



25
YEARS

2025 SUSTAINABILITY REPORT

FORTINET

TABLE OF CONTENTS

03 INTRODUCTION

- 03 Who we are
- 04 Message from our CSR committee
- 05 2025 sustainability highlights
- 06 25 years of securing the digital world

07 SUSTAINABILITY AT FORTINET

- 08 Strategy
- 10 Double materiality assessment
- 11 Stakeholder engagement
- 13 Sustainability reporting and disclosures

14 SECURING THE DIGITAL WORLD

- 15 Responsible technology
- 19 Cybersecurity innovation
- 23 Cybercrime disruption
- 28 Customer success enablement

30 MINIMIZING OUR ENVIRONMENTAL FOOTPRINT

- 31 Climate
- 34 Sustainable operations
- 38 Sustainable products
- 43 Supplier engagement

44 EMPOWERING PEOPLE AND COMMUNITIES

- 45 Our people
- 51 Cybersecurity skills gap

59 DEMONSTRATING INTEGRITY

- 60 Responsible AI
- 61 Information security and data privacy
- 64 Business ethics
- 66 Human rights
- 68 Corporate governance

72 APPENDIX

- | | | |
|-------------------------|------------------|-----------------------------------|
| 72
About this report | 76
TCFD index | 81
SASB index |
| 73
Performance data | 79
GRI index | 82
Limited assurance statement |

WHO WE ARE
MESSAGE FROM OUR CSR COMMITTEE
2025 SUSTAINABILITY HIGHLIGHTS
25 YEARS OF SECURING
THE DIGITAL WORLD

WHO WE ARE



OF INNOVATION FOR A SECURE AND SUSTAINABLE DIGITAL WORLD

Founded in 2000 in Sunnyvale, California, Fortinet is a global leader in cybersecurity and a driving force in the convergence of networking and security. By protecting people, devices, and data everywhere, we help build a safe, trusted, and sustainable digital world for all. We are committed to securing the digital world, minimizing our environmental footprint, empowering people and communities, and demonstrating integrity across our value chain.



Fortinet Development & Support ■ Headquarters ■ Development centers ■ Support centers ■ Regional offices • Cloud locations

Founded **2000**

Corporate headquarters **SUNNYVALE**
California, USA

Number of locations **100+**

Fortinet employees in 2025* **15,100+**

2025 revenue **\$6.8B**

Cash and investments* **\$3.9B**

Market capitalization* **\$59.0B**

85%
of Fortune 100 and **73%** of Global 2000
companies depend on Fortinet to stay secure

Included in
NASDAQ 100 AND S&P 500

900,000+ Lifetime customers*

\$815M R&D investment
in 2025

1,400+ Patents globally*

* As of Dec. 31, 2025

MESSAGE FROM OUR CSR COMMITTEE

Sustainability at Fortinet is guided by our CSR committee, with support of our executive management team, bringing together leaders across the organization to ensure our strategy is embedded in our operations, innovation and culture. Through this collective approach, we align our business priorities with our responsibility to help build a secure and sustainable digital world.

In 2025, Fortinet marked 25 years of serving customers worldwide. Over this time, we have secured people, devices, and data everywhere through waves of extraordinary technological progress alongside moments of unprecedented disruption. Today, our cybersecurity services and solutions protect organizations of every size, supported by one of the industry's largest patent portfolios and continuous innovation across Secure Networking, Unified SASE, and AI-Driven Security Operations.

We are proud that our products, services, and people contribute to building a more secure and sustainable digital society, securing 85% of the Fortune 100 and organizations across critical sectors, including financial services, manufacturing, retail, and telecommunications. This progress was not achieved alone. It reflects the dedication of our employees, the trust of our customers, and the ongoing collaboration with partners across industries and communities around the world.

The past year has reinforced how complex and interconnected our world has become. Geopolitical tensions, environmental pressures, and economic uncertainty continue to reshape societies and organizations. At the same time, transformative technologies—most notably

artificial intelligence (AI)—are raising expectations around trust, security, and accountability. In this context, responsible innovation and strong governance are more important than ever.

AI is reshaping every industry and affecting communities worldwide at an unprecedented pace. While AI offers tremendous potential, its benefits depend on strong foundations of security, data protection, and responsible governance. Fortinet has been applying AI to its cybersecurity solutions and services for over 15 years, helping customers detect threats faster, automate responses, and strengthen resilience. In 2025, we reinforced this commitment by establishing our AI Governance committee, formalizing our Principles for Responsible AI Use and Development, and expanding AI education for our employees and communities.

Across our FortiOS operating system, solutions, and threat intelligence services, AI enables stronger protection while improving operational performance. Our AI leadership also extends beyond product innovation to collaboration with global institutions, law enforcement, and industry bodies.

We are also preparing for the risks and opportunities associated with emerging technologies such as quantum computing. Fortinet has been at the forefront of efforts to protect organizations from future quantum-related threats, including the “harvest now, decrypt later” risk—where encrypted data collected today could be decrypted by quantum computers in the future. We began developing quantum-safe capabilities more than five years ago, integrating early protections into our cybersecurity platform. In 2025, we further

advanced these capabilities within FortiOS to help organizations protect sensitive and mission-critical data and strengthen long-term cyber resilience. Through continued innovation and collaboration, we are helping sectors essential to society—from healthcare to government—prepare for the future of cybersecurity.

Cybercrime continues to increase globally, reinforcing the need for strong public-private collaboration to protect organizations and individuals. For more than a decade, Fortinet has worked with public and private organizations worldwide, sharing threat intelligence and expertise. In 2025, these efforts helped disrupt thousands of malicious infrastructures and supported law enforcement actions globally. We also launched a global, anonymous Cybercrime Bounty program in partnership with Crime Stoppers International, empowering citizens, industry, and law enforcement to strengthen our collective defenses.

We remain committed to minimizing our environmental impact. In 2025, our product innovations achieved up to 62% lower energy consumption compared to prior generations, while a range of sustainable packaging initiatives helped reduce plastic use. We also became the first company in our industry to publish Environmental Product Declarations, increasing transparency around the environmental performance of our products.

To ensure our operations remain resilient and future-ready, we completed a comprehensive climate risk assessment that informs our long-term sustainability strategy and strengthens our ability to anticipate and respond to future challenges.

The security of our digital world ultimately depends on people. Since 2022, Fortinet has trained more than 914,800 individuals in cybersecurity, reaching 91% of our five-year goal. We are on track to achieve our 1 million goal by the end of 2026. Through continued investment in education and skills development—from foundational cyber awareness for students to professional training for cybersecurity experts—we help expand access to skills, foster career opportunities, and strengthen the workforce that protects organizations and society.

As we reflect on this 25-year milestone, we recognize that our work is ongoing. New challenges will continue to emerge, and expectations will continue to evolve. What remains constant is our commitment to doing our part in building a secure and sustainable digital world.

We will continue to strengthen our approach by enhancing transparency, aligning with evolving regulatory expectations, and measuring progress against our commitments.

We thank our employees, partners, customers, and communities for their continued trust and collaboration. Together, we will continue to innovate responsibly, act with integrity, and make a lasting positive impact.

On behalf of the CSR committee

Meera Ramanathan
Head of CSR and chair
of the CSR committee, Fortinet

WHO WE ARE
MESSAGE FROM OUR CSR COMMITTEE
2025 SUSTAINABILITY HIGHLIGHTS
25 YEARS OF SECURING
THE DIGITAL WORLD

2025 SUSTAINABILITY HIGHLIGHTS

CONTRIBUTED TO INTERPOL-LED OPERATION SERENGETI 2.0, WHICH ACHIEVED:

11,400+

MALICIOUS INFRASTRUCTURES
DISRUPTED

1,200+

CYBERCRIMINALS ARRESTED

15+ years

OF EXPERIENCE APPLYING AI
TO CYBERSECURITY AND
NETWORK SOLUTIONS

ESTABLISHED THE
**Fortinet AI Governance
Committee**
AND PUBLISHED OUR
**Principles for Responsible
AI Use and Development**

FORTINET'S COMPLIANCE AND BUSINESS
ETHICS TRAINING COMPLETED BY

100%

OF OUR DISTRIBUTORS

100%

OF OUR TOP CONTRACT MANUFACTURERS*

* Representing >90% of spend.



UP TO
62%

REDUCTION IN PRODUCT ENERGY
CONSUMPTION

1st

CYBERSECURITY COMPANY TO
PUBLISH ENVIRONMENTAL PRODUCT
DECLARATIONS



914,800+

PEOPLE TRAINED
IN CYBERSECURITY
SINCE 2022

7

EXTERNAL EMPLOYER
AND WORKPLACE RECOGNITIONS

WHO WE ARE
MESSAGE FROM OUR CSR COMMITTEE
2025 SUSTAINABILITY HIGHLIGHTS
25 YEARS OF SECURING
THE DIGITAL WORLD

25 YEARS OF SECURING THE DIGITAL WORLD

Fortinet Inc. founding

Ken and Michael Xie co-founded Fortinet in Sunnyvale, California, establishing a vision for a secure and trusted digital world.

Responsible collaboration

Fortinet joined Microsoft's MAPP Zero-Day program, contributing to the responsible disclosure of 1,020+ zero-day vulnerabilities to strengthen global digital infrastructure.

Fortinet Training Institute

The company launched the Fortinet Training Institute,* expanding access to cybersecurity education to strengthen the global cyber workforce.

Cybersecurity certification program

Fortinet introduced industry-recognized certifications to support career development and workforce readiness.

INTERPOL partnership

The company began partnering with INTERPOL and other agencies to support global cybercrime disruption efforts.

Free cybersecurity training

The company expanded access to free cybersecurity training to help organizations and individuals strengthen digital resilience during the global shift to remote work.

Africa Cyber Surge Operation

FortiGuard Labs provided threat intelligence to support INTERPOL and AFRIPOL's Africa Cyber Surge Operation, contributing to coordinated disruption of cybercriminal infrastructure across the region.

Global skills pledge

Fortinet pledged to train 1 million people in cybersecurity by the end of 2026 to help close the global cyber skills gap.

K-12 security awareness

The company launched free K-12 security awareness training to promote safe and responsible digital behavior from an early age.

European skills pledge

The company pledged to train 75,000 European citizens in cybersecurity by February 2027 to strengthen regional digital resilience.

Secure by Design pledge

Fortinet was one of the first companies to sign the CISA Secure by Design Pledge, reinforcing its commitment to embedding security-by-design principles across the product lifecycle.

SBTi validation

The Science Based Targets initiative (SBTi) validated Fortinet's near-term emissions reduction targets, which are aligned with a 1.5°C pathway.

Operation Serengeti

The company supported INTERPOL's Operation Serengeti in Africa, which led to 1,000+ arrests and the dismantling of nearly 135,000 malicious infrastructures.

First product

Fortinet released FortiGate firewall, showcasing the company's cybersecurity innovation.

FortiGuard Labs

The company established FortiGuard Labs to deliver real-time threat intelligence, enabling faster detection and disruption of emerging cyberthreats.

Collective cyber defense

Fortinet co-founded the Cyber Threat Alliance to share threat intelligence with peers, advancing collaborative cybersecurity efforts to combat cybercrime.

Veterans program

Fortinet launched its Veterans program, which delivers free cybersecurity training and certifications to veterans, service members, and military spouses.

CSR function

Fortinet formalized its Corporate Social Responsibility (CSR) function to drive a more structured and strategic approach to sustainability.

First sustainability report

The Fortinet Sustainability Report 2021 (published in 2022) covered ESG priorities in cybersecurity, environment, social impact, and governance.

Product energy efficiency

For the first time, Fortinet disclosed the average reduction in product energy consumption—61% compared to the prior generation—demonstrating progress in energy-efficient product design.

Cybercrime Atlas

Fortinet worked with the World Economic Forum to help launch the Cybercrime Atlas initiative, a collaborative platform that maps cybercriminal activity on a global scale and accelerates coordinated takedowns.

Renewable energy commitment

Fortinet committed to achieving 100% renewable energy use across all owned sites by 2030.

Operation Serengeti 2.0

Fortinet supported INTERPOL-led cybercrime disruption efforts, resulting in 1,200+ arrests, the takedown of more than 11,400 malicious infrastructures, and recovery of \$97.4 million.

Global Cybercrime Bounty program

The company launched a first-of-its-kind Global Cybercrime Bounty program with Crime Stoppers International to strengthen cybercrime deterrence and disruption efforts.

Responsible AI governance

Fortinet established its AI Governance committee and published the company's Principles for Responsible AI Use and Development.

Industry-first EPDs

The company published the cybersecurity industry's first Environmental Product Declarations (EPDs), increasing transparency on product environmental impacts.



*It was initially launched as the Fortinet Learning Center, later renamed the NSE Training Institute and became the Fortinet Training Institute in 2020.

SUSTAINABILITY AT FORTINET

Fortinet's sustainability strategy helps us respond to global trends—from AI and evolving cyberthreats to climate change, new environmental, social, and governance (ESG) regulations, and rising stakeholder expectations. Guided by accountability and transparency, we work across the company and with partners to identify risks and opportunities, strengthen our programs, and drive measurable positive impact.



STRATEGY

Fortinet operates in a world shaped by rapid and constant change—political, regulatory, technological, social, and environmental. The pace and scale of these shifts require agility and foresight, reinforcing the need for companies to act responsibly, transparently, and with long-term value in mind.

Cybersecurity is foundational to modern society and a critical enabler of social and economic resilience. As the world becomes more interconnected and dependent on digital systems, protecting people, devices, and data has never been more essential. Fortinet's mission to secure the digital world positions us at the heart of this transformation. This perspective is reinforced by global risk assessments such as the *World Economic Forum's Global Risks Report 2026*, which ranks cyber insecurity among the top global risks in both the short and the long term—highlighting the growing importance of digital resilience to economic stability and societal trust.

At the same time, increasingly severe weather events and growing resource constraints underscore the urgency of advancing climate mitigation and adaptation, supporting the energy transition, improving product energy efficiency and circularity, and strengthening water stewardship across our operations and value chain.

These priorities sit alongside other critical topics—such as responsible AI, ethical business practices, data privacy, and skills development—that shape our impacts, risks, and opportunities, and strongly influence the expectations of our customers, employees, and the communities we serve.

Stakeholders increasingly expect companies, including Fortinet, to demonstrate positive and measurable contributions across this broad spectrum of topics—to help build secure, sustainable and inclusive digital societies.

In response, Fortinet has established public sustainability goals, including advancing climate action through science-based targets and expanding access to cybersecurity education.

We continually engage with stakeholders to understand their evolving perspectives, and we periodically conduct materiality assessments to validate and refine our priority sustainability topics.

Within Fortinet, sustainability is a shared responsibility embedded across business units. We have established robust governance structures and processes to drive accountability, integrate sustainability into decision-making, and support consistent execution across the company.

Our employees play a central role in bringing this strategy to life. From innovation and product design to customer engagement and community action, their daily work contributes to Fortinet's broader environmental and social purpose. We support this through programs to build awareness, enhance capabilities, and strengthen engagement.

Our sustainability strategy guides how we manage risks and capitalize on opportunities in this dynamic environment. It is informed by and aligned with globally recognized sustainability frameworks and disclosure standards. We focus on four strategic pillars, outlined on this page. Together, these address the broad range of topics that are most relevant to Fortinet and our stakeholders and reinforce our commitment to long-term value creation.

OUR FOUR STRATEGIC PILLARS

SECURING THE DIGITAL WORLD



We work to advance the cybersecurity industry by continuously innovating to protect organizations against evolving cyberthreats. Through collaboration with public and private organizations worldwide, we help combat cybercrime and support customer resilience, contributing to a safer ecosystem for all.

MINIMIZING OUR ENVIRONMENTAL FOOTPRINT



We address the impacts of climate change by minimizing the environmental footprint of our solutions, operations, and broader value chain. Our products drive most of our environmental impacts, so we focus on improving energy efficiency, developing sustainable packaging, and advancing circular solutions that extend product life and reduce waste.

EMPOWERING PEOPLE AND COMMUNITIES



We foster an inclusive workforce within Fortinet and across the industry. By empowering individuals from all backgrounds to reach their full potential and expanding access to cybersecurity education, we help bridge the global cybersecurity talent gap and build a safer, more resilient digital future for all.

We conduct business ethically across our value chain, including respecting human rights, complying with all laws, and ensuring our employees, partners, and others follow our standards. We safeguard our systems and data by embedding responsible AI alongside industry best practices in information security, data protection, and privacy.

STRATEGY
DOUBLE MATERIALITY ASSESSMENT
STAKEHOLDER ENGAGEMENT
SUSTAINABILITY REPORTING AND DISCLOSURES

AWARDS AND RECOGNITIONS



ECOVADIS

Awarded a Committed EcoVadis sustainability badge with a score of 57 (out of 100), ranked in the 51st percentile of all companies

MSCI
ESG
RATINGS



CCC B BB BBB A AA AAA
As of Jan 2026

MSCI

Received a rating of AAA in the MSCI ESG ratings assessment



ISS ESG

Achieved Prime status by fulfilling ISS ESG requirements regarding sustainability performance in our sector



FORBES MOST TRUSTED COMPANIES

Recognized for two consecutive years in the Forbes Most Trusted Companies in America list



SUSTAINALYTICS

Received an ESG Risk Rating of 16 from Sustainalytics and assessed to have a low risk of experiencing material financial impacts from ESG factors



CDP

Received a B score for climate and B- for water security

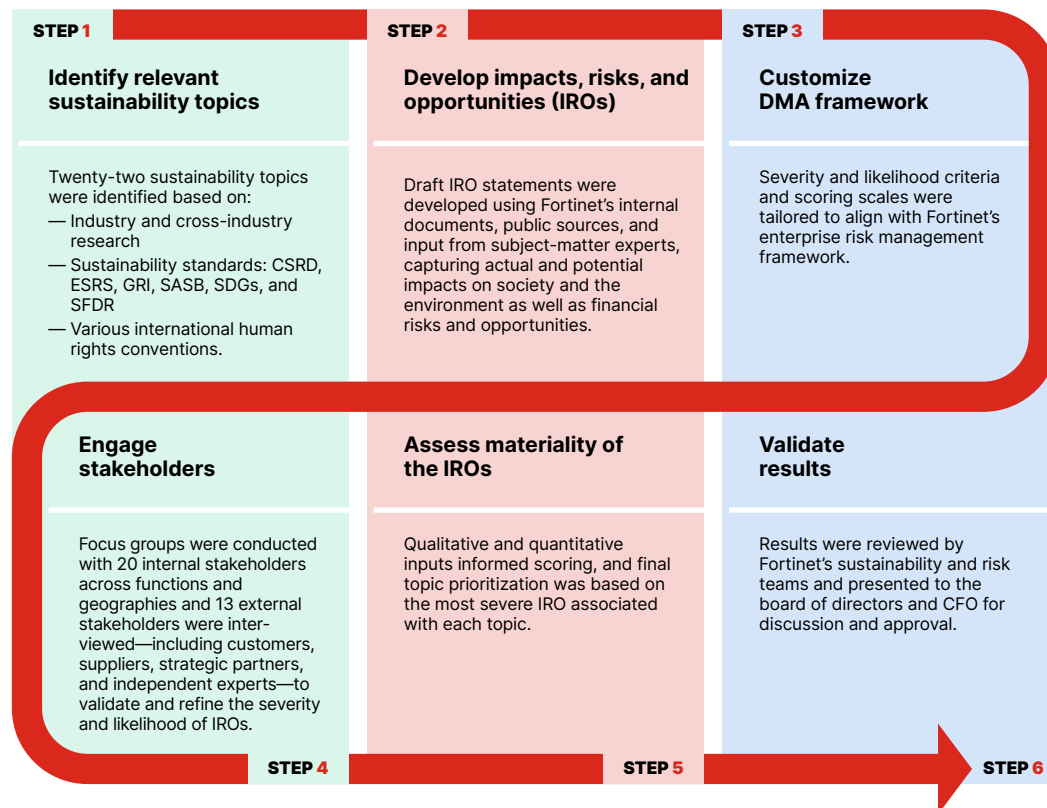


DOUBLE MATERIALITY ASSESSMENT

In 2025, we worked with BSR to conduct a double materiality assessment (DMA) to identify the sustainability topics that are most relevant from both an impact and a financial risk and opportunity perspective. This is an essential input to our [sustainability strategy](#) and disclosure.

Building on the materiality assessments conducted in [2021](#) and [2024](#), the 2025 DMA expanded the scope of analysis by identifying and assessing material impacts, risks, and a opportunities (IROs). This process considered Fortinet's impacts on society and the environment as well as sustainability-related factors that may influence the company's financial performance. The assessment covered our own operations and key upstream suppliers and qualitatively accounted for downstream impacts.

DOUBLE MATERIALITY ASSESSMENT PROCESS



The DMA results inform the continued evolution of Fortinet's sustainability strategy, provide a foundation for sustainability reporting, and support preparedness for future disclosures, including those aligned with the Corporate Sustainability Reporting Directive (CSRD) and other emerging frameworks. To maintain relevance and rigor, we plan to review IROs annually and refresh the DMA approximately every three years.

The priority topics identified through the DMA, along with the corresponding sections of this report, are detailed in the table below. Although business ethics was not identified as a priority topic through the DMA, it remains a core priority for Fortinet, and this report includes extensive information on our programs and progress in that area.

Priority topic	Report section
Climate action	— Climate — Sustainable operations — Sustainable products — TCFD index
Cybersecurity collaboration and public engagement	— Cybercrime disruption — Cybersecurity skills gap — Public policy
Cybersecurity skills gap	— Cybersecurity skills gap
Information security and data privacy	— Information security and data privacy — Responsible AI
Innovation and responsible technology	— Responsible technology — Cybersecurity innovation — Responsible AI — Human rights
Product environmental impacts	— Climate — Sustainable products
Sustainable supply chain	— Supplier engagement — Information security and data privacy — Business ethics — Human rights
Talent acquisition, development, retention, and well-being	— Our people

STAKEHOLDER ENGAGEMENT

We engage with stakeholders across our value chain and use their feedback and insights to advance our sustainability priorities, programs, and performance. Examples of engagement and collaboration include the following:



Customers and channel partners

We communicate Fortinet's sustainability priorities and performance through our annual sustainability report, website, blogs, and partner portal, and respond to ESG-related inquiries through RFPs and periodic sustainability performance reviews with customers and channel partners. Engagement focuses on cybersecurity risk management, data privacy, environmental impacts, ethics, compliance, and digital inclusion. In 2025, demand increased for more frequent ESG disclosures, and we continued collaborating with customers and partners to jointly drive sustainability efforts, including cybersecurity skills development through our certification and awareness programs.



Investors

We engage investors through quarterly earnings calls, analyst events, conferences, and ESG-focused discussions with our top shareholders, with participation from our board of directors, executive team, and investor relations team. These engagements cover long-term sustainability strategy, governance, responsible AI, climate, operational energy use, and product energy efficiency, and deepen our understanding of investors' priorities.



Industry partners

We collaborate with industry peers and multi-stakeholder organizations to strengthen global resilience. In 2025, we continued working with organizations such as Cyber Threat Alliance (CTA), the International Criminal Police Organization (INTERPOL), the World Economic Forum, and national Computer Emergency Response Teams (CERTs) to share actionable threat intelligence, disrupt cybercrime, and support initiatives to close the global cybersecurity skills gap.



Employees

We engage our employees through ongoing sustainability awareness campaigns, employee resource groups, the ambassadors and allies network, and FortIdeas (an internal idea generation tool). Training programs build knowledge across business ethics, compliance, responsible AI, information security, and environmental topics. In 2025, we launched the Fortinet CSR Ambassador program and delivered targeted sustainability training to embed responsible practices into daily work.



Supply chain

Supplier engagement is embedded in our due diligence processes and includes risk assessments, audits, and performance monitoring. A significant portion of our environmental footprint occurs in our supply chain, so we work closely with suppliers to communicate our requirements, improve transparency, and support continuous improvement.



Government and regulators

We engage in public policy advocacy to advance the interests of Fortinet, our customers, and other stakeholders, with a primary focus on smart government policies that ensure or enable strong cyber resilience across the economy. We work with international, regional, and national authorities to exchange threat intelligence, address emerging cyber risks, and support coordinated efforts to disrupt cybercrime and protect critical infrastructure and communities.



Communities, schools, and NGOs

We collaborate with communities, schools, and NGOs to advance digital inclusion, women's empowerment, and sustainability. In 2025, collaborations with Women in Cybersecurity (WiCyS), WOMCY, and Women4Cyber helped expand access to cybersecurity education and worked to develop talent pipelines. Through the Fortinet Academic Partner program, we also donated hardware to universities and launched 110 new academic partnerships, enhancing hands-on learning and workforce development opportunities.

EMPLOYEE AWARENESS AND ENGAGEMENT

In 2025, we continued to embed sustainability into Fortinet's organizational culture, raising awareness and empowering employees to drive change.

We help our employees expand their knowledge in numerous ways:

— Sustainability e-learning

We offer voluntary e-learning modules on Fortinet's sustainability approach, product environmental impacts, ecolabels, and other topics to help our employees discuss sustainability with colleagues, prospects, and customers. In 2025, more than 900 employees completed at least one sustainability e-learning module, an 18% year-over-year increase. These modules are integrated into our onboarding programs and selected role-based programs, supporting growing employee awareness and engagement on sustainability topics.

— Company-wide awareness campaigns

We run periodic awareness campaigns to educate Fortinet employees about critical environmental and social topics. In 2025, campaigns focused on plastics reduction, climate action, LGBTQIA+, and well-being and mental health.

— Sustainability monthly digest

Our monthly newsletter, available to all employees, provides updates on Fortinet's sustainability highlights, industry news, sustainability-related tools, ESG reporting and regulations, and other information.

— Additional resources and engagement opportunities

Employees access information through regional human resources newsletters, CSR blog posts, quarterly all-hands meetings, and our [ESG Resource Center](#).

We also engage employees through onboarding, the CSR Ambassador program (see box), [employee volunteering projects](#), [employee resource group activities](#), [product donation initiatives](#), training and the CSR Champions video series, which showcases how our CSR Champions committee advances sustainability and drives progress.



In 2025, the Events team integrated sustainability into corporate events by reducing waste, optimizing energy use, and applying environmentally conscious sourcing practices (see [Fortinet Accelerate 2025: A low-impact global event](#)). In addition, the IT team advanced its global laptop donation program; all regions now donate used devices to NGOs that support digital inclusion.

CSR AMBASSADOR PROGRAM

In 2025, we launched the Fortinet CSR Ambassador program to empower our sales and systems engineer teams to communicate confidently about our sustainability strategy, initiatives, and achievements with customers, partners, and prospects. These ambassadors act as local champions, promoting Fortinet's CSR efforts, integrating sustainability into customer conversations, and providing feedback on regional expectations and engagement opportunities.

The program began with a pilot in Europe, engaging 35 ambassadors to test content, gather insights, and refine the approach before broader rollout.

To support our CSR Ambassador network, we introduced the CSR Ambassador Platform, offering interactive learning resources—including on-demand training modules, quizzes, and monthly challenges—to build knowledge and track progress. The platform also provides collaboration spaces for ambassadors to connect with one another, exchange best practices, highlight successes, and share insights from customer and team interactions, helping to refine Fortinet's CSR content and strategy.



SUSTAINABILITY REPORTING AND DISCLOSURES

Fortinet continually enhances its sustainability reporting practices by aligning with globally recognized disclosure frameworks, including:

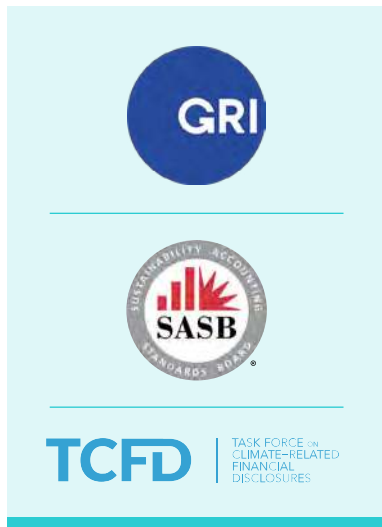
- Global Reporting Initiative (GRI) Standards
- Sustainability Accounting Standards Board (SASB) Standards
- Task Force on Climate-related Financial Disclosures (TCFD)
- United Nations Global Compact (UNGC)
- CDP

Our [GRI](#), [SASB](#), and [TCFD](#) indices are included in the Appendix of this report. This 2025 Sustainability Report also serves as Fortinet's annual Communication on Progress under the UN Global Compact.

Sustainability-related regulations and disclosure requirements, along with stakeholder expectations, continue to increase globally, and Fortinet is adapting to this evolving landscape. This aligns with industry trends and reflects our commitment to transparency.

In 2025, we expanded the scope and quality of sustainability-related data captured across our operations. Nineteen additional electric and natural utility accounts were onboarded into our energy management and reporting tools, increasing the total number of sites with measured energy data to 48. This enhances the completeness and accuracy of the information we report.

Our [ESG Resource Center](#) contains additional sustainability-related information, including past sustainability reports, EEO-1 disclosures, board of directors charters, codes of conduct, sustainability policies, product certifications, and regulatory environmental product compliance details.



UNITED NATIONS SUSTAINABLE DEVELOPMENT GOALS

The United Nations Sustainable Development Goals (SDGs) provide an essential global framework for driving social, environmental, and economic progress. Fortinet has identified seven SDGs on which it can have a positive impact, as noted in the graphic. Throughout the report, we indicate where the content aligns with these goals.



SECURING THE DIGITAL WORLD

As cyberthreats grow in scale and impact, Fortinet works continually to reduce risks to people, organizations, and society. Through ongoing cybersecurity innovation, responsible security practices, and collaboration with public and private organizations worldwide, we help protect against evolving cyberthreats, strengthen customer resilience, and support efforts to combat cybercrime—contributing to a safer, more resilient digital ecosystem for all.

