.23%	2.23%
Mandatum Life Insurance Company Ltd	3,896,136	2.23%	2.23%
Investment fund Aktia Capital	3,425,164	1.96%	1.96%
Danske Invest Finnish Equity Fund	3,264,981	1.87%	1.87%
Proprius Partners Micro Finland	3,100,000	1.77%	1.77%
Säästöpankki Kotimaa investment fund	2,762,499	1.58%	1.58%

Administrative register	Shares	% of shares	% of votes
Skandinaviska Enskilda Banken	8,715,743	4.99%	4.99%
Citibank Europe Plc	6,244,666	3.57%	3.57%
Other registers	1,080,392	0.62%	0.62%
Other shareholders	158,666,269	90.82%	90.82%
Total	**174,707,070**	**100.00%**	**100.00%**

Ownership of management

Board of Directors	Shares	% of shares
Pertti Ervi	140,232	0.08%
Petra Teräsaho	33,875	0.02%
Tommi Uitto	17,325	0.01%
Alessandro Adriani	9,362	0.01%
Roxana Diaconescu	9,362	0.01%
Cornelia Schaurecker	9,362	0.01%
Rachit Mittal	2,964	0.00%
Total	**222,482**	**0.13%**

Leadership team	Shares	% of shares
Antero Norkio	70,017	0.04%
Timo Laaksonen	49,986	0.03%
Sari Somerkallio	20,099	0.01%
Richard Larcombe	15,100	0.01%
Viswanathan Tirunillai	5,883	0.00%
Nina Lehto	3,556	0.00%
Kaisa Tikka-Mustonen	2,134	0.00%
Bruno Rodriguez		0.00%
Santeri Kangas		0.00%
Total	**166,775**	**0.10%**

Group Sustainability Report

GROUP SUSTAINABILITY REPORT -

General

Reporting principles

BP-1 Basis for preparation

This group sustainability report has been prepared in accordance with the Accounting Act Chapter 7 and European Sustainability Reporting Standards (ESRS). The F-Secure group sustainability report has been prepared on a consolidated basis, and it covers the F-Secure Group with the same scope as our financial statements. The statement includes information on material Impacts, Risks and Opportunities (IROs) connected with our direct and indirect business relationships in our upstream and downstream value chain.

F-Secure has not omitted any information corresponding to intellectual property, know-how or innovation results, nor used the exemption from disclosure of impending developments in negotiations.

BP-2 Disclosures in relation to specific circumstances

Planning horizon

F-Secure defines short-term as 0-1 years, medium-term as 1-3 years, and long-term as 3+ years, aligning with our strategic planning cycles.

Value chain estimation

For GHG emissions, we use value chain estimations where actual data is unavailable, following GHG Protocol methodology. We aim to improve data quality by moving from estimations to actual emission data through stakeholder collaboration.

The quantification of GHG emissions in F-Secure's emissions is systematical and any uncertainties have been reduced as far as practical. Consistent methodology has been used to allow for meaningful comparisons of emissions over time. Any changes to the data, inventory boundary, methods, or any other relevant factors are documented. It is usual to use estimations and sector averages in GHG calculation in cases where actual data is unavailable.

Section E1-6 Gross Scopes 1, 2, 3 and Total GHG emissions provides more detailed information on methodology and value chain estimation.

Sources of estimation and outcome uncertainty

GHG emission calculations contain uncertainty, particularly for Scope 3. Our limitations include restricted site-specific consumption data for Scope 2 and spend-based calculations for key Scope 3 categories. In Scope 1, leased cars data is limited, and the calculations have been done based on estimating contract kilometres and average consumption of car models. Section *E1-6 Gross Scopes 1, 2, 3 and Total GHG emissions* provides more detailed information on methodology and estimation uncertainty. Additional uncertainties exist in cybersecurity metrics objectivity. Section *S4-5 Progress towards targets* provides more detailed information on methodology and estimation uncertainty. Finally, the measurement of the metrics in this group sustainability report has not been validated by an external body apart from the assurance of this Group sustainability report, unless specifically stated otherwise under the disclosure requirement section of such metrics.

The reported Code of Conduct training target excludes individuals for whom employee status information is unavailable.

Forward-looking statement

Forward-looking information should be considered with caution as it's subject to risks and uncertainties that could impact our ability to achieve the described objectives or anticipated results.

Changes in preparation or presentation of sustainability information

F-Secure has chosen to change the E1 scope 3 related target of absolute emission reduction of 42% to emission intensity reduction of 52% between 2024 and 2030. The change has been made due to business growth compatibility, and it allows for better comparisons between different companies. We will continue to report absolute emission reduction of scope 3 in section E1-6 Gross Scopes 1, 2, 3 and Total GHG emissions.

Continue to report qualitative information but drop from Consumers and end-users S-4 targets the "*Ratio of externally reported vulnerabilities compared to internally reported vulnerabilities*" due to data quality issues affecting annual comparability.

The 2024 cybersecurity training completion rate initially excluded employees on extended leave. This has been corrected in 2025, and the 2024 cybersecurity training completion rate has been updated to include all employees.

Reporting errors in prior periods

The nature of the error was that calculation method for disclosure in table S1-9 Gender distribution was updated based on approved targets. In prior period section S1-5 Own workforce targets gender diversity (directors including leadership team, %) percentage for females was 25,1% and male 74,9%. Those were corrected this reporting period and corrected figures are female 23,5% and male 76,5 %.

The nature of the error was that calculation method for disclosure S1-13 Training was updated. In prior period section S1-5 Own workforce targets and career review target percentage was 82%. That was were corrected this reporting period and corrected figure is 88%.

Disclosures stemming from other legislation or reporting pronouncements

F-Secure has included in the Group sustainability report disclosures in section S4 Consumers and End-users related to the following legislation, standards and international principles:

1. Cybersecurity policy-related metrics and targets including cybersecurity training, cybersecurity incidents and bug bounty program, based on

- EU General Data Protection Regulation
- ISO 27001 information security management standard

2. Code of Conduct policy- and practice-related metrics, anti-corruption incidents and code of conduct training also based on (see section ESRS S4-1 for further details)

- OECD Guidelines for multinational enterprises
- United Nations Global Compact
- United Nations Guiding principles on Business and Human rights
- United Nations Convention against Corruption
- International Bill of Human Rights
- The Declaration of the International Labour Organization on Fundamental Principles and Rights at Work

Incorporation by reference

F-Secure calculates GHG intensity based on net revenue by dividing total GHG emissions (t CO_2eq) by net revenue (€). Net revenue is based on our financial statement (Cross-reference to financial section 3. Revenue).

The measures provided in the group sustainability report own workforce section are aligned with related data provided in other sections of the annual report noting that average annual number of personnel is used in the financial statement (Cross-reference to financial section 7. Personnel expenses).

Phase-In provisions

As a company with fewer than 750 employees in reporting year of 2025, we've omitted certain information required by ESRS E1 and ESRS S1 in accordance with Appendix C of ESRS 1.. F-Secure has chosen to omit the information prescribed by ESRS 2 SBM-3 paragraph 48(e) anticipated financial effects based on European Sustainability Reporting Standards 'quick-fix' delegated act of 11 July 2025. In addition, F-Secure has in our 2025 statement decided to omit matters related to "E1-9 Anticipated financial effects from material physical and transition risks and potential climate-related opportunities". Related to our own workforce (S1), we've omitted "S1-7 Characteristics of non-employees in the undertaking´s own workforce" in full and "S1-14 Health and safety metrics" partially.

Governance

GOV-1 The role of the administrative, management and supervisory bodies

In this Group sustainability report, 'supervisory bodies' refer to the F-Secure Board of Directors, its Audit Committee and Personnel and Nomination Committee. 'Management body' refers to the F-Secure Leadership Team, including the CEO and leadership team members. The Board oversees company administration and appoints the CEO, who manages daily operations per Board instructions.

The highest decision-making body is the General Meeting of Shareholders, which elects Board members. The Board is responsible for F-Secure Group administration and the appropriate organization of its operations. The Board's duties are defined according to the Articles of Association, Finnish Companies Act, and other applicable laws and regulations, including overseeing business conduct and compliance, and approving significant governance policies.

Roles and Responsibilities

The Board has established an Audit Committee and a Personnel and Nomination Committee to enhance efficiency. The Audit Committee monitors risk management, internal controls, IT strategy, sustainability, and financial reporting, as well as auditing. Most committee members must be independent from the company, and at least one must be independent from significant shareholders. The Personnel and Nomination Committee prepares matters on Board composition and compensation, actively seeking qualified new Board members.

The Board and Leadership Team are supported by the Legal Team, which maintains business conduct policies and provides related training. Each Leadership Team member supervises policy implementation in their respective functions.

Composition and Diversity Information

As of 31 December 2025, F-Secure had 9 executive members in its management body and 7 non-executive members in its supervisory body (Board of Directors).

Board of Directors composition	2024	2025
Non-executive members	6 non-executive	6 non-executive
Employee representation	One Board member elected from personnel with term ending at next AGM	One Board member elected from personnel with term ending at next AGM
Experience relevance	Board members have international experience from technology, telecom, and cybersecurity sectors across Europe, North America, APAC/Japan	Board members have international experience from technology, telecom, and cybersecurity sectors across Europe, North America, APAC/Japan
Board gender diversity	Female: 33.3 (2), Male: 66.7% (4)	Female: 42.8% (3), Male: 57.2% (4)
Independent Board members	~67% (4 of 6 members independent from company and major shareholders)	~85.7% (6 of 7 members independent from company and major shareholders)

Table1. Composition and Diversity Information.

The Diversity Principles established by the Board strive for appropriately balanced gender distribution and diverse backgrounds. The Board comprises members aged 44-68 years with five different nationalities represented.

Access to Expertise on Sustainability Matters

The Board of Directors has received ESG training in 2024 to build appropriate skills and expertise to oversee sustainability matters. The training included information about the relevant EU-related regulations and the related responsibility of the Board of Directors. In addition, the training included information about the Double Materiality Assessment and third-party assurance of the Group sustainability report.

Additionally, a member of the Board who is also the current Chair of the Audit Committee has previous expertise in establishing sustainability-related reporting practices. Our financial assurer has the option to participate in Audit Committee meetings when ESG topics are reviewed, providing further access to ESG knowledge to the F-Secure Audit Committee. F-Secure Sustainability Council drives the ESG agenda across the company, with the Chair having previous experience in ESG-related matters, while our Chief People Officer similarly has previous experience in ESRS reporting.

ESG Governance Structure

Board of Directors

- Reviews and approves the company's strategy, business model and related targets, which include ESG.
- ESG progress and achievements reported to the Board annually.
- The Board reviews remuneration policies aligned to ESG requirements.

Audit committee

- Review related strategy and activities
- Review sustainability related policies including ESG reporting, Corporate Governance, Cyber Security, and Risk Management
- Other duties assigned to AC under applicable law relating to sustainability reporting

Leadership Team

- Responsible for establishing and reviewing company sustainability strategy and business model
- Ensures that ESG is part of company culture and approves policies and principles
- Risk Management review conducted minimum twice a year
- Reviews annual sustainability statement, targets and metrics

F-Secure Sustainability Council

- Identify and assess ESG impacts, risks and opportunity
- Develop and implement sustainability strategies and preparation of annual sustainability statement
- Propose targets and metrics, and develop policies & principles
- Drives ESG compliance, and provides views on certifications and standards
- Ensures required stakeholder engagement in matters related to ESG

ESG Function
Leading Sustainability Council and facilitating sustainability strategy execution and reporting. Together with Legal function ensures ESG activities meet regulative requirements.

General Counsel
Align ESG governance with the overall corporate governance and Code of Conduct and other relevant policies.

ESG Committee

DEI
Reviews and sets ambition on DEI related plans. Evaluates and provides feedback on progress.

Wellbeing[1]
Reviews and sets ambition on wellbeing related plans. Evaluates and provides feedback on progress.

Environment
Driving environmental initiatives and climate change related targets.

Topics covered by Sustainability council

Donations & Sponsorship
Reviews and set principles for allocations of corporate donations and sponsorship.

Customers and end-users
Reviews and sets ambition on stakeholder sustainability. Specific task force appointed.

Business conduct
Ensure that ESG governance is aligned with the overall corporate governance and Code of Conduct.

Figure 1. ESG governance at F-Secure

ESG oversight is organized in layers:

1. Board of Directors: Reviews/approves strategy with ESG elements; updated at least annually on ESG progress
2. Audit Committee: Monitors ESG reporting, risks, and internal controls; reviews group sustainability report preparation and external assurance
3. Leadership Team: Establishes ESG strategy, ensures integration with company culture, approves policies and principles
4. Sustainability Council: Facilitates ESG strategy implementation, identifies/assesses ESG impacts and risks, drives sustainability reporting
5. Sustainability Function: Leads Sustainability Council and facilitates sustainability strategy implementation and ensures regulatory compliance
6. ESG Committees: Drive specific ESG initiatives (DEI, Wellbeing, and Environment)

The Sustainability Council typically meets monthly with key members, including the CFO, CPO, Legal Counsel, SVP of Corporate Development, and the Sustainability function lead. The Council includes participants from other functions like sales and product management.

The ESG Committees works in close collaboration with the sustainability function lead. ESG committees drive initiatives related to their respective topics through committee meetings to define and progress actions. Each ESG committee reports to the Sustainability Council at least twice annually. These progress updates include reviews of actions and targets. The ESG committees also participate in the annual IRO review process.

ESG activities are fully integrated with the company strategy and based on F-Secure values, Code of Conduct, and related policies. Management of identified IROs is conducted at least once a year by the Sustainability Council, with results shared with the Audit Committee for review and oversight. In the sustainability council, targets related to the IROs are proposed, and they are reviewed by the Audit Committee and Board of Directors and approved by the Leadership team. Targets are monitored in sustainability council meetings at least twice a year and reviewed by the Audit Committee and Board of Directors at least once a year.

GOV-2 Information provided to and sustainability matters addressed by F-Secure administrative, management and supervisory bodies

Information flow and frequency

The F-Secure Board reviews ESG annually, while the Audit Committee discussed ESG in 2 of 5 meetings during 2025. Updates on ESG topics to the Board, the F-Secure Leadership team, and the Audit Committee have been presented by the SVP of Corporate Development based on input from the monthly Sustainability Council meetings, which include key management representatives (CFO, CPO, Legal Counsel), the sustainability function, and other function representatives. Updates include F-Secure ESG plans and actions, policies and targets, and reports on their progress, as well as implementation of due diligence.

Consideration of IROs when overseeing company strategy and risk management

Sustainability-related risks and impacts are managed as part of F-Secure's risk management process. The primary goal is to enable the organization to identify and manage risks effectively by monitoring potential negative impacts and the likelihood of various situations arising from operations, markets, customers, and partners.

F-Secure encourages continuous risk assessment by personnel. Operational risks identified through this process are regularly reviewed by each function, including bi-annual reviews with the CEO, Leadership Team, and Audit Committee. Positive impacts and opportunities are embedded into the strategy process and considered during operating plan reviews.

Trade-offs related to IROs are evaluated during strategy development, weighing costs and benefits of different options to ensure alignment with organizational goals and stakeholder expectations. This approach ensures that sustainability considerations are integrated into company decision-making while balancing potential risks and opportunities.

Material Topics Addressed in 2025

In addition to the F-Secure Sustainability Council and its ESG committees, the respective management members and supervisory bodies have addressed the following material topics:

Standard	Type	Description	Supervisory	Management
Environment	Potential positive impact (OO)	Implementation of green coding principles can reduce battery use in consumer devices and computational power in cloud environments	No	Yes
	Risk (DVC/OO)	Failure to meet climate change mitigation targets may negatively impact channel business	Yes	Yes
Social	Actual positive impact (OO)	Protect consumers' digital moments with relevant, effective cybersecurity solutions	Yes	Yes
	Actual positive impact (DVC, OO)	Create awareness about cybercrimes through campaigns, and events	No	Yes
	Actual positive impact (OO)	Family leaves (sometimes exceeding local requirements) and enhancing work life balance of employees.	No	Yes
	Actual positive impact (OO)	Promote gender equality through recruitment and gender pay gap mitigation	No	Yes
	Actual positive impact (OO)	Further ramp up strategic learning and development activities and track investment into learning activities.	Yes	Yes
	Actual positive impact (OO)	Foster inclusive culture with speak-up environment where workplace is safe for everyone	Yes	Yes
	Potential positive impact (OO)	Continuously identify the internal competencies critical to our strategy	No	Yes
	Opportunity (OO)	Evolving threat landscape, protecting consumers against evolving threat landscape (for example scams) benefits both F-Secure and partners	Yes	Yes
	Opportunity (OO)	Use data and AI in security applications, for more effective protection and better user experience. AI-powered (network) monitoring tools can track user behavior, detect anomalies, and react accordingly.	Yes	Yes
	Opportunity (OO)	Enhance employer reputation through DEI activities to attract younger generations	Yes	Yes
	Opportunity (OO)	Use of AI in workforce development, including process improvements, competency maturity and AI sentiment	Yes	Yes
	Risk (DVC)	Channel strategy, significant agreement changes or existing partner loss can negatively impact outlook	Yes	Yes

Standard	Type	Description	Supervisory	Management
Governance	Risk (OO)	Decreasing consumer willingness to pay for premium security due to competition/economic situation	No	Yes
	Risk (OO)	Talent acquisition and retention, loss of key persons or inability to acquire new talent	Yes	Yes
	Risk (OO, DVC/UVC)	Security vulnerabilities from suppliers and partners, relying on external vendors, especially vendors who are one step removed in the supply chain, adds layers of vulnerability.	Yes	Yes
	Risk (OO)	Cybersecurity attacks impacting reputation and business	Yes	Yes
	Risk (OO)	Mental health related absences detected.	No	Yes
	Risk (OO)	AI increases risk of security breach, effective AI experimentation and roll-out dependent on high quality data sources and may also increase risk of a security breach.	Yes	Yes
	Actual positive impact (OO/DVC)	Whistleblower channel available to all employees and business partners, with awareness raised through mandatory internal training	Yes	Yes
	Actual positive impact (OO)	F-Secure is strengthening its culture by reviewing people and culture structures to reflect the desired culture, supporting leadership and team development, and fostering a culture of experimentation	No	Yes
	Risk (DVC)	Partnership business, use of agents and other intermediaries increases bribery and corruption risk.	Yes	Yes
	Risk (DVC/UVC ,OO)	Anti-Bribery and Corruption risks increase as a result of M&A transactions due to limited understanding of the target.	No	No

Table 2. Material topics addressed by management and supervisory bodies.

Specifically, with regard to Audit Committee and Board of Directors engagement and in addition to what is described under “ESG Governance Structure”, any changes in the DMA and/or IROs, and updates to targets have been reviewed by the Audit Committee during 2025. In addition, the decision was taken to commit to SBTi during this reporting year, and the decision to commit was reviewed by the Audit Committee.

GOV-3 Integration of sustainability related performance in incentive schemes

The F-Secure Leadership Team is eligible for the non-sales Short-Term Incentive (STI) Plan designed to reward achievement of financial and operational objectives, foster a performance culture, and focus on business plan execution.

The Leadership Team is also eligible for share-based long-term incentives (LTI), aligning shareholder and Leadership Team interests. Similar LTI plans apply to certain members of our administrative and supervisory bodies.

Role of sustainability-related targets in incentive schemes

The 2025 non-sales STI Plan includes Company Business Results (combined growth % and profitability %) and Company Employee Engagement (eNPS). These elements connect to our material sustainability drivers - growth indicates consumers are protected globally (building trust in digitality), while eNPS reflects employee well-being and satisfaction.

The non-sales STI Plan is included in the remuneration policy, with goals approved annually by the Board. Share-based LTI programs may be based on long-term

financial/strategic performance or share value increase, with criteria focused on strategic financial targets.

Proportion of variable remuneration dependent on sustainability-related targets and approvals

The non-sales STI consists of:

- Business Results (combined growth % and profitability %): 60-80% weight
- Function-specific targets (may include sustainability-related targets): 0-20% weight
- Company Employee Engagement (eNPS): 20% weight

The Long-Term Incentive criteria for performance periods are based on strategic financial targets.

The Board of Directors approves annual STI designs and company-level targets based on Leadership Team proposals. For LTI programs, the Board determines terms, conditions, performance criteria, and objectives for each performance/vesting period.

STI or LTI plans do not currently contain climate-related targets.

GOV-4 Statement on Due Diligence

F-Secure's due diligence process identifies, mitigates, and addresses actual and potential negative impacts connected to our business, operations, value chain, offering, and business partners. This ongoing practice informs changes in our ESG governance, strategy, business model, operations, and sourcing activities.

Core elements of due diligence paragraphs in the Group sustainability statement

a) Embedding due diligence in governance, strategy and business model

ESG governance at F-Secure is described in the GOV-1 and GOV-2 sections. Our Leadership Team and Board of Directors oversee due diligence processes, with the Sustainability Council driving implementation. Due diligence considerations are integrated into our strategy and business model decisions.

b) Engaging with affected stakeholders in all key steps of due diligence

Through mapping all relevant stakeholders and conducting regular stakeholder engagement, F-Secure ensures an effective corporate sustainability due diligence process. The mapping includes employees, customers, suppliers, investors, and government bodies. We will review the stakeholder map when significant changes in the business model and strategy occur or if new impacts are identified as part of our IRO reviews, as described further under IRO-1 section.

c) Identifying and assessing adverse impacts

We identify potential impacts through our IRO assessment process outlined in the IRO-1 section. Our risk management is aligned with ISO-31000:2018 guidelines. No adverse impacts as described under "F-Secure impacts on people and the environment" have been identified.

d) Taking actions to address those adverse impacts

We address identified risks according to F-Secure's risk management policy, where risks have designated owners driving mitigation activities. We use risk modeling and quantification methods to identify and manage risks effectively, with proactive monitoring to build strategic resilience.

e) Tracking the effectiveness of these efforts and communicating

Each function tracks mitigation effectiveness and coordinates with relevant stakeholders. The Leadership Team and Audit Committee review risks biannually, while the Audit Committee regularly evaluates risk management process effectiveness. We communicate progress through our annual group sustainability report and regular stakeholder updates.

GOV-5 Risk management and internal controls over sustainability reporting

Control over sustainability matters is organized through policies, procedures, and processes developed by the sustainability function in collaboration with the Sustainability Council and relevant functions. These controls are approved by appropriate supervisory and management levels to support reliable and transparent sustainability reporting. The Audit Committee reviews Board-level policies and the group sustainability report preparation process, with the Code of Conduct and annual group sustainability report being approved by the Board of Directors.

Risk management and control processes in relation to sustainability reporting

F-Secure's internal control framework follows the Finnish Corporate Governance Code, covering policies, procedures, control activities, and monitoring. ESG is identified as a key process with specific internal controls for material topics. For sustainability reporting, we've implemented dedicated controls to ensure data accuracy, completeness, and reliability, including review procedures for ESG metrics before disclosure.

Internal control monitoring includes:

- Annual risk assessment
- Catalogue updates and gap follow-up
- Internal control self-assessments
- Internal control reporting

Risk assessment approach and main risks and mitigation strategies

The main identified risk related to sustainability reporting is the risk of reporting errors occurring, especially related to data points. Key risks related to data management and their controls are identified for each material topic and integrated into our internal controls matrix. Risks include ensuring climate change model updates are aligned with changes in accounting policy, talent acquisition/ retention data validation, business approvals outside of workday, validation of reported vulnerabilities data accuracy, assessing the number of security breaches/incidents involving AI tools, etc. Each data point has a defined person of responsibility, control, and testing mechanism. The Sustainability Council reviews these controls annually, ensuring alignment between our materiality assessment, risk management approach, reported data, and related controls.

The scope of reported data points has not changed since 2024. Some controls have been updated to better focus on the part of the process of data management where we have identified the greatest risk.

Main risks, mitigation strategies and controls:

Risk Identified	Management and Mitigation	Controls and Tracking
Risk of reporting errors, especially related to data points.	We have developed more detailed internal descriptions of datapoints for Own workforce in 2025 to mitigate risks of error.	Comprehensive internal controls for metrics and targets, which have been updated in 2025 from lessons learned last year.

Table 3. Main risks, mitigation strategies and controls.

Integration with company processes

Our internal controls support reliable reporting and regulatory compliance. Sustainability-specific data collection procedures and verification processes have been established for material ESG metrics to ensure accuracy. Risk management is integrated across all levels, from function-specific reviews to Leadership Team and Audit Committee oversight of the preparation of the group sustainability report. The ESG controls are owned and implemented by the sustainability function and developed in collaboration with control owners and the CFO office. The findings of the controls are documented by control owners and reviewed by the sustainability function. Failure of a control triggers control and/or process improvement, and this is evaluated on a case-by-case basis. The updated control catalogue is shared with the CFO office responsible for the group control matrix. The CFO office reports control findings to the Audit Committee.

Furthermore, every employee at F-Secure who is responsible for producing data or narrative for the group sustainability report is invited to several information sessions where process instructions are shared. In addition, a writing instruction document has been created to support the functions responsible for producing the narrative. To support functions responsible for data management, a step-by-step description of how to conduct internal controls has been made available. Each function takes responsibility and ensures instructions and processes are followed. The ESG governance, in conjunction with the risk management policy and internal controls, and detailed process descriptions, ensures that the relevant internal functions remain aware of their responsibilities and that actions are taken to mitigate the risk of reporting errors, with proper oversight from the Audit committee, Leadership Team and Sustainability Council.

Strategy

SBM-1 Strategy, business model and value chain

Product and services offering

F-Secure provides cybersecurity solutions for consumers to protect their digital moments. Our portfolio offering includes Security Suite (F-Secure Total) with endpoint security, scam protection, privacy protection, password management, and identity protection capabilities. Our Embedded Security offering is embedded in partners' existing or new apps to protect consumers. During the reporting period, F-Secure has expanded the protection capabilities in its portfolio, especially in scam protection.

While F-Secure sells Total directly to consumers, the entire portfolio is built to be “fit to channel sales” and allows the customer experience to be seamlessly integrated with our partner’s go-to-market model, including co-branding and billing.

Furthermore, to support our partners, we offer a cloud-based Security Business Platform to drive growth, such as data-led business insights, marketing support and customer care support. In addition, our Partner Success teams support partners’ go-to-market activities such as Marketing & Sales Enablement and Lifecycle Messaging Services.

Markets and customer groups served

Our end-customers are consumers seeking holistic, easy-to-use security solutions. We serve consumers directly and through approximately 200+ Service Provider partners (communication service providers, retailers, banks, and insurance companies). Revenue in 2025 was 82% through partners and 18% direct, with a geographical distribution shown in Table 4.

Revenue per geographic regions

Regions	2024 Revenue (M€)	2025 Revenue (M€)
Nordic countries	42.0	44.8
Rest of Europe	48.1	45.4
North America	45.5	44.3
Rest of the world	10.6	11.3
Total	146.3	145.7

Table 4. Revenue geographical distribution.

F-Secure belongs to the Technology - Software & IT Services ESRS sector. Our operations and profitability are reported as a single operating segment, and F-Secure’s revenue in 2025 is 145.7 M€.

Employees per geographic regions

Regions	Employees 2024	Employees 2025
Nordic countries	280	274
Rest of Europe	67	58
North America	33	30
Rest of the world	149	187
Total	529	549

Table 5. Employees per geographic region.

Sustainability-related goals

Our strategy focuses on understanding human behavior to deliver effective security experiences and becoming the number #1 security experience company. We've shifted from point solutions to delivering all-in-one, holistic, and easy-to-use security applications or embedded protection in partners' offerings. Our portfolio strategy and delivering "brilliantly simple security experiences" approach allows us to ensure that we protect consumers and improve our product satisfaction scores (Net Promoter Score, NPS).

Furthermore, to realize our purpose of making every digital moment more secure for everyone, our go-to-market model is primarily channel-based and through Service Providers allows us to reach hundreds of millions of consumers behind these partners in our focus regions in Europe, North America and APAC/Japan.

Our channel-based go-to-market model through Service Providers creates the potential to reach hundreds of millions of consumers, prioritizing win-win partner relationships measured by revenue and partner satisfaction. Measuring our partner satisfaction is another critical sustainability-related goal to realize our purpose and protect consumers' digital moments, as described in more detail in the chapter "Consumers and End-users".

Business model and value chain

Our business model is based on selling subscription-based consumer cybersecurity software products and services directly through our own e-commerce platform and app stores, as well as through our channel partners such as Communication Service Providers. Our high-level value chain, including notable actors, operations and stakeholders are visualized in the Value Chain and Actors figure below.

Upstream Operations

1. **Human Resources and Talent:** Attracting scarce cybersecurity expertise through strong employer branding
2. **Suppliers (Technology):** Strategic mix of in-house capabilities and third-party solutions
3. **Suppliers (IT):** Cloud infrastructure and business system providers
4. **Partnerships:** Collaborations with industry organizations and academia
5. **Financial:** Access to funding and addressing investor needs through profitable growth
6. **Regulatory Compliance:** Monitoring ESG, AI and data privacy regulations

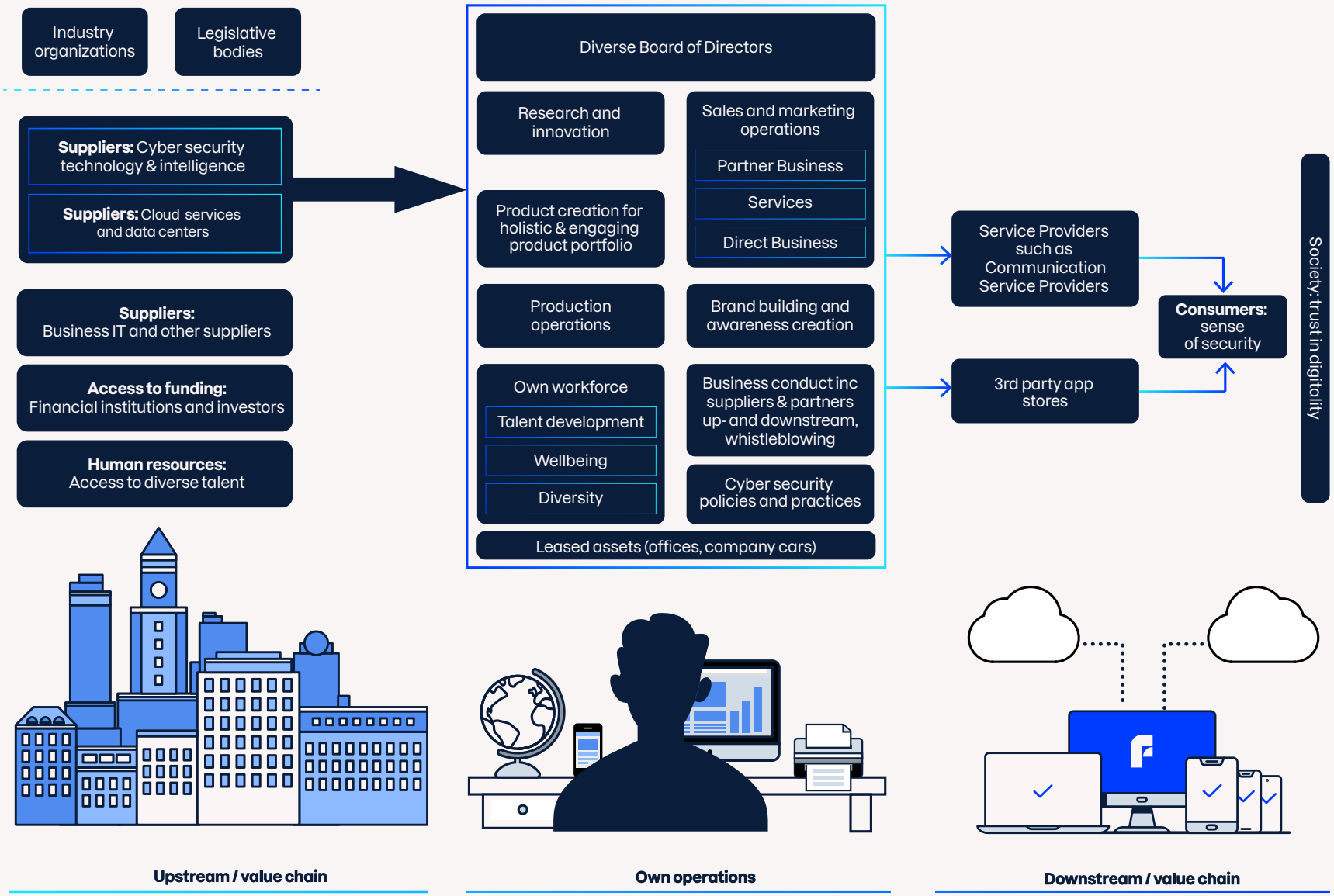
Core Operations

1. **Product Development:** Research and innovation, setting portfolio vision, roadmap, and product creation and maintenance
2. **Partner Sales:** Primary sales channel through Service Providers
3. **Direct Consumer Sales:** Revenue source and consumer insight generator
4. **Services:** Delivery, production, operations, customer care, and partner success services
5. **Trust Foundation:** Secure data handling, operations and ethical business conduct
6. **Talent Development:** Employee well-being and diversity initiatives
7. **Business Support:** Finance, HR, Legal and other enabling functions
8. **Governance:** Board-level strategic direction and oversight

Downstream Operations

1. **Partner Channel**: Partnerships with Service Providers to deliver security as a core service or a value-added service, creating a new revenue stream and positively impacting their core business, customer retention, and brand relevancy
2. **Direct Distribution Channels**: Consumer security services made available through our own e-Commerce platform and third-party app stores (Apple and Google)

Figure 2. F-Secure Value Chain.



SBM-2 Interest and views of stakeholders

	Stakeholder expectations	How engagement is organized	F-Secure actions and outcome from engagement
Investors and financial institutions 	Consistent growth and progression Clear and attainable goals Transparency in sustainability reporting Good Business conducts and data protection Ability to pay, liquidity	ESG surveys, calls and emails ESG ratings Capital market day Regular meetings with banks and analysts	Renewing relevant ESG ratings Renewing relevant ESG ratings, ESG targets and progress available on webpagese
Employees (Fellows) 	Caring employer Securing retention and incentivizing compensation Opportunities for professional development Good business ethics and capability to protect our customers Global DEI agenda	Employee surveys Personal development dialogues DEI Committee and Wellbeing and Committee Employee-elected board member Townhalls and trainings	Increase internal Sustainability communication Organize first Sustainability day Improvement of personal development dialogues Update of of Wellbeing committee and launch of wellbeing hour every week Development of F-Secure sustainable AI framework.
Partners 	Securing digital moments, together Reducing GHG emissions Good margins and shared values Reporting and targets on relevant ESG topics ESG policies aligned with partners policies	Partner survey and discussions Engagement with Sales ESG ratings	Renewing relevant ESG ratings Improvement on reporting ESG webpages updated ESG training of sales improving dialogue with partners ESG training of sales improving dialogue with partners SBTi Commitment
Consumers 	High level of protection for good price Understanding customer needs Knowledge about cybercrime Reliable and simple solution	Customer support and guidance Surveys	ProduESG webpage update Improve EcoVadis rating Increase cybersecurity awareness through campaigns
Policymakers and regulators 	Regulatory compliance Transparency in sustainability reporting Addressing ESG Risks and opportunities	Answering public consultations Participating in feedback rounds concerning new regulations and legislations	Flexibility to changing regulatory environment Value creation and risk mitigation
Suppliers 	Favorable payment terms Good business ethics and conduct Climate change and human rights Trust and transparency	Cybersecurity examination of suppliers conducted by CISO office Basic supplier onboarding process Basic review of main suppliers ESG priorities	Development of Procurement policy of conduct covering main sustainability topics Launch of supplier environmental data gathering program as part of GHG emission mitigation strategy

Table 6. F-Secure stakeholder map.

Through ongoing dialogue and engagement with our stakeholders, we strive to understand our stakeholders' positions, requirements, concerns, and expectations in more detail. This continuous interaction provides input to our strategy and ESG-related policies, actions, and processes, allowing us to align with the interests and views expressed by our stakeholders. As part of our Double Materiality Assessment review, we engaged key stakeholders, including financial institutions, our workforce, end-customers, the Board, and sales providing channel partners, while also analyzing regulatory requirements.

While the DMA review didn't result in material changes to our strategy or business model, we expect stronger stakeholder relationships through regular dialogue and complementary ESG agendas, particularly with Service Providers. We'll continue acting transparently, pursuing our goals and fostering future stakeholder collaboration.

Informing internal stakeholders on stakeholder interests

Stakeholder feedback has been reviewed by the Sustainability Council, which includes several Leadership team members. Our Sustainability Council regularly reviews and updates DMA and IROs, and management bodies will be informed of any significant stakeholder feedback changes affecting strategy and business model. We'll continue considering feedback in our risk management process and annual strategy reviews.

Consumer interests

For clarity, within the context of this Group sustainability report, the terms "consumer" and "end-user" should be treated as synonyms unless explicitly stated otherwise.

F-Secure conducts regular consumer and market surveys to align product roadmaps with needs, gathering additional feedback through customer care and Service Providers. Market studies and consumer insights inform both product and channel strategies, with 81% of consumers expecting security services from internet providers. We simplify security by embedding it in partners' apps, eliminating the need for consumers to download new applications.

F-Secure's commitment to international principles is not limited to internal operations but extends to its end-users. The company ensures that its products and services are designed and delivered in a manner that respects human rights and ethical standards. This includes data privacy protections, secure processing of personal data, and transparent communication about user rights and responsibilities. Finally, we are continuously monitoring evolving legislation in our key markets that impacts consumers. This includes, for example, EU GDPR and its impacts on the extent to which we collect consumer data and how it is processed at F-Secure.

Own Workforce interests

F-Secure involves its workforce in the Double Materiality Assessment, regularly gauges well-being, and obtains feedback on current events and company strategy. These results are reviewed by the Leadership Team and each function to drive related actions (where needed). Furthermore, we

- Ensure that we work according to our Code of Conduct, which includes respecting human rights
- Actively communicate company direction and priorities. This allows every employee to understand how their roles contribute to the broader company goals, thus making them feel connected to the company's direction
- Emphasize F-Secure's cultural values and how things are done at F-Secure to encourage employees to align their actions with shared values. Values are also used as part of our performance management ("how" things got done in addition to "what").

Value chain workers' interests

F-Secure respects its value chain workers' human rights through supplier Code of Conduct and partner agreements, focusing on fair labor practices, safe working conditions, and freedom of association and collective bargaining. F-Secure has a supplier Code of Conduct and agreements with certain partners, which seek to ensure that they meet the company's standards for responsible business conduct, including the treatment of their workers.

SBM-3 Material impacts, risks and opportunities and their interaction with strategy and business model

F-Secure creates positive social impact through its core business of protecting people from cybersecurity threats via its consumer security products and services. The company extends this impact by providing free tools and educational resources to raise society-wide awareness of cyber threats.

For its workforce, F-Secure prioritizes employee well-being through equal treatment and professional development opportunities. The company fosters an open culture where employees are encouraged to speak up, supported by a whistleblower channel that ensures concerns can be raised without fear of retribution.

Environmentally, while F-Secure currently deploys solutions on climate-neutral platforms like AWS, the company recognizes future challenges as AI adoption and customer growth increase energy demands. This drives the company's focus on green coding practices to minimize environmental impact as operations scale.

Standard	Type	Description	Time horizon
Environment	Potential positive impact (OO)	Implementation of green coding principles can reduce battery use in consumer devices and computational power in cloud environments	Long-term
Social	Actual positive impact (OO)	Protect consumers' digital moments with relevant, effective cybersecurity solutions	Short-term, mid-term and long-term
	Actual positive impact (DVC, OO)	Create awareness about cybercrimes through campaigns, and events	Short-term, mid-term and long-term
	Actual positive impact (OO)	Family leaves (sometimes exceeding local requirements) and enhancing work life balance of employees.	Short-term
	Actual positive impact (OO)	Promote gender equality through recruitment and gender pay gap mitigation	Short-term
	Actual positive impact (OO)	Further ramp up strategic learning and development activities and track investment into learning activities.	Short-term
	Actual positive impact (OO)	Foster inclusive culture with speak-up environment where workplace is safe for everyone	Short-term
	Potential positive impact (OO)	Continuously identify the internal competencies critical to our strategy	Mid-term
Governance	Actual positive impact (OO/DVC)	Whistleblower channel available to all employees and business partners	Short-term, mid-term and long-term
	Actual positive impact (OO)	F-Secure is strengthening its culture by reviewing people and culture structures to reflect the desired culture, supporting leadership and team development, and fostering a culture of experimentation	Short-term

Table 7. F-Secure impacts.

Standard	Type	Description	Time horizon
Environment	Risk (DVC/OO)	Failure to meet climate change mitigation targets may negatively impact channel business	Mid-term and Long-term
	Opportunity (OO)	Evolving threat landscape, protecting consumers against evolving threat landscape (for example scams) benefits both F-Secure and partners	Short-term, mid-term and long-term
	Opportunity (OO)	Use data and AI in security applications, for more effective protection and better user experience. AI-powered (network) monitoring tools can track user behavior, detect anomalies, and react accordingly.	Short-term, mid-term and long-term
	Opportunity (OO)	Enhance employer reputation through DEI activities to attract younger generations	Mid-term and Long-term
	Opportunity (OO)	Use of AI in workforce development, including process improvements, competency maturity and AI sentiment	Long-term
	Risk (DVC)	Channel strategy, significant agreement changes or existing partner loss can negatively impact outlook	Short-term, mid-term and long-term
Social	Risk (OO)	Decreasing consumer willingness to pay for premium security due to competition/ economic situation	Short-term, mid-term and long-term
	Risk (OO)	Talent acquisition and retention, loss of key persons or inability to acquire new talent	Short-term, mid-term and long-term
	Risk (OO, DVC/UVC)	Security vulnerabilities from suppliers and partners, relying on external vendors, especially vendors who are one step removed in the supply chain, adds layers of vulnerability.	Short-term, mid-term and long-term
	Risk (OO)	Cybersecurity attacks impacting reputation and business	Short-term, mid-term and long-term
	Risk (OO)	Mental health related absences detected.	Mid-term and Long-term
	Risk (OO)	AI increases risk of security breach, effective AI experimentation and roll-out dependent on high quality data sources and may also increase risk of a security breach.	Short-term, mid-term and long-term
Governance	Risk (DVC)	Partnership business, use of agents and other intermediaries increases bribery and corruption risk.	Short-term, mid-term and long-term
	Risk (DVC/UVC ,OO)	Anti-Bribery and Corruption risks increase as a result of M&A transactions due to limited understanding of the target.	Mid-term and Long-term

Table 8. F-Secure risks and opportunities.

Interaction with strategy and business model

F-Secure sustainability commitments

The positive impacts related to consumers and end-users are directly linked to F-Secure's purpose, the reason why we exist, and thereby with our business model and strategy. We are in the business of protecting consumers' digital moments against cyber threats, especially scams, directly and through our partners.

F-Secure's ambition for the long term is to increase our positive impact further globally based on our growth strategy of i) continuously expanding how we protect consumers' digital moments and ii) increasing reach and scale through our Service Provider partners. We continue to see end-customers turning to Service Providers for protection, while our partners see consumer security as an integral part of their brand promise and a business opportunity. Therefore, in every aspect of our operations, we emphasize responsible business as trust is foundational in our industry and applies to both our partners and consumers.

Positive social sustainability- and governance-related impacts have already materialized, and we see them having an increasingly positive impact also in the long term. The potential positive impacts related to green coding will grow over time, and we expect an actual impact to materialize in the long term.

Effects of IROs on strategy and decision making

Our strategy is directly informed by our most material positive impact: Protecting consumers' digital moments. Our continuous and comprehensive analysis of the threat landscape and consumer needs guides product investments, go-to-market and marketing strategies, and channel partnerships. We also see the rapidly evolving threat landscape as a growth opportunity, creating further need for effective scam protection and leveraging AI capabilities.

Employees turn our strategy into cohesive execution plans. To support these plans, our culture program, DEI initiatives, and employee well-being strategies mitigate risks related to talent acquisition and retention while making positive impacts on our workforce. We've implemented gender pay gap adjustments and are fostering an inclusive culture with speak-up values.

To maintain trust in the cybersecurity industry, we've improved vulnerability management processes and maintain high standards supported by our ISO27001 certification, which was validated again during 2025. Our Code of Conduct awareness programs address business ethics risks, which is fundamental in building trust.

For climate change, we're developing reduction pathways across Scope 1-3 emissions, focusing on supplier engagement, green energy use and electric vehicle adoption to reach our 2030 reduction targets.

