
2024
SUSTAINABILITY
REPORT
FORTINET

TABLE OF CONTENTS

WHO WE ARE

MAKING POSSIBLE A DIGITAL WORLD YOU CAN ALWAYS TRUST

Founded more than 20 years ago in Sunnyvale, California, Fortinet is a global leader in cybersecurity and a driving force in the convergence of networking and security. By securing people, devices, and data everywhere, we help build a safe, trusted and sustainable digital world for all. We are committed to addressing cybersecurity risks to society, respecting the environment, growing an inclusive cybersecurity workforce, and promoting responsible business across our value chain.

Founded
OCTOBER 2000

Corporate headquarters
Sunnyvale
California, USA

Number of locations
100+

Fortinet employees in 2024*
14,138

Cash and investments*
$4.1B

2024 revenue
$5.96B

Market capitalization*
$72.5B

80%
of Fortune 100 and **72%** of Global 2000 companies depend on Fortinet to stay secure

Included in
Nasdaq NASDAQ-100
STANDARD &POOR'S500

Global customer base*
830,000+

R&D investment in 2024
$717M

Patents globally*
1,378

*As of Dec. 31, 2024.

LETTER FROM OUR CEO

The year 2024 brought profound changes to society on multiple fronts. Rapid technological disruption, geopolitical tensions, escalating climate impacts, and evolving stakeholder expectations reshaped how people and businesses operate globally. Amid this shift, the critical role of cybersecurity in safeguarding not only business but society became increasingly evident. As digital transformation accelerated, securing data, infrastructure, and operations proved essential for business resilience and continuity and the protection of our interconnected world.

At Fortinet, we are proud that our products, services, and people contribute to building a more secure and sustainable society. For over 20 years, we've led cybersecurity innovation, embedding security into every stage of product development. In 2024, we strengthened this commitment by becoming one of the first cybersecurity companies to sign the Cybersecurity and Infrastructure Security Agency (CISA) Secure by Design Pledge.

At the same time, artificial intelligence (AI) is rapidly evolving, reshaping industries, communities, and individuals. Fortinet has long been at the forefront of this evolution, integrating over 10 years of AI and machine learning expertise into our cybersecurity solutions. With more than 500 AI-related patents issued and pending, we remain committed to pushing the boundaries of AI innovation, as reflected in the continued expansion of AI capabilities across our products and services over the past year.

The growing scale of cybercrime also demands stronger public-private collaboration. For over a decade, we've partnered with law enforcement and cybersecurity agencies worldwide, sharing our threat intelligence and expertise. In 2024, we supported initiatives like INTERPOL's Operation Serengeti and the World Economic Forum's (WEF) Cybercrime Atlas project, contributing to the arrest of over 1,000 cybercriminal groups and the dismantling of more than 134,000 malicious networks.

Beyond securing the digital world, we are committed to making a broader societal impact. Addressing the global cybersecurity skills gap remains a top priority. I am pleased to share that we now stand at 63% of our goal to train one million people in cybersecurity by 2026. In 2024, we strengthened this commitment by joining the European Commission Cybersecurity Skills Academy, pledging to train 75,000 individuals in the EU by 2027. We also launched a global employee engagement initiative, empowering our teams to deliver cybersecurity awareness workshops to children in local communities.

Our commitment to sustainability extends to helping tackle climate change, which remains an urgent global challenge. The past year was the hottest on record since tracking began in 1880, leading to numerous global catastrophes—from Hurricane Helene and wildfires in Chile to floods in Spain and extreme heatwaves worldwide. 2024 marked an important milestone in our climate strategy with the validation of our near-term greenhouse gas (GHG) emissions reduction targets established by the Science Based Targets initiative (SBTi). We also continued to focus on reducing the environmental impact of our products by improving our product energy efficiency while maximizing performance and adopting sustainable product packaging.

At the heart of all this work are our employees who make it possible. Reflecting our progress across various facets of sustainability, Fortinet was named to the 2024 Dow Jones Best-in-Class World and North America Indices for the third consecutive year.

We were also recognized as No. 7 on Forbes' Most Trusted Companies in America 2025—the most trusted US-based cybersecurity company. I'm grateful for the trust of our stakeholders, and we remain committed to fostering a business grounded in integrity, privacy, and respect for human rights.

Our vision of making possible a digital world you can always trust is more important than ever. Cybersecurity is essential for the sustainability of society and the global economy. While much work remains, we are committed to making progress, delivering value, and contributing to a secure and sustainable tomorrow.

Ken Xie

Fortinet Founder, CEO
and Chairman of the Board

2024 SUSTAINABILITY HIGHLIGHTS

CONTRIBUTED TO
1,006
CYBERCRIMINAL GROUP ARRESTS

DISMANTLING
134,000+
MALICIOUS NETWORKS

AND RECOVERING
$44M
THROUGH INTERPOL GATEWAY AND WEF CYBERCRIME ATLAS

6
RECOGNITIONS AS ONE OF
THE BEST PLACES TO WORK

NEAR-TERM CLIMATE TARGETS
VALIDATED BY SBTi

61%
AVERAGE REDUCTION IN PRODUCT ENERGY CONSUMPTION

~387
METRIC TONS OF CO_2e EMISSIONS AND

~77
METRIC TONS OF PLASTIC AVOIDED THROUGH ECO-FRIENDLY PACKAGING

CISA SECURE
BY DESIGN PLEDGE

630,859
PEOPLE TRAINED IN CYBERSECURITY SINCE 2022

NEW PLEDGE:
75,000
INDIVIDUALS TRAINED IN CYBERSECURITY IN THE EUROPEAN UNION (2024–2027)

81
INFORMATION SECURITY CERTIFICATIONS AND EXAMINATIONS

BOARD-LEVEL
CYBERSECURITY COMMITTEE

FORTINET'S TRAINING ON COMPLIANCE AND BUSINESS ETHICS COMPLETED BY

100%
OF OUR DISTRIBUTORS

100%
OF OUR TOP CONTRACT MANUFACTURERS

SUSTAINABILITY AT FORTINET

SUSTAINABILITY APPROACH

ADDRESSING CYBERSECURITY RISKS TO SOCIETY

We work to advance the industry through continually innovating in our products and services to protect organizations against evolving cyber threats, collaborating with public and private organizations globally to combat cybercrime, and engaging customers to support their continued success.

PRIORITY TOPICS*
- Innovation and responsible technology
- Cybercrime disruption

RESPECTING THE ENVIRONMENT

We are focused on addressing the impacts of climate change and minimizing the environmental footprint of our solutions, operations, and broader value chain.

PRIORITY TOPICS*
- Climate change
- Product environmental impacts

GROWING AN INCLUSIVE CYBERSECURITY WORKFORCE

We are committed to fostering an inclusive and diverse workforce within our organization and across the cybersecurity industry. By empowering individuals from all backgrounds to reach their full potential and providing the knowledge needed to navigate the digital world securely, we help bridge the cybersecurity skills gap and build a safer, more resilient digital future for all.

PRIORITY TOPICS*
- Inclusion and belonging
- Cybersecurity skills gap

PROMOTING RESPONSIBLE BUSINESS

We are committed to conducting business ethically across our entire value chain, including respecting human rights, complying with all laws, and ensuring our employees, partners and others adhere to our policies. To protect our information systems and our employees' and customers' data, we implement industry best practices and uphold the highest standards internally for information security, data protection, and privacy.