2025 HIGHLIGHTS

Contributed to **INTERPOL-led Operation Serengeti 2.0**, which achieved:

11,400+ malicious infrastructures disrupted

1,200+ cybercriminals arrested

Launched **Global Cybercrime Bounty program**

15+ years of experience applying AI

192,000+ members of the Fortinet Community



RESPONSIBLE TECHNOLOGY
CYBERSECURITY INNOVATION
CYBERCRIME DISRUPTION
CUSTOMER SUCCESS ENABLEMENT

RESPONSIBLE TECHNOLOGY

At Fortinet, responsible technology is central to our mission to secure the digital world. We embed secure-by-design and secure-by-default principles into every stage of the product lifecycle, from initial concept and R&D through development, deployment, and end-of-life management. This proactive approach ensures that products are secure by default, not as an afterthought, helping Fortinet and our customers navigate the rapidly evolving cyberthreat landscape.

Cybercriminals increasingly leverage AI, automated attack kits, and other sophisticated tools to exploit vulnerabilities at scale. By embedding security into the design of every product, Fortinet reduces systemic risk while meeting stakeholder expectations worldwide for certifications, regulatory compliance, and responsible disclosure.

The Fortinet approach



Secure product design lifecycle covers every stage, from design through end of life.



Security is baked into the product from first conception.



Strong product scrutiny at all stages of the product development lifecycle, internal and external.



Rapid remediation with a transparent incident response plan.



Operating as a partnership with our customers, transparently sharing information and feedback.



Collaborating with the industry to develop and implement stronger standards for the benefit of all our customers.

WHY CYBERSECURITY MATTERS FOR SOCIETY

The accelerating scale and economic impact of cyberthreats have made cybersecurity a societal imperative. Global risk assessments, including the [World Economic Forum's Global Risks Report](#), consistently rank cyberthreats among the most significant challenges facing governments, businesses, and communities. As critical infrastructure, public services, and daily life become increasingly digital, the resilience of these systems directly influences societal stability.

Cyberattacks have consequences far beyond the technical domain. They can disrupt essential services, compromise public safety, and erode trust in institutions—impacting citizens, communities, and entire economies.

The increasing interconnection of systems further amplifies these risks, creating an environment where a single vulnerability can ripple across sectors.

Fortinet's mission is to secure people, devices, and data everywhere, enabling society to thrive. Through product innovation, responsible technology, collaboration to combat cybercrime, and customer engagement to build resilient digital environments, we help make secure technology a foundation for sustainable development and long-term societal well-being.

Michael Xie
Fortinet co-founder,
president, and CTO



SECURE PRODUCT DEVELOPMENT LIFECYCLE

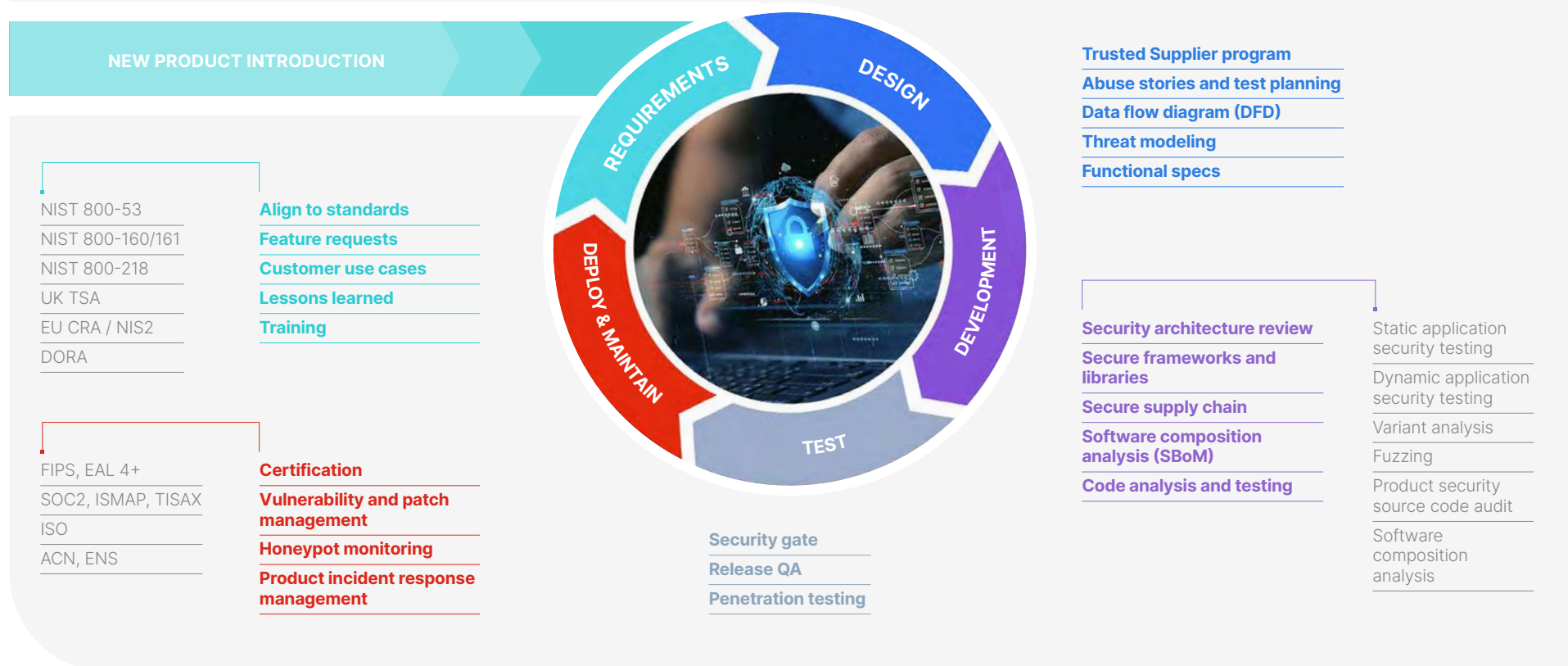
Our Secure Product Development Lifecycle Policy ensures security is embedded from inception and maintained through all product stages. This encompasses secure development practices, in-house development of system-on-a-chip application-specific integrated circuits (ASICs), and rigorous selection and qualification of manufacturing partners through our Trusted Supplier program.

Independent third-party penetration testing and continuous risk assessments are conducted to validate compliance with the highest security standards. We maintain over 90 information security certifications, with our product portfolio continuing to grow, demonstrating our commitment to transparency and trust. More information is available in the Fortinet Trust Resource Center.

Our Information Security and Product Security teams collaborate closely with Fortinet R&D to test, provide feedback, and re-test products, confirming compliance before release. Fortinet applies secure product development best practices aligned with leading industry standards and global regulatory expectations.

Fortinet also published its CISA Secure Product Development attestation on the DHS Repository for Software Attestations and Artifacts portal).

FORTINET SECURE PRODUCT DEVELOPMENT LIFECYCLE



RESPONSIBLE TECHNOLOGY
CYBERSECURITY INNOVATION
CYBERCRIME DISRUPTION
CUSTOMER SUCCESS ENABLEMENT

INCIDENT RESPONSE AND VULNERABILITY MANAGEMENT

Fortinet's ability to help customers operate securely depends on the integrity of our own products and the transparency of our security processes. The Fortinet Product Security Incident Response Team (PSIRT) is central to this commitment. PSIRT oversees vulnerability intake, analysis, remediation, and disclosure across all Fortinet solutions, following globally recognized guidelines, including ISO/IEC 29147 (Vulnerability Disclosure) and ISO/IEC 30111 (Vulnerability Handling Processes).

This work is governed by Fortinet's publicly available [Product Security program](#), which defines our approach to product security, vulnerability handling, and responsible disclosure, and is adhered to across the organization.

In 2025, we continued to strengthen our vulnerability management program by expanding internal auditing, deepening industry collaboration, and investing in new mechanisms to enhance transparency and stakeholder trust.

Proactive identification and responsible remediation

Proactive identification remains a cornerstone of Fortinet's vulnerability management strategy. In 2025, 56% of Fortinet vulnerabilities were proactively identified internally through our rigorous auditing process. These internal controls reduce customer risk and shorten remediation timelines by addressing issues before they are observed or exploited externally.

Across all products and geographies, PSIRT ensures consistent and efficient handling of vulnerabilities—from intake through remediation and communication—using standardized workflows, severity scoring processes, and cross-functional collaboration with engineering, product management, and technical support teams.

Collaboration with the security research community

Fortinet engages with the security research ecosystem globally to improve collective cyber resilience. As a long-standing member of the Forum of Incident Response and Security Teams (FIRST), we participate in information sharing, best practice incident handling, and coordinated vulnerability disclosure. This collaboration also helps us align Fortinet's processes with standards globally and ensure consistent, responsible communication with customers.

In 2025, we enhanced Fortinet's external collaboration by launching a private bug-bounty program in partnership with HackerOne, supported by a reward pool of up to \$1 million. This initiative engages a select group of ethical hackers to identify and responsibly report vulnerabilities, strengthening our overall security posture. We plan to expand the program to the public in 2026.

Transparent communication

Customers, partners, and regulators all expect transparent and timely communication. We publish all resolved, security-related vulnerabilities—whether identified internally or externally—through multiple channels, notably our [Monthly Vulnerability Advisory](#), issued on the second Tuesday of each month. These advisories summarize remediated vulnerabilities, affected products, available patches, and guidance for customers and partners. In addition to formal advisories, Fortinet maintains open communication through:

- The [Fortinet PSIRT portal](#), providing up-to-date vulnerability disclosures, remediation guidance, and severity assessments.
- The [Fortinet Community](#), offering troubleshooting resources, peer-to-peer support, and expert commentary.

- The [Fortinet PSIRT blog](#), sharing timely insights on emerging threats, vulnerability trends, and security best practices.

Through these practices, Fortinet aims to maintain the highest level of transparency, enabling customers to take prompt action and maintain a strong security posture.

In 2025, we also led the development and rollout of the [CTA Responsible Vulnerability Communication Policy](#), a cross-industry framework that enhances ecosystem-wide coordination and supports timely, systematic, and responsible disclosure practices. [Learn more](#) about our collaboration with CTA.

2025 IMPACT AT A GLANCE

56%

of vulnerabilities were identified internally

Launched

\$1M

HackerOne private bug-bounty program

Participated actively in

FIRST

Led the CTA Responsible Vulnerability Communication

Policy

A common misconception is that a larger number of vulnerabilities reported publicly is a sign of weaker security. In reality, every IT product has vulnerabilities—over 48,000 CVEs were published in 2025, up 20% since 2024. A higher percentage of internally identified vulnerabilities reflects stronger security practices, as it shows that a company is actively testing its own products and proactively finding issues rather than relying on others to do so. The real measure of security is not the number of vulnerabilities, but how quickly and transparently a company identifies, communicates, and fixes them to protect customers.



Carl Windsor
CISO and member of the
CSR committee at Fortinet

CISA SECURE BY DESIGN PLEDGE

Fortinet was among the first cybersecurity companies to sign the CISA Secure by Design Pledge, committing to actionable steps across seven key areas (see table) to strengthen secure product development globally. This pledge complements our existing secure product development practices and reinforces our leadership in delivering resilient technologies. We are committed to achieving ongoing, measurable improvements and to regularly publishing progress toward the Secure by Design Pledge. [Learn more.](#)

Secure by Design Pledge area	Fortinet progress in 2025
Increase the use of multi-factor authentication (MFA)	Enabled MFA for all Fortinet customer cloud accounts, with 95% adoption of MFA safeguards
Reduce default passwords	Deprecated default passwords in Fortinet's Secure Development Lifecycle Policy; all products now require unique passwords during installation
Reduce prevalence of entire classes of vulnerability	Continued ongoing engineering initiative targeting systemic removal of vulnerability classes such as SQL injection and buffer overflows
Increase the installation of security patches	Approximately 1.5 million devices updated using the auto update feature since its introduction in 2024
Publish a vulnerability disclosure policy (VDP)	Maintained public VDP via the Fortinet PSIRT Policy page and Security.txt , ensuring consistent and accessible disclosure information
Demonstrate transparency in vulnerability reporting	Continued radical transparency program for common vulnerability and exposure (CVE) publication and communication, including common weakness enumeration and common platform enumeration fields in every Fortinet CVE, and comprehensive monthly advisories
Demonstrate increased customer ability to gather evidence of cybersecurity intrusions affecting the manufacturer's products	Introduced file system integrity checking features in FortiOS 7.4.4 and later versions to detect and log unauthorized file changes or additions

CYBERSECURITY INNOVATION

For 25 years, Fortinet has been at the forefront of cybersecurity innovation, helping organizations, communities, and critical infrastructure operate securely through waves of technological disruption. Since our founding in 2000, we have anticipated and addressed every major shift in the digital landscape—from the rise of cloud computing and bring your own device, to remote work, AI-driven operations, and the early emergence of quantum computing. Each transition has introduced new opportunities and increasingly sophisticated cyber risks, reinforcing the need for adaptive and integrated security.

Fortinet's innovation philosophy is grounded in building technologies that strengthen societal resilience while enabling customers to embrace digital transformation with confidence. From the beginning, this approach has been driven by engineering excellence—most notably through our proprietary ASIC technology. By designing specialized security processing units (SPUs), Fortinet pioneered a breakthrough in cybersecurity performance, enabling high-speed threat protection with significantly lower energy consumption than traditional processors. This advancement laid the foundation for a more scalable and sustainable model of security innovation.

Over two decades, Fortinet has expanded from offering next-generation firewalls (NGFWs) to delivering a comprehensive, integrated cybersecurity platform. Today, the Fortinet Security Fabric—our unified platform integrating more than 30 networking and security functions—is central to this evolution. Powered by FortiOS, supported by over 50 products, and enhanced through open APIs and a global ecosystem of technology partners, the Security Fabric enables customers to enhance protection while maximizing existing infrastructure. Through continuous product innovation, Fortinet also focuses on improving energy efficiency across product generations, helping customers strengthen cybersecurity while optimizing energy use. In 2025, our Fabric-Ready Technology Alliance Partner program surpassed 3,000 integrations, demonstrating broad adoption and collaboration across the cybersecurity ecosystem.

3,000+

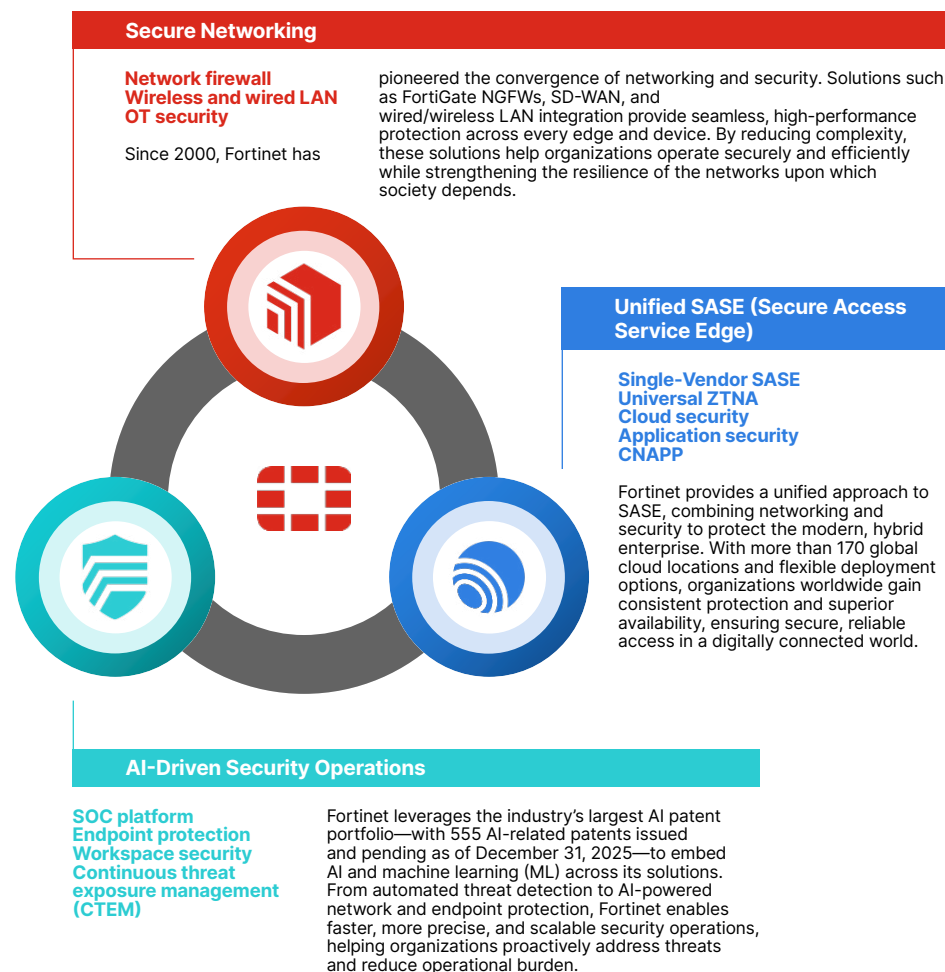
tech integrations

400+

Fabric-Ready partners
(one of the industry's
largest ecosystems)

OUR APPROACH: THREE PILLARS OF INNOVATION

Fortinet's innovation strategy has three complementary pillars, which together deliver holistic cybersecurity for organizations and society.



2025 MAJOR PRODUCT LAUNCHES AND ENHANCEMENTS

In 2025, Fortinet continued to expand its legacy of innovation, delivering solutions that protect organizations, critical infrastructure, and communities worldwide. Major highlights include:

Preparing for the quantum future

Fortinet advanced [quantum-safe security capabilities](#), helping organizations protect long-lived, mission-critical data against future quantum-enabled threats. Innovations include the deployment of post-quantum cryptography algorithms such as NIST-approved ML-KEM and emerging protocols (BIKE, HQC, Frodo), hybrid encryption methods, and [Secure AI data center](#) solution that integrates AI infrastructure protection with quantum-safe security.

Embedding AI across security operations

Fortinet continues to embed AI across the Fortinet Security Fabric to strengthen threat detection, accelerate response, and simplify network operations.

In 2025, the expansion of FortiAI introduced new capabilities through [FortiAI-Assist](#), delivering agentic and autonomous AI that automates network operations—such as configuration validation, optimization, and troubleshooting—as well as security operations, including alert triage, adaptive threat hunting, and contextual threat enrichment.

Fortinet also advanced AI-driven protection with [FortiAI-Protect](#), an AI/ML-powered intrusion prevention system designed to stop ransomware earlier in the attack lifecycle. Using adaptive, behavior-based detection, FortiAI-Protect identifies and blocks command-and-control (C2) frameworks, and limits lateral movement, reducing the risk of data theft and extortion.

Complementing these innovations, [FortiAnalyzer](#) evolved into a turnkey AI-driven platform that delivers real-time visibility, actionable insights, and automated responses, helping organizations shift from reactive defense to proactive cyber resilience.

High-performance and resilient security infrastructure

In 2025, Fortinet pushed the boundaries of secure networking performance with the launch of the [FortiGate 3800G series](#), one of the most powerful compact firewall platforms in its class. Delivered in a three-rack-unit form factor and delivering 200 Gbps of threat protection throughput, the FortiGate 3800G enables large enterprises, data centers, and service providers to secure massive traffic volumes without compromising performance or space efficiency.

Fortinet introduced key hardware-level innovations embedded into FortiGate systems:

- [FortiSentry](#) provides continuous silent monitoring to detect signs of intrusion or tampering.
- [Blackbox](#) continuously records system health metrics, network events, and anomalies with encrypted, secure retention. Collecting historical data accelerates incident root-cause investigation and resolution, reducing downtime and eliminating gaps caused by missing system information.

Delivering high-performance security for distributed enterprises

The FortiGate 700G series delivers high-security performance across branch offices, remote sites, and distributed enterprise networks. Designed for edge deployments, these NGFWs provide strong threat protection and high throughput while consuming seven times less energy per gigabit of traffic, helping organizations scale securely while reducing operational and environmental impact.

Protecting the modern digital workplace

Fortinet introduced a [new AI-powered Workspace Security suite](#) to safeguard email, collaboration tools, cloud applications, and shared documents. By stopping phishing, business email compromise, malware, and data leakage, the suite ensures secure employee collaboration—a key component of protecting sensitive information in hybrid work environments.

Enhancing cloud and identity security

[FortiCloud](#) enhancements provide secure identity management, communication, and data storage across hybrid and multicloud environments, supporting safer access for employees, customers, and partners.

Securing critical infrastructure and industrial operations

Fortinet expanded its [OT Security Platform](#) with ruggedized solutions and secure connectivity to enhance cyber resilience for industrial systems, utilities, and critical infrastructure worldwide.

FORTIGATE RUGGED FIREWALL RECOGNITIONS

In 2025, the FortiGate Rugged series earned two major industry accolades: the prestigious Red Dot Product Design Award for its purpose-built design, and the Control Engineering Product of the Year—Gold in the Safety & Security category—for the FortiGate Rugged 70G-5G Dual model. Built to operate in demanding, industrial-edge environments—from remote energy substations and manufacturing facilities to transportation systems and utility control centers—these devices feature a fanless, ruggedized design that resists dust, moisture, shock, vibration, and extreme temperatures.



reddot winner 2025



CULTURE OF INNOVATION

Fortinet fosters a company culture that encourages and rewards innovation. The company makes significant investments in R&D, ensuring the continuous advancement of cybersecurity technologies. Each year, our R&D team files approximately 60–80 patent applications, bringing the total to 1,405 issued patents and 365 pending applications as of the end of 2025.

Fortinet champions a culture of innovation by engaging employees at all levels and fostering collaboration with customers to continually improve our offerings. This includes:

- **FortiHours:** R&D team members can dedicate time to crafting new ideas or tools, with support and guidance from management.
- **FortiIdeas:** Any employee can submit product concepts and company suggestions to Fortinet's Innovations Council.
- **Patent submission system:** Employees can submit potentially patentable innovations to a patent review board.
- **New feature request process:** Employees can propose new product features through the New Feature Request (NFR) process. In 2025, over 3,600 NFRs were submitted, with 39% implemented or in progress.

— Customer engagement programs:

Through its Customer Advisory Boards and Xperts Academy, Fortinet periodically invites VIP customers from various sectors (OT, finance, healthcare, etc.) to generate ideas, identify new perspectives, and provide feedback directly to our CTO.

— Customer Quality Excellence Board:

In 2025, Fortinet launched a customer-facing Quality Excellence Board that brings together strategic customers, including large ISPs and very large enterprises. The Board provides direct, structured feedback to Fortinet's executive leadership, helping guide product quality, performance, and innovation priorities based on real-world cybersecurity needs.

\$815M

investment
in R&D in 2025

1,400+

patents issued

6

new products
and services
introduced in 2025

CYBERSECURITY INDUSTRY ADVANCEMENT

As a key part of Fortinet's innovation journey, the company embraces disruptive technologies and collaborates externally to advance the cybersecurity industry.

Artificial intelligence

Fortinet has leveraged AI for more than 15 years to enhance cybersecurity, optimize operations, and deliver more robust protection to customers. Beginning with early ML models used to identify threats and automate responses, AI has become foundational to the Fortinet Security Fabric, enabling real-time analysis across networks, endpoints, and cloud environments. FortiGuard Labs also uses advanced AI techniques to identify and mitigate emerging threats faster than traditional approaches. Across our portfolio, AI is embedded into Fortinet products, from predictive threat intelligence to AI-driven analytics to enhance operational efficiency. With more than 550 AI-related patents issued and pending, AI was at the core of our 2025 product innovations ([see 2025 major product launches and enhancements](#)).

In 2025, Fortinet's AI leadership extended beyond product development to active participation in global research and collaboration initiatives. Highlights during the year included our collaboration with UC Berkeley on the AI-enabled cybercrime tabletop exercise (TTX) series, as well as AI-enabled cybercrime workshops in Singapore, in partnership with Nanyang Technological University, and in Israel, bringing together academic institutions, government agencies, and private-sector experts. These engagements focused on simulating emerging AI-driven threats, sharing knowledge, and strengthening collaborative approaches to safeguard organizations and society from malicious AI use.

We also supported additional industry initiatives in 2025, including [INTERPOL CyberEX](#), where we provided expertise on emerging AI-related threats such as deepfakes to help strengthen global efforts to detect, deter, and disrupt cybercrime.

Through our collaboration with the World Economic Forum, we also contributed to the whitepaper [Artificial Intelligence and Cybersecurity: Balancing Risks and Rewards](#), which offers a clear perspective and actionable recommendations for managing the cyber risks associated with AI adoption. In addition, we supported the development of the World Economic Forum [AI at Work](#) paper, released at Davos 2026, helping to shape global guidance on responsible AI adoption.

Through these collaborations, Fortinet advances collective understanding of AI-enabled threats and contributes to a safer, more resilient digital ecosystem worldwide.

550+

AI-related
patents issued
and pending
(as of Dec. 31,
2025)



Pioneering AI
in Cybersecurity

15+

Years of Experience
Applying AI

RESPONSIBLE TECHNOLOGY
CYBERSECURITY INNOVATION
CYBERCRIME DISRUPTION
CUSTOMER SUCCESS ENABLEMENT

Quantum-safe readiness: securing the future

The day when quantum computers become a reality and pose a risk to our current encryption standards is not far away. In the meantime, the threat of “harvest now, decrypt later” attacks poses a significant risk to organizations with sensitive, long-lived data in sectors such as government, financial services, telecommunications, and healthcare. Fortinet is at the forefront of quantum-safe cybersecurity, helping organizations prepare for next-generation threats while advancing industry readiness.

In 2025, we enhanced FortiOS capabilities to enable organizations to deploy post-quantum cryptography (PQC) algorithms, combine multiple encryption methods for robust protection, and transition smoothly to quantum-safe standards. Supported algorithms include NIST-approved ML-KEM and emerging protocols such as BIKE, HQC, and Frodo. [Learn more](#). These enhancements enable customers using FortiGate NGFWs and Fortinet Secure SD-WAN to begin adopting quantum-resistant security with minimal disruption to their existing environments.

FortiOS also introduced support for hybrid PQC and quantum key distribution (QKD) deployments, algorithm stacking, and post-quantum cryptography for agentless VPN, with new CLI options that allow administrators to select quantum-resistant algorithms, helping future-proof VPN infrastructure against coming cryptographic threats. Quantum-safe readiness is available to our customers at no additional cost.

Beyond product innovation, we are helping to advance industry awareness and preparedness for the quantum era. In 2025, Fortinet was named a Leader in the [2025 Gartner® Magic Quadrant™ for Hybrid Mesh Firewall](#), with specific recognition for its early focus on PQC across its portfolio. This underscores our leadership in embedding quantum-safe capabilities into real-world security platforms.

Fortinet also contributes to thought leadership in this space. In 2025, we co-authored the report [Approaching Quantum Dawn: Closing the Cybersecurity Readiness Gap Before It's Too Late](#), which offers organizations guidance on assessing risks, modernizing cryptography, and building a roadmap for quantum-resilient security. Through this work, we are helping customers and the broader ecosystem move from awareness to action.

To accelerate the adoption of quantum-safe security, we continued to expand our ecosystem of strategic partnerships in 2025. This included a new collaboration with QuintessenceLabs to deliver a joint quantum-enhanced cybersecurity solution that integrates quantum-enhanced key security and encryption technologies with Fortinet infrastructure. The solution combines PQC and QKD to help organizations strengthen the protection of sensitive data while minimizing operational disruption. Fortinet also continues to work with established partners, including Toshiba and ID Quantique, to advance QKD capabilities.

Later in the year, we also announced an expansion of our open partner ecosystem with [TELSY](#), the cybersecurity company of the TIM Group, to enable European Telecommunications Standards Institute (ETSI)-compliant quantum-safe solutions to protect the critical data of governments and other organizations, as well as critical infrastructure against emerging threats related to quantum computing.

This partnership brings together TELSYP's expertise in secure communications and cryptography and Fortinet's network and security platforms to support the deployment of quantum-safe QKD solutions, helping organizations prepare for future quantum threats while addressing today's security requirements.

We further broadened our quantum-safe portfolio in 2025 with the introduction of the [Secure AI Data Center solution](#), which integrates protections for AI infrastructure—including data, applications, and large language models—alongside quantum-safe security based on PQC and QKD.

By embedding quantum-safe technologies into our core products, contributing to industry research, and collaborating with leaders in quantum innovation, Fortinet is moving beyond theoretical readiness to deliver practical, affordable, deployable, and scalable solutions. This helps organizations strengthen long-term cyber resilience and safeguard the digital systems on which society depends against modern threats.



CONTRIBUTING TO GLOBAL CYBERSECURITY LEADERSHIP

In 2025, Fortinet extended its role in advancing cybersecurity for society by contributing to global leadership dialogues and cross-sector collaboration. We provided expertise to the World Economic Forum's [Elevating Cybersecurity: Ensuring Strategic and Sustainable Impact for CISOs](#) report, which explores how organizations can embed cybersecurity as a strategic driver of resilience, trust, and sustainable value creation.

We also support cybersecurity leadership communities through platforms such as the CISO Collective, enabling peer-to-peer knowledge exchange on emerging threats, risk governance, and cyber resilience across industries. These initiatives reflect our commitment to collaborative approaches that strengthen the global cybersecurity ecosystem and support informed, strategic decision-making. [Learn more about the CISO Collective.](#)

CYBERCRIME DISRUPTION

Cybercrime is evolving at an unprecedented pace, fueled by increasingly sophisticated criminal groups that leverage advanced tools including weaponized AI, global networks, and business-like coordination. No matter how prepared any single organization may be, no company can defend society alone. Cybersecurity is a shared responsibility requiring collaboration across the entire digital ecosystem.

For 25 years, Fortinet has played a leading role in strengthening global cyber resilience. Through long-standing partnerships with international law enforcement, Computer Emergency Response Teams (CERTs), and cross-industry alliances—many of which we helped establish—Fortinet takes a prominent position in advancing collective cyber defense. We provide critical expertise, intelligence, and operational support to help mitigate and disrupt cybercrime at scale.