Effects on F-Secure's financial position

Management has not recognized that F-Secure's material risks and opportunities have affected the undertaking's most recently reported financial performance, financial position and cash flow, or identified any material risks and opportunities for which there is a significant risk of a material adjustment within the next annual reporting period to the carrying amounts of assets and liabilities reported in the related financial statements.

Resilience addressing material IROs

F-Secure's strategy and business model are considered resilient to address material impacts and risks, and leverage opportunities identified as part of our strategy process for the next strategy period (2026–2028), which is F-Secure's definition of the mid-term period (1–3 years). This included both qualitative and quantitative analysis, expert assessments, and external consultation. Additionally, F-Secure is a highly profitable company with a strong cash flow, providing the ability to invest in our growth initiatives and mitigate key risks.

For resilience against climate change, refer to the Climate Change section for transition and physical-related risks.

Entity-specific IROs

F-Secure has identified some entity-specific impacts, risks and opportunities related to social topics, which is where F-Secure makes the largest contribution. The descriptions in the entity-specific section include contextual information and any assumptions made when calculating the measure or target, see Section *S4-5 Progress towards targets* for more detailed information on methodology and estimation uncertainty. When developing entity-specific measures and targets, F-Secure has considered how they can support reducing negative outcomes and increasing positive outcomes for people. The measures and targets have been developed for IROs where we have identified material impacts, risks or possibilities in the short, medium or long term that exceed the threshold for financial impact (see section IRO-1).

In short, and based on our double-materiality analysis, these entity-specific disclosure requirements apply to S4 Consumers and End-Users, see table *Consumers and end-users list of IROs* for the specification of those impacts, risks and opportunities.

Changes to the material impacts, risks and opportunities compared to the previous reporting period

Change	Description	Topic
Risk (DVC) removed	Removing: DEI Partner retention and acquisition related to DEI requirements", risk due to change in US politics.	Own Workforce
Risk (OO) added	"Effective AI experimentation and roll-out dependent on high quality data sources and may also increase risk of a security breach."	Consumers and end-users
Risk (DVC) Removed	Tier 1 partnership risk removed as it is seen as more of a pure business risk rather than a sustainability-related risk.	Consumers and end-users
Opportunity (OO) removed	Set policy for e-cars opportunity removed as it was more of an impact and as such does not reach the financial threshold of materiality.	Climate change
Opportunity (OO) removed	Expand use of worktime tracking at APAC level removed as it does not reach the threshold of financial materiality.	Own Workforce
Opportunity (OO) changed to potential positive impacts	Critical strategic competences opportunity changed to potential positive impact as it represents a potential positive effect on people.	Own Workforce
Opportunity (OO) changed to actual positive impacts	Learning and development changed to actual positive impact as it has a positive impact on our employees as it represents a positive effect on people.	Own Workforce
Opportunity (OO) added	Use of AI in workforce development: Process improvements, competency maturity and AI sentiment	Own Workforce
Opportunity (OO) changed to actual positive impacts	F-Secure is strengthening its culture by reviewing people and culture structures to reflect the desired culture, supporting leadership and team development, and fostering a culture of experimentation	Governance

Table 9. Changes in impacts, risks and opportunities since last reporting year.

Impact, risk and opportunity management

IRO-1 Identify and assess material impacts, risks and opportunities

F-Secure completed its first Double Materiality Assessment (DMA) in 2022 and refined it in 2023-2024, aligning with the final European Sustainability Reporting Standards and EFRAG guidance. The assessment follows these principles:

- ESG matters based on EFRAG standards, with SFRD and NFI regulations reviewed
- Sector and entity-specific topics assessed when relevant, particularly for cybersecurity
- Double materiality approach considering impacts on F-Secure and F-Secure's impacts on sustainability
- Use of quantitative and qualitative thresholds for IROs
- Engagement with affected stakeholders to inform the process
- Cross-cutting matters reported regardless of materiality assessment outcome

Critical input came from dialogue with key stakeholders, including Service Provider partners, investors, bankers, our workforce, consumers, suppliers, and regulators, as described under 1.3.2 SBM-2 Interest and views of stakeholders. We applied EFRAG guidance and expert interpretation to develop scoring matrices identifying material sustainability matters.

F-Secure recognizes that impacts, risks, and opportunities are interdependent and form an interconnected system. This understanding shapes the company's approach to sustainability management and governance, which is integrated into business strategy and risk management. For example, understanding that consumer protection impact depends on partner relationships, which creates both risks towards partnership channel and opportunities through, for example, increasing awareness, which can increase positive impacts.

In 2025, we reviewed the Double materiality assessment with internal relevant functions and conducted stakeholder engagement with our own workforce, financial institutions, and sales to get the partner point of view to ensure all IROs are up to date.

Material ESG Topics

Based on our assessment, we identified the following material topics:

Topic	Sub-topic	Materiality
Environment		
	Climate change adaptation	No
Climate change	Climate change mitigation	Yes
	Energy	No
Social		
	Working conditions	Yes
Own workforce	Equal treatment and opportunities for all	Yes
	Other work-related rights	No
	Information-related impacts for consumers and/or end-users	Yes
Consumers and end-users	Personal safety of consumers and/or end users	Yes
	Social inclusion of consumers and/or end users	No
Governance		
	Corporate culture	Yes
	Protection of whistle blowers	Yes
Business conduct	Animal welfare	No
	Political engagement	No
	Management of relationships with suppliers including payment practices	No
	Corruption and bribery	Yes

Table 10. F-Secure material topics.

After screening the locations, we did not identify material impacts, risks or opportunities related to pollution, water resources, biodiversity, or resource use. We have no operations near biodiversity-sensitive areas or activities negatively impacting land. Both own operations and value chain have been assessed as part of the double materiality assessment. The assessment methodology was the same for all topics and has been described in section IRO-1, *Double Materiality Assessment Methodology.*

The scope of topics assessed as material has not changed since 2024.

Business Conduct Assessment

We assessed business conduct on a global level, considering M&A activities and operations in countries with elevated corruption risks. The financial impact of

potential unethical behavior is estimated to reach the thresholds of materiality, but the likelihood is assessed as low. F-Secure is operating with large international partners with clear business codes of ethics and practices decreasing the risk of any anti-business conduct behavior. As F-Secure's operations are global, there are countries in which F-Secure has operations and where risks related to corruption and fraud are elevated.

Financial Effects of Risks and Opportunities

The assessment of risks and opportunities with potential financial effect was based on thresholds for financial materiality (magnitude) and likelihood. The risks are included in the company's risk management process, where the company-level risks are prioritized based on risk impact and likelihood, while opportunities are managed as part of the company's strategy and function-specific execution plans.

Assessment Process

When assessing IROs, we focused on areas where impacts, risks and opportunities are likely to arise based on our activities, relationships, and geographies. Both own operations and value chain have been assessed as part of the double materiality assessment. We indicate whether impacts and risks are in our own operations (OO) or value chain; Downstream (DVC) and Upstream (UVC), and whether impacts are positive or negative. Impacts were assessed using the scale and scope criteria presented in Table 11. Where impacts were potential rather than actual, likelihood was also assessed. For negative impacts, the assessment additionally considered remediability.

Material items exceeded one or more thresholds: strong stakeholder request, financial impact, scope/scale of event impact, or likelihood. A topic was considered material if it scored '3' in any category or met the financial impact threshold. The Double materiality assessment has been reviewed by the Sustainability Council and the Audit Committee and approved by the Board of Directors. The assessment process and methodology have not changed since the last reporting period.

As a result of the analysis, no adverse impacts have been recognized, however we have recognized risks that might lead to adverse impacts if realized. The impacts have not been included in the materiality analysis as the likelihood that these risks would materialize is more unlikely than likely. Assessment and prioritization of risks were made based on the threshold set for determining materiality as described in the Table Description of assessment methodology.

Scope	Scale	Financial impact
1 = Impact on group of people which is relatively small in the context of company's value chain, or impact on local natural area	1 = Impact with short-term effects which may be either negative or positive. Impacts are temporary in nature.	Financial impact (revenue threshold 5 % of revenue, costs threshold 3% of business costs and EBIT-margin threshold 2%)
2 =Impact on a community, several groups of people, region or broader natural area	2 = Impact with medium-term effects which might be either negative or positive. Impacts are temporary in nature but to recover there needs to be investments or programs to remediate the negative impacts. In case of positive impacts, beneficiary can benefit from the impact relatively long time	
3 = Impact on a global or multiregional scale on nature, people or society	3 = Impact is severe and either positive or negative. Either large groups of people, nature or larger communities are impacted or can benefit from the impact. Impact is long-term in nature and benefits are replacing inefficient existing processes or negative existing impacts with significant potential to improve the lives of people and/or the planet.	

Table 11. Description of assessment methodology.

Decision-Making Process and Internal Controls

Our Sustainability Council reassesses our DMA and IROs regularly. Updating of controls is presented to the Sustainability Council and Financial Controlling. The Council is informed of any control failures and presents risk mitigation actions. Depending on the nature of the control failure, the Audit Committee may be informed. The internal control procedure is described in more detail in section *GOV-5 Risk management and internal controls over sustainability reporting.*

F-Secure's risk management is a continuous process, with material sustainability risks included in our company-wide top 9 risk map. Each Leadership Team member is accountable for risk management in their functions.

Integration with Risk Management Process

Our Risk Management Policy explicitly requires evaluating the short-, medium- and long-term time horizons, taking into consideration the severity of the impact (scale, scope, remendability) and probability for any ESG-related risks, including actual and potential negative impacts, and in the case of a potential negative human rights impact, the severity of the impact takes precedence over its likelihood.

The responsibility of keeping our DMA relevant and up to date lies with F-Secure's Sustainability Council, through annual reviews. Any actual or potential negative impacts or risks found during the assessment would be assigned and owned by each respective function to mitigate the risk or negative impact as part of our risk management process, while actual or potential positive impacts, as well as opportunities, are integrated as part of F-Secure's strategy and relevant function execution plans.

Process to identify and assess climate-related impacts, risks and opportunities

F-Secure conducted a systematic assessment of climate-related impacts, risks, and opportunities as part of the double materiality assessment process. The identification process incorporated collaboration with internal functions, stakeholder engagement, and review by the Sustainability Council.

Physical Risk Assessment

F-Secure screened climate-related hazards to determine whether assets or business activities may be exposed to these hazards. The assessment considered F-Secure's operational footprint across different geographic locations, evaluating vulnerability based on regional climate risk profiles. Given the company's limited physical asset base as a cloud-based software provider, physical risks were assessed as having limited materiality. The analysis considered both acute events, such as flooding, and chronic conditions, such as heat stress, particularly for locations with higher vulnerability, such as India and Malaysia.

Transition Risk Assessment

The process to identify transition risks evaluated policy and legal developments, technology shifts, market changes, and reputational factors. F-Secure assessed potential impacts across short-term, medium-term, and long-term horizons, aligned with standard financial planning periods. The assessment considered F-Secure's value chain, with particular focus on Scope 3 emissions representing over 90% of total emissions.

Use of scenarios in the process and consideration of limiting global warming to 1,5 degrees

F-Secure developed three climate scenarios aligned with IPCC AR6 pathways to test strategy resilience: Orderly Transition (SSP1-2.6), Disorderly Transition (SSP2-4.5), and Hot House World (SSP5-8.5). This scenario analysis examined how climate-related risks might materialize under different futures, with specific consideration of pathway limiting global warming to 1.5-2°C consistent with Paris Agreement objectives.

The scenarios evaluated critical uncertainties, including policy implementation speed, stakeholder expectations evolution, and supply chain decarbonization pace. Through this process, F-Secure identified reputational risk from failing to meet emission reduction targets as the primary material climate risk, given stakeholder expectations and the company's dependency on supply chain emission reductions to achieve its target by 2030. The scenarios confirmed that physical risks exist and may increase over time, but they remain below the materiality threshold compared to transition risks.

IRO-2 Disclosure requirements

F-Secure has included the following disclosure requirements in our group sustainability report, as outlined in the following table.

Topic	Disclosure requirements	Index
General disclosure		
Basis for preparation	BP-1 – General basis for preparation of sustainability statements	29
Basis for preparation	BP-2 – Disclosures in relation to specific circumstances	29-30
Governance	GOV-1 – The role of the administrative, management and supervisory bodies	31-33
Governance	GOV-2 – Information provided to and sustainability matters addressed by the undertaking's administrative, management and supervisory bodies	33-35
Governance	GOV-3 - Integration of sustainability-related performance in incentive schemes	35-36
Governance	GOV-4 - Statement on due diligence	36-36
Governance	GOV-5 - Risk management and internal controls over sustainability reporting 3. Strategy	36-37
Strategy	SBM-1 – Strategy, business model and value chain	36
Strategy	SBM-2 – Interests and views of stakeholders	41
Strategy	SBM-3 - Material impacts, risks and opportunities and their interaction with strategy and business model	43-46
Impact, risk and opportunity management	IRO-1 - Description of the processes to identify and assess material impacts, risks and opportunities	47
Impact, risk and opportunity management	IRO-2 – Disclosure requirements in ESRS covered by the undertaking's sustainability statement	50-57

Topic	Disclosure requirements	Index
Environment		
Climate change	GOV-3 Integration of sustainability related performance in incentive schemes	35-36
Climate change	E1-1 Transition plan for climate change mitigation	70
Climate change	SBM-3 Material impacts, risks and opportunities and their interaction with strategy and business model	43-46
Climate change	IRO-1 Description of the processes to identify and assess material climate-related impacts, risks and opportunities	49-50
Climate change	E1-2 Policies related to climate change mitigation	72
Climate change	E1-3 Actions and resources in relation to climate change policies	73-74
Climate change	E1-4 Targets related to climate change mitigation	75-76
Climate change	E1-6 Gross Scopes 1, 2, 3 and Total GHG emissions	76
Social		
Own workforce	SBM-2 Interests and views of stakeholders	42-42
Own workforce	SBM-3 Material impacts, risks and opportunities and their interaction with strategy and business model	43-46
Own workforce	S1-1 Policies related to own workforce	83-85
Own workforce	S1-2 Processes for engaging with own workers and workers' representatives	85-86
Own workforce	S1-3 Processes to remediate negative impacts and channels for own workers to raise concerns	86

Topic	Disclosure requirements	Index
Own workforce	S1-4 Taking action on material impacts on own workforce, and approaches to mitigating material risks and pursuing material opportunities related to own workforce, and effectiveness of those actions	86-89
Own workforce	S1-5 Targets related to managing material negative impacts, advancing positive impacts, and managing material risks and opportunities	89-90
Own workforce	S1-6 Characteristics of the undertaking's employees	91-91
Own workforce	S1-9 Diversity metrics	93
Own workforce	S1-13 Training and skills development metrics	94
Own workforce	S1-14 Health and safety metrics	94
Own workforce	S1-15 Work-life balance metrics	94
Own workforce	S1-16 Remuneration metrics	95
Own workforce	S1-17 Incidents, complaints and severe human rights impacts	95
Consumers and end-users	SBM-2 Interests and views of stakeholders	96-106
Consumers and end-users	SBM-3 Material impacts, risks and opportunities and their interaction with strategy and business model	96
Consumers and end-users	S4-1 Policies related to consumers and end-users S4-2 – Processes for engaging with consumers and end-users about impacts	98
Consumers and end-users	S4-3 Processes to remediate negative impacts and channels for consumers and end-users to raise concerns	100
Consumers and end-users	S4-4 Taking action on material impacts on consumers and end-users, and approaches to mitigating material risks and pursuing material opportunities	101-104
Consumers and end-users	S4-5 Targets related to managing material negative impacts, advancing positive impacts, and managing material risks and opportunities	104-106
Governance		
Business conduct	GOV-1 The role of the administrative, supervisory and management bodies	31-33
Business conduct	IRO-1 Description of the processes to identify and assess material impacts, risks and opportunities Impact, risk and opportunity management	47
Business conduct	G1-1 Corporate culture and business conduct policies	110-111
Business conduct	G1-3 Prevention and detection of corruption or bribery	111-112
Business conduct	G1-4 – Confirmed incidents of corruption or bribery	112-112

Table 12. Topic Disclosure requirements Index.

Disclosure Requirement and related datapoint	SFDR reference[1]	Pillar 3 reference[2]	Benchmark Regulation reference[3]	EU Climate Law reference[4]	Index
ESRS 2 GOV-1 Board's gender diversity paragraph 21 (d)	Indicator number 13 of Table #1 of Annex 1		Commission Delegated Regulation (EU) 2020/1816, Annex II[5]		31
ESRS 2 GOV-1 Percentage of board members who are independent paragraph 21 (e)			Delegated Regulation (EU) 2020/1816, Annex II		31
ESRS 2 GOV-4 Statement on due diligence paragraph 30	Indicator number 10 Table #3 of Annex 1				36
ESRS 2 SBM-1 Involvement in activities related to fossil fuel activities paragraph 40 (d) i	Indicators number 4 Table #1 of Annex 1	Article 449a Regulation (EU) No 575/2013; Commission Implementing Regulation (EU) 2022/2453 Table 1: Qualitative information on Environmental risk and Table 2: Qualitative information on social risk[6]	Delegated Regulation (EU) 2020/1816, Annex II		Not applicable to F-Secure
ESRS 2 SBM-1 Involvement in activities related to chemical production paragraph 40 (d) ii	Indicator number 9 Table #2 of Annex 1		Delegated Regulation (EU) 2020/1816, Annex II		Not applicable to F-Secure
ESRS 2 SBM-1 Involvement in activities related to controversial weapons paragraph 40 (d) iii	Indicator number 14 Table #1 of Annex 1		Delegated Regulation (EU) 2020/1818, Article 12(1); Delegated Regulation (EU) 2020/1816, Annex II[7]		Not applicable to F-Secure
ESRS 2 SBM-1 Involvement in activities related to cultivation and production of tobacco paragraph 40 (d) iv			Delegated Regulation (EU) 2020/1818, Article 12(1); Delegated Regulation (EU) 2020/1816, Annex II		Not applicable toF-Secure
ESRS E1-1 Transition plan to reach climate neutrality by 2050 paragraph 14				Regulation (EU) 2021/1119, Article 2(1)	70
ESRS E1-1 Undertakings excluded from Paris-aligned Benchmarks paragraph 16 (g)		Article 449a Regulation (EU) No 575/2013; Commission Implementing Regulation (EU) 2022/2453 Template 1: Banking book Climate Change transition risk: Credit quality of exposures by sector, emissions and residual maturity	Delegated Regulation (EU) 2020/1818 , Article 12.1 (d) to (g), and Article 12.2		71

Disclosure Requirement and related datapoint	SFDR reference[1]	Pillar 3 reference[2]	Benchmark Regulation reference[3]	EU Climate Law reference[4]	Index
ESRS E1-4 GHG emission reduction targets paragraph 34	Indicator number 4 Table #2 of Annex 1	Article 449a Regulation (EU) No 575/2013; Commission Implementing Regulation (EU) 2022/2453 Template 3: Banking book – Climate change transition risk: alignment metrics	Delegated Regulation (EU) 2020/1818, Article 6		75
ESRS E1-5 Energy consumption from fossil sources disaggregated by sources (only high climate impact sectors) paragraph 38	Indicator number 5 Table #1 and Indicator n. 5 Table #2 of Annex 1				Not material
ESRS E1-5 Energy consumption and mix paragraph 37	Indicator number 5 Table #1 of Annex 1				Not material
ESRS E1-5 Energy intensity associated with activities in high climate impact sectors paragraphs 40 to 43	Indicator number 6 Table #1 of Annex 1				Not material
ESRS E1-6 Gross Scope 1, 2, 3 and Total GHG emissions paragraph 44	Indicators number 1 and 2 Table #1 of Annex 1	Article 449a; Regulation (EU) No 575/2013; Commission Implementing Regulation (EU) 2022/2453 Template 1: Banking book – Climate change transition risk: Credit quality of exposures by sector, emissions and residual maturity	Delegated Regulation (EU) 2020/1818, Article 5(1), 6 and 8(1)		76
ESRS E1-6 Gross GHG emissions intensity paragraphs 53 to 55	Indicators number 3 Table #1 of Annex 1	Article 449a Regulation (EU) No 575/2013; Commission Implementing Regulation (EU) 2022/2453 Template 3: Banking book – Climate change transition risk: alignment metrics	Delegated Regulation (EU) 2020/1818, Article 8(1)		79
ESRS E1-7 GHG removals and carbon credits paragraph 56				Regulation (EU) 2021/1119, Article 2(1)	Not material
ESRS E1-9 Exposure of the benchmark portfolio to climate-related physical risks paragraph 66			Delegated Regulation (EU) 2020/1818, Annex II Delegated Regulation (EU) 2020/1816, Annex II		Omitted 2025
ESRS E1-9 Disaggregation of monetary amounts by acute and chronic physical risk paragraph 66 (a) ESRS E1-9 Location of significant assets at material physical risk paragraph 66 (c)		Article 449a Regulation (EU) No 575/2013; Commission Implementing Regulation (EU) 2022/2453 paragraphs 46 and 47; Template 5: Banking book – Climate change physical risk: Exposures subject to physical risk.			Omitted 2025

Disclosure Requirement and related datapoint	SFDR reference[1]	Pillar 3 reference[2]	Benchmark Regulation reference[3]	EU Climate Law reference[4]	Index
ESRS E1-9 Breakdown of the carrying value of its real estate assets by energy-efficiency classes paragraph 67 (c)		Article 449a Regulation (EU) No 575/2013; Commission Implementing Regulation (EU) 2022/2453 paragraph 34; Template 2: Banking book – Climate change transition risk: Loans collateralised by immovable property – Energy efficiency of the collateral			Omitted 2025
ESRS E1-9 Degree of exposure of the portfolio to climate related opportunities paragraph 69			Delegated Regulation (EU) 2020/1818, Annex II		Omitted 2025
ESRS E2-4 Amount of each pollutant listed in Annex II of the EPRTR Regulation (European Pollutant Release and Transfer Register) emitted to air, water and soil, paragraph 28	Indicator number 8 Table #1 of Annex 1	Indicator number 2 Table #2 of Annex 1	Indicator number 1 Table #2 of Annex 1	Indicator number 3 Table #2 of Annex 1	Not material
ESRS E3-1 Water and marine resources paragraph 9	Indicator number 7 Table #2 of Annex 1				Not material
ESRS E3-1 Dedicated policy paragraph 13	Indicator number 8 Table 2 of Annex 1				Not material
ESRS E3-1 Sustainable oceans and seas paragraph 14	Indicator number 12 Table #2 of Annex 1				Not material
ESRS E3-4 Total water recycled and reused paragraph 28 (c)	Indicator number 6.2 Table #2 of Annex 1				Not material
ESRS E3-4 Total water consumption in m3 per net revenue on own operations paragraph 29	Indicator number 6.1 Table #2 of Annex 1				Not material
ESRS 2- SBM3 - E4 paragraph 16 (a) i	Indicator number 7 Table #1 of Annex 1				Not material
ESRS 2- SBM3 - E4 paragraph 16 (b)	Indicator number 10 Table #2 of Annex 1				Not material
ESRS 2- SBM3 - E4 paragraph 16 (c)	Indicator number 14 Table #2 of Annex 1				Not material
ESRS E4-2 Sustainable land / agriculture practices or policies paragraph 24 (b)	Indicator number 11 Table #2 of Annex 1				Not material
ESRS E4-2 Sustainable oceans / seas practices or policies paragraph 24 (c)	Indicator number 12 Table #2 of Annex 1				Not material

Disclosure Requirement and related datapoint	SFDR reference[1]	Pillar 3 reference[2]	Benchmark Regulation reference[3]	EU Climate Law reference[4]	Index
ESRS E4-2 Policies to address deforestation paragraph 24 (d)	Indicator number 15 Table #2 of Annex 1				Not material
ESRS E5-5 Non-recycled waste paragraph 37 (d)	Indicator number 13 Table #2 of Annex 1				Not material
ESRS E5-5 Hazardous waste and radioactive waste paragraph 39	Indicator number 9 Table #1 of Annex 1				Not material
ESRS 2- SBM3 - S1 Risk of incidents of forced labour paragraph 14 (f)	Indicator number 13 Table #3 of Annex I				Not applicable to F-Secure
ESRS 2- SBM3 - S1 Risk of incidents of child labour paragraph 14 (g)	Indicator number 12 Table #3 of Annex I				Not applicable to F-Secure
ESRS S1-1 Human rights policy commitments paragraph 20	Indicator number 9 Table #3 and Indicator number 11 Table #1 of Annex I				84
ESRS S1-1 Due diligence policies on issues addressed by the fundamental International Labor Organisation Conventions 1 to 8, paragraph 21			Delegated Regulation (EU) 2020/1816, Annex II		83-85
ESRS S1-1 processes and measures for preventing trafficking in human beings paragraph 22	Indicator number 11 Table #3 of Annex I				Not applicable to F-Secure
ESRS S1-1 workplace accident prevention policy or management system paragraph 23	Indicator number 1 Table #3 of Annex I				85
ESRS S1-3 grievance/complaints handling mechanisms paragraph 32 (c)	Indicator number 5 Table #3 of Annex I				86
ESRS S1-14 Number of fatalities and number and rate of work-related accidents paragraph 88 (b) and (c)	Indicator number 2 Table #3 of Annex I		Delegated Regulation (EU) 2020/1816, Annex II		94
ESRS S1-14 Number of days lost to injuries, accidents, fatalities or illness paragraph 88 (e)	Indicator number 3 Table #3 of Annex I				Omitted 2025
ESRS S1-16 Unadjusted gender pay gap paragraph 97 (a)	Indicator number 12 Table #1 of Annex I		Delegated Regulation (EU) 2020/1816, Annex II		95
ESRS S1-16 Excessive CEO pay ratio paragraph 97 (b)	Indicator number 8 Table #3 of Annex I				95

Disclosure Requirement and related datapoint	SFDR reference[1]	Pillar 3 reference[2]	Benchmark Regulation reference[3]	EU Climate Law reference[4]	Index
ESRS S1-17 Incidents of discrimination paragraph 103 (a)	Indicator number 7 Table #3 of Annex I				95
ESRS S1-17 Nonrespect of UNGPs on Business and Human Rights and OECD paragraph 104 (a)	Indicator number 10 Table #1 and Indicator n. 14 Table #3 of Annex I		Delegated Regulation (EU) 2020/1816, Annex II	Delegated Regulation (EU) 2020/1818 Art 12 (1)	95-95
ESRS 2- SBM3 – S2 Significant risk of child labour or forced labour in the value chain paragraph 11 (b)	Indicators number 12 and n. 13 Table #3 of Annex I				Not applicable to F-Secure
ESRS S2-1 Human rights policy commitments paragraph 17	Indicator number 9 Table #3 and Indicator n. 11 Table #1 of Annex 1				42
ESRS S2-1 Policies related to value chain workers paragraph 18	Indicator number 11 and n. 4 Table #3 of Annex 1				Not material
ESRS S2-1 Nonrespect of UNGPs on Business and Human Rights principles and OECD guidelines paragraph 19	Indicator number 10 Table #1 of Annex 1		Delegated Regulation (EU) 2020/1816, Annex II	Delegated Regulation (EU) 2020/1818, Art 12 (1)	Not material
ESRS S2-1 Due diligence policies on issues addressed by the fundamental International Labor Organisation Conventions 1 to 8, paragraph 19			Delegated Regulation (EU) 2020/1816, Annex II		Not material
ESRS S2-4 Human rights issues and incidents connected to its upstream and downstream value chain paragraph 36	Indicator number 14 Table #3 of Annex 1				Not material
ESRS S3-1 Human rights policy commitments paragraph 16	Indicator number 9 Table #3 of Annex 1 and Indicator number 11 Table #1 of Annex 1				Not material
ESRS S3-1 non-respect of UNGPs on Business and Human Rights, ILO principles or and OECD guidelines paragraph 17	Indicator number 10 Table #1 Annex 1		Delegated Regulation (EU) 2020/1816, Annex II Delegated Regulation (EU) 2020/1818, Art 12 (1)		Not material
ESRS S3-4 Human rights issues and incidents paragraph 36	Indicator number 14 Table #3 of Annex 1				Not material
ESRS S4-1 Policies related to consumers and end-users paragraph 16	Indicator number 9 Table #3 and Indicator number 11 Table #1 of Annex 1				98

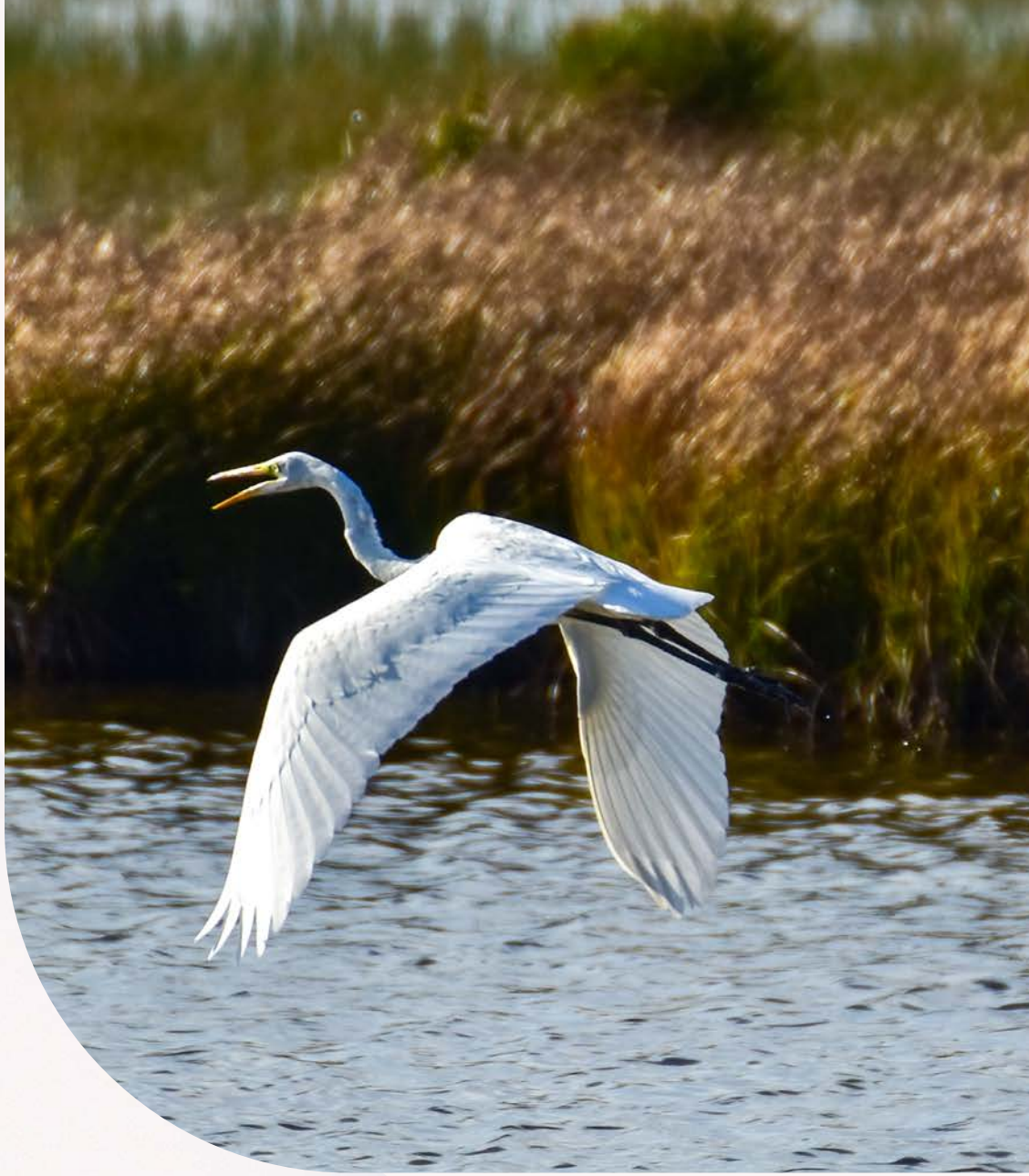
Disclosure Requirement and related datapoint	SFDR reference[1]	Pillar 3 reference[2]	Benchmark Regulation reference[3]	EU Climate Law reference[4]	Index
ESRS S4-1 Non-respect of UNGPs on Business and Human Rights and OECD guidelines paragraph 17	Indicator number 10 Table #1 of Annex 1		Delegated Regulation (EU) 2020/1816, Annex II Delegated Regulation (EU) 2020/1818, Art 12 (1)		98
ESRS S4-4 Human rights issues and incidents paragraph 35	Indicator number 14 Table #3 of Annex 1				103
ESRS G1-1 United Nations Convention against Corruption paragraph 10 (b)	Indicator number 15 Table #3 of Annex 1				110-111
ESRS G1-1 Protection of whistle-blowers paragraph 10 (d)	Indicator number 6 Table #3 of Annex 1				110-111
ESRS G1-4 fines for violation of anti-corruption and anti-bribery laws paragraph 24 (a)	Indicator number 17 Table #3 of Annex 1		Delegated Regulation (EU) 2020/1816, Annex II		112
ESRS G1-4 Standards of anti-corruption and anti-bribery paragraph 24 (b)	Indicator number 16 Table #3 of Annex 1				112

1) Regulation (EU) 2019/2088 of the European Parliament and of the Council of 27 November 2019 on sustainability-related disclosures in the financial services sector (Sustainable Finance Disclosures Regulation) (OJ L 317, 9.12.2019, p. 1).
2) Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (Capital Requirements Regulation "CRR") (OJ L 176, 27.6.2013, p. 1).
3) Regulation (EU) 2016/1011 of the European Parliament and of the Council of 8 June 2016 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds and amending Directives 2008/48/EC and 2014/17/EU and Regulation (EU) No 596/2014 (OJ L 171, 29.6.2016, p. 1).
4) Regulation (EU) 2021/1119 of the European Parliament and of the Council of 30 June 2021 establishing the framework for achieving climate neutrality and amending Regulations (EC) No 401/2009 and (EU) 2018/1999 ('European Climate Law') (OJ L 243, 9.7.2021, p. 1).
5) Commission Delegated Regulation (EU) 2020/1816 of 17 July 2020 supplementing Regulation (EU) 2016/1011 of the European Parliament and of the Council as regards the explanation in the benchmark statement of how environmental, social and governance factors are reflected in each benchmark provided and published (OJ L 406, 3.12.2020, p. 1).
6) Commission Implementing Regulation (EU) 2022/2453 of 30 November 2022 amending the implementing technical standards laid down in Implementing Regulation (EU) 2021/637 as regards the disclosure of environmental, social and governance risks (OJ L 324,19.12.2022, p.1.).
7) Commission Delegated Regulation (EU) 2020/1818 of 17 July 2020 supplementing Regulation (EU) 2016/1011 of the European Parliament and of the Council as regards minimum standards for EU Climate Transition Benchmarks and EU Paris-aligned Benchmarks (OJ L 406, 3.12.2020, p. 17).

Table 13. Disclosure Requirement and related datapoint SFDR reference.

GROUP SUSTAINABILITY REPORT -

Environment



EU Taxonomy

Taxonomy reporting

F-Secure has assessed the taxonomy-eligibility and taxonomy-alignment of its economic activities according to the EU Taxonomy Regulation (EU) 2020/852, the Climate Delegated Acts (EU) 2021/2139 and (EU) 2023/2485, the Environmental Delegated Act (EU) 2023/2486, the Disclosures Delegated Act (EU) 2021/2178 and other related guidance from the European Commission.

The analysis has been performed in collaboration between the F-Secure financial controlling and sustainability function and reviewed by an external sustainability consultant.

A taxonomy-non-eligible activity is defined as an activity not listed in Commission Delegated Regulations (EU) 2021/2139 and (EU) 2023/2485 or Commission Delegated Regulation (EU) 2023/2486. F-Secure operates in the field of cybersecurity software, which is a business area currently not covered by the EU Taxonomy and is therefore not taxonomy eligible. While Commission Delegated Regulation (EU) 2021/2139 (Climate Delegated Act) endorses computer programming as a taxonomy eligible activity (8.2 Computer programming, consultancy and related activities), the description of the activity is broad and does not specify whether or not the activity needs to be associated with software and consulting relevant to climate change adaptation or mitigation. It is also evident, based on Section 8.2 in Annex II, that it concerns expert services rather than the type of activities F-Secure offers. As F-Secure's business activities are clearly not aimed towards climate change adaptation or mitigation, and climate change adaptation has been identified as not material in a recent double materiality assessment for the company, we do not consider our business activities to be taxonomy-eligible, and we provide the tables for turnover, capex and opex with only taxonomy-non-eligible information (part B of the tables). F-Secure has taken into account the 4 other climate and environmental objectives (water and marine, circular economy, pollution, biodiversity, and ecosystem), and they do not lead to potentially eligible economic activities in this section. Furthermore, F-Secure is not involved with any nuclear energy-related activities or fossil gas-related activities as disclosed in the section Involvement with nuclear energy and fossil gas-related activities. We closely follow further developments of the taxonomy reporting requirements and will update the assessments when new legislation is published or when new information regarding its application becomes available. New activities, with new environmental targets in future versions of the taxonomy, might be more relevant for F-Secure and trigger a need of re-assessing both eligibility and alignment. Taxonomy-eligible turnover is defined as the proportion of net turnover derived from products or services, including intangibles, associated with taxonomy-eligible economic activities. As F-secure has not recognized any taxonomy-eligible economic activities, only the turnover on taxonomy-non-eligible activities is disclosed.

EU Taxonomy disclosure, reporting change from 2024; IFRS 16 Leases are included in Capex instead of Opex. At the same time right-of-use assets related depreciations are excluded in Opex.

Turnover

Taxonomy-eligible turnover is defined as the proportion of net turnover derived from products or services, including intangibles, associated with taxonomy-eligible economic activities. As F-secure has not recognized any taxonomy-eligible economic activities, only the turnover on taxonomy-non-eligible activities is disclosed.

Turnover is based on our financial statement (Cross-reference to financial section 3. Revenue).

Turnover

Financial year 2025		2025		Substantial contribution criteria						DNSH criteria									
Economic Activities	Code(s)	Turnover	Proportion of Turnover 2025	Climate change mitigation	Climate change adaptation	Water	Circular economy	Pollution	Biodiversity	Climate change mitigation	Climate change adaptation	Water	Circular economy	Pollution	Biodiversity	Minimum safeguards	Proportion of Taxonomy-aligned (A.1) or -eligible (A.2) turnover 2023	Category (enabling activity)	Category (transitional activity)
Text		*EUR 1000*	*%*	*Y; N; N/EL*	*Y; N; N/EL*	*Y; N; N/EL*	*Y; N; N/EL*	*Y; N; N/EL*	*Y; N; N/EL*	*Y/N*	*Y/N*	*Y/N*	*Y/N*	*Y/N*	*Y/N*	*Y/N*	*%*	*E*	*T*
A. TAXONOMY-ELIGIBLE ACTIVITIES																			
A.1 Environmentally sustainable activities (Taxonomy-aligned)																			
Turnover of environmentally sustainable activities (Taxonomy-aligned) (A.1)		0 €	0.0 %	**0.0 %**	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %								0%		
Of which enabling		0 €	0.0 %	**0.0 %**	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %								0%	E	
Of which transitional		0 €	0.0 %	**0.0 %**													0%		T
A.2 Taxonomy-eligible but not environmentally sustainable activities (not Taxonomy-aligned activities)																			
				EL; N/EL	*EL; N/EL*	*EL; N/EL*	*EL; N/EL*	*EL; N/EL*	*EL; N/EL*										
				EL; N/EL	*EL; N/EL*	*EL; N/EL*	*EL; N/EL*	*EL; N/EL*	*EL; N/EL*								0%		
Turnover of Taxonomy-eligible but not environmentally sustainable activities (not-Taxonomy-aligned activities) (A.2)		0 €	0.0 %	**0.0 %**	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %								0%		
A. Turnover of Taxonomy-eligible activities (A.1 + A.2)		0 €	0.0 %	**0.0 %**	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %								0%		
B. TAXONOMY-NON-ELIGIBLE ACTIVITIES																			
Turnover of Taxonomy-non-eligible activities		145,739	100.0 %																
TOTAL		145,739	100.0 %																

Operating expenditure

The operating expenses (0.720 MEUR) included in the taxonomy assessment are defined as direct non-capitalized costs that relate to research and development, building renovation measures, short-term lease, maintenance and repair, and any other direct expenditure relating to the day-to-day servicing of assets of property, plant and equipment by the undertaking or a third party to whom activities are outsourced that are necessary to ensure the continued and effective functioning of such assets (2021/2178). In F-Secure's calculation, the operating expenses related to the maintenance of premises are included. F-Secure utilizes the third-party cloud platforms of Amazon Web Services (AWS) and Microsoft Azure for the majority of its operations. Cloud hosting costs are not included in the operating expenses, subject to the taxonomy assessment.

As F-secure has not recognized any taxonomy-eligible economic activities, only the Opex of taxonomy-non-eligible activities is disclosed.

Operating expenditure

Financial year 2025		2025			Substantial contribution criteria						DNSH criteria									
Economic Activities	Code(s)	OpEx	Proportion of OpEx 2025	Climate change mitigation	Climate change adaptation	Water	Circular economy	Pollution	Biodiversity	Climate change mitigation	Climate change adaptation	Water	Circular economy	Pollution	Biodiversity	Minimum safeguards	Proportion of Taxonomy-aligned (A.1) or -eligible (A.2) OpEx 2023	Category (enabling activity)	Category (transitional activity)
Text		*EUR 1000*	*%*	*Y; N; N/EL*	*Y; N; N/EL*	*Y; N; N/EL*	*Y; N; N/EL*	*Y; N; N/EL*	*Y; N; N/EL*	*Y/N*	*Y/N*	*Y/N*	*Y/N*	*Y/N*	*Y/N*	*Y/N*	*%*	*E*	*T*
A. TAXONOMY-ELIGIBLE ACTIVITIES																			
A.1 Environmentally sustainable activities (Taxonomy-aligned)																			
OpEx of environmentally sustainable activities (Taxonomy-aligned) (A.1)		0 €	0%	**0%**	0%	0%	0%	0%	0%								0%		
Of which enabling		0 €	0%	**0%**	0%	0%	0%	0%	0%								0%	E	
Of which transitional		0 €	0%	**0%**													0%		T
A.2 Taxonomy-eligible but not environmentally sustainable activities (not Taxonomy-aligned activities)																			
				EL; N/EL	*EL; N/EL*	*EL; N/EL*	*EL; N/EL*	*EL; N/EL*	*EL; N/EL*										
				EL	EL	N/EL	N/EL	N/EL	N/EL								0%		
OpEx of Taxonomy-eligible but not environmentally sustainable activities (not-Taxonomy-aligned activities) (A.2)		0 €	0%	**0%**	0%	0%	0%	0%	0%								0%		
A. OpEx of Taxonomy-eligible activities (A.1 + A.2)		0 €	0%	**0%**	0%	0%	0%	0%	0%								0%		
B. TAXONOMY-NON-ELIGIBLE ACTIVITIES																			
OpEx of Taxonomy-non-eligible activities		720	100.0 %																
TOTAL		720	100.0 %																

Capital expenditure

The capital expenses included in the taxonomy assessment are defined as additions to tangible and intangible assets during the financial year, considered before depreciation, amortization and any re-measurements, including those resulting from revaluations and impairments, for the relevant financial year and excluding fair value changes (2021/2178). F-Secure's capital expenses are 17.799 MEUR in total. Capital expenditure includes capitalizations of development expenditure on new products or product versions with significant new features, partially or completely internally developed intangible assets that relate, for example, to platforms and software licenses. These are intangible assets according to the IAS 38 accounting standard. Capital expenditure also includes right-of-use assets according to IFRS16 Leases. A minor part of capital expenses relates to capitalization of employee laptops and other hardware, as well as office furniture and renovation expenses.

As F-secure has not recognized any taxonomy-eligible economic activities, only the Capex of taxonomy-non-eligible activities is disclosed.

Capital expenditure is based on our financial statement (Cross-reference to financial section 14. Non-current assets).