PRIORITY TOPICS*
- Business ethics
- Information security and data privacy

AWARDS AND RECOGNITION

Dow Jones Best-in-Class Indices

DOW JONES BEST-IN-CLASS INDICES

Named in the 2024 Dow Jones Best-in-Class World and North America Indices for the third consecutive year

CDP

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

ECOVADIS

Awarded a Bronze EcoVadis medal in 2024 with a score of 59 (out of 100), ranked in the 67th percentile of all companies

FORBES MOST TRUSTED COMPANIES

Recognized as one of the top 10 companies on Forbes' Most Trusted Companies in America

MSCI

Received a rating of BBB in the MSCI ESG rating assessment

SUSTAINALYTICS

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

ISS ESG

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

**These reflect the sustainability topics that matter most to our business and stakeholders, as identified in our 2024 sustainability materiality assessment.*
Note that certain topic names have been updated since the prior materiality assessment due to evolutions in the market.

SUSTAINABILITY APPROACH

Meera Ramanathan
Director, Global Sustainability and CSR at Fortinet
Chairman of the CSR Committee

How has Fortinet approached sustainability?
Since embarking on our sustainability journey, we have continually challenged ourselves to understand how we can most effectively help to address broader societal challenges while bolstering the resilience and longevity of our business and creating value for our stakeholders. Our sustainability framework, defined through a materiality assessment, reflects the key topics that matter most to our business and stakeholders, guiding our strategy and programs.

How does Fortinet implement its sustainability strategy?
Our sustainability efforts involve collaborations across various functions and business groups across our company. We've established robust Corporate Social Responsibility (CSR) governance structures to drive and coordinate these efforts, and we engage our stakeholders though multiple channels to ensure we meet their evolving expectations. Transparent disclosure is central to our approach, using established reporting frameworks to communicate our progress.

What were some key sustainability advancements in 2024?
In 2024, we advanced our sustainability strategy in multiple areas. We continued to enhance our programs, for example, by establishing our decarbonization plan, validating our near-term GHG emission targets by SBTi, reducing e-waste though our new hardware donation program, expanding eco-friendly packaging, and developing energy-efficient cybersecurity solutions. We also increased awareness of sustainability throughout our employee base through new educational modules and awareness campaigns related to the environment and inclusion.

How is sustainability integrated across Fortinet's operations?
Sustainability is integrated into all aspects of our business. In 2024, we trained our R&D team on circularity, empowered our employee resource group members to help them with their mission and align with our strategy, and implemented sustainable practices in our events, particularly in the EMEA region. These efforts have inspired our employees to adopt innovative approaches, and we remain committed to advancing our sustainability journey with their continued support.

How does Fortinet adapt its sustainability practices?
Sustainability is dynamic, and we continually enhance our practices to align with evolving external frameworks, regulations, and stakeholder interests. The introduction of the Corporate Sustainability Reporting Directive (CSRD) in European countries and the development of other regional and national requirements around the world, including upcoming regulations in the USA, require expanded reporting. We are actively preparing for these comprehensive disclosures, covering a wide range of sustainability topics.

REPORTING FRAMEWORKS

Fortinet continually enhances its sustainability reporting practices by aligning with globally recognized disclosure frameworks. These are GRI (Global Reporting Initiative) Standards, Sustainability Accounting Standards Board (SASB) Standards, Task Force on Climate-related Financial Disclosures (TCFD), United Nations Global Compact (UNGC), and CDP. Our GRI, SASB, and TCFD indices are included in the Appendix of this report. This 2024 Sustainability Report serves as Fortinet's UNGC Communication on Progress for the year.

Given the increasing prevalence of mandated ESG disclosures, Fortinet is preparing for further initiatives to support the evolving sustainability landscape. This aligns with industry trends and showcases our commitment to upholding the highest standards of transparency in our operations and sustainability reporting.

UNITED NATIONS SUSTAINABLE DEVELOPMENT GOALS

The United Nations Sustainable Development Goals (UN SDGs) provide an essential global framework for driving social, environmental, and economic progress. Fortinet has identified seven UN SDGs on which it can have a positive impact: Quality Education, Gender Equality, Affordable and Clean Energy, Decent Work and Economic Growth, Reduced Inequalities, Climate Action, and Peace, Justice, and Strong Institutions. Throughout the report, we indicate where our commitments align with these UN SDGs.

SUSTAINABILITY MATERIALITY

Engaging with our stakeholders and understanding the environmental, social, and governance (ESG) topics that matter most to them is essential to guiding our sustainability strategy.

We conducted a materiality assessment in 2021 to identify the key ESG topics driving our business success and stakeholder interests. In 2024, we refreshed our materiality assessment, partnering with BSR (Business for Social Responsibility) to align with evolving stakeholder expectations, industry best practices, and regulatory evolutions. The assessment followed best practice phases of conducting research, engagement, and topic ranking, aligning our topic definitions with the European Sustainability Reporting Standards. BSR and Fortinet gathered input via individual interviews and group workshops with a wide range of key stakeholders, including employees, executives, Board members, customers, peers, partners, nongovernmental organizations (NGOs), and investors.

Results largely aligned with our 2021 findings, reaffirming the importance of topics such as data privacy and cybersecurity, responsible innovation, product environmental impacts, climate change mitigation, the cybersecurity skills gap, diversity and inclusion, business ethics, and sustainable supply chain.

DOUBLE MATERIALITY ASSESSMENT

We are initiating our first double materiality assessment in preparation for future disclosures aligned with the Corporate Sustainability Reporting Directive. This assessment will expand on current materiality efforts by identifying material impacts, risks and opportunities that at once impact our stakeholders and society, and affect Fortinet's financial performance over time. We will complete this assessment in 2025 to guide disclosures in the near future.

STAKEHOLDER ENGAGEMENT

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

CUSTOMERS AND CHANNEL PARTNERS

We communicate with customers and channel partners about Fortinet's sustainability priorities and performance through our annual sustainability report, website, blogs, and partner portal. Through responses to customer requests for proposals (RFPs), inquiries, and assessments, we provide details regarding topics such as cybersecurity risk, data privacy, environmental impact, compliance, ethics, and digital inclusion. We also collaborate with customers and partners to jointly drive sustainability efforts. Examples in 2024 included advising a customer on how to embed sustainability into its RFP process and helping customers and partners address the skills gap through our certification programs and security awareness training.

EMPLOYEES

We engage our employees on sustainability initiatives through ongoing awareness campaigns, employee resource groups, the Ambassadors and Allies network, and our idea submission tool, FortiIdeas. Through ongoing training, we help employees enhance their knowledge in areas such as business ethics, compliance, information security, inclusion, and the environment. In 2024, we also provided targeted training, such as circularity workshops, to further embed sustainability into employees' daily activities.

INVESTORS

We regularly communicate with investors through quarterly earnings calls, analyst days, conferences, and other ongoing communications. These interactions allow us to discuss topics such as Fortinet's strategy and performance, corporate governance, and sustainability initiatives while deepening our understanding of investors' priorities.

SUPPLY CHAIN

As part of our due diligence processes, we continually engage with our suppliers to assess risks, monitor key areas for our business, conduct audits, and provide guidance to resolve non conformance. In 2024, we also conducted a project to identify opportunities to help our suppliers advance their GHG emissions reduction targets in alignment with SBTi.