OUR GLOBAL ENGAGEMENT MODEL

Fortinet collaborates with academia, global institutions, and law enforcement to drive a systemic approach to cybercrime disruption. Our efforts focus on:

Public-private partnerships

We maintain deep collaboration with organizations worldwide—including the CTA, INTERPOL, Crime Stoppers International (CSI), the World Economic Forum, government agencies, national CERTs and other multi-stakeholder alliances—to share actionable threat intelligence and coordinate to disrupt cybercriminal activities.

In 2025, we expanded these partnerships to strengthen information sharing, improve incident-response capabilities, and contribute expert analysis to joint mitigation initiatives.

Threat intelligence sharing

Through automated analysis and expert human validation, we deliver real-time insights into emerging malware families, threat actor behaviors, and potential vulnerabilities. Our threat intelligence contributes to global early-warning systems, cross-border investigations, and coordinated takedown operations. By enabling earlier detection and faster, synchronized defensive actions, we help improve security outcomes for governments, businesses, and communities. For a detailed analysis of current trends, read the [2025 Fortinet Global Threat Landscape Report](#).

Disruption of criminal organizations

We support law enforcement in high-impact efforts to map cybercriminal ecosystems, identify perpetrators and support disruption operations. This includes takedowns of malicious infrastructure, dismantling of criminal networks, and seizures of cybercrime infrastructure. These collaborative actions reduce harm to victims and increase the costs and risks for cybercriminal organizations.

Global cyber policy and capacity-building

We participate in leading multi-stakeholder initiatives, such as the World Economic Forum's Centre for Cybersecurity and INTERPOL Gateway, to advance responsible, secure digital ecosystems. By sharing knowledge and taking on leadership roles, we help shape global policy frameworks and operational norms that reinforce systemic approaches to combating cybercrime.

WHY COLLABORATION MATTERS

Cyber adversaries are rapidly adopting automation, generative AI, and Cybercrime-as-a-Service (CaaS) models. Tools such as FraudGPT and voice-cloning technologies are enabling criminals to create more convincing phishing lures, deepfake videos, and impersonation campaigns. At the same time, dark-web marketplaces now offer turnkey attack kits, access to compromised systems, and stolen credentials—lowering the technical barriers for would-be attackers. Criminal networks increasingly blend cyber and physical crime, including human trafficking linked to scam farms, adding new layers of complexity and societal impact. These escalating dynamics make real-time, cross-sector collaboration essential.

Fortinet works closely with international partners to map the cybercriminal ecosystem, identify systemic choke points, disrupt malicious operations, and support accountability and deterrence models by identifying and prosecuting threat actors. These joint efforts help protect individuals, communities, public institutions, critical infrastructure worldwide, and society—while also helping victims recover.

Derek Manky
Chief security strategist & global VP threat intelligence and member of the CSR committee at Fortinet



FORTIGUARD LABS: ADVANCING GLOBAL THREAT INTELLIGENCE

Founded in 2002, FortiGuard Labs is Fortinet's elite cybersecurity threat intelligence and research organization. A pioneer and innovator in the security industry, FortiGuard Labs develops and applies advanced ML and AI technologies to deliver real-time protection and actionable threat intelligence. The team works with law enforcement agencies, government organizations, and security vendor alliances worldwide to strengthen coordinated responses to global security risks.



Cybersecurity Leadership Award

For excellence in cybercrime awareness, prevention, and data protection



Corporate Leadership in Crime Prevention Award

For advancing safety and prevention through awareness initiatives, workforce development, and responsible technology innovation

[Learn more](#)

The challenge

- AI-powered attacks
- Deepfakes and voice cloning
- Cybercrime-as-a-Service
- Dark-web economy
- Convergence of cyber and physical crimes

Our collaborative approach

1 Build the ecosystem



2 Share actionable intelligence

- Real-time, contextualized threat intelligence
- Outbreak alerts
- Joint analysis and reporting
- Early-warning intelligence advisories

3 Disrupt criminal operations

- Coordinated infrastructure takedowns
- Seizure of illicit cryptocurrency
- Support of multi-agency investigations
- Intelligence that leads to the arrest of threat actors

4 Strengthen global policy

- Contributions to cyber norms
- Operational models for collective defense
- Capacity-building programs



Powered by FortiGuard Labs

2025 impact:

- **Trillions** of events analyzed daily
- **Millions** of global sensors
- **500+** researchers and analysts
- **48** threat signals
- **23** outbreak alerts
- **30+** threat actors mapped

Community impact

- Accelerated disruption of global cybercrime
- Stronger protective posture for critical sectors
- Reduced risks to people, organizations, and communities, including through the seizure of illicitly gained funds

GLOBAL CYBERCRIME BOUNTY PROGRAM: A FIRST-OF-ITS-KIND COLLABORATION

Fortinet and Crime Stoppers International (CSI) launched the groundbreaking Global Cybercrime Bounty program, creating the world's first anonymous, citizen-powered platform dedicated to reporting cybercriminal activity. This initiative bridges CSI's trusted, anonymous crime-reporting infrastructure with Fortinet's global threat intelligence and cybersecurity expertise to accelerate action against cybercrime.

Through the program, individuals worldwide can submit information about cyberthreats safely and anonymously. Fortinet analyzes and validates submissions and, where appropriate, works with law enforcement partners to support investigations and accountability efforts.

The partnership strengthens global cyber resilience by:

- **Enhancing public-private collaboration** by mobilizing communities to surface intelligence on fast-moving and converged cyber-physical crime.
- **Scaling disruption** of cybercriminal networks through rapid, actionable threat information.
- **Fusing threat intelligence** to validate tips and reduce strain on law enforcement resources, enabling more effective operations at scale.
- **Advancing deterrence and accountability** by increasing the likelihood of detection and accountability for threat actors.

THREAT ACTOR ENCYCLOPEDIA

Launched in 2025 and powered by FortiGuard Labs, our Threat Actor Encyclopedia provides defenders with a searchable database of detailed profiles on more than 30 threat actors worldwide. This resource supports advanced threat hunting by enabling users to quickly access context on adversary motivations, tactics, and behaviors to strengthen preparedness and response.



KEY CONTRIBUTIONS IN 2025



Fortinet has been a trusted INTERPOL partner since 2015 and an INTERPOL Gateway partner since 2018, supporting intelligence sharing, coordinated takedowns, and regional cyber resilience initiatives.

Operation Serengeti 2.0

In 2025, Fortinet, along with nine other partners, supported Operation Serengeti 2.0, a large-scale campaign targeting cybercriminal groups across 18 African nations and the United Kingdom. Fortinet contributed in two complementary ways: as a Gateway partner and through leadership and joint contributions to the Cybercrime Atlas. FortiGuard Labs provided advanced intelligence—including indicators of compromise, C2 infrastructure data, and other forensic insights—to help identify malicious actors and enable coordinated cross-border investigations. INTERPOL recognized Fortinet as a key private-sector information-sharing partner for this operation.

The operation uncovered significant cyber-enabled fraud schemes, including:

- **Angola:** Dismantling of 25 illegal cryptocurrency mining centers, operated by 60 Chinese nationals generating illicit crypto revenue.
- **Côte d'Ivoire:** Disruption of a transnational inheritance scam originating in Germany, resulting in \$1.6 million in losses.
- **Zambia:** Shutdown of a large-scale online investment fraud scheme, with 65,000 victims losing an estimated \$300 million. Authorities also disrupted a related human trafficking network.

“Each INTERPOL-coordinated operation builds on the last, deepening cooperation, increasing information sharing, and developing investigative skills across member countries. With more contributions and shared expertise, the results continue to grow in scale and impact. This global network is stronger than ever, delivering real outcomes and safeguarding victims.”

Valdecy Urquiza

Secretary General of INTERPOL

IMPACT OF OPERATION SERENGETI 2.0

1,200+
arrests

11,400+
malicious
infrastructures
dismantled

~88,000
victims identified

\$97.4M
recovered



In 2025, Fortinet contributed to the Europol Joint Cybercrime Action Taskforce (J-CAT), a permanent operational taskforce based at Europol's headquarters, working alongside the European Cybercrime Centre (EC3). Through this collaboration, Fortinet provides actionable threat intelligence, supports joint investigations, and shares operational insights to enable coordinated disruption of cross-border cybercrime.

STRENGTHENING CYBER RESILIENCE IN LATIN AMERICA AND ASIA-PACIFIC

Fortinet collaborated with INTERPOL, the World Economic Forum, and the Organization of American States (OAS) to address the evolving cybercrime landscape, where limited institutional capacity, lower digital literacy, and multi-jurisdictional complexity amplify risk.

Key initiatives in 2025 included:

Latin America

- INTERPOL's 10th Americas Working Group on Cybercrime (in Panama) to assess AI misuse and CaaS, and develop a roadmap of joint operational capacity.
- OAS ransomware tabletop exercises that simulate attacks on critical infrastructure to test real-time coordination between national teams, law enforcement, and international actors.

Asia and the South Pacific

- Support for the Asia and South Pacific Joint Operation Against Cybercrime, including participation in Operation SECURE workshops to enhance regional cooperation and operational readiness.



As a founding member of the CTA, Fortinet strengthens collective cyber defense by sharing timely, high-fidelity threat intelligence across the industry. CTA enables defenders to collaborate beyond competitive boundaries, accelerating detection, response, and global protection.

In 2025, Fortinet contributed to several key CTA initiatives:

- **Early-share program:** Provided 40 early shares of critical, pre-publication threat intelligence to help member organizations deploy defenses sooner and coordinate faster responses. In total, 189 early shares were delivered through CTA members.
- **High-volume intelligence distribution:** Supported the daily distribution of over 500,000 observables, enhancing real-time situational awareness and helping organizations worldwide counter emerging threats.
- **Industry leadership in vulnerability communication:** Led CTA's [Responsible Vulnerability Communication Policy](#), which strengthens ecosystem-wide coordination and helps ensure more systematic, responsible disclosure practices.
- **Thought leadership on emerging risks:** Co-authored the report [Approaching Quantum Dawn: Closing the Cybersecurity Readiness Gap Before It's Too Late](#), providing guidance on preparing for quantum-driven security challenges.



Fortinet partnered with UC Berkeley to advance the understanding of AI-enabled cybercrime through a global tabletop exercise (TTX) series. These exercises bring together cybersecurity experts, industry leaders, and policymakers to simulate emerging AI-driven threats, explore response strategies, and strengthen collaborative defenses against evolving cybercrime.

2025 milestones included:

- **RSA USA 2025:** Co-hosted a panel highlighting insights from the AI-enabled cybercrime TTX series.
- **Singapore:** Completed the second TTX, convening regional stakeholders to test response strategies against AI-driven attacks. [Read more.](#)
- **Israel:** Completed the third TTX, extending the global reach of the initiative and reinforcing cross-border collaboration on emerging threats.





Fortinet continues to play a leadership role in the World Economic Forum's global cybersecurity community, advancing public-private collaboration to address systemic cyber risks. As the first cybersecurity founding partner of the World Economic Forum Centre for Cybersecurity, Fortinet contributes expertise, threat intelligence, and strategic guidance across multiple workstreams.

Key contributions in 2025 included:

- **Cybercrime Atlas: Impact Report 2025:** Co-launched the latest Impact Report, showcasing significant progress in global cybercrime disruption and intelligence collaboration. The report reflects the Cybercrime Atlas's evolution into a powerful, multi-sector platform that maps criminal ecosystems, identifies key disruption points, and supports coordinated operational action. In 2025, Cybercrime Atlas contributors, including Fortinet, helped strengthen this global knowledge base by sharing over 17,000 community-vetted and actionable data points, creating 13 comprehensive intelligence packages on emerging cyberthreats for broad distribution, supporting four cross-border cybercrime disruption operations, expanding participation from 22 to 30 organizations, and extending reach across more than 40 countries.
- **Engagement across the global CISO Community:** Participated in the global CISO Community and represented Fortinet at the World Economic Forum's Annual Meeting on Cybersecurity 2025 in Dubai, United Arab Emirates, including the panel Scaling Disruption: The Next Chapter in Cybercrime Collaboration and interdisciplinary sessions on cybersecurity as a global public good. These engagements help align cross-industry strategies for addressing the rise of AI-enabled threats and CaaS models.

- **Global Cybersecurity Outlook 2026:** Supported the development of the World Economic Forum's flagship global assessment of cybersecurity trends, risks, and societal impacts, contributing insights on the evolving threat landscape and effective approaches to resilience-building.
- **Thought leadership on AI and emerging risks:** Contributed to the World Economic Forum whitepaper Artificial Intelligence and Cybersecurity: Balancing Risks and Rewards, which offers a clear perspective and actionable recommendations on managing cyber risks associated with AI adoption. Supported development of the AI at Work paper released at Davos 2026, helping to shape global guidance on responsible AI adoption.
- **Growing cyber talent through public-private partnerships:** Contributed to the World Economic Forum whitepaper Growing Cyber Talent Through Public-Private Partnerships, which highlights how cross-sector collaboration can accelerate workforce development and defines the foundational elements required for successful public-private coordination.



Fortinet is a long-standing member of and contributor to FIRST. In 2025, Fortinet became the only founding partner from the cybersecurity industry of FIRST's newly launched Community, Operations, Resilience, and Empower (CORE) initiative.

FIRST CORE strengthens incident-response capabilities worldwide through capacity-building, training, and community development. Fortinet supports the initiative by developing training content, subsidizing participation for under-resourced partners, expanding fellowship opportunities through the Suguru Yamaguchi Fellowship program, and establishing regional liaisons and mentors to support local CERTs and security teams. In 2025, Fortinet participated in training exercises for first responders and incident-response teams in Copenhagen, Denmark, during the FIRST 2025 Annual Conference.

Fortinet's leadership as our founding partner demonstrates their commitment to strengthening cybersecurity knowledge across industries and borders. Together, we're building communities grounded in internationally recognized best practices that will enhance incident-response capabilities across the globe.

Chris Gibson
CEO, FIRST



CUSTOMER SUCCESS ENABLEMENT

Fortinet empowers organizations to operate securely, efficiently, and confidently across their digital environments. By combining advanced cybersecurity technologies, expert services, education programs, and a global partner network, we help customers strengthen their security postures, maximize the value of our solutions, and maintain operational continuity. These efforts directly support resilient organizations and, by extension, the critical services that rely on them and society more broadly.

COMPREHENSIVE CUSTOMER SUPPORT

Fortinet delivers trusted, high-quality service, accessibility, and expertise across the product lifecycle. Through our 25 global support centers, we provide 24x7 expert assistance to every country where our products are deployed. Complex challenges or requests requiring deeper expertise are addressed by our Professional Services and Advanced Support teams, ensuring focused, high-level assistance.

Our extensive partner network further enhances this coverage, offering localized guidance and relevant solutions to meet the needs of enterprise customers and smaller organizations alike. Customers can easily identify partners based on location, specialization, and services offered, using the Find a Partner page, ensuring relevant support and solutions to meet their unique needs.

We also ship spare parts and provide industry-leading coverage for time-sensitive deliveries to ensure rapid resolution. Our Global Service Availability page includes detailed information about service options by country.

AI-POWERED SUPPORT AND INNOVATION

In 2025, Fortinet advanced the use of AI support tools to enhance responsiveness and efficiency. Customers can use the instant search capability in our support environment to quickly locate support resources online, often avoiding the need to submit a ticket. Meanwhile, Technical Assistance Center (TAC) engineers leverage FortiChatAI and Smart Assist to address queries faster, summarize interactions, and improve overall customer satisfaction. These AI capabilities enable more efficient knowledge delivery, faster issue resolution, and deeper insights into customer needs. We are also exploring additional AI applications to further enhance customer experience.

SUPPORT CAPABILITIES

Fortinet empowers customers at every stage of the deployment lifecycle, ensuring they can maximize the value of our technology through a range of support options and resources. Our FortiCare Services page provides detailed information on customer support offerings, including Professional Services, Advanced Support, Priority Return Merchandise Authorization, Secure RMA, and Technical Support.

We aim to equip our customers, either directly or through our global partner network, with the resources and guidance they need—whether they are designing, deploying, or refreshing their Fortinet security solutions. For customers across all skill levels, we offer self-service options and access to a collaborative, active community to further enhance their knowledge and expertise.

HOW FORTINET SERVICES SUPPORT SECURE, RESILIENT DIGITAL INFRASTRUCTURE

Fortinet's services help customers operate and secure their digital infrastructure throughout its lifecycle—from deployment and optimization to ongoing support. By combining cybersecurity expertise, centralized management, and continuous support, Fortinet enables customers to reduce operational risk, improve resilience, and maintain continuity of essential services.

Customer: Mississippi Department of Employment Security (USA)

Services challenge

The agency needed to protect sensitive citizen data and ensure reliable service delivery with limited internal IT resources.

Fortinet services enablement

Fortinet support and security services provided continuous protection, simplified management, and expert assistance, enabling a small IT team to securely manage remote access and network operations.

Service impact

- Long-term protection of sensitive data with minimal operational overhead
- Secure access supporting workforce flexibility and service continuity
- Reduced need for additional IT staffing and resources

See customer case studies from around the world.



24x7 GLOBAL
SUPPORT



1,900+ NSE AND INDUSTRY-
CERTIFIED GLOBAL RESOURCES



3 REGIONAL CENTERS
OF EXPERTISE



25 SUPPORT CENTERS AND
40 REGIONAL DEPOTS



200+ IN-COUNTRY
DEPOTS



4-HOUR EXPEDITED HARDWARE
REPLACEMENT AVAILABILITY

RESPONSIBLE TECHNOLOGY
CYBERSECURITY INNOVATION
CYBERCRIME DISRUPTION
CUSTOMER SUCCESS ENABLEMENT

KNOWLEDGE SHARING AND PARTNER ENABLEMENT

The [Fortinet Community](#) remains a cornerstone of peer-to-peer learning and knowledge exchange. In 2025, the Community supported more than 192,000 members who had access to over 21,000 knowledge articles, of which 25% were newly created or updated during the year to reflect the latest product capabilities, security guidance, and best practices. Members engaged in over 8,200 forum discussions, enabling peer-to-peer support and expert advice, while the platform recorded approximately 23 million visits. Surveys indicated that 76% of respondents found the information they needed, reflecting both the depth and the accessibility of the resources available. These interactions help customers resolve issues faster and contribute to building a collective knowledge base that benefits the broader cybersecurity community.

The [Fortinet Engage Partner program](#) continued to increase its impact in 2025, enhancing partner expertise in technical support and professional services through the Engage Tech Support Partners (ETSP) and Engage Preferred Service Partners (EPSP) certifications. In 2025, the EPSP program grew by 19% while ETSP increased its partner base by 47%, bringing the total to 143 certified partners globally. During the year, individuals completed more than 2,100 training modules through targeted programs, building expertise in incident response and advanced technical troubleshooting to better meet customer needs across the product portfolio. Fortinet also hosted the EPSP Summit in Kuala Lumpur, Malaysia, to recognize top-performing partners and provide an additional forum for knowledge exchange.

Customer enablement and support experience

To address evolving customer needs, we introduced several new enablement initiatives in 2025:

- The SASE enablement program equips Fortinet Engage Partner program members to deploy Secure Access Service Edge (SASE) solutions for smaller Fortinet customers, leveraging the expertise gained from larger-scale deployments. We provided training to 81 program members during the year.
- Enhanced communication around firmware end-of-support encouraged customers to update their systems proactively, resulting in a roughly 31% increase in updates and ensuring continued protection against evolving threats.
- The [Support entry point](#) was redesigned to proactively provide solutions through intelligent search tools, reducing ticket volume and shortening resolution times.

“At Fortinet, we believe that cybersecurity excellence requires both cutting-edge technology and empowered people. Our approach to customer success brings together community engagement, partner certification, and proactive support to help organizations worldwide deploy and operate resilient, secure environments. These efforts reflect our commitment to providing customers with solutions and the skills and support they need to maximize protection and operational efficiency.”

CUSTOMER SATISFACTION

Customer satisfaction is central to Fortinet's approach. We continually monitor customer satisfaction through both transactional and quarterly customer satisfaction (CSAT) scores. In 2025, our TAC achieved a CSAT score of 9.34 out of 10.

We prioritize validating and enhancing our teams' technical expertise to uphold high standards and deliver reliable customer support. As part of this commitment, 100% of our TAC team members are required to complete training through the [Fortinet NSE Certification program](#). Core product TAC members pursue Fortinet professional-level certifications, while senior and advanced-support teams progress toward Fortinet expert-level certifications.



Colin Broadbent
Director of services portfolio
and member of the CSR
committee at Fortinet

2025 HIGHLIGHTS

Fortinet Community

192,000+

members engaged globally

23M

platform visits

76%

of members found the information they needed

Fortinet Engage Partner program

140+

certified partners globally
(43% combined growth vs. 2024)

2,100+

training topics completed through technical and professional service programs

Enablement and support outcomes

31%

increase in customer upgrades to supported firmware

9.34/10 TAC CSAT score

100%

of TAC staff required to complete NSE Certification training

MINIMIZING OUR ENVIRONMENTAL FOOTPRINT

As the world faces escalating climate and resource challenges, stakeholders expect companies to reduce environmental impacts across their value chains. Our approach spans climate risk assessment, science-based decarbonization targets, sustainable operations, and continuous improvement in product sustainability through eco-design, energy efficiency, sustainable packaging, and circularity. In collaboration with employees, customers, and suppliers, we drive progress toward a more sustainable future.

2025 HIGHLIGHTS



Up to 62% lower in product energy consumption

1st cybersecurity company to publish Environmental Product Declarations

Climate risk assessment completed in line with TCFD

~91.6

metric tons of plastic removed from packaging

CLIMATE

Understanding Fortinet's climate impact and decarbonizing across our value chain are core pillars of our environmental strategy. Our products, operations, and supply chain affect our customers' value chains worldwide, so demonstrating progress is increasingly essential to meeting their expectations. In 2025, we strengthened internal data collection processes and methodologies to enhance the accuracy and completeness of our Scope 3 emissions inventory, supporting future transparency and evolving regulatory expectations.

CLIMATE SCENARIO ANALYSIS

In 2025, we conducted Fortinet's first comprehensive climate scenario analysis. The assessment—which included qualitative and quantitative aspects—examined the most material climate-related risks and opportunities to Fortinet across multiple climate scenarios and time horizons.

Following the TCFD framework, we assessed physical climate risks using the Intergovernmental Panel on Climate Change (IPCC) SSP5-8.5/RCP 8.5 scenario and transition risks using the Network for Greening the Financial System (NGFS) Below 2°C scenario. In total, seven climate risks were prioritized based on a combination of potential financial impact and likelihood.

The analysis focused on medium-term (2030) and long-term (2040) risks and opportunities. Short-term (2026) climate-related risks and opportunities are addressed through Fortinet's enterprise risk management program.

Insights from this analysis will inform our climate transition planning, strengthen future CDP- and TCFD-aligned disclosures, and enhance our preparedness for evolving climate-related reporting expectations.

Medium-term (2030) risks and opportunities

Key physical risks include increased frequency and severity of extreme weather events and rising average temperatures, which are leading to shifts in precipitation patterns.

These impacts could disrupt Fortinet's supply chain, affect business operations, and ultimately influence revenue generation.

Key transition risks relate to evolving policy and regulatory requirements, including the potential introduction or expansion of carbon pricing mechanisms such as carbon taxes, tariffs, or cap-and-trade schemes.

Medium-term opportunities include increased demand for Fortinet's energy-efficient products, driven by growing demand for sustainable and low-energy devices. Additional opportunities may arise from advancing sustainable product design through improved resource management, circularity, and the use of more sustainable materials.

Long-term (2040) risks and opportunities

Over the long term, more frequent and severe weather events may affect infrastructure and operations. Activities to mitigate these risks include prioritizing climate-resilient building design, strengthening business continuity planning with suppliers in hurricane-prone regions, and enhancing data center thermal design to accommodate rising temperatures.

Transition trends in 2040 also present risks—such as those associated with increased AI use—and opportunities, including sustained demand for energy-efficient products and greater integration of circular economy and eco-design principles across our product portfolio.

CLIMATE-RELATED REGULATORY REPORTING

We are committed to transparency in our climate-related disclosures and continue to monitor and respond to evolving regulatory reporting requirements across the regions in which we operate.

In the UK, we submit an annual Streamlined Energy and Carbon Reporting (SECR) report alongside our financial filings, covering energy use and greenhouse gas (GHG) emissions. SECR disclosures also include information on energy efficiency actions aligned with the UK's Energy Savings Opportunity Scheme (ESOS). We have submitted SECR reports since 2023.

Globally, Fortinet continues to monitor the development and implementation of climate-related reporting frameworks. We are strengthening internal processes and governance to align with evolving expectations for climate-related transparency.

Assessments such as these help Fortinet identify emerging priority topics relevant to the company—such as how physical climate risks and the global transition to a low-carbon economy may affect our operations, products, and value chain. By integrating these insights into strategic planning, we can strengthen business resilience, guide investments in decarbonization, and ensure our solutions continue to support customers in an increasingly climate- and regulatory-impacted world. This proactive approach allows us to anticipate risks, identify opportunities, and align with evolving expectations on climate disclosure globally.



Meera Ramanathan
Head of sustainability & CSR and chair of the CSR committee at Fortinet

DECARBONIZATION PLAN AND SCIENCE-BASED TARGETS

Our decarbonization plan defines a clear path to align our business with a 1.5°C trajectory. This pathway is anchored in our near-term science-based targets validated by the Science Based Targets initiative (SBTi), which provide a robust foundation for our decarbonization roadmap. The plan outlines how we will reduce GHG emissions across our most significant impact areas while remaining aligned with leading international climate standards.

We focus on reducing GHG emissions in our direct operations, partnering with suppliers to lower upstream impacts, and advancing product energy efficiency and circularity. By reducing the energy intensity of our solutions and promoting responsible end-of-life practices, we help customers reduce environmental impacts while enabling secure digital transformation.

We've established our near-term targets in 2024. While our 2025 emissions data is reporting in this report, progress against these targets will be disclosed through CDP.



DRIVING AMBITIOUS CORPORATE CLIMATE ACTION

OUR FIRST STEPS TOWARD NET ZERO 2050

SBTi-VALIDATED NEAR-TERM TARGETS

SUSTAINABLE OPERATIONS



Scope 1

Direct emissions

- Reducing natural gas usage in our buildings
- Transition to low-emissions cooling systems for our buildings



Scope 2

Indirect emissions

- Use 100% renewable electricity for owned sites by 2030
- Invest in on-site (solar panels, etc.) and off-site (VPPAs, etc.) solutions

58.80%

absolute reduction by 2030¹

SUSTAINABLE SUPPLY CHAIN



Scope 3 category 1

Purchased goods and services

- Ensure that suppliers have climate programs that align with ours
- Include sustainability criteria in decision-making

60.50%

of suppliers² to have SBTi-validated targets by 2029

SUSTAINABLE PRODUCTS



Scope 3 category 11

Use of sold products

- Reduce energy consumption of our products
- Further embed circular practices in our products and packaging

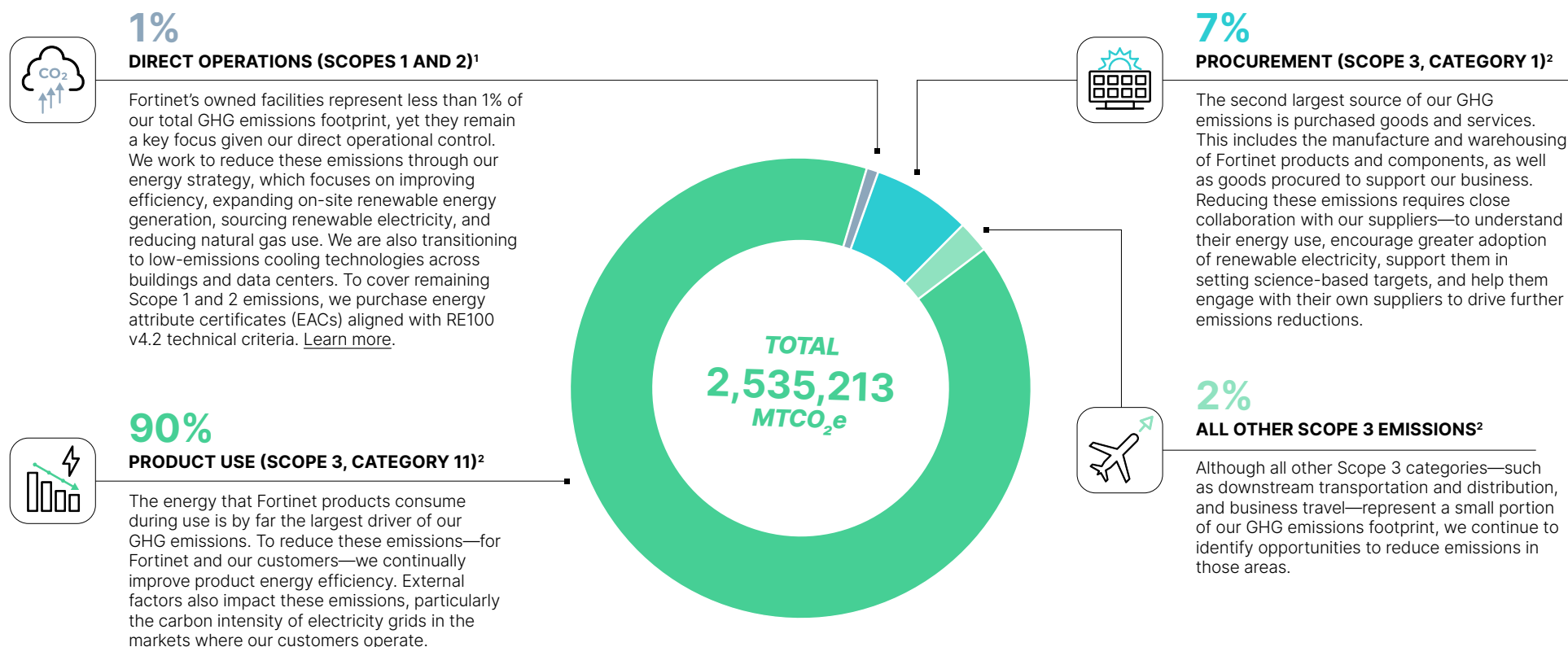
69.24%

of customers³ to have SBTi-validated targets by 2029

1. Baseline 2021. 2. By spend. 3. By revenue.

FORTINET 2025 CARBON FOOTPRINT AND PATHWAY TO REDUCTION

We inventory our GHG emissions annually to understand Fortinet's performance and identify opportunities for ongoing improvement. We use globally recognized standards and methodologies, including The Greenhouse Gas Protocol: A Corporate Accounting and Reporting Standard (revised version), to calculate our GHG emissions across Scope 1, Scope 2, and Scope 3.