Capital expenditure

Financial year 2025		2025			Substantial contribution criteria						DNSH criteria									
Economic Activities	Code(s)	CapEx	Proportion of CapEx 2025	Climate change mitigation	Climate change adaptation	Water	Circular economy	Pollution	Biodiversity	Climate change mitigation	Climate change adaptation	Water	Circular economy	Pollution	Biodiversity	Minimum safeguards	Proportion of Taxonomy-aligned (A.1) or -eligible (A.2) CapEx 2023	Category (enabling activity)	Category (transitional activity)
Text		*EUR 1000*	*%*	*Y; N; N/EL*	*Y; N; N/EL*	*Y; N; N/EL*	*Y; N; N/EL*	*Y; N; N/EL*	*Y; N; N/EL*	*Y/N*	*Y/N*	*Y/N*	*Y/N*	*Y/N*	*Y/N*	*Y/N*	*%*	*E*	*T*
A. TAXONOMY-ELIGIBLE ACTIVITIES																			
A.1 Environmentally sustainable activities (Taxonomy-aligned)																			
CapEx of environmentally sustainable activities (Taxonomy-aligned) (A.1)		0 €	0.0 %	**0.0 %**	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %								0%		
Of which enabling		0 €	0.0 %	**0.0 %**	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %								0%	E	
Of which transitional		0 €	0.0 %	**0.0 %**													0%		T
A.2 Taxonomy-eligible but not environmentally sustainable activities (not Taxonomy-aligned activities)																			
				EL; N/EL	*EL; N/EL*	*EL; N/EL*	*EL; N/EL*	*EL; N/EL*	*EL; N/EL*										
				EL; N/EL	*EL; N/EL*	*EL; N/EL*	*EL; N/EL*	*EL; N/EL*	*EL; N/EL*								0%		
CapEx of Taxonomy-eligible but not environmentally sustainable activities (not-Taxonomy-aligned activities) (A.2)		0 €	0.0 %	**0.0 %**	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %								0%		
A. CapEx of Taxonomy-eligible activities (A.1 + A.2)		0 €	0.0 %	**0.0 %**	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %								0%		
B. TAXONOMY-NON-ELIGIBLE ACTIVITIES																			
CapEx of Taxonomy-non-eligible activities		17,799	100.0 %																
TOTAL		17,799	100.0 %																

Involvement with nuclear energy and fossil gas related activities.

Row	Nuclear energy related activities	
1	The undertaking carries out, funds or has exposures to research, development, demonstration and deployment of innovative electricity generation facilities that produce energy from nuclear processes with minimal waste from the fuel cycle.	NO
2	The undertaking carries out, funds or has exposures to construction and safe operation of new nuclear installations to produce electricity or process heat, including for the purposes of district heating or industrial processes such as hydrogen production, as well as their safety upgrades, using best available technologies.	NO
3	The undertaking carries out, funds or has exposures to safe operation of existing nuclear installations that produce electricity or process heat, including for the purposes of district heating or industrial processes such as hydrogen production from nuclear energy, as well as their safety upgrades.	NO
	Fossil gas related activities	
4	The undertaking carries out, funds or has exposures to construction or operation of electricity generation facilities that produce electricity using fossil gaseous fuels.	NO
5	The undertaking carries out, funds or has exposures to construction, refurbishment, and operation of combined heat/cool and power generation facilities using fossil gaseous fuels.	NO
6	The undertaking carries out, funds or has exposures to construction, refurbishment and operation of heat generation facilities that produce heat/cool using fossil gaseous fuels.	NO

Table 14. Involvement with nuclear energy and fossil fuel generating activities.

E1 – Climate change

SBM-3 Material impacts, risks and opportunities

	Material impact, risk or opportunity	Description
Climate change mitigation		
Risk (OO)	Failure to meet climate change mitigation targets may negatively impact channel business	Investing and finance linked to ESG ambition and targets of the company. Some partners not willing to continue business if not sufficient climate ambition.
Potential positive impact (OO)	Implementation of green coding principles	Through implementing green coding, we can reduce the impact of our end-product. Including optimizing device performance, battery use and cloud computing.

Table 15. Climate change list of IROs.

Interaction with strategy and business model

F-Secure's climate resilience analysis covers its own operations, upstream and downstream value chain activities. The resilience analysis covers transition risks, including policy and regulatory developments, technology changes, market requirements, and reputational risks related to climate mitigation targets. Physical risks assessed are marked with "x" in *Table 16, Climate SBM-3 physical risks*. Physical risks in locations with fewer than 20 employees have been excluded from the analysis due to limited operational footprint and the absence of owned assets in these areas. These material IROs are evaluated in terms of their impact on F-Secure's strategy and business model, ensuring that the scope of the analysis comprehensively addresses potential vulnerabilities and opportunities for adaptation.

Climate physical risks

F-Secure has assessed and defined its strategic response to climate change through scenario analysis aligned with limiting global warming to 1.5°C in accordance with the Paris Agreement. The assessment confirms that F-Secure's existing business model remains compatible with this pathway when complemented by targeted climate mitigation measures integrated into current operational processes and strategy. The details of this strategic response are disclosed in the section *Ability to adapt strategy and business model to climate change.*

	Chronic		Acute
	Temperature-Related		
x[1)]	Changing temperature (air, freshwater, marine water)	x	Heat wave
x	Heat stress	x	Cold wave/frost
x	Temperature variability	x	Wildfire
	Permafrost thawing		
	Wind-Related		
	Changing wind patterns	x	Cyclone, hurricane, typhoon
		x	Storm (including blizzards, dust and sandstorms)
		x	Tornado
			Glacial lake outburst
	Water-Related		
x	Changing precipitation patterns and types (rain, hail, snow/ice)	x	Drought
	Precipitation and/or hydrological variability	x	Heavy precipitation (rain, hail, snow/ice)
	Ocean acidification	x	Flood (coastal, fluvial, pluvial, ground water)
	Saline intrusion		
	Sea level rise		
	Water stress		
	Solid Mass-Related		
	Coastal erosion		Avalanche
	Soil degradation	x	Landslide
	Soil erosion	x	Subsidence
	Solifluction		

1) x = hazard included in the assessment

Table 16. Climate physical risks.

Transition assumptions

The transition to a lower-carbon and resilient economy will likely influence macroeconomic trends by driving economic growth through green technologies and sustainable practices. Energy consumption will shift towards renewable sources like solar and wind, reducing reliance on fossil fuels. National and international policies will be crucial in promoting GHG emission reductions and supporting renewable energy adoption.

Key Transition Events

Using the STEEP framework, we identified the following key driving forces that could impact F-Secure's climate strategy:

STEEP Category	Driving Force
Social	Rate of change in partner and investor climate expectations Increasing stakeholder pressure for transparency
Technological	Pace of decarbonization in IT supply chains Energy efficiency improvements in data centers
Economic	Evolution of carbon pricing mechanisms Cost of human labor
Environmental	Physical climate impacts on operations in vulnerable regions Supply chain disruption from extreme events
Political	Speed and stringency of global climate policy implementation Degree of divergence in regional climate approaches

Table 17. Key driving forces.

The only material transition risk identified is reputational risk from failing to meet mitigation targets aligned with the Paris Agreement, which could affect stakeholder expectations. This risk is significant because 97% of F-Secure's emissions come from Scope 3 categories, making emission reduction heavily dependent on supply chain performance.

Time horizons, climate scenarios and reduction targets

F-Secure has set a GHG reduction target for 2030 and developed a transition plan with defined reduction pathways and annual actions. We use scenarios as a tool to analyze environmental resilience, with time horizons for 2030. Our scenario analysis follows TCFD methodology and incorporates the latest IPCC AR6 findings to evaluate three distinct scenarios:

1. **Orderly Transition (SSP1-2.6)**: Coordinated global climate policy with gradual carbon price increases by 2030. Partner SBTi commitments rise steadily from approximately half by mid-decade to a significant majority by 2030. Supply chain costs increase moderately. F-Secure's 52% intensity reduction target is achievable with systematic supplier engagement requiring moderate annual investments, generating positive returns through market differentiation and potential modest revenue premiums in enterprise segments.
2. **Disorderly Transition (SSP2-4.5)**: Fragmented policy until 2027-2028, then sudden, stringent responses. Carbon prices spike dramatically within 18 months. Partner requirements accelerate abruptly, potentially threatening material revenue if unmet. Supply chain costs surge significantly. Target achievement faces a moderate to high failure probability, requiring substantially increased emergency investments from 2027. Non-compliance penalties could reach material percentages of global turnover.
3. **Hot House World (SSP5-8.5)**: Weak, fragmented policy with low carbon prices. Market segmentation creates divergent standards: a significant minority of partners (primarily EU/US West Coast) require science-based targets, while others maintain business-as-usual. Physical disruptions cause several days of annual supply chain disruption by 2030, moderately increasing costs. F-Secure risks exclusion from a portion of EU/Nordic enterprise RFPs without climate credentials. Target achievement depends on internal commitment, requiring higher annual investments justified primarily through market access rather than regulatory compliance.

Physical risks were not found to be significant as F-Secure has no assets in high-risk regions. The majority of employees are located in Finland and other Nordic countries with relatively mild projected climate impacts, while some limited exposure exists in India and Malaysia. For transition risks, we identified reputational risk if we fail to meet Paris Agreement-aligned targets.

Utilization of scenario analysis and transition plan

The utilization of F-Secure scenario analysis is to answer the focal and secondary questions that F-Secure has on climate change related to its own business and strategy:

Focal Question:

- "If F-Secure fails to meet its climate change mitigation target of reducing emission intensity by 52% by 2030, what would be the strategic and financial implications under different climate futures, and what actions should be taken to address these risks?"

Secondary focal questions:

- "How will climate-related transition risks, particularly stakeholder expectations, evolve over different time horizons and scenarios?"

- "What strategic and operational adjustments are needed to ensure F-Secure can meet its climate targets under different climate futures?"
- "What climate-related opportunities might emerge for F-Secure under different scenarios?"

A climate transition plan is utilized as a strategic roadmap that guides a company's pathway toward aligning its business model and operations with the transition to limit global warming to 1.5°C in line with the Paris Agreement. The transition plan translates climate commitments into actions, resource allocations, and governance mechanisms across business functions through clear decarbonization levers and implementation timelines.

Anticipated financial effects

Regarding material transition risks related to supply chain dependency, F-Secure may face economic impacts if we fail to meet climate targets aligned with stakeholder expectations. While specific financial impacts vary across scenarios, our analysis shows that meeting our 52% intensity reduction target requires different levels of investment and supplier engagement in each scenario, with the disorderly transition presenting the highest potential costs.

Results of the resilience analysis

F-Secure is considered climate resilient due to our business nature as a software company. Our current strategy aligns well with an orderly transition scenario, providing sufficient time to implement emissions reductions methodically. However, our strategy would face some challenges in a disorderly transition due to abrupt policy changes and rapidly evolving partner requirements. In a hot-house world scenario, our strategy would likely not meet its targets due to limited transition pressure in the supply chain.

Key strengths include our current emissions tracking approach and early work on emissions inventory. Vulnerabilities include heavy supply chain dependency in reaching the scope 3 target.

Performance Under Orderly Transition: F-Secure's current strategy aligns well with this scenario, providing sufficient time to implement emissions reductions in a measured way.

Performance Under Disorderly Transition: F-Secure's current strategy would face challenges in this scenario due to the abrupt policy changes and rapidly evolving partner requirements.

Performance Under Hot House World: The current strategy would likely not meet its targets in this scenario due to limited transition pressure in the supply chain, and would face increasing physical impacts, particularly in vulnerable locations.

Strategic response: ability to adapt strategy and business model to climate change

F-Secure's ability to adapt is embedded in our dynamic strategy process. Based on the scenario analysis, F-Secure has identified strategic measures to enhance climate resilience:

1. **Enhanced Supplier Emissions Data Collection**: Implementing systematic data collection from major suppliers and integrating climate criteria into supplier selection.
2. **Climate Governance Strengthening**: Establishing clear responsibilities through our Environment Committee and maintaining voluntary climate disclosure regardless of F-Secure is in scope of CSRD.
3. **Formal Science-Based Target Commitment**: Submitting commitment to the Science-Based Targets initiative near-term target and considering long-term net-zero target for the future.
4. **Low-Carbon Service Differentiation**: Developing green coding initiatives and a sustainable AI use framework.
5. **Climate Transition Contingency Planning**: Maintaining rapid response protocols for policy changes and financial reserves for climate initiatives.
6. **Partner Requirement Anticipation**: Establishing early warning systems for changing partner requirements through sales surveys.
7. **Distributed Work Enhancement**: Maintaining a strong remote work infrastructure and flexible arrangements for climate disruptions.

Our strategic response includes near-term (0-2 years, 2024-2026) actions like enhanced supplier emissions data collection and climate governance strengthening, alongside medium-term (2-5 years, 2026-2029) initiatives such as establishing a long-term net-zero target and implementing climate transition contingency planning.

We track emerging trends and adapt our strategy accordingly, ensuring ongoing resilience to evolving climate risks and opportunities.

Conclusion of scenario analysis

The scenarios highlight the importance of supplier engagement, given that over 90% of F-Secure's emissions are in Scope 3 categories. They also underscore the need for flexibility in implementation timelines and approaches, as the pace and nature of the climate transition remain uncertain.

Drawing on the IPCC AR6 finding that "there is a rapidly closing window of opportunity to secure a liveable and sustainable future for all," F-Secure's recommended strategy emphasizes early action on governance, sudden changes in requirements, and supply chain management while building capabilities to adapt to different potential futures. By implementing this strategy, F-Secure can enhance its climate resilience while positioning itself to thrive in a range of possible futures.

This scenario analysis will be reviewed annually to account for new developments in climate science, policy, technology, and market expectations, ensuring F-Secure's strategy remains resilient to evolving climate risks and opportunities.

E1-1 Transition plan for climate change mitigation

During 2025, F-Secure has continued to develop the details of the transition plan for climate change mitigation covering Scope 1, 2 and 3. The transition plan implementation is in the initial phase, with the four decarbonization levers disclosed under section *E1-3 and E1-4 and key actions planned,* which include operationalized implementation roadmaps. Governance oversight is established through the Environment Committee (operational Q3 2024), with bi-annual Sustainability Council reviews and annual Board reporting, ensuring accountability. Each decarbonization lever has assigned functional ownership, time-bound milestones, and defined expected impact by 2030.

Reference to GHG emission reduction targets: Paris Agreement

F-Secure has set key greenhouse gas (GHG) emissions reduction targets in line with the Paris Agreement, limiting global warming to 1.5°C. We've adopted the Greenhouse Gas Protocol and CSRD as our framework for measuring and managing emissions, targeting 42% absolute reduction across Scope 1, 2, and 52% emission intensity reduction of Scope 3, between 2024 and 2030, with 2024 as our base year. These targets align with IPCC 1.5°C Pathways. Sectoral decarbonization standards are not yet available for IT and Software companies.

Reference to GHG emission reduction targets: E1-3 and E1-4 and key actions planned

Decarbonization Lever	2025	2026-2027	2028-2030	Expected Impact by 2030
Fuel switching	Begin phasing in electric and hybrid vehicles	Continue fleet transition to hybrid/electric	Complete transition to 100% electric/hybrid fleet	55% reduction in fleet emissions (17 tCO_2e)
Renewable energy and energy efficiency	Prefer renewable energy in current and new lease agreements, especially in controlled facilities			40% reduction from 2024 baseline (75tCO_2e)
Supply chain decarbonization	Include sustainability into F-Secure procurement policy	Include sustainability in supplier selection process	Widen scope of suppliers included in supplier sustainability program	52% reduction in emission intensity of Scop 3
Green coding principles	Develop sustainable AI framework Begin developer training	Implement architecture cost review for energy efficiency Support and enhance sustainable AI framework Monitor developments in the sector to uncover technical opportunities for improving sustainability Engage strategic partners' engineering teams around green software practices	Regular efficiency reporting Regular code and system architecture Reviews considering efficiency All Engineering Fellows have awareness of green software engineering	Keep 2024 emission levels

Table 18. Key actions planned.

F-Secure transition plan does not necessitate material dedicated investments or funding beyond normal business operations. The implementation of the four primary decarbonization levers is executed within existing operational budgets and business processes.

Changes in product portfolio

Our main emission sources from production and technologies are in Scope 3 Category 1, including data centers and other purchased services. We're primarily using AWS for cloud computing and plan to continue this approach, as AWS offers near-zero-emission solutions.

We'll emphasize developing efficient, high-quality code to improve product performance, customer experience, and overall efficiency. The integration of AI and machine learning technologies will enhance product functionality and drive competitiveness. We'll partner with major AI providers who commit to reducing emissions, ensuring our overall emission profile remains unchanged despite increased energy use from AI models.

Reference to climate change mitigation actions

As per disclosure requirement E1-3, F-Secure does not have taxonomy-compliant activities, and therefore, no linked investments and financing that would support its transition plan. See more under the EU Taxonomy section.

Locked-in GHG emissions

Carbon lock-in is generally associated with physical infrastructure and long-term investments in carbon-intensive technologies. This topic is not considered material for F-Secure as the impacts are small due to actions already taken, and our implementation of green coding further reduces locked-in emissions.

Economic activities and benchmark regulation (Pillar 3)

A taxonomy-non-eligible activity is defined as an activity not listed in Commission Delegated Regulation (EU) 2021/2139 or Commission Delegated Regulation (EU) 2023/2486. F-Secure operates in the field of cybersecurity software, which is a business area currently not covered by the EU Taxonomy and is, therefore, not taxonomy eligible. See our EU Taxonomy statement for more details. F-Secure is not excluded from the EU Paris-aligned Benchmarks.

Transition plan alignment with F-Secure's strategy and financial planning

Resource Area	Requirements	Integration with Business Planning
Supply Chain Engagement	Dedicated supplier management resources	Procurement processes to integrate supplier emissions considerations
Energy Efficiency	Investments in office upgrades at controlled premises	Integrate energy consideration in office space leasing decisions
Green Coding	Developer training and performance optimization	Development of sustainable AI framework
Fuel switching	Achieve 100% e-/hybrid fleet	Policy to enforce change

Table 19. Transition plan alignment with strategy and financial planning.

ESG is integrated into our company strategy rather than being a separate initiative. Our transition plan actions will be implemented by appropriate functions with consideration to their annual budgets, with progress tracked by our Environment Committee and Sustainability Council. The transition plan will be further developed as part of the SBTi process. In 2026, it will be reviewed by the Audit Committee and approved by the Board of Directors.

Impact, risk and opportunity management

E1-2 Policies

F-Secure has the ambition to deliver sustainable security experiences to our partners and consumers. To ensure we deliver on our climate change targets, we have adopted several policies that address climate-related impacts, risks and opportunities.

The Climate Change Policy is based on the values and principles defined in F-Secure's Code of Conduct and informed by stakeholder input from our materiality assessment. Our Supplier Code of Conduct explicitly requires suppliers to commit to working in an environmentally responsible and efficient manner and strive to minimize the environmental footprint of operations.

Policy	Key Contents	Scope	Responsibility	Link to IROs
Climate Change Policy	Targets across Scopes 1, 2, and 3 Alignment with Paris Agreement and IPCC 1.5°C pathways Process for identifying climate impacts, risks and opportunities Renewable energy deployment in offices and operation (excluding energy efficiency) Climate change mitigation and adaptation	All employees, operations and value chain across all relevant geographies	CEO with implementation by Sustainability Council and Environment Committee	Failure to meet climate change mitigation targets may negatively impact channel business
Supplier Code of Conduct	Sustainable usage of natural resources Increasing energy efficiency and renewable energy use Reducing environmental impact of global operations	Suppliers (only apply where included or referenced in agreement)	Procurement with monitoring by F-Secure	Failure to meet climate change mitigation targets may negatively impact channel business
Procurement policy	Establish clear standards for all procurement activities Ensuring vendor evaluation, compliance with listed F-Secure policies, counterparty screening procedure, Regulatory and Industry Compliance and promoting environmental, social, and governance responsibilities	Suppliers and employees	Approved by CEO with monitoring by Procurement function	Failure to meet climate change mitigation targets may negatively impact channel business

Table 20. Climate policies.

E1-3 Actions and resources

To achieve Climate change policy targets and mitigate emissions, we have implemented four decarbonization levers linked to our environmental IROs.

To further strengthen our transition plan, F-Secure has committed to set near-term, company-wide greenhouse gas emission reduction targets in line with climate science through the Science Based Targets initiative (SBTi). By joining the SBTi, F-Secure is taking a clear step toward aligning its climate strategy with what science says is necessary to limit global temperature rise to 1.5°C. This commitment reflects F-Secure's ambition to act responsibly and be a sustainable, long-term partner for customers, partners, and society.

Fuel switching

For the opportunity to set a policy for e-vehicles, several cars have already been replaced with hybrid or electric models, and this transition will continue as leasing contracts are renewed. In the future, we aim to update our car policy to ensure that by 2030, all leased cars are electric.

Renewable energy and energy efficiency

In 2025, F-Secure's headquarters in Helsinki moved to new office spaces. In the process, renewable energy was considered, and the electricity used in the new Helsinki office is 100% renewable. Our plan is to ensure all large offices, as well as smaller facilities where energy contracts can be controlled, use 100% renewable energy by 2030.

Supply chain decarbonization

Regarding the risk that F-Secure would fail to meet mitigation targets, as emission reduction is heavily reliant on suppliers, we have initiated actions to mitigate emissions in our value chain. In 2025, we set up our supplier climate mitigation program to reduce our emissions. The program focuses on supplier engagement and climate data gathering from suppliers. We've also implemented our Procurement policy, which requires suppliers to work in an environmentally responsible manner, continuously improve energy efficiency, and reduce waste and emissions. No quantitative emission reductions are available for these actions in 2025, but we expect a 52% emission intensity reduction by 2030.

Efficient coding principles

For the potential positive impact of implementing green coding principles, emissions for sold products are calculated based on the number of products sold annually. During 2025, actions towards this lever include developing and launching our company-wide framework for Sustainable AI use and training the organization on these principles. AI is a strategic priority at F-Secure, and we are moving fast. This framework provides the guardrails we need for rapid, responsible innovation. The framework clarifies what F-Secure does to ensure sustainable AI implementation and what we expect from our workforce. In addition, we organized a panel discussion on AI innovation and sustainability in software development with external experts joining. This panel discussion aimed to share knowledge about the scale of environmental impact of software and AI, learn strategies for green coding and sustainable AI in production, and understand how to make the business case for responsible development. While no quantitative emission reductions are expected in 2025 due to the low material impact. By 2030, we do not expect emission reductions as the number of sold products is projected to grow, while we optimize energy consumption.

For more specific information on progress towards climate targets, see Disclosure Requirement E1-4 – Targets related to climate change mitigation and adaptation. No significant monetary amounts of Capex and Opex have been required to implement these actions.

Resource Allocation

The management of impacts, risks and opportunities is conducted by the F-Secure Environment committee, including internal stakeholders for each decarbonization lever.

Metrics and targets

E1-4 Targets

F-Secure describes its sustainability-related baseline measures and targets in the table below. 2024 is established as a baseline year, and progress will be reported annually.

Methodologies and frameworks

Methodologies for tracking emission reduction targets vary. Scope 1 emissions are calculated using fuel consumption data and leasing contracts. Scope 2 emissions use both market-based and location-based methods with data collected from sites. Scope 3 emissions primarily use the spend-based method, with some data obtained directly from suppliers. More details are in E1-6 – Gross Scopes 1, 2, 3 and Total GHG emissions.

Our 2025 energy-related emission factors were updated by an external consultant. Metrics were selected based on legislative requirements, material ESG topics, and stakeholder feedback. In 2025, we have updated our Scope 3 target from actual emission reduction to 52% reduction in emission intensity (GHG emissions (t CO_2eq) by net revenue (€)) of Scope 3. Targets have been approved by the Board of Directors.

In the event of significant structural changes such as acquisitions, divestments, mergers, or changes in calculation methodologies, F-Secure will evaluate whether baseline recalculation is necessary. Recalculation would be conducted if structural changes result in a material impact on the baseline emissions, following GHG Protocol guidance. Any baseline adjustments will be transparently disclosed, documenting the rationale, methodology, and quantitative impact of the recalculation to maintain comparability and integrity of target tracking over time. In 2025, baseline recalculation has not been conducted as there have not been significant changes. F-Secure has not adopted new technologies in 2025, which would significantly affect the emission reduction targets.

We track our actions' effectiveness using total GHG emissions (tons of CO_2eq), emissions intensity per revenue, and their impact. We disclose combined GHG emission reduction targets for Scope 1 and 2 emissions. Scope 2 emissions are calculated using both market-based and location-based methods, with market-based used for the 2030 target. Our targets align with GHG inventory boundaries and don't include GHG removals, carbon credits or avoided emissions.

E1-4 Climate targets & progress

	2024 base year	2025	Target values	2030 target
Gross Scope 1 & Scope 2 (market-based) (tCO2eq)	220	195	127	42% emission reduction
Scope 3 (tCO2-ekv./MEUR) emission intensity	57	57	27	52% emission intensity reduction

Table 21. Climate targets and progress.

E1-4 Progress towards targets

Current base year and baseline value

2024 is chosen as the base year for emissions to ensure an accurate view and to avoid external influences. After 2030, the base year is set every five years. The 2024 baseline values are described in chapter E1-6.

Framework and methodology for target setting

F-Secure has established GHG emission reduction targets compatible with limiting global warming to 1.5°C by 2030. In 2030, Scope 1&2 emissions aim to be 127 tons of CO_2eq, and the Scope 3 target of 52% reduction in emission intensity (GHG emissions (t CO_2eq) by net revenue (€)). The GHG Protocol and IPCC's cross-sector pathway serve as our framework. Future technological advancements, regulatory changes, and market shifts have been considered in our target setting. F-Secure is dedicated to continuously reviewing and adjusting its strategies to ensure they remain aligned with the latest scientific and industry standards, thereby maintaining the integrity and feasibility of its emission reduction goals. The targets are defined by the Sustainability Council and approved by the Board of Directors.

Decarbonization levers and their contributions to achieve reduction targets.

- **Fuel switching:** We plan to transition to hybrid and electric vehicles, with a projected 50/50 split by 2030. In 2025, the emissions of Scope 1 were 33 tCO_2eq. Emissions will be within the 42% decrease target by 2027.
- **Renewable energy and energy efficiency:** The Scope 2 emissions have decreased 14% during 2025, mostly due to removal of Poland office and the decrease of Helsinki office heating.
- **Supply chain decarbonization:** This lever includes Scope 3 category 1, which represented over 80 % of our Scope 3 emissions in 2025. Our purchased goods and services (excluding data center services) were 6610 tCO_2eq. Our cloud computing and data center services increased from 2024 due to an increase in the AWS services.
- **Efficient coding principles:** No material reduction expected as customer base growth will likely cancel out energy efficiency improvements. This covers Scope 3 category 11. We are still in the early stages of implementation, and assessing the effectiveness of the actions and policies cannot be quantified at this early stage.

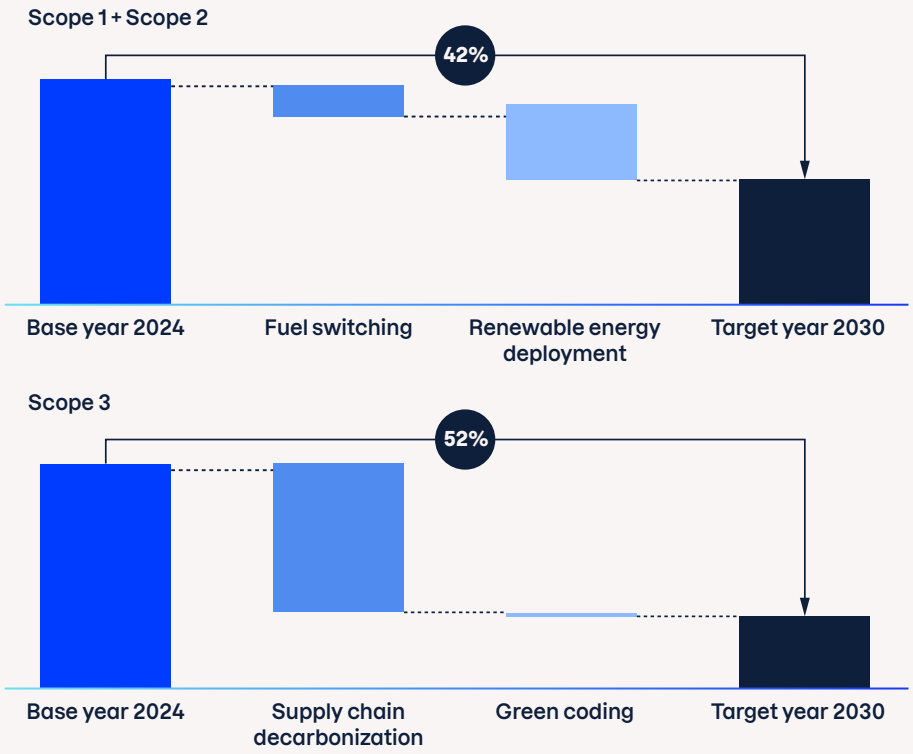


Figure 3. Graphical pathway waterfall shows the development of emissions in line with the Transition plan.

E1-6 Gross scopes 1, 2, 3 and Total GHG Emissions

In our GHG emission calculations, we've considered the GHG Protocol Corporate Standard for principles, requirements and guidance. We use primary data where available (currently only from AWS, representing <1% of total Scope 3 emissions) and standardized emission factors for the remainder. Our emissions consolidation approach follows the operational control method.

	Retrospective				Milestones and target years			
	Base year 2024	Comparative	2025	% N / N-1	2025	2030	(2050)	Annual % target / Base year
Scope 1 GHG emissions								
Gross Scope 1 GHG emissions (tCO_2eq)	31	31	33	6%	-	18[1]	-	8.70%[2]
Percentage of Scope 1 GHG emissions from regulated emission trading schemes (%)	0%	0%	0%		-	-	-	-
Scope 2 GHG emissions								
Gross location-based Scope 2 GHG emissions (tCO_2eq)	233	233	198	-15%	-	-	-	-
Gross market-based Scope 2 GHG emissions (tCO_2eq)	189	189	162	-14%	-	110[1]	-	8.70%[2]
Scope 3 GHG emissions								
Total Gross indirect (Scope 3) GHG emissions (tCO_2eq)	8330	8330	8282	-1%	-	NA[3]	-	-
1. Purchased goods and services (excluding data center services)	6466	6466	6610	2%	-	-	-	-
Sub-category: Cloud computing and data center services	43	43	318	640%	-	-	-	-
3. Fuel and energy-related activities	49	49	43	-12%	-	-	-	-
5. Waste generated in operations	2	2	3	50%	-	-	-	-
6. Business travel	1675	1675	1211	-28%	-	-	-	-
7. Employee commuting	23	23	22	-4%	-	-	-	-
8. Upstream leased assets	11	11	15	36%	-	-	-	-
11. Use of sold products	61	61	61	0%	-	-	-	-
Total GHG emissions								
Total GHG emissions (location-based) (tCO_2eq)	8594	8594	8513	-1%	-	-	-	-
Total GHG emissions (market-based) (tCO_2eq)	8550	8550	8477	-1%	-	NA[3]	-	-

1) Scope 1 and Scope 2 target is combined and not measured separately.

2) Value is based on a linear progression. Our impact is not expected to follow a linear pattern. Scope 1 and Scope 2 target is combined and not measured separately.

3) An absolute value cannot be given because an accurate revenue estimate cannot be made.

Table 22. Gross scopes and total emissions.

To create an accurate emission calculation, the most relevant data and methodologies have been used.

Scope 1

F-Secure's Scope 1 emissions originate from fuel combustion in company vehicles. Emissions are calculated using fuel consumption data from leasing car systems and directly from individuals leasing the vehicles. Emission factors from Statistics Finland convert fuel data into GHG emissions in metric tons of CO2e. F-Secure's operations do not generate biogenic Scope 1 GHG emissions from biomass combustion or decomposition.

Scope 2

F-Secure uses both market-based and location-based methodologies. Data on purchased electricity is collected from five sites via country or site representatives. Emissions from heating and cooling are calculated using the office area and heating/cooling factors. Compared to the 2024 calculations, the Poland office no longer exists, and Helsinki offices moved to larger facilities within the same building. Emission factors are sourced from multiple authorities, including Energy Authority, Association of Issuing Bodies, Ember, Energiateollisuus, Statistics Finland, CO2Emissiefactoren, Defra, and Our World in Data.

Scope 3

Scope 3 categories:

Scope 3 category	Categories included in F-Secure Oyj's calculations
1. Purchased goods and services	x
2. Capital goods	Not relevant, F-Secure has not purchased or acquired capital goods
3. Emissions from fuels and energy that are not included in scope 1 or scope 2 emissions	x
4. Upstream transportation and distribution	Not relevant, F-Secure does not have upstream transportation or distribution
5. Waste generated in operations	x
6. Business travel	x
7. Employee commuting	x
8. Upstream leasing-commodities	x
9. Downstream transportation and distribution	Not relevant, F-Secure does not have downstream transportation or distribution
10. Processing of sold products	Not relevant, F-Secure does not have processing of sold products as our product is software
11. Use of sold products	x
12. End-of-life treatment of sold products	Not relevant, no physical products are sold by F-Secure
13. Downstream leasing-commodities	Not relevant, F-Secure does not lease any assets
14. Franchisee's emissions	Not relevant, F-Secure does not have operation of franchises
15. Investments	Not relevant, F-Secure does not have investments that falls into this category

Table 23. Scope 3 categories.

Category 1: Purchased goods and services (excluding data center services) Values derived from financial reports representing expenditure on goods and services. Emissions from some vendors are calculated separately by comparing their emissions to revenue. These vendor expenses are excluded from financial report data to avoid double-counting. Emission factors from Lenovo and Exiobase.

Category 1 sub-category: Data center services 3-month delay in retrieving AWS figures. VPN energy usage is primarily from Ficolo (Finnish VPN server provider). Other VPN providers' electricity usage is extrapolated based on known traffic. Emission factors from AWS, EEA, Australian government, Carbon Footprint, Government of Canada, Ficolo, Climate Transparency, Singapore government, EPA and Vietnam government.

Category 3: Fuel and energy-related activities Calculated based on Scope 1 and Scope 2 values. Emission factors from GLEC, Defra and the UK Government.

Category 5: Waste generated in operations Waste amounts are estimated by extrapolating general waste amounts in a conventional office. Laptop and monitor data collected from Finnish offices and extrapolated to other offices. Emission factors from Fujitsu and the Environmental Protection Agency.

Category 6: Business travel Flight data from two travel agencies and from the company HR system. For HR system data emission calculators used for emissions or flight lengths. Emissions regarding business travel decreased around 30% from 2024. Emission factors from travel agencies, including Defra.

Category 7: Employee commuting Work travel distance, and type based on external data sources and estimations. Office workdays are calculated based on Helsinki and Oulu office data. Emission factors from Defra, Statistics Finland, GreenTech Malaysia and Carbon Footprint.

Category 8: Upstream leased assets Emissions from home offices and coworking spaces are assumed from electricity consumption of ICT equipment. Home offices and coworking spaces are not separated as they work similarly. Emission factors from Carbon Footprint.

Category 11: Use of sold products Assumed all sold products are taken into use. Emission factor from Statistics Finland.

F-Secure has no operational control of associates, joint ventures or unconsolidated subsidiaries, nor contractual arrangements in joint arrangements not structured through an entity.

Emission factors used are carbon dioxide equivalents, including greenhouse gases listed in the Kyoto Protocol (CH4, N2O, HFCs, PFCs, SF6, and NF3). Equivalents are calculated using a 100-year time horizon for CO_2eq emissions of non-CO_2 gases.

E1-6 GHG intensity based on net revenue

F-Secure calculates GHG intensity based on net revenue by dividing total GHG emissions (t CO_2eq) by net revenue (€). Values are represented both in market-based and location-based methods. Net revenue is based on our financial statement (Cross-reference to financial section 3. Revenue) and our E1-6 GHG intensity is presented in the table below.

GHG intensity per net revenue	2024 base year	2025
Total GHG emissions (location-based) per net revenue in millions (tCO_2eq/MEUR)	58.76	58.41
Total GHG emissions (market-based) per net revenue in millions (tCO_2eq/MEUR)	58.46	58.17
Net revenue used to calculate GHG intensity		
Total net revenue (in financial statements) MEUR	146.30	€ 146

Table 24. GHG intensity per net revenue.

GROUP SUSTAINABILITY REPORT -

Social

S1 – Own workforce

SBM-3 Material impacts, risks and opportunitites

	Material impact, risk or opportunity	Description
Working conditions		
Work-life balance		
Actual positive impact (OO)	Family leaves	Family leaves for F-Secure employees exceeding local requirements in some countries.
Health and safety		
Risk (OO)	Workload and mental wellbeing	Mental health related absences detected.
Equal treatment and opportunities for all		
Gender equality and equal pay for work of equal value		
Actual positive impact (OO)	Promoting gender equality	Recruiting and advancing women and under-represented groups and mitigating the gender pay gap.
Training and skills development		
Opportunity (OO)	Use of AI in workforce development	Process improvements, competency maturity and AI sentiment
Actual positive impact (OO)	Learning and development	Further ramp up strategic learning and development activities and track investment into learning activities.
Potential positive impact (OO)	Critical strategic competences	Continuously identify the internal competencies critical to our strategy.
Risk (OO)	Talent acquisition and retention	Loss of key persons or inability to acquire new talent
Measures against violence and harassment in the workplace		
Actual positive impact (OO)	Inclusive culture with a speak up-culture	Inclusive culture where the workplace is a safe environment for everyone. We foster a speak-up culture (“dare to care”).
Measures against violence and harassment in the workplace		
Opportunity (OO)	Employer reputation	Especially younger generations value DEI topics and we need to ensure that F-Secure meet expectations.

Table 25. Own workforce IROs.

F-Secure has identified key impacts, risks, and opportunities (IROs) related to working conditions, equal treatment, and career development. The company aims to support an inclusive culture, promote equality, and encourage a healthy work–life balance in order to provide conditions that enable employees to perform effectively.

No material negative impacts have been identified related to our workforce, whether widespread, systemic, or linked to individual incidents.

F-Secure material impacts, risks, and opportunities are related to all people in its workforce.

Interaction with strategy and business model

F-Secure's actual and potential workforce impacts—covering working conditions, equal treatment, well-being, and career development—originate directly from its strategy and people-driven business model. Through ESG materiality assessments and HR processes, these impacts, risks, and opportunities are systematically identified and evaluated.

Positive impacts, such as inclusive practices, skill development, and work–life balance initiatives, strengthen the company's ability to attract and retain talent and therefore support strategic execution. Similarly, risks such as burnout or turnover inform workforce planning and guide improvements to employment practices. The insights gained from these assessments contribute to adapting the strategy and business model, ensuring alignment between workforce impacts and long-term business performance.

Disclosure scope

All employees who can be materially impacted by F-Secure are included in this disclosure scope, encompassing impacts connected with their own operations.

Types of employees

F-Secure measures full-time employees by FTEs (full-time equivalent) with no "non-guaranteed hours" employees. Employee categories include:

- **Permanent employees:** Employed with no predefined contract end date
- **Fixed-term employees:** Hired for a specific duration with defined end dates
- **Contractors:** All non-employees, including Employee-like (integral team participants), Consultants (project-based supplementary workforce), and Other (facility access without system access)

The types of non-employees include "Employee-like", "Consultant" and "Other" as described in more detail next.

Employee-like (also called "Fellowlike"):

- An integral part of the F-Secure teams, participating in daily activities and team meetings. Usually, contracts are fixed and time-based. Regardless of the contractor status, our contract with any non-employee is with a legal entity and not with a natural person.
- Examples of Employee-like who work for a third party engaged in "labor activities" and whose work is managed by the company: People who do the same work as our employees, in case those are temporarily absent (due to illness, vacation, parental leave, etc.) or work in the same workplace as our employees

Consultant

- Consultants are contractors who supplement F-Secure's workforce on a project basis, related to a specific assignment or project in question. Regardless of the contractor status, our contract with any non-employee is with a legal entity and not with a natural person.
- They may have the necessary access to a F-Secure facility or to F-Secure systems based on, e.g., a project or frame agreement to perform their duties.

Other

- Covers non-employees who have access to a F-Secure facility but not to F-Secure systems, such as Board members or people providing facility services.

Impact, risk and opportunity management

S1-1 Policies

This section specifies the material sustainability topics addressed by each policy and clearly outlines the target audience for each policy, maintaining transparency and alignment with F-Secure's sustainability objectives.

In developing workforce-related policies, F-Secure considers the interests and needs of employees through continuous feedback mechanisms such as employee surveys, development discussions, consultation with employee representatives, and insights gathered through internal materiality assessments. These inputs help ensure that policies address the most relevant impacts, risks, and opportunities identified by the workforce. All workforce-related policies are made available to employees through the company intranet. Policy updates are communicated through internal channels, and managers are responsible for ensuring employees are aware of policy requirements. Mandatory training modules (e.g., Code of Conduct) ensure that key policies are understood and implemented across the organization.

Additional details on F-Secure's Code of Conduct are provided in *ESRS G1-1*.

F-Secure supplier code of conduct includes provisions addressing the safety of workers, precarious work, human trafficking, the use of forced labour or child labour, and is fully in line with applicable ILO standards.

Policy	Key Contents	Scope	Responsibility	Link to IROs
DEI Policy	Promotes diversity, equity, and inclusion aligned with values and Code of Conduct Anti-harassment and non-discrimination guidelines Targets for talent acquisition and accountability mechanisms Training, targeted recruitment, programs supporting vulnerable groups and leadership development DEI Committee	All employees, employee-like contractors, leadership.	CPO (Chief People Officer)	Employer reputation Promoting gender equality Inclusive culture with a speak up-culture
Recruitment Policy	Fair and transparent hiring processes Adherence to local requirements and non-discrimination laws Background checks and compliance factors Recruitment process, employer branding, metrics, legal considerations Aligned with ILO principles on non-discrimination and equal opportunity Addresses training and skills development aligned with DEI goals	All employees, leadership and employee-like contractors	CPO	Promoting gender equality Learning and development Critical strategic competences Talent acquisition and retention

Policy	Key Contents	Scope	Responsibility	Link to IROs
Health and Well-being Policy	Principles and practices for employee health and well-being Healthy work culture, leadership role, local health compliance Health activities, continuous learning, flexible work environments Monitoring success of activities Adherence to local legislation and regulatory standards Addresses work-life balance, health and safety (ILO standards)	All employees and leadership	CPO	Family leaves Workload and mental wellbeing Talent acquisition and retention Inclusive culture with a speak up-culture
Learning and Development Policy	Continuous learning to enhance workforce expertise Foster collaboration and structured learning frameworks Training definition, roles and responsibilities Learning framework, data management and reporting Measuring effectiveness of learning efforts Addresses training and skills development	All employees and leadership	CPO	Use of AI in workforce development Critical strategic competences Talent acquisition and retention
Rewards and Recognition Policy	Fair and transparent rewarding principles and practices Job architecture, base salary, benefits, incentive plans Recognition and pensions Rewards framework consistent with global standards Aligned with OECD and ILO principles Addresses fair and equal treatment and transparent working conditions	All employees and leadership	CPO	Promoting gender equality Critical strategic competences Talent acquisition and retention

Table 26. Own workforce policies.

Human Rights Policy Commitments

F-Secure's workforce policies align with international standards, including OECD Guidelines for Multinational Enterprises, UN Global Compact, UN Guiding Principles on Business and Human Rights, ILO Declaration on Fundamental Principles and Rights at Work, and the International Bill of Human Rights. These principles are embedded throughout our policies as detailed below. Human rights are incorporated in our Code of Conduct, with which all F-Secure employees must comply.

Our commitment focuses on three core areas:

- **Respect for Human Rights** - Uphold global standards, respect freedom of opinion, expression, conscience, and religion; act swiftly on adverse impacts; protect digital lives by combating scams.
- **Labor Rights & Safety** - Ensure compliance with laws, safe working conditions, freedom of association, and zero tolerance for child labor, forced labor, or trafficking.
- **Application of Standards -** If local laws are less restrictive than the Code of Conduct, the Code of Conduct prevails. If local laws are more restrictive, those laws are followed for compliance. F-Secure suppliers and partners are also expected to act responsibly and comply with principles set in the Code of Conduct and local laws.

Furthermore, F-Secure does not operate in industries/sectors where the risk of forced, compulsory, or child labour is significant. F-Secure has an office in Malaysia and employees in India, which are considered countries with higher risks. However, F-Secure hires educated specialists and leaders and conducts background checks during the hiring process as part of our Recruitment Policy, which reduces the risk.