COMMUNITIES, SCHOOLS AND NGOS

We collaborate with NGOs to drive progress in women's empowerment, digital inclusion, and environmental sustainability. In 2024, we continued working with organizations such as WiCyS, WOMCY, and Women4Cyber to help build a diverse cybersecurity talent pool. Through our Education Partners Program, we donated Fortinet hardware to universities to enhance student labs. New partnerships in 2024 included Laurette Fugain in France (donation of repurposed Fortinet access points) and United Way Bengaluru in India (laptop donations for students impacted by natural disasters).

INDUSTRY COLLABORATION

We collaborate with industry partners to advance the cybersecurity industry through workshops, advisory/thought leadership activities, partnerships, and other initiatives. In 2024, we focused particularly on efforts related to AI (such as the WEF AI and Cyber Initiative) and threat intelligence sharing to fight cybercrime (such as the "early share" program through the Cyber Threat Alliance). As a founding member of the WEF Cybercrime Atlas initiative, we continued our work to disrupt cybercrime by mapping and exposing the cybercriminal ecosystems to enhance collective defense. We also introduced new initiatives through the WEF to help close the cybersecurity skills gap.

GOVERNMENT AND REGULATORS

Fighting cybercrime requires strong collaboration between the public and private sectors, and we work closely with international, regional, and national government law enforcement to support these efforts. In 2024, Fortinet contributed to Operation Serengeti with INTERPOL, which led to 1,006 arrests and demonstrated the impact of coordinated action against cybercrime on a global scale. To advance the industry and enhance cybersecurity throughout the product development lifecycle, in 2024, Fortinet signed the CISA Secure by Design Pledge. We also joined the European Commission's Cybersecurity Skills Academy initiative, pledging to train up to 75,000 individuals in the EU to help close the cybersecurity skills gap. Additionally, we engage in public policy advocacy to advance the interests of our company, our customers, and other stakeholders.

CSR GOVERNANCE

Through robust CSR governance structures across Fortinet, we ensure efficient and collaborative deployment of our sustainability strategy. These structures underpin our work to implement and continually improve programs and initiatives, communicate performance, drive accountability for ongoing progress, and engage and educate leaders and employees throughout the company.

Our approach to CSR is based on a strong corporate governance structure, starting with our Board of Directors. As Fortinet's lead sponsor of CSR, the Board of Directors oversees and approves our commitments to ESG priorities.

In 2024, the Fortinet Board's Governance and Social Responsibility Committee was formed as a joint committee comprising at least two Board members to oversee both the company's governance and its sustainability strategies. This committee reviews CSR risks and opportunities quarterly. As appropriate, the Governance and Social Responsibility Committee collaborates with other Board committees, such as the Cybersecurity Committee, new in 2024, which oversees cybersecurity and other information technology risks, controls, and processes.

Fortinet's Executive Team validates the sustainability strategy, approves targets, monitors execution, and provides sponsorship to integrate sustainability into business operations and decision-making processes.

Fortinet's internal CSR Committee defines the company's sustainability priorities, sets objectives and strategy, and oversees related initiatives and programs. It also engages internal and external stakeholders to raise awareness of sustainability topics and ensure transparency. Chaired by Fortinet's Global Sustainability and CSR Director, the committee is composed of CSR Champions—cross-functional management representatives from across the company. These CSR Champions are responsible for driving progress in their areas of subject matter expertise, ensuring accountability and advancing specific roadmaps tied to Fortinet's sustainability priorities. The Committee meets at least four times a year and shares progress and recommendations with Fortinet's Executive Team and the Board's Governance and Social Responsibility Committee once a quarter.

The Fortinet CSR Team leads strategy development and oversees sustainability reporting. It also engages across all company levels to execute Fortinet's sustainability strategy.

Business units across Fortinet contribute to implementing our sustainability strategy and further embedding sustainability into the company's operations. Each business unit has its own CSR Champion, who is accountable for implementing action plans, achieving operational goals, and measuring and reporting progress. In addition, volunteer employee CSR Ambassadors help educate and engage Fortinet's broader workforce on sustainability.

ADDRESSING CYBERSECURITY RISKS TO SOCIETY

As digitization transforms nearly every aspect of our personal and professional lives, cybersecurity has become fundamental to the sustainability of our society. Simply put, cybersecurity is the backbone of our modern world. Without it, individuals, organizations, and even nations are at risk. We are committed to advancing the cybersecurity industry through continuous product and service innovation, collaboration with public and private organizations worldwide to combat cybercrime, and customer engagement to support their ongoing success. Through this multifaceted approach, we work to strengthen our collective defenses against cyber adversaries and create a more secure and sustainable society.

2024 HIGHLIGHTS

CISA SECURE BY DESIGN PLEDGE

Through the INTERPOL Gateway program and the WEF Cybercrime Atlas, we contributed to

THE ARREST OF **1,006** cybercriminal groups

THE DISMANTLING OF **134,000+** malicious infrastructures and networks

AND THE RECOVERY OF **$44M**

CYBER RISKS: A GROWING THREAT TO SOCIETY

Cyber risks have become one of the most significant threats to society, affecting national security, economic stability, and individual safety. As digitization becomes embedded in nearly every aspect of life—spanning critical infrastructure, healthcare, and commerce—the risks posed by cyberattacks have grown exponentially. According to the WEF's Global Risks Report 2025, cyber espionage and warfare are ranked as the fifth most significant short-term risks (within two years) across all stakeholder groups and the fourth most significant long-term risks (within 10 years) for the private sector, emphasizing the societal impact of these threats.

Critical infrastructures, the backbone of our modern society, are increasingly susceptible to cyber risks. Power grids, water supplies, transportation systems, and healthcare networks rely heavily on interconnected digital technologies, making them prime targets for cyberattacks. A single breach of these critical infrastructures could cause widespread disruption, destabilize economies and threaten public safety.

Beyond critical infrastructures, cyber risks impact individuals and communities directly. Phishing scams, identity theft, and financial fraud undermine trust, while disinformation campaigns destabilize societies by manipulating public opinion and eroding confidence in democratic processes. As geopolitical tensions rise, state-sponsored cyberattacks targeting elections, financial systems, or essential services threaten global stability and amplify the urgency of addressing cyber risks.

Emerging technologies, such as AI, compound these risks by expanding the attack surface. AI-driven phishing campaigns, for example, are increasingly difficult to detect, while unsecured Internet of Things (IoT) devices can serve as entry points for hackers to infiltrate larger systems. The interconnected nature of supply chains also means a single compromised vendor could disrupt industries worldwide, further exposing societies to the ripple effects of cyberattacks.

Addressing these cyber risks is not just a technical challenge—it is a societal imperative. Protecting society from these risks requires a collective effort from governments, businesses, and individuals. This includes investing in robust cybersecurity measures, fostering international collaboration, and addressing disparities in cyber preparedness to ensure all communities are equipped to navigate the growing threat landscape. Public awareness and education are also essential to empowering individuals to recognize and mitigate risks.

As our world becomes increasingly interconnected, cyber risks to society grow—not only in scale but also in impact. Cybersecurity is a fundamental pillar of our society's resilience, trust, stability, and security. By addressing these risks collectively, we can build a safer, more resilient digital world.

WORLD ECONOMIC FORUM

GLOBAL RISKS RANKED BY SEVERITY OVER THE SHORT AND LONG TERM

"Please estimate the likely impact (severity) of the following risks over a 2-year and 10-year period."