1. Scope 1 GHG emissions are direct emissions from Fortinet-owned facilities. Primary contributors include natural gas used for heating buildings, refrigerants with high global warming potential (GWP) used for cooling, and fuel consumed by emergency generators. Scope 2 GHG emissions are indirect emissions related to purchased energy consumption, such as electricity, steam, heating and cooling in our owned facilities. Fortinet's primary source of Scope 2 GHG emissions is the electricity purchased for our facilities.
2. Scope 3 GHG emissions include indirect emissions from upstream and downstream sources in our value chain.

See detailed GHG emissions data in the [appendix](#).

SUSTAINABLE OPERATIONS

We continue to enhance energy and resource efficiency across our global operations by investing in sustainable technologies, integrating green building principles, sourcing renewable energy, and improving processes to reduce consumption and waste. As our data center footprint expands and employees increasingly return to offices, ensuring efficient, resilient, and low-impact operations has become even more essential. All employees play a critical role in delivering on the Fortinet environmental program, and we work to promote sustainable practices and encourage a culture of environmental responsibility across our organization.

ENVIRONMENTAL MANAGEMENT IN OPERATIONS

In line with the [Fortinet Environmental Policy](#), we work to identify, manage, and reduce our impacts related to energy, water, and waste. Our comprehensive environmental management system is ISO 14001-certified and covers our largest owned warehouses in Union City, California. In 2025, employees at this warehouse completed ISO 14001, e-waste, and environment, health, and safety training.

Fortinet's commitment to strong environmental management extends to its owned warehouses and subsidiaries, with two locations currently

ISO 14001-certified. We also implement water conservation projects in our data centers, including rainwater capture and chiller upgrades, helping conserve natural resources across operations. Beyond operational improvements, we continue to increase environmental transparency company-wide, demonstrating our commitment to responsible environmental management.

GREEN BUILDINGS

To guide new real estate investments and renovations, we apply Fortinet's Green Guidelines—our internal framework inspired by LEED and BREEAM standards. The guidelines

help ensure alignment with our decarbonization targets and support continuous improvement across facilities. They address a range of sustainability considerations, including green building certifications, energy performance, renewable energy sourcing and on-site generation, EV charging infrastructure, indoor air quality, water efficiency, access to low-carbon transportation, bicycle storage, waste and recycling, and other related areas.

These principles help ensure that our buildings support long-term operational efficiency, employee well-being, and progress toward our climate goals.

EXAMPLES OF FORTINET BUILDINGS WITH STRONG ENVIRONMENTAL FEATURES:



Chicago, Illinois, United States: This Fortinet-owned facility includes an R&D center, Fortinet Cloud Point of Presence, Executive Briefing Center, Training Facility, and Support Center to drive innovation, collaboration, and growth in the region. The site is powered entirely by 100% renewable energy.



Santa Clara, California, United States: The site sources 100% renewable energy and hosts one of our data centers. It also includes a built-in pond to conserve water, supporting the site's overall sustainability initiatives.



Sunnyvale, California, United States: LEED Gold certified and fully powered by renewable electricity, this site consumes 30% less energy than a standard building. Solar panels on the parking garage and campus generate additional renewable energy. Drought-tolerant landscaping conserved over 280 cubic meters of water in 2025.



Almere, Netherlands: Located in a major European logistics hub, this 12,000-square-meter distribution center offers direct access to road, rail, airport, and waterway networks. The facility features LED lighting with motion sensors, and electric vehicle charging points. It is designed to accommodate future sustainability measures. Local handling and shorter transportation routes help reduce logistics costs and GHG emissions from product transportation for European customers.



Madrid, Spain: This B-rated low-carbon emission data center is equipped with photovoltaic panels for on-site renewable energy and indirect air coolers for efficient heat exchange. It achieved a PUE of 1.2 in 2025, with only 10% of energy used for cooling and other overhead.



Sydney, Australia: This facility has a 4-Star Green Star rating, with solar panels generating 9% of the site's electricity annually. The remaining energy needs are met with 100% renewable electricity from the utility. The facility incorporates recycled furnishings sourced from non-Fortinet buildings and First Nations suppliers, and was shortlisted for the 2025 Better Future Sydney Design Awards in the corporate interior design category.

ENERGY

Energy consumption is the main driver of GHG emissions in our facilities and represents a significant operational cost, so energy efficiency and renewable energy sourcing are central to our environmental strategy. An energy strategy sub-committee within Fortinet's CSR committee—comprising experts from operations, global real estate, CSR, facilities, and our global energy broker—provides oversight of these efforts.

In 2025, our owned facilities consumed 266,878 gigajoules (GJ) of energy, up 27% compared to 2024, largely due to the addition of new data centers in Calgary, and Plano.

Of total energy use in Fortinet-owned facilities in 2025, 61% came from renewable sources. 87% of our owned sites (by square footage) used 100% renewable electricity, including all facilities in California, Illinois, Spain and France.

For the remaining owned sites, we purchased renewable energy certificates (RECs) to reach 100% renewable electricity in 2025 across our entire owned real estate portfolio. In parallel, we continued to prioritize renewable electricity access for newly acquired sites and leased data centers in alignment with Fortinet's Green Guidelines.

Several Fortinet locations globally, including our headquarters in Sunnyvale, California and our facility in Sydney, Australia generate renewable energy on-site. [Learn more](#). To support the expansion of renewable electricity as our global footprint grows, we partner with an energy broker that helps us procure renewable electricity solutions.

We are also reducing reliance on natural gas across our operations. In 2025, 62% of Fortinet's owned and occupied sites reported zero natural gas consumption.

ENERGY-REDUCTION INITIATIVES IN FORTINET UK OPERATIONS

In the UK, we completed the UK Environment Agency's [Energy Savings Opportunity Scheme \(ESOS\)](#) assessment with support from an external expert. ESOS requires large organizations with a presence in the UK to periodically assess energy use across buildings, transportation, and industrial processes, and to identify potential efficiency opportunities.

The assessment identified a range of potential energy-reduction opportunities, including optimizing HVAC schedules, exploring on-site solar generation, and improving vehicle and transportation efficiency. These initiatives are being evaluated as part of our ongoing strategy to reduce operational energy use.



GOAL

100%

renewable energy
use across all owned
Fortinet sites by 2030

PROGRESS IN 2025:

61%

achieved



REDUCTION OF ELECTRICITY CONSUMPTION AT FORTINET TECHNICAL ASSISTANCE CENTERS LAB

Building on the successful 2024 pilot at our Sophia Antipolis Technical Assistance Center (TAC) in France, Fortinet expanded the availability of an energy-saving feature in our lab automation software to all TAC labs globally in 2025. The initial deployment in Sophia Antipolis demonstrated strong results, reducing lab electricity consumption by approximately 40% and overall site electricity consumption by 18%, avoiding an estimated 40 metric tons of CO₂e annually.

With the functionality now available across all TAC labs, additional sites began to observe similar benefits in 2025. For example, our Ottawa, Canada, TAC reported an approximately 50% reduction in lab energy consumption.



DATA CENTER ENERGY EFFICIENCY IMPROVEMENTS

In 2025, we improved the energy efficiency of our Plano, Texas, data center through targeted improvements to cooling infrastructure, reducing energy intensity and lowering GHG emissions. Average power usage effectiveness (PUE) improved by approximately 21% year on year, and data center infrastructure efficiency (DCIE) increased from 41% to 53%, demonstrating significant operational gains. We will continue to monitor and optimize data center operations to support efficient energy use in line with operational requirements.

WATER

Although Fortinet's direct water footprint is relatively small, we recognize the growing importance of responsible water management—particularly as our data center portfolio expands and more stakeholders request transparency into water-related risks. In 2025, we again completed the CDP Water Security Questionnaire to support accountability and strengthen our understanding of water-related risks and opportunities across our operations. We received a B- score, reflecting our ongoing efforts to assess and manage water-related impacts.

In 2025, water consumption at Fortinet's owned facilities totaled 100,086 cubic meters. As our operations evolve, particularly through data center expansion, we will continue to improve water data collection, evaluate water-related risks, and identify opportunities to responsibly manage water consumption in existing and future facilities.

Data centers are the largest contributors to our operational water consumption, primarily due to cooling needs for servers and other equipment. To manage this impact, we focus on improving energy efficiency—which lowers cooling demand—and on implementing site-specific measures to optimize water consumption where feasible. For example, Fortinet's data center in Torija, Spain, collects 32.6 cubic meters of rainwater annually for landscaping and uses a solar thermal system to heat water for showers and the dining area, reducing water and energy consumption.

Across our broader real estate portfolio, we incorporate water considerations into building design and operations. For example, drought tolerant landscaping at our Sunnyvale, California, site helped conserve approximately 280 cubic meters of water in 2025. At our Plano, Texas, data center, water usage decreased by 85% in 2025—from 11,007 cubic meters to 1,653 cubic meters annually—following the replacement of chillers.

WASTE

We work to reduce waste across our operations and aspire to follow the hierarchy of prevention, reuse, recycling, recovery (including energy recovery), and disposal. Waste management activities are governed by our ISO 14001-certified environmental management system, which ensures compliance with applicable global and regional regulations.

Our operational waste is primarily non-hazardous. Hazardous waste in our operations is limited to universal waste streams such as lighting, e-waste, and small quantities of maintenance-related chemicals, such as cleaners. These waste items are properly disposed of or recycled by qualified recyclers in accordance with local environmental regulations.

In 2025, we continued to improve waste tracking practices across our owned facilities, with a particular focus on e-waste. Through our [Fortinet Product Donation program](#), selected Fortinet hardware and unused IT equipment are repurposed, extending product life and reducing the volume of items entering end-of-life recycling streams. This program supports nonprofit organizations, educational institutions, and community-based NGOs focused on digital inclusion, cybersecurity education, and climate resilience.

Seven Fortinet sites also segregate food waste for composting. We continue to explore opportunities to increase reuse and recycling, improve data collection, and reduce overall waste generation across our operations. Fortinet also integrates sustainability into corporate events, embedding responsible practices into operations and engagement (see box).



FORTINET ACCELERATE 2025: A LOW-IMPACT GLOBAL EVENT

At Fortinet Accelerate 2025 in Berlin, Germany, the company showcased how large-scale events can be delivered sustainably. The entire technology showcase and staging were built from reusable or recycled materials, including timber and aluminum structures designed for future use. More than 2,500 square meters of printed vinyl were upcycled into tote bags, pouches, and other items after the event, and event artwork and frames were reused

in Fortinet offices and the Executive Briefing Center in France.

Menus prioritized low-carbon options, with 80% of ingredients sourced locally and no beef served. Leftover food was either redistributed to local charities or sent to a biogas facility. Single-use plastics were replaced with biodegradable utensils and reusable glass bottles, and digital signage was used to reduce printing.

We encouraged sustainable mobility by collaborating with Berlin's public transport network, allowing attendees to use their event badges for unlimited travel. Locally based staff, rental furniture, and plant decorations donated to charities further reduced the event's environmental footprint. Badges and lanyards made from recycled materials were collected for reuse or recycling, demonstrating Fortinet's commitment to minimizing waste at every touchpoint.

SUSTAINABLE PRODUCTS

Because 90% of our carbon footprint is due to product energy use during the use phase, improving energy efficiency is a key focus to reduce GHG emissions for Fortinet and our customers. Beyond energy use, our products have environmental impacts related to materials, manufacturing, and end-of-life. Our holistic approach to address these combines eco-design principles, sustainable packaging, circularity practices, and regulatory compliance. Together, these efforts enhance the environmental performance of our portfolio while helping customers advance their own sustainability goals.

ECO-DESIGN PRINCIPLES

We integrate sustainability considerations from the earliest stages of product development, understanding that design choices largely determine a product's environmental impact across its lifecycle. Our eco-design framework focuses on:

FORTINET ECO-DESIGN PRINCIPLES

				
Product energy efficiency	Packaging sustainability	Designing for durability	Circularity	Regulatory alignment and compliance
Improving energy efficiency in the use phase—the primary driver of our products' GHG emissions—is central to our eco-design approach. We focus on maximizing performance per watt, reducing power and cooling needs, and enabling equipment consolidation to help customers lower energy consumption and operational emissions.	Our products are packaged with sustainability in mind. We prioritize using recycled and renewable materials where feasible, minimize foam and single-use plastics, and include only necessary accessories. Packaging design also emphasizes material efficiency and recyclability to support responsible end-of-life management.	Products are designed for long-term reliability and robustness to extend useful life and reduce replacement frequency, supporting lower overall resource use throughout the product lifecycle.	Extending product life and keeping materials in use longer are key parts of our eco-design framework. Through our Fortinet Product Donation program, select equipment is given a second life, supporting responsible resource use and helping limit e-waste.	Proactive alignment with evolving global environmental regulations—such as energy efficiency standards, substance restrictions, eco-design directives, and extended producer responsibility requirements—ensures our products meet or exceed regulatory requirements.



Wei Ling Neo
VP product management and member
of the CSR committee at Fortinet

“We embed eco-design from the earliest stages of our engineering process to guide how we reduce environmental impacts across the product lifecycle. Our approach focuses on improving energy efficiency in the use phase, designing more sustainable packaging, extending product life through durability and circularity, and proactively aligning with global environmental regulations. These principles help us deliver high-performance solutions while supporting customers in achieving their own sustainability goals.”

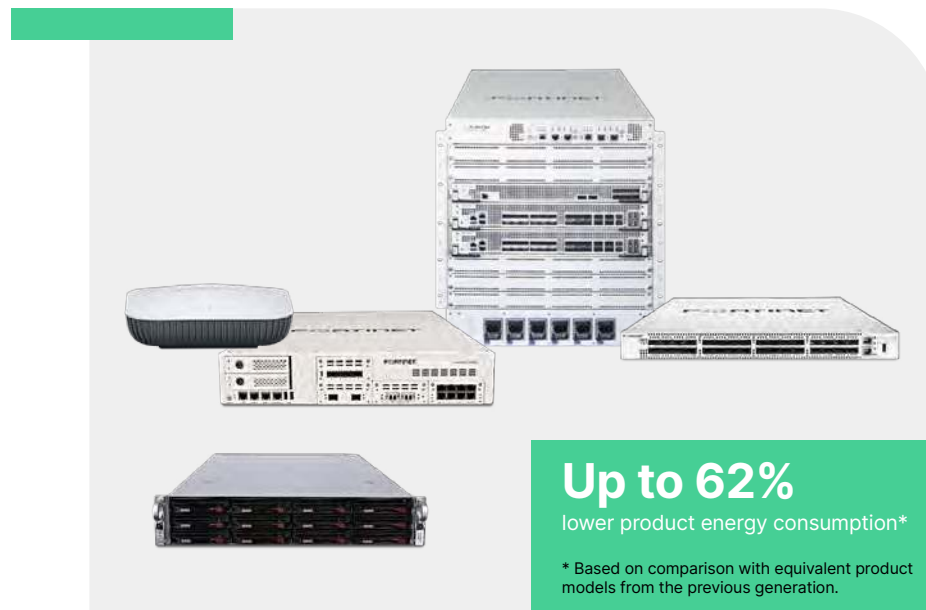
PRODUCT ENERGY EFFICIENCY

Energy efficiency is central to Fortinet's decarbonization strategy, as the use phase of our products is the largest contributor to our carbon footprint. To address this, we integrate energy-performance requirements into every product design, engineering our solutions to maximize performance per watt and help customers reduce electricity use and associated GHG emissions. Our Security Processing Unit 5 (SP5) ASIC achieves industry-leading performance per watt and consumes 88% less power than industry-standard CPUs.

Fortinet's platform-consolidation approach—combining multiple security and networking functions into a single platform—reduces the need for separate appliances, thereby lowering power, cooling, and space requirements. Continuous R&D improvements ensure each product generation consumes less energy than its predecessor while delivering higher performance. These efforts help customers optimize operations, decrease device counts, and make progress toward their climate goals.

In 2025, new products, including FortiGate 700G and FortiGate 3800G achieved energy reductions of 55% and 62%, respectively, compared with equivalent models from the previous generation, further reducing GHG emissions across our value chain.

In 2025, we also estimated GHG emissions associated with running next-generation FortiGate firewall products as virtual machines (VMs). VMs are software-based versions of physical hardware that enable multiple operating systems and applications to run on a single cloud server, increasing server utilization and significantly improving energy efficiency.



Fortinet's cybersecurity platform enables us to deliver strong security performance while advancing our sustainability goals. Fortinet's product carbon footprint insights informed our technology decisions, helping us align our cybersecurity investments with environmental considerations. By combining energy-efficient security solutions with robust security capabilities, Fortinet supports our efforts to reduce environmental impact while strengthening a resilient security posture.

Lai Heng-Hu

CISO, Chang Chun Petrochemical Co., Ltd.

INDUSTRY RECOGNITION

The FortiGate-50G received the 2025 Most Energy Efficient Cybersecurity Solution award at Ignite 2025. This underscores our focus on sustainability and innovation, and our commitment to delivering trusted, high-performance security solutions that set new standards for energy efficiency.



LIFECYCLE ASSESSMENT AND ENVIRONMENTAL PRODUCT DECLARATIONS

We conduct lifecycle assessments (LCAs) on select high-volume products to understand environmental impacts across the product lifecycle—from raw materials extraction and manufacturing to distribution, use, and end-of-life. Aligned with ISO 14025, ISO 14040, ISO 14067, and ISO 14044 standards, LCAs quantify multiple impact categories and identify hotspots for improvement. These insights inform product design decisions and support transparent reporting that helps customers make more informed sustainability choices.

In 2025, Fortinet became the first cybersecurity company to publish an Environmental Product Declaration (EPD), for the FortiGate 40F NGFW. An EPD is an independently verified, standardized report that provides product-specific environmental impact data across the full lifecycle, including carbon footprint, energy use, water consumption, resource depletion, and waste generation. Developed under the latest Product Category Rules (PCR 2024:06) and grounded in LCA methodology, EPDs offer procurement teams and sustainability leaders credible, comparable data, replacing unverified claims with validated information.

Insights from the EPD reinforce the importance of our product energy efficiency efforts. For the FortiGate 40F, approximately 83% of estimated lifecycle GHG emissions occur during the product use phase, underscoring the critical importance of designing energy-efficient solutions.

In 2025, we expanded our EPD program to the FortiGate 50G series, further demonstrating our commitment to transparency and continuous improvement in product sustainability.



Jorge Luis Juarez Cruz
*IT Infrastructure Coordinator,
Bradescard*

Fortinet's publication of a verified Environmental Product Declaration for the FortiGate 40F and FortiGate 50G Series is a remarkable achievement. As transparency and sustainability become increasingly critical across industries, this milestone sets a new benchmark for environmental accountability within the cybersecurity sector. For customers like us, having a cybersecurity partner that demonstrates verified environmental performance is increasingly important. As organizations work to reduce the footprint of their entire value chain, understanding the environmental impact of technology products is becoming a key factor in procurement and decision-making. Fortinet's leadership in publishing third-party-verified data reflects a strong commitment to sustainability and gives us confidence that our cybersecurity partner shares our environmental values and long-term objectives.

FORTINET PRODUCT CARBON FOOTPRINT CALCULATOR

Many Fortinet customers are committed to reducing GHG emissions across their own operations and IT suppliers. To support these efforts, the Fortinet Product Carbon Footprint Calculator provides transparent, product-specific lifecycle emissions data to inform sustainable decision-making.

This online tool, available exclusively to Fortinet employees, calculates the carbon footprint of selected products across their lifecycle, considering the country of use. In 2025, we aligned the methodology for estimating GHG emissions during

product use with our EPD approach, and third-party TÜV SÜD America verified that the methodology is compliant with the GHG Protocol.

In 2025, Fortinet expanded the calculator to cover more than 200 additional models, bringing the total to approximately 780 models across 60 countries. This tool helps customers understand the environmental impact of our products, optimize energy use, and make informed choices that align with their sustainability goals.



SUSTAINABLE PACKAGING

We design packaging that protects our products during transportation while reducing material use, avoiding waste, eliminating plastic where possible, and improving recyclability. In 2025, Fortinet's sustainable packaging initiatives helped address evolving regulations worldwide, including extended producer responsibility (EPR) requirements in the United States, the EU, and many other countries, and the EU Packaging and Packaging Waste Regulation (PPWR), which introduced stricter requirements on recyclability, reusability, and material reduction. Our eco-design approach supports regulatory alignment while advancing our circular economy objectives.

In 2025, we continued to implement sustainable packaging principles across new and existing product packaging. We prioritize materials that are recyclable, reusable, or derived from renewable sources, and we

design packaging to minimize both volume and weight. During the year, we developed 27 new packaging models using renewable materials such as corrugated fiberboard. All these models were certified by the Forest Stewardship Council® (FSC), and we shipped more than 341,000 FSC certified boxes.

When feasible, we eliminate plastic from our packaging. In 2025, we worked with an external packaging expert to replace polyethylene (PE) foam in several high-volume products. After reviewing multiple design options, we adopted reinforced molded pulp for small- and medium-sized products and corrugated cushioning for larger formats. This transition is expected to prevent approximately 91.6 metric tons of plastic from entering the environment. These new designs also avoided an estimated 458 metric tons of CO₂e emissions in 2025.

We also expanded our packaging initiative, piloted in 2023, to replace PE foam with Korrvu®/ Sealed Air cushioning for repurposed products shipped through our Return Merchandise Authorization (RMA) service. This packaging provides robust product protection, reduces plastic use by up to 95%, and is easily recyclable and reusable for return shipments. The initiative is expected to reduce GHG emissions by approximately 37 metric tons of CO₂e and eliminate an estimated 7.5 metric tons of plastics annually.



Reinforced molded pulp inserts secure small- and medium-sized products, reducing the need for plastic cushioning.

Corrugated cushioning protects larger products while minimizing material use and supporting recyclability.

ECO-FRIENDLY PACKAGING IN 2025

103

models of Fortinet's top-selling product lines are designed with eco-friendly packaging

~91.6

metric tons of plastic removed from product packaging

~458

metric tons of CO₂e emissions avoided through eco-friendly packaging

27

product packaging models certified by the Forest Stewardship Council® (FSC)



CIRCULARITY

We embrace circular economy practices that promote refurbishment, reuse, and responsible end-of-life management. Our approach focuses on extending product lifespans, keeping materials in use for as long as possible, and reducing e-waste. These efforts require close collaboration with customers, suppliers, and partners to identify and implement best practices.

Refurbishment and reuse

A key component of our circularity strategy is maximizing the life of existing equipment. Through our RMA process, customer-returned defective units are systematically evaluated for refurbishment and reuse. Units that meet our quality and performance standards are refurbished and reintegrated

into our RMA replacement inventory, and prioritized for customer replacements where possible. This approach reduces the need for new manufacturing while maintaining service quality. In countries where regulations restrict the import of reused parts, we have established local repair programs to service customer-returned components, reducing transportation-related emissions and improving turnaround times.

Fortinet Internal Refurbishing program

The Fortinet Internal Refurbishing program enables employees to return unused customer evaluation or demonstration units, or internally used testing and development units, at no cost, allowing these devices to enter a circular reuse process.

In 2025, 16,590 products were returned through this program—an 11% increase compared with 2024—with over 87% repaired and reintegrated for reuse. The program now operates in more than 30 countries. Units that cannot be repaired or reused are sent to certified recycling partners to ensure responsible material recovery or recycling.

Fortinet Product Donation program

We also extend product lifecycles through the Fortinet Product Donation program, which repurposes eligible hardware (excess inventory or Fortinet products from the Internal Refurbishing program) for nonprofits, schools, and underserved communities. This initiative supports digital inclusion while reducing the need for new equipment manufacturing and associated resource use.

16,590
units returned

87%
success rate on
repair of returns

GIVING TECHNOLOGY PRODUCTS A SECOND LIFE

In 2025, Fortinet expanded its Product Donation program, repurposing excess Fortinet hardware and IT equipment to support nonprofits and educational institutions worldwide. Donations—including FortiGate, FortiAP, laptops, smartphones, and monitors—help establish hands-on cybersecurity labs, advance digital inclusion, and support underserved communities.

By extending product lifecycles, the program reduces electronic waste and avoids associated GHG emissions.

2025 HIGHLIGHTS:



110+

laptops donated to Emmaüs Connect (France)

45

laptops donated to YouMeWe (Japan)

60

laptops donated to reBOOT (Canada)



300+

Fortinet hardware units donated to British Columbia Institute of Technology, University of Oregon and University of Arkansas

EMBEDDING SUSTAINABILITY AND CIRCULARITY IN PRODUCT AND PACKAGING DESIGN

Increasing employees' understanding of sustainability and circularity is fundamental to designing and delivering products and packaging with lower environmental impacts. In 2025, we held two workshops for R&D, product management, and operations teams. One session discussed sustainable design trends and the benefits of using Fortinet resources, such as EPDs and the Product Carbon Footprint Calculator, to design cybersecurity solutions with sustainability in mind. The other session explored how compliance with global eco-design and packaging regulations—including extended producer responsibility and EU Packaging and Packaging Waste Regulation—strengthens customer experience, ensures operational efficiency, and protects Fortinet's reputation. We recorded about 120 employee participations across these two workshops, enhancing our ability to embed circularity and sustainability considerations in product and packaging design and decision-making.

PRODUCT REGULATORY ENVIRONMENTAL COMPLIANCE

Fortinet is committed to meeting or exceeding all applicable environmental laws and regulations to protect human health and the environment. As a vendor of hardware security appliances, we strive to minimize the environmental impact of our products while ensuring compliance with evolving global standards.

To stay current with regulatory developments, we continually monitor legislation and guidance from multiple sources, including BOMcheck, the European Chemicals Agency, SGS, and Green Soft Technologies. We regularly review and update policies, procedures, and reporting templates to maintain compliance with all current regulatory requirements.

Fortinet's products comply with all applicable environmental directives and regulations worldwide. Our Design for Compliance approach integrates environmental considerations into our product development process.

A key tool in this process is the Fortinet Restricted & Declarable Substances List, which helps our design teams and contract manufacturers proactively address compliance requirements and avoid hazardous substances. In addition, Fortinet complies with the Waste Framework Directive (WFD), submitting required data to relevant databases and ensuring proper disposal and recycling of its products.

Regulatory compliance delivers measurable environmental benefits. For instance, lead in electronic solder has largely been replaced by safer alternatives in response to the EU Restriction of Hazardous Substances (RoHS) Directive. In the Fortinet FortiGate 51G, 6.4 grams of solder now contain no lead, reducing lead content by approximately 1.9 grams per unit compared to pre-RoHS designs.

KEY DIRECTIVES AND REGULATIONS

PRODUCT ENVIRONMENTAL COMPLIANCE

- EU RoHS Directive 2011/65/ EU RoHS "Recast" (RoHS 2) as amended by Directive (EU) 2015/863 and further amended by Directive 2018/739 and Directive 2018/740
- EU REACH Regulation 1907/2006
- U.S. SEC Conflict Minerals Rule
- EU Battery Regulation 2023/1542

WASTE MANAGEMENT

- EU WFD
- EU Waste from Electrical and Electronic Equipment (WEEE) Directive

HOW IS FORTINET PREPARING FOR THE EU ECO-DESIGN FOR SUSTAINABLE PRODUCTS REGULATION (ESPR)?

The ESPR introduces new requirements to improve the energy efficiency, durability, repairability, recyclability, and overall environmental performance of products sold in the EU. Thanks to our existing eco-design framework and strong compliance programs, Fortinet is well-positioned to meet these expectations. Our teams are already assessing impacts across product groups to ensure we continue delivering safe, reliable, and environmentally responsible solutions as the regulation is implemented.

Andrew Rybacha
Compliance manager
and member of the
CSR committee
at Fortinet



SUPPLIER ENGAGEMENT

Reducing Scope 3 GHG emissions from product manufacturing requires close collaboration across our supply chain. Engaging our suppliers is crucial to reducing environmental impacts and ensuring they share our commitment to sustainability.

A key step in this effort is ensuring that our suppliers are committed to setting and achieving science-based GHG emissions reduction targets. In line with this, we have established a near-term target, approved by the SBTi, to have 60.50% of our suppliers—by spend—set public, science-based GHG emissions reduction targets by 2029.

SBTi-validated near-term supplier target

60.50%

of suppliers, by spend, set science-based GHG emissions reduction targets by 2029

EMPOWERING PEOPLE AND COMMUNITIES

A secure and sustainable digital future depends on widespread cyber skills, literacy, and awareness across society. We are committed to supporting our own employees and building the cybersecurity workforce of the future. By empowering a broad range of individuals—within and outside Fortinet, from primary school students to career-level learners to experts in the field—we provide the training, knowledge, and opportunities needed to close the cybersecurity skills gap, foster a more inclusive workforce, and ensure a safe digital world for all.

2025 HIGHLIGHTS



914,800+

people trained in cybersecurity since 2022

91%

of our five-year goal achieved

890+

colleges and universities in the Fortinet Academic Partner program across **100+ countries**

7

external employer and workplace recognitions

OUR PEOPLE

At Fortinet, our people are essential to our success. We are committed to fostering a supportive and engaging workplace where employees can grow, contribute, and thrive. Our approach to people and workplace culture integrates our priorities around creating a positive work environment, enhancing the employee experience, promoting well-being, and encouraging meaningful community engagement.