Engagement with our workforce

F-Secure has established systematic workforce engagement methods, including regular Townhalls, personnel surveys, and workers' representative consultations. Detailed engagement processes are described in section *S1-2 Processes for engagement about impacts.*

Measures to provide and/or enable remedies for human rights impacts

F-Secure provides multiple channels for employees to raise human rights concerns, including direct contact with managers, HR, Legal, or via the Whistleblowing channel. All concerns are handled confidentially. For detailed information on reporting channels and remediation processes, see section *S1-3 Processes to remediate negative impacts and channels to raise concerns.*

Policies addressing trafficking in human beings, forced labor and child labor

F-Secure's Human Rights Policy prohibits child labor, forced labor, human trafficking, and other violations, with background checks as part of our Recruitment Policy and compliance with local labor laws, regularly updated to align with legal requirements.

Workplace accident prevention

F-Secure tracks and manages workplace accidents using HR systems, where all incidents are reported and monitored for compliance with local laws and regulations. While physical injuries are rare in the software and cybersecurity industry, any workplace accident or harm is recorded and managed according to country-specific practices. Our intranet provides employees with detailed workplace safety information. We define occupational accidents as unexpected events resulting in injury, including incidents within the workplace, during business trips, or while carrying out employer-ordered errands. We address injuries such as muscle or tendon pain, which may be compensable under certain conditions.

Any occupational accident is addressed according to local legislation and requirements, and occupational healthcare is provided by F-Secure.

S1-2 Processes for engagement about impacts

F-Secure actively incorporates the perspectives of its employees into the management of workforce-related impacts, risks, and opportunities. Senior leadership—comprising the CEO, Chief People Officer, and Leadership Team —leads employee engagement through regular Townhalls and monthly Leadership Forums.

F-Secure has established systematic methods to engage with its workforce:

1. **Employee Engagement**: Monthly Townhalls with Q&A, function-specific all-hands meetings, Leadership Lab for Team Leaders, and digital suggestion channel promote inclusive participation.
2. **Employee Feedback**: Biannual anonymous personnel surveys are conducted to gather feedback from all employees. The results are analyzed and presented at company, function, and team levels (where at least five responses are available). Other feedback mechanisms such as the whistleblowing channel, exit interviews and HR consultations.
3. **Project-Based Engagement**: Employees participate in specific processes or projects, such as people processes or cultural initiatives.
4. **Workers' representatives**: People and Culture Operations Director organize monthly meetings with Shop Steward to address current topics. HR Board meets monthly with Shop Steward and country-specific elected representatives (People & Culture Advisor)
5. **Collective Bargaining Compliance**: F-Secure adheres to collective bargaining agreements in Finland, France, and Spain, maintaining alignment of policies and practices through the People & Culture Operations Director.

Accessibility and Inclusivity

In addition to the engagement methods described above, F-Secure places strong emphasis on accessibility and inclusivity as essential components of workforce engagement. The company ensures equal participation by offering accessible Learning Management Systems and survey tools with screen reader compatibility, text-to-speech features, and closed captioning. Virtual Townhalls include real-time captions and recorded transcripts in audio and text formats. Wheelchair-accessible facilities and clear, easy-to-understand language across all communications enable employees with mobility or cognitive disabilities to engage fully. These measures reflect F-Secure's commitment to ensuring that every employee can contribute and participate without barriers.

Insights from these channels are used to identify and reassess material workforce IROs, including topics such as well-being, workload, equal treatment, skills development, and workplace culture. Employee feedback directly informs decisions related to improvement actions, for example, updates to hybrid work practices, development of well-being initiatives, targeted training programs, and adjustments to career development frameworks.

This process ensures that employee needs and expectations are considered when designing and implementing measures to manage both actual and potential impacts on the workforce.

S1-3 Processes to remediate negative impacts and channels to raise concerns

F-Secure strongly encourages employees to speak up regarding concerns related to their employment or daily work. We aim to avoid adverse human rights impacts and take actions to remediate them when they occur. Every employee at F-Secure has the right and obligation to raise concerns about Code of Conduct violations, including human rights.

Our organization assesses potential negative impacts through structured processes. We assess the effectiveness of the remedy provided through follow-up reviews with the affected individuals, monitoring for recurrence of the issue, and evaluating whether the corrective actions have addressed the root cause. Feedback from employees, case-closure criteria, and ongoing monitoring help us confirm that the remedy has achieved its intended outcome.

Primary Reporting Channels

Concerns should primarily be reported through:

- Team leader, local People & Culture advisor, legal or personnel surveys
- Verbal or electronic communication methods
- Team leader's leader or People & Culture if issues relate to the direct team leader
- Shop Steward or employee representatives
- Direct contact with the CEO or Board of Directors

The Whistleblowing Channel serves as a way for anonymous reporting (see G1-1 for details). All concerns are handled confidentially, reviewed thoroughly, and addressed through appropriate measures for any Code of Conduct violations, including human rights. Retaliation against anyone raising a good-faith concern is strictly prohibited. We actively communicate and train team leaders and employees on the available reporting channels, which are regularly updated on our intranet.

Our whistleblowing channel is operated through a third-party provider to ensure independence, confidentiality, and anonymity. The channel is made available and maintained by F-Secure, but the reporting mechanism itself is administered externally.

We are committed to maintaining a culture where everyone feels comfortable raising good-faith concerns about employment or daily work. We do not tolerate adverse action against anyone who raises good-faith concerns. We actively communicate and train team leaders and employees on ways and channels for raising concerns. Channels are updated regularly on our intranet.

Assessment and Continuous Improvement

We assess awareness and trust in our structures and processes through:

- Regular employee surveys (biannual personnel surveys)
- Feedback mechanisms (1-on-1 meetings with team leaders and Townhalls)
- Trust metrics tracking, such as eNPS (employee Net Promoter Score)

These surveys and feedback channels gauge employees' understanding of internal processes and confidence in the company's commitment to transparency, ethics, and fairness. Results are used to identify areas for improvement and drive continuous enhancement of our practices. All reporting channels are easily accessible to employees across all levels of the organization.

S1-4 Actions and resources

Scope: All employees globally; targeted initiatives for underrepresented groups.
Time Horizon: Ongoing; programs launched and maintained in 2025.

Actions to address material impacts

F-Secure actively implements measures to enhance positive impacts on its workforce while managing related risks and opportunities identified in the materiality assessment. The company's initiatives focus on maintaining a stable, equitable, and inclusive working environment, as outlined below. No actual

or potential negative impacts related to F-Secure's own workforce have been identified that exceed the threshold defined in the impact, risk, and opportunity assessment conducted as part of the DMA.

Family leaves

F-Secure is committed to creating an inclusive and supportive work environment where employees can balance personal and professional responsibilities. We ensure equal access to parental and caregiving leave so that no one is disadvantaged for prioritizing family. Our Wellbeing Strategy focuses on strengthening physical, mental, and emotional health through proactive programs and initiatives. Comprehensive support is provided across Finland, India, the US, and Malaysia, addressing risks such as stress and burnout while promoting long-term health and satisfaction. In addition, the Culture, Health & Well-being Committee ensures compliance with both global and local health and safety standards, embedding well-being into our culture and everyday practices.

Learning and Development

Targeted training for R&D and leadership roles supports upskilling, addresses skill shortages, and promotes career growth. F-Secure enhances workforce competencies through capability and competence analysis, employee surveys, and centralized training via the Learning Management System (LMS).

Gender Equality

A diverse workforce is a strategically important topic for F-Secure, and due to this, we have implemented targeted recruitment for underrepresented groups.

Culture Building

We take action to foster a speak-up culture via training and feedback mechanisms, which we have continued to develop in 2025. We have linked our monthly superheroes to our cultural values, and they are presented at our Townhalls. This creates a clear link between the desired behavior of a Fellow and the culture we want to develop.

Secure Employment and Flexible Workplace

F-Secure offers stability by prioritizing permanent contracts over fixed-term agreements, minimizing uncertainty for employees. Remote/ Hybrid work allows employees to work from home several days a week, promoting work-life balance and improving well-being. In regions like India and Malaysia, where commuting can be time-consuming, remote/hybrid work enhances employee satisfaction and productivity. Progress: Engagement with DEI rate.

Fair Working Environment

We continuously evaluate and update policies and procedures across all locations for full compliance with local, regional, and national regulations. This maintains a fair and transparent work environment, fostering trust and inclusivity. Comprehensive benefits suite includes health insurance and vacation/leaves, offering mental health and personal well-being resources.

Prevention of Negative Impacts on Workforce

F-Secure has assessed its practices and confirms that it does not cause or contribute to material negative impacts on its own workforce. Our employment practices are governed by global HR policies, the Code of Conduct, and data protection standards, which ensure fair, safe, and responsible working conditions.

To ensure we do not cause or contribute to negative impacts, we monitor workforce well-being, engagement, development, and workplace conditions through surveys, absence trend analysis, performance processes, and established grievance and whistleblowing channels. No tensions were identified between preventing negative impacts and other business pressures during the reporting period.

We expect to continue monitoring and assessing key workforce areas—including employee well-being, engagement, development, and the effectiveness of HR processes—throughout the strategy period (2026–2028). These activities did not require any material operating (Opex) or capital expenditures (Capex) in 2025, and we expect this to remain unchanged during the strategy period.

Tracking Effectiveness

Systematic Tracking Methods:

- **Employee Surveys**: Anonymous engagement surveys, including eNPS, to monitor workforce satisfaction
- **Policy Reviews**: Regular evaluations for compliance with labor laws and international standards
- **Gender Equality Monitoring**: Pay gap analyses conducted before and after salary reviews
- **Culture Assessment**: Biannual surveys measuring eNPS, retention rates, and leadership effectiveness
- **Sustainability Council reviews**: Updates on Own workforce related topics through DEI and Wellbeing Committee.

Actions related to material opportunities

Actions related to our material opportunities were executed during 2025. We continue to see them as relevant also for the current strategy period (2026-2028):

Opportunity	Actions 2025	Effectiveness Measures and expected outcomes
Employer Reputation	DEI development projects DEI talks platform Mothers in business Program Women in Tech Initiatives	Strengthened talent, attraction, and retention. Employer brand engagement metrics
Use of AI	Implement AI tools to enhance employee experience and processes	Improved efficiency & consistent solutions across the organization

Table 28. Actions to pursue own workforce opportunities.

Actions to mitigate material risks

We have identified two risks with corresponding mitigation strategies as listed in the table below. These mitigation activities were executed in 2025 in our own workforce, and we see them as relevant during the strategy period (2026-2028):

Risk	Actions 2025	Effectiveness Measures and expected outcomes
Employee Workload and Well-being	Provide well-being programs, support resources, and regular check-ins. Monitor health trends and ensure adequate healthcare coverage. Occupational Health Care (Finland). Comprehensive health coverage (India, US, France and Malaysia)	Engagement and Fellow survey feedback Well-being initiative participation rates Absence and Mental health-related tracking Ensure wellbeing in workforce
Talent Acquisition and Retention	Recruitment aligned with strategic workforce planning and strengthened pre/onboarding & development Programs Support career growth and leadership development through centralized learning Management system.	Time-to-hire metrics Total attrition and HiPo retention rates Engagement, training & Performance review completion rates. Talent density % & Succession pipeline % Build a future-ready workforce by attracting the right talent, accelerating development, and improving retention through strategic hiring, effective onboarding, and continuous learning

Table 27. Actions to mitigate own workforce risks.

Resource Allocation:

- **People and Culture function:**

Manages all material impacts, risks, and opportunities related to our workforce, covering all employees globally. This includes oversight of the full employee experience, from recruitment and onboarding to talent development, performance management, diversity and inclusion, well-being initiatives, payroll and rewards, HR systems, and support for all regional offices. In addition, well-being and DEI activities are coordinated through cross-functional committees that represent employees across the organization.

Metrics and targets

S1-5 Targets

F-Secure has defined the following absolute targets related to its own workforce.

Methodologies and frameworks

Methodologies for collecting and tracking targets are based on F-Secure's HR systems as described under each target. Metrics have been selected based on alignment with material F-Secure ESG topics, ESG regulation, DMA, and stakeholder feedback. Targets have been approved by the Board of Directors.

S1-5 Own workforce targets

Target	Baseline 2023	2024	2025	2030 target
Gender Diversity (directors including leadership team, %)	F: 23 M: 77	F: 23,5% ; M: 76,5 %[1]	F: 25.81%; M: 74.19%	F: 33 M: 67
Gender Diversity (all employees)	*Third gender not implemented, F: 30% M: 70%*	M- 69.19%; F- 30.62%	F: 30,29%; M: 69,71%; ND:0,18%	No gender should represent more than 65% of workers.
Nationality among senior management	24	28	28	> 20
Age target (all employees, age groups are <30, 30-40, 40-50, 50-60 and 60-70)	Under 30: 22.1%, under 40: 35.7%, under 50: 29.4%, under 60: 11.1%, above: 60 1.7%	Under 30: 20,6%, under 40: 36,7%, under 50: 30,1%, under 60: 11,5%, above: 60 1,1%	Under 30: 20,77%, under 40: 36,98%, under 50: 29,14%, under 60: 11,66%, above: 60 1,46%	No age group should represent more than 35% of the total
eNPS evolution	2	40	33	> 50
Performance and career review target	*Baseline year is 2024*	88%[2]	98.91%	98%

1) The percentage for Gender Diversity directors including leadership team, % target has been corrected for 2024 reported numbers (F: 25.1% ; M: 74.9%).

2) The percentage for Performance and career review target has been corrected for 2024 reported numbers (82.04%).

Table 29. Own workforce targets.

S1-5 Progress towards targets

Diversity (DEI) related targets

These targets help make intentional hiring and promotion decisions based on skills and competencies in alignment with our values, driving inclusion and equality. Targets are set by the F-Secure Chief People Officer and apply globally. We review progress regularly and build remediation plans when negative trends or issues are identified.

1. Gender Diversity - Directorss: We have set a 2030 gender target that 33% of senior leaders at the director level should be female. This target applies globally to all F-Secure employees, excluding contractors and employee-like consultants. The baseline year is 2023 with 23% female representation. Our 2025 outcome is 25.81% female and M: 74.19%% male representation among senior leaders.

Progress is measured using HR management system data, aligning with the EU gender equality strategy 2020–2025 and the directive on gender balance in corporate boards.

2. Gender Diversity - All Employees: This target reinforces F-Secure's commitment to gender inclusivity beyond binary categories, maintaining fair representation of all genders. We have set a target that no gender (including third gender) should represent more than 65% of the workforce by 2030. The baseline year is 2023 with 70% male representation. Our 2025 outcome is 69,71% male representation.

Data is collected through the HR system, where employees can self-identify as male, female, or third gender. Goals align with international standards on gender equality, including the EU gender equality strategy.

3. Nationality Among Senior Management: Maintaining nationality diversity provides global representation in decision-making and fosters inclusive environment where leadership reflects our diverse workforce. F-Secure maintains or exceeds 20 nationalities within senior leadership positions. Our baseline year is 2023 with 24 nationalities represented. Our 2025 outcome is 28 nationalities.

4. Age Target: Age diversity fosters a vibrant workforce with wide-ranging experiences. By preventing single age group dominance, we create space for intergenerational learning, innovation, and mentorship. We have set a 2030 target that no single age group represents more than 35% of total workforce. Our baseline year is 2023 where the largest age group represented 35.7% of workforce (30-40y).

Our 2025 outcome shows one age group exceeding 35%, specifically the 30-40y group at 36,98%.

Employee well-being and satisfaction (eNPS)

The eNPS target relates to our health and well-being policy. Employee NPS score directly reflects company culture health, leadership effectiveness, and employee well-being. Higher eNPS indicates more engaged and satisfied workforce, aligned with cultivating healthy and inclusive work environment.

We have set a target to reach an eNPS above 50 in 2030, excluding contractors. This absolute target is measured on a scale from -100 to +100. Our baseline year is 2023 with an eNPS score of 2. Our 2025 outcome is 33.

eNPS is measured through regular anonymous employee surveys using the same survey tool globally. The eNPS target is defined by F-Secure's CPO, and when part of remuneration plans like a non-sales STI plan, also with the CEO.

Performance review

This target supports the company's Performance Dialogue policies and process, maintaining that employees actively set and follow up on development goals. It fosters continuous professional growth by aligning individual aspirations with organizational vision and strategy.

Our target is to achieve 98% completion rate of performance and career target setting for all employees by 2030. This applies to all company employees globally, excluding employee-like contractors unless specified otherwise. 2024 is the first year to capture data, serving as baseline year. Our 2025 outcome is 98.91%.

Target setting process and engagement with the workforce

Overall company-level targets for short term (fiscal year) and strategy period (typically 3 years) are defined by the Leadership Team. For Own Workforce-related measures, targets are defined by the CPO in collaboration with other Leadership Team members, Sustainability Council and the CEO for part of incentive schemes.

Employee input into target setting is considered based on surveys conducted during the year or experts participating in target setting within respective functions. Progress is shared with workforce through monthly Townhalls and internal communications, where feedback is gathered to improve actions or policies aimed at achieving targets.

Employee engagement (eNPS) is measured through regular anonymous employee surveys using a standardized global tool. Corrective actions are identified based on survey results at the company, function, and individual team levels.

Individual performance and development goals are jointly defined by line managers and employees at year start, aligned with company and function plans. Progress is tracked through regular 1:1 meetings and team discussions. Mid-year reviews assess organizational progress, and end-of-year reviews reflect on goal achievement, alignment with company values, and future development plans documented in the HR system.

S1-6 Characteristics of the undertaking´s employees

Methodologies and assumptions used to compile and report the data

The data for this disclosure is sourced from our HR system (Workday), which serves as the single source of truth for all workforce data, maintaining accuracy and consistency across all reporting metrics.

Methodology:

- **Data Entry and Categorization**: All employees, including permanent and fixed-term employees, are managed through the HR system. This ensures all workforce data, regardless of employment type, is systematically recorded and tracked in a standardized manner.
- **Processes and Validation**: Standardized data entry processes with regular validation steps, including cross-checks by HR teams to confirm data accuracy
- **Data Reporting**: Metrics are directly derived from the HR system and extracted through consolidated reporting tools to reduce errors and maintain reliability

The reporting period is annual, and workforce data is captured through the HR system, providing real-time data on headcount. Data reflects status at the end of the reporting period.

Cross-reference with financial statements

The measures provided in the group sustainability report own workforce section are aligned with related data provided in other sections of the annual report noting that average annual number of personnel is used in the financial statement (Cross-reference to financial section 7. Personnel expenses).

S1-6 Employee gender

Gender	Number of employees, 2024	Number of employees, 2025
Male	366	382
Female	162	166
Non-Binary	0	
Not reported	1	1
Total Employees	529	549

Table 30. Employee gender.

S1-6 Employee per country

Country	Number of employees, 2024	Number of employees, 2025
Finland	270	266
India	70	105
Malaysia	74	76
Total	**414**	**447**

Table 31. Employee per country.

S1-6 Employee turnover

Employee turnover is calculated as the number of employees who have left voluntarily or due to dismissal, retirement, or death in service, divided by the F-Secure headcount as of December 31, 2025.

Employee turnover in the reporting period, by number of employees	2024	2025
Total number	107	103
Rate, %	20.23%	18.76%

Table 32. Employee turnover.

S1-6 Employee per contract

2024

Employee per contract type, head count	Female	Male	Other[1]	Not disclosed	Total
Number of employees	162	366	0	1	529
Number of permanent employees	160	364	0	1	525
Number of temporary employees	2	2	0	0	4
Number of non-guaranteed hours employees	0	0	0	0	0
Number of full-time employees	153	359	0	1	513
Number of part-time employees	9	7	0	0	16

1) Gender as specified by the employee themselves.

Table 33. Employee per contract 2024.

2025

Employee per contract type, head count	Female	Male	Other[1]	Not disclosed	Total
Number of employees	166	382	0	1	549
Number of permanent employees	164	378	0	1	543
Number of temporary employees	2	4	0	0	6
Number of non-guaranteed hours employees	0	0	0	0	0
Number of full-time employees	159	373	0	1	533
Number of part-time employees	7	9	0	0	16

1) Gender as specified by the employee themselves.

Table 34. Employee per contract 2025.

S1-6 Employee per region

2024

Employee per region, head count	Europe	North America	Asia[1]	Total
Number of employees	347	33	149	529
Number of permanent employees	343	33	149	525
Number of temporary employees	4	0	0	4
Number of non-guaranteed hours employees	0	0	0	0
Number of full-time employees	331	33	149	513
Number of part-time employees	16	0	0	16

1) Gender as specified by the employee themselves.

Table 35. Employee per region 2024.

2025

Employee per region, head count	Europe	North America	Asia[1]	Total
Number of employees	332	30	187	549
Number of permanent employees	328	30	185	543
Number of temporary employees	4	0	2	6
Number of non-guaranteed hours employees	0	0	0	0
Number of full-time employees	316	30	187	533
Number of part-time employees	16	0	0	16

1) Gender as specified by the employee themselves.

Table 36. Employee per region 2025.

S1-9 Diversity metrics

Methodology

Age Distribution by Job Grade: Employees under 30, 30–50, and over 50 years.

Gender Distribution by Job Grade and Compensation Grade: Gender representation across all F-Secure's job grades, and the gender distribution in number and percentage at the top management level. According to F-Secure's Job Architecture, employees in roles classified as F6 and above are considered part of top management.

Data includes employees only and excludes contractors.

Our HR system allows employees to self-identify their gender as female, male, other, or not declared, ensuring inclusivity and respect for all gender identities. The term "other" refers to individuals whose gender identity does not fall strictly within the categories of male or female.

S1-9 Gender distribution

Gender distribution of top management, 2024	Female	Male	Other
Total number	12	39	0
Percentage, %	23.5%	76.5%	0
Gender distribution of top management, 2025	**Female**	**Male**	**Other**
Total number	16	46	0
Percentage, %	25.81%	74.19%	0

Table 37. Gender distribution.

S1-9 Age distribution

Distribution of employees by age group, 2024	Under 30 years old	30 - 50	Over 50
Total number	109	353	67
Percentage, %	20.60%	66.73%	12.67%
Distribution of employees by age group, 2025	**Under 30 years old**	**30 - 50**	**Over 50**
Total number	114	363	72
Percentage, %	20.77%	66.12%	13.11%

Table 38. Age distribution.

S1-13 Training and skills development metrics

Methodology

Data is available on e-learning completions and global training session participation since August 2023 in our Learning Management System (LMS). Each employee undergoes two performance reviews per year: mid-year and end-of-year reviews assessing goal achievement and overall performance.

S1-13 Training

2024	Female	Male	Other	Total
Percentage of employees that participated in regular performance and career development reviews (%)	85.8%	88.2%	No Other Gender as of review date	88%[1]
Number of performance reviews per employee	1.68	1,70		1.7
Average number of training hours per employee (h)				1.84

1) This excludes a single employee who has not reported gender

Table 39. Training and skills development metrics 2024.

2025	Female	Male	Other	Total
Percentage of employees that participated in regular performance and career development reviews (%)	98.78%	98.95%	100%	98.91%[1]
Number of performance reviews per employee	2.79	2.70	3.00	2.72
Average number of training hours per employee (h)				1.48

1) This excludes a single employee who has not reported gender

Table 40. Training and skills development metrics 2025.

Performance and career development review percentage is calculated based on all employees as of December 31, 2025, counting each employee once regardless of whether they had 1 or 2 reviews during the year, excluding employees terminated during 2025.

S1-14 Health and safety metrics

During autumn 2024, we introduced a dedicated form within our HR system to systematically track work-related accidents and resulting absences. This initiative enhances monitoring of workplace incidents with a proactive approach to employee health and safety. For 2024, employees were requested to retrospectively record any accidents that occurred earlier in the year. Beginning in 2025, all accident reports are expected to be submitted promptly following incident occurrence.

In Finland, where we have a large portion of employees, all health-related data is managed by our occupational health care provider, providing valuable insights into workforce health and safety and guiding preventive measures and policies.

S1-14 Health and safety

	2024	2025
Percentage of people in its own workforce who are covered by the undertaking's health and safety management system based on legal requirements and/or recognized standards or guidelines,%	100%	100%
Number of fatalities as a result of work-related injuries and work-related ill health	0	0
Number and share of recordable work-related accidents	0	0

Table 41. Health and safety metrics.

Health and safety data include only employees. F-Secure has chosen to omit the number of cases of recordable work-related ill health and the number of days lost to work-related injuries, subject to legal restrictions on data collection.

S1-15 Work-life balance metric

All employees are entitled to take family leave as outlined by applicable laws of the countries, company policies, and collective agreements where relevant. F-Secure supports work-life balance culture, maintaining that employees can access and utilize family leave without barriers. F-Secure actively monitors these metrics to ensure equitable access to family leave across all genders. We remain committed to addressing any gaps in usage or access to support our broader objectives of work-life balance and inclusion.

S1-15 Work-life balance

Data point	2024	2025
Percentage of employees entitled to family leave	100%	100%
Percentage of employed personnel who took family leave, broken down by gender	Male: 3.2% Female: 2.6% Total: 5.86%	Female: 3.46%; Male: 4.55%; Total: 8.01%

Table 42. Work-life balance metrics.

S1-16 Remuneration metrics

The main data source is our HR system from where we extract the annual base salary, and the annual total of allowances and benefits paid on top of the base salary valid at the end of the year. We also extract the total amount of one-time payments (including incentives), and overtime compensation (where available) paid during the year. The annual payout amounts from the LTI programs are also obtained. After extracting the data, we calculate the annual total compensation per employee in euros and sort the amounts from the highest to the lowest.

We use the following formula to calculate the gender pay gap and express the outcome as a percentage: (Average annual total compensation of male employees – average annual total compensation of female employees) divided by the average annual total compensation of male employees.

For the annual total remuneration ratio, we first calculate the median annual total compensation amount excluding the highest amount. Then we calculate the ratio using the following formula: (The highest annual total compensation amount) divided by (the median annual total compensation amount).The CEO is excluded from pay gap calculation.

S1-16 Remuneration

Remuneration	2024	2025
Gender pay gap, %	12.74%	8.15%
The annual total remuneration ratio of the highest paid individual to the median annual total remuneration for all employees	5.11	7.17

Table 43. Remuneration metrics.

F-Secure measures the pay gap as part of our annual global salary increase process.

S1-17 Incidents, complaints and severe human rights impacts

F-Secure is committed to fostering an inclusive and respectful workplace where all forms of discrimination are prohibited. In alignment with our zero-tolerance policy, we closely monitor and address any incidents of discrimination or harassment across all operations. During the reporting period, there have been no reported work-related incidents of discrimination based on gender, racial or ethnic origin, nationality, religion or belief, disability, age, sexual orientation, or other forms of discrimination involving internal or external stakeholders.

F-Secure provides a confidential **Whistleblowing Channel**, accessible 24/7 to all employees and stakeholders. This platform supports transparent and ethical business conduct by enabling the safe reporting of concerns related to discrimination, harassment, or unfair treatment. All reports are handled in accordance with F-Secure's governance framework, privacy standards, and applicable local legislation, reinforcing our dedication to integrity, accountability, and respect for human rights.

S1-17 Incidents

	2024	2025
Harassment & discrimination		
Total number of incidents of discrimination, including harassment, reported in the reporting period	0	0
Number of complaints made through channels available to the company's own employees (including grievance mechanisms)	0	0
Total amount of material fines, penalties, and compensation for damages as a result of the incidents and complaints disclosed above	0	0
Severe human rights incidents		
Number of severe human rights incidents connected to the undertaking's workforce in the reporting period	0	0
Total amount of fines, penalties and compensation for damages for the incidents described above	0	0

Table 44. Incidents, complaints and severe human rights impacts.

S4 – Consumers and end-users

SBM-3 Material impacts, risks and opportunities

F-Secure confirms that all consumers impacted by F-Secure are in the scope of S4 disclosure. "Consumers" and "end-users" are used as synonyms unless stated otherwise.

	Material impact, risk or opportunity	Description
Personal safety of consumers and/ or end-users		
Security of a person - Protecting our customers		
Opportunity (OO)	Use of AI in security applications	AI-powered monitoring tools observe user behavior, detect anomalies, and react accordingly
Opportunity (OO)	Evolving threat landscape	Scams have become commonplace. Opportunities to offer engaging and relevant protection services
Risk (OO)	Consumer willingness to pay	Intensifying competition and negative macro-economic situation may have negative impact on consumer willingness to pay.
Risk (DVC)	Channel strategy	Significant agreement changes or loss of a major Service Provider account, or Direct Business decline
Actual positive impact (OO)	Protecting digital moments	According to our product questionnaire, consumers are worried about their online protection. F-Secure provides solutions to these threats through its offering.
Risk (DVC/UVC, OO)	Security of vendors and partners	Security vulnerabilities from suppliers and partners, relying on external vendors, especially vendors who are one step removed in the supply chain, adds layers of vulnerability.
Risk (OO)	AI increases risk of security breach	Effective AI experimentation and roll-out dependent on high quality data sources and may also increases risk of a security breach.
Risk (OO)	Cyber security	Cyber security attacks negatively impact reputation and business
Information-related impacts for consumers and/or end-users		
Access to (quality) information (Awareness and education)		
Actual positive impact (DVC, OO)	Create awareness about cybercrimes	Increase consumers awareness about cybersecurity and cybercrime through marketing campaigns and events.

Table 45. Consumers and end-users list of IROs.

Interaction with strategy and business model

F-Secure has identified an actual positive impact in protecting consumers' digital moments, which continues to guide company strategy, decision-making and execution during 2025 and for the next strategy period (2026-2028):

1. **Product and Technology Investments:** Provide relevant, engaging and effective protection against modern threats through innovation, threat research, and consumer needs analysis. Our portfolio and protection roadmaps focus on scam protection and leveraging AI capabilities for both effective protection and engaging user experience.
2. **Growth Opportunities:** The evolving threat landscape, including the rise of scams and cybercriminals using AI, presents significant growth opportunities for F-Secure and our Service Provider partners. We leverage AI as an

opportunity to innovate new protection capabilities, improve customer experience, and increase internal efficiencies.

3. **Channel Sales Model**: Develop our channel sales capabilities further and continue to build a portfolio that is "fit to channel" to reach large customer bases through our partners. Increase cyber threat awareness both directly and through our 200 channel partners by offering free tools and providing educational content

We recognize risks in our channel strategy, including changes in agreement scope, potential loss of significant Service Provider partners, and requirements especially when working with Tier 1 Service Providers. These risks could impact revenue, increase costs, or hinder operations. However, investing in capabilities for our Tier 1 business enhances resilience across all partner segments.

Additionally, F-Secure acknowledges the risk of cybersecurity attacks that may negatively impact our reputation and business, as well as security risks from suppliers and partners. We handle personally identifiable information securely, never sell it to third parties, and provide regular workforce training on PII handling as part of our Code of Conduct.

Types of consumers negatively impacted by F-Secure

F-Secure provides software-based products and services designed for all consumer types and age groups. Our cybersecurity software-based products are not inherently harmful to people and do not increase risks for chronic disease. We have not identified any material negative impact related to consumers and end-users, or any consumer subsegments.

No products or services exist that may potentially negatively impact consumer rights to privacy, personal data protection, freedom of expression, and non-discrimination. F-Secure's cybersecurity offering is built to protect consumers and their rights online, including privacy and identity protection capabilities. We collect information only for the purpose of providing the security service and do not sell any such information to third parties.

We have built our products to guide onboarding and usage to minimize the need for manuals, while offering support via community articles and support channels. Our software-based products are promoted and sold through F-Secure or reputable Service Providers and are not targeted at children or financially vulnerable individuals.

Types of consumers positively impacted by F-Secure

F-Secure's purpose is to protect consumers' digital moments, and for that purpose, we have created a design system to make products perceivable, operable, understandable, and robust for the widest possible audience. Our product design focuses on creating solutions that empower users and enhance their safety and confidence online.

We prioritize accessibility by designing simple, intuitive products that minimize cognitive load and follow guidelines for visual accessibility, including sufficient contrasts, appropriate text sizes, and awareness of seizure triggers. Compliance with accessibility practices allows creation of an inclusive product experience for individuals with disabilities and the elderly while serving the general population.

Additionally, we increase global cybersecurity awareness to combat cybercrime by educating consumers how to stay safe online. Our global campaigns target diverse regions and involve collaboration with educational institutions, government bodies, NGOs, and customers, emphasizing shared responsibility for cybersecurity. This aligns with our goals of mitigating cyber threats and promoting a secure digital environment through educational content and free tools for online safety.

Impact, risk and opportunity management

S4-1 Policies

Policy	Key Contents	Scope	Responsibility	Link to IROs
Personal Data Policy	Controls and principles for protecting customer privacy Privacy organization and roles Key privacy principles and processes Privacy training and monitoring Based on EU GDPR and relevant privacy regulations	All employees, leadership, employee-like contractors and suppliers	CEO and leadership team	Evolving threat landscape Cybersecurity Protecting digital moments
Cyber Security Policy	Objectives for strategic cybersecurity activities Governance practices and focus areas Information security, privacy, and software security management Based on ISO 27001 standard Protection of customer and employee data Maintaining availability of company services	All employees and leadership, employee-like contractors, and suppliers.	CEO (accountable), Chief Information Security Officer (implementation)	Protecting digital moments Security of vendors and partners
AI Policy	Encourages innovation with AI applications Adherence to high standards in privacy, cybersecurity, intellectual property rights, and business integrity Based on Code of Conduct values: Building Trust in Society, IP Rights and Confidentiality, Protecting Human Rights	All employees and employee-like contractors.	CEO	Use of AI in security applications AI increases risk of security breach

Table 46. Consumer and end-user policies.

While our Code of Conduct is applicable for Consumers and End-Users, serving customers and partners in a business ethical manner is described in the Business Conduct section and under the "Code of Conduct training target".

The following IROs do not have policies inked to them but are managed as part of F-Secure's business operations:

- Create awareness about cybercrimes
- Channel strategy
- Consumer willingness to pay

Externally reported targets have not been set for Create awareness about cybercrimes. However, F-Secure tracks the effectiveness of consumer cybersecurity awareness activities through quantitative engagement metrics including audience reach of partner campaigns, click-through rates on threat reports and guides, web session volumes for direct-to-consumer content, media article readership, and social media following.

Human rights commitments relevant to consumers

F-Secure has embedded commitment to international human rights in its Code of Conduct, considering globally recognized principles (refer to S1-1 for details).

F-Secure's internal policies, procedures and guidelines are aligned with the Code of Conduct and these international principles. Our commitment extends to end-users through products and services designed to respect human rights and ethical standards, including data privacy protections, secure processing of personal data, and transparent communication about user rights and responsibilities.

Engagement and Reporting Mechanisms: End-users can provide feedback and report concerns about F-Secure products through Customer Care or the whistleblowing channel. The whistleblowing channel allows anonymous reporting of Code of Conduct violations including human rights violations without fear of retaliation. All reports are investigated with prompt corrective actions implemented, including remedies for human rights impacts where appropriate.

Alignment with internationally recognized instruments (SFRD and Pillar)

F-Secure is certified to **ISO 27001:2022 Standard for Information Security Management** across all operations. The standard defines controls for managing information security covering people security, secure software development, security incident response, and business continuity. Sub-standards and reference controls include:

- ISO 27001 Annex A controls
- NIST CSF & 800-63B
- OWASP Top10, MASV & MASG
- ISO 3001:2018
- ISO 22301:2019

Compliance Record: No reported cases of non-respect of UN Guiding Principles on Business and Human Rights, ILO Declaration on Fundamental Principles and Rights at Work, or OECD Guidelines for Multinational Enterprises involving consumers and/or end-users.

Progress Monitoring: Processes for monitoring and measuring progress are described under the Metrics and Targets section where cybersecurity training completion rate, cybersecurity incidents, and ratio of externally reported product vulnerabilities to internally identified vulnerabilities are primary metrics.

S4-2 Processes for engaging about impacts

F-Secure deploys several methods of collecting and analyzing consumer perspectives. The majority of engagements are direct with dialog between F-Secure and consumers, including customer care contacts, app store feedback, and social media feedback. F-Secure requests formal feedback through a continuous product survey process. All data is analyzed, responded to (when channels allow), and reported to applicable F-Secure stakeholders for processing.

We receive feedback from channel partners regarding their end-users that is processed similarly. Engagement scope and frequency vary between partners through joint customer need surveys, generic feedback from partners' market and consumer surveys, or feedback from their customer care teams.

Stage and frequency of engagement

F-Secure closely follows customer lifecycle performance in Direct Business. The majority of consumer engagement happens after onboarding, once consumers have installed and activated protection services. Daily engagement occurs through the protection app working in the background, protecting device use and consumers' digital moments.

Consumer feedback is obtained continuously, enabling F-Secure to respond promptly to challenges through communication channels mentioned above. All consumer feedback is consolidated, analyzed, and processed monthly.

F-Secure's Chief Product Business Officer, part of the Leadership Team reporting directly to the CEO, has operational responsibility for engagement and integration of results into F-Secure's strategy, business model, and daily activities.

Assessing the effectiveness of our engagement

F-Secure follows multiple consumer-generated metrics, including the number of support cases, NPS (Net Promoter Score), CES (Customer Effort Score), and app store ratings to assess engagement effectiveness. These metrics enable close connection with consumer sentiment, even though most business originates via Service Provider partners. We measure and track app store ratings with partners in Apple App Store and Google Play. Significant changes in metrics or feedback are investigated with corrective actions taken regardless of channel.

Gaining insights into consumers, particularly vulnerable consumers

F-Secure emphasizes the ease of use of protection apps. We strive for demographic representation in testing processes to provide a multitude of cultural perspectives in feedback applied to product creation, avoiding exclusion of consumer groups.

We include compliance with the EU Accessibility Act to maintain wide product usability. No consumer group is excluded in design, with target to make protection easy to activate and use without advanced technical skills. By complying with the

European Accessibility Act and W3C accessibility recommendations, F-Secure strives for ease of use for users with various disabilities.

F-Secure uses its beta community to verify design decisions before product availability to larger audiences.

S4-3 Processes to remediate negative impacts and channels to raise concerns

Channels to raise concerns

End-users can reach F-Secure through self-help (community forum and chatbot) and assisted (chat and phone) channels. F-Secure Customer Care is active on social media and app store channels to assist customers. All customer contacts are evaluated with satisfaction measures through post-ticket surveys, including open feedback options. F-Secure provides support services in-house with dedicated resources.

- Phone support multiple languages: Available during business hours for immediate assistance. English for extended business hours.
- Chat support in multiple languages, including chatbot: Available during extended business hours. English 24/7.
- Email Support: Monitored email addresses integrated to create cases to CRM system. Dedicated address for GDPR requests.
- Feedback Forms: Integrated into customer contact cases for product/service feedback.
- Community and Social Media Channels: Official accounts on major platforms for engagement and issue resolution.

These channels are managed internally by the undertaking to ensure timely and consistent responses.

F-Secure has defined support models with channel partners where end-user support services are provided by F-Secure or partners. When channel partners are the first point of contact, we provide help desk training and maintain open support channels for partner assistance. F-Secure provides technical support for partners related to offerings per agreed Service Level Agreements.

Effectiveness and trustworthiness of our support channels

F-Secure logs all customer contacts (inquiries and support requests) within a ticketing system to identify trends, track performance metrics, and make data-driven decisions about customer experience and service improvement. This tracks ticket volume, resolution time, and customer satisfaction (post-ticket survey) per contact channel.

For common issues, we have monthly internal review and verification processes through the customer experience council with action points to remediate issues and follow up on progress. When relevant, we benchmark offered service and customer care metrics, especially post-incident customer satisfaction, with other cybersecurity industry companies and technology sector associations providing insight and research data.

Trustworthiness measures:

- Engage with end-users during the customer lifecycle through the protection app and lifecycle messages informing about available contact channels
- All contact channels are publicly available on the web for anyone to find and use
- Continuously follow the utilization of each channel to maintain effectiveness
- Consumers may provide feedback under the whistleblowing policy through a publicly available whistleblowing channel without fear of retaliation

Customer trust building: All customer care contacts and issue remediation are evaluated with satisfaction surveys after support case resolution, including open feedback options. F-Secure has a complaint process triggered by low post-ticket survey scores and customer requests for contact. This process engages customers to understand perceptions and handles complaints with actions to solve issues to satisfaction, plus internal actions to improve service and build trust. Post-complaint surveys measure complaint handling effectiveness.

S4-4 Actions and resources

Actions to Address Material Impacts

Protecting Digital Moments

Our cybersecurity products and services like F-Secure Total help consumers stay safe online and build trust in digitality. We continuously improve protection capabilities in our apps, SDKs and cloud to increase security efficacy and deliver real-time protection while regularly launching new product versions with new protection capabilities against scams.

During 2025, we continued to expand our scam protection capabilities and launched a dedicated Scam Protection offering in our Direct Business in May 2025. This activity continues during our strategy period (2026–2028) and is executed across our focus regions and channels. Expected outcomes include increasing the number of consumers we protect globally, consumer and partner satisfaction, while creating value for our channel partners and shareholders.

Creating Awareness About Cyber Crimes

Increasing consumer awareness on cybercrime is critical to help consumers stay safe when online. Our dual strategy raises awareness directly with service providers and consumers while equipping our 200+ channel partners to educate their customers. We achieve consumer awareness by making free tools for consumers available, especially in our Direct Business such as identity theft checker, messaging scam analysis, and online scanners. Additionally, we regularly create relevant new content to inform of blog posts, tips and guides, especially related to scams.

For service providers and partners, our annual Cyber Threats Guide drives partner awareness measured in terms of click-through-rates and time spent on the pages, while we measure the effectiveness of our direct-to-consumer articles through sessions and time spent on our web pages. Our PR secures expert placement in major outlets and uses LinkedIn to further increase awareness as measured through reach and/or followers.

With channel partners, our annual Cybersecurity Awareness Month Campaign provides partners with ready-to-use materials to educate their end-customers about cybercrime. Furthermore, we supplement this with year-round white-labelled content and monthly F-Alert bulletins offering timely threat insights. We track the effectiveness of these activities in 2025 through audience reach (consumers reached) and page visits. Expected outcomes of these actions include increased partner satisfaction and preventing consumers from becoming victims of cybercrime. We'll continue expanding these activities throughout 2026 directly and through our partners.

Actions to avoid causing or contributing to a material negative impact on consumers and end-users

F-Secure has not identified material negative impacts on consumers and end-users. Furthermore, F-Secure sees no negative impacts related to health or privacy from our portfolio, or arising from our or our partners' marketing and sales strategies toward potentially vulnerable individuals. Our software-based products, including protecting consumer privacy online, are promoted and sold either directly by F-Secure or through reputable Service Providers and are not targeted at children or financially vulnerable individuals.

To ensure we don't cause or contribute to material negative impacts towards consumers, we've during 2025 reviewed the effectiveness and trustworthiness of our support channels as described in chapter "S4-3 Processes to remediate negative impacts and channels to raise concerns" in addition to tracking any reports received via our whistleblowing channel. Additionally, our product Net Promoter Score surveys conducted during 2025 serve as a further sensor to gauge, if our product would start to have material negative impact(s).

We expect to continue to assess our support channel effectiveness and trustworthiness as well as conduct product surveys during the strategy period (2026-2028). These activities did not require any material operating expenditures (Opex) and/or capital expenditures 2025, and we expect it to remain the same for the strategy period.

Actions to pursue material opportunities

Actions related to our material opportunities were executed during 2025. We continue to see them as relevant also for the current strategy period (2026-2028):

Opportunity	Actions 2025	Effectiveness Measures and expected outcomes
Evolving Threat Landscape	Re-direct resourcing and investments into research, innovation, and product creation capabilities around scam protection Support channel partners by upgrading them to latest F-Secure product versions with scam protection capabilities Support launching, promoting, and selling security directly to consumers, and via existing and new partners	Number of new scam protection capabilities launched during the year as part of Embedded or Security Suite portfolios. Outcomes directly connected to consumer satisfaction and F-Secure's revenue growth in key regions and channels
Use of AI in Security Applications	More engaging, relevant, and contextual protection experience (user experience) Improved security efficacy where AI technologies advance F-Secure's threat research capabilities and allow providing more effective protection capabilities	Enhances our consumer and channel partner offerings leading to a differentiated market position in our key regions and channels, further driving growth. Improves product NPS.

Table 47. Actions in pursuit of opportunities related to consumers and end-users.