2 years		10 years	
1	Misinformation and disinformation	1	Extreme weather events
2	Extreme weather events	2	Biodiversity loss and ecosystem collapse
3	State-based armed conflict	3	Critical change to Earth systems
4	Societal polarization	4	Natural resource shortages
5	Cyber espionage and warfare	5	Misinformation and disinformation
6	Pollution	6	Adverse outcomes of AI technologies
7	Inequality	7	Inequality
8	Involuntary migration or displacement	8	Societal polarization
9	Geoeconomic confrontation	9	Cyber espionage and warfare
10	Erosion of human rights and/or civic freedoms	10	Pollution

SECURE BY DESIGN, SECURE BY DEFAULT

Our top priority is protecting our customers' security at all stages of the product lifecycle and continually improving our policies and processes. We recognize the importance of robust supply chain security for our customers and are committed to providing products that are secure by design and secure by default to support a safe digital society that benefits everyone.

SECURE PRODUCT DEVELOPMENT LIFECYCLE

Our Secure Product Development Lifecycle Policy, based on secure by design and secure by default principles, helps ensure that security is designed into each product from inception, covering every stage of the product lifecycle through to end-of-life. This includes efforts such as developing our own system-on-a-chip (SOC) application-specific integrated circuits (ASICs) in-house, operating a Trusted Supplier Program with rigorous selection and qualification of manufacturing partners, aligning with secure development best practices, and performing independent third-party penetration testing at regular intervals, among others.

Fortinet applies secure product development best practices aligned with leading standards such as NIST 800-53, NIST 800-160, NIST 800-218, U.S. EO 14028, and UK TSA. We have also completed CISA attestation for Secure Product Development (Fortinet's attestations are available on the DHS Repository for Software Attestations and Artifacts portal).

INCIDENT RESPONSE

The Fortinet Product Security Incident Response Team (PSIRT) maintains security standards for Fortinet products. Our culture of proactive, transparent, and responsible vulnerability disclosure and handling follows ISO/IEC 29147 and ISO/IEC 30111 and recommendations from government entities, such as the CISA in the United States. In 2024, 65% of Fortinet vulnerabilities were proactively and internally identified through our rigorous auditing process, which allows Fortinet and our customers to stay one step ahead of threat actors.

To accomplish its PSIRT mission, Fortinet collaborates with customers, independent security researchers, consultants, industry organizations, and other vendors. We respond appropriately to findings obtained through these exercises and publish all remediated issues, whether discovered internally or externally, including through a Monthly Vulnerability Advisory released on the second Tuesday of each month.

Carl Windsor
Chief Information Security Officer (CISO)
and Member of the CSR Committee at Fortinet

« In an interconnected world facing growing cyberattacks, it's critical to ensure that technology systems are resilient to keep organizations, individuals, nations, governments, and economies safe. For over 20 years, Fortinet has pioneered a secure by design approach, embedding security into every phase of our product and software development lifecycle—not just at the beginning or end. In 2024, we deepened this commitment by becoming an early signer of CISA's Secure by Design pledge, reinforcing our dedication to delivering measurable improvements. As part of this effort, we are working to improve the adoption of Fortinet-issued security patches, aligning with the pledge's goals to strengthen our customers' security postures. We look forward to sharing more progress. Securing our digital ecosystem requires collaboration, and we encourage industry partners, policymakers, and security experts to join this important work. »

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA) SECURE BY DESIGN PLEDGE

In 2024, Fortinet was one of the first cybersecurity companies to sign the CISA Secure by Design Pledge. CISA, together with its global partners, introduced this pledge to prioritize cybersecurity throughout the product development lifecycle and use data-driven intelligence to deliver measurable improvements that strengthen cybersecurity for customers across the globe.

By committing to actionable and measurable steps across seven key areas—enforcing multi-factor authentication, removing default passwords, reducing entire classes of vulnerability, increasing the uptake of security patches, implementing a robust vulnerability disclosure policy, documenting common vulnerabilities and exposures, and logging evidence of intrusions—Fortinet reinforces its secure product development processes. This pledge complements and builds on existing Fortinet software security best practices—including those developed by CISA, NIST, other federal agencies, and international and industry partners—and enhances our ability to deliver trusted, resilient technologies to customers.

As part of this pledge, Fortinet has made progress, including the successful auto-updating to help secure over 750,000 devices in 2024. Fortinet is committed to continuing measurable improvements and regularly publishing progress toward the Secure by Design pledge.

SECURITY INNOVATION

Cybersecurity innovation is the only way to keep up with the ever-evolving threat landscape. For more than 20 years, Fortinet's commitment to remaining at the forefront of innovation has been essential to helping organizations protect themselves digitally.

Our innovation is founded on the principles of converging networking and security technologies into an integrated platform—The Fortinet Security Fabric—providing customers with a holistic approach to cybersecurity that ensures comprehensive protection across the entire infrastructure and attack surface. It also reduces complexity, eliminates security silos, and improves operational efficiency. Our portfolio of more than 50 products, combined with open APIs and a technology alliance partner ecosystem of over 500 third-party vendors, enables customers to build on their existing deployments.

We've spent more than two decades organically developing our solutions around the FortiOS operating system and Security Processing Units (SPUs)—proprietary purpose-built ASICs that deliver high performance while enabling power-efficient products that reduce environmental impact. In 2024, Fortinet announced the latest version of FortiOS (version 7.6) with hundreds of enhancements including new generative AI (GenAI), data protection, managed services, and unified agent features that help customers better mitigate risks, reduce complexity, and improve user experience across their networks.

790+
tech integrations

420
Fabric-Ready partners (one of the industry's largest ecosystems)

2024 MAJOR PRODUCT LAUNCHES AND ENHANCEMENTS

Fortinet fuels its industry-leading innovation engine through a company culture that encourages and rewards innovative thinking. Our R&D team files approximatively 15-20 patent applications each quarter, bringing our total to 1,378 patents issued and 451 patents pending. In 2024, Fortinet's R&D investments led to three new products and services, showcasing our commitment to delivering innovative security solutions that stay ahead of evolving cyber threats and empower our customers.

Secure networking

In 2024, Fortinet introduced key innovations in secure networking, including the industry's first WiFi 7 access point and a 10 Gigabit power over ethernet switch, delivering faster speed, higher power, and improved performance. We also launched several next-generation firewalls, including the FortiGate 200G, which combines industry-leading security and networking performance with energy efficiency—four times better than the industry average. The FortiGate Rugged 70G with Dual 5G Modems earned the Red Dot Product Design Award, a testament to Fortinet's commitment to design excellence and innovation.

Unified SASE

Fortinet made significant advancements in Secure Access Service Edge (SASE) in 2024 with monthly updates, including launching a sovereign SASE offering and the integration of GenAI technology. These innovations deliver greater flexibility, simplicity and control over their data and security operations. We also introduced the FortiDLP product family, combining powerful endpoint data loss prevention with insider risk management to help organizations anticipate and prevent data theft.

AI-driven security operations

In 2024, Fortinet expanded its GenAI portfolio by introducing the industry's first GenAI IoT security assistant, enabling SecOps and NetOps teams to make faster, more informed decisions while improving response time and operational efficiency. Learn more on how we leverage AI and collaborate to advance AI in cybersecurity. We also launched Lacework FortiCNAPP, a solution designed to simplify risk management, accelerate threat detection and response, and enhance security effectiveness from code to cloud.