INCLUSIVE WORKPLACE

Fortinet's core values—Teamwork, Innovation and Openness—shape how we collaborate and the culture we nurture across our global workforce. As we continue to grow globally, we remain focused on creating a workplace where employees feel connected, supported, and able to develop professionally. In 2025, we expanded opportunities for employees to build communities, strengthen leadership capabilities, and engage in activities that reinforce a positive workplace experience.

Employee Resource Groups

Employee Resource Groups (ERGs) are voluntary, employee-led communities that foster connection, peer support, and professional development. Open to all our employees, ERGs help broaden awareness, encourage collaboration, and enrich our global culture.

In 2025, Fortinet had 12 ERGs around the world, including three new ERGs that employees launched during the year:

- **Support Group for Parents of Neurodivergent Children (Brazil):** Provides peer support and raises awareness of neurodiversity across Fortinet Latin America (LATAM) through expert-led discussions and practical resources for families.
- **LATAM LGBTQI+:** Offers an open and empowering space for employees and allies to engage in dialogue, learning, and community building.
- **WISA (Women in Sophia Antipolis) Group (France):** Encourages networking and knowledge-sharing across roles and seniority levels, fostering connection and career development in technology.

Throughout the year, ERGs across regions hosted regular activities, meetings, and events that encouraged knowledge sharing, strengthened relationships, and highlighted the varied experiences and opportunities within the cybersecurity field. In EMEA, ERG members also joined monthly Coffee Chats—informal sessions to exchange perspectives on workplace experience, collaboration, and personal growth.

“Participating in the Support Group for Parents of Neurodivergent Children has been an extremely valuable experience for me. Having a safe space to share challenges, hear real stories, and learn from other parents makes a meaningful difference in my daily life. Gaining access to information about Fortinet's health plan benefits and attending talks that help us plan for our children's future also shows that this group goes beyond emotional support—it fosters knowledge, guidance, and hope.”



Felipe E Silva
Fortinet systems engineer, Brazil

STRENGTHENING ERG LEADERSHIP AND IMPACT

Building on the success of our 2024 pilot, we expanded our EMEA ERG collaboration initiative in 2025. A series of co-development sessions brought together EMEA ERG leaders in small groups to exchange experiences and discuss practical challenges—such as planning annual activities, boosting outreach, and recruiting members. Participants co-created actionable solutions, with key learnings and resources captured and shared via Fortinet's resources hub for ERGs, to support continuous capability building and knowledge sharing.

“The workshop series really helped me develop an understanding of how to approach an ERG strategically and systematically, and consequently be more effective and successful. The ERG workshops were also great to meet and network with other like-minded Fortinet colleagues who drive other local initiatives.”

Kathrin Hammer
Fortinet field marketing
director DACH,
ERG leader in Germany



RECOGNITIONS IN 2025



EMPLOYEE EXPERIENCE

Attracting, developing, and retaining skilled employees is critical to driving innovation and business success. We actively engage individuals with diverse backgrounds, experiences, and perspectives, sourcing talent through multiple pathways and hiring inclusively. From new hires and early-career professionals to experienced professionals and leaders, we empower Fortinet employees by providing opportunities for learning, growth, and meaningful contributions.

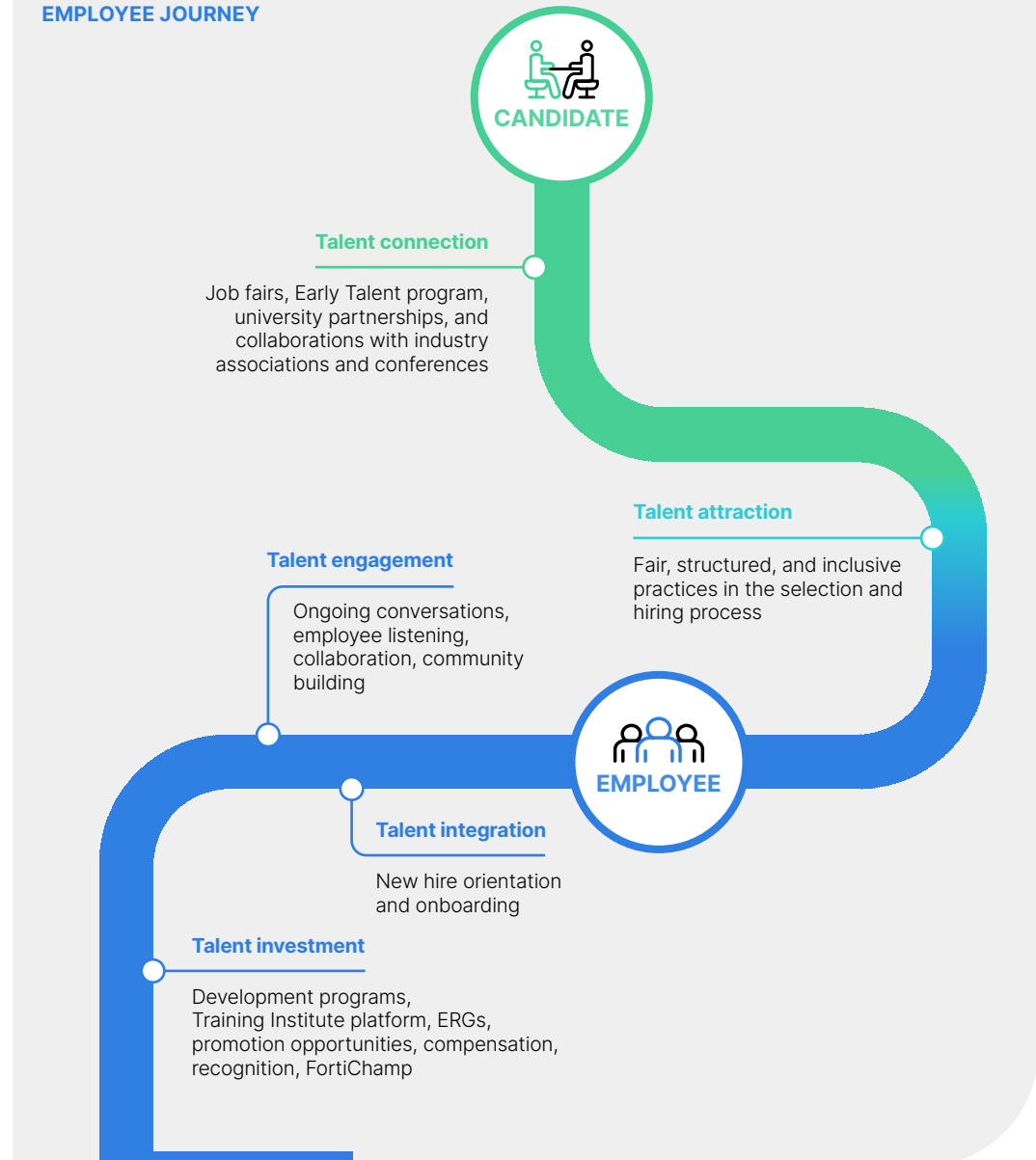
“Looking back, the biggest driver of my career growth was intrinsic motivation—curiosity, high standards, and a constant desire to learn. That drive pushed me to seek challenges, welcome feedback, and persist through setbacks. Equally important were the sponsors, leaders, and peers who trusted me, advocated for me, and offered honest perspectives. Learning to use my voice—asking for opportunities, setting boundaries, and staying true to my values—was pivotal.



Svetla Aleksandrova
Vice President EMEA
customer success and
support, Fortinet

Fortinet didn't just offer roles—it invested in me. Through trust, real responsibility, and timely feedback, it built my confidence and enabled my growth. Guided by grit, clarity, and strong values, I didn't just grow into bigger roles—I grew into a confident, impact-driven leader.

EMPLOYEE JOURNEY



OUR PEOPLE

CYBERSECURITY SKILLS GAP

Talent recruitment and hiring

We attract talent through a broad range of sourcing strategies to reach individuals with diverse experiences, skills, and perspectives.

Inclusive hiring practices

Hiring at Fortinet is designed to ensure fair, consistent, and accessible recruitment processes for all candidates. Our recruiters engage talent across regions using digital tools, targeted outreach, and relationship-driven engagement, supported by AI-enabled platforms and tailored online campaigns to broaden access to qualified candidates worldwide.

Additionally, job fairs, internship programs, university partnerships, and collaborations with industry associations continue to connect Fortinet with early-career talent and reach candidates with varied professional backgrounds. Fortinet uses inclusive job description principles and recruitment practices that support balanced candidate pipelines while remaining aligned with local market contexts and legal frameworks.

Early Talent program

Our Early Talent program prepares students and graduates for careers in cybersecurity and related fields. The program offers internship and graduate opportunities across technical and non-technical roles, combined with structured training, hands-on project experience, mentorship, and exposure to Fortinet technologies.

In 2025, we expanded our early-career offerings with the launch of a sales graduates program in the UK, an 18-month journey designed to help recent graduates and early-career professionals build foundational skills in technology sales.

Career fairs

Fortinet participates in regional career fairs to strengthen our employer brand and build talent pipelines. In 2025, this included events at top universities and virtual fairs—connecting with students, recent graduates, and emerging talent to raise awareness of Fortinet careers and expand our recruitment network.

2025 talent pipeline highlights

Nearly
2,600
hires worldwide

across
89
countries

**Talent development and retention**

Development is central to how we engage, empower, and retain our people. Fortinet's overall attrition rate was 11% in 2025, down from 12% in 2024 and reflecting continued workforce stability. We continue to strengthen our programs to equip employees with the skills, support, and opportunities needed to innovate and thrive in a rapidly evolving digital environment. Our programs are reviewed and refined annually to remain responsive to the evolving needs of our workforce, customers, and global operations.

New hire orientation and onboarding

Fortinet supports new employees from day one through an onboarding approach designed to encourage early engagement, help employees understand the company and its culture, and support a smooth transition into their roles.

Onboarding is delivered through regionally managed programs, that reflect local needs and practices while aligning with Fortinet's overall commitment to employee experience. These programs typically combine digital tools, orientation sessions, access to internal resources, and role-specific training to help new hires quickly navigate the organization and begin contributing effectively.

For example, in EMEA, the onboarding journey is supported through automated workflows within our human capital management system, complemented by HR-led orientation sessions and mandatory sales enablement training for sales employees. In Australia and New Zealand, new hires join in-person induction sessions and structured follow-ups designed to support engagement and integration.

“I joined Fortinet in September 2023 as a part of my master's program in management engineering from Audencia Business School, Nantes, France. Having previously worked in cybersecurity as an analyst, I was already familiar with Fortinet and its products. When I decided to make a career jump to project management, I wanted to remain in the cybersecurity industry. And, right on time, Fortinet had an opportunity that ticked all the boxes for me. After a six-month internship, I was offered a full-time position as a Consulting Systems Engineering (CSE) Project Manager, which I happily accepted. In my role, I work with the Executive Briefing Center events team and on major CSE projects.”



Bianca Binoy
CSE project manager, Fortinet

Leadership development programs

In 2025, Fortinet provided development opportunities to equip managers with the skills needed to enable talent, drive innovation, and deliver sustainable value for our customers. Our programs strengthened leadership capabilities; reinforced Fortinet's values of Teamwork, Innovation, and Openness; and promoted high-performing teams aligned with our business priorities.

Manage for Success, a leadership development program, focuses on strengthening core management and leadership capabilities. In 2025, 41 leaders across six cohorts completed the program. Our Ignite Your Potential program supports new and emerging leaders by building foundational people-management skills. Forty-four leaders participated in 2025.

To reinforce team alignment and performance priorities at scale, we brought groups of managers together, facilitating a series of meetings where a combined total of 150 leaders strengthened competencies, cohesion, and their impact on business results. We also delivered a leadership capability webinar series attended by over 2,000 current and emerging managers worldwide, covering topics such as coaching for retention, delivering effective feedback, and leading through organizational change.

Inclusive leadership is embedded across our leadership development approach. Our programs and webinars incorporate themes such as inclusive decision-making, collaboration, and psychological safety. In addition, foundational e-learning for people managers on inclusive leadership supports consistent people-management practices globally; 95% of our people managers completed the course in 2025.

Regionally tailored workplace training further supports managers and employees by addressing respectful conduct and preventing harassment and discrimination.

Employee development

Fortinet is committed to fostering continuous learning and professional growth for employees. Our employees have access to a digital learning platform that offers an extensive library of courses, videos, and curated learning paths covering technical, leadership, and professional skills. The platform enables employees to build capabilities with leaders at their own pace and apply new knowledge directly to their roles.

As part of this approach, the [Fortinet Training Institute](#) provides our employees with access to industry-recognized cybersecurity training and certifications, as well as learning content across a range of specialized areas, including sustainability. These offerings support continuous upskilling, enable career progression, and help close the broader cybersecurity skills gap.

Complementing formal learning, our [ERGs](#) offer voluntary, peer-led development by creating opportunities for all employees to share knowledge, enhance professional visibility, and build community across regions.

In addition, we delivered role-specific learning in 2025, including [sustainability workshops for R&D teams](#) to build internal capabilities and further embed sustainability considerations into product development.



Mentoring program

Fortinet continues to invest in mentorship as a key lever for employee development, knowledge sharing, and career progression. In 2025, we rolled out a six-month sales mentoring program in India and Singapore, engaging mentors and mentees to support the growth of high-potential talent through structured guidance and coaching. To ensure consistency and quality, we provide managers with guidance that offers perspective and outlines best practices for mentoring others.

Career development

Developing talent is a core part of how Fortinet supports employee growth, engagement, and alignment with business priorities. At the heart of this approach is Fortinet's Conversations, a set of shared management practices that guide how managers and employees connect, collaborate, and grow.

Managers across Fortinet engage employees through ongoing conversations to build strong relationships, support them in achieving their potential, and strengthen our collective capabilities and achievements. This continuous dialogue reinforces clarity, shared expectations, and alignment.

Fortinet's Conversations are designed around several types of conversations that vary in purpose, frequency, and depth, including:

- **Direction setting conversations** to align on strategy, priorities, and expectations.
- **Continuous conversations** to provide regular feedback, recognition, and course correction.
- **Coaching conversations** to support development, engagement, and potential.
- **Reflect conversations** to reflect on key milestones and discuss learnings.

Together, these conversations serve as an important mechanism for employee listening. They enable leaders to better understand how employees are experiencing their roles, where support or skill development may be needed, and how individual goals align with team and organizational objectives.

Talent review and succession planning

To ensure we have the right people in the right roles to support Fortinet's long-term success, we continued to strengthen our global talent review process in 2025. Talent reviews assess performance and potential across areas selected by the business, where leaders identify workforce objectives and build succession strength. Outputs inform personalized development plans, support enrollment in enablement resources or programs, and strengthen our talent pipeline to meet future business needs.

Health, safety, and well-being

We are committed to supporting the health, safety, and well-being of our workforce globally.

Our [Global Health and Safety Policy](#) outlines our approach to maintaining safe and secure workplaces, including workplace hazard management, emergency preparedness, and compliance with local occupational health and safety regulations. In 2025, employees across regions participated in targeted health and safety initiatives, for example:

- **Canada:** We introduced an Employee Health and Safety checklist to raise awareness of workplace safety practices, employee rights, and potential risks, supporting proactive risk management.
- **EMEA:** Employees received training on health and safety awareness, fire safety, and ergonomic considerations for display screen equipment.
- **India:** We introduced an Annual Health Check-Up program to promote preventive healthcare and proactive health management across the workforce.
- **Taiwan:** Employees joined sessions on fire and earthquake preparedness and participated in practical exercises, including the proper use of fire hydrants and fire extinguishers.

We also promote employee well-being through a holistic approach that encompasses financial, physical, emotional, social, and other forms of support. Programs are available to our employees and their families, with offerings adapted to local market contexts. For example, some programs provide 24x7, 365-day access to confidential counseling and resources in over 100 languages, covering topics such as stress management, relationships, life transitions, workplace challenges, confidence-building, and more.

In 2025, local and regional well-being initiatives complemented these programs. Examples included:

- **France:** Wellness Week featured nutrition consultations, chair yoga, and self-confidence workshops to support employee well-being and stress management.
- **India:** Our Bangalore site launched an in-house gym facility, open during designated hours, to promote physical health and well-being. The Crèche Enrollment facility also debuted, allowing employees to select childcare centers that best suit their needs, supporting working parents and fostering a family-friendly workplace.
- **LATAM:** Health fairs (in person in Brazil, Colombia, and Mexico, and virtual across the region) offered activities and resources covering mental health, dental care, vision diagnostics, active breaks, office massages, breast cancer awareness talks, financial wellness, and exercise, engaging employees across local offices and online.
- **Mexico:** A three-month nutritional challenge offered personalized guidance from a nutritionist, helping participants build healthy lifestyle habits and achieve wellness goals.
- **United States:** All U.S. sites have access to the Modern Health platform, which includes resources such as therapy and coaching sessions for employees and dependents, unlimited live and pre-recorded group sessions, and a library of self-paced digital programs, meditations, courses, and more.

**EMPLOYEE BENEFITS SUPPORTING WELL-BEING**

Our benefits programs play a critical role in supporting employees' well-being. These programs are designed around three pillars—financial, physical, and psychosocial well-being—to ensure employees receive meaningful support aligned with their needs.

Fortinet employee benefits*

Financial	— Restricted Stock Unit plan — Stock awards — Incentive compensation programs — Retirement plan — Corporate discounts — Recognition and rewards programs
Physical	— Medical plans tailored to local markets — Access to on-site gyms where available — Access to global and local health and wellness initiatives — Annual health check-up
Psycho-social well-being	— Well-being seminars and activities — 24/7 access to confidential counseling through the Wellness Assistance program — Paid volunteer time off — Company-supported volunteering opportunities — Global cash matching program — Childcare and parenting support — Surrogacy and adoption support

* While many Fortinet employee benefits are available globally, some vary based on regional needs.

EMPLOYEE COMMUNITY IMPACT

Our commitment to community engagement and social impact extends well beyond the workplace. We encourage our employees to volunteer in community projects, and Fortinet matches their donations to eligible nonprofit organizations—up to \$1,000 per employee annually.

In 2025, we launched an internal blog series that spotlights employee volunteers, the causes they support, and their impact. This program has increased volunteer participation and reinforced a culture of giving back to the communities where we live and work.

In 2025, Fortinet employees led volunteer and fundraising initiatives across LATAM, North America, Europe, Africa, the Middle East, and Asia-Pacific, supporting digital inclusion, education, health, and essential needs in their local communities.



2025 GLOBAL IMPACT AT A GLANCE

750+

students reached
through cybersecurity
awareness workshops

\$115,000+

raised globally for nonprofit
and community organizations

500+

children and families supported
through education, health, and
seasonal campaigns

Clothing, food, hygiene products, and
essential supplies distributed across

10

countries

FOCUS AREAS

Digital skills and online safety

Employees delivered cybersecurity awareness sessions to students across Asia (India), Europe (Italy, Poland, and Spain), LATAM (Brazil, Colombia, and Ecuador), and North America (USA), promoting phishing prevention, password security, and responsible online behavior.

Children and youth empowerment

Initiatives supported vulnerable children and families through scholarships, disability services, school supplies, and seasonal campaigns across Africa (South Africa), Asia (India), Europe (France, Ireland, and the UK), and LATAM (Bolivia, Brazil, Mexico, and Paraguay).



Health, well-being and essential needs

Employees contributed to homelessness relief, cancer support organizations, disaster recovery, and senior citizen care initiatives across Africa (South Africa), Asia-Pacific (Australia), LATAM (Colombia) and North America (Canada and the USA).



Employee and partner fundraising

Significant employee-led fundraising efforts included campaigns in Africa (~R25,000 raised in South Africa), Europe (£80,000 raised in Ireland and the UK), and North America (~CA\$35,000 raised in Canada).



“My profound and deeply rewarding experience bringing digital awareness to the young students of the Miguel Iturralde N° 2 Educational Unit, in Tumbaco, Ecuador, was far more than a technical task. It was a heartwarming opportunity to transcend my usual role and deliver to these young students essential learning that will serve them for years to come. Thanks to invaluable initiatives such as Cybersecurity for Kids, Fortinet offers us a priceless gift: ready-made, polished

material, saving countless hours of development. This makes our work easier and motivates us to replicate this mission everywhere, acting as passionate ambassadors for our company and, most importantly, as true agents of change within our own communities.”

Esteban Tayo

Fortinet Systems Engineer, Ecuador



CYBERSECURITY SKILLS GAP

The rapid evolution of cyberthreats—including AI-driven attacks—continues to increase pressure on organizations to maintain a capable, scalable cybersecurity workforce. According to the [Fortinet Training Institute 2025 Cybersecurity Skills Gap Global Research Report](#), 49% of cybersecurity leaders are concerned that AI will increase both the volume and the sophistication of cyberattacks. While advanced technologies are essential, a skilled cybersecurity workforce remains the most critical line of defense.

Through the [Fortinet Training Institute](#), we deliver industry-recognized certifications and continuously updated courses to equip cybersecurity professionals with the skills required to address evolving threats. These programs are foundational to our workforce development initiatives, enabling learners—from early-career professionals to seasoned practitioners—to upskill, reskill, or transition within the cybersecurity field. We deliver industry-recognized certifications and continuously updated courses to equip cybersecurity professionals with the skills required to address evolving threats.

Building on this foundation, we collaborate with governments, private-sector partners, academic institutions and nonprofits to develop a resilient, diverse, and sustainable global talent pipeline that prepares the workforce of the future. While programs for students help cultivate early interest in cybersecurity, our certification program ensures that industry professionals remain proficient and ready to meet any emerging challenges. By strengthening skills at all levels, we contribute to a more resilient digital ecosystem and a safer society.

CYBERSECURITY SKILLS PLEDGES

Train
1 million
people in cybersecurity by
2026 (2022 base year)

PROGRESS:
914,800+
people trained since 2022

91%
of the goal achieved

Train
75,000
individuals in cybersecurity
in Europe by 2027 (2024 base year)

PROGRESS:
42,200+
people trained in Europe since 2024

56%
of our goal

EUROPEAN COMMISSION CYBERSECURITY SKILLS ACADEMY PLEDGE PROGRESS



In 2025, Fortinet advanced its commitments to the European Commission through the [EU Cybersecurity Skills Academy](#), a flagship EU initiative to strengthen cyber resilience and enhance critical skills across member states, as part of Europe's broader Digital Decade objectives. Through this public-private partnership, we contribute industry expertise, training, and certifications to help build a more resilient and inclusive regional workforce.

Progress toward 2027 commitments

PLEDGE	PROGRESS THROUGH 2025
Train 75,000 individuals in cybersecurity in Europe by February 2027 (2024 base year)	42,200+ individuals trained since 2024, including 22,500 in 2025
Enable 5,000 students to access Fortinet cybersecurity curriculum, labs, self-paced training, and certifications through the Fortinet Academic Partner program	1,300+ students reached, including 950+ in 2025
Deliver cybersecurity and digital safety education to 10,000 EU students aged 5–18 through Fortinet's Security Awareness Curriculum	750+ young learners reached, all in 2025

We expanded our footprint across all 27 EU member states, partnering with 214 academic institutions, including 27 new partners in 2025. Notable additions to the [Industry-Academia Network](#) of the Cybersecurity Skills Academy included [CodeAcademy](#) (Lithuania), the [University of Girona](#) (Spain), and [Scheer School of Digital Sciences](#) at Saarland University (Germany).

Our partnership with the [European Union Agency for Cybersecurity \(ENISA\)](#) further strengthens alignment with EU workforce standards. Fortinet Training Institute courses map to both the [European Cybersecurity Skills Framework \(ECSF\)](#) and the [NICE Framework](#), providing learners with structured, role-based [pathways](#) that support smooth transitions into cybersecurity careers.

Building on this model, we are actively engaging with governments and cyber organizations in other regions to replicate similar public-private partnerships, helping create a global community committed to closing the cybersecurity skills gap and strengthening defenses against rising, AI-driven threats.

BUILDING A SUSTAINABLE TALENT PIPELINE

Founded in 2015, the Fortinet Training Institute* is the cornerstone of our global efforts to close the cybersecurity skills gap by making industry-leading cybersecurity training and certification accessible to everyone—removing financial, geographic, and technological barriers. As AI increases the scale and sophistication of cyberthreats, demand for skilled professionals has risen, requiring training and certification to keep pace with the evolving attack landscape.

We deliver role-based training and certification pathways that support learners at every stage of the cybersecurity journey, including:

- **Professionals at all career levels**, from foundational certifications for those entering the field, through core training on secure networking and Fortinet's flagship technologies, to advanced architecture and expert-level certifications, enabling continuous upskilling and progression to deep technical expertise.
- **Adults reskilling or transitioning into cybersecurity**, equipping career changers with the practical knowledge and credentials needed to enter the profession.
- **Post-secondary and young adult students**, preparing the next generation of cybersecurity professionals with industry-aligned curricula, labs, and certifications.
- **Secondary school students**, building early technical skills and awareness of cybersecurity career pathways.
- **Primary school students**, fostering foundational cyber awareness and safe digital behaviors through free, age-appropriate curricula, while inspiring future generations to pursue cybersecurity careers.

*Initially launched as the Fortinet Learning Center, later renamed the NSE Training Institute; it became the Fortinet Training Institute in 2020.

Our work is rooted in collaboration. By partnering with universities and higher education institutions, schools, ministries of education, NGOs, governments, and industry organizations worldwide, we are helping create a diverse and sustainable talent pipeline capable of protecting communities, economies, and critical systems. These partnerships also accelerate progress toward our public pledges and enable us to scale impact in regions where cyber skills development is most urgently needed.



Melonia da Gama
Director of training and
learning programs and member
of the CSR committee at Fortinet

“The cybersecurity workforce of tomorrow depends on the education and training we invest in today. By breaking down barriers to cybersecurity careers, we can expand the global talent pipeline and reinforce the critical role cybersecurity plays in society. Building foundational skills and a problem-solving mindset early prepares the next generation to succeed in AI-enabled digital environments, while public-private partnerships help turn that potential into job-ready talent and a stronger cybersecurity ecosystem.”

FROM EARLY CYBER AWARENESS TO PROFESSIONAL MASTERY



Primary education

Foundational cyber awareness

- Fostering safe digital behaviors through age-appropriate education and community engagement
- Program callouts: Security awareness curriculum, online security awareness teacher training, employee engagement and volunteerism



Secondary education

Early skills and career awareness

- Building cyber awareness and introducing cybersecurity skills and career pathways
- Program callouts: Security, online security awareness teacher training, fundamental and introductory cybersecurity training and certifications



Post-secondary education

Job-ready cyber skills

- Equipping students with industry-aligned skills through education partnerships
- Program callout: Academic Partner program, hands-on experience (labs) and certifications

NSE CERTIFICATION PROGRAM

At the core of Fortinet's approach to global cyber skills development



Professional mastery

Continuous upskilling and expertise

- Enabling continuous learning and career advancement for cybersecurity professionals
- Program callout: Fortinet Certified Trainer program, Authorized Training Centers, Fortinet Training Institute



Career transition and reskilling

Pathways into cybersecurity careers

- Expanding access to cybersecurity careers for adults who are transitioning or reskilling
- Program callouts: Veterans program, Education Outreach**

** Including initiatives for women in cybersecurity.

FORTINET CYBER SKILLS RESEARCH AND THOUGHT LEADERSHIP

Our commitment to closing the global cybersecurity skills gap is reinforced by extensive research, global partnerships, and influential thought leadership. In 2025, we contributed to several major international initiatives that are shaping how governments, industries, and educational institutions build resilient cyber workforces.

Fortinet played an active role in the World Economic Forum community on bridging the cyber skills gap, which includes capacity-building initiatives providing practical recommendations for fostering a sustainable cybersecurity workforce. We also contributed to the World Economic Forum whitepaper, *Growing Cyber Talent Through Public-Private Partnerships*, which highlights how cross-sector collaboration can accelerate workforce development and defines the foundational elements required for successful public-private coordination. These contributions reflect Fortinet's commitment to advancing systemic solutions—not just for our customers, but also for society's broader digital resilience.

In 2025, we also published *AI is revolutionizing cybersecurity. How should we train the next generation of defenders?*, based on proprietary insights from the *Fortinet Training Institute 2025 Cybersecurity Skills Gap Global Research Report*. The report highlights two parallel imperatives: deploying advanced security technologies such as AI and investing in human talent capable of using them effectively. This dual focus reinforces the need for organizations worldwide to develop technological and human capacity to navigate an increasingly complex threat landscape.

Fortinet's thought leadership also extends to high-level policy engagement. In 2025, we testified before the U.S. House committee on Homeland Security at the hearing, *Preparing the Pipeline: Examining the State of America's Cyber Workforce*. We emphasized the urgency of addressing the national shortfall of more than 500,000 cybersecurity professionals and advocated for broader recognition of alternative career pathways, including certification-based education and hands-on training. Our recommendations highlighted

the importance of reducing barriers to entry and supporting non-traditional learners to strengthen national security.

Fortinet also deepened its global leadership role by contributing to the *Global Conference on Cyber Capacity Building (GC3B)* in Geneva, Switzerland, which brought together more than 600 participants from over 100 countries. Workforce development emerged as a dominant theme, underscoring the need for scalable training ecosystems, talent attraction strategies, and continuous upskilling. During the event, we reinforced how Fortinet Training Institute programs, collaborations with NGOs, governments, and academic institutions, and accessible, no-cost training directly support inclusive, long-term capacity-building on a global scale.



2025 FORTINET TRAINING INSTITUTE AWARDS



Cybersecurity Breakthrough Award
WINNER: Best Security Awareness program



Global InfoSec Awards
WINNER: Cybersecurity Training and Certification
WINNER: Security Awareness and Training



Globe Awards
GOLD WINNER: Cybersecurity Education and Training
GOLD WINNER: Security Awareness and Training



Cybersecurity Excellence Awards
WINNER: Cybersecurity Training
WINNER: Certification program
WINNER: Security Awareness program

PREPARING THE NEXT GENERATION

The [Fortinet Academic Partner program](#) bridges education and employment by embedding industry-recognized cybersecurity training and certification into higher education curricula worldwide. Through partnerships with colleges, universities, and vocational institutions, Fortinet integrates its NSE Certification curriculum, hands-on labs, and certification pathways directly into academic programs—equipping students with practical, job-ready skills before they enter the workforce.