Actions to mitigate material risks

Our most material impact is protecting consumers' digital moments through holistic, engaging cybersecurity products and services directly and through partners. This carries five inherent risks with corresponding mitigation strategies as listed in the table below. These mitigation activities were executed in 2025 in our focus geographies and channels, and we see them being relevant during the strategy period (2026-2028):

Risk	Actions 2025	Effectiveness Measures and expected outcomes
Consumer willingness to pay decline	Continuously add new relevant scam protection capabilities that increase value to consumers. Service Provider partners combine security with their own services or apps for increased value or offer as a new core/ value-added service.	Partner and product NPS tracking, service provisioning, activation and usage rates leading to subscriber base growth and ARPU increase.
Channel strategy risks	Help partners drive their topline growth, lower churn. Deliver value based on a compelling vision and roadmap to meet partners' business needs. Develop healthy sales pipeline.	Partner commitment to sales/ marketing activities, adoption of new versions of our products, NPS evolution and overall funnel development leading to revenue and ARPU increase. Service provisioning and activation tracked similar to previous risk.
Security of suppliers and partners	Security review gateways in procurement process, contractual security requirements enforcement, regular security audits of critical vendors.	% share applied globally to all suppliers and partners. Expected outcome is 100% coverage for critical suppliers.
Cyber security attacks	ISO 27001 standard implementation, proactive security monitoring, vulnerability management, regular crisis rehearsals, continuous policy monitoring and improvement	Number and criticality of security incidents and vulnerabilities in software and third-party solutions. Expected outcome is 0 critical security incidents.
AI increase risk of security breach	Security review of new AI tools, limiting AI access to sensitive information, information processing instructions and security awareness	Number and criticality of security incidents involving AI tools

Table 48. Actions to mitigate risks related to consumers and end-users.

Human rights issues connected to consumers

F-Secure has zero (0) human rights issues or incidents connected to consumers during 2025.

Resources allocated to the management of the material impacts

- **Product Management and Technology:** F-Secure's product management function is responsible for creating product vision, offering, and related product roadmaps to meet partners' and consumer customers' needs in the short and long term. Product management steers our Product Board, which prioritizes product initiatives and roadmaps for technology organization resource allocation for implementation projects (product releases). New product experimentations or initiatives may also be implemented within the Product organization. The Technology organization is also responsible for threat intelligence and research activities, providing effective protection against modern threats.

- **Marketing and Content Creation:** Marketing teams drive a content creation strategy aligned with direct business and partner channel needs and opportunities, supported by technology organization threat intelligence teams providing expert views on latest scams. Implementation of free tools is governed through the Product Board process.

Metrics and targets

S4-5 Targets

F-Secure describes its sustainability-related baseline measures and long-term targets in the table below. 2023 is established as the baseline year in all targets except ratio of reported vulnerabilities and completion rate of security awareness where the baseline year is 2024. Progress will be reported annually.

Methodologies

All NPS results are measured through a dedicated marketing survey solution. Cybersecurity training metrics are tracked through F-Secure's Learning Management System. Major cybersecurity incidents and bug bounty-related issues are tracked with a dedicated ticketing system. All systems are used globally with no need for regional data collection.

The metrics have been selected based on alignment with material F-Secure ESG topics, Double Materiality Assessment, industry benchmarking and our own insights, and stakeholder feedback. The targets have been developed in collaboration with relevant functions and reviewed and approved by the Board of Directors as described above, while no external stakeholders are directly involved in target setting. We track the effectiveness of our actions and policies toward the impacts, risks and opportunities by monitoring the targets we set below.

S4-5 Targets Consumers

Target	Baseline 2023	2024	2025	2030 target
F-Secure consumer product NPS (Total)	49	49	52	55
Partner Business NPS	56	63	55	Above 55
Completion rate of internal cyber security training	Baseline is 2024	95%[1)]	94%	98% (all employees)
Number of major cyber security incidents	2 (no customer data was compromised)	1 (no customer data was compromised)	0	0 incidents involving leaked customer personal data

1) Target updated for 2024 (97%) including all employees.

Table 49. Consumer and end-user targets.

S4-5 Progress towards targets

F-Secure consumer product NPS evolution (Total)

The target on Consumer Product NPS evolution is related to IROs around measuring our effectiveness in delivering easy-to-use, engaging and effective protection, leveraging opportunities in the evolving threat landscape, and mitigating risks around consumer willingness to pay.

Net Promoter Score (NPS) measures customer loyalty and satisfaction by asking customers how likely they are to recommend a company's product or service to others on a scale from 0 to 10. The score is calculated by subtracting the percentage of detractors (those who score 0–6) from the percentage of promoters (those who score 9–10), resulting in a score ranging from -100 to +100.

At F-Secure, NPS tracks progress in fulfilling our vision to become the number 1 security experience company and mission to continuously deliver brilliantly simple, frictionless security experiences. NPS reflects product quality, customer journey, sense of security, and trust-related sentiments of consumer customers.

An NPS target has been set for our main consumer product F-Secure Total, measured in our Direct Business channel. The F-Secure Total NPS target for 2027 is 50 and 55 for 2030. The 2025 outcome for product NPS is 52. We review progress monthly and report the NPS outcome annually as part of the sustainability report.

The stakeholders who participate in target setting are F-Secure executives relevant for product NPS, namely the Chief Product Business Officer, respective product manager(s), the CEO and the Chief People Officer. The target is set annually with final measurement conducted at year-end.

Partner Business NPS evolution

The Partner Business NPS evolution target is related to IROs around measuring our effectiveness in supporting channel partners growing their cyber security business and mitigating risks around losing a material Service Provider partner or not being able to support our Tier 1 partners.

We apply NPS to measure partner business satisfaction, which is critical for F-Secure as a vast majority of our revenue originates from partners. We invite Service Providers across industries and geographies to respond to the satisfaction survey and report the outcome annually.

F-Secure's global NPS survey outcome in 2025 was 55. We expect our NPS score to remain above 55 in the medium and long term.

F-Secure's Chief Revenue Officer is accountable for target setting in alignment with the sales strategy. The target is set annually and measured once a year. Regional sales leads and account managers review survey results to identify issues and corrective actions in partner engagement.

The stakeholders who participate in target setting are F-Secure executives relevant for product NPS, namely the Chief Product Business Officer, respective product manager(s), the CEO and the Chief People Officer. The target is set annually with final measurement conducted at year-end.

Completion rate of internal cybersecurity training

The completion rate target of F-Secure cybersecurity training measures F-Secure employees' awareness of internal security policies. This target is based on objectives defined in F-Secure Cybersecurity Policy and Personal Data Policy, measuring employee knowledge against the company's general cybersecurity objectives, security policies and guidelines.

The target is calculated based on the current employee count, and presented as a completion percentage (%). All F-Secure employees are part of the target with no geographical boundaries.

We have set a 2030 target of reaching a training completion rate of over 98%. For 2025, the training completion outcome was 94%. We review progress regularly and report the outcome annually.

The stakeholders who participate in target setting are F-Secure executives relevant to cybersecurity, including the CEO, CFO, CTO, CDO, General Counsel, and CISO. The target is set annually with final measurement conducted at year-end.

Training data is extracted from F-Secure's learning management system, and information related to long-term absences comes from our HR systems.

Number of major cybersecurity incidents

The number of major cybersecurity incidents target is based on objectives related to information security and privacy defined in F-Secure Cybersecurity Policy. It measures company security processes and their capability to prevent

major incidents from occurring, and the impact of cybersecurity incidents on F-Secure customers.

The occurrence of major cybersecurity incidents is tracked as part of F-Secure security incident management and crisis management processes. A major incident is defined as an incident impacting critical systems, security of significant amount of our employees or data classified as restricted or confidential, as well as all incidents where customer data is externally exposed.

All incidents are tracked in F-Secure's incident management system from where the data is extracted and regularly monitored. In 2023, F-Secure had two major incidents but neither of them impacted customer data. For 2024, our outcome was 1, while the target is to have no major incidents impacting customer data in 2030. In 2025 our outcome was 0.

The target measurement is not completely absolute since it is dependent on human assessment of the incident. This shortcoming is mitigated by having multiple security team members review all incidents.

The stakeholders who participate in target setting are F-Secure executives relevant for cybersecurity, including the CEO, CFO, CTO, CDO, General Counsel, and CISO. The target is continuously measured annually with final measurement conducted at year-end.

Metrics tracked internally

Ratio of externally reported product vulnerabilities to internally identified vulnerabilities

F-Secure also tracks the effectiveness of cybersecurity-related policies and actions with alternative processes through monitoring bug bounty reports and internally identified vulnerabilities. This bug bounty-related metric is based on objectives related to software security defined in F-Secure's Cybersecurity Policy. It measures F-Secure's engagement with the cybersecurity researchers' community and the efficiency of the company's secure software development processes.

The number of bug bounty reports, their criticality, and the bounty amount paid to researchers are tracked as part of F-Secure's bug bounty program. All reported cases are tracked in F-Secure's ticketing system from where the reports are assessed by the relevant development team and for potential paid bounty.

The target tracks ratio of externally reported product vulnerabilities where bounty has been paid to internally identified vulnerabilities. This includes comparing externally reported medium, high and critical vulnerabilities to what has been found by F-Secure internally. 2024 is the baseline year.

The target measurement is not completely absolute as it depends on human assessment of the reported finding. This shortcoming is mitigated by having multiple developers review the reports and criticality and the suggested bounty compared to earlier paid bounties.

GROUP SUSTAINABILITY REPORT -

Governance

G1 – Business conduct

SBM-3 Material impacts, risks and opportunitites

	Material impact, risk or opportunity	Description
Business Conduct		
Corruption or bribery		
Risk (DVC)	Partnership business, use of agents and other intermediaries	Partner business model may increase risks of bribery and corruption in cases where middle-men are used
Risk (DVC/UVC ,OO)	M&A transactions	Anti-Bribery and Corruption risks increase as a result of M&A transactions due to limited understanding of the target
Corporate culture		
Actual Positive impact (OO)	Culture reinforcement	F-Secure is strengthening its culture by reviewing people and culture structures to reflect the desired culture, supporting leadership and team development, and fostering a culture of experimentation
Protection of whistleblowers		
Actual Positive impact (OO/DVC)	Whistleblower channel available	Protection of whistleblowers encourages and enables all stakeholders to speak up. F-Secure has a whistleblower channel available for all Fellows and business partners.

Table 50. Business conduct-related list of IROs.

Impact, risk and opportunity management

G1-1 Company culture

F-Secure is committed to fostering its corporate culture systematically and sustainably. To us, culture means the ways we think and act to pursue our vision and goals as an F-Secure team, including the ways we act on our Code of Conduct. Our desired culture includes values, aspired behaviors, and leadership principles. Our culture is called “Fellowship” and it includes four values: 1) Keep focus, 2) I make a difference, 3) Just do it, and 4) Dare to care.

To foster our corporate culture, we have implemented the following key actions:

- We have implemented a Leadership Academy with learning programs for current and aspiring leaders. Through the Leadership Academy, our goal is to strengthen our ‘ready-now’ leadership succession pipeline to 65% by the end of 2026. The program targets current Team Leaders and high-potential employees identified through talent calibration processes. Launched in 2023, the Leadership Academy has ongoing annual programs continuing through 2025 and beyond. The programs are funded through annual operational budgets.
- We have established a strategic forum for leaders called Leadership Lab. The expected outcome is to foster strategic alignment and execution, measured by F-Secure Objectives and Key Results achievement, enable collaborative decision-making, and create a shared understanding of organizational priorities among leadership. All F-Secure Team Leaders are invited to the sessions (approximately 90 leaders). The forum was established in a different format already in 2022 and is organized quarterly in 2025, continuing as a permanent leadership practice.
- We have strengthened active and transparent internal communications through clarifying our key internal communication channels, and strengthening the opportunities of employees to actively participate and provide feedback in monthly townhalls. We aim to increase employee understanding of strategic direction and priorities and enhance two-way dialogue. The scope includes all Fellows across F-Secure's global locations. These actions have been enhanced starting in 2024, with continuous improvement and regular communication touchpoints.
- We have supported team performance dynamics building. We expect Talent Density (i.e., the proportion of high-performers in the organization) to grow to 50% by the end of 2025 and the results will be available in March 2026. We have been focusing on teams where we have identified needs for enhancing trust and psychological safety, impact and meaning, clarity and structure, and/or accountability and dependability. We measure this in our Fellow survey with a high-performing team index covering the above-mentioned four dimensions of high-performing teams. Thus far, we’ve focused on the most crucial 10% of our teams that are identified through our Fellow survey as having gaps in high-performing team components mentioned above. This is an ongoing effort started in 2025 and continuing going forward.
- We have renewed our leadership annual clock in 2025. We aim to systematically lead performance, learning and development, as well as recognition and rewards. The annual process cycle enables linkages between these core processes in a way that performance and learning boost the growth of employees, and where high performance is recognized and rewarded. The annual leadership processes concern all Fellows and are a continued effort going forward.
- We have also continued reviewing employee lifecycle processes aligned with our culture to ensure value-aligned experiences throughout the employee journey from pre-boarding and onboarding through performance management, learning and development, and exit. Through the above-mentioned actions, voluntary attrition remained under 12%. The scope includes all Fellows across the organization. The renewal of the processes was initiated in 2024, with implementation aimed to be completed in 2026. Yet, we will continuously improve these structures and processes going forward.
- We track cultural development through regular Fellow surveys. Through the survey, we monitor cultural health, measure engagement levels, identify improvement areas, and inform action planning to address any concerns while maintaining high engagement. The main outcome is employee engagement measured by eNPS, where we aim for 50 by the end of 2030. The scope includes all Fellows biannually. The survey is a continuous action with regular survey cycles.

G1-1 Policies

Policy	Key Contents	Scope	Responsibility	Link to IROs
Code of Conduct	Outlines F-Secure's ethical principles, values, and expected behaviors. Includes anti-corruption standards and reporting procedures. Further information regarding which third-party standards and initiatives F-Secure commits to respecting through the Code of Conduct is disclosed under S1-1.	All employees and leadership. Suppliers and channel partners expected to adhere to principles.	Owned by the General Counsel, approved by the Board of Directors	Partnership business, use of agents and other intermediaries M&A transactions Whistleblower channel available Culture reinforcement
Anti-Bribery and Corruption Policy	Covers prohibited conduct, gifts, conflicts of interest, third-party due diligence, compliance requirements, and enforcement procedures. Based on the UN Convention Against Corruption.	All employees and leadership. External officers.	Owned by the General Counsel, approved by the Board of Directors	Partnership business, use of agents and other intermediaries M&A transactions
Whistleblowing Policy	Defines reporting channels, investigation procedures, and protections for whistleblowers, including confidentiality and anti-retaliation measures.	All employees and external stakeholders.	Owned by the General Counsel, approved by the Board of Directors	Whistleblower channel available

Table 51. Business conduct policies.

These policies and relevant complementary procedures and guidelines are available to employees on the F-Secure intranet and SharePoint, which are accessible to all employees. Any updates to the policies are communicated via the news section on the intranet, the monthly newsletter, and Townhall meetings. The mandatory Code of Conduct training also outlines the key elements of these policies to help employees understand their implications. The Code of Conduct and Whistleblowing Policy are also available to the public on the F-Secure website. These policies are owned by the General Counsel and approved by the Board of Directors, and other stakeholders have not been directly involved in setting these policies.

External officer in this context refers to any agent or any other party representing or acting on behalf of F-Secure who is not in an employment relationship with F-Secure.

Mechanisms for identifying concerns about unlawful behavior or code of conduct violation

F-Secure employees have multiple channels to report Code of Conduct violations: direct communication with managers, Legal, or HR; our anonymous whistleblowing channel; or writing to our CEO or Board. External stakeholders can use our public whistleblowing channel.

All reports are handled confidentially with appropriate measures taken against violations. F-Secure provides measures to protect against retaliation against its own employees who are whistleblowers in accordance with Directive (EU)2019/1937, including:

- identity protection;
- protection from retaliation and possible reversal of the burden of proof in the handling of a claim related to retaliation in the courts and other authorities;
- possible compensation and remedies, e.g., due to retaliation; and
- possible protection against civil, criminal, and administrative liability.

In addition to protection provided to the whistleblower, F-Secure also provides protection to person(s) who are suspected of having committed the breach. Such protection includes, for instance, that the person is treated in an equal and non-discriminating manner and the consequences of the breach are based on F-Secure's policies and applicable laws.

Procedures to investigate business conduct incidents

In accordance with the F-Secure Anti-Bribery and Corruption Policy, we monitor anti-corruption effectiveness through regular audits and reviews. F-Secure has procedures to investigate business conduct incidents promptly, independently, and objectively. All employees must accurately record financial transactions with proper documentation.

Policy for business conduct training

Our Code of Conduct training is mandatory for all employees, including specific modules on anti-corruption and reporting procedures. New employees complete this during onboarding, with refresher training required every two years. This training covers 100% of high-risk functions, particularly sales and procurement teams, which we've identified as most susceptible to corruption and bribery risks. The Code of Conduct training also includes information to employees about the whistleblowing channel and other mechanisms for reporting Code of Conduct violations.

G1-3 Procedures to address corruption and bribery

F-Secure encourages a culture of openness and accountability. Employees who suspect policy violations can report through multiple channels: speaking to managers, Legal, or HR; using our whistleblowing channel; or writing to the CEO or Board. We guarantee a confidential review of all reports and protect whistleblowers from retaliation.

We require an accurate recording of all financial transactions involving F-Secure expenses or asset transfers. Our expense management systems maintain proper documentation and transparency. The effectiveness of our anti-corruption efforts is monitored through regular audits and reviews that identify and address risk areas or compliance issues.

No action plans require significant capital expenditure (CapEx) or operating expenditure (OpEx), and all actions are funded through normal business operations.

Investigating and reporting incidents

When investigating suspected incidents, we ensure investigators are separate from the management chain involved in the matter. Investigation teams are determined on a case-by-case basis to ensure impartiality. Substantiated investigations involving corruption or bribery are reported to the Audit Committee, with outcomes communicated to relevant management bodies and to authorities when legally required.

Nature and scope of the training programs

F-Secure's anti-corruption training is mandatory for all employees, with particular focus on high-risk functions. The training includes realistic scenarios that test employees' ability to apply Code of Conduct principles to decision-making situations and covers appropriate reporting mechanisms. This comprehensive training ensures 100% coverage of functions at risk, particularly those in sales and procurement, as well as our executive management, including the Leadership Team.

Metrics and targets

G1-4 Targets

G1-4 Targets Business Conduct

F-Secure has established two targets related to business conduct:

Target	Baseline 2023	2024	2025	2030 target
Zero-tolerance on bribery & corruption	0 incidents	0 incidents	0 incidents	0 incidents
Code of conduct training target	*Baseline is 2024*	96%	96%	98% (Permanent and fixed-term employees)

Table 52. Business conduct targets.

G1-4 Progress towards targets

F-Secure reports zero convictions and zero fines for violations of anti-corruption and anti-bribery laws during 2025. As there have been no known breaches in anti-corruption procedures or standards, we have not needed to take remedial actions.

Zero-tolerance on bribery & corruption

Our zero-tolerance target is based on our Code of Conduct principles and Anti-Bribery and Corruption Policy. Both the Code of Conduct and the F-Secure Anti-Bribery and Corruption Policy, which create the basis for this target, have been approved by F-Secure's Board of Directors. The target applies to all F-Secure operations globally and aims to maintain zero incidents of bribery or corruption. The performance against this target is monitored by reviewing the number of corruption and/or bribery-related incidents reported through the whistleblowing channel or to line managers, the CEO, the HR team, the Legal team, or the Board of Directors. The target is absolute, and it is measured in the number of incidents related to bribery or corruption. With zero incidents since our 2023 baseline, we are on track to maintain this performance through 2030.

With this target and the accompanying policy, F-Secure is committed to complying with all laws and regulations that apply to our business activities around the world, including but not limited to the Foreign Corrupt Practices Act (FCPA) and the UK Bribery Act 2010.

Code of Conduct training target

This target aims to ensure that F-Secure employees recognize situations where the Code of Conduct is relevant and know how to make decisions in alignment with the Code in their daily work, as well as how to report any concerns or misconduct to foster ethics, transparency, and accountability. The training includes anti-corruption components and proper reporting procedures. With 2024 as our baseline year, we've achieved 96% completion, working toward our 2030 target of 98%. The General Counsel, together with the Leadership Team, has set this target. This target acknowledges practical limitations like recent hires and employees on extended leave. We monitor performance through our Learning Academy platform and implement targeted follow-up for non-completions. The reported Code of Conduct training target includes permanent and fixed-term employees and excludes individuals for whom employee status information is unavailable.

G1-4 Incidents of corruption or bribery

G1-4 Confirmed incidents

	2024	2025
Number of convictions and amount of fines for violations of anti-corruption and anti-bribery laws	0	0

Table 53. Incidents of corruption or bribery.

Consolidated financial statements

Statement of comprehensive income

EUR 1,000	Note	2025	2024
Revenue	(3)	145,739	146,258
Cost of revenue		-22,348	-20,243
Gross Margin		**123,391**	**126,015**
Other operating income	(4)	771	751
Sales and marketing	(5,6,7)	-33,738	-34,591
Research and development	(5,6,7)	-30,934	-29,275
Administration[1]	(5,6,7)	-23,953	-24,478
EBIT		**35,538**	**38,422**
Financial income	(9)	1,295	1,714
Financial expenses	(9)	-9,285	-13,124
Profit before taxes		**27,548**	**27,011**
Income tax	(10)	-5,178	-5,944
Result for the financial year		**22,370**	**21,067**
Other comprehensive income			
Exchange difference on translation of foreign operations		-7,468	4,047
Comprehensive income for the year		**14,902**	**25,114**
Result of the financial year is attributable to:			
Equity holders of the parent		22,370	21,067
Comprehensive income for the year is attributable to:			
Equity holders of the parent		14,902	25,114
Earnings per share, eur (basic and diluted)[2]	(11)	0.13	0.12

1) Costs related to restructuring decrease administration expense by EUR 0.1 million in 2025 (EUR 1.4 million).

2) Earnings per share is based on the average number of shares.

Statement of financial position

EUR 1,000	Note	2025	2024
ASSETS			
Non-Current Assets			
Tangible assets	(14)	967	326
Right-of-use assets	(5,14)	4,825	1,200
Intangible assets	(14)	119,443	125,736
Goodwill	(13,14)	87,029	89,783
Deferred tax assets	(22)	187	58
Other non-current receivables	(17)	590	223
Total non-current assets		**213,040**	**217,327**
Current Assets			
Inventories	(15)	20	29
Accrued income	(17)	2,435	3,333
Trade and other receivables	(16,17,21)	33,980	37,049
Interest-bearing receivables, current	(16,21)	-	3,757
Income tax receivables	(17)	861	968
Cash and cash equivalents	(16,21)	10,771	8,095
Total current assets		**48,067**	**53,231**
TOTAL ASSETS		**261,106**	**270,558**

EUR 1,000	Note	2025	2024
EQUITY AND LIABILITIES			
Shareholder's Equity	(18)		
Share capital		80	80
Translation differences		-5,491	1,977
Unrestricted equity reserve		9,590	9,590
Retained earnings		51,837	35,371
Equity attributable to equity holders of the parent		**56,017**	**47,018**
Non-Current Liabilities			
Interest bearing liabilities, non-current	(5,20,21)	124,691	131,431
Deferred tax liabilities	(22)	5,873	3,584
Other non-current liabilities	(23)	5,953	6,443
Total non-current liabilities		**136,517**	**141,459**
Current Liabilties			
Interest bearing liabilities, current	(5,20,21)	31,710	44,046
Trade and other payables	(21,23)	14,720	14,142
Provisions	(23)	640	1,427
Income tax liabilities	(23)	435	387
Other current liabilities	(23)	21,068	22,079
Total current liabilities		**68,573**	**82,081**
TOTAL EQUITY AND LIABILITIES		**261,106**	**270,558**

Statement of cash flows

EUR 1,000	Note	2025	2024
Cash flow from operations			
Result for the financial year		22,370	21,067
Adjustments			
Depreciation and amortization	(6)	16,443	13,621
Provisions	(23)	-787	-312
Share-based payments	(19)	1,140	1,045
Other adjustments		-230	177
Financial income and expenses	(9)	7,950	11,324
Income taxes	(10)	5,178	5,944
Cash flow from operations before change in working capital		**52,064**	**52,866**
Change in net working capital			
Current receivables, increase (-), decrease (+)	(16)	3,078	-2,812
Inventories, increase (-), decrease (+)	(15)	10	6
Non-interest bearing debt, increase (+), decrease (-)	(23)	-1,145	3,812
Cash flow from operations before financial items and taxes		**54,007**	**53,872**
Interest expenses paid	(9)	-6,846	-11,283
Interest income received	(9)	403	838
Other financial income and expenses	(9)	-1,132	-945
Income taxes paid	(10)	-2,862	-3,664
Cash flow from operations		**43,569**	**38,817**

EUR 1,000	Note	2025	2024
Cash flow from investments			
Investments in intangible and tangible assets	(14)	-12,772	-11,109
Profit/loss from sale of intangible and tangible assets		-3	1
Acquisition of subsidiaries, net of cash acquired	(12)	-	-132
Cash flow from investments		**-12,775**	**-11,240**
Cash flow from financing activities			
Increase in interest bearing liabilities, non-current	(20)	35,000	-
Repayments of lease liabilities	(5)	-1,227	-1,174
Repayments of interest-bearing liabilities, non-current	(20)	-50,334	-30,000
Change of short-term interest-bearing liabilities	(20)	-8,000	8,000
Decrease in loan receivables		3,757	-
Dividends paid		-6,987	-12,227
Cash flow from financing activities		**-27,790**	**-35,401**
Change in cash		3,003	-7,824
Cash and bank at the beginning of the period	(21)	8,095	15,867
Effects of exchange rate changes		-327	52
Cash and bank at period end		**10,771**	**8,095**

Statement of changes in equity

Attributable to the owners of F-Secure

EUR 1,000	Note	Share capital	Unrestricted equity reserve	Retained earnings	Translation differences	Total
Equity 31 December 2023		**80**	**9,590**	**25,485**	**-2,070**	**33,086**
Result of the financial year		-	-	21,067	-	21,067
Translation difference		-	-	-	4,047	4,047
Total comprehensive income for the year		-	-	**21,067**	**4,047**	**25,114**
Transactions with owners in their capacity as owners						
Cost of share-based payments	(19)	-	-	1,045	-	1,045
Dividend		-	-	-12,227	-	-12,227
Equity 31 December 2024		**80**	**9,590**	**35,371**	**1,977**	**47,018**
Result of the financial year		-	-	22,370	-	22,370
Translation difference		-	-	-	-7,468	-7,468
Total comprehensive income for the year		-	-	**22,370**	**-7,468**	**14,902**
Transactions with owners in their capacity as owners						
Cost of share-based payments	(19)	-	-	1,083	-	1,083
Dividend		-	-	-6,987	-	-6,987
Equity 31 December 2025		**80**	**9,590**	**51,837**	**-5,491**	**56,017**

1. Basis of preparation and accounting principles

1.1 Basis of preparation

Background

F-Secure is a Finnish, globally operating cybersecurity company. The parent company of the Group is F-Secure Corporation incorporated in Finland and domiciled in Helsinki, Finland. The company's registered address is Tammasaarenkatu 7, 00180 Helsinki. F-Secure operates globally with presence in multiple locations, and its headquarters is located in Helsinki.

F-Secure Corporation formed a separate legal group ("F-Secure", the "Group") as of 30 June 2022 when all assets and liabilities of the Consumer Security Business were transferred from WithSecure Corporation ("WithSecure") to a company incorporated in connection with the partial demerger ("Demerger") and named F-Secure Corporation ("F-Secure"). The trading in F-Secure's shares on Nasdaq Helsinki began 1 July 2022.

A copy of consolidated financial statements can be downloaded on www.f-secure.com or can be received from the parent company's registered address. These financial statements were authorized for issue by the Board of Directors on 25 February 2026.

F-Secure business

F-Secure designs and offers security and privacy products and services that help millions of consumers to protect themselves against online threats. F-Secure's offering includes a comprehensive range of security and privacy products and services related to endpoint security, privacy protection, password management and digital identity protection, and router security that protects consumers' entire connected home. The majority of F-Secure's sales come from selling products and services through its extensive and global Channel Partner network, including approximately 200 Channel Partners. Channel Partners include, for example, communication service providers, retailers, banks, and insurance companies. In addition to selling products through Channel Partners, F-Secure makes standalone and all-in-one security offerings available to consumers through various e-commerce channels such as mobile application stores and its own online store.

Basis of preparation for the consolidated financial statements

The consolidated financial statements for the year ended 31 December 2025 have been prepared for the purpose of presenting the financial position, results of operations and cash flows of F-Secure on a consolidated basis. The consolidated financial statements of F-Secure Corporation of 2025 have been prepared in accordance with IFRS Accounting Standards, applying the IAS and IFRS accounting standards as well as SIC and IFRIC interpretations that were in force and had been approved by the EU by 31 December 2025. In addition, accounting and limited liability company legislation and official regulations of Finland have been considered in the preparation of the consolidated financial statements.

F-Secure also publishes its financial statements in XHTML format in accordance with the European Single Electronic Format (ESEF) reporting requirements. In line with the ESEF requirements, the primary financial statements have been labelled with XBRL tags. Notes to financial statements have been labelled with XBRL block tags.

The consolidated financial statements have been prepared on a going concern basis and management has not recognized any material uncertainties related to continuity of operations.

The financial information is presented in thousands of euros unless otherwise stated. All figures have been rounded which may cause the sum of individual figures to deviate from the sum of the presented line-item totals.

Global economy and geopolitical conflicts

Global economic instability, geopolitical tensions, and shifts in trade policies expose F-Secure to risks and uncertainties in its operating environment. Geopolitical instability has increased uncertainty and the risk of unexpected economic disruptions. For example, the war in Ukraine has caused some exceptional consequences to the cybersecurity landscape. These factors could adversely impact on the company's operations, financial performance, and financial position.

Operations outside the eurozone expose F-Secure to currency fluctuation risks. Exchange rate changes could adversely affect F-Secure's financial position, key figures, and covenants. F-Secure may also be indirectly affected by escalating trade tariffs that could increase inflation, reduce purchasing power, or negatively affect consumers and channel partners.

Despite mitigating factors, if these risks materialize, they may disrupt F-Secure's operations, employees, markets, suppliers, and customers. Such disruptions could materially impact demand. Prolonged reduced demand or adverse business performance could negatively affect the valuation of non-current assets, including deferred tax assets and goodwill.

1.2 Accounting principles

Accounting principles applied in F-Secure's financial statements.

Management judgment on significant accounting principles and use of estimates

The preparation of consolidated financial statements requires use of estimates and assumptions as well as use of judgment when applying accounting principles. These affect the contents of the financial statements, and it is possible that actual results may differ from estimates.

Estimates made in connection with preparation of financial statements are based on management's best knowledge at the reporting date. Estimates build upon past experience as well as assumptions of future development of economic environment of the Group. Revisions in estimates and assumptions are recognized in the period they occur and in future periods if the revision affects both current and future periods.

The following areas require significant judgement and estimation:

- Impairment testing: Recoverable amount of goodwill from acquisitions is based on present value of estimated future cash flows which are subject to management judgment. In addition to goodwill the intangible assets that are not yet ready for use are tested annually for impairment. The recoverable amount of these assets is based on estimated future cash flows from sales and/or use of the asset.
- Expected credit losses: Management applies expected credit loss model to assess accounts receivable. Credit losses are estimated based on aging category as well as individual assessment. The allowance for expected credit losses in F-Secure's statement of financial position is EUR 412 thousand as at 31 December 2025 (See Note 16 Financial assets).
- Deferred tax assets from tax losses: The Group has recognized a total of EUR 141 thousand deferred tax assets related to tax losses carried forward in Spain and Slovakia at 31 December 2025 (See Note 22 Deferred tax). Recognition of the deferred tax assets is based on the Group's assessment that sufficient future taxable profits will be available against which the tax losses can be utilized.
- Share-based payments: The Group's share-based incentives programs are mainly tied to market-based conditions. Management uses external valuations in determining the fair value of the shares granted under these incentive programs. The method for the valuation is either Monte Carlo Simulation or Cox, Ross & Rubenstein method.
- Provisions: The amount of provision is the best estimate of the cost required to settle the obligation at the reporting date. Provisions are reviewed on a regular basis and adjusted when necessary.

Consolidation principles

The consolidated financial statements incorporate the financial statements of F-Secure Corporation and entities controlled by F-Secure Corporation. Consolidation is done using the acquisition method and begins when control over the subsidiary is obtained. The consolidation stops when the control ceases. The Group does not have any associated companies nor is there any non-controlling interest in the Group.

All intra-group transactions and balances, including unrealized profits arising from intra-group transactions, have been eliminated on consolidation. Where necessary, accounting policies of the subsidiaries have been adjusted to ensure consistency with the policies adopted by the Group.

Transactions in foreign currency

The financial statements are presented in euros, which is the functional and presentation currency of F-Secure's parent company. At each reporting date for the purpose of presenting financial statements, the income statements of foreign Group companies are translated at the average exchange rates for the reporting period and the balance sheets are translated using the European Central Bank's exchange rates prevailing on the reporting date. Foreign currency transactions are translated using the exchange rates prevailing at the dates of the transactions. Exchange rate gains and losses are recognized in financial items in the statement of comprehensive income.

Revenue recognition

F-Secure provides a comprehensive range of cybersecurity products and services related to endpoint protection, privacy protection, digital identity protection and security for all consumers' connected devices at home. Revenue derives from the sale of security products and services through partner and direct (ecommerce) channels. Majority of revenue comes from the sale of cybersecurity products through the partner channel. F-Secure also sells consumer products through various retail partners, as well as F-Secure's own web shop.

Partner channel sells Security Suite and Embedded Security products whereas direct channel sells Security Suite products.

F-Secure's cybersecurity products are sold as Security-as-a-Service. Customers are granted access to use the intellectual property during the license period and they are provided with access to continuously updated software. All software and the accompanied services F-Secure provides are highly interdependent and therefore treated as one performance obligation for which revenue is recognized over time on a straight-line basis for license period despite the sales channel.

Partner channel customers can have different invoicing depending on the customer agreement. Majority of the agreements are licenses fees – either Security Suite or Embedded Security – which are provided as a continuous service, when they are invoiced and revenue is recognized each month. Some agreements are for a fixed term. These agreements are invoiced upfront (e.g., annually), and the revenue is recognized over the contract period. Non-recurring revenue, which e.g. relates to custom built integration, is usually invoiced in the beginning of the agreement period and revenue is recognized over time on a straight-line basis for the contract period.

Direct channel selling Security Suite products is usually invoiced fully upfront for the license period and the revenue is recognized over time on a straight-line basis for the license period. The typical length of a license period is 12, 24, or 36 months.

Generally, the term between invoicing and when payment is due is not significant.

Pensions

All of F-Secure's pension arrangements are defined contribution plans. Contributions to defined contribution plans are recognized in the statement of comprehensive income in the period to which the contributions relate.

Leases

Leases are recorded in the balance sheet as right-of-use asset with a corresponding lease liability. Right-of-use assets and lease liabilities are initially measured at the present value of the remaining lease payments. An incremental borrowing rate is applied in discounting the remaining payments. F-Secure's incremental borrowing rate varies between 1.45% and 6.9% depending on geographical location of the leased asset and lease period, and the rate of 3.75% applies to the majority of the right-of-use assets.

Changes in estimates are accounted for at each reporting date. In measuring the present value of the liabilities arising from leases, any service-related fees are excluded from the lease payment. F-Secure's lease contracts do not contain residual value guarantees or purchase options. The estimated duration for on-going contracts varies between 1 to 5 years and the total liability from on-going contracts is EUR 5,065 thousand (EUR 1,210 thousand) (see Note 5 Leases and Note 20 Financial liabilities).

Income taxes

The income tax expense in statement of comprehensive income represents the sum of current taxes and deferred taxes. Current taxes are calculated on the taxable income for all Group companies in accordance with the local tax rules. Deferred taxes, resulting from temporary differences between the financial statement and the income tax basis of assets and liabilities, use the enacted tax rates in effect in the years in which the differences are expected to reverse. Deferred tax assets are recognized to the extent that it is probable that future taxable profit will be available. Deferred tax liabilities are recognized for all temporary differences.

Deferred tax assets and liabilities are offset when there is a legally enforceable right to set off current tax assets against current tax liabilities and when they relate to the same taxation authority and the Group intends to settle the assets and liabilities on a net basis.

Business combinations

Acquisition method is used for accounting the acquisition of businesses. The consideration transferred in a business combination is measured at fair value, which is calculated as the sum of the acquisition date fair values of assets transferred by the Group and liabilities incurred by the Group to the former owners of the acquiree. Costs related to the acquisition are recognized in profit and loss statement. The identifiable assets acquired and the liabilities assumed are recognized at fair value at the acquisition date except for deferred tax assets or liabilities which are measured in accordance with IAS 12 Income taxes. Goodwill is measured as the excess of the transferred consideration over the net amount of the acquired identifiable assets and assumed liabilities.

Goodwill

Goodwill is initially recognized and measured in business combinations as set out above. Goodwill is not amortized but is instead tested for impairment at least annually and whenever there is an indication that it may be impaired. For the purpose of impairment testing goodwill has been allocated to cash generating unit (CGU) expected to benefit from

the synergies of the combination. If the recoverable amount of the cash generating unit is less than the carrying amount of the unit, the impairment loss is allocated first to reduce the carrying amount of any goodwill allocated to the unit and then to the other assets of the unit. If an impairment loss for goodwill is recognized it will not be reversed in the subsequent periods. Goodwill is recorded at historical cost less accumulated impairment losses. F-Secure has only one CGU which consists of F-Secure's total business and the carrying amount of goodwill is allocated to this CGU.

Intangible assets

Research and development expenditure

Research expenditure is recognized as an expense at the time it is incurred. Development expenditure on new products or product versions with significant new features are recognized as intangible assets when F-Secure has the technical feasibility to complete the asset, has the ability and intention to use or sell the asset; can demonstrate that the asset will generate future economic benefits; has resources available to complete the asset; and has the ability to measure reliably the expenditure during development.

Development assets relate to developing new products and services or developing essential improvements for products and services. Amortization is recorded once the asset is ready on a straight-line basis over the estimated useful life, which is 3-5 years for these assets. These assets are reported either under Capitalized development or under Advance payments & incomplete development in Note 14 Non-current asset.

Intangible assets acquired in business combinations

Intangible assets acquired in business combinations and recognized separately from goodwill are initially recognized at fair value on the acquisition date. Subsequent to initial recognition these assets are reported at initial value less accumulated amortization and accumulated impairment losses. Intangible assets acquired in business combinations include technology and customer relationships, which all have a finite useful life. These assets are reported under Intellectual property and Other intangibles (see Note 14 Non-current asset). The estimated useful lives for intangible assets acquired in business combinations are:

Technology 15 years

Customer relationships 5–15 years

Other intangible assets

Other intangible assets include intangible rights and software licenses, all with a finite useful life. Other intangible assets include also partially or completely internally developed intangible assets which e.g. relate to platforms. Other intangible assets are recorded at historical cost less accumulated amortization and possible impairment. Amortization is recorded on a straight-line basis over the estimated useful life, which is 3–5 years for these assets.

Tangible assets

Tangible assets are recorded at historical cost less accumulated depreciation and possible impairment. Depreciation is recorded on a straight-line basis over the estimated useful life of an asset. The estimated useful lives of tangible assets are as follows:

Machinery and equipment 2–5 years

Other tangible assets 2–5 years

Impairment of assets

At each reporting date, or more frequently if needed, F-Secure assesses whether there is any indication that an asset may be impaired. Where an indicator of impairment exists, F-Secure makes a formal estimate of the recoverable amount. The recoverable amount of goodwill and intangible assets that are not ready for use are estimated annually regardless of whether any indication of impairment exists. The intangible assets that are not ready for use are software projects which cannot be assessed on its own because they don't have independent cash flow. If it is stated at the end of reporting period that the projects are finalized and will be taken in use, there is no need for impairment testing. Intangible assets that are not ready for use are tested as part of F-Secure's single cash generating unit. Where the carrying amount of an asset exceeds its recoverable amount, the asset is considered impaired and the carrying amount is reduced to its recoverable amount. The recoverable amount is the fair value of an asset less costs of disposal or value in use, whichever is higher. An impairment loss is recorded in the statement of comprehensive income.

A previously recognized impairment loss is reversed only if there has been a change in the estimates used to determine the asset's recoverable amount since the last impairment loss was recognized. The maximum reversal of an impairment loss amounts to no more than the carrying amount of the asset if no impairment loss had been recognized, net of depreciation.

Inventories

Inventories are measured at the lower of cost and net realizable value. Cost is determined by the first-in first-out method. Net realizable value is the estimated

selling price that is obtainable, less estimated costs of completion and the estimated costs necessary to make the sale.

Financial instruments

Financial instruments are originally measured at fair value. Subsequentially, financial assets are classified into the following categories: at amortized cost or fair value through profit and loss. The classification is made at the time of acquisition and is based on the cash flow characteristics and the business model of managing the financial asset. Financial liabilities are subsequentially classified and recognized at amortized cost or at fair value through profit and loss.

Financial instruments measured at fair value through profit and loss include derivative instruments to which hedge accounting is not applied. Realized and unrealized gains or losses arising from changes in fair values are recognized in the profit and loss in the period in which they incur.

According to F-Secure's treasury policy, company may enter derivative contracts to hedge against exchange rates and interest rates fluctuations. Company has no outstanding derivative contracts on the reporting date 31.12.2025.

Financial instruments are classified as current financial instruments unless the maturity exceed 12 months from the end of the reporting period.

Financial assets

Cash and cash equivalents, interest-bearing receivables and trade receivables are considered as financial assets. Financial assets are originally measured at fair value. Cash and cash equivalents in the balance sheet comprise cash at bank, deposits held at bank, and other highly liquid short-term investment with original maturity less than 3 months. Interest-bearing receivables are measured at amortized cost.

Trade receivables are originally measured with transaction price and later with amortized cost reduced by an expected credit loss for trade receivables. Trade receivables and other receivables are written off from the balance sheet as the rights to associated cash flows end or become transferred to the counterparty. An expected credit loss is recognized for trade receivables according to IFRS 9, Financial Instruments. The amount of expected credit loss is updated at each reporting date to reflect changes in credit risk since initial recognition of the respective financial instrument. The expected credit loss is estimated using a provision matrix where trade receivables are grouped based on historical credit loss experience and characteristics that depict the credit risk of receivables (e.g. geographical area and days past due).

Financial liabilities

F-Secure classifies bank loans, trade payables, lease liabilities and other interest-bearing liabilities as financial liabilities. Bank loans are initially recognized at the fair value of consideration plus directly attributable transaction costs. After initial recognition, bank loans are measured at amortized cost using the effective interest method. Other financial liabilities are measured at amortized cost.

Provisions

Provisions are recognized when F-Secure has a present obligation (legal or constructive) as a result of a past event, the outflow of resources is probable, and a reliable estimate of the amount of the obligation can be made. The amount recognized is a best estimate of the consideration required to settle the obligation at each reporting date. Risks and uncertainties are taken into account when making the estimate.

As at 31 December 2025, management has recognized a provision of EUR 425 thousand related to legal expenses and EUR 215 thousand (EUR 1,427 thousand) related to restructuring. See Note 23 Other liabilities .

Share-based payment transactions

F-Secure provides incentives to employees in the form of equity-settled share-based instruments. F-Secure's share-based incentive programs are targeted to F-Secure's key personnel. The programs are equity-settled. Equity-settled program is valued at fair value at grant date, and the expense is recognized evenly in the statement of comprehensive income over the vesting period with the counter-entry in retained earnings. In programs with market based conditions, the fair value is determined by utilizing commonly used valuation techniques. If a person leaves the company before vesting, the reward is forfeited. F-Secure updates its estimate of the ultimate number of shares at each reporting date. These changes in the estimate are recorded in the statement of comprehensive income.

Presentation of expenses

Classification of expenses by function has been made by presenting direct expenses in their respective functions.

Operating result

IAS 1, Presentation of Financial Statements, does not define the concept of Earnings before interest and taxes (EBIT). F-Secure has defined it as follows: EBIT is the net amount, which consists of revenue and other operating income less cost of revenue, personnel costs, depreciation and

amortization, possible impairment losses, and other operating expenses.

New standards and interpretations not yet effective

New or amended standards or interpretations are not expected to have an impact on the financial statements.

Effective 1 January 2027:

New IFRS standard "IFRS18 Presentation and disclosure in Financial Statements" will impact presentation and disclosure in financial statements. The structure of the statement of profit or loss will change and at the same time certain related measures, i.e. management-defined performance measures.