$717M
investment in R&D in 2024

1,378
patents issued

3
new products and services introduced in 2024

CULTURE OF INNOVATION

Fortinet champions a culture of innovation by engaging employees at all levels through its crowdsourcing initiatives. These include:

- **FortiHours:** This program enables our R&D team to dedicate time to crafting new ideas or tools, with support and guidance from management.
- **FortiIdeas:** This initiative, open to all employees, facilitates the submission of product concepts and company suggestions to Fortinet's Innovations Council. Some of the ideas that have been submitted and accepted included an academic donation program based on Fortinet refurbished devices, improvements to the quality of release notes, and the introduction of auto-updates for devices as part of the Secure by Design pledge.
- **Patent submission system:** Employees across the company can submit potentially patentable innovations to a patent review board.
- **Feature request tool:** Employees can propose new product features through the New Feature Request (NFR) process, ensuring a steady flow of ideas from all corners of the organization. In 2024, over 3,000 NFRs were submitted, with 40% completed 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 direct feedback to our CTO.

CYBERSECURITY INDUSTRY ADVANCEMENT

While cybersecurity enables innovation in every sector of the digital economy, innovative technologies also enable cybersecurity to more effectively secure networks, people, organizations, and data worldwide. As a key part of Fortinet's innovation journey, the company has embraced disruptive technologies to advance the cybersecurity industry.

Artificial intelligence

Fortinet has pioneered AI innovation across its cybersecurity products and services, leveraging over a decade of expertise in AI and machine learning. We use AI in several ways, including GenAI to improve product optimization, Big Data AI to process and analyze trillions of events for actionable threat intelligence, network operations AI to create self-healing networks with end-to-end automation, and AI for large language models (LLMs) to improve data security.

We also have more than 500 AI-related patents issued and pending, and we continue to invest in expanding AI into our products and services (see 2024 major product launches and enhancements).

In 2024, Fortinet strengthened its commitment to advancing the cybersecurity industry by collaborating on key research projects and initiatives focused on AI and its impact on cybercrime and cybersecurity. Partnering with the UC Berkeley Center for Long-Term Cybersecurity (CLTC), the Berkeley Risk and Security Lab (BRSL), and other public and private organizations, we contributed to the "AI-Enabled Cybercrime: Exploring Risks, Building Awareness, and Guiding Policy Responses" project. This nine-month initiative combined tabletop exercises, surveys, workshops, and expert interviews, including Fortinet's insights, to develop proactive defense strategies against AI-powered cybercrime.

We also participated in the CLTC's "Weaponization of AI" workshop, contributing to a one-and-a-half-year project addressing AI misuse risks. As a founding member of the WEF's AI and Cyber Initiative, we shared real-world insights from FortiGuard Labs to help organizations manage AI-related cyber risks. Additionally, we engaged in a CISA-led AI Cyber Tabletop Exercise, collaborating with experts across sectors to tackle AI-driven cybersecurity incidents.

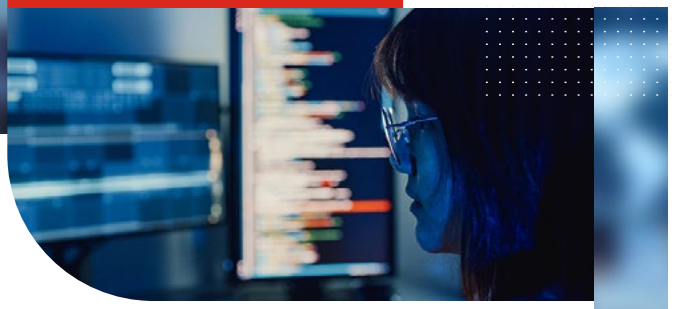
A secure future with quantum-safe readiness

With rapid advancements in quantum computing, it is predicted that today's encryption standards could be compromised sooner rather than later, prompting governments, industries, and regulatory bodies worldwide to prioritize quantum-safe encryption such as Post-Quantum Cryptography (PQC) as the new standard for data encryption. Fortinet is at the forefront of this quantum shift, shaping the future of cybersecurity to protect today's data from the potential threats posed by cybercriminals seeking to exploit advancements in quantum computing.

2024 marked a year of significant quantum-related innovation for Fortinet. The company enhanced its FortiOS operating system with NIST-approved post-quantum cryptography capabilities, providing organizations with robust protection for VPN connections against potential quantum computing threats.

Fortinet extended its commitment to quantum-safe computing through strategic collaborations with global leaders in 2024. In partnership with Singtel, Fortinet supported the upgrade of its cybersecurity infrastructure with a quantum-safe network powered by Fortinet. Fortinet also joined forces with SPTel, ST Engineering, and Nokia to launch quantum-safe services, demonstrating a collective effort to protect against future quantum threats. Additionally, Fortinet collaborated with Telefónica, Quantum Xchange, and Warpcom to unveil a quantum cybersecurity solution, further reinforcing its leadership in the field. Another significant achievement was Fortinet's contribution to Toshiba's efforts to advance quantum-safe encryption, marking an important milestone in the global push for secure quantum technologies.

500+
AI-related patents issued and pending



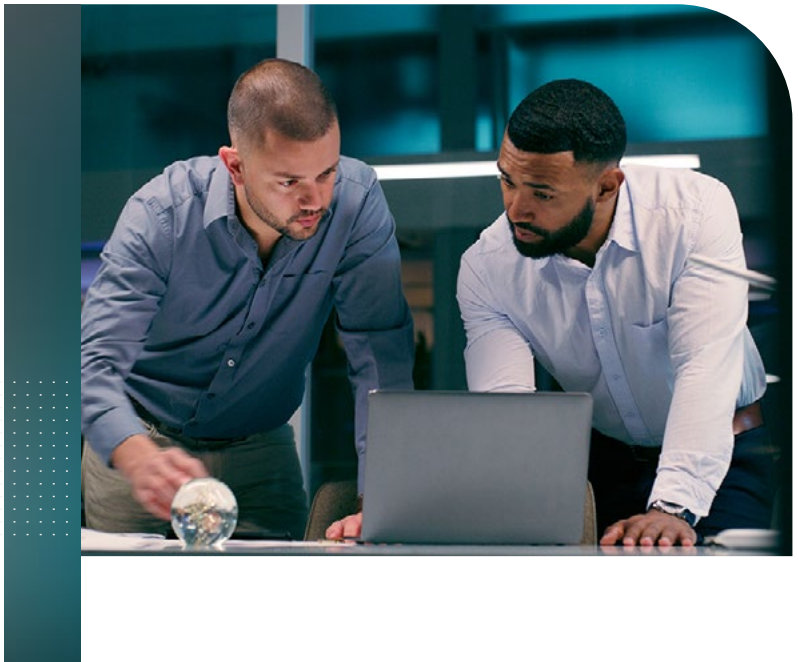
CYBERCRIME DISRUPTION

Fortinet is committed to proactively staying ahead of and defeating cybercrime. Dismantling cybercriminal organizations requires building strong, trusted relationships and collaborating globally with public and private entities. For over a decade, we have worked closely with international, regional, and national law enforcement agencies and cybersecurity companies, sharing actionable threat intelligence and providing expertise. These efforts not only help disrupt cybercriminal operations but also ensure accountability by supporting the identification and prosecution of cybercriminals. By working together with global partners, we help drive effective investigations and prevent future cybercrime.

FORTIGUARD LABS

Founded in 2002, FortiGuard Labs is Fortinet's elite cybersecurity threat intelligence and research organization. A pioneer in the field and security industry innovator, FortiGuard Labs develops and uses machine learning and AI technologies to provide real-time protection and actionable threat intelligence.