To support high-quality delivery, we provide a comprehensive suite of resources for academic institutions and instructors. Monthly onboarding sessions guide new partners who are incorporating Fortinet content—such as labs, course modules, and certification preparation—into their programs. Live train-the-trainer sessions connect educators with Fortinet experts who offer technical insights, best practices, and guidance on effective instruction.

In 2025, 110 new academic institutions joined the Fortinet Academic Partner program, including Poznań University of Technology in Poland, De La Salle University in the Philippines, and the National University of Colombia, integrating Fortinet training and certifications into their graduate programs in areas such as computer and IT security, as well as related fields.

Hands-on learning remains a defining strength of the Academic Partner program. In 2025, we introduced a new Education security operations center (SOC) course and lab environment, offering immersive training in threat detection, incident response, and cyberattack simulation. Early adopters included Metropolitan State University (Minnesota, USA) and the University of Ontario Institute of Technology (Ontario, Canada).

To support the practical components of these programs, the Academic Partner program collaborated closely with the [Fortinet Product](#)

[Donation program](#). In 2025, Fortinet donated equipment to various partner institutions, including the University of Oregon, supporting the development of a training SOC environment.

Fast Track workshops further complement academic curricula, delivering intensive, applied cybersecurity sessions. In 2025, Fast Track workshops reached more than 50 students at Sastra University in India and were also delivered at multiple universities and a high school in Australia.

Fortinet Academic Partner program

890+ colleges and universities
(including **110** added in 2025)
across **100+** countries

EXPANDING REGIONAL IMPACT BEYOND THE EU: PARTNERSHIP WITH MOROCCO

In 2025, we partnered with Morocco's Ministry of Higher Education, Scientific Research, and Innovation to support the national Code 212 initiative, which aims to train 100,000 Moroccan students in cybersecurity by 2030.

Fortinet's contributions in 2025:

- Free access to cybersecurity curriculum, labs, and certification across 12 universities (280+ students trained).
- In-person train-the-trainer session for 25+ educators nationwide.
- Ongoing support for events, labs, and academic activities, including repurposed Fortinet equipment used for learning environments.

This partnership emphasizes sustainable capacity building, supports equitable access to high-quality cybersecurity education, and positions Morocco as a regional leader in cyber talent development.

SCALING HIGH-IMPACT TRAINING IN INDIA

India remained a high-growth region for Fortinet's training programs in 2025. Through collaborations with organizations—including ASAP Kerala, BFSI Sector Skill Council, CareerTiQ, CCC, EduSkills, and ICT Academy—we expanded access to career-ready cybersecurity education nationwide.

2025 impact:

- 2,000 students trained through EduSkills (24,500+ since 2023).
- 600 students certified through CareerTiQ, with 280+ placed in cybersecurity roles.
- Fortinet courses integrated into undergraduate programs at leading institutions, with participation in multiple university boards of studies to support curriculum modernization.

We also strengthened engagement with national and state-level skilling bodies and industry forums, aligning academic pathways with workforce demand. Together, these efforts enhance job readiness and help build a future-ready cybersecurity workforce in India.



Students practicing Fortinet Certified Professional (FCP) lab exercises.



ISTS students after completing the FCP training and ready for certification.



Fortinet addressing more than 80 vice-chancellors from various universities in India.

FORTINET EDUCATION OUTREACH PROGRAM: EXPANDING ACCESS TO UNDERREPRESENTED COMMUNITIES

The cybersecurity skills gap cannot be addressed without ensuring equitable access to education and careers. Fortinet's Education Outreach program partners with nonprofit organizations serving veterans, military spouses, women, and students from underserved or marginalized communities. Through strategic collaboration with 53 partners, including five added in 2025, learners receive free cybersecurity training, self-paced and instructor-led coursework, and access to industry-recognized certifications. In addition, we connect participants with our employer ecosystem to further support job placement. By the end of 2025, more than 12,500 learners globally had participated in the Education Outreach program. This included over 5,800 in 2025, who earned approximately 1,300 certifications—demonstrating the program's growing global reach and its ability to drive transformative impact for individuals and communities.

Fortinet Veterans program

The Fortinet Veterans program continues to play a pivotal role in building a more diverse and resilient cybersecurity workforce by supporting military service members, veterans, and their spouses as they transition into civilian cyber careers. Participants gain free access to self-paced courses, hands-on labs, and industry-recognized certifications, while partner organizations provide tailored career guidance, coaching, and employment support. This integrated model helps veterans translate their military experience into in-demand cybersecurity skills and long-term professional growth.

Since launching in 2018, the program has delivered over 14,000 courses, with more than 2,200 veterans and spouses actively engaged since 2020. In 2025, more than 700 participants advanced their skills through flagship initiatives, including the Networking Fundamentals Bootcamp and the Veterans Bootcamp, held in conjunction with Education Outreach partners. These programs provided structured, immersive training—equipping participants with competencies ranging from networking essentials to safeguarding critical infrastructure systems. The Fortinet Veterans program is further supported by the [Veterans Program Advisory Council](#), which comprises representatives from the Five Eyes countries—Australia, Canada, New Zealand, the United Kingdom, and the United States. In 2025, the council continued to provide strategic guidance on expanding upskilling opportunities, increasing program accessibility, and strengthening pathways into cybersecurity roles for transitioning military families.

Fortinet's engagement in 2025 also included a range of targeted partnerships and outreach efforts:

- **Partnership with WiCyS Military Affiliate:** Together, we supported women veterans entering the cybersecurity field by offering training resources and highlighting the unique strengths they bring to cyber roles.
- **Veterans Affairs Canada Digital Employment Series:** Fortinet and Tech Vets Canada engaged hundreds of Canadian veterans and military spouses, offering practical insights into cybersecurity career pathways and how participants can leverage Fortinet's training programs to enter the field.

- **Hire Heroes USA Professional Development Conference:** Fortinet trainers delivered sessions on web application security for an audience composed of 40% veterans and 70% women, strengthening technical awareness and supporting the organization's mission to advance career opportunities for military-connected communities.
- **VetSecCon'25 Virtual Conference:** Fortinet contributed expert insights through the session "Proactive Defense—Unlocking the Power of Threat Hunting in Cybersecurity," reinforcing our role as a trusted training and knowledge partner within the veteran community.

“Perseverance is the most valuable skill the military gave me. It teaches you to never give up, no matter how difficult things get.

Bianca Caouette, Education Outreach partner

Stress management skills from the military have proven invaluable. Cybersecurity is a demanding field, and the ability to stay calm under pressure makes a difference.

Daniel Hruska, Education Outreach partner

[Read the interview.](#)

FORTINET'S VETERAN PARTNERS



Women in cybersecurity

Women are significantly underrepresented in the cybersecurity field, accounting for only 12%–22% of the global workforce¹. Through the Fortinet Education Outreach program, we partner with women's associations and professional networks worldwide to expand access to cybersecurity learning, certifications, and career pathways. These partnerships focus on dismantling systemic barriers, strengthening technical and leadership skills, and enabling women to progress at every stage of their cybersecurity journeys.

WiCyS

In 2025, we expanded our collaboration with WiCyS, whose global community now includes more than 11,000 members, by extending our support to the Australian and Indian chapters and contributing additional instructors to the Networking Fundamentals Bootcamp. This instructor-led program provides participants with the essential technical foundation needed to pursue cybersecurity roles.

At the 2025 WiCyS annual conference, we hosted a hands-on SOC workshop, attended by over 150 women, that offered a realistic environment to build troubleshooting and incident-response skills comparable to those required for early SOC analyst roles.

Women4Cyber, Women in Tech, and Circle of Women in Cybersecurity

In Europe, we supported Women4Cyber, Women in Tech, and Circle of Women in Cybersecurity (CEFCYS) across training sessions, conference participation, and mentoring circles. These initiatives connected women with pathways to Fortinet certifications and introduced them to employers seeking new cybersecurity talent.

Expanding access for young women and girls

Across several regions, we contributed training content and awareness resources targeted at students and young women exploring cybersecurity careers. These grassroots efforts play a critical role in increasing long-term gender diversity in the industry.

NETWORKING FUNDAMENTALS BOOTCAMP

In 2025, we expanded our Networking Fundamentals Bootcamp worldwide, specifically to empower underrepresented talent.

Program expansion in 2025

- Offered two 12-week global bootcamps
- Delivered sessions across multiple time zones to ensure global accessibility
- Made the program available to all Fortinet Education Outreach and Veteran partners

Program outcomes

- 700+ participants around the world
- Training covered essential networking, data communication, and IT fundamentals, preparing participants for roles in IT support, infrastructure, and entry-level cybersecurity

Combining self-paced training with weekly instructor-led sessions helps learners—particularly those reskilling or transitioning into the field—build confidence and deepen their technical understanding. Cohort-based delivery also fosters peer learning, collaboration, and professional networking, enabling participants to progress together while developing job-ready, foundational skills and contributing to a more diverse global cyber workforce.

**VOICES FROM OUR LEARNERS**

The training helped me see that a company's security is only as strong as its people. Before the training, I knew very little about Fortinet products—now I can connect technical knowledge to business protection.

Sofia Alejandra Martinez Cruz
Master's student in cybersecurity and LAIC member

The training was highly practical. The Fortinet Certified Professional NSE 4 path made it easy to focus on skills relevant to the roles I want in network security and SOC operations.

I. Mammad, LAIC member

REGIONAL SPOTLIGHT: AFRICA

Through the Pan African Information Communication Technology Association (PAICTA) Cybersecurity Certification Programme, we continued to support inclusivity and digital empowerment across Africa in 2025. We provided course materials and access to certifications to help women and girls gain essential cybersecurity competencies. Approximately 1,600 people aged 18–25 participated in the program during the year, completing over 2,800 courses and earning more than 400 certifications.



PAICTA's Cybersecurity Certification Programme aligns perfectly with my academic and career goals, and this training helped me solidify my commitment in my journey to becoming a skilled certified professional cybersecurity and networking engineer. Gaining the skills from the training makes me eligible for a swift transition from intern to permanent employee. Acquiring a Security Operations certification made me even more committed to upskilling.

Paul Mpho Sesinyi
Recent PAICTA student

1. According to different data points from [International Women in Cyber Day](#) and [ISC2 Cybersecurity Workforce Study](#).

CYBERSECURITY PROFESSIONAL UPSKILLING

Fortinet helps cybersecurity professionals, including our customers, partners, and employees, to improve their skills through our flagship NSE Certification program and global network of Authorized Training Centers (ATCs).

Fortinet NSE Certification program

The NSE Certification program is the cornerstone of our approach to addressing the cybersecurity skills gap. Established in 2015, the program has issued more than 1.8 million certifications worldwide through 2025, making it one of the most widely adopted cybersecurity certification programs in the industry. From this foundation, we can deliver high-quality training and certification across all our education and outreach initiatives, demonstrating the program's scalability and impact.

The program meets learners wherever they are in their professional journeys. Instructor-led, hands-on, role-based learning that equips security professionals with practical, job-ready skills is at the core of the program. Free self-paced courses are also available to those seeking flexible learning, skill refreshers, or foundational knowledge. The program defines four career roles in today's most prominent cybersecurity domains—network security, SASE, cloud security, and security operations—and provides a structured pathway to develop professionals into cybersecurity experts. AI is integrated across the curriculum to help learners understand emerging threats and how to leverage advanced technologies for defense.

In 2025, the NSE program introduced seven new courses and exams—including FortiOS Administrator and Security Operations Architect—aligning it more closely with emerging skill needs and helping professionals stay current in a rapidly evolving threat landscape.

Fortinet Certified Trainer program

Fortinet Certified Trainers (FCTs) are essential to our global instructor-led learning ecosystem, ensuring consistent, high-quality, hands-on cybersecurity education. Our network of 142 FCTs spans EMEA, Asia Pacific, North America, and Latin America, and includes both Fortinet employees and ATC trainers. Each FCT receives ongoing support through mentorship and continuous learning opportunities, including “Train the Trainer” sessions and regional webinars, to stay current with new courses and technology updates. By combining rigorous assessment, structured development, and global reach, the FCT program empowers trainers to deliver impactful instruction, strengthen cybersecurity skills, and help build the next generation of professionals worldwide.

Authorized Training Centers

To further scale access to professional skills development, Fortinet's ATC network provides instructor-led NSE Certification training through accredited organizations in more than 160 countries and territories. Over 110 ATCs deliver cybersecurity training in 26 local languages, helping ensure that cybersecurity education is culturally relevant, regionally accessible, and globally consistent. In 2025, we further expanded this network, welcoming five new ATC partners.

A STRUCTURED PATHWAY FOR CYBERSECURITY CAREERS

Industry research confirms the increasing importance of cybersecurity certifications in hiring and career progression. Fortinet's 2025 [Global Cybersecurity Skills Gap Report](#) found that 89% of IT leaders prefer candidates with certifications, reflecting a growing reliance on credential-based hiring to validate practical skills. For individuals, certifications are associated with faster job placement, greater mobility, and higher earning potential—even for those from non-traditional backgrounds.

Fortinet's certification framework offers progressive stages that align with exam levels and professional roles across the talent pipeline.

- **Fortinet NSE 8** validates expert proficiency in complex network security design, configuration, and troubleshooting. It is Fortinet's highest-level certification and represents one of the most respected qualifications in the industry.
- **Fortinet NSE 7** is designed for learners who need to design, administer, monitor, and troubleshoot specialized solutions across secure networking, SASE, cloud security and security operations.
- **Fortinet NSE 4, NSE 5, and NSE 6** provide role-based training across three key cybersecurity domains: secure networking, SASE, cloud security and security operations.
- **Fortinet NSE 3** recognizes the ability to perform high-level operations on FortiGate Next-Generation Firewalls. Learners gain essential skills in configuring and operating FortiGate features.
- **Fortinet NSE 1 and NSE 2** validate foundational cybersecurity knowledge required for entry-level positions. The curriculum covers today's threat landscape, digital safety essentials, and core cybersecurity concepts, and was recently translated into Spanish, French, and Portuguese.

110+
ATCs

In more than
160
countries and territories

Teaching in
26
languages

CYBERSECURITY FOR ALL AGES: CULTIVATING RESPONSIBLE AND SAFE DIGITAL CITIZENS

As digital engagement continues to increase among children and young people, so does exposure to online risks—including cyberbullying, phishing, password attacks, and the misuse of personally identifiable information. As a global leader in cybersecurity, we equip the current and next generations of digital citizens with the fundamental knowledge needed to stay safe online—at school, at home, and anywhere they go.

Fortinet supports cybersecurity education globally through free, multilingual curricula and awareness programs that help educators and students in primary and secondary schools build essential cyber literacy. These initiatives form a critical pillar of our broader commitment to closing the cybersecurity skills gap and creating long-term pathways to a more resilient, cyber-aware society.

The Fortinet Security Awareness and Training Service equips faculty and staff in primary and secondary schools with the skills and knowledge they need to make smarter choices as they navigate the connected digital world. Available at no cost and in local languages in Australia, Brazil, Canada, India, Saudi Arabia, the United Kingdom, and the United States, the service is accessible to approximately 12 million education staff. [Learn more.](#)

To help learners navigate rapidly evolving cyber risks, we introduced two new AI-focused modules to the Fortinet Security Awareness and Training Service in 2025. Generative AI (GenAI) introduces core concepts, responsible use, benefits, limitations, and common misconceptions. AI-Powered Threats raises awareness of deepfakes, voice cloning, AI-driven malware, privacy risks, and misinformation campaigns.

Additionally, we added educator-specific modules that provide guidance on cyberbullying prevention, strategies for safe online learning, and the effective use of educational technologies. Integrating these modules prepares young digital citizens—and their educators—for a world where AI plays a central role in innovation and cyber risk.

To support learners directly, the Security Awareness Curriculum provides age-appropriate resources for students aged 4–18, accessible to over 70 million K–12 (primary and secondary education) students globally. Available at no cost in multiple countries, the curriculum covers key themes—including Online Presence, Digital Safety, Secure Privacy, Ethical Integrity, Digital Impact, Cybersecurity Landscape, and Online Information—providing students with fundamental knowledge on topics such as creating strong passwords, managing online identities, navigating social media responsibly, recognizing cyberbullying, and understanding basic cybersecurity concepts.

In 2025, the curriculum was expanded with the introduction of a new Novices learning group (ages 8–11), further strengthening age-appropriate progression. The curriculum is organized into five learning groups—Rookies (4–7), Novices (8–11), Specialists (12–14), Leaders (15–18), and Future Professionals (electives for 15–18).

In 2025, we also hosted “Take Your Kids to Work” at our Brazil, Canada, and Mexico offices, giving more than 70 of our employees’ children the opportunity to see where their parents work and to experience our workplace environment. As part of the day, the children also received an introduction to cybersecurity, which helped inspire curiosity and awareness of digital safety from an early age.

ARMY WELFARE EDUCATION SOCIETY

In 2025, Fortinet signed a MoU with the Army Welfare Education Society to launch its first large-scale K–12 Cybersecurity Awareness program in India.

This partnership provides structured access to:

- 137 Army Public Schools
- Nearly 230,000 students
- More than 8,500 teachers

Following a successful pilot in two schools, implementation expanded to four additional locations by the end of 2025. Educators reported strong engagement and high relevance of the program’s practical lessons to students.

In addition, Fortinet collaborates with Heritage Xperiential Learning School (formerly The Heritage School, Gurgaon) to deliver cybersecurity awareness education. This collaboration is expected to expand across two campuses, reaching nearly 7,000 students and more than 640 teachers.

FORTINET EMPLOYEE VOLUNTEERING: EXTENDING CYBER AWARENESS TO YOUTH

Employee volunteerism also plays an important role in expanding cyber literacy. Through our global engagement initiative, Fortinet employees deliver interactive awareness sessions to students aged 8–14, using ready-to-use training resources and practical exercises. These efforts help young learners develop safe online habits, understand digital risks, and build foundational cybersecurity knowledge, while reinforcing Fortinet’s role in supporting cybersecurity education in the communities where we operate.

[Learn more.](#)

2025 impact:

750+
students trained
across Ecuador,
Italy, Poland, and
Spain

DEMONSTRATING INTEGRITY

As society becomes increasingly dependent on digital systems, stakeholders expect technology companies to operate with high integrity and a strong commitment to protecting people and data. At Fortinet, trust is foundational to how we implement AI, secure digital infrastructure, safeguard privacy, uphold ethical conduct, and engage in public policy advocacy that supports societal progress. Through robust oversight and a culture of accountability, we inspire confidence in what we build and how we operate.

2025 HIGHLIGHTS

Established the
AI Governance Committee

and published the
Principles for Responsible AI Use and Development

Fortinet's compliance and business ethics training completed by:

100% of our distributors

100% of our top contract manufacturers*

* Representing >90% of spend.



RESPONSIBLE AI

Artificial intelligence and machine learning are transforming how the world operates—from streamlining business processes to improving customer experiences and automating critical security tasks. While the benefits of AI are extensive, the rapid pace of innovation brings equally significant challenges. Issues such as bias, misleading outputs, lack of transparency, potential exposure of confidential information, model drift, and overreliance on automated systems present formidable risks if not addressed with robust governance and ethical safeguards. As a global cybersecurity leader, we are committed to developing and deploying AI securely, ethically, and with

strong governance, to protect the interests of customers, employees, partners, and society.

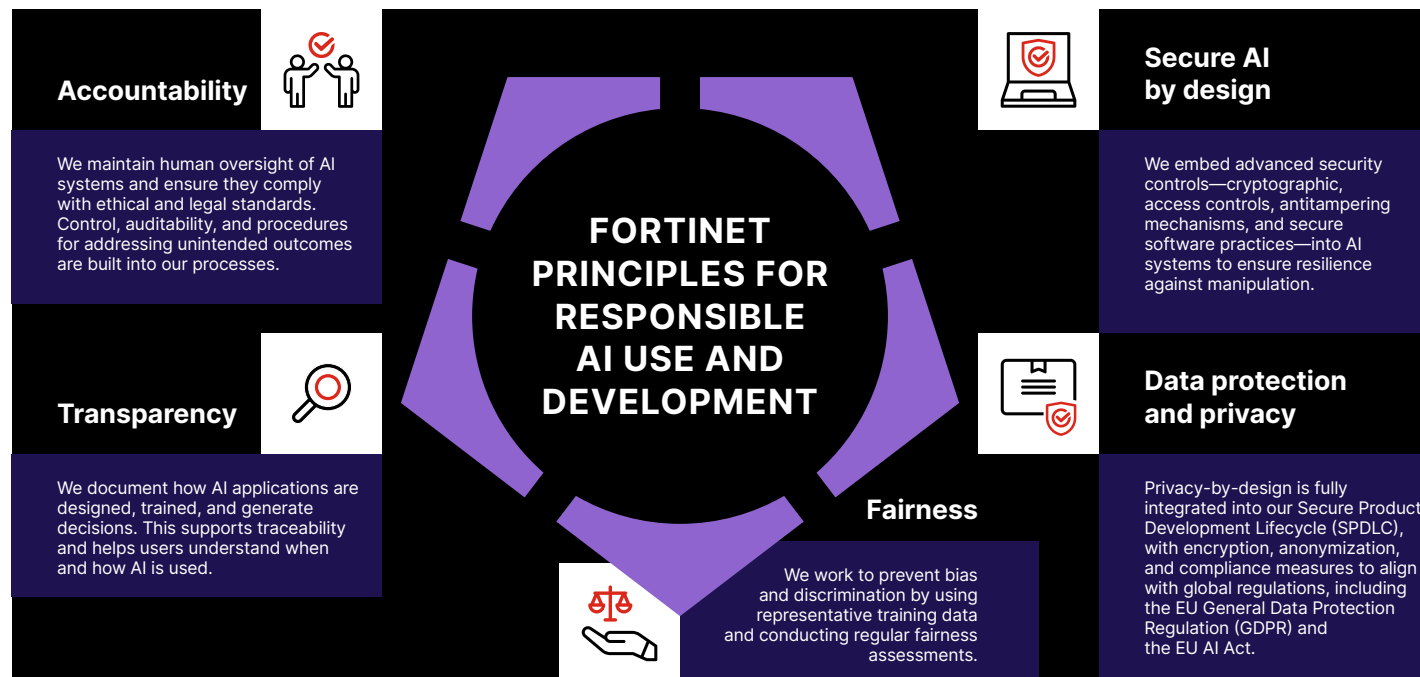
Our long-standing approach to responsible innovation has guided Fortinet's work for more than 25 years. As the pace of AI innovation accelerates and the complexity of these technologies grows—particularly with the emergence of GenAI—Fortinet continues to enhance its governance model to ensure responsible AI use, in alignment with global standards, human rights principles, and our broader commitments to trust, transparency, and security.

AI GOVERNANCE COMMITTEE

In 2025, Fortinet established a cross-functional AI Governance committee to oversee the ethical, secure, and responsible development and use of AI technologies throughout the organization. The committee includes Fortinet executives from information security, legal, human resources, product development, privacy and compliance, and customer services and support. The committee monitors compliance with global standards and regulatory requirements, establishes AI-related policies and development frameworks, provides technical guidance to AI users and developers, and conducts and oversees AI risk assessments.

AI SECURITY POLICY

To provide a unified foundation for ethical and secure AI development, Fortinet introduced its AI Security Policy in 2025. The policy establishes clear, company-wide requirements to ensure responsible and consistent use of AI systems, in compliance with international standards, including ISO/IEC 42001:2023, and regulatory frameworks such as the European Union Artificial Intelligence Act (EU AI Act). Although Fortinet's current AI applications are not categorized as "high risk" under the EU AI Act, we apply a high level of rigor to all our systems. Our policy ensures the secure deployment of AI technologies, the proactive mitigation of related risks, and the consistent use of AI with integrity and in full compliance with regulatory requirements.



INFORMATION SECURITY AND DATA PRIVACY

Information security and data privacy are integral to our business and essential to maintaining the trust of our customers, partners, employees, and other stakeholders. Our commitment is embedded across our operations, governance, and every phase of product development, manufacturing, and delivery. By integrating security and privacy across our operations, we safeguard sensitive data, enhance the resilience of our infrastructure, and help build a trusted digital ecosystem. We also maintain an Insider Threat program as part of our comprehensive approach to protecting information and managing security risks across the organization.

GOVERNANCE AND OVERSIGHT

Fortinet integrates cybersecurity into its enterprise risk management framework, ensuring that information security is treated as a strategic priority at the highest levels of the organization. Our board of directors oversees these efforts through a dedicated cybersecurity committee, which governs cybersecurity and information technology risks consistent with our leadership role in the industry.

The cybersecurity committee regularly reviews Fortinet's cybersecurity risk posture, including processes for preventing or mitigating cybersecurity risks, responding to incidents, and monitoring emerging threats. Fortinet executives responsible for cybersecurity provide quarterly updates to the cybersecurity committee, the chief executive officer, and other members of our senior management, covering ongoing initiatives, assessments of the information security program, project status for strengthening security controls, and analyses of emerging threats.

The company's deputy CISO leads day-to-day cybersecurity operations and execution of the Information Security Management System (ISMS).

INFORMATION SECURITY MEASURES

Fortinet's robust ISMS ensures the confidentiality, integrity, availability and resilience of the customer data in our systems. It incorporates policies, programs, standards, procedures, and controls aligned with industry standards, including ISO 27001/2, ISO 27017, ISO 27018, and NIST 800-53/161, as well as data privacy laws such as GDPR and the California Consumer Privacy Act (CCPA). We continuously assess and integrate additional standards to address new regulations such as the Cyber Resilience Act (CRA), NIS2, DORA, the EU AI Act, and the EU Data Act, as well as unique industry or regional requirements.

As part of our security architecture, our zero trust access model enforces verification at every stage, never assuming trust based on network location. Access to applications and internal resources is controlled through policy-based mechanisms that validate user identity, device posture, and compliance before each session. Continuous monitoring and adaptive controls help ensure that only authorized and secure users and devices can connect to IT resources, reducing risk across IT and remote environments.

Fortinet conducts regular risk assessments and engages internal experts and third-party auditors to verify that our practices align with industry standards and evolving best practices. Security policies are reviewed at least annually, or whenever significant changes occur, to ensure continued suitability and effectiveness. We communicate policy changes to all employees to reinforce compliance and awareness.

“As global requirements such as NIS2, the Cyber Resilience Act, the UK Telecom Security Act, DORA, the EU AI Act, and the EU Data Act continue to evolve, we track developments closely and assess their impact on our business. I work with teams across IT, R&D, operations, cloud services, and support to ensure we adapt quickly by strengthening our policies, processes, and controls as needed. This proactive approach helps Fortinet maintain compliance and enables us to guide customers as they update their own security and compliance programs in response to these changing expectations.”



Rafi Brenner

Deputy CISO, chair of the AI Governance committee, and member of the CSR committee at Fortinet

FORTINET ON FORTINET

As an early adopter of our own technology, we strengthen our security posture and accelerate product innovation through the Fortinet on Fortinet program. By embedding our own security solutions and services across our infrastructure, we enhance network protection, validate new features in real-world environments, and demonstrate actionable use cases for customers. In 2025, we expanded deployment of Fortinet technologies internally, further improving enterprise-wide security controls and providing timely, informed feedback to R&D teams to enhance functionality, security, and performance.



We also assure customers of our information security and data privacy practices through certifications and independent assessments against internationally recognized standards. In 2025, Fortinet reaffirmed its commitment to cybersecurity by renewing and expanding the scope of its ISO 27001/17/18 certifications and SOC2 Type II examinations. During the year, we also earned new certifications required in specific markets—such as GovRAMP for the U.S. state and local government sector—and in industry verticals, including healthcare and automotive. We also earned regional certifications, including ISMAP, IRAP, ENS and ACN.

Fortinet also implements security best practices in its product development process, aligned with standards such as NIST 800-53, NIST 800-160, NIST 800-218, and U.S. EO 14028. Our internal and external product review processes ensure that all products, from design through end-of-life, are secure by design and secure by default. We promptly remediate any identified issues, in accordance with comprehensive response plans. See [Secure by design](#), [secure by default](#).

2025 HIGHLIGHTS

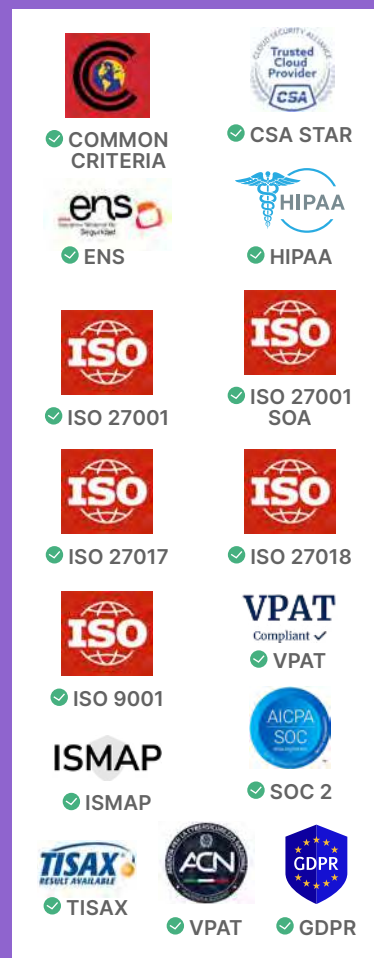
90

information security
certifications and
examinations renewed

0

material breaches

2025 INFORMATION SECURITY AND PRIVACY CERTIFICATIONS



INFORMATION SECURITY AWARENESS AND TRAINING

Every Fortinet employee contributes to protecting the company's information security and infrastructure. We promote strong cyber awareness among our employees through mandatory training and ongoing engagement.

In 2025, over 96% of our employees completed Fortinet's annual Information Security Awareness Compliance training, which combines videos, gamification, quizzes, and interactive learning techniques. We conduct periodic phishing campaigns to 100% of Fortinet employees

to reinforce awareness of social engineering and other attack techniques. In addition, developers must complete secure code development training, and specialized training is required for employees in IT and information security roles. The information security team also regularly publishes alerts on new and emerging threats, provides actionable security tips, and maintains internal guidance on secure use of AI tools through internal communication channels.