The adoption of IFRS 18 standard is expected to have a limited impact on our financial statements. The most significant change relates to the presentation of foreign exchange gains and losses, which will be reclassified from financing activities mostly to operating profit. However, we expect this impact to be relatively immaterial.

Additionally, the new standard will require changes to F-Secure's cash flow statement presentation to align with the new income statement categories introduced by IFRS 18. These changes are presentational in nature and will not affect our cash generation or underlying financial performance.

We anticipate that current Alternative Performance Measures (APMs) will largely transition to Management Performance Measures (MPMs) under the new standard, maintaining consistency in how we communicate our financial performance to stakeholders.

2. Segment information

F-Secure's operations and profitability is reported as a single operating segment which is consistent with the internal reporting and the way that operative decisions and assessment of performance have been made by Chief operating decision maker (CODM). For F-Secure CODM is leadership team which consists of CEO and currently 8 leadership team members. F-Secure's total business consists of designing and providing a comprehensive range of cybersecurity products and services related to data security, privacy protection as well as privacy protection and digital identity protection of consumers' terminal devices, networks and devices connected to a network, sold, in each case, either directly or indirectly, to consumers.

Geographical information

Geographical information about revenue is presented in Note 3 Revenue .

EUR 1,000	2025	2024
Long-term assets		
Nordic countries	167,022	163,160
Rest of Europe	435	342
North America	44,994	53,064
Rest of world	589	761
Total	**213,040**	**217,327**

3. Revenue

Principles of revenue recognition are stated in Note 1.2 Accounting principles, section Revenue recognition.

Disaggregation of revenue

EUR 1,000	2025	2024
Sales channels		
Revenue from external customers		
Partner channel	118,975	118,237
Security Suite	95,569	95,734
Embedded Security	23,406	22,503
Direct channel (E-commerce)	26,764	28,021
Total	**145,739**	**146,258**

The table above has been updated to show main product portfolios in partner channel.

EUR 1,000	2025	2024
Geographical information		
Revenue from external customers		
Nordic countries	44,756	42,019
Rest of Europe	45,403	48,099
North America	44,317	45,518
Rest of world	11,263	10,621
Total	**145,739**	**146,258**

F-Secure had one individual customer which represented more than 10% of Group's 2025 revenue. Total revenue from this customer was EUR 16,559 thousand (EUR 17,147 thousand).

Assets and liabilities from contracts with customers

Satisfied performance obligations from contracts with customers that have not yet been invoiced on the reporting date are presented in the balance sheet as Accrued income. The balances relate to products delivered to customers and recognised as revenue but not invoiced. Liabilities from contracts with customers are presented in the balance sheet as Deferred revenue and included in Total non-current liabilities or Total current liabilities depending on the duration of the liability. Prior year current deferred revenue is recognised as revenue in the current period. Remaining performance obligations from contracts with customers represent contracted revenue that has not yet been recognised. These balances are presented as Deferred revenue and relate to obligations to provide software subscription services in contracts with a duration of multiple years.

EUR 1,000	2025	2024
Accrued income	2,435	3,333
Deferred revenue, non-current	5,940	6,398
Deferred revenue, current	21,068	22,079

Increases in deferred revenue resulting from billing were EUR 20,610 thousand for the year ended (EUR 22,640 thousand). Decreases in deferred revenue resulting from satisfying performance obligations were EUR 22,079 thousand for the year (EUR 19,788 thousand).

4. Other operating income

EUR 1,000	2025	2024
Government grants	748	228
Transition services	11	515
Other	13	8
Total	**771**	**751**

The government grants are received for certain research and development projects and are recognised as income over those periods in which the corresponding expenses arise.

None of the amounts included in Other are individually significant.

5. Leases

The principles of lease accounting are stated in Note 1.2 Accounting principles, section Leases.

EUR 1,000	2025	2024
Depreciation		
Right of use assets		
Buildings	1,234	1,049
Cars and machiney	201	117
Total	**1,435**	**1,165**
Interest expense on lease liabilities	132	66
Short-term leases booked as rent expense	291	213

Right of use assets	2025	2024
Buildings	4,099	969
Cars and machiney	726	231
Total	**4,825**	**1,200**

Lease liabilities	2025	2024
Buildings	4,330	988
Cars and machiney	735	222
Total	**5,065**	**1,210**
Repayments of lease liabilities	1,227	1,174

The increase in lease liabilities relates to the new lease agreement for headquarter office premises which was recorded in the balance sheet as right-of-use asset and lease liability in July 2025 when the lease term started. The four-year contract increased right-of-use assets value by EUR 4.0 million.

Right of use assets related changes are stated in Note 14. Non-current assets.

Interest expenses related to lease liabilities are stated in Note 9. Financial income and expenses.

Maturity of lease liabilities is stated in Note 20. Financial liabilities.

6. Depreciation and amortization

EUR 1,000	2025	2024
Depreciation and amortization of non-current assets		
Other intangible assets	10,119	9,663
Capitalized development	4,598	2,581
Intangible assets	**14,716**	**12,244**
Right of use assets	1,435	1,165
Other tangible assets	293	211
Tangible assets	**1,727**	**1,377**
Total depreciation and amortization	**16,443**	**13,621**

Depreciation and amortization by function (EUR 1,000)		
Sales and marketing	1,533	1,213
Research and development	6,243	3,882
Administration	8,668	8,525
Total depreciation and amortization	**16,443**	**13,621**

7. Personnel expenses

EUR 1,000	2025	2024
Personnel expenses		
Wages and salaries	33,971	36,065
Pension expenses - defined contribution plan	4,960	4,856
Share-based payments	1,140	1,045
Other social expenses	2,742	3,062
Total	**42,812**	**45,029**

For share-based payments, see further in Note 19. Share-based payment transactions.

Employee benefits of the management are stated in Note 24. Related party transactions.

	2025	2024
Average number of personnel	526	519

Personnel by function December 31		
Sales and marketing	189	169
Research and development	301	308
Administration	59	52
Total	**549**	**529**

8. Audit fees

EUR 1,000	2025	2024
Group auditor		
Audit fees, PricewaterhouseCoopers	162	159
Audit related fees, PricewaterhouseCoopers		21
Tax consulting, PricewaterhouseCoopers		11
Other services, PricewaterhouseCoopers	117	126
Total	**278**	**317**

Other services include, among others sustainability assurance.

EUR 1,000	2025	2024
Other auditors		
Audit fees	22	26
Total	**22**	**26**

9. Financial income and expenses

EUR 1,000	2025	2024
Financial income		
Exchange gains	889	850
Interest income	403	838
Other financial income	3	26
Total	**1,295**	**1,714**
Financial expenses		
Exchange losses	-1,216	-1,090
Interest expenses	-7,289	-11,370
Other financial expenses	-648	-597
Interest expense from lease liabilities	-132	-66
Total	**-9,285**	**-13,124**

10. Income tax

This note presents F-Secure's income tax expenses included in the financial statements. The accounting principles of income taxes are stated in Note 1.2 Accounting principle, Income taxes.

EUR 1,000	2025	2024
Current income tax for the year	3,002	3,610
Change in deferred tax	2,175	2,334
Total	**5,178**	**5,944**

A reconciliation of income tax expense in the income statement and income tax calculated at the parent company's country of residence income tax rate (20%):

EUR 1,000	2025	2024
Profit before taxes	27,548	27,011
Income tax at Finnish tax rate of 20%	-5,510	-5,402
Effect of overseas tax rates	-254	-425
Non-deductible expenses/tax-exempt revenue	94	-130
Effect of deferred tax not recognized	0	8
Deferred tax adjustments	245	41
Adjustments for prior period current tax	250	10
Other	-3	-46
Total	**-5,178**	**-5,944**

11. Earnings per share

Basic earnings per share amounts are calculated by dividing net profit for the year attributable to ordinary equity holders of the parent by the weighted average number of ordinary shares outstanding during the year. Diluted earnings per share amounts are calculated by dividing the net profit attributable to ordinary shareholders by the weighted average number of ordinary shares outstanding during the year adjusted for the effects of dilutive options.

EUR 1,000	2025	2024
Net profit attributable to equity holders from	22,370	21,067
Weighted average number of ordinary shares (1 000)	174,682	174,673
Weighted average number of ordinary shares (1 000), diluted	175,453	174,924
Basic and diluted earnings per share (EUR/share)	0.13	0.12

Earnings per share is based on the average number of shares. During the period, F-Secure hasn't had Treasury shares.

12. Acquisitions

Group hasn't made any acquisitions during 2025 or 2024.

13. Goodwill

For impairment testing goodwill is allocated to cash-generating units (CGUs). F-Secure has only one CGU which consists of F-Secure's total business. The carrying amount of goodwill EUR 87,029 thousand is allocated to this CGU.

Goodwill is tested for impairment annually, or more frequently if there are indications that goodwill might be impaired. The recoverable amount for the CGU is determined based on a value in use calculation which uses cash flows for the period determined for the CGU. Cash flows are based on financial budgets and forecasts approved by the Board of Directors. Forecast period of five years is used. Discount rate is 8.72% (8.39%) before taxes.

Cash flows beyond forecast period have been extrapolated using steady 2% (2%) per annum growth rate. Markets where CGU operates are expected to grow faster than the terminal growth rate in impairment testing. Market is expected to grow mid single digit annually by 2027 (based on F-Secure management estimate and industry analyst reports).

Sensitivity analysis

F-Secure has prepared a sensitivity analysis of the impairment tests, adjusting the key assumptions which are revenue, profitability, and discount rate -based on management judgment. Any reasonable possible changes in the key assumptions in impairment tests would not cause the aggregate carrying amounts exceeding the recoverable amounts.

14. Non-current asset

	Intangible assets						Tangible assets			
EUR 1,000	Intellectual property[1]	Other Intangible[2]	Goodwill	Capitalized development[3]	Advance payments & incomplete development	Total	Machinery & Equipment	Right of use assets	Other Tangible	Total
Acquisition cost Dec 31, 2023	**82,910**	**34,607**	**88,361**	**9,182**	**6,152**	**221,212**	**444**	**3,020**	**108**	**3,573**
Translation difference		2,002	1,422			3,424	15	-10		5
Additions					10,986	10,986	170	1,193	2	1,365
Transfers		6,955		8,322	-15,662	-385				
Disposals							-14	-831		-845
Acquisition cost Dec 31, 2024	**82,910**	**43,563**	**89,783**	**17,504**	**1,475**	**235,237**	**615**	**3,372**	**110**	**4,097**
Translation difference		-3,783	-2,754			-6,537	-65	-15		-79
Additions					11,707	11,707	880	5,082	130	6,092
Transfers		3,542		3,735	-7,277	0				
Disposals							-115	-2,239	-2	-2,356
Acquisition cost Dec 31, 2025	**82,910**	**43,322**	**87,029**	**21,240**	**5,906**	**240,407**	**1,316**	**6,200**	**238**	**7,754**
Acc. depreciation Dec 31, 2023	**-3,125**	**-1,670**		**-2,876**		**-7,672**	**-121**	**-1,763**	**-71**	**-1,956**
Translation difference		-154				-154	-3	7		5
Transfers		282		103		385				
Depreciation for the period	-5,546	-4,149		-2,581		-12,276	-182	-1,175	-34	-1,391
Depreciation of disposals							12	759		770
Acc. depreciation Dec 31, 2024	**-8,671**	**-5,691**		**-5,354**		**-19,717**	**-294**	**-2,172**	**-105**	**-2,571**
Translation difference	400					400	19	4		23
Transfers	-119	551		-432		0				
Depreciation for the period	-5,592	-4,979		-4,047		-14,617	-270	-1,436	-19	-1,725
Depreciation of disposals							81	2,229		2,310
Acc. depreciation Dec 31, 2025	**-13,982**	**-10,119**		**-9,833**		**-33,934**	**-463**	**-1,375**	**-125**	**-1,963**
Book value as at Dec 31, 2024	74,239	37,872	89,783	12,150	1,475	215,520	321	1,200	5	1,526
Book value as at Dec 31, 2025	**68,929**	**33,203**	**87,029**	**11,406**	**5,906**	**206,473**	**853**	**4,825**	**113**	**5,791**

1) Intellectual property consists of technology from acquisition EUR 68,929 thousand as at 31 December 2025

2) Other intangible consists mainly of customer relationship from acquisition EUR 30,411 thousand as at 31 Dec 2025.

3) Capitalised development expenses relate to new products and development of new product versions with significant new features (refer to the section on Research and development expenditure included within Intangible assets in Note 1.2 Accounting principles).

15. Inventories

The accounting principles of inventories are stated in Note 1.2 Accounting principles, section Inventories.

EUR 1,000	2025	2024
Inventories	20	29

The inventory balances included in the financial statements consist of the packaging used for license key cards.

16. Financial assets

This note presents F-Secure's financial assets included in the financial statements. The accounting principles of financial assets are stated in Note 1.2 Accounting principles, section Financial instruments.

EUR 1,000	2025	2024
Cash at bank and in hand	10,771	8,095
Interest-bearing receivables, current		3,757
Trade receivables	25,594	27,604
Total	**36,365**	**39,455**

Interest-bearing receivables in 2024 relate to WithSecure structuring loans which were paid in the second quarter of 2025.

Aging of trade receivables and expected credit losses

Trade receivables 31 Dec 2025 (EUR 1,000)	Not fallen due	Overdue 1-30 days	Overdue 31-60 days	Overdue 61-90 days	Overdue 91-120 days	Overdue more than 120 days	Total
Average expected credit loss rate	0.3 %	0.3 %	5.0 %	12.0 %	17.0 %	35.0 %	
Gross trade receivables	22,189	2,568	446	17	427	359	26,005
Loss allowance	-67	-8	-23	-3	-73	-108	-281
Additional provision						-131	-131
Total trade receivables at amortized cost Dec 31, 2025	**22,122**	**2,560**	**423**	**14**	**354**	**120**	**25,594**

Trade receivables 31 Dec 2024 (EUR 1,000)	Not fallen due	Overdue 1-30 days	Overdue 31-60 days	Overdue 61-90 days	Overdue 91-120 days	Overdue more than 120 days	Total
Average expected credit loss rate	0.4 %	0.4 %	5.0 %	12.0 %	17.0 %	35.0 %	
Gross trade receivables	22,039	4,058	413	685	421	675	28,291
Loss allowance	-88	-16	-21	-82	-71	-249	-528
Additional provision						-160	-160
Total trade receivables at amortized cost Dec 31, 2024	**21,951**	**4,042**	**392**	**603**	**349**	**266**	**27,604**

EUR 1,000	2025	2024
Movements in loss allowances on trade receivables		
Book value as at Jan 1	687	547
Change for the year	-271	190
Receivables written off during the year	-5	-49
Book value as at Dec 31	**412**	**687**

17. Other receivables

Non-current receivables

EUR 1,000	2025	2024
Other receivables	590	223
Total	**590**	**223**

Current receivables

EUR 1,000	2025	2024
Other receivables	551	845
Prepaid expenses	7,836	8,600
Accrued income	2,435	3,333
Income tax receivables	861	968
Total	**11,682**	**13,747**

Material items included in prepaid expenses

EUR 1,000	2025	2024
Prepaid software subscriptions	1,967	1,688
Accrued sales commissions	1,698	2,215
Prepaid and accrued royalty	1,746	2,440
Merchandise cost	1,347	453
Grant receivable	563	192
Other prepaid expenses	515	1,612
Total	**7,836**	**8,600**

Comparison year figures have been reclassified to give more accurate view on material items.

18. Shareholders' Equity

Issued and fully paid

EUR 1,000	Number of shares	Share capital	Unrestricted equity reserve
31 December 2023	174,673,165	80	9,590
31 December 2024	174,673,165	80	9,590
Share issue 2025	33,905		
31 December 2025	**174,707,070**	**80**	**9,590**

The share capital amounting to 80,000 euro was formed in the demerger on 30 June 2022. The number of shares was 174,707,070 (no own shares) at the end of 2025.

The Board of Directors resolved a directed share issue in September 2025 to the plan participants of the Company's Employee share savings plan. The shares issued account for the rewards earned from the period 2022-2025.

A share has no nominal value. Accountable par value is EUR 0.01.

Translation differences

The translation difference is used to record exchange difference arising from the translation of the financial statements of foreign subsidiaries.

Unrestricted equity reserve

Unrestricted equity reserve was formed in connection with demerger on 30 June 2022. Unrestricted equity reserve includes other equity-related investments and that part of the share subscription price which is not recognized in share capital according to a specific decision.

Dividends proposed and paid

Proposed for approval at AGM for financial year 2025 is that dividend of 0.04 euro per share will be paid.

Dividend for financial year 2024 was 0.04 per share, paid during 2025 (6,986,926.60 euro in total).

Dividend for financial year 2023 was 0.07 per share, paid during 2024 (12,227,121.55 euro in total).

Treasury shares

At the end of 2025 company doesn't hold any treasury shares.

19. Share-based payment transactions

F-Secure has had several share-based incentive programs during the period. The purpose of the plans is to align the interests of the shareholders and the plan participants in order to increase the value of F-Secure share and retain and motivate key management by offering them a competitive incentive plan.

The effect of the plans and related expenses are presented below. Accounting principles for share-based payments are stated in Note 1.2 Accounting principles, section Share-based payment transactions.

Share-based incentive programs

The share-based incentive programs offer the participants a possibility to receive shares of F-Secure Corporation as an incentive reward if the company's financial targets set for the earning period have been achieved. The share-based compensation is forfeited if the employment relationship is terminated by either party before the end of the lock-up period. The plan structure is following: a Performance Matching Share Plan (PMSP) for the members of Leadership team and selected key employees, a Performance Share Plan (PSP) for the company's senior management, a Restricted Share Plan for individually selected key employees and an Employee Share Savings Plan for all employees. Members of the Leadership Team and selected key employees can participate in either PSP or PMSP according to their choice, not both plans.

Performance share plan 2023–2025

F-Secure established a share-based program 2023–2025. The program's duration is three years with the grant date in April 2023. The value of F-Secure share at grant date for the program was EUR 3.39 for the earning period 2023-2025. The current program ends in March 2026 with a possible reward payment, paid during spring 2026. The payment of the reward is conditional on the achievement of the performance targets. The maximum total of shares to be given is 800,000 shares. The potential reward will be paid either in shares, in cash or in a combination of these.

The vesting of the rewards is conditional to the participant remaining in the service of F-Secure. The incentive plan has a performance condition based on F-Secure's absolute total shareholder return and revenue growth and profitability.

In accordance with the terms of the program, no retentions are expected at the date of this financial statement. The expense arising from the Performance share plan 2023–2025 was EUR 92 (351) thousand in 2025.

Performance share plan 2024–2026

F-Secure established a share-based program 2024–2026. The program's duration is three years with the grant date in April 2024. The value of F-Secure share at grant date for the program was EUR 1.72 for the earning period 2024-2026. The current program ends in March 2027 with a possible reward payment, paid during spring 2027. The payment of the reward is conditional on the achievement of the performance targets. The maximum total of shares to be given is 1,512,000 shares. The potential reward will be paid either in shares, in cash or in a combination of these.

The vesting of the rewards is conditional to the participant remaining in the service of F-Secure. The incentive plan has a performance condition based on F-Secure's absolute total shareholder return, earnings per share (EPS) and revenue growth.

In accordance with the terms of the program, no retentions are expected at the date of this financial statement. The expense arising from the Performance share plan 2024–2026 was EUR 212 (267) thousand in 2025.

Performance share plan 2025–2027

F-Secure established a share-based program 2025–2027. The program's duration is three years with the grant date in March 2025. The value of F-Secure share at grant date for the program was EUR 1.64 for the earning period 2025-2027. The current program ends in March 2028 with a possible reward payment, paid during spring 2028. The payment of the reward is conditional on the achievement of the performance targets. The maximum total of shares to be given is 1,740,000 shares. The potential reward will be paid either in shares, in cash or in a combination of these.

The vesting of the rewards is conditional to the participant remaining in the service of F-Secure. The incentive plan has a performance condition based on F-Secure's absolute total shareholder return, earnings per share (EPS) and revenue growth.

In accordance with the terms of the program, no retentions are expected at the date of this financial statement. The expense arising from the Performance share plan 2025–2027 was EUR 197 thousand in 2025.

Performance matching share plan 2025–2028

F-Secure established a performance matching share plan 2025–2028. It is possible to earn matching rewards and performance-based matching rewards. The program's duration is three years with one year retention period. The grant date was in March 2025. The potential rewards from the PMSP will be paid in two equal instalments, first instalment within spring 2028 after the end of the performance period and second instalment within spring 2029 after the end of the retention period. The payment of the reward is conditional on the achievement of the performance targets. The maximum total of shares to be given is 5,640,000 shares. The potential reward will be paid either in shares, in cash or in a combination of these.

The prerequisite for participation in the PMSP and receiving reward is that a participant personally invests in F-Secure's shares. The final number of shares will depend on the participants' personal investments in F-Secure's share and the achievement of the targets set for the performance criteria. The personal investments vary between 10%-40% of annual base pay. The matching reward is determined based on the fulfilment of the share ownership obligation and valid employment or director agreement. The performance-based matching reward is in addition determined based on the achievement of targets set for the performance criterion. The incentive plan has a performance condition based on F-Secure's share price. The program rewards for considerable increase in F-Secure's share price development.

In accordance with the terms of the program, no retentions are expected at the date of this financial statement. The expense arising from the Performance matching share plan 2025–2028 was EUR 321 thousand in 2025.

Restricted share plan 2023–2025

F-Secure established a restricted share plan in March 2023. The program's duration is three years and potential reward will be paid during spring 2026. Company can grant fixed share rewards during retention period. The restricted share plan complements the incentive programs for separately selected key persons in special situations. The values of the F-Secure share at grant date for this program was EUR 2.98 and EUR 2.05 and the maximum total of shares to be given is 80,000 shares. The potential reward will be paid either in shares, in cash or in a combination of these.

The vesting of the rewards for all periods is conditional on the participant remaining in the service of F-Secure. The Board approved the metrics, targets and participants on an annual basis for each earning period. In accordance with the terms of the program, no retentions are expected at the date of this financial statement. The reversal of expense arising from the restricted share plan was EUR 11 thousand in 2025 (expense EUR 18 thousand in 2024).

The participating employee of a share-based incentive program shall be entitled to the shareholder rights of the reward shares (e.g., dividend) from the moment the shares have been entered into the participating employee's book-entry account.

The costs of equity-settled transactions are measured by reference to the fair value of shares at the date on which they are granted. Fair value for performance based programs is based on the share price on the grant date. Fair value for market based programs is based on externally accepted valuation methods. The costs of cashsettled transactions are measured by reference to the market price of the share on the balance sheet date. F-Secure updates the estimate of the number of equity instruments that will ultimately vest at each reporting date.

Restricted share plan 2024–2026

F-Secure established a restricted share plan in March 2024. The program's duration is three years and potential reward will be paid during spring 2027. Company can grant fixed share rewards during retention period. The restricted share plan complements the incentive programs for separately selected key persons in special situations. The values of the F-Secure share at grant date for this program was EUR 1.65, EUR 2.01 and 1.87 and the maximum total of shares to be given is 300,000 shares. The potential reward will be paid either in shares, in cash or in a combination of these.

The vesting of the rewards for all periods is conditional on the participant remaining in the service of F-Secure. The Board approved the metrics, targets and participants on an annual basis for each earning period. In accordance with the terms of the program, no retentions are expected at the date of this financial statement. The expense arising from the restricted share plan was EUR 113 (65) thousand in 2025.

The participating employee of a share-based incentive program shall be entitled to the shareholder rights of the reward shares (e.g., dividend) from the moment the shares have been entered into the participating employee's book-entry account.

The costs of equity-settled transactions are measured by reference to the fair value of shares at the date on which they are granted. Fair value for performance based programs is based on the share price on the grant date. Fair value for market based programs is based on externally accepted valuation methods. The costs of cashsettled transactions are measured by reference to the market price of the share on the balance sheet date. F-Secure updates the estimate of the number of equity instruments that will ultimately vest at each reporting date.

Restricted share plan 2025–2027

F-Secure established a restricted share plan in March 2025. The program's duration is three years and potential reward will be paid during spring 2028. Company can grant fixed share rewards during retention period. The restricted share plan complements the incentive programs for separately selected key persons in special situations. The values of the F-Secure share at grant date for this program was EUR 1.81 and 1.60 and the maximum total of shares to be given is 500,000 shares. The potential reward will be paid either in shares, in cash or in a combination of these.

The vesting of the rewards for all periods is conditional on the participant remaining in the service of F-Secure. The Board approved the metrics, targets and participants on an annual basis for each earning period. In accordance with the terms of the program, no retentions are expected at the date of this financial statement. The expense arising from the restricted share plan was EUR 87 thousand in 2025.

The participating employee of a share-based incentive program shall be entitled to the shareholder rights of the reward shares (e.g., dividend) from the moment the shares have been entered into the participating employee's book-entry account.

The costs of equity-settled transactions are measured by reference to the fair value of shares at the date on which they are granted. Fair value for performance based programs is based on the share price on the grant date. Fair value for market based programs is based on externally accepted valuation methods. The costs of cashsettled transactions are measured by reference to the market price of the share on the balance sheet date. F-Secure updates the estimate of the number of equity instruments that will ultimately vest at each reporting date.

Employee share savings plan

During 2022, F-Secure launched a employee share savings plan which was available for all employees. The plan consists of annually commencing plan periods, each one comprising of a 12-month savings period and a holding period following the savings period. The first plan period commenced on 1 October 2022 and ended on 30 September 2025. The second plan period commenced on 1 October 2023 and ends on 30 September 2026. Third plan period commenced on 1 October 2024 and ends on 30 September 2027. The fourth plan period commenced on 1 October 2025 and ends on 30 September 2028. Every employee was eligible to save a proportion of their salaries and invest those savings in F-Secure shares. The savings will be used for acquiring F-Secure shares quarterly after the publication of the respective interim reports. F-Secure grants the participating employees a gross reward of one matching share for every two shares acquired with their savings. For the first plan period the maximum number of of matching shares is approximately 200 000 shares, for the second plan period 250 000 shares, for the third plan period 392,023 shares and for the fourth plan period 449,600 shares.

The vesting of the rewards is conditional on the participant remaining in the service of F-Secure and on an initial investment. The Board approves the metrics, targets, and participants on an annual basis for each earning period. The expense arising from the employee shares savings plan was EUR 130 (85) thousand in 2025.

Impacts of share-based payment transactions on financial statements

EUR 1,000	2025	2024
Booked as expense during the period	1,140	1,045
Booked in retained earnings during the period	1,083	1,045
Balance sheet liability at the end of the period	67	84

20. Financial liabilities

F-Secure's financial liabilities consist of interest-bearing liabilities and trade payables. Interest-bearing liabilities include bank loans, and lease liabilities from building, office equipment and cars (see Note 1.2 Accounting principles, section Leases and Note 5. Leases).

Interest-bearing liabilities

EUR 1,000	2025	2024
Bank loans	151,336	168,933
Lease liabilities	5,065	1,210
Other interest-bearing liabilities		5,334
Total	**156,401**	**175,477**

The Lookout consumer business unit acquisition in 2023 was financed with debt for which facilities agreement was entered into with Danske Bank A/S and OP Corporate Bank plc. The financing package consisted of two facilities, (i) a EUR 202 million amortizing term loan to finance the acquisition, and (ii) an EUR 20 million revolving loan facility to be used for general corporate purposes of the group. Both facilities held a maturity of 5 years since F-Secure has exercised the extension options. Facilities mature in 2028. The interest rate for credit facilities is variable. During the accounting period, the term loan was repaid by EUR 45.0 million (EUR 30.0 million). The revolving credit facility is undrawn at the reporting date.

During the second quarter of 2025, F-Secure signed and withdrew EUR 35 million loan from Nordic Investment Bank (NIB). The loan has seven-year maturity, and the first two years of the loan are repayment-free.

All Group's loan agreements include a financial covenant, measured on a quarterly basis. The covenant relates to the ratio between net debt and EBITDA, as defined under the terms of the loan agreement. The group has met covenant terms and conditions on the reporting date. Carrying amount for bank loans at the end of reporting period is EUR 151.4 million (EUR 168.9 million).

Prior to completion of the demerger, WithSecure's consumer business conducted by its foreign subsidiaries was separated from the rest of the business into separate companies through business acquisitions or similar transactions in each relevant country. These balances were due for payment in the second quarter of 2025. F-Secure's payables totaled EUR 5.3 million and the receivables totaled EUR 3.7 million. There are no more outstanding balances between WithSecure and F-Secure.

F-Secure has no outstanding derivative contracts on 31 December 2025.

Contractual maturities of interest-bearing liabilities

EUR 1,000	2025	2024
Amount due for settlement within 12 months	31,710	44,046
Amount due for settlement after 12 months	124,691	131,431
Total	**156,401**	**175,477**

Bank loan carry variable interest rates. The weighted average interest rates paid during the year were as follows:

	2025	2024
Bank loans	3.8 %	5.8 %

Contractual maturities of financial liabilities

Contractual maturities of financial liabilities (EUR 1,000)	Less than 1 year	1 to 2 years	2 to 3 years	3 to 4 years	4 to 5 years	over 5 years	Total contractual cash flows	Carrying amount
2025								
Bank loans	30,000	36,364	63,364	6,364	6,364	9,545	152,000	151,336
Interest payment for bank loan	5,469	4,282	1,762	821	568	378		
Lease liabilities	1,791	1,568	1,291	752	66	39	5,507	5,065
Trade payables	2,530						2,530	2,530
Total	**39,791**	**42,214**	**66,416**	**7,937**	**6,998**	**9,962**	**160,037**	**158,931**

Contractual maturities of financial liabilities (EUR 1,000)	Less than 1 year	1 to 2 years	2 to 3 years	3 to 4 years	4 to 5 years	over 5 years	Total contractual cash flows	Carrying amount
2024								
Bank loans	38,000	30,000	102,000				170,000	168,933
Interest payment for bank loan	7,059	5,507	1,435					
Lease liabilities	756	328	111	37	14		1,247	1,210
Other interest-bearing liabilities	5,334						5,334	5,334
Trade payables	1,545						1,545	1,545
Total	**52,694**	**35,835**	**103,545**	**37**	**14**	**0**	**178,125**	**177,022**

21. Financial risk management

Classes and categories of financial assets and liabilities and their fair values

Fair value hierarchy levels 1 to 3 are based on the degree to which the fair value is observable:

Level 1: Fair values of financial instruments are based on quoted prices in active markets for identical assets and liabilities.

Level 2: Financial instruments are not subject to trading in active and liquid markets. The fair values of financial instruments can be determined based on quoted market prices and deduced valuation.

Level 3: Measurement of financial instruments is not based on verifiable market information, and information on other circumstances affecting the value of the instruments is not available or verifiable.

The carrying amount of the Group's interest-bearing financial assets and liabilities does not significantly differ from their fair value. The carrying amount of the Group's bank loans as of the December 31, 2025, is EUR 151.3 million, and the fair value is EUR 151.8 million.

			Carrying value		
2025			Financial assets	Financial liabilities	
EUR 1,000	Note	Fair value hierarchy	Amortized cost	Amortized cost	TOTAL
Cash and bank	16		10,771		10,771
Trade receivables	16		25,594		25,594
Trade payables	20			2,530	2,530
Lease liabilities	20			5,065	5,065
Bank loans	20	Level 2		151,336	151,336

2024			Carrying value		
			Financial assets	Financial liabilities	
EUR 1,000	Note	Fair value hierarchy	Amortized cost	Amortized cost	TOTAL
Cash and bank	16		8,095		8,095
Interest-bearing receivables	16	Level 2	3,980		3,980
Trade receivables	16		27,604		27,604
Trade payables	20			1,545	1,545
Lease liabilities	20			1,210	1,210
Bank loans	20	Level 2		168,933	168,933
Other interest-bearing liabilities	20	Level 2		5,334	5,334

General

The responsibility for F-Secure's risk management lies with the CEO, management and ultimately with the Board of Directors. The goal of risk management is to identify risks that may hinder the company from achieving its business objectives. F-Secure is exposed to various financial risks in its business operations. Main financial risks are credit risk, liquidity risk, foreign currency exchange risk and interest rate risk. The Board of Directors of F-Secure approves the general principles of risk management, and the Group's treasury function is responsible for managing market risks.

Credit risk

F-Secure manages credit risk on group level with Credit risk policy. Credit risk derives from trade receivables. The maximum exposure to credit risk at the reporting date is the carrying value of trade receivables. Trade receivables do not include any major concentrations of credit risk by customer. Group trades only with recognized, creditworthy third parties and monitors customers' creditworthiness. Trade receivables are monitored and collected on an ongoing basis. The top three customers account for 10.4%, 6.4% and 5.8% in 2025 (16.0%, 6.6% and 5.5% in 2024) of trade receivables. See Note 16. Financial assets.

Liquidity risk

Liquidity risk arises if the Group's existing liquidity reserves, net cash flows and available additional financing are not sufficient to cover commitments falling due within next 12 months. Group manages its liquidity risk by centralizing the management of cash reserves, maintaining sufficient cash balances, and utilizing committed credit facilities. F-Secure has a revolving credit facility (RCF) of EUR 20 million that matures in 2028. The revolving credit facility is undrawn at the reporting date. Group Treasury is responsible for monitoring cash balances and cash forecasts to keep liquidity risk at manageable level. We expect the stable and positive cash flow from operations, existing cash balances, and revolving credit facilities to be sufficient to fund our operations and obligations for the next 12 months. Contractual maturities of financial liabilities are presented in Note 20 Financial liabilities.

All Group's loan agreements include a financial covenant, measured on quarterly basis. The covenant relates to the ratio between net debt and EBITDA, as defined under the terms of the loan agreement. The group closely monitors the covenant situation and will take action if necessary. Group has met covenant terms and conditions during the reporting period. Carrying amount for bank loan at the end of reporting period is EUR 151.3 million (EUR 168.9 million).

Foreign currency risk

The Group operates globally and is exposed to a currency risk arising from exchange rate fluctuations against its reporting currency euro. Transaction risk is related to foreign currency transactions in sales and expenses. Translation risk arises from the Group's net investments outside euro zone.

Transaction risk

Transaction risk arises from future commercial transactions and recognized assets and liabilities denominated in a currency that is not the functional currency of the relevant group entity. The majority of sales is invoiced in Euro. The other main currencies for invoicing are US dollar (USD), the Swedish krona (SEK), the pound

sterling (GBP) and the Japanese yen (JPY). The currency risk arising from sales invoicing is reduced by operational expenses arising in the same currencies as the sales invoicing. The transaction risk is managed centrally such that the F-Secure operations mainly have transactions in their legal entities' functional currency and intercompany transactions are carried out in the group entities functional currencies. The main foreign currency risk arises from USD denominated sales invoicing, purchases and intercompany transactions at the F-Secure parent entity level, creating volatility in the financial income and expenses.

Exchange gains were EUR 0.9 million (EUR 0.9 million) and exchange losses EUR -1.2 million (EUR -1.1 million).

Sales in different currencies	2025 %	2024 %
EUR	60	59
USD	27	30
JPY	5	5
SEK	5	4
GBP	1	2
Other currencies	1	1
Total	**100**	**100**

The carrying Euro (thousand) amounts of the Group's financial assets and liabilities at the reporting date are as follows:

Financial assets (EUR 1,000)	2025	%	2024	%
EUR	20,338	56	19,255	49
USD	10,147	28	12,090	30
SEK	2,204	6	1,544	4
GBP	1,289	4	2,958	7
JPY	1,204	3	2,023	5
Other currencies	1,181	9	1,809	5
Total	**36,365**	**100**	**39,678**	**100**

Financial liabilities (EUR 1,000)	2025	%	2024	%
EUR	158,106	99	173,526	98
USD	702	0	327	0
MYR	43	0	1,356	1
JPY	4	0	1,306	1
Other currencies	76	0	506	0
Total	**158,931**	**100**	**177,022**	**100**

Financial liabilities in the above table also include lease liabilities.

The table below demonstrates how sensitive F-Secure's profit before taxes is to foreign exchange rate fluctuations when all other variables are held constant. The open exposure against USD arising from F-Secure trade receivables and trade payables have an impact on F-Secure's profit before taxes. The sensitivity calculation is based on a change of 10% in the Euro exchange rate against the functional currencies F-Secure operates in. There were no other material exposures.

EUR million	2025	2024
USD	-0.6/+0.7	-1.0/+1.2

Translation risk

Translation risk arises from the F-Secure's net investments in foreign currencies. Translation differences arise from translating balances into euro using exchange rates prevailing on the reporting date. Most significant translation risks arise from goodwill EUR 21.0 million (EUR 23.8 million) and intangible assets EUR 23.9 million (EUR 29.2 million) generated in acquisition of mobile consumer security business unit from Lookout Inc. Main currency is USD. According to current policy, F-Secure does not hedge investments made in its subsidiaries.

Change in foreign exchange translation differences amounted EUR -7.5 million in 2025 (EUR 4.0 million).

The table below demonstrates how sensitive the Group's equity is to foreign exchange rate fluctuations when all other variables are held constant. The sensitivity calculation is based on a change of 10% in the Euro exchange rate against the functional currencies exposing the Group to translation risk. There were no other material exposures.

EUR million	2025	2024
USD	-6.6/+5.4	-7.0/+5.7

Interest rate risk

F-Secure is exposed to interest rate arising from interest-bearing liabilities which relate to bank loans. The interest rate of bank loans (Facility A EUR 117 million, NIB EUR 35 million) is tied to variable reference interest rate. F-Secure is regularly evaluating the need for hedging interest rate risk. In the financial year 2025, the company did not hedge against interest rate risk. Apart from bank loans there were no other material exposures. The table below demonstrates the sensitivity of Group's profit before taxes to 1% change in interest rate when all other variables are held constant.

EUR million	2025	2024
Interest-bearing liabilities, bank loans	-1.7/+1.7	-1.9/+1.9

Capital management

F-Secure's shareholders' equity is managed as capital. The objective of F-Secure's capital management is to maintain an efficient capital structure that ensures the functioning of business operations and promotes shareholder value. F-Secure's capital structure is reviewed regularly as a part of financial performance monitoring. The capital structure can be adjusted among other things by distribution of dividends, share repurchase or capital repayment. The dividend policy of F-Secure Corporation is to aim to pay around or above 50 per cent of its net profit as dividend on an annual basis. This can be adjusted as long as leverage is higher than the targeted level (below 2.5x). Subject to circumstances, the F-Secure can deviate from this policy.

22. Deferred tax

EUR 1,000	2025	2024
Deferred tax assets relate to following:		
Intangible assets and property, plant and equipment	1,095	1,162
Provisions and other liabilities	619	178
Tax losses carried forward and unused credits	141	
Other temporary differences	690	640
Total	**2,545**	**1,980**
Offset against deferred tax liabilities	-2,359	-1,921
Net deferred tax assets	**187**	**58**
Change in deferred tax assets:		
Recognized in profit or loss	566	-561
Total, increase (+), decrease (-)	**566**	**-561**

The Group has recognized a total of EUR 141 thousand deferred tax assets related to tax losses carried forward in Spain and Slovakia. The losses arise from non-recurring transactions and timing differences in the tax deductibility of certain expenses. Recognition of the deferred tax assets is based on the Group's assessment that sufficient future taxable profits will be available against which the tax losses can be utilized.

EUR 1,000	2025	2024
Deferred tax liabilities relate to the following:		
Intangible assets and property, plant and equipment	7,570	4,874
Provisions and other liabilities	438	349
Other temporary differences	224	283
Total	**8,232**	**5,506**
Offset against deferred tax assets	-2,359	-1,921
Net deferred tax liabilities	**5,873**	**3,584**
Change in deferred tax liabilities:		
Recognized in profit or loss	2,726	1,783
Total, increase (+), decrease (-)	**2,726**	**1,783**

The main additions to deferred tax liabilities in 2025 relate to tax-deductible amortization of intangible assets, primarily goodwill and other acquisition-related assets, where tax depreciation exceeds book depreciation. Intangible assets and property, plant and equipment at 31 December 2025 includes deferred tax liabilities of EUR 427 thousand (EUR 451 thousand) from the fair value adjustments of the acquired net assets in the mobile consumer security business of Lookout Inc.

23. Other liabilities

EUR 1,000	2025	2024
Non-current liabilities		
Deferred revenue	5,940	6,398
Other non-current liabilities	13	45
Total	**5,953**	**6,443**
Current liabilities		
Deferred revenue	21,068	22,079
Trade payables	2,530	1,545
Provisions	640	1,427
Other liabilities	1,917	2,135
Accrued expenses	10,273	10,462
Income tax liabilities	435	387
Total	**36,863**	**38,035**
Material amounts shown under accrued expenses		
Accrued personnel expenses	5,915	7,937
Other accrued expenses	4,358	2,525
Total	**10,273**	**10,462**

Other liabilities under Current liabilities consist mainly of personnel and VAT related accruals.

Provisions

EUR 1,000	2025	2024
Book value as at 1.1.	1,427	1,739
Increases during the year	640	1,427
Used during the year	-1,427	-1,739
Book value as at 31.12.	**640**	**1,427**

Management has recognized a provision of EUR 425 thousand related to legal expenses and EUR 215 thousand (EUR 1,427 thousand) related to restructuring.

24. Related party disclosures

The Group's related parties include members of the Board, CEO and other members of the Leadership Team, their family members and organizations in which these individuals have direct or indirect control or significant influence.

Compensation of key management personnel of the Group

EUR 1,000	2025	2024
Wages and other short-term employee benefits	2,306	1,897
Pensions	317	211
Total	**2,623**	**2,108**

Wages and other short-term employee benefits

EUR 1,000	2025	2024
CEO and President	472	334
Leadership Team	1,835	1,564
Members of the Boards of Directors	320	267
Total	**2,626**	**2,164**

Board of Directors and CEO and President

EUR 1,000	Wages	Fees
Timo Laaksonen, CEO and President	472	
Pertti Ervi, Chair of the Board		90
Petra Teräsaho		48
Tommi Uitto		38
Roxana Diaconescu		43
Cornelia Schaurecker		43
Alessandro Adriani		43
Thomas Jul		2
Rachit Mittal		13
Total	**472**	**320**

The CEO's retirement age and the determination of his pension conform to the standard rules specified by Finland's Employee Pension Act (TYEL). The pension cost of the CEO during the financial period was EUR 82 thousand (EUR 58 thousand). The period of notice for the CEO is six (6) months both ways and CEO is entitled to severance payment equivalent of six (6) months' salary.

25. Subsidiaries

Name	Country of incorporation	Group (%)
Parent F-Secure Corporation, Helsinki	Finland	
F-Secure Data Oy, Helsinki	Finland	100
F-Secure Data Oy, Norwegian branch	Norway	100
F-Secure Data Oy, Danish branch	Denmark	100
F-Secure Inc., Palo Alto	United States	100
F-Secure (UK) Ltd, Buckinghamshire	United Kingdom	100
F-Secure KK, Tokyo	Japan	100
F-Secure GmbH, Munich	Germany	100
F-Secure SAS, Paris	France	100
F-Secure AB, Stockholm	Sweden	100
F-Secure Srl in liquidation, Milan	Italy	100
F-Secure Poland SP z.o.o., Poznan	Poland	100
F-Secure Sdn Bhd, Kuala Lumpur	Malaysia	100
F-Secure Pvt Ltd, Mumbai	India	100
F-Secure B.V., Hilversum	The Netherlands	100
F-Secure Iberia SL, Madrid	Spain	100
F-Secure s.r.o., Bratislava	Slovakia	100

26. Subsequent events

After the review period, on 13 January 2026, company announced the appointment of a new Chief Strategy Officer (CSO). F-Secure's SVP, Corporate Development and a member of the Leadership Team, **Antero Norkio**, will leave the Company on 30 January 2026. **Jyrki Tulokas** was appointed CSO and a member of the Leadership Team of F-Secure Corporation, effective 2 February 2026.

On 4 February 2026, F-Secure Board's Personnel and Nomination Committee gave proposals to the Annual General Meeting scheduled for 25 March 2026 for the composition and remuneration of the Board of Directors. The Board's Personnel and Nomination Committee proposes to that the Board of Directors consists of a total of seven (7) members and that the following persons be elected as members of the Board of Directors for a term expiring at the end of the Annual General Meeting 2027: Alessandro Adriani, Roxana Diaconescu, Pertti Ervi, Cornelia Schaurecker, Petra Teräsaho, Tommi Uitto are proposed to be re-elected as members. As F-Secure personnel member to-be-elected, the Personnel and Nomination Committee proposes Wilhelm Lamptey.