Partnering with law enforcement agencies, government organizations, and security vendor alliances worldwide, FortiGuard is a driving force in ensuring the industry collaborates effectively to fight emerging global security risks.



FORTIGUARD LABS IN NUMBERS

Trillions
of events processed daily

Millions
of Fortinet devices and sensors globally

Hundreds
of issued patents from FortiGuard Labs

500+
experienced threat hunters, researchers, analysts, engineers, and data scientists

52
Threat signals issued in 2024

28
Outbreak alerts issued in 2024

Derek Manky
Chief Security Strategist & Global VP Threat Intelligence and Member of the CSR Committee at Fortinet

« When faced with an increasing number of cyberattacks, many organizations think about adding more security tools. While important, building alliances is just as critical—yet frequently disregarded. Cybercriminals excel at working together, creating a profitable ecosystem with models like Ransomware-as-a-Service. They're constantly exploiting weaknesses in organizations and critical infrastructures, which means we need to work together to disrupt their operations at scale. This is where partnerships and trust come in. When public and private organizations build stronger relationships and share intelligence, we can drive real impact by mapping threat actor activities and creating a chain of disruption in the cybercriminal ecosystem. At Fortinet, we've been working with law enforcement agencies and peers for many years to hold cybercriminals accountable. This collective effort helps disrupt adversaries, preventing financial losses and mitigating risks—not just for businesses and organizations, but for society. »

A LONG HISTORY OF COLLABORATION

2006

Member of Microsoft's MAPP Zero-Day program, contributing to 1,020+ zero-day discoveries to strengthen infrastructure through responsible disclosure

2012

Member of FIRST, collaborating with CERTs globally. Fortinet contributed to the EPSS project and SIG launch (2020) to enhance security via dynamic risk evaluation and early warnings

2013

Partnership with MITRE. Fortinet contribution projects. STIX and TAXII 1.0 development before ratification

2014

Founding member of the CTA, a nonprofit uniting cybersecurity leaders to share threat intelligence and enhance global security

2015

Joined INTERPOL's Global Cybercrime Expert Group, aiding investigations and achieving a first arrest in 2016

2016

Partnership with NATO NCI Agency via NICP to share cyber threat intelligence and enhance national and regional security

2018

Joined INTERPOL Gateway, sharing FortiGuard Labs threat data weekly, responding to RFIs, and supporting Cyber Surge law enforcement training

2019

First cybersecurity founding partner of the WEF Centre for Cybersecurity

2020

Founding member of WEF PAC, fostering public-private threat sharing and contributing to the Partnership Against Cybercrime report on global cooperation

2021

Research partner with MITRE CTID. Fortinet contributed to:
- Sightings Ecosystem (2021): 353 techniques, 1.6M sightings in 198 countries (Aug 2021–Nov 2023)
- Attack Flow I & II (2022)
- ATT&CK Workbench, Summitting the Pyramid (2023)
- Sightings Ecosystem II, Summiting the Pyramid II, and Technique Inference Engine (2024)

2023

- Founding grantor of the PAC Cybercrime Atlas project
- Partnership with UC Berkeley CLTC contributing to Cybersecurity Futures 2030
- Joined Cyber Defense Collaborative (JCDC), contributing to OSS initiative

2024

Key contributor to
- the operationalization of the WEF Cybercrime Atlas
- INTERPOL in Operation Serengeti
- the UC Berkeley AI-Enabled Cybercrime initiative

KEY CONTRIBUTIONS IN 2024

MITRE ENGENUITY
A Foundation for Public Good

Global threat-informed defense with MITRE Engenuity Center for Threat-Informed Defense

As a MITRE Engenuity CTID research partner, Fortinet was a key contributor to three major open-source projects in 2024, driving progress across the industry: Sightings Ecosystem II, Summiting the Pyramid II, and Technique Inference Engine.

- Sightings Ecosystem II provides cyber defenders with visibility into adversary behaviors with a comprehensive database of observed attack techniques to enhance threat detection, improve defense strategies, and strengthen global cybersecurity.
- Summiting the Pyramid develops cyber analytics to counter evolving attack techniques and improve resilience. The second phase of the project, Summiting the Pyramid II, enhances scoring methodologies, reduces false positives, and expands to network-based analytics.
- The Technique Inference Engine is a machine-learning-powered tool that infers unseen adversary techniques, providing security teams with actionable intelligence. This helps analysts quickly understand what is likely to happen next based on a broad corpus of threat intelligence.

INTERPOL

International cybercrime collaboration with INTERPOL

Fortinet has been a trusted partner to INTERPOL since 2015 and an INTERPOL Gateway partner since 2018, contributing to global cybercrime efforts. In 2024, we assisted INTERPOL in Operation Serengeti, targeting cybercriminals behind ransomware, business email compromise, digital extortion, and online scams in 19 African countries.

The operation also uncovered fraud schemes, including:

- The arrest of eight individuals in Senegal for running an online Ponzi scheme affecting over 1,800 victims and causing $6 million in losses.
- The dismantling of a multi-level marketing scam in Cameroon, where victims were held captive and forced to recruit others.
- The resolution of a large-scale online credit card fraud campaign in Kenya.

Along with six other private-sector partners, Fortinet's FortiGuard Labs provided actionable threat intelligence, helping identify malicious actors and supporting investigations to disrupt cybercrime activities. Learn more.

THIS OPERATION LED TO

1,006
suspects arrested

35,000+
victims identified

134,000+
malicious infrastructures and networks dismantled

$44M
in recovered losses (out of $193M)

« Operation Serengeti shows what we can achieve by working together, and these arrests alone will save countless potential future victims from real personal and financial pain. We know that this is just the tip of the iceberg, which is why we will continue targeting these criminal groups worldwide. »

Valdecy Urquiza
Secretary General of INTERPOL

Proactive threat information sharing through Cyber Threat Alliance

In 2014, Fortinet was a founding member of the Cyber Threat Alliance (CTA), an independent NGO comprising cybersecurity providers and practitioners dedicated to sharing critical threat intelligence and raising the level of security for organizations globally. Through the CTA, we participate in an "early share" program, which enables members to share critical defensive information about cybersecurity threats before making it public. Members can use this information to develop controls and implement more timely and coordinated responses, enhancing network resiliency. In 2024, the program resulted in 207 early shares, including 35 by Fortinet. The CTA also shared more than 483,000 observables per day, on average. In addition, in 2024, Fortinet played a key role in developing the CTA Responsible Vulnerability Communication Code of Ethics, which outlines best practices for ethical vulnerability disclosure and aims to set a new industry standard for responsible communication and collaboration in addressing cybersecurity vulnerabilities.

Our role with the World Economic Forum

Fortinet has a long-standing collaboration with the WEF on cybersecurity issues. As the first cybersecurity founding partner of the WEF Centre for Cybersecurity, established in 2018, we work alongside private and public organizations, academia, and law enforcement to share critical insights and address both current and emerging cyber risks. We are also a founding member of the WEF Partnership Against Cybercrime, which fosters trusted public-private sector threat sharing. Additionally, as a founding partner of the Cybercrime Atlas project (see box), we support global efforts to collect and share threat intelligence, generate policy recommendations, and identify opportunities for coordinated action to combat cybercrime worldwide.