SUPPLY CHAIN SECURITY RISK MANAGEMENT PROGRAM

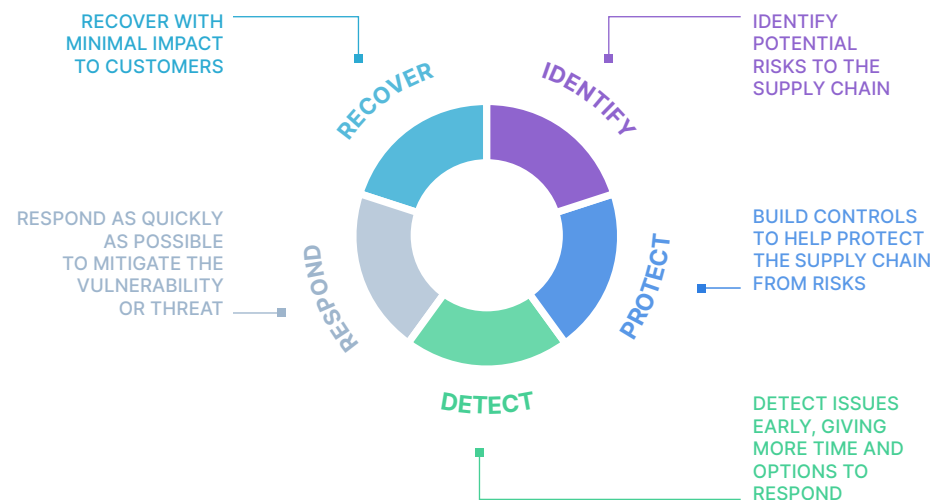
The security and integrity of Fortinet's products begin with a trusted global supply chain. Our approach starts with establishing control over a qualified supplier base, which in turn provides trusted components for design, development, and manufacturing services, as well as post-sale product support. The Fortinet Trusted Supplier program (TSP) forms the foundation of our supply chain security efforts. It follows a five-step process—Identify, Protect, Detect, Respond, and Recover—to manage risks across our supplier base.

The TSP aligns with requirements defined in NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, and other directives periodically established by the U.S. government for securing the ICT services supply chain. We developed the TSP to address increasing customer demand for transparency regarding the security of the hardware, firmware, and software included in Fortinet's products and to comply with U.S. government directives.

Fortinet conducts a thorough security assessment of its TSP partners to ensure they comply with applicable controls defined in NIST SP 800-161, and works side by side with them to remediate gaps and monitor their security posture. In 2025, we expanded the TSP to include additional contract manufacturers and sites, covering more companies and new manufacturing locations.

We maintain ongoing oversight of our TSP partners through continuous monitoring, close collaboration to address new and emerging threats to their infrastructure, and periodic on-site audits to ensure that required security controls remain effective and findings are addressed in a timely manner.

In addition, we assess the security posture of infrastructure hosting providers and cloud service providers to ensure compliance with physical, organizational, cybersecurity, and data privacy requirements, including adherence to global regulatory standards and recognized certifications.



DATA PRIVACY

Ensuring the trust and confidence of our employees, business partners, and customers is vital to Fortinet's reputation and ongoing success. Protecting data privacy is central to maintaining trust and is embedded across all aspects of our operations.

Fortinet's governance structure includes a dedicated privacy expert who oversees the company's privacy program and related initiatives, and reports, as appropriate, indirectly to the board of directors. A cross-functional committee of Fortinet privacy champions from different business units—including R&D, product management, sales, marketing—meets regularly to review privacy practices and policies, monitor legislative developments, update our processes as needed, and address privacy questions and comments to help ensure our employees remain updated and aware of data privacy matters. Our Fortinet data protection officers in Mexico, Singapore, and Spain provide local oversight, ensure compliance with applicable regional privacy laws, and guide regional initiatives.

Fortinet's practices for processing personal data are detailed in the Fortinet Privacy Policy, which aligns with global data privacy laws and principles. The Fortinet Data Privacy Practices document outlines how our products and services handle personal information. Annual exercises simulate potential breach scenarios to ensure our teams are prepared, in accordance with the company's Incident Response Policy. We continually enhance our practices to align with evolving regulations and stakeholder expectations worldwide, including participation in the EU-U.S. Data Privacy Framework.

All Fortinet employees are required to complete mandatory privacy training upon hire and at least annually thereafter. In 2025, over 99% of employees completed the required training, supporting strong awareness and adherence to privacy standards. To help maintain strong privacy standards across our value chain, third-party vendors are subject to internal privacy assessments and, where appropriate, additional contractual obligations. They are also required to demonstrate independent third-party audit coverage.

FORTINET TRUST RESOURCE CENTER

Fortinet provides transparency and resources through the Fortinet Trust Resource Center, which offers detailed information on data privacy practices, data protection officers, data subject access requests, privacy-by-design measures, and AI governance. In 2025, we introduced a web-based tool enabling customers to enter into data protection agreements directly with Fortinet, replacing a previously manual process. This improves customer convenience while streamlining internal operations.

BUSINESS ETHICS

Upholding ethical business practices and ensuring legal compliance underpin Fortinet's culture built on integrity, accountability, and trust. This commitment is led from the top and embedded throughout our global workforce, extending to our partners and suppliers. Our governance framework—including our codes of conduct and engagement with employees, partners, and other third parties—reflects our dedication to promoting responsible business practices across our value chain.

We review and update our policies and standards each year to align with strong practice and evolving expectations. To reinforce accountability and drive continuous improvement, we conduct third-party audits that assess ethical compliance across our operations and key contract manufacturers.

ETHICS GOVERNANCE

Our governance structure, which oversees and reinforces ethical practices throughout our value chain, is central to Fortinet's ethical framework. The board of directors, supported by a cross-functional ethics committee, guides and monitors the company's ethical initiatives.

Our Third-Party Risk Management Steering committee plays a vital role in identifying and mitigating third-party risks and supporting Fortinet's efforts to maintain the highest ethical standards wherever it operates.

CODES OF BUSINESS CONDUCT AND ETHICS

Fortinet's codes of business conduct and ethics for all employees, partners, suppliers, and vendors outline our expectations and requirements, covering areas such as general standards of conduct; avoiding conflicts of interest; anti-corruption; public communications; financial reporting; safeguarding company assets; responsibilities to our customers, suppliers, and competitors; working with governments; and procedural matters.

The [Code of Business Conduct and Ethics](#) applies to all directors, officers, and employees of Fortinet and its subsidiaries. Fortinet's agents and contractors are also expected to read, understand, and abide by the Code.

We hold our partners, suppliers, and vendors to the same high ethical standards we set for ourselves and require them to agree to our expectations before formalizing our partnership. Fortinet's [Partner Code of Conduct](#) and [Vendor/Supplier Code of Conduct](#) clearly set out our expectations, and we may terminate relationships with partners, vendors, and suppliers that don't align with those standards.

REPORTING CONCERNS

Any employee or third party who suspects or is aware of a violation of Fortinet's Code of Business Conduct and Ethics or policies is empowered to raise concerns, without fear of retaliation, through the avenues outlined in the [Fortinet Whistleblower Policy](#). All employees are trained to report concerns during the Annual Trust and Compliance training. This includes the option to report concerns confidentially and, if desired, anonymously to our third-party whistleblower hotline. A dedicated team promptly reviews and investigates all relevant allegations—with most investigations completed within 45-60 days of receipt. The team then takes necessary actions to mitigate and remediate any adverse impacts. Our telephony options ensure that local languages are available in our larger offices, along with direct phone numbers for reporting incidents. We offer live telephone interpretation in over 150 languages, which streamlines the reporting process. Our compliance posters include a QR code that links to detailed information on how to make one's voice heard. This comprehensive approach underscores our dedication to maintaining a workplace where concerns are addressed with diligence and fairness.



ANTI-CORRUPTION PROGRAM AND POLICY

We are committed to winning business only on the merits and integrity of our products, services, and people, and we take a strict zero-tolerance approach to bribery and corruption across our global operations. Our [Global Anti-Corruption Policy](#) applies worldwide to all Fortinet entities and governs the conduct of all employees, officers, agents, representatives, and wholly owned subsidiaries. The policy clearly prohibits improper payments, kickbacks, and facilitation payments and is reinforced through mandatory Annual Trust and Compliance training for employees, partners, and contract manufacturers, as well as onboarding programs and ongoing communications linked to our Code of Business Conduct and Ethics. Employees are required to attest to the policy annually as part of this training. We also require our channel partners, consultants, and other intermediaries to uphold the same high standards, supported by robust third-party due diligence and continuous monitoring. Employees, partners, and other stakeholders are encouraged to report concerns through our dedicated, confidential reporting channel at www.fortinet.ethicspoint.com.

TRADE COMPLIANCE PROGRAM

Our multifaceted compliance and ethics training strategy, which covers Fortinet and third parties, ensures that people throughout our ecosystem remain well informed about ethical and regulatory obligations. Fortinet employees must complete Annual Trust and Compliance training, and 99% achieved this in 2025. Members of our sales team are also required to complete sales compliance training every six months, complemented by a quarterly compliance certification. A compliance toolkit equips all employees with resources to foster awareness and understanding of Fortinet's business ethics and compliance program.

Managers play a critical role in setting the tone for their teams, driving ethical action, and helping reduce opportunities to act unethically. Our manager compliance toolkit provides useful resources to help managers reinforce a culture of integrity and accountability.

We also collaborate closely with our suppliers and vendors to ensure they meet our business ethics standards. In 2025, 100% of Fortinet's top contract manufacturers, representing more than 90% of our spend, completed the Fortinet Vendor/Supplier Compliance Training. This was complemented by a live trade compliance training conducted by the Fortinet Global Trade Compliance team for our key contract manufacturers, covering topics such as the Trade Agreement Act (TAA), human rights, and import/export compliance regulations.

Our partners are also integral to this effort and engage in mandatory business ethics and compliance training. In 2025, 100% of distributors completed the Partner Compliance training.

To make business ethics and compliance training as engaging as possible, we continually enhance our training methods by incorporating elements such as gamification, quizzes, videos, and learning checks.

AUDITS AND ACCOUNTABILITY

Fortinet employs focused audits as systematic and proactive measures to ensure compliance with its ethical standards. In 2025, Fortinet conducted several audits, notably for its Global Trade Compliance program and supply chain, covering company governance, import/export standards, conflict mineral standards, employee conditions, returns, and product safety. These evaluations demonstrate Fortinet's commitment to accountability and continuous improvement.

FEEDBACK FROM OUR EMPLOYEE COMPLIANCE SURVEY

We gather feedback on our programs to drive continual improvement. In 2025, our employee compliance survey highlighted strong awareness and trust in our ethics processes, including:

100%

of respondents stated they know where to report a concern

99%

of respondents stated they are confident their concern will be addressed

100%

of respondents stated they trust Fortinet's executive leadership to operate with ethics and integrity

HUMAN RIGHTS

We are committed to respecting internationally recognized human rights, as expressed in the International Bill of Human Rights and the [UN Guiding Principles on Business and Human Rights](#). Our responsibility extends across our value chain, from our employees and workers to our supply chain partners and the users of our products and services.

As a cybersecurity leader, we use our technologies to protect individuals, businesses, and critical infrastructure from cybercrime, supporting the security and privacy that underpin fundamental human rights. [Learn more](#). Through our efforts to close the cybersecurity skills gap, we also contribute to expanding access to digital inclusion and fostering a more inclusive cybersecurity workforce. [Learn more](#).

POLICIES AND STANDARDS

Fortinet's [Global Human Rights Policy](#) sets the foundation for how we respect human rights across our operations and value chain. It guides our due diligence approach and informs engagement with stakeholders.

We periodically review our Global Human Rights Policy to ensure it reflects the evolving landscape of human rights risks. In 2025, working with an external human rights expert, we updated the policy to strengthen alignment with internationally recognized labor and human rights standards, clarify expectations on issues such as prohibitions of forced labor and support for freedom of association, and reinforce our commitment to apply the higher standards when local and international requirements differ. The updated policy was approved and signed by Fortinet's COO, underscoring executive-level oversight and accountability for our human rights commitments.

Human rights language is integrated into key Fortinet documents, including our End-User License Agreement, product datasheets, and our codes of conduct for partners and suppliers. In 2025, we strengthened Fortinet's [Partner Code of Conduct](#) and [Vendor/Supplier Code of Conduct](#) to more explicitly address labor rights, including maximum working hours, protection of young workers, written employment agreements, and equal pay for equal work. We also detailed expectations for worker health and safety—including hazard prevention, emergency preparedness, and living conditions.

Fortinet also expects all suppliers to comply with the [Responsible Business Alliance \(RBA\) Code of Conduct](#), which includes comprehensive requirements related to labor, ethics, environmental management, and worker well-being. Our updated Partner Code of Conduct and Vendor/Supplier Code of Conduct align with the RBA Code of Conduct and reflect its principles across our global value chain.

TRAINING AND AWARENESS

We promote awareness of Fortinet's human rights commitments through regular communication and training. Human rights content is included in our mandatory Annual Trust and Compliance training for all employees. In 2025, 100% of employees were required to complete the training, and 99% did so successfully. Vendors and partners, including distributors and our largest contract manufacturers, receive guidance on human rights expectations through Fortinet's Vendor/Supplier Compliance Training and live trade compliance sessions; in 2025, 100% of these vendors and partners completed the training. These programs support consistent understanding and implementation across our global value chain.

In addition, employees and third parties are encouraged to raise concerns or report alleged human rights abuses through our confidential reporting channels. [Learn more](#).

HUMAN RIGHTS IN OUR WORKPLACE

Fortinet's employees drive innovation and progress throughout the company and are key to our success. We work to provide an engaging culture where they can learn, grow, and advance in their careers. Our policies and standards related to fair labor practices, equal opportunity, and nondiscrimination outline our commitments in those areas. Health, safety, and well-being are also important priorities, and our [Global Health and Safety Policy](#) outlines how we provide safe and secure workplaces wherever we operate. [Learn more](#).

HUMAN RIGHTS IN OUR SUPPLY CHAIN

Fortinet works with suppliers and contractors to help ensure that our products and services are produced in conditions that respect workers' rights and promote health, safety, and dignity. We communicate expectations through our [Partner Code of Conduct](#), [Vendor/Supplier Code of Conduct](#), and contract manufacturer agreements.

We apply a risk-based screening process to assess prospective and existing Fortinet vendors and suppliers for potential human rights violations. This includes two-step verification, third-party verification, and continuous monitoring in high-risk areas, all on a widely recognized, reputable platform. To assess direct vendors and suppliers, we apply criteria related to internationally recognized human rights standards, the U.S. Foreign Corrupt Practices Act, and sanctions lists. In 2025, 100% of vendors and suppliers in high-risk areas that were onboarded and approved in Fortinet's ERP system were screened, and no human-rights-related matters required escalation or remediation.

In addition, Fortinet conducts proactive anti-corruption and compliance evaluations of third parties and works closely to address any reported non-compliance issues. Our commitment to risk mitigation includes an agile response and resolution process. An external assessment of our third-party program was recently conducted to validate its effectiveness.

During the year, we also sent a questionnaire about bribery and corruption-related risks to a sub-set of our resellers, based on risk, size, and revenue. We are assessing whether those resellers will be required to complete the same training as distributors moving forward.

Fortinet expects its suppliers to comply with its [Responsible Minerals Sourcing Policy](#). If a supplier does not meet Fortinet's expectations, we reserve the right to engage with them to address the issue appropriately. This may involve corrective action plans or reevaluation of the business relationship.

We are also committed to preventing modern slavery and human trafficking. Through our [Statement on Modern Slavery](#) and compliance with regulations such as the California Transparency in Supply Chains Act of 2010, Australia's Modern Slavery Act 2018, the Trafficking Victims Protection Act, the UK Modern Slavery Act, and the Uyghur Forced Labor Prevention Act ([UFLPA](#)), we maintain rigorous screening, require compliance certifications from high-risk contract manufacturers, and investigate and rectify non-compliance with disciplinary actions, including termination when necessary.

RESPONSIBLE USE OF PRODUCTS AND SERVICES

Fortinet develops, sells, and manages products and services in ways that respect human rights. We fully adhere to the UN Guiding Principles on Business and Human Rights and comply with the laws of the countries where we operate.

We have a team dedicated to ensuring compliance with trade laws, including prohibitions on selling our products to certain countries, some of which have poor human rights records. Through our End-User License Agreement, our end-customers contractually commit that Fortinet's products and services cannot be used to engage in or in any way support violations or abuses of human rights.

We also conduct quarterly Global Trade Compliance business review meetings with Fortinet operations teams and service providers (such as customs brokers and RMA service providers) to discuss trade compliance matters and controls.



CORPORATE GOVERNANCE

Fortinet is committed to strong corporate governance as the foundation for long-term value creation, ethical conduct, and responsible growth. Our governance structure provides clear oversight of strategy, risk, and performance while ensuring accountability to shareholders, customers, employees, and the broader community. We continually enhance our governance practices to align with evolving regulatory requirements, stakeholder expectations, and industry best practices.

BOARD GOVERNANCE

Fortinet's board of directors sets high standards for ethical conduct, accountability, and oversight across the company. As fiduciaries, directors are committed to serving the best interests of shareholders and overseeing the management of Fortinet's business with diligence and integrity.

Fortinet's board comprises experienced leaders with deep expertise across cybersecurity, technology, finance, public policy, and global operations. The board periodically reviews its composition to ensure that a variety of experiences, perspectives, and skillsets are aligned with Fortinet's strategic needs.

The board delegates certain responsibilities to its standing committees, which operate under charters reviewed annually:

- **Audit committee:** Oversees financial reporting, internal controls, compliance, and privacy risk management.
- **Governance and Social Responsibility committee:** Oversees board governance practices, director nominations, and ESG strategy and reporting.
- **Human Resources committee:** Oversees organization and human resources activities, and compensation policies, plans, and benefits programs.
- **Cybersecurity committee:** Oversees cybersecurity and information technology risks, controls, and processes.

View the [charters](#) of each committee and learn more about the board's [composition](#) and the [skills and experience](#) of its members.



ESG GOVERNANCE

Fortinet's ESG governance structure ensures clear accountability, cross-functional collaboration, and effective deployment of our sustainability strategy across the company.

Board of directors

The board of directors is the lead sponsor of Fortinet's CSR strategy and commitments. Oversight is provided by the board's Governance and Social Responsibility committee, composed of at least two directors dedicated to governance and sustainability. The committee reviews ESG-related risks and opportunities quarterly and collaborates with other board committees.

Executive team

Fortinet's executive team validates the company's sustainability strategy, approves goals, monitors execution, and sponsors integration of ESG considerations into business operations and decision-making processes. The team also reviews and vets approaches proposed by the CSR team to ensure alignment with Fortinet's business priorities and risk management frameworks.

For example, the executive team guided the decision to adopt a near-term target approach to the company's Science Based Targets initiative (SBTi) commitments, reflecting a thoughtful and pragmatic path toward decarbonization. It also supported the formalization of the Fortinet Product Donation program, which complements e-waste reduction by providing equipment to academic training programs that advance digital inclusion. The executive team continues to play an active role in driving accountability across business units, ensuring that sustainability is embedded in long-term strategy, product innovation, and stakeholder engagement.

CSR committee

The internal CSR committee defines Fortinet's sustainability priorities, sets objectives, and oversees related initiatives and programs. Chaired by the Global Sustainability and CSR director, the committee brings together CSR champions from across the company who drive progress in their areas of expertise and advance roadmaps aligned with Fortinet's sustainability priorities. The committee meets at least four times per year and provides quarterly updates to the executive team and the board's Governance and Social Responsibility committee.

CSR team

The CSR team leads strategy development and oversees sustainability reporting, engagement, and performance tracking across all pillars of the company's CSR framework. It engages throughout all company levels to execute Fortinet's sustainability strategy. The team monitors global sustainability trends and regulatory developments—such as CSRD, climate risk management, and responsible AI—and translates those into actionable initiatives across the organization.

Working closely with the CSR committee and cross-functional teams, the CSR team helps embed sustainability into Fortinet's operations and culture through training and awareness campaigns. The team also calculates and reports key performance indicators across GHG emissions, product and environmental management system (EMS) certifications, employee engagement, cybersecurity education, and community impact.

Together, these efforts help ensure that Fortinet's sustainability approach remains both globally informed and locally actionable.

CSR champions

Each business unit has a designated CSR champion responsible for executing action plans, achieving operational sustainability goals, and reporting progress. This network embeds sustainability across engineering, supply chain, operations, human resources, facilities, support, and product functions. In 2025, we expanded this team to cover additional functional areas.

Employee CSR ambassadors

Volunteer employee CSR ambassadors help educate and engage the broader workforce on sustainability topics, supporting global participation in company-wide initiatives.

Governance framework

Fortinet's sustainability governance is anchored in key policies, processes, and frameworks designed to ensure effective oversight, accountability, and transparency. Key elements of this governance approach include:

- Integration of sustainability into decision-making processes, supported by strong oversight and engagement at both board and executive levels.

- Clear understanding of sustainability-related issues across the organization, ensuring that employees, executives, and board members are informed of relevant regulatory requirements, risks, and operational initiatives.
- Defined escalation pathways that enable stakeholders to raise and address sustainability-related issues in a timely and effective manner.
- Transparent and consistent disclosure, guided by recognized reporting standards and frameworks such as GRI, TCFD, and ISSB.
- Alignment with external guidelines, systems, and stakeholders, including SBTi, ISO 14001, CDP, MSCI, MorningStar, and independent third-party auditors.



RISK MANAGEMENT

Risk management is a core component of Fortinet's governance framework. The board and management team maintain a comprehensive enterprise risk management (ERM) program that identifies, assesses, and mitigates risks across strategic, operational, financial, environmental, cyber, and compliance domains. Our ERM program strengthens enterprise-wide risk awareness, establishes best practices, and highlights critical risk areas to support informed decision-making and effective resource allocation.

Fortinet continually evaluates its risk environment through ongoing monitoring and updates to risk registers, supplemented by an annual enterprise risk assessment. This assessment draws on internal risk data, industry trends, third-party risk intelligence, peer benchmarking, and insights from interviews with senior leaders and subject-matter experts. Risks are evaluated across short-, medium-, and long-term time horizons and prioritized accordingly. Periodic external reviews help benchmark the maturity of our ERM program against leading practices. The results of the enterprise risk assessment inform Fortinet's risk-based internal audit plan. Regular updates on risk trends are provided to the board and relevant board committees as part of our governance oversight model.

For additional detail on risks that may impact Fortinet's performance, see our [U.S. Securities and Exchange Commission \(SEC\) Form 10-K—Risk Factors](#).

Integration of sustainability into ERM

We are progressively integrating sustainability- and climate-related considerations into our ERM program to strengthen the connection between risk management, financial resilience, and long-term value creation.

In 2025, we advanced this integration through our climate risk assessment and our first double materiality assessment (DMA), both aligned with Fortinet's enterprise risk assessment processes and business decision-making priorities. These assessments, reviewed by executive leadership, are designed to inform the incorporation of sustainability-related impacts, risks, and opportunities into enterprise planning and risk prioritization.

Looking ahead, Fortinet plans to further embed these considerations into the company's ERM framework, enabling a more holistic view of risks and opportunities across strategic, operational, financial, environmental, and social dimensions.

Double materiality assessment

Fortinet periodically conducts materiality assessments to identify sustainability topics that are most significant to Fortinet, our stakeholders, and long-term enterprise value. In 2025, we completed our first DMA, aligning with emerging requirements, including the EU CSRD. This assessment provides a more comprehensive understanding of the sustainability topics that are most material to Fortinet.

The DMA results will inform further integration of sustainability considerations into enterprise planning, risk management, and decision-making, and provide a foundation for future sustainability disclosures aligned with the CSRD and other emerging global frameworks. [Learn more.](#)

Climate risk management

In line with the TCFD, Fortinet evaluates the potential impact of climate-related risks—both transition and physical—such as evolving climate regulations globally, exposure to carbon pricing, supply chain vulnerabilities, and the physical effects of a changing climate. We assess these risks using Fortinet's ERM framework, ensuring climate-related risks are evaluated alongside other strategic and financial risks and governed through consistent processes.

In 2025, we conducted a climate risk assessment using scenario analysis informed by the latest [Intergovernmental Panel on Climate Change Assessment scenarios](#). [Learn more.](#)

This work strengthens Fortinet's preparedness for regulatory requirements—such as the EU CSRD and California SB 253 and SB 261—and supports customer and government expectations for TCFD-aligned disclosures.



PUBLIC POLICY

Building and maintaining a secure and resilient digital future requires sustained collaboration across industries, sectors, and borders. Smart government policies that ensure or enable strong and widespread cyber resilience are essential, and we focus our advocacy efforts accordingly. We also promote policies that support the development of a robust cybersecurity workforce and strengthen general security awareness. Through public policy advocacy, we seek to advance the interests of our company, our customers, and other stakeholders.

Public-private partnerships

Collaboration with the public sector and industry partners to advance cybersecurity has been a core element of Fortinet's strategy for many years. In 2025, examples of these efforts included:

- Continuing our collaboration with INTERPOL to support Operation Serengeti 2.0, a large-scale campaign targeting cybercriminal groups across 18 African nations and the United Kingdom. [Learn more.](#)
- Launching a groundbreaking Global Cybercrime Bounty program in collaboration with Crime Stoppers International (CSI), creating the world's first anonymous, citizen-powered platform dedicated to reporting cybercriminal activity. [Learn more.](#)
- Leading the development and launch of the CTA Responsible Vulnerability Communication Policy, a framework designed to enhance cross-industry cooperation and promote timely, systematic, and responsible vulnerability disclosure practices.

- Collaborating with the World Economic Forum to develop practical recommendations for fostering a sustainable cybersecurity workforce, highlighting how cross-sector collaboration and public-private coordination can accelerate workforce development. [Learn more.](#)
- Participating in public sector events in Australia, including Pacific Cyber Week, to discuss regional capacity-building and the role of cybersecurity in driving innovation and economic productivity.
- Engaging in India on emerging cybersecurity policies and standards, as well as initiatives to address the cybersecurity skills gap in K-12 and higher education. [Learn more.](#)

[Learn more](#) about our international partnerships and engagements with key government and trade associations.

Engagement with policymakers

Fortinet engages in discussions with policymakers across different levels of government, as permitted. In 2025, we testified twice before the U.S. Congress and twice before the UK Parliament on topics such as secure-by-design principles, network resilience, and the cybersecurity skills gap. [Learn more.](#) We comply with all applicable public policy disclosure requirements, including [filings](#) under the U.S. Lobbying Disclosure Act and equivalent reporting obligations in other jurisdictions.

Governance of public policy engagement

Fortinet is committed to ensuring appropriate controls and transparency in its public policy engagements through oversight at the highest levels. Our chief operating officer and VP of corporate affairs lead these efforts. They oversee high-level government engagements, develop the company's public policy strategy, and ensure compliance with related laws and regulations, including proper disclosure.

Political contributions

Fortinet has not made corporate donations to campaigns for public office or to elected public officials. Additionally, it has not established, and does not currently maintain, a political action committee (PAC), and it does not use company funds or assets to contribute to any PAC. If Fortinet decides to make political contributions in the future, we are committed to complying appropriately and to the required disclosure and reporting of ities.



APPENDIX

ABOUT THIS REPORT

Fortinet's 2025 Sustainability Report presents a balanced and transparent overview of our performance across the company's key environmental, social, and governance topics. It enables our stakeholders to better understand our approach to sustainability, how we manage our most material topics, and our progress in integrating sustainability across the company. Since 2021, we have published an annual sustainability report detailing our commitments, actions, and performance across our sustainability pillars and priority topics. Prior-year reports are available on our [website](#).

This report includes a performance data section with detailed metrics. TÜV SÜD America, Inc. conducted a limited assurance review of Fortinet's 2025 GHG emissions inventory. See the [assurance statement](#).

Fortinet aligns its reporting with leading external frameworks and standards, including [GRI](#) (Global Reporting Initiative) Standards, [Sustainability Accounting Standards Board](#) (SASB) Standards, the [Task Force on Climate-related Financial Disclosures](#) (TCFD), the [United Nations Global Compact](#) (UNGC), and [CDP](#). Our GRI, SASB, and TCFD indices are included in this Appendix.

Unless stated otherwise, this report covers Fortinet's operations and activities worldwide for fiscal year 2025 (Jan. 1, 2025–Dec. 31, 2025). All financial figures are reported in U.S. dollars unless noted otherwise. A [glossary](#) of key cybersecurity terms is provided for additional clarity.

CONTACT US

Please email sustainability@fortinet.com with any questions or comments.

PERFORMANCE DATA

SECURING THE DIGITAL WORLD

Innovation

	2025	2024	2023
% of revenue generated from innovation ¹	46.3%	30.6%	38.3%
Number of new product families introduced	6	3	6
R&D investment (\$ in millions)	815.5	716.8	613.8
Number of issued and pending global patents	1,770	1,829	1,551

1. Represents percentage of newly commercialized hardware models, product families, and cloud-based services launched during the previous two years.

Partnership against cybercrime

	2025	2024	2023
Number of actionable human-vetted data points mapped and analyzed for disruption opportunities in the cybercriminal ecosystem (through the World Economic Forum Cybercrime ATLAS)	17,000	10,000+	8,584
Number of early discovery shares on threat campaigns (through Cyber Threat Alliance)	189	207	223

DEMONSTRATING INTEGRITY

Business ethics

	2025	2024	2023
Percentage of employees who were communicated Fortinet's Code of Business Conduct and Ethics	100%	100%	100%
Percentage of Fortinet's new direct suppliers that were screened using human rights criteria, FCPA, sanction lists, embargoed countries	100%	100%	100%
Percentage of distributors globally who completed Fortinet's Compliance and Business Ethics training	100%	100%	100%
Percentage of key contract manufacturers ² who completed Fortinet's Compliance and Business Ethics training	100%	100%	100%

2. Represents >90% of total contract manufacturing spend.

MINIMIZING OUR ENVIRONMENTAL FOOTPRINT

Waste

	2025	2024	2023
E-waste (in tonnes) ³	90	83	42
Recyclable waste (in tonnes) ⁴	27	12	13
Total waste	117	95	55

3. Data represents e-waste removed during the year from the largest warehouses and RMA centers (Union City—USA, Burnaby—Canada and Sophia Antipolis—France).