The Personnel and Nomination Committee proposes to the Annual General Meeting that the following annual remuneration be paid to the members of Board of Directors to be elected at the Annual General Meeting: EUR 80,000 annually for the Chair of the Board of Directors; EUR 38,000 annually for the external members of the Board of Directors; EUR 12,667 for members employed by F-Secure; EUR 10,000 additional remuneration for the Audit Committee Chair; EUR 4,000 additional remuneration for the Personnel and Nomination Committee Chair; EUR 2,000 additional remuneration for the members of Audit Committee as well as Personnel and Nomination Committee. The proposed annual fee and the fees for Committee work correspond to the current remuneration. In addition, The Personnel and Nomination Committee proposes that approximately 40 percent of the remuneration be paid as shares in the company repurchased from the market or as treasury shares held by the company.

F-Secure Corporation financial statements

Income statement

EUR 1,000	Note	FAS 2025	FAS 2024
Revenue	(1)	124,132	125,913
Cost of revenue		-20,559	-18,996
Gross Margin		**103,573**	**106,917**
Other operating income	(2)	2,042	2,181
Sales and marketing	(3,4)	-32,289	-30,604
Research and development	(3,4)	-24,781	-26,917
Administration	(3,4)	-25,353	-25,406
EBIT		**23,192**	**26,170**
Financial income and expenses	(6)	-3,816	-4,417
PROFIT (LOSS) BEFORE APPROPRIATIONS AND TAXES		**19,375**	**21,754**
Appropriations	(7)	-6,231	-2,726
Income taxes	(8)	-1,659	-2,488
RESULT FOR THE FINANCIAL YEAR		**11,484**	**16,539**

Balance sheet

EUR 1,000	Note	FAS 2025	FAS 2024
ASSETS			
Non-current assets			
Intangible assets	(9)	144,176	151,788
Tangible assets	(9)	704	36
Investments in group companies	(10)	59,601	63,831
Other financial assets	(12)	4,026	36
Total non-current assets		**208,506**	**215,692**
Current assets			
Inventories	(11)	20	29
Trade and other receivables	(12)	27,424	29,493
Cash and bank accounts	(13)	8,689	5,395
Total current assets		**36,133**	**34,917**
TOTAL ASSETS		**244,639**	**250,609**

EUR 1,000	Note	FAS 2025	FAS 2024
EQUITY AND LIABILITIES			
Shareholder's equity	(14,15)		
Share capital		80	80
Reserve for invested unrestricted equity		9,590	9,590
Retained earnings		9,949	397
Profit for the financial year		11,484	16,539
Total shareholders' equity		**31,104**	**26,607**
Appropriations			
Depreciation difference		16,524	10,293
Non-current liabilities	(17)		
Interest bearing liabilities, non-current		122,521	132,811
Other non-current liabilities		4,301	4,952
Total non-current liabilities		**126,822**	**137,763**
Current liabilities	(17)		
Interest bearing liabilities, current		30,000	38,000
Trade and other payables		20,708	17,837
Other current liabilities		19,481	20,110
Total current liabilities		**70,190**	**75,947**
TOTAL SHAREHOLDERS' EQUITY AND LIABILITIES		**244,639**	**250,609**

Cash flow statement

EUR 1,000	FAS 2025	FAS 2024
Cash flow from operations		
Result for the financial year	11,484	16,539
Adjustments		
Depreciation and amortization	19,452	16,854
Provisions		-200
Change in depreciation difference	6,231	2,726
Other adjustments	568	-105
Financial income and expenses	3,816	4,417
Income taxes	1,659	2,488
Cash flow from operations before change in working capital	**43,212**	**42,719**
Current receivables, increase (-), decrease (+)	1,688	1,727
Inventories, increase (-), decrease (+)	10	6
Non-interest bearing debt, increase (+), decrease (-)	738	-1,588
Cash flow from operations before financial items and taxes	**45,647**	**42,864**
Interest expenses paid	-6,838	-10,657
Interest income received	356	442
Other financial income and expenses	-879	-437
Income taxes paid	-1,565	-1,991
Cash flow from operations	**36,721**	**30,221**

EUR 1,000	FAS 2025	FAS 2024
Cash flow from investments		
Investments in intangible and tangible assets	-12,507	-12,733
Acquisition of subsidiaries		-456
Intercompany loans granted	-3,640	
Other received distribution of assets from subsidiaries	4,230	3,446
Dividends received	3,529	6,169
Cash flow from investments	**-8,387**	**-3,574**
Cash flow from financing activities		
Increase in interest-bearing liabilities	35,000	8,000
Decrease in interest-bearing liabilities	-53,000	-30,000
Dividends paid	-6,987	-12,227
Cash flow from financing activities	**-24,987**	**-34,227**
Change in cash	3,347	-7,579
Effect of exchange rate changes on cash	-53	40
Cash and bank at the beginning of the period	5,395	12,935
Cash and bank at period end	**8,689**	**5,395**

Notes to the parent company Financial Statements

Basic information

F-Secure is a cybersecurity company who designs and offers security and privacy products and services to consumers to protect themselves against online threats.

F-Secure Corporation is the parent company of F-Secure Group, incorporated in Finland and domiciled in Helsinki. F-Secure Corporation was established through partial demerger on 30 June 2022. In the demerger F-Secure Corporation received assets and liabilities from WithSecure Corporation on 30 June 2022. Assets and liabilities were transferrwww.f-secure.comed with book values, and the transferred net equity was 9,670 thousand euro. Demerger plan, dated 17 February 2022, defines further which assets and liabilities were transferred. Company's registered address is Tammasaarenkatu 7, 00180 Helsinki. Copy of consolidated financial statements can be downloaded from www.f-secure.com.

Accounting principles

The financial statement of F-Secure Corporation has been prepared in accordance with Finnish Accounting Standards (FAS).

Foreign currency translation

Foreign currency transactions are translated using the exchange rates prevailing at the dates of the transactions. On the reporting date, assets and liabilities denominated in foreign currencies are translated using the European Central Bank's exchange rates prevailing at that date. Exchange rate gains and losses are recognized in financial items in the income statement.

Revenue recognition

F-Secure provides a comprehensive range of cybersecurity products and services related to endpoint protection, privacy protection, digital identity protection and security for all consumers' connected devices at home. Revenue derives from the sale of security products and services through partner and direct (ecommerce) channels. Majority of revenue comes from the sale of cybersecurity products through the partner channel. F-Secure also sells consumer products through various retail partners, as well as F-Secure's own web shop. Partner channel sells Security Suite and Embedded Security products whereas direct channel sells Security Suite products.

F-Secure's cybersecurity products are sold as Security-as-a-Service. Customers are granted access to use the intellectual property during the license period and they are provided with access to continuously updated software. All software and the accompanied services F-Secure provides are highly interdependent and therefore treated as one performance obligation for which revenue is recognized over time on a straight-line basis for license period despite the sales channel.

Partner channel customers can have different invoicing depending on the customer agreement. Majority of the agreements are licenses fees – either Security Suite or Embedded Security – which are provided as a continuous service, when they are invoiced and revenue is recognized each month. Some agreements are for a fixed term. These agreements are invoiced upfront (e.g., annually), and the revenue is recognized over the contract period. Non-recurring revenue, which e.g. relates to custom built integration, is usually invoiced in the beginning of the agreement period and revenue is recognized over time on a straight-line basis for the contract period.

Direct channel selling Security Suite products is usually invoiced fully upfront for the license period and the revenue is recognized over time on a straight-line basis for the license period. The typical length of a license period is 12, 24, or 36 months.

Generally, the term between invoicing and when payment is due is not significant.

Pensions

F-Secure's pension arrangements are defined contribution plans in accordance with local statutory requirements. Contributions to defined contribution plans are recognized in income statement in the period to which the contributions relate. The company recognizes the disability commitment of TyEL pension plan when disability appears.

Income taxes

Current income taxes are calculated in accordance with the local tax and accounting rules.

Tangible and intangible assets

Intangible assets include intangible rights and software licenses. Tangible and intangible assets are recorded at historical cost less accumulated depreciation, amortization, and possible impairment. Depreciation and amortization is recorded on a straight-line basis over the estimated useful life of

an asset. The estimated useful lives of tangible and intangible assets are as follows:

Machinery and equipment	2–5 years
Capitalized development costs	3–5 years
Intangible rights	3–5 years
Intangible assets	5–15 years
Goodwill	10 years

Ordinary repairs and maintenance costs are charged to the income statement during the financial period in which they are incurred. The cost of major renovations is included in the assets' carrying amount when it is probable that the Company will derive future economic benefits in excess of the originally assessed standard or performance of the existing asset. Any gain or loss arising on derecognition of the asset (calculated as the difference between the net disposal proceeds and the carrying amount of the asset) is included in the income statement in the year the asset is derecognized.

Subsidiary shares

Subsidiary shares in the balance sheet are measured at historical cost less impairment losses. The carrying amounts of the subsidiary shares are assessed annually as part of the Group's impairment testing. An impairment loss is recognised, if the carrying amount of the subsidiary shares and the amount of net loan receivables from the subsidiary exceed the recoverable amount of the corresponding assets and the impairment is considered permanent.

Research and development expenditure

Research expenditure is recognized as an expense at the time it is incurred. Development expenditures relate to new products or development of significant new features including new product versions.

Inventories

Inventories are measured at probable replacement cost. Cost is determined by first-in first-out method. Net realizable value is the estimated selling price that is obtainable, less estimated costs of completion and the estimated costs necessary to make the sale.

Financial assets and liabilities

Cash and cash equivalents and trade receivables are considered as financial assets. Cash and cash equivalents in the balance sheet comprise cash at bank, deposits held at banks, and other highly liquid short-term investment with original maturity less than 3 months.

F-Secure classifies bank loans, trade payables and other payables as other financial liabilities which are measured at amortized cost. Financial liabilities are classified as current unless F-Secure has unconditional right to postpone their repayment by at least 12 months from the end date of the reporting period.

Presentation of expenses

Classification of the functionally presented expenses has been made by presenting direct expenses in their respective functions.

1. Revenue

EUR 1,000	2025	2024
Geographical information		
Nordic countries	44,556	41,682
Rest of Europe	44,713	46,905
North America	26,324	29,278
Rest of the world	8,539	8,049
Total	**124,132**	**125,913**

2. Other operating income

EUR 1,000	2025	2024
Government grants	748	221
Transition services	11	515
Intercompany	1,272	1,437
Other	12	9
Total	**2,042**	**2,181**

Government grants are recognized as income over those periods in which the corresponding expenses arise.

3. Depreciation and amortization

EUR 1,000	2025	2024
Depreciation and amortization of non-current assets		
Other intangible assets	8,662	8,091
Goodwill	6,079	6,079
Capitalized development	4,598	2,650
Intangible assets	**19,339**	**16,821**
Machinery and equipment	113	33
Tangible assets	**113**	**33**
Total depreciation and amortization	**19,452**	**16,854**
Depreciation and amortization by function		
Sales and marketing	132	53
Research and development	6,150	3,726
Administration	13,170	13,075
Total depreciation and amortization	**19,452**	**16,854**

Amortization of goodwill and most of amortization of other intangible assets relate to acquisition of mobile consumer security business from Lookout Inc in 2023.

4. Personnel expenses

EUR 1,000	2025	2024
Personnel expenses		
Wages and salaries	14,571	16,011
Pension expenses	3,722	3,803
Other social expenses	535	524
Total	**18,828**	**20,337**

EUR 1,000	2025	2024
Compensation of key management personnel		
Wages and other short-term employee benefits	1,886	1,405
Total	**1,886**	**1,405**

EUR 1,000	2025	2024
Wages and other short-term employee benefits		
CEO and President	472	334
Members of the Board of Directors	320	267

Wages and other short-term employee benefits of the Board of Directors and CEO and President: see group Note 24. Related party disclosures.

The CEO's retirement age and the determination of his pension conform to the standard rules specified by Finland's Employee Pension Act (TYEL). The pension cost of the CEO during the financial period was 82 thousand euro (58 thousand euro). The period of notice for the CEO is six (6) months both ways and CEO is entitled to severance payment equivalent of six (6) months' salary.

	2025	2024
Average number of personnel	262	273
Personnel by function 31 Dec		
Sales and marketing	60	68
Research and development	166	165
Administration	38	35
Total	**264**	**268**

5. Audit fees

EUR 1,000	2025	2024
Audit fees, PricewaterhouseCoopers	145	148
Audit related fees, PricewaterhouseCoopers		21
Tax consulting, PricewaterhouseCoopers		11
Other services, PricewaterhouseCoopers	117	126
Total	**262**	**306**

Other services include, among others CSRD assurance.

6. Financial income and expenses

EUR 1,000	2025	2024
Interest income	356	442
Interest expense	-6,838	-10,657
Dividends	3,529	6,169
Exchange gains and losses	-340	73
Other financial expenses	-523	-443
Total	**-3,816**	**-4,417**

7. Appropriations

EUR 1,000	2025	2024
Change in depreciation difference	-6,231	-2,726
Total	**-6,231**	**-2,726**

8. Income taxes

EUR 1,000	2025	2024
Income tax for the year	-1,659	-2,488
Total	**-1,659**	**-2,488**
Result before appropriations and tax	**19,375**	**21,754**

9. Non-current assets

	Intangible assets						Tangible assets		
EUR 1,000	Other intangible	Goodwill	Capitalized development	Incomplete development	Advance payments	Total	Machinery & equip.	Other tangible	Total
Acquisition cost Dec 31, 2023	89,570	60,791	9,079		6152	165,592	76	50	126
Additions	1,725			9,173	1813	12,710	20	2	22
Transfers	7,237		8,425	-8,425	-7,237				
Acquisition cost Dec 31, 2024	98,533	60,791	17,504	747	728	178,302	96	52	148
Additions				7,618	4,089	11,707	671	128	800
Transfers	3,542		3,735	-3,735	-3,542				
Acquisition cost Dec 31, 2025	**102,074**	**60,791**	**21,240**	**4,630**	**1,276**	**190,010**	**768**	**180**	**948**
Acc. depreciation Dec 31, 2023	-3,395	-3,546	-2,773			-9,715	-32	-26	-58
Depreciation for the period	-8,070	-6,079	-2,650			-16,800	-33	-21	-54
Acc. depreciation Dec 31, 2024	-11,466	-9,625	-5,424	-	-	-26,515	-65	-47	-112
Depreciation for the period	-8,643	-6,079	-4,598			-19,320	-113	-19	-132
Acc. depreciation Dec 30, 2025	**-20,109**	**-15,704**	**-10,021**	-	-	**-45,834**	**-177**	**-66**	**-244**
Book value as at Dec 31, 2024	87,067	51,165	12,080	747	728	151,788	32	4	36
Book value as at Dec 31, 2025	**81,966**	**45,086**	**11,218**	**4,630**	**1,276**	**144,175**	**590**	**114**	**704**

Goodwill and most of other intangible assets additions relate to acquisition of mobile consumer security business from Lookout Inc in 2023.

10. Investments in group companies

EUR 1,000	Shares in group companies	Total
Book value as at 1 Jan	63,831	63,831
Decreases	-4,230	-4,230
Book value as at 31 Dec	**59,601**	**59,601**

Name	Country of incorporation	Share of ownership (%)
Parent F-Secure Corporation, Helsinki	Finland	100
F-Secure Data Oy, Helsinki	Finland	100
F-Secure Inc., Palo Alto	United States	100
F-Secure (UK) Ltd, Buckinghamshire	United Kingdom	100
F-Secure GmbH, Munich	Germany	100
F-Secure Pvt Ltd, Mumbai	India	100
F-Secure Iberia SL, Barcelona	Spain	100
F-Secure s.r.o, Bratislava	Slovakia	100

11. Inventories

EUR 1,000	2025	2024
Other inventories	20	29

12. Receivables

EUR 1,000	2025	2024
Non-Current receivables		
Loan receivable from group companies	3,640	
Other financial assets	386	36
Total	**4,026**	**36**
Current receivables		
Trade receivables	17,393	17,515
Income tax receivable	583	677
Other receivables	435	1,156
Prepaid expenses	6,463	7,662
Accrued income	1,271	1,359
Total	**26,144**	**28,369**
Receivables from group companies		
Trade receivables	587	779
Other receivables	694	345
Total	**1,281**	**1,124**
Current receivables total	**27,424**	**29,493**

F-Secure Corporation has loan receivables from group companies totaling EUR 3 640 thousand. The loans are unsecured, mature in 2030, and have been provided on market terms.

Other short-term receivables from group companies arise from the normal course of business and contain no special terms.

Material items included in prepaid expenses		
Prepaid software subscriptions	1,931	1,659
Deferred sales commissions	1,698	2,215
Prepaid and accrued royalty	1,742	2,440
Grant receivables	563	192
Other prepaid expenses	278	711
Merchandise cost	251	444
Total	**6,463**	**7,662**

13. Cash and short-term deposits

EUR 1,000	2025	2024
Cash at bank and in hand	8,689	5,395

14. Statement of changes in shareholders' equity

EUR 1,000	Share capital	Unrestricted equity reserve	Retained Earnings	Total Equity
Equity 31 December 2023	**80**	**9,590**	**12,624**	**22,294**
Result of the financial year			16,539	16,539
Dividends paid			-12,227	-12,227
Equity 31 December 2024	**80**	**9,590**	**16,936**	**26,607**
Result of the financial year			11,484	11,484
Dividends paid			-6,987	-6,987
Equity 31 December 2025	**80**	**9,590**	**21,434**	**31,104**

15. Shareholders' equity

Issued and fully paid

EUR 1,000	Number of shares	Share capital	Unrestricted equity reserve
1 January 2025	174,673,165	80	9,590
Issued 2025	33,905		
31 December 2025	**174,707,070**	**80**	**9,590**

The share capital amounting to 80,000 euro was formed in the demerger on 30 June 2022. The number of shares was 174,707,070 (no own shares) at the end of 2025.

Company has made a directed share issue in September 2025 to the plan participants of the Company's Employee share savings plan. The shares issued account for the rewards earned from the period 2022-2025.

A share has no nominal value. Accountable par value is EUR 0.01.

Distributable shareholders' equity on 31 December 2025

EUR 1,000	
Unrestricted equity reserve	9,590
Retained earnings	9,949
Result of the financial year	11,484
Less capitalized development expense	-15,848
Distributable shareholders' equity on 31 December 2025	**15,176**

16. Share-based payment transactions

See group Note 19. Share-based payment transactions.

17. Liabilities

EUR 1,000	2025	2024
Non-current liabilities		
Deferred revenue	4,301	4,952
Bank loans	122,000	132,000
Total	**126,301**	**136,952**
Liabilities to the group companies		
Cash pool	521	811
Total	**521**	**811**
Total non-current liabilities	**126,822**	**137,763**
Current liabilities		
Deferred revenue	18,724	18,617
Trade payables	2,179	1,512
Bank loans	30,000	38,000
Other liabilities	924	929
Accrued expenses	8,223	9,613
Total	**60,051**	**68,671**
Liabilities to the group companies		
Trade payables	5,726	2,189
Other liabilities	4,413	5,087
Total	**10,138**	**7,276**
Total current liabilities	**70,190**	**75,947**

EUR 1,000	2025	2024
Material amounts shown under accruals and deferred income		
Accrued personnel expenses	4,356	5,826
Restructuring	179	685
Accrued expenses	3,688	3,102
Total	**8,223**	**9,613**

18. Financial risk management

See group Note 21. Financial risk management.

19. Operating lease commitments

The Group has commercial leases on office space, office equipment and on motor vehicles. Leases have an average life of two to four years with renewal terms included in the contracts.

Future minimum rentals payable under non-cancellable operating leases as at 31 December are as follows:

EUR 1,000	2025	2024
As lessee		
Within one year	1,339	940
After one year but not more than five years	3,030	5,042
Total	**4,369**	**5,982**

Signatures of the Board of Directors' report and Financial statements

The financial statements, prepared in accordance with the applicable accounting regulations, give a true and fair view of both the company and the group of companies included in its consolidated financial statements, in terms of assets, liabilities, financial position, and profit and loss.

The management report provides an accurate description of the development and results of the company's operations on one hand, and the business development and results of the group of companies included in the consolidated financial statements on the other. It also includes a description of significant risks, uncertainties, and other aspects of the company's state. Additionally, the sustainability report included in the management report has been prepared in accordance with the reporting standards referred to in Chapter 7 and Article 8 of the Taxonomy Regulation.

Helsinki, 25 February 2026

Pertti Ervi
Chair

Petra Teräsaho

Tommi Uitto

Alessandro Adriani

Roxana Diaconescu

Cornelia Schaurecker

Rachit Mittal

TImo Laaksonen
CEO and President

F-Secure

The auditor's note

A report on the audit performed has been issued today.

Helsinki, 25 February 2026

PricewaterhouseCoopers Oy
Authorized Public Accountants

Samuli Perälä
Authorized Public Accountant (KHT)

Information for shareholders

Contact information:

Sari Somerkallio, Chief Financial Officer

investor.relations@f-secure.com
+358 40 356 9251

Financial calendar

During the year 2026, F-Secure Corporation will publish financial information as follows:

- Interim Report for January–March 2026 on Wednesday 29 April 2026
- Half-year Financial Report for January–June 2026 on Friday 17 July 2026
- Interim Report for January–September 2026 on Wednesday 28 October 2026.

Annual General Meeting 2026

The Annual General Meeting 2026 is scheduled for Wednesday 25 March 2026.

Auditor's report

(Translation of the Finnish Original)

To the Annual General Meeting of F-Secure Corporation

Report on the Audit of the Financial Statements

Opinion

In our opinion

- the consolidated financial statements give a true and fair view of the group's financial position, financial performance and cash flows in accordance with IFRS Accounting Standards as adopted by the EU
- the financial statements give a true and fair view of the parent company's financial performance and financial position in accordance with the laws and regulations governing the preparation of financial statements in Finland and comply with statutory requirements.

Our opinion is consistent with the additional report to the Audit Committee.

What we have audited

We have audited the financial statements of F-Secure Corporation (business identity code 3269349-7) for the year ended 31 December 2025. The financial statements comprise:

- the consolidated balance sheet, statement of comprehensive income, statement of changes in equity, statement of cash flows and notes, which include material accounting policy information and other explanatory information
- the parent company's balance sheet, income statement, cash flow statement and notes.

Basis for Opinion

We conducted our audit in accordance with good auditing practice in Finland. Our responsibilities under good auditing practice are further described in the Auditor's Responsibilities for the Audit of the Financial Statements section of our report.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Independence

We are independent of the parent company and of the group companies in accordance with the ethical requirements that are applicable in Finland and are relevant to our audit, and we have fulfilled our other ethical responsibilities in accordance with these requirements.

To the best of our knowledge and belief, the non-audit services that we have provided to the parent company and group companies are in accordance with the applicable law and regulations in Finland and we have not provided non-audit services that are prohibited under Article 5(1) of Regulation (EU) No 537/2014. The non-audit services that we have provided are disclosed in note 8 to the Financial Statements.

Our Audit Approach

Overview

- Overall group materiality: 1.45 million euros.
- The audit of the consolidated financial statements covered the parent company and one subsidiary.
- Valuation of goodwill and intangible assets acquired in connection with the business combination
- Revenue recognition

As part of designing our audit, we determined materiality and assessed the risks of material misstatement in the financial statements. In particular, we considered where management made subjective judgements; for example, in respect of significant accounting estimates that involved making assumptions and considering future events that are inherently uncertain.

Materiality

The scope of our audit was influenced by our application of materiality. An audit is designed to obtain reasonable assurance whether the financial statements are free from material misstatement. Misstatements may arise due to fraud or error. They are considered material if individually or in aggregate, they could reasonably be expected to influence the economic decisions of users taken on the basis of the financial statements.

Based on our professional judgement, we determined certain quantitative thresholds for materiality, including the overall group materiality for the consolidated financial statements as set out in the table below. These, together with qualitative considerations, helped us to determine the scope of our audit and the nature, timing and extent of our audit procedures and to evaluate the effect of misstatements on the financial statements as a whole.

Overall group materiality	1.45 million euros
How we determined it	The materiality of the consolidated financial statements has been determined based on the profit before tax for the financial year.
Rationale for the materiality benchmark applied	We chose profit before tax as the benchmark because, in our view, it is relevant benchmark to describe the volume and profitability of the Group's operations.

How we tailored our group audit scope

We tailored the scope of our audit, taking into account the structure of the F-Secure Group, the accounting processes and controls, and the industry in which the group operates.

The audit of the consolidated financial statements covered the parent company and one subsidiary. In our view, we have determined the scope of the audit of the consolidated financial statements to cover the consolidated financial statements to a sufficient extent.

Key Audit Matters

Key audit matters are those matters that, in our professional judgment, were of most significance in our audit of the financial statements of the current period. These matters were addressed in the context of our audit of the financial statements as a whole, and in forming our opinion thereon, and we do not provide a separate opinion on these matters.

As in all of our audits, we also addressed the risk of management override of internal controls, including among other matters consideration of whether there was evidence of bias that represented a risk of material misstatement due to fraud.

Key audit matter in the audit of the group	How our audit addressed the key audit matter
Valuation of goodwill and intangible assets acquired in connection with the business combination *Relevant information is presented in notes 1, 12 and 13*	
The consolidated balance sheet had a total of 87.0 million euros in goodwill as of December 31, 2025 . Goodwill is not amortised but is tested annually, or more frequently if there are indications that its value might be impaired. Other intangible assets acquired in business combinations are recorded at fair value at the time of acquisition and expensed through amortisation over their economic useful life. For impairment testing, goodwill is allocated to a single cash-generating unit. In the impairment test, the recoverable amount of the cash-generating unit is determined based on the present value of estimated future cash flows. Management's estimates are used to determine the present value of the forecasted cash flows. Due to the management judgment involved in valuation and the materiality of the balance sheet value, the valuation of goodwill and intangible assets acquired in connection with business combinations is a key audit matter.	Our audit procedures included, among others, the following actions: • We obtained an understanding of the methods and assumptions used in the impairment testing of goodwill, • We assessed the reasonableness and consistency of the forecasted profitability levels against approved budgets and forecasts, • We tested the mathematical accuracy of the calculations, • We evaluated the discount rates used, long-term growth forecasts, and certain other assumptions, for example, by comparing these input data to observable market information, • We assessed the adequacy of the information provided in the financial statements.

Key audit matter in the audit of the group	How our audit addressed the key audit matter
Revenue recognition *Relevant information is presented in notes 1 and 3*	
The majority of F-Secure's revenue is generated from the sale of endpoint security solutions through the partner channel, but the group also sells consumer products through resellers and F-Secure's own online store. Customers are typically granted a license to use the software for a license period and are provided access to continuously updated software. The software and accompanying services are closely related, and therefore they are treated as a single performance obligation, with revenue being recognized primarily evenly over the license period as time passes. Revenue recognition has been considered a key audit matter due to the large number of transactions and the fact that revenue is a critical measure of the company's financial performance.	Our audit procedures have included, among others, the following actions: • We assessed the adequacy of controls related to the revenue process, • We tested, on sample basis, the revenue recorded during the financial year, • We tested, on sample basis, trade receivables, • We checked the appropriateness of the of received advances on sample basis, • We examined a sample of the revenue recognition of fixed-price contracts.

We have no key audit matters to report with respect to our audit of the parent company financial statements.

There are no significant risks of material misstatement referred to in Article 10(2c) of Regulation (EU) No 537/2014 with respect to the consolidated financial statements or the parent company financial statements.

Responsibilities of the Board of Directors and the Managing Director for the Financial Statements

The Board of Directors and the Managing Director are responsible for the preparation of consolidated financial statements that give a true and fair view in accordance with IFRS Accounting Standards as adopted by the EU, and of financial statements that give a true and fair view in accordance with the laws and regulations governing the preparation of financial statements in Finland and comply with statutory requirements. The Board of Directors and the Managing Director are also responsible for such internal control as they determine is necessary to enable the preparation of financial statements that are free from material misstatement, whether due to fraud or error.

In preparing the financial statements, the Board of Directors and the Managing Director are responsible for assessing the parent company's and the group's ability to continue as a going concern, disclosing, as applicable, matters relating to going concern and using the going concern basis of accounting. The financial statements are prepared using the going concern basis of accounting unless there is an intention to liquidate the parent company or the group or to cease operations, or there is no realistic alternative but to do so.

Auditor's Responsibilities for the Audit of the Financial Statements

Our objectives are to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes our opinion. Reasonable assurance is a high level of assurance, but is not a guarantee that an audit conducted in accordance with good auditing practice will always detect a material misstatement when it exists. Misstatements can arise from fraud or error and are considered material if, individually or in the aggregate, they could reasonably be expected to influence the economic decisions of users taken on the basis of these financial statements.

As part of an audit in accordance with good auditing practice, we exercise professional judgment and maintain professional skepticism throughout the audit. We also:

- Identify and assess the risks of material misstatement of the financial statements, whether due to fraud or error, design and perform audit procedures responsive to those risks, and obtain audit evidence that is sufficient and appropriate to provide a basis for our opinion. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control.
- Obtain an understanding of internal control relevant to the audit in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the parent company's or the group's internal control.
- Evaluate the appropriateness of accounting policies used and the reasonableness of accounting estimates and related disclosures made by management.
- Conclude on the appropriateness of the Board of Directors' and the Managing Director's use of the going concern basis of accounting and based on the audit evidence obtained, whether a material uncertainty exists related to events or conditions that may cast significant doubt on the parent company's or the group's ability to continue as a going concern. If we conclude that a material uncertainty exists, we are required to draw attention in our auditor's report to the related disclosures in the financial statements or, if such disclosures are inadequate, to modify our opinion. Our conclusions are based on the audit evidence obtained up to the date of our auditor's report. However, future events or conditions may cause the parent company or the group to cease to continue as a going concern.
- Evaluate the overall presentation, structure and content of the financial statements, including the disclosures, and whether the financial statements represent the underlying transactions and events so that the financial statements give a true and fair view.
- Plan and perform the group audit to obtain sufficient appropriate audit evidence regarding the financial information of the entities or business units within the group as a basis for forming an opinion on the group financial statements. We are responsible for the direction, supervision and review of the audit work performed for purposes of the group audit. We remain solely responsible for our audit opinion.

We communicate with those charged with governance regarding, among other matters, the planned scope and timing of the audit and significant audit findings, including any significant deficiencies in internal control that we identify during our audit.

We also provide those charged with governance with a statement that we have complied with relevant ethical requirements regarding independence, and communicate with them all relationships and other matters that may

reasonably be thought to bear on our independence, and where applicable, related safeguards.

From the matters communicated with those charged with governance, we determine those matters that were of most significance in the audit of the financial statements of the current period and are therefore the key audit matters. We describe these matters in our auditor's report unless law or regulation precludes public disclosure about the matter or when, in extremely rare circumstances, we determine that a matter should not be communicated in our report because the adverse consequences of doing so would reasonably be expected to outweigh the public interest benefits of such communication.

Other Reporting Requirements

Appointment

We were first appointed as auditors by the annual general meeting on 31 May 2022. Our appointment represents a total period of uninterrupted engagement of 3 years.

Other Information

The Board of Directors and the Managing Director are responsible for the other information. The other information comprises the report of the Board of Directors and the information included in the Annual Report but does not include the financial statements and our auditor's report thereon.

Our opinion on the financial statements does not cover the other information.

In connection with our audit of the financial statements, our responsibility is to read the other information and, in doing so, consider whether the other information is materially inconsistent with the financial statements or our knowledge obtained in the audit, or otherwise appears to be materially misstated. With respect to the report of the Board of Directors, our responsibility also includes considering whether the report of the Board of Directors has been prepared in compliance with the applicable provisions, excluding the sustainability report information on which there are provisions in Chapter 7 of the Accounting Act and in the sustainability reporting standards.

In our opinion, the information in the report of the Board of Directors is consistent with the information in the financial statements and the report of the Board of Directors has been prepared in compliance with the applicable provisions.

Our opinion does not cover the sustainability report information on which there are provisions in Chapter 7 of the Accounting Act and in the sustainability reporting standards.

If, based on the work we have performed, we conclude that there is a material misstatement of the other information, we are required to report that fact. We have nothing to report in this regard.

Helsinki 25 February 2026

PricewaterhouseCoopers Oy

Authorized Public Accountants

Samuli Perälä

Authorised Public Accountant (KHT)

Assurance Report on the Sustainability Report

(Translation of the Finnish Original)

To the Annual General Meeting of F-Secure Oyj

We have performed a limited assurance engagement on the group sustainability report of F-Secure Oyj (business identity code 3269349-7) that is referred to in Chapter 7 of the Accounting Act and that is included in the report of the Board of Directors for the reporting period 1.1.–31.12.2025.

Opinion

Based on the procedures we have performed and the evidence we have obtained, nothing has come to our attention that causes us to believe that the group sustainability report does not comply, in all material respects, with

1) the requirements laid down in Chapter 7 of the Accounting Act and the sustainability reporting standards (ESRS), and

2) the requirements laid down in Article 8 of the Regulation (EU) 2020/852 of the European Parliament and of the Council on the establishment of a framework to facilitate sustainable investment, and amending Regulation (EU) 2019/2088 (EU Taxonomy).

Point 1 above also contains the process in which F-Secure Oyj has identified the information for reporting in accordance with the sustainability reporting standards (double materiality assessment).

Our opinion does not cover the tagging of the group sustainability report with digital XBRL sustainability tags in accordance with Chapter 7, Section 22, Subsection 1(2), of the Accounting Act, because sustainability reporting companies have not had the possibility to comply with that requirement in the absence of requirements for the tagging of sustainability information in the ESEF regulation or other European Union legislation.

Basis for Opinion

We performed the assurance of the group sustainability report as a limited assurance engagement in compliance with good assurance practice in Finland and with the International Standard on Assurance Engagements (ISAE) 3000 (Revised) Assurance Engagements Other than Audits or Reviews of Historical Financial Information.

Our responsibilities under this standard are further described in the Responsibilities of the Authorised Group Sustainability Auditor section of our report.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Authorised Group Sustainability Auditor's Independence and Quality Management

We are independent of the parent company and of the group companies in accordance with the ethical requirements that are applicable in Finland and are relevant to our engagement, and we have fulfilled our other ethical responsibilities in accordance with these requirements.

The authorised group sustainability auditor applies International Standard on Quality Management ISQM 1, which requires the authorised sustainability audit firm to design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Responsibilities of the Board of Directors and the Managing Director

The Board of Directors and the Managing Director of F-Secure Oyj are responsible for:

- the group sustainability report and for its preparation and presentation in accordance with the provisions of Chapter 7 of the Accounting Act, including the process that has been defined in the sustainability reporting standards and

in which the information for reporting in accordance with the sustainability reporting standards has been identified,

- the compliance of the group sustainability report with the requirements laid down in Article 8 of the Regulation (EU) 2020/852 of the European Parliament and of the Council on the establishment of a framework to facilitate sustainable investment, and amending Regulation (EU) 2019/2088, and for
- such internal control as the Board of Directors and the Managing Director determine is necessary to enable the preparation of a group sustainability report that is free from material misstatement, whether due to fraud or error.

Inherent Limitations in the Preparation of a Sustainability Report

In reporting forward-looking information in accordance with ESRS, management of the Company is required to prepare the forward-looking information on the basis of assumptions that have been disclosed in the sustainability report about events that may occur in the future and possible future actions by the Group. Actual outcomes are likely to be different since anticipated events frequently do not occur as expected.

Responsibilities of the Authorised Group Sustainability Auditor

Our responsibility is to perform an assurance engagement to obtain limited assurance about whether the group sustainability report is free from material misstatement, whether due to fraud or error, and to issue a limited assurance report that includes our opinion. Misstatements can arise from fraud or error and are considered material if, individually or in the aggregate, they could reasonably be expected to influence the decisions of users taken on the basis of the group sustainability report.

Compliance with the International Standard on Assurance Engagements (ISAE) 3000 (Revised) requires that we exercise professional judgment and maintain professional skepticism throughout the engagement. We also:

- Identify and assess the risks of material misstatement of the group sustainability report, whether due to fraud or error, and obtain an understanding of internal control relevant to the engagement in order to design assurance procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the parent company's or the group's internal control.
- Design and perform assurance procedures responsive to those risks to obtain evidence that is sufficient and appropriate to provide a basis for our opinion. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control.

Description of the Procedures That Have Been Performed

The procedures performed in a limited assurance engagement vary in nature and timing from, and are less in extent than for, a reasonable assurance engagement. The nature, timing and extent of assurance procedures selected depend on professional judgment, including the assessment of risks of material misstatement, whether due to fraud or error. Consequently, the level of assurance obtained in a limited assurance engagement is substantially lower than the assurance that would have been obtained had a reasonable assurance engagement been performed.

Our procedures included for example the following:

- We interviewed the company's management and the individuals responsible for collecting and reporting the information contained in the group sustainability report at the group level to gain an understanding of the sustainability reporting process and the related internal controls and information systems.
- We familiarised ourselves with the background documentation and records prepared by the company where applicable, and assessed whether they support the information contained in the group sustainability report.
- We assessed the company's double materiality assessment process in relation to the requirements of the ESRS standards, as well as whether the information provided about the assessment process complies with the ESRS standards.
- We assessed whether the sustainability information contained in the group sustainability report complies with the ESRS standards.
- Regarding the EU taxonomy information, we gained an understanding of the process by which the company has identified the group's taxonomy-eligible and taxonomy-aligned economic activities, and we assessed the compliance of the information provided with the regulations.

Helsinki 25 February 2026

PricewaterhouseCoopers Oy

Authorised Sustainability Auditors

Samuli Perälä

Authorised Sustainability Auditor

Independent auditor's report on the ESEF financial statements of F-Secure Oyj

(Translation of the Finnish Original)

To the Management of F-Secure Oyj

We have performed a reasonable assurance engagement on the financial statements 9845006BFDJF0375E466-2025-12-31-fi.xbri of F-Secure Oyj (business identity code 3269349-7) that have been prepared in accordance with the Commission's regulatory technical standard for the financial year 1 January 2025-31 December 2025.

Responsibilities of the Board of Directors and the Managing Director

The Board of Directors and the Managing Director are responsible for the preparation of the company's report of the Board of Directors and financial statements (the ESEF financial statements) in such a way that they comply with the requirements of the Commission's regulatory technical standard. This responsibility includes:

- preparing the ESEF financial statements in XHTML format in accordance with Article 3 of the Commission's regulatory technical standard
- tagging the primary financial statements, notes and company's identification data in the consolidated financial statements that are included in the ESEF financial statements with iXBRL tags in accordance with Article 4 of the Commission's regulatory technical standard and
- ensuring the consistency between the ESEF financial statements and the audited financial statements.

The Board of Directors and the Managing Director are also responsible for such internal control as they determine is necessary to enable the preparation of ESEF financial statements in accordance with the requirements of the Commission's regulatory technical standard.

Auditor's independence and quality management

We are independent of the company in accordance with the ethical requirements that are applicable in Finland and are relevant to the engagement we have performed, and we have fulfilled our other ethical responsibilities in accordance with these requirements.

The auditor applies International Standard on Quality Management (ISQM) 1, which requires the firm to design, implement and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Auditor's responsibilities

Our responsibility is to, in accordance with Chapter 7, Section 8 of the Securities Markets Act, provide assurance on the financial statements that have been prepared in accordance with the Commission's regulatory technical standard. We express an opinion on whether the consolidated financial statements that are included in the ESEF financial statements have been tagged, in all material respects, in accordance with the requirements of Article 4 of the Commission's regulatory technical standard.

Our responsibility is to indicate in our opinion to what extent the assurance has been provided. We conducted a reasonable assurance engagement in accordance with International Standard on Assurance Engagements (ISAE) 3000 (Revised).

The engagement includes procedures to obtain evidence on:

- whether the primary financial statements in the consolidated financial statements that are included in the ESEF financial statements have been tagged, in all material respects, with iXBRL tags in accordance with the requirements of Article 4 of the Commission's regulatory technical standard and

- whether the notes and company's identification data in the consolidated financial statements that are included in the ESEF financial statements have been tagged, in all material respects, with iXBRL tags in accordance with the requirements of Article 4 of the Commission's regulatory technical standard and
- whether there is consistency between the ESEF financial statements and the audited financial statements.

The nature, timing and extent of the selected procedures depend on the auditor's judgment. This includes an assessment of the risk of a material deviation due to fraud or error from the requirements of the Commission's regulatory technical standard.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Opinion

Our opinion pursuant to Chapter 7, Section 8 of the Securities Markets Act is that the primary financial statements, notes and company's identification data in the consolidated financial statements that are included in the ESEF financial statements of F-Secure Oyj 9845006BFDJF0375E466-2025-12-31-fi.zip for the financial year 1 January 2025-31 December 2025 have been tagged, in all material respects, in accordance with the requirements of the Commission's regulatory technical standard.

Our opinion on the audit of the consolidated financial statements of F-Secure Oyj for the financial year 1 January 2025-31 December 2025 has been expressed in our auditor's report dated 25 February 2026. With this report we do not express an opinion on the audit of the consolidated financial statements nor express another assurance conclusion.

Helsinki 25 February 2026

PricewaterhouseCoopers Oy
Authorised Public Accountants

Samuli Perälä

Authorised Public Accountant (KHT)

Corporate Governance

F-Secure Corporate Governance Statement

Corporate Governance at F-Secure

F-Secure corporate governance practices are based on applicable Finnish laws, the rules of Helsinki Stock Exchange (Nasdaq Helsinki Oy) and the regulations and guidelines of Finnish Financial Supervisory Authority as well as with the company's Articles of Association. This corporate governance statement (later simply referred to as 'statement') has been prepared in accordance with the Finnish Corporate Governance Code 2025 (publicly available at http://cgfinland.fi/en/) issued by the Securities Market Association of Finland.

Up-to-date information about F-Secure corporate governance is available on the company's investor website at https://investors.f-secure.com/en. This statement is issued separately from the Board of Directors' report, and is also available on the investor website, as well as is included in the 2025 Annual Report.

Governing bodies

The highest decision-making body in F-Secure is the General Meeting of Shareholders which elects the members of the Board of Directors. The Board of Directors is responsible for the administration of F-Secure Corporation and appropriate organization of its operations. The Board of Directors appoints the CEO. The CEO, assisted by the Leadership Team, is responsible for managing the company's business and implementing its strategic and operational targets.

General Meeting of Shareholders

Under the Finnish Companies Act, shareholders exercise their decision-making power at the General Meeting.

The General Meeting is normally held once a year as an Annual General Meeting (AGM). The AGM decides on matters stipulated by the Articles of Association and the Finnish Companies Act, including:

- adoption of the Financial Statements
- distribution of profit for the year
- discharging the members of the Board of Directors and the President and CEO from liability
- selection of members of the Board
- the decision on the remuneration of the Board members
- approval of the Remuneration Policy and the Remuneration Report
- election of the auditor and sustainability reporting assurance provider and the decision on the auditor's and the sustainability assurance provider's remuneration, and
- other proposals submitted to General Meeting

Each share carries one vote in the General Meeting.

A shareholder may propose items to be included on the agenda provided they are within the authority of the General Meeting, and the Board of Directors has received the request in advance in accordance with the set schedule. The invitation to the AGM is published as a stock exchange release and is made available on the company's website.

2025:

In 2025, the Annual General Meeting of the company was held on 1 April 2025 at the company's headquarters in Helsinki, Finland.

Board of Directors

The Board of Directors is responsible for the administration of F-Secure Corporation and appropriate organization of its operations. The Board's operations, responsibilities and duties are based on the Finnish Companies Act and other applicable legislation and are supplemented by the Board Charter. These cover the following main areas:

- approving the strategy of F-Secure, overseeing its operations and annual budgets
- appointing and dismissing the President and CEO and the Chair of the Board
- approving any major investments, acquisitions, changes in corporate structure or other matters that are significant or far-reaching
- ensuring that the supervision of the company's accounting and financial management is duly organized
- ensuring that internal control and risk management systems are in place
- approving personnel policies and rewards systems
- preparing most matters to be handled at the General Meeting

The Board of Directors meets as frequently as necessary and according to the Board Charter at least five times during its term. The Board of Directors has quorum when more than half of the members are present. An annual self-assessment is carried out by the Board to evaluate its operations. The Board of Directors primarily strives at unanimous decisions. If a decision cannot be made unanimously, the decision will be made by voting and with single majority. If the votes are even, the Chair's vote is decisive.

In accordance with F-Secure's Articles of Association, the Board of Directors comprises three to seven members, who are elected at the Annual General Meeting for a period of office that extends to the end of subsequent AGM. The Board of Directors represents all shareholders.