Highlights of our collaboration with the WEF in 2024:

- Launched the Cybercrime Atlas: Impact Report 2024 including highlights from the project's first year.
- Supported two cross-border operation campaigns, delivered seven research packages, and mapped 10,000+ actionable data points on cybercrime actors and their infrastructure.
- Joined the WEF AI and Cyber Initiative, aiming to guide organizations in managing cyber risks related to AI adoption.
- Contributed to key WEF initiatives, including the Disrupting Cybercrime Networks: A Collaboration Framework (outlining effective partnerships and intelligence-sharing recommendations), the Global Cybersecurity Outlook 2025 (analyzing cybersecurity trends and their economic and societal impact), and the Strategic Cybersecurity Talent Framework (addressing global talent development).
- Contributed to the global CISO Community and participated at the 2024 WEF Annual Meeting and Annual Meeting on Cybersecurity.

Derek Manky (Fortinet), Edvardas Sileris (Europol EC3 Head), Samantha Kight (GSMA Head of Industry), Craig Rice (Cyber Defence Alliance CEO), Jürgen Stock (INTERPOL, Former Secretary General)

CYBERCRIME ATLAS PROJECT: THE YEAR IN REVIEW

The WEF published the Cybercrime Atlas: Impact Report 2024, highlighting the progress of this initiative since its launch in January 2023. The Cybercrime Atlas is a collaborative, action-oriented global knowledge base designed to mitigate and disrupt cybercrime at scale. Building on the expertise of the WEF's Partnership Against Cybercrime, it provides a comprehensive view of the cybercrime landscape, detailing criminal operations, shared infrastructure, and networks to help law enforcement and government agencies take down cybercriminals worldwide.

In 2024, Cybercrime Atlas contributors, including Fortinet, shared more than 10,000 community-vetted and actionable data points, created seven comprehensive intelligence packages on emerging threats for broad distribution, and supported two cross-border cybercrime disruption efforts.

CUSTOMER SUCCESS

Fortinet is committed to delivering trusted, high-quality service, accessibility, and expertise to help customers maximize the value of our products and strengthen their security posture. Working closely with our global network of partners, we provide robust capabilities, extensive coverage, and continually enhance support options to meet customers' needs and support their success.

GLOBAL COVERAGE

Fortinet offers 24×7 support through its 25 global support centers, providing expert assistance to 100% of the countries where our products can be purchased. We can ship spare parts wherever our products are deployed, providing industry-leading coverage for time-sensitive deliveries. Detailed service options by country are available on our Global Service Availability page.

Our extensive partner network further enhances this service coverage, offering localized expertise and support. Customers can easily identify partners based on location, specialization, and services offered, using the Find a Partner page, ensuring tailored support and solutions to meet their unique needs.

SUPPORT CAPABILITIES

Fortinet prioritizes empowering customers at every stage of their 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 (RMA), 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 with advanced skill sets, we offer self-service options and access to a collaborative and active community to further enhance their knowledge and expertise.

24×7 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

KEY 2024 ACHIEVEMENTS

— **Fortinet Community:** The Fortinet Community fosters a collaborative environment for sharing insights and expertise about our products and services. In 2024:

- 140,000 members accessed 18,000+ knowledge articles, 94% of which were created or updated during the year.
- Members engaged actively with 27,000 forum replies and visited the platform 22.2 million times.
- A customer survey revealed that 73% of respondents found the information they needed.
- Fortinet was awarded 2024 Best Time to Value Community by the platform provider.

— **Customer deployment:** To accelerate customer success in the deployment phase, we expanded our consulting services and added several specific products to the QuickStart portfolio. This enables our customers to implement solutions more efficiently.

— **Fortinet Engage Partner program:** Through the Fortinet Engage Partner program, we provide certifications for Engage Tech Support Partners (ETSP) and Engage Preferred Service Partners (EPSP), recognizing their expertise in technical support and professional services, respectively. In 2024, certified partners increased by 74%, reaching 121 globally. We also hosted our first EMEA EPSP Summit to honor top partners, with plans to expand similar events to other geographies. Partner development was a priority, with 141 technical webinars delivered and training provided to over 2.789 individuals. Seven ETSP engineers participated in Fortinet Xperts Summit events in the EMEA and APAC regions.

CUSTOMER SATISFACTION

Fortinet continually monitors customer satisfaction through both transactional and quarterly customer satisfaction scores (CSAT). In 2024, our Technical Assistance Center (TAC) achieved a CSAT score of 9.4 out of 10.

We also 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 Network Security Expert (NSE) Certification program. Core product TAC members pursue Fortinet professional-level certifications, while senior-level and advanced support teams progress toward Fortinet expert-level certifications.

CSAT score of

9.4/10

RESPECTING THE ENVIRONMENT

The urgency to address climate change has never been greater, and every organization has a role in building a more sustainable future. As a global cybersecurity company with suppliers, operations, and customers worldwide, we are committed to understanding and minimizing our environmental impact across the value chain.

NEAR-TERM CLIMATE TARGETS
validated by SBTi

2024 HIGHLIGHTS

Through eco-friendly packaging

61%
average reduction in product energy consumption

~387
metric tons of CO_2e emissions avoided

~77
metric tons of plastic avoided

CLIMATE STRATEGY

We aspire to reach net zero GHG emissions by 2050 across our value chain (Scope 1, Scope 2, and Scope 3). Achieving this requires a deep understanding of our carbon footprint and a commitment to reducing emissions across our operations and broader value chain.

As a first step toward this goal, we developed near-term science-based emissions reduction targets, which were validated by the Science Based Targets initiative (SBTi) in 2024.

FORTINET'S PATH TO NET ZERO

Our decarbonization plan, developed in 2024, 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 to reduce their impacts, and designing and delivering more energy-efficient and circular products to help customers reduce their environmental impact while securing their digital transformation.

Fortinet decarbonization plan

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 2030

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 suppliers set science-based GHG emissions reduction 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 customers set science-based GHG emissions reduction targets by 2029

OUR NEAR-TERM EMISSIONS REDUCTION TARGETS VALIDATED BY THE SBTi

In 2024, we defined our near-term company-wide emissions reduction targets in line with the SBTi. SBTi is a corporate climate action organization that enables companies and financial institutions worldwide to play their part in combating the climate crisis. It develops standards, tools and guidance which allow companies to set greenhouse gas emissions reductions targets in line with what is needed to keep global heating below catastrophic levels and reach net-zero by 2050 at latest.

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, were validated by the 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. To achieve this, we are implementing advanced energy-efficiency measures and investing in renewable energy to decarbonize our operations.

Fortinet also 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. These targets are a first step toward reducing Scope 3 emissions, driving progress in our most significant Scope 3 categories: purchased goods and services and use of sold products.