4. Data represents recyclable waste from all sites where waste is diverted from landfill, which includes the large owned sites and one leased site in London. More sites will be added as the program is expanded.

GHG emissions and energy consumption

	2025	2024	2023
Scope 1 (MTCO ₂ e) ⁵	1,728	1,606	1,328
Scope 2—Location based (MTCO ₂ e) ⁵	15,385	9,839	5,422
Scope 2—Market based (MTCO ₂ e)	0	0	792
GHG emissions intensity (MTCO ₂ e/\$billion revenue)	2.52E-06	1.92E-06	1.27E-06
Energy consumption (GJ)	266,878	210,853	182,280
Energy intensity (GJ/\$MTCO ₂ e/\$billion revenue)	3.92E-05	3.54E-05	3.44E-05

5. Scope 1 and Scope 2 emissions are calculated for sites under Fortinet's operational control. Data presented here is from owned sites.

Water

	2025	2024	2023
Water (m ³) ⁶	100,086	60,313	29,188

6. Data presented here is from owned sites.

GHG emissions and energy consumption (cont.)

Scope 3 GHG Emissions (MTCO₂e)

	2025	2024	2023
Purchased goods and services	181,387	110,259	94,208
Capital goods	2,012	3,689	6,180
Fuel- and energy-related activities	5,482	5,300	5,246
Upstream transportation and distribution	7,750	8,475	7,541
Waste generated in operations	94	843	622
Business travel	13,183	14,131	7,842
Employee commuting	14,601	16,936	5,250
Upstream leased assets	5,018	4,768	6,432
Downstream leased assets	14	14	15,747
Use of sold products	2,288,041	1,690,540	1,874,729
End-of-life treatment of sold products	518	461	150
Total Scope 3	2,518,100	1,855,416	2,023,947

EMPOWERING PEOPLE AND COMMUNITIES

Board of directors

	2025	2024	2023
Size of the board	8	10	8
Women on the board	38%	40%	25%

Number of employees

	2025	2024	2023
Total	15,109	14,138	13,568
Americas	8,136	7,665	7,407
APAC	2,827	2,725	2,735
EMEA	4,146	3,748	3,426

Number of new hires

	2025	2024	2023
Total	2,598	2,199	2,306
Americas	1,325	1,185	1,200
APAC	458	329	500
EMEA	815	685	606

Employee turnover

	2025	2024	2023
Total	1,627	1,628	1,333
Americas	857	926	808
APAC	351	336	247
EMEA	419	366	278

Representation of women

	2025	2024	2023
All	20%	20%	20%
Management	17%	17%	17%
Technical ⁷	17%	17%	20%
Other	23%	23%	24%
Sales	17%	16%	16%
R&D	18%	18%	18%
New hires	19%	21%	19%
Turnover	21%	20%	21%

7. Technical staff is the EEO-1 Category/Job group of Professional/Technical Professional.

Ethnicity—USA only

	2025	2024	2023
White	48.7%	48.5%	49.5%
Asian	36.6%	37.2%	35.9%
Latinx	9.7%	9.4%	9.6%
Black	2.7%	2.7%	2.9%
Two or more races	1.9%	1.8%	1.7%
Pacific Islander	0.2%	0.3%	0.3%
Native American	0.1%	0.1%	0.1%
Not disclosed	0.0%	0.0%	0.0%

Cybersecurity skills gap

	2025	2024	2023
Total individual people trained ⁸	914,810	630,859	432,905
Certifications obtained from the learning platform	119,638	203,062	334,429
EU Pledge	26,012	19,789	Not Applicable

8. The data was calculated based on training completion records and is based on unique individuals. As such, an individual is counted only once regardless of how many courses they took. The 1 million goal was launched on Jan. 1, 2022, and is targeted to be completed by Dec. 31, 2026.

TCFD INDEX

Fortinet supports the recommendations of the Task Force on Climate-related Financial Disclosures (TCFD), which were integrated into the International Sustainability Standards Board Standards in 2023. As part of our commitment to climate action, this TCFD index summarizes our approach to the TCFD recommendations on climate-related governance, strategy, risk management, and metrics and targets.

Topic	Required disclosure	Reference/disclosure
GOVERNANCE Disclosure of the organization's governance around climate-related risks and opportunities	A. Describe the board's oversight of climate-related risks and opportunities	Fortinet's board of directors, through its Governance and Social Responsibility (GSR) committee, oversees our objectives, strategies, and risks related to sustainability and corporate social responsibility (CSR), including climate change. The GSR committee oversees Fortinet's sustainability programs, including ESG matters, and reviews and assesses management performance, risks, controls and procedures related to CSR and sustainability, including climate change. Fortinet's Global Sustainability & CSR director, with the occasional assistance of specialized consulting firms, conducts presentations to the board to review ESG-related strategies, risks, and opportunities, share information about the evolution of climate-related regulations, report progress in sustainability, and provide recommendations for ongoing improvement. Learn more about ESG governance at Fortinet and our board of directors GSR committee.
	B. Describe management's role in assessing and managing climate-related risks and opportunities	Fortinet's executive team validates the company's sustainability strategy, including the assessment and management of climate-related risks and opportunities. The executive team approves targets, monitors execution, and sponsors integration of ESG considerations into business operations and decision-making processes. Fortinet's internal CSR committee, comprising cross-functional management representatives from across the company, defines the company's sustainability priorities, sets objectives, and oversees related initiatives and programs. The CSR committee provides quarterly updates to the executive team and the board's GSR committee and assists the GSR committee in overseeing Fortinet's CSR programs, including climate-related issues. The CSR committee and the CSR team, both led by Fortinet's Global Sustainability & CSR director, are responsible for identifying, assessing, and managing topics related to the environment, climate change, and other ESG matters. They also present specific items with reputational, strategic impact, and financial risks to the board of directors for guidance. The CSR team works closely with business units—such as finance, facilities, R&D, and supply chain—as well as other stakeholders to implement agreed-upon solutions. To support these efforts, Fortinet has an incentives scheme for the CSR team and Global Sustainability & CSR director, based on the achievement of sustainability-related quarterly business goals. Learn more about ESG governance at Fortinet.
STRATEGY Disclosure of the actual and potential impacts of climate-related risks and opportunities on the organization's businesses, strategy, and financial planning where such information is material	A. Describe the climate-related risks and opportunities the organization has identified over the short, medium, and long term	In 2025, we conducted Fortinet's first comprehensive climate scenario analysis. The assessment—which included qualitative and quantitative aspects—examined the most material climate-related risks and opportunities to Fortinet across multiple climate scenarios and time horizons, as set by Intergovernmental Panel on Climate Change (IPCC) scenario SSP5-8.5/RCP 8.5 for physical risks and the Network for Greening the Financial System (NGFS) Below 2°C scenario for transition risks, respectively. Short-term (2026) climate-related risks and opportunities are addressed through Fortinet's enterprise risk management program. Medium-term (2030) risks and opportunities: • Key physical risks include an increased frequency and severity of extreme weather events and rising average temperatures leading to shifts in precipitation patterns. These impacts could disrupt Fortinet's supply chain, affect business operations, and ultimately influence revenue generation. • Key transition risks relate to evolving policy and regulatory requirements, including the potential introduction or expansion of carbon-pricing mechanisms such as carbon taxes, tariffs, or cap-and-trade schemes. • Medium-term opportunities include the continued development of energy-efficient products, driven by growing demand for sustainable and low-energy devices. Additional opportunities arise from advancing sustainable product design through improved resource management, circularity, and the use of more sustainable materials. Long-term (2040) risks and opportunities: • Over the long term, more frequent and severe weather events could impact infrastructure and operations. Opportunities to mitigate these risks include prioritizing climate-resilient building design, strengthening business continuity planning with suppliers in hurricane-prone regions, and enhancing thermal design in data centers to accommodate rising temperatures. • Transition trends in 2040 also present opportunities, including sustained demand for energy-efficient products, a growing need to address risks related to increased AI usage, and increased integration of circular economy and eco-design principles across our product portfolio.
	B. Describe the impact of climate-related risks and opportunities on the organization's businesses, strategy, and financial planning	Climate-related risks and opportunities inform our strategy across our operations, supply chain, and products and services. Our near-term science-based emissions targets for Scopes 1 and 2, which are aligned with a 1.5°C trajectory, along with our Scope 3 supplier and customer engagement targets, guide our efforts. SBTi validated these targets in 2024. Learn more. Our decarbonization plan defines a clear path to reduce our GHG emissions through targeted strategies across our value chain. Our focus areas include reducing GHG emissions across our operations, engaging with our suppliers and other business partners to reduce their impacts, and designing and delivering more energy-efficient and circular products. Operations: We strive to continually enhance energy and resource efficiency across our operations by investing in sustainable technologies, sourcing renewable energy and optimizing processes to reduce consumption. 87% of our owned facilities by square footage used 100% renewable electricity in 2025; this increases to 100% of owned facilities when renewable energy credits (RECs) and energy attribute certificates (EACs) are included. Fortinet's green guidelines for its data centers and offices include renewable energy availability, green certifications, alternative transportation accessibility and waste management. We use these guidelines to help align new real estate investments and building renovations with our decarbonization targets. Learn more. Suppliers and other business partners: Fortinet is engaging its suppliers, contract manufacturers, channel distributors, and resellers on its climate journey. Learn more. Products and services: The energy consumed by our products in use is by far the main contributor to Fortinet's GHG emissions across our value chain. Therefore, we continually enhance product designs to reduce power, cooling, and space, helping customers minimize energy consumption and GHG emissions. The Fortinet Product Carbon Footprint Calculator, which provides the carbon footprint of many of our products, supports customer decision-making in this area. We also focus on sustainable packaging and circular economy practices that increase repair, reuse, and responsible end-of-life management. Learn more.

Topic	Required disclosure	Reference/disclosure
STRATEGY	C. Describe the resilience of the organization's strategy, taking into consideration different climate-related scenarios, including a 2°C or lower scenario	Our near-term GHG emissions-reduction targets for Scopes 1 and 2, which are aligned with a 1.5°C trajectory, along with our Scope 3 supplier and customer engagement targets, were validated by SBTi in 2024. Driving progress against these targets enhances our resilience against climate change. Energy consumption is a key driver of GHG emissions in our facilities and represents a significant operational cost. Improving energy efficiency and transitioning to lower-impact energy sources saves resources, decreases GHG emissions, and supports resilience in our operations. Customers increasingly value energy efficiency and other aspects of environmental performance in our products. Ongoing innovation in this area positions us to capitalize on this opportunity.
RISK MANAGEMENT Disclosure of how the organization identifies, assesses, and manages climate-related risks	A. Describe the organization's processes for identifying and assessing climate-related risks	In 2025, we conducted Fortinet's first comprehensive climate scenario analysis, building on a qualitative analysis in 2022 of current and potential climate-related transition and physical risks and opportunities with impact on our company. The 2025 assessment—which included qualitative and quantitative aspects—examined the most material climate-related risks and opportunities to Fortinet across multiple climate scenarios and time horizons. Following the TCFD framework, we assessed physical climate risks using IPCC scenarios SSP5-8.5/RCP 8.5 and transition risks using the NGFS Below 2°C scenario. In total, nine climate scenarios were evaluated, spanning low- and high-warming pathways—from a 1.5°C-aligned low-carbon transition to higher-warming scenarios ranging from 3°C to 6°C. Risks and opportunities were prioritized based on a combination of potential financial impact, likelihood, time horizon, and scenario severity. The analysis focused on medium-term (2030) and long-term (2040) risks and opportunities. Short-term (2026) climate-related risks and opportunities are addressed through Fortinet's enterprise risk management program. Insights from this analysis will inform our climate transition planning, strengthen future CDP and TCFD-aligned disclosures, and contribute to our preparedness for evolving climate-related reporting expectations. Fortinet's internal CSR committee and CSR team assess various ESG topics and related reputational, strategic, and financial risks. Related to climate risk, we consider factors including current and emerging regulations, technology trends, market dynamics, and potential reputational impacts. We consider acute and chronic physical risks, and consider factors such as disruptions to our operations and potential damage to our brand. Climate-related risks are also assessed as a part of Fortinet's periodic materiality assessment process. Several analyses in recent years have also informed our understanding of climate-related risks and opportunities, including the following: • We conducted a Scope 3 and product carbon footprint analysis in 2023 to assess the impacts of our supply chain partners and vendors on climate change. • In 2024, Fortinet completed a full lifecycle assessment of the FortiGate 40F firewall appliance—aligned with ISO 14040, 14067, and 14044 standards—which provided actionable insights into the product's environmental impact throughout its lifecycle. Based on that analysis, in 2025 Fortinet became the first cybersecurity company to publish an Environmental Product Declaration (EPD), for the FortiGate 40F Next-Generation Firewall, and we expanded our EPD program during the year to the FortiGate 50G Series.
	B. Describe the organization's processes for managing climate-related risks	CSR issues, including climate-related risks, are managed through Fortinet's ESG governance process. Learn more. In line with the Fortinet Environmental Policy, we are committed to reducing our environmental impact and improving our operations, including related to climate risk. We identify and control environmental impacts related to energy, water, and waste, and continually improve our performance through a comprehensive environmental management system certified to ISO 14001, which covers our largest owned warehouse and overflow warehouse, located in Union City, California. We continue to expand our programs and disclosure in this area. Increasing our employees' understanding of sustainability and circularity is fundamental to designing and delivering products and packaging with reduced environmental impacts. We engage our teams to deepen their knowledge in these areas and empower them to implement new ideas, including through workshops that employees in R&D, product management, and operations participated in during 2025. These covered sustainable design trends, Fortinet resources such as EPDs and the Product Carbon Footprint Calculator, and global eco-design and packaging regulations. Learn more. We also inform internal teams about climate-related issues through a monthly sustainability digest, training modules on sustainability, e-learning modules, company-wide awareness campaigns on topics such as plastics reduction and climate action, and other resources. Learn more.
	C. Describe how processes for identifying, assessing, and managing climate-related risks are integrated into the organization's overall risk management.	As part of our efforts on climate change oversight, our CSR and risk management teams (including Finance) have begun to collaborate on defining the best approach to integrating climate risk into the company's broader risk management priorities. Learn more. During 2025, this collaboration supported Fortinet's first comprehensive climate scenario analysis. Learn more.

Topic	Required disclosure	Reference/disclosure
METRICS AND TARGETS Disclosure of the metrics and targets used to assess and manage relevant climate-related risks and opportunities where such information is material	A. Disclose the metrics used by the organization to assess climate-related risks and opportunities in line with its strategy and risk management process	Fortinet tracks and discloses the following metrics related to performance in this area: • Scope 1 emissions • Scope 2 emissions (location based and market based) • GHG emissions intensity (normalized to revenue) • Energy consumption • Energy intensity (normalized to revenue) • Scope 3 emissions (the 11 categories that are relevant to Fortinet) • Percentage improvement in power efficiency per throughput for top products • E-waste • Recyclable waste • Total waste • Water consumption See Performance data for detail.
	B. Disclose Scope 1, Scope 2, and, if appropriate, Scope 3 greenhouse gas (GHG) emissions, and the related risks	See Performance data for Fortinet's Scope 1, Scope 2, and Scope 3 GHG emissions. Fortinet uses globally recognized standards and methodologies, such as the GHG Protocol Corporate Accounting and Reporting Standard (revised version), to calculate our GHG emissions. We calculate our GHG emissions across all Scopes, including the 11 Scope 3 categories that are relevant to Fortinet. See verification opinion from TÜV SÜD America, Inc.
	C. Describe the targets used by the organization to manage climate-related risks and opportunities and performance against targets	We aspire to reach net-zero GHG emissions by 2050 across our value chain (Scope 1, Scope 2, and Scope 3). In 2024, we defined our near-term GHG emissions-reduction targets for Scopes 1, 2, and 3 using the SBTi methodology and criteria. Our near-term GHG emissions-reduction targets for Scopes 1 and 2, which are aligned with a 1.5°C trajectory, along with our Scope 3 supplier and customer engagement targets, were validated by SBTi in 2024: • Fortinet commits to reduce 58.80% of absolute Scope 1 and Scope 2 emissions by 2030 (from a 2021 base year), covering all Fortinet-owned facilities globally. • Fortinet commits that 60.50% of its suppliers (by spend) and 69.24% of its customers (by revenue) will have science-based GHG emissions-reduction targets by 2029.

GRI INDEX

Statement of use		
Fortinet has reported with reference to the GRI Standards for the period Jan. 1–Dec. 31, 2025.		
GRI 1 used	GRI 1: Foundation 2021	
Applicable GRI Sector Standard(s)	None	
Disclosure	Reference	Alignment to the SDGs ¹
GRI 2: General disclosures 2021		
2-1 Organizational details	Who we are p. 3 2025 Form 10-K pp. 3–9	
2-2 Entities included in the organization's sustainability reporting	About this report p. 72	
2-3 Reporting period, frequency and contact point	About this report p. 72	
2-4 Restatement of information	There are no restatements.	
2-5 External Assurance	Limited assurance statement p. 82	
2-6 Activities, value chain and other business relationships	Who we are p. 3 2025 Form 10-K pp. 3–9	
2-7 Employees	Performance data p. 75	5.1, 5.5, 8.5
2-9 Governance structure and composition	ESG governance p. 69 Governance and Social Responsibility Committee Charter Human Resources Committee Charter Audit Committee Charter	
2-10 Nomination and selection of the highest governance body	Governance and Social Responsibility Committee Charter 2025 Proxy Statement pp. 36–37	
2-11 Chair of the highest governance body	Ken Xie, CEO and Chairman 2025 Proxy Statement p. 13	
2-12 Role of the highest governance body in overseeing the management of impacts	Governance and Social Responsibility Committee Charter 2025 Proxy Statement pp. 30–31	
2-13 Delegation of responsibility for managing impacts	ESG governance p. 69 Governance and Social Responsibility Committee Charter CSR Committee Charter	
2-14 Role of the highest governance body in sustainability reporting	The Board has approved this Sustainability Report.	
2-15 Conflicts of interest	Audit Committee Charter Governance Guidelines	

1. The sections and external resources noted in the Reference column of this GRI index directly or indirectly align with the Sustainable Development Goals (SDGs) items noted in this column.

Disclosure	Reference	Alignment to the SDGs ²
2-16 Communication of critical concerns	2025 Proxy Statement p. 37	
2-17 Collective knowledge of highest governance body	ESG governance p. 69	
2-18 Evaluation of the performance of the highest governance body	Governance and Social Responsibility Committee Charter	
2-19 Remuneration policies	2025 Proxy Statement pp. 39–43	
2-20 Process to determine remuneration	2025 Proxy Statement pp. 39–43 Human Resources Committee Charter	
2-22 Statement on sustainable development	Message from our CSR Committee p. 4	
2-23 Policy commitments	Anti-Corruption Policy Code of Business Conduct and Ethics Environmental Policy Global Health and Safety Policy Global Human Rights Policy Partner Code of Conduct Privacy Policy Responsible Minerals Sourcing Policy Secure Product Development Lifecycle Policy Vendor/Supplier Code of Conduct Whistleblower Policy	
2-24 Embedding policy commitments	Secure product development lifecycle p. 16 Sustainable operations pp. 34–37 Health, safety, and well-being p. 49 Data privacy p. 63 Business ethics pp. 64–65 Human rights pp. 66–67	
2-26 Mechanisms for seeking advice and raising concerns	Business ethics pp. 64–65	
2-28 Membership associations	Stakeholder engagement p. 11 Responsible technology pp. 15–18 Cybersecurity innovation pp. 19–22 Cybercrime disruption pp. 23–27 Cybersecurity skills gap pp. 51–58 Public policy p. 71	
2-29 Approach to stakeholder engagement	Stakeholder engagement pp. 11–12	
GRI 3: Material topics 2021		
3-1 Process to determine material topics	Double materiality assessment p. 10	
3-2 List of material topics	Double materiality assessment p. 10	
3-3 Management of material topics	The table of priority topics on p. 10 references the sections in this report that include detail about Fortinet's management approach and performance in each area.	

Disclosure	Reference	Alignment to the SDGs ¹
GRI 203: Indirect economic impacts 2016		
Management approach	Cybercrime disruption pp. 23–27 Cybersecurity skills gap pp. 51–58	
203-2 Significant indirect economic impacts	Cybercrime disruption pp. 23–27 Cybersecurity skills gap pp. 51–58 Performance data p. 75	16.3
GRI 205: Anticorruption 2016		
Management approach	Business ethics pp. 64–65 Anti-Corruption Policy	
205-2 Communication and training about anticorruption policies and procedures	Anti-corruption program and policy p. 65 Human rights in our supply chain p. 67 Performance data p. 73	16.5
GRI 302: Energy 2016		
Management approach	Energy pp. 35–36 Environmental Policy	
302-1 Energy consumption within the organization	Performance data p. 74	7.2, 7.3, 7.a, 13.1, 13.2
302-3 Energy intensity	Performance data p. 74	13.1, 13.2
302-4 Reduction of energy consumption	Energy pp. 35–36	13.1, 13.2
302-5 Reductions in energy requirements of products and services	Product energy efficiency p. 39 Performance data p. 74	7.2, 7.3, 7.a, 13.1, 13.2
GRI 303: Water and Effluents 2018		
Management approach	Water p. 37 Environmental Policy	
303-5 Water consumption	Performance data p. 74	6.4
GRI 305: Emissions 2016		
Management approach	Climate pp. 31–33 Environmental Policy	
305-1 Direct (Scope 1) GHG emissions	Performance data p. 74	13.1, 13.2
305-2 Energy indirect (Scope 2) GHG emissions	Performance data p. 74	13.1, 13.2
305-3 Other indirect (Scope 3) GHG emissions	Performance data p. 74	13.1, 13.2
305-4 GHG emissions intensity	Performance data p. 74	13.1, 13.2
305-5 Reduction of GHG emissions	Energy pp. 35–36	13.1, 13.2
GRI 306: Waste 2020		
Management approach	Waste p. 37 Sustainable packaging p. 41 Circularity p. 42 Environmental Policy	
306-3 Waste generated	Performance data p. 74	12

Disclosure	Reference	Alignment to the SDGs ¹
GRI 401: Employment 2016		
Management approach	Employee experience pp. 46–49	
401-1 New employee hires and employee turnover	Performance data p. 75	5.1, 5.5, 8.5, 10.2, 10.3, 10.4
GRI 404: Training and education 2016		
Management approach	Employee experience pp. 46–49	
404-2 Programs for upgrading employee skills and transition assistance programs	Employee awareness and engagement p. 12 Talent development and retention pp. 47–48 Cybersecurity skills gap pp. 51–58	8.6, 8.8
GRI 405: Diversity and equal opportunity 2016		
Management approach	Inclusive workplace p. 45	
405-1 Diversity of governance bodies and employees	Performance data p. 75	5.1, 5.5, 8.5
GRI 414: Supplier social assessment 2016		
Management approach	Human rights in our supply chain p. 67 Partner Code of Conduct Vendor/Supplier Code of Conduct	
414-1 New suppliers that were screened using social criteria	Performance data p. 73	
GRI 415: Public policy 2016		
Management approach	Public policy p. 71	
415-1 Political contributions	Public policy p. 71	
GRI 418: Customer Privacy 2016		
Management approach	Information security and data privacy pp. 61–63	
418-1 Substantiated complaints concerning breaches of customer privacy and losses of customer data	Information security and data privacy p. 62	

1. The sections and external resources noted in the Reference column of this GRI index directly or indirectly align with the Sustainable Development Goals (SDGs) items noted in this column.

SASB INDEX

The following index maps Fortinet disclosures to relevant indicators in the Sustainability Accounting Standards Board (SASB) Software & IT Services and Hardware Standards.

Topic	Accounting Metric(s)	SASB Code	Reference/Disclosure
Environmental footprint of hardware infrastructure	(1) Total energy consumed, (2) percentage grid electricity, (3) percentage renewable Unit: GJ, percentage	TC-SI-130a.1	Performance data p. 74
	Discussion of the integration of environmental considerations into strategic planning for data center needs	TC-SI-130a.3	Climate pp. 31–33 Sustainable operations pp. 34–37 Product energy efficiency p. 39
Data privacy & freedom of expression	Description of policies and practices relating to behavioral advertising and user privacy	TC-SI-220a.1	Data privacy p. 63
Data security	Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards	TC-SI-230a.2	Information security and data privacy pp. 61–63 Certifications list: ENS certification GovRAMP HIPAA examination ISMAP certification ISO 27001/27017/27018 certification National Security Framework (ENS) NIST 800-53/161 NIST 800/171 SOC2 Type II examination TISAX certification Up-to-date certifications can be found here .
Recruiting & managing a global, diverse & skilled workforce	Percentage of gender and racial/ethnic group representation for: (1) management, (2) technical staff, and (3) all other employees	TC-SI-330a.3/ TC-HW-330a.1	Performance data p. 75
Managing systemic risks from technology disruptions	Description of business continuity risks related to disruptions of operations	TC-SI-550a.2	Securing the digital world pp. 14–29 Information security and data privacy pp. 61–63

TÜV SÜD America Inc.
750 Main Street, Suite 200
Grand Junction, CO 81501



Verification Opinion

Submitted to: Fortinet Inc.
Verification Body: TÜV SÜD America Inc.
Lead Verifier: Issaí Medellín
Submitted: 4/16/2026

TÜV SÜD America Inc. (TÜV SÜD) conducted the verification of Fortinet's 2025 GHG Inventory according to the requirements found in ISO 14064-1:2019, 14064-3:2019, 14065:2020, and 17029:2019. The objective of this verification was to ensure that the GHG statement is materially correct and conforms to all relevant criteria. The GHG statement is the responsibility of Fortinet. A summary of the GHG statement is as follows:

- GHG-related activity: Fortinet's US & Global Operations
- GHG statement period: Calendar Year (CY) 2025
- Criteria:
 - The Greenhouse Gas Protocol (GHG Protocol): Corporate Accounting and Reporting Standard, World Resources Institute and World Business Council for Sustainable Development, March 2004
 - Appendix F to the GHG Protocol Corporate Accounting and Reporting Standard – Revised Addition, June 2006, version 1.0
 - ISO 14064-1:2019 “Greenhouse gases – Part 1: Specification with guidance at the organization level for quantification and reporting of greenhouse gas emissions and removals”
 - ISO 14064-3:2019 “Greenhouse gases – Part 3: Specification with guidance for the validation and verification of greenhouse gas statements”

The data and information supporting the GHG statement were historical in nature.

Based on the examination of the evidence, nothing comes to TÜV SÜD's attention which gives cause to believe that the GHG statement is not a fair representation of GHG data and information.

TÜV SÜD has verified Fortinet's inventory to a limited level of assurance, and confirms that there is no evidence that the GHG statement:

- Is not materially correct and
- Has not been prepared in accordance with all applicable criteria.

The verified GHG statement is summarized on the following page.

TABLE 2. CY 2025 ENTITY EMISSIONS

EMISSIONS VERIFIED	CO ₂ E (METRIC TONS)
Stationary Combustion	1,469
Fugitive	259
Total Scope 1	1,728
Scope 2 (Location-Based)	15,721
Scope 2 (Market-Based)	0
Total Scope 1 & 2	17,449

LEAD VERIFIER SIGNATURE

ISSAÍ MEDELLÍN

INDEPENDENT REVIEWER SIGNATURE

SAM PHILLIPS



Global Headquarters

909 Kifer Road, Sunnyvale, CA 94086, USA
Tel: +1-408-235-7700 / Fax: +1-408-235-7737

Forward-looking information

This report contains forward-looking statements that involve risks and uncertainties that are subject to the safe harbors created under the Securities Act of 1933, as amended, and the Securities Exchange Act of 1934, as amended. All statements herein other than statements of historical fact are statements that could be deemed forward-looking statements. These statements are based on expectations, estimates, forecasts, objectives, and projections, and words such as “expects,” “anticipates,” “targets,” “goals,” “objectives,” “projects,” “commits,” “intends,” “plans,” “believes,” “seeks,” “estimates,” “continues,” “endeavors,” “strives,” “may,” variations of such words, and similar expressions are intended to identify such forward-looking statements. In addition, statements are forward-looking statements if they are statements that refer to (1) our goals, objectives, future commitments, and programs; (2) our business plans and initiatives; (3) our assumptions and expectations; (4) the scope and impact of our corporate responsibility risks and opportunities; and (5) standards and expectations of third parties. Readers are cautioned that these forward-looking statements are only predictions and are subject to risks, uncertainties, and assumptions that are difficult to predict. It is possible that future circumstances might differ from the assumptions on which such statements are based and actual results may differ for other reasons, such that actual results are materially different from our forward-looking statements in this report. Important factors that could cause results to differ materially from the statements herein include the following: general economic risks, changes in circumstances, delays in meeting objectives for any reason, changes in plans or objectives for any reason, risks associated with disruption caused by natural disasters and health emergencies such as earthquakes, fires, power outages, typhoons, floods, health epidemics, and by man-made events such as civil unrest, labor disruption, international trade disputes, wars, and critical infrastructure attacks, and other risk factors set forth from time to time in our most recent Annual Report on Form 10-K, our most recent Quarterly Report on Form 10-Q, and our other filings with the Securities and Exchange Commission (SEC), copies of which are available free of charge at the SEC’s website at www.sec.gov or upon request from our investor relations department. Forward-looking statements speak only as of the date they are made, and we do not undertake any obligation to update, and we hereby expressly disclaim any obligation to update, any forward-looking statement in light of new information or future events.

www.fortinet.com