Diversity is an essential part of F-Secure success. According to Diversity Principles established by the Board of Directors, an optimal mix of diverse backgrounds, expertise and experience strengthens the Board's performance and promotes creation of long-term shareholder value. The Diversity Principles of the Board of Directors aim to strive towards appropriately balanced gender distribution. At the Annual General Meeting in 2025 seven members representing five different nationalities were elected to the Board. The age structure of the Board members is 44–68 years and three Board members are female and four are male, and thus the underrepresented gender comprises 42.9% of all members of the Board. The Board members have international experience in different roles in global companies operating in different businesses and geographical market areas. More information on the educational and professional background of the Board members is available on chapter Board of Directors 31 December 2025 (see pages 186-194) of the Annual Report 2025.

To create openness, one member of the Board of Directors is proposed to be elected from among F-Secure personnel. An election is arranged annually for F-Secure personnel and each permanent F-Secure employee, except the people belonging to the company's Leadership Team, is eligible to stand as a candidate. The representatives of the Board of Directors interview persons who have obtained the highest number of votes in the elections and choose a candidate from amongst them to be proposed for election as a member of the Board by the Annual General Meeting. Rachit Mittal was appointed to the Board of Directors from among the employees in 2025.

As an employee of the company, the Board member elected from among F-Secure personnel does not participate in any matters that relate to, for example, leadership appointment (or dismissal), remuneration or other terms of employment or service, or industrial action, as the Board may handle from time to time. Board member who is appointed to the Board from among the employees serves on the Board for a period of one year, until the end of next year's Annual General Meeting.

The majority of Board members are independent from the company and from its major shareholders. For a detailed description of the members of the Board of Directors and their shareholdings see the end of this statement.

2025:

In 2025, the Board of Directors held 14 meetings, 4 of which were held without convening. Audit Committee convened 5 times. Personnel and Nomination Committee convened 6 times.

Board of Directors and the Committee members' attendance at meetings in 2025

Members	Independence of the company	Independence of major shareholders	Board of Directors (meeting attendance)	Audit Committee (meeting attendance)	Personnel and Nomination Committee (meeting attendance)
Alessandro Adriani	Yes	Yes	Member (9/9)[1]		Member (3/3)
Roxana Diaconescu	Yes	Yes	Member (9/9)[1]		Member (3/3)
Pertti Ervi	Yes	Yes	Chair (14/14)	Member (5/5)	Chair (6/6)
Rachit Mittal	No[2]	Yes	Member (9/9)[3]		
Cornelia Schaurecker	Yes	Yes	Member (9/9)[1]	Member (4/4)	
Petra Teräsaho	Yes	Yes	Member (14/14)	Chair (5/5)	
Thomas Jul	Yes	Yes	Member (5/5)[1]		Member (3/3)
Katja Kuusikumpu	No[2]	Yes	Member (4/5)[3]		
Risto Siilasmaa	Yes	No[4]	Member (5/5)[1]	Member (1/1)	Member (3/3)
Tommi Uitto	Yes	Yes	Member (14/14)		

1) Thomas Jul and Risto Siilasmaa served on the Board until the end of 2025 Annual General Meeting and Alessandro Adriani, Roxana Diaconescu and Cornelia Schaurecker have been serving on the Board since the 2025 Annual General Meeting.

2) Rachit Mittal was elected from among F-Secure personnel, according to the aforedescribed process in 2025. In addition, Katja Kuusikumpu who had been appointed to the Board in 2024 served on the Board until the end of 2025 Annual General Meeting.

3) Excused from one meeting as employee Board member.

4) Risto Siilasmaa is the founder of F-Secure and on 31 December 2025 owned 34.36% of F-Secure shares.

Board Committees

The Board of Directors appoints from among itself the members and the Chairs of the committees. Each committee must have at least three members. The Board of Directors confirms the main duties and operating principles of each committee.

Audit Committee

The Audit Committee functions as a preparatory body, and the matters it addresses are brought to be decided on by the Board of Directors.

The Audit Committee monitors and evaluates risk management, internal controls, IT strategy and practices, financial and sustainability reporting as well as auditing and sustainability auditing. The Audit Committee also prepares a proposal for the election of an auditor to the Board of Directors and regularly considers the need for a separate internal audit function. Members of the Audit Committee must have broad business knowledge, as well as sufficient expertise and experience with respect to the committee's area of responsibility and the mandatory tasks relating to auditing.

The majority of members of the Audit Committee shall be independent of the company and at least one member shall be independent of the company's significant shareholders. The Audit Committee invites experts to its meetings when necessary for the issues to be discussed. External auditors are permanent invitees to the meetings of the Audit Committee. Minutes of the Audit Committee meetings are made available for all members of the Board of Directors.

The Audit Committee convenes at least four (4) times a year as notified by the Chair of the Committee. Members of the Audit Committee are listed in the table above.

Personnel and Nomination Committee

The Personnel and Nomination Committee prepares material and instructs with issues related to the composition and compensation of the Board of Directors and remuneration of the other members of the top management of the company. The Committee prepares proposals to the General Meeting of Shareholders related to these matters.

The majority of the members of the Personnel and Nomination Committee shall be independent of the company. The Committee calls in experts to its meetings when necessary for the issues to be discussed. Minutes of the Personnel and Nomination

Committee meetings are made available for all members of the Board of Directors.

The Personnel and Nomination Committee convenes at least two times a year as notified by the Chair of the Committee. Members of the Committee are listed in the table above.

President and CEO

The Board of Directors appoints and may dismiss the President and CEO and decides upon the President and CEO's remuneration and other benefits in accordance with the Remuneration Policy. The CEO is responsible for the day-to-day management of the company. The CEO's main duties include:

- managing the business according to the instructions issued by the Board of Directors
- presenting the matters to be handled in the Board of Directors' meetings
- implementing the decisions made by the Board of Directors
- other duties determined in the Finnish Companies Act

2025:

Timo Laaksonen has been F-Secure President and CEO since 30 June 2022.

The biographical details of the President and CEO including the President and CEO's shareholdings are specified at the end of this statement. The remuneration of the President and CEO is specified in F-Secure Remuneration Policy and Report.

Leadership Team

The Leadership Team supports the President and CEO in the daily operative management of the company.

2025:

Current information on the F-Secure Leadership Team can be found on our website: https://investors.f-secure. com/en/investors/ corporate_governance/ leadership_team.

For descriptions of all members of the Leadership Team during 2025 and their roles, respective membership periods and shareholdings, see the end of this statement.

Internal control and risk management

Risk management

Risk management and internal control processes at F-Secure seek to ensure that risks related to the business operations of the company are properly identified, evaluated, monitored, mitigated and reported in compliance with the applicable regulations.

F-Secure Board of Directors defines the principles of risk management and internal controls which are followed within the company. The Audit Committee assists the Board in the supervision of F-Secure risk management process. The President and CEO is accountable for ensuring that the risk management principles are implemented and applied constantly and consistently across the organization, supported by the Corporate Development function.

The primary goal of F-Secure risk management principles is to empower the organization to identify and manage risks more effectively. The potential negative impact and probability of different situations arising from business operations of the company, its markets, its customers, or its partners are monitored as part of the risk management process.

F-Secure promotes continuous risk evaluation by the company's personnel. The relevant operational risks identified through the risk management process are regularly reviewed by each function, including the twice a year review with the President and CEO and the Leadership Team, and the Audit Committee. Company's statutory auditor reviews risks part of each interim release (quarterly). Risk Management is an integrated part of F-Secure's governance and management, and the risk management process is aligned with the ISO-31000:2018 guidelines. The Audit Committee regularly evaluates the effectiveness of the risk management system.

Internal control

The purpose of Internal Control is to ensure that operations are effective and aligned with the strategy, and that financial reporting and management information is reliable and in compliance with applicable regulations and operating principles.

Internal control consists of all the guidelines, policies, processes, practices and relevant information about organizational structure that help ensure that the business conduct is in compliance with all applicable regulations. The purpose of internal control is also to ensure that accounting and financial information provides a true and accurate reflection of the activities and financial situation of the company.

The company constantly monitors its key financial processes linked to sales, revenue, costs and profitability as well as incoming and outgoing

payment transactions. If any inconsistencies appear, the issues are handled without delay. The company's finance department is responsible for the consistency and reliability of internal control methods. The finance team, led by the CFO, works in close cooperation with businesses, providing relevant data for business planning purposes and sales estimates. The team also regularly assesses and monitors the reliability of estimates and revenue recognition.

Internal audit

Audit Committee considers the need for and appropriateness of a separate Internal Audit function on a regular basis. To date, the Audit Committee has concluded that, due to the size, organizational structure and largely centrally controlled financial management of the company, a separate Internal Audit function is not necessary.

In the absence of an Internal Audit function, attention is paid to periodical review of the written guidelines and policies concerning accounting, reporting, documentation, authorization, risk management, internal control and other relevant matters across the company. Related controls are also tested from time to time. The guidelines and policies are coordinated by the company's finance team with active involvement by the legal team.

The absence of a separate Internal Audit function is considered when defining the scope of the company's external audit. Where necessary, the Internal Audit services will be purchased from an external service provider.

To facilitate transparency and exchange of information on Internal Audit related matters, the financial management team has frequent meetings with the auditors. The auditors also participate in the meetings of the Audit Committee as permanent invitees.

The company has taken into use a Whistleblowing Channel for employees and other stakeholders to report any possibly corrupt, illegal, or other undesirable conduct.

Related party transactions

The Audit Committee defines the principles for monitoring and assessing F-Secure related party transactions. The definition of the related parties is based on IAS 24 standard. F-Secure collects information about its related parties on regular basis. The Board of Directors decides on related party transactions that are not conducted in the ordinary course of business of the company or are not implemented under arm's-length terms. Related party transactions are disclosed as part of financial statements according to the applicable legislation.

Insider management

F-Secure complies with the applicable legislation, including EU Market Abuse Regulation (MAR), the regulations of the Finnish Financial Supervisory Authority as well as Nasdaq Helsinki's Guidelines for Insiders. F-Secure has established its own insider policy to complement the regulation and guidelines above.

F-Secure maintains a list of all persons who have regular access to company's financial data. Due to the sensitive nature of financial information, persons having access to financial information before publication of an interim financial report or a year-end report shall be subject to a thirty (30) day trading restriction prior to publication of such report.

In addition, F-Secure maintains a project-specific insider list of any projects and events which, if realized, would be likely to have a significant effect on the value of F-Secure share or other financial instruments, and which have been subject to delaying of disclosure in accordance with MAR.

F-Secure has decided not to include any persons as permanent insiders. All persons with inside information regarding a project will be included in the project specific insider list.

Persons discharging managerial responsibilities comprise the Board of Directors, the President and CEO and other members of the Leadership Team. These persons have a duty to notify F-Secure and the Finnish Financial Supervisory Authority of every transaction in their own account relating to Financial Instruments of F-Secure within three business days (after a cumulative threshold of EUR 20,000 per annum). The company publishes these notifications as stock exchange releases, as specified by MAR. All releases published on managers' transactions are available on the company's website.

Auditors

The auditor is elected by the Annual General Meeting for a term of service ending at the close of the next Annual General Meeting. The auditor is responsible for auditing the consolidated and parent company financial statements and accounting. The auditor reports to the Board of Directors or the Audit Committee at least once a year.

2025:

The Annual General Meeting held 1 April 2025 re-elected the audit firm PricewaterhouseCoopers Oy as the company's auditor with Authorized Public Accountant (APA) Samuli Perälä as the responsible auditor of F-Secure Corporation. The same audit firm was elected as sustainability reporting assurance provider for the financial year 2025.

F-Secure paid the auditor EUR 162 (159) thousand for the auditing services. In addition, F-Secure paid a total of EUR 117 (126) thousand for other advisory services unrelated to auditing. The other advisory services mainly concerned sustainability advisory and sustainability reporting assurance. Comparison period had also EUR 21 thousand for audit related fees and EUR 11 thousand for tax consulting.

31 DECEMBER 2025

Board of Directors

Pertti Ervi

Chair of the Board since 2022
Member of the Audit Committee since 2022
Chair of the Personnel and Nomination Committee since 2024

Finnish citizen
b. 1957, male

Main occupation: Independent management consultant and a professional board member

Key positions of trust

QPR Software Corporation, Chair of the Board of Directors since 2021

Pointsharp Holding AB, member of the Board of Directors since 2021

Efecte Corporation, Chair of the Board of Directors between 2011 and 2024. Member of the Board of Directors between 2008 and 2024

WithSecure, member of the Board of Directors between 2003 and 2023, Chair of the Board between 2004 and 2006 and Chair of the Audit Committee between 2008 and 2022

Mintly Oy, founding member and Chair of the Board of Directors between 2017 and 2022

Teleste Corporation, member of the Board of Directors between 2009 and 2020, Chair between 2017 and 2020

Comptel Corporation, Chair of the Board of Directors between 2011 and 2017

Stonesoft Corporation, Chair of the Board of Directors between 2004 and 2007

Primary working experience

Computer 2000 AG, Co-CEO and member of the Executive Board between 1995 and 2000

Computer 2000 Finland Corporation, Co-founder and CEO between 1983 and 1995

Education

Ervi holds a Bachelor of Science degree in electronics and several management studies.

Holdings at the end of December 2025: number of shares 140,232, holding 0.08%

Alessandro Adriani

Board member since 2025
Member of the Personnel and Nomination Committee since 2025

Italian citizen
b. 1971, male

Main occupation: Independent Board Member, Professor in Economics and Digital

Key working experience

British Telecom, London, SVP Sales To and Through Channels / Global System Integrators and Communication Service Providers from 2020 to 2024

Deutsche Telekom, Frankfurt, MD Sd-Wan / SASE at T-Systems International, ngena from 2016 to 2020

Singapore Telecom International, Singapore, CEO at Bridge - Enterprise Managed Mobility, IoT and Roaming from 2012 to 2015

Vodafone Group, London, VP at Vodafone Sales and Services / Partner Markets - Enterprise Managed Mobility, IoT and Roaming from 2002 to 2012

Arthur D Little, Milan, Senior Consultant at Tech, ICT, Media and Entertainment Practice - M&A from 2000 to 2002

TIM International, Rome, M&A Financial Analyst from 1998 to 2000.

Education

Adriani holds MBAs from CUOA Business School and Henley Business School along with a BA in Economics from Siena University and Reading University.

Holdings at the end of December 2025: number of shares 9,362, holding 0.01%

Roxana Diaconescu

Board member since 2025
Member of the Personnel and Nomination Committee since 2025.

Romanian citizen
b. 1974, female

Main occupation: CTO, SilverRail Technologies

Primary working experience

Meta, Engineering Leadership from 2020 to 2021

Sysdig, Senior Director, Engineering from 2019 to 2020

Uber, Engineering Leadership from 2016 to 2018

Cloudera, Engineering Leadership from 2016 to 2016

Expedia, Engineering Leadership from 2013 to 2015

Markit, VP Software Engineering from 2008 to 2013

Yahoo!, Senior Software Engineer from 2006 to 2008

Caltech (California Institute of Technology), Postdoctoral Researcher from 2004 to 2006

UCI (University of California, Irvine), Postdoctoral Researcher from 2003 to 2004

Stanford University, Visiting Researcher from 2021 to 2021

Education

Diaconescu has a Masters degree from the University Politehnica Bucharest and a doctorate in computer science from Norwegian University of Technology and Natural Science (NTNU).

Holdings at the end of December 2025: number of shares 9,362, holding 0.01%

Cornelia Schaurecker

Board member since 2025
Member of the Audit Committee since 2025.

Austrian citizen
b. 1977, female

Main occupation: CEO Innotech AI Consulting (Senior Executive Advisor for Applied AI Initiative, Bain & Company, Airbus and others).

Primary working experience

VODAFONE Group: Global Group Director Big Data & AI, London, UK from 2019 to 2023

BMW Group: Vice President IT (CIO) EMEA Region, Munich, Germany from 2017 to 2019

VW Group: Founder & Director VW Group Data:Lab, Munich, Germany from 2013 to 2017

VW Group UK: CIO VW Group UK (all National Sales Company brands); Milton Keynes, UK from 2012 to 2013

AUDI AG: Diverse Commercial/IT-Mgt. positions Ingolstadt, Germany from 2000 to 2012:

- Head of IT Internat. Sales/Own Retail, CRM, Websites from 2006 to 2012
- Head of IT & Organisation Strategy, IT Governance from 2005 to 2006
- Chief of Staff to Group CIO Audi/Seat/Lamborghini from 2002 to 2004
- CRM & Retail Marketing: Mgt. Audi PartnerNet (Extranet) from 2000 to 2002

Education

Schaurecker holds a Master's Degree in International Business from Johannes Kepler University Linz, Austria, and a Master of Science (Economics) Degree („Industrieökonom") from Hanken Swedish School of Economics and Business Administration, Finland, along with studies at University of Hohenheim, Stuttgart and Oxford University's Saïd Business School (Artificial Intelligence postgraduate programme).

Holdings at the end of December 2025: number of shares 9,362, holding 0.01%

Petra Teräsaho

Board member since 2022
Chair of the Audit Committee since 2022.

Finnish citizen
b. 1966, female

Main occupation: CFO of Transmeri Group

Key positions of trust

Paulig Group, member of the Board of Directors since 2020, and Chair of Audit Committee

Solar Foods, member of the Board of Directors sinse 2025, and Chair of Audit Committee

Primary working experience

Valmet Automotive, CFO between 2023 and 2024

Enfo Group, CFO 2022

Stora Enso, Senior Vice President, Group Controller between 2016 and 2022

Outotec Group, Vice President Group Controller between 2014 and 2015

Nokia Corporation between 1993 and 2014, Several leadership roles in Finance, Marketing, Strategy & Business Development, e.g.

- CFO of Nokia Mobile Phones operations in India between 2007 and 2012
- Finance Director, Mobile Phones & Nokia Strategic Marketing between 2004-2007
- Head of Developer Business Marketing, Mobile Phones between 2003-2004
- Head of Business Planning of Mobile Applications unit between 2000 and 2001
- Head of Value-Based Marketing (Nokia Networks) between 1999 and 2000
- Accounting Manager (Network Systems) between 1996 and 1998
- Nokia Group Accounting, Financial Analyst between 1993 and 1996

United Paper Mills France SA, Paris France, Controller between 1991 and 1993

Education

Teräsaho holds a Master of Science in Accounting and Finance.

Holdings at the end of December 2025: number of shares 33,873, holding 0.02%

Tommi Uitto

Board Member since 2024

Finnish citizen
b. 1969, male

Main occupation: Nokia, President, Mobile Networks

Key positions of trust

Technology Industries of Finland, member of the Board, and member of Working Committee since 2024

Primary working experience

Nokia Mobile Networks, President, 2018–2025

Nokia Mobile Networks, Senior Vice President, Global Product Sales, 2015–2018

Nokia Networks, Senior Vice President, West Europe, Customer Operations, 2013–2015

Nokia Siemens Networks, Head of Global 4G/LTE Radio Access Business Line, Mobile Broadband, 2011–2012

Nokia Siemens Networks, Head of Product Management, Network Systems, 2009-2010

Nokia Siemens Networks, Head of WCDMA/HSPA and Radio Platforms Product Management, 2007-2008

Nokia Networks, General Manager, Radio Controller Product Management, 2005–2007.

Nokia Networks, Director, Sales & Marketing (Lead Sales Director), France Telecom/Orange 2002–2005

Nokia Networks, Operations Director, Northeast Europe, Central & Eastern Europe and Middle East, 1999–2002

Nokia Networks, Manager, Product Business Management and Logistics, Cellular Transmission, 1996–1999

Valmet Logging Americas Inc., Director, Production and Development, 1994–1995

Education

Uitto holds a degree of Master of Science in Industrial Management from Aalto University and a degree of Master of Science in Operations Management from Michigan Technological University.

Holdings at the end of December 2025: number of shares 17,325, holding 0.01%

Rachit Mittal

Board member since 2025

Indian citizen
b. 1981, male

Main occupation: Director of Engineering, Scam Protection at F-Secure

Primary working experience

F-Secure, Senior Engineering Manager between 2023 and 2024

Lookout Inc, Senior Software Engineering Manager between 2022 and 2023

Lookout Inc, Senior Staff Software Engineer between 2020 and 2021

Motorola Mobility (Lenovo), Software Development Manager between 2017 and 2020

Motorola Mobility (Lenovo), Senior Staff Software Engineer between 2014 and 2017

Motorola Mobility (Google), Senior Staff Software Engineer between 2012 and 2014

Motorola Mobility, Lead Software Engineer between 2011 and 2012

Motorola Inc, Lead Software Engineer between 2010 and 2011

Motorola Inc, Senior Software Engineer between 2007 and 2010

Motorola Inc, Software Engineer between 2004 and 2007

Education

Mittal holds a Bachelor of Engineering degree in Computer Science and Engineering.

Holdings at the end of December 2025: number of shares 2,964, holding 0.00%

31 DECEMBER 2025

Leadership Team

Timo Laaksonen

President and Chief Executive Officer since 2022

Finnish citizen
b. 1961 , male

Primary working experience

WithSecure, Executive Vice President of Consumer Security, and various executive positions in F-Secure between 2012 and 2022

Tecnotree, Chief Commercial Officer between 2010 and 2012

Xtract, CEO between 2008 and 2010

First Hop, CEO between 2001 and 2008.

Sonera SmartTrust, Executive Vice President between 1998 and 2001

Teamware Group, Regional Business Manager and Vice President between 1993 and 1998

ICL Travel Systems, Marketing Manager between 1992 and 1993

Nokia Data, Sales and Business Development Manager between 1986 and 1991

Key positions of trust

Finnish Information Security Cluster (FISC), member of the Board since 2024

Helsinki Region Chamber of Commerce, member of the Commission between 2024 and 2025

Broadband Forum Executive Advisory Board member between 2023 and 2024

Finnish American Chamber of Commerce in New York, member of the Board of between 2018 and 2019.

Broadband Multimedia Marketing Association (USA), a member of the Board of Directors between 2018 and 2019

Education

Laaksonen holds a Master of Science degree in Economics and Business Administration.

Holdings at the end of December 2025: number of shares 49,986, holding 0.03%

Richard Larcombe

Chief Marketing Officer since 2022

British citizen
b. 1974, male

Primary working experience

WithSecure, Vice President of Global Marketing between 2019 and 2021

ismybillfair.com, co-founder and Chief Marketing Officer between 2017 and 2019

Tesco Bank, Brand and Marketing Director between 2015 and 2017

Virgin Media, Chief Marketing Officer and Director of Advertising and Sponsorship between 2010 and 2015

The Times, Sunday Times and Times Online, Head of Marketing between 2004 and 2010

AMV BBDO, Account Director between 1998 and 2004

Grey, Account Director between 1996 and 1998

Education

Larcombe holds a degree in Psychology (BA Hons).

Holdings at the end of December 2025: number of shares 15,100 holding 0.01%

Nina Lehto

Senior Vice President, Services since 2024

Finnish citizen
b. 1976, female

Primary working experience

Nokia, Head of Mediation Business Line, and various other positions between 2018 and 2024

Comptel, VP, Delivery & Support, and various other positions between 2006 and 2017

Roschier, Attorneys, Lawyer between 2002 and 2006

Education

Lehto holds a Master of Laws degree.

Holdings at the end of December 2025: number of shares 3,556, holding 0.00%

Antero Norkio[1)]

Senior Vice President, Corporate Development
since 2022

Finnish citizen
b. 1972, male

Primary working experience

WithSecure, Vice President Product Management (Consumer Business), and various other positions between 2011 and 2022

Airwide Solutions, Head of Global Channel Partners and Director of Product Management between 2002 and 2011 (including the acquisition of First Hop 2007)

Taika Technologies, Vice President of Product Management between 2001 and 2002

Sonera SmartTrust, Director of Product Management between 1997 and 2001

Education

Norkio holds a Master of Science degree in Industrial Engineering and Management (Strategy and International Business).

Holdings at the end of December 2025: number of shares 70,017, holding 0.04%

1) After the reporting period, on 13 January 2026, it was announced that Antero Norkio will leave the company on 30 January 2026.

Bruno Rodriguez

Chief Revenue Officer since 2024

Spanish citizen
b. 1973, male

Primary working experience

Bitdefender, Global VP Sales Service Providers and Technology Licensing and Strategic Partnerships Director between 2012 and 2024

Panda Security, Global Product Management Director, Global Business Development Director, Business Unit Director and other positions between 2006 and 2012

Euskaltel, Business Development Manager between 2000 and 2006

Education

Rodriguez holds a Master of Science degree in Business Administration and a Bachelor Degree in Computer Engineering.

Holdings at the end of December 2025: number of shares 0

Sari Somerkallio[1)]

Chief Financial Officer since 2022

Finnish citizen
b. 1972, female

Primary working experience

WithSecure, Head of Finance in Consumer Security from February to June 2022

Fiskars Group, several manager and VP positions such as Vice President of Business Finance, Senior Vice President of Finance & Business Development, and Manager of Development Projects between 2008 and 2021

Wärtsilä Corporation, Project Manager and Process Manager between 2002 and 2008

Wärtsilä Corporation, Investor Relations Manager between 1999 and 2002

Merita Stockbrokers, Analyst between 1997 and 1999

Interbank, Analyst between 1996 and 1997

Key positions of trust

Aktia Bank, member of the Board of Directors and Chair of Audit Committee since 2025

Education

Somerkallio holds a Master of Science degree in Mathematics and a Master of Science degree in Economics (Finance).

Holdings at the end of December 2025: number of shares 20,099, holding 0.01%

1) On 18 December 2025 it was announced that Sari Somerkallio will leave the company and remain at F-Secure until 30 April, 2026

Kaisa Tikka-Mustonen

Chief People Officer since September 2024

Finnish citizen
b. 1978, female

Primary working experience

Helvar, Chief People Officer between 2020 and 2024

Nordcloud, VP, Talent Acceleration & People Operations between 2018 and 2020

Nets Group, Merchant Services, HR Director between 2015 and 2018, HR Business Partner between 2014 and 2015

Tieto, various Human Resources positions between 2007 and 2013

Education

Tikka-Mustonen holds a master's degree in Education.

Holdings at the end of December 2025: number of shares 2,134, holding 0.00%

TL Viswanathan

Chief Product Officer since 2023

Indian citizen
b. 1979, male

Primary working experience

F-Secure, Vice President, Embedded security, 2022

Nokia, Head of Digital Operations Portfolio, between 2018 and 2022

Comptel, Director & Vice President Global Alliances, between 2014 and 2018

Oracle, Senior Account Manager APAC, between 2013 and 2014.

Nokia Siemens Networks, various leadership and business development roles for Applications, Systems integration business between 2006 and 2013

Siemens Communications, Solution Consultant between 2000 and 2006

Education

Viswanathan holds a Master's degree in Business Administration (International Business).

Holdings at the end of December 2025: number of shares 5,883, holding 0.00%

Santeri Kangas

Chief Technology Officer (CTO) since 2025

Finnish citizen
b. 1971, male

Primary working experience

CUJO AI, CTO betweern 2018 and 2025

Omada A/S, CTO between 2016 and 2018

Flexera Software LLC, Vice President and Chief Architect between 2015 and 2016

Secunia ApS, CTO in 2015

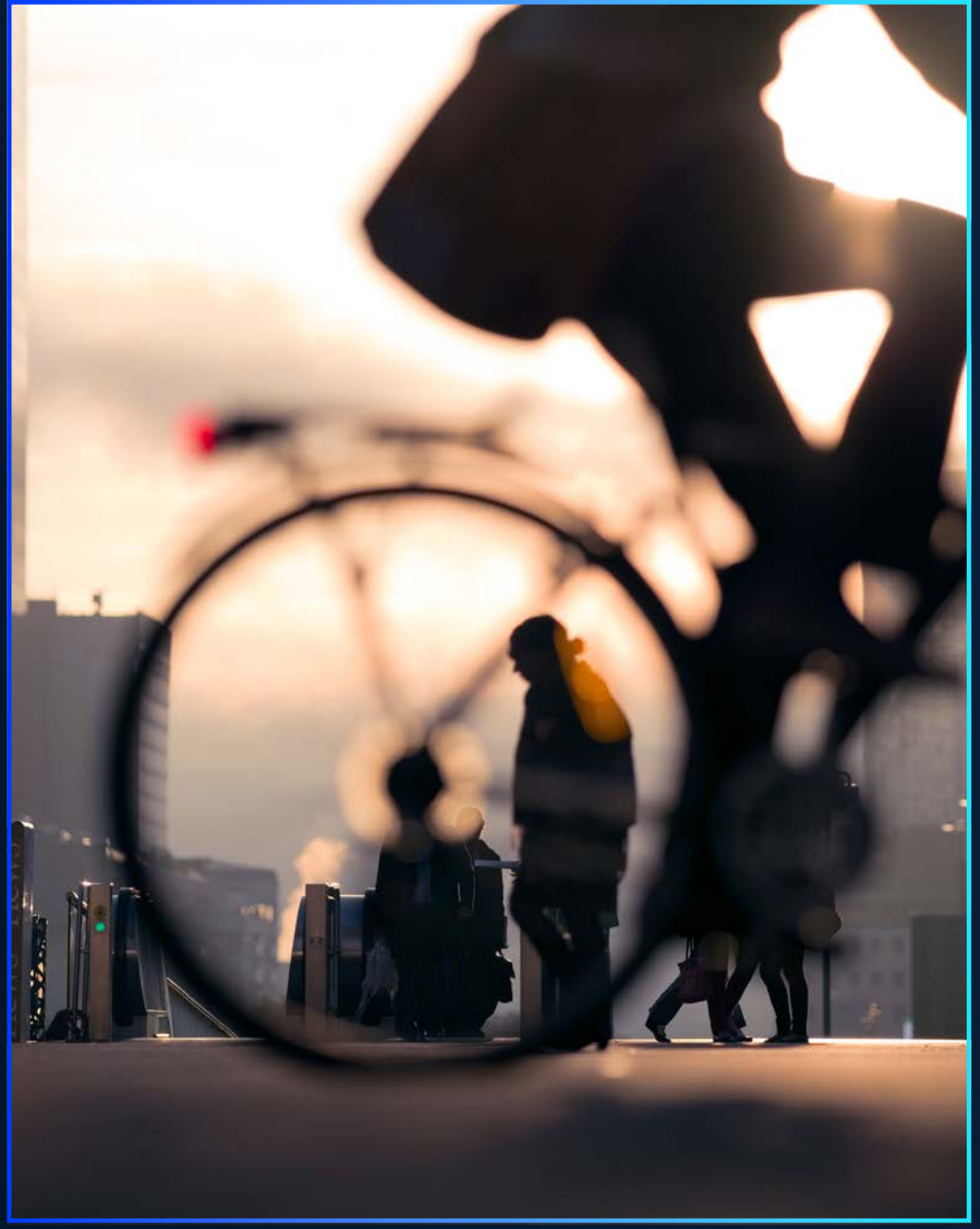
F-Secure Corporation, several technology leadership positions including CTO, Chief Architect, VP Research, and VP Technology between 1999 and 2015

Education

Santeri Kangas holds a Master of Science degree in Business Administration and a Bachelor Degree in Information Technology.

Holdings at the end of December 2025: number of shares 0

Remuneration



Remuneration Report

Introduction

This Remuneration Report 2025 has been prepared in accordance with the Finnish Corporate Governance Code 2025 (publicly available at http://cgfinland.fi/en/) and contains comprehensive information on remuneration of the Board of Directors and the President and CEO. All remuneration information in this report is from 1 January 2025 until 31 December 2025, except that the Board of Directors remuneration is based on their term of office that began in 2025 and will expire at the end of the 2026 Annual General Meeting (as explained in further detail in the F-Secure Corporate Governance Statement 2025).

F-Secure Remuneration Policy, which has been applicable since June 2022, describes the remuneration for the Board of Directors and the President and CEO and the considerations of determining the policy and operation of the policy. Remuneration Policy of F-Secure complies with the recommendations of the Finnish Corporate Governance Code for listed companies, Shareholders' Rights Directive legislation and any other regulations and guidelines concerning remuneration in listed companies. New Remuneration Policy will be presented at the Annual General Meeting in Spring 2026 and is planned to be applicable 2026-2029. The proposal for new Remuneration Policy is available at F-Secure website as a part of the Annual General Meeting material.

According to F-Secure Remuneration Policy, the remuneration for F-Secure management is designed to advance the business objectives and long-term profitability of the company. F-Secure remuneration in general is based on rewarding for performance and talent. Remuneration is designed to be competitive compared to relevant reference markets, to increase commitment and work engagement and to be consistent across the organization. Incentive schemes are developed to support the company's strategy by aligning the interests of the shareholders and the key employees for strong performance and short and long-term value creation of the company. The remuneration of employees across the company is reviewed regularly with the intention that all employees are paid appropriately in the context of the market and considering their individual performance and competencies.

These principles have been considered in the company's remuneration in the financial year 2025. In 2025, the remuneration of the Board of Directors and the President and CEO complied with the Remuneration Policy, and there were no deviations.

The President and CEO's remuneration follows the same principles as the remuneration of all other employees, and this is evident in the performance criteria set for the variable remuneration. Approximately half of the President and CEO's remuneration package is based on performance. The existing short- and long-term incentive plans are based on the company's financial performance, employee engagement and shareholder value development to ensure a strong link between the company's performance and CEO remuneration. The President and CEO is recommended to hold at least 50% of the shares received as rewards from the long-term incentive programs and to accumulate the shares from the incentive programs until the value of the shares received from the share programs equals the annual gross base salary of the President and CEO. There are no other restrictions set for the shares received from the share-based incentive programs.

Remuneration in 2025

The Board of Directors of F-Secure Corporation decided on the establishment of share-based long-term incentive plans targeted to the management and selected key employees of F-Secure. The share-based long-term incentive plans include a Performance Share Plan ("PSP") as the main plan and Restricted Share Plan ("RSP") as a complementary share-based incentive plan for individually selected key employees in specific situations. New plan periods 2025–2027 for PSP and RSP commenced at the beginning of 2025 and include a three-year performance period followed by a possible reward payment. In addition to PSP and RSP the Board of Directors decided on a Performance Matching Share Plan ("PMSP") as an alternative to PSP for selected key individuals , mostly President and CEO and LT members. Members of the Leadership Team and selected key employees can participate in either PSP or PMSP according to their choice, not both plans. PMSP requires initial investment from the participant. The plan commenced in 2025 and includes one performance period, covering financial years 2025—2027. The performance period is followed by a one-year retention period, covering the financial year 2028. The potential rewards from the PMSP will be paid in two equal instalments, first instalment within 5 months after the end of the performance period and second instalment within 5 months after the end of the retention period. The plan includes a guaranteed matching reward (1 reward share to 2 purchased) shares and a possible performance-based matching reward. The share-based compensation is forfeited if the employment relationship is terminated by either party.

The total remuneration paid to the President and CEO in 2025 was EUR 474,330. This included a short-term incentive of EUR 131,712.

At the end of 2025, the President and CEO held 49,986 shares of F-Secure.

Annual remuneration in 2025

F-Secure's paid average remuneration in 2025 is described in the table below.

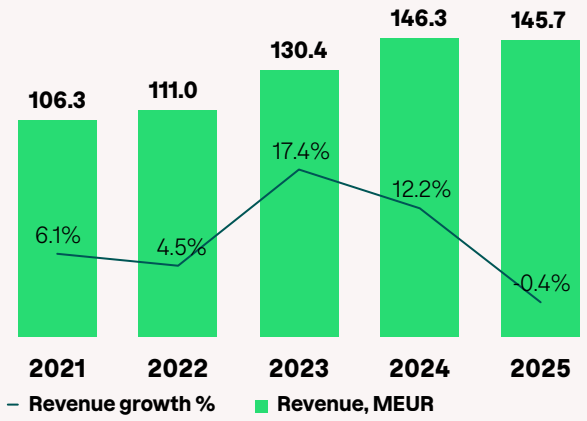
Average annual remuneration (EUR)	2025	2024
President and CEO[1]	474,330	333,840
Chair of the Board	86,000	80,000
Other Board Members[2]	41,200	40,500
Average employee[3]	63,250	76,836

1) Remuneration paid during the financial year, including the base salary as well as short- and long-term incentives bonus.

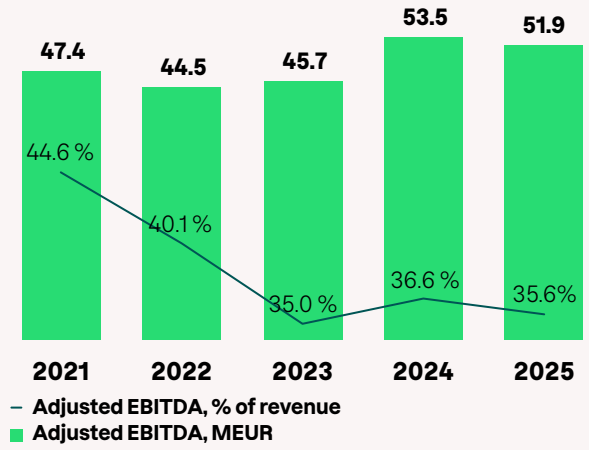
2) The average remuneration paid to the Board Members, excluding the employee Board member.

3) The total wages and salaries, including sales and non-sales incentives, paid / average full-time equivalent headcount during the same period in all countries. The amount excludes end of employment related severances.

Revenue development 2021-2025



Adjusted EBITDA development 2021–2025



The key figures are presented combining actuals and carve-out basis for 1-12/2022 and on an actuals basis for financial position at 31 December 2022. For period 2021 financial information is on carve-out basis.

Remuneration of the Board of Directors

F-Secure's General Meeting, held on 1 April 2025, decided that the remuneration for the Board of Directors of F-Secure shall be paid as follows: EUR 80,000 for the Chairman of the Board of Directors, EUR 38,000 for other members of the Board of Directors, and EUR 12,667 for a member of the Board of Directors employed by F-Secure, EUR 10,000 additional remuneration for the Audit Committee Chair, EUR 4,000 additional remuneration for the Personnel and Nomination Committee Chair, EUR 2,000 additional remuneration for the Audit Committee members, and EUR 2,000 additional remuneration for the Personnel and Nomination Committee members.

Pursuant to the decision by F-Secure's General Meeting in April 2025, F-Secure Corporation repurchased its shares from the market on the 11th and 12th September for and on behalf of F-Secure Board members, in such quantity that represents approximately 40 per cent of the Board's remuneration.

For the Members of the Board of Directors, changes in the holdings of the company shares and rewards paid in shares are reported according to the Market Abuse Regulation. Related stock exchange releases are available on the company's website.

The travel expenses and other costs of the members of the Board of Directors of F-Secure directly related to board work are paid in accordance with F-Secure compensation policy in force from time to time.

Each member of the Board of Directors of F-Secure is paid a predetermined travel fee in addition to travel expenses for meetings held outside their country of residence. A separate meeting fee of EUR 1,000 is paid to the Board members travelling from another country to an on-site meeting within the European continent. If inter-continental travel is required, the fee is EUR 2,000. The travel expenses and other costs directly related to the Board work of the members of the Board of Directors are paid in accordance with the company's compensation policy in force at any given time.

The Board of Directors Remuneration in 2025
Remuneration for the board term 2025-2026

Member	Annual fee paid in cash, EUR	Annual fee paid in shares, EUR	Annual fee paid in shares, pcs	Meeting fees paid EUR[1)]	Total, EUR
Pertti Ervi	51,601	34,400	20,924	4,000	90,000
Thomas Jul Pfeiffer (1.1.-31.3.2025)				2,000	2,000
Petra Teräsaho	28,801	19,199	11,678		48,000
Tommi Uitto	22,801	15,199	9,245		38,000
Roxana Diaconescu (1.4.-31.12.2025)	24,001	15,999	9,732	3000	43,000
Cornelia Schaurecker (1.4.-31.12.2025)	24,001	15,999	9,732	3000	43,000
Alessandro Adriani (1.4.-31.12.2025)	24,001	15,999	9,732	3000	43,000
Rachit Mittal (1.4.-31.12.2025)	7,602	5,065	3,081		12,667
Total	182,808	121,860	74,124	15,000	319,667

1) The remuneration presented includes travel allowance granted from abroad to board meetings.

Remuneration of the President and CEO

The remuneration of the President and CEO is decided by the Board of Directors. The main components of the President and CEO's total remuneration are base salary and short- and long-term incentives. In addition, he may participate in the voluntary Employee Share Savings Plan (ESSP) as approved by the Board of Directors. The aim of the ESSP is to encourage employees to acquire and own F-Secure shares, and it is intended to align the interests of the shareholders and the employees as well as to increase employees' long-term commitment to the company.

Salaries and financial benefits paid in and accrued based on 2025 are described below:

EUR	Payments in 2025
Base salary, including fringe benefits	342,618
Pension / Other financial benefits	-
Short-term incentive (STI	131,712
Long-term incentive (LTI)	-
Total	474,330

Short-term incentive (STI) payout for the President and CEO is 50% of annual base salary if targets are met, maximum payout being equal to the annual base salary.

F-Secure Short Term Incentive plan objectives were set for the period of 1 January–31 December 2025. The STI Plan of 2025 for the President and CEO was based on F-Secure 2025 combined revenue and adjusted EBITA growth with 80% weight and employee Net Promoter Score with 20% weight of total. The overall performance for these two criteria was evaluated and resulted in 11% weighted performance outcome.

In 2025, the President and CEO, Timo Laaksonen received a STI payment in March. The objectives of the plan were 2024 combined revenue growth and adjusted EBITA growth with 80% weight and employee Net Promoter Score growth with 20% weight. The weighted performance for these two criteria for 2024 was 78,4%. The reward was in total EUR 131,712.

STI Plan 2025	STI Target (% of base salary)	Performance Criteria	Weight	Performance	Total Weighted Performance	Payment
STI 2025 (January–December)	50%	Revenue and adjusted EBITA Growth	80%	0%	11%	March 2026
		Employee Engagement (eNPS)	20%	55%		

STI Plan 2024	STI Target (% of base salary)	Performance Criteria	Weight	Performance	Total Weighted Performance	Payment
STI 2024 (January–December)	50%	Revenue and adjusted EBITA Growth	80%	73%	78%	March 2025
		Employee Engagement (eNPS)	20%	100%		

STI Plan 2023	STI Target (% of base salary)	Performance Criteria	Weight	Performance	Total Weighted Performance	Payment
STI 2023 (January–December)	50%	Revenue and adjusted EBITDA growth	80%	0%		February 2024
		Employee Engagement (eNPS)	20%	0%		

There was no long-term incentive (LTI) payment made to the President and CEO in 2025. In 2025 the President and CEO participated in the Performance Matching Share Plan (PMSP) 2025-2028.

The President and CEO – Current LTI Plans

Share Plan	LTI Target (pcs of shares)	Performance Criteria	Weight	Performance	Payment
PSP 2022–2024	41,562	Absolute Total Shareholder Return	100%	–	H1 / 2025
PSP 2023–2025	47,000	Profitable growth (average revenue growth 2023–2025 (%) and adjusted EBITA 2025 (%))	30%	– / Plan ongoing	H1 / 2026
RSP 2023–2025	12,373	Fixed share reward amount and a retention period of three years	–	– / Plan ongoing	H1 / 2026
PSP 2024–2026	82,555	Absolute Total Shareholder Return	50%	– / Plan ongoing	H1/2027
		Earnings per share sum	25%		
		Revenue growth (EUR in 2026 vs proforma 2023)	25%		
PMSP 2025-2028	169,492	Share price development	100%	-/Plan ongoing	H1/2028 & H1/2029

The key terms of service of the President and CEO

The contract of the President and CEO is an indefinite contract with a six-month period of notice both ways. If the company terminates the contract for reasons other than a breach of the contract, the President and CEO shall be entitled to receive severance pay equivalent to six months' salary in addition to the salary for the notice period.

The company has obtained a life insurance for the President and CEO with an amount equaling the annual gross salary of the President and CEO.

The President and CEO does not have a supplementary pension plan, and the determination of his pension conforms to the standard rules specified by Finland's Employee Pension Act (TYEL). The President and CEO's retirement age is also determined by the statutory pension system and is 65 years under the applicable Finnish legislation.

President and CEO Pay mix 2025

President and CEO Pay mix in 2025 consisted of base pay, including fringe benefits plus a short-term incentive payment. There were no long-term incentive payments due to the payout thresholds were not met.

F-Secure Corporation
Tammasaarenkatu 7
00180 Helsinki
Tel. +358 9 2520 0100
helsinki@f-secure.com
www.f-secure.com