SCIENCE BASED TARGETS
DRIVING AMBITIOUS CORPORATE CLIMATE ACTION

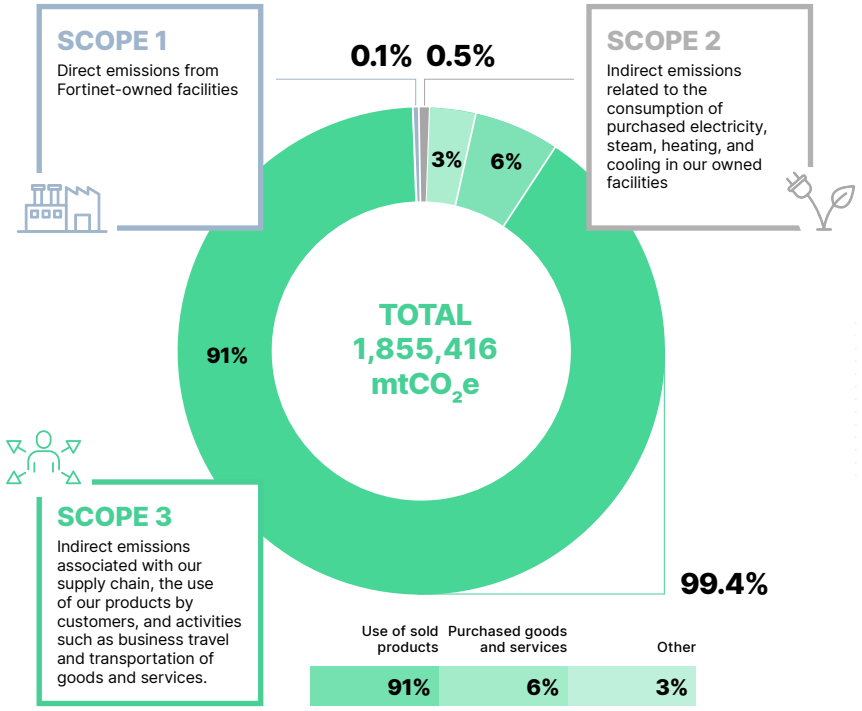
FORTINET 2024 CARBON FOOTPRINT

We inventory our GHG emissions annually to understand our performance and identify opportunities to reduce Fortinet's environmental impact. 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 categories.

Scope 1 and Scope 2 GHG emissions

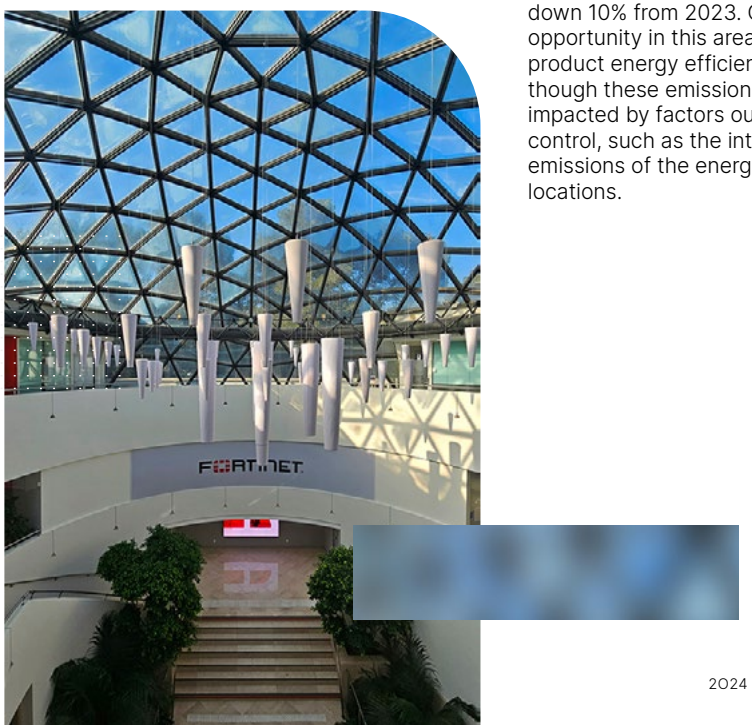
Scope 1 and location-based Scope 2 GHG emissions account for 0.6% of our total footprint. In 2024, Scope 1 emissions totaled 1,606 metric tons carbon dioxide equivalents (CO_2e), reflecting a 21% increase from 2023 and a 27% increase from 2021. This increase is attributed to the expansion of data center operations through new facilities and acquisitions. To address this growth, we have achieved 100% renewable power coverage through a combination of renewable energy sources and Renewable Energy Certificates (RECs).

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 GHG emissions is the electricity purchased for our facilities.

We're addressing Scope 1 and Scope 2 GHG emissions primarily through our energy strategy. Focus areas include improving energy efficiency in our facilities, generating renewable electricity on-site, purchasing renewable energy directly from utilities, and purchasing RECs. Our approach also involves reducing natural gas use and transitioning to low-emissions cooling technologies in our buildings and data centers. To offset the residual Scope 1 and 2 GHG emissions related to our owned sites, we purchase energy attribute certificates (EACs) in alignment with the rigorous technical criteria outlined in version 4.2 of RE100. See Energy for more details.



Scope 3 GHG emissions

Scope 3 GHG emissions include indirect emissions from upstream and downstream sources in our value chain. In line with the GHG Protocol, we identify and report Scope 3 GHG emissions in 11 categories relevant to our company. These represent over 99% of Fortinet's GHG emissions, underscoring the need for deep engagement across our value chain to achieve reductions.

Two categories are by far the most significant for Fortinet and represent the greatest opportunities to reduce our carbon footprint:

- Purchased goods and services (Category 1) accounted for 110,259 metric tons of CO_2e in 2024. Reducing GHG emissions related to purchased goods and services requires close collaboration with suppliers to decarbonize our supply chain.
- Use of sold products (Category 11) contributed 1,690,540 metric tons of CO_2e to our carbon footprint in 2024, down 10% from 2023. Our biggest opportunity in this area is to improve our product energy efficiency (learn more), though these emissions are also impacted by factors outside of our control, such as the intensity of the GHG emissions of the energy mix in different locations.

SUSTAINABLE OPERATIONS

Although our owned facilities represent only a small part of our environmental footprint, we have direct control over those impacts. 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.

Our efforts also focus on minimizing waste, particularly e-waste, through improved tracking and extending product life via our hardware donation program. Additionally, we promote sustainable practices and encourage a culture of environmental responsibility throughout our organization.

ENVIRONMENTAL MANAGEMENT IN OPERATIONS

In line with the Fortinet Environmental Policy, we are committed to reducing our environmental impact and improving our operations. We identify and control environmental impacts related to energy, water, and waste. We continually improve our performance through a comprehensive environmental management system, certified to ISO 14001, which covers our largest owned warehouse and overflow warehouse in Union City, California. As part of this effort, we provided ISO 14001, e-waste, and environment, health and safety training to management and employees at the Union City site. Fortinet's ongoing commitment to the environment extends to its owned warehouses and subsidiaries, with 2 locations currently ISO 14001 certified. Beyond certifications, we continue to broaden our environmental programs and disclosures. In 2024, Fortinet furthered its transparency efforts by making its first submission to the CDP Water Security questionnaire.

GREEN BUILDINGS

Fortinet's green guidelines for its data centers and offices, based on the LEED and BREEAM green building rating systems, 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 while identifying opportunities for continuous facility improvement.

Examples of Fortinet buildings with strong environmental features include:

- **Sunnyvale, California, United States:** LEED GOLD certified, powered entirely by renewable electricity, with 30% less energy consumed than a standard building. Solar panels on the parking garage and the HQ campus generate renewable energy used to power the campus. At the same time, the site's drought-tolerant landscaping helped conserve over 280 cubic meters of water in 2024.
- **Sydney, Australia:** 4-Star Green Star rating with solar panels generating 9% of electricity annually, and the site sources 100% renewable energy for its remaining energy needs from the utility. The facility also uses recycled furnishings from non-Fortinet buildings and First Nations suppliers.
- **Madrid, Spain:** B-rated low-carbon emission data center, equipped with photovoltaic panels for on-site renewable energy, and Indirect Air Coolers (IAC) for efficient heat exchange. This site has achieved a Power Usage Effectiveness (PUE) of 1.1, with only 10% of energy used for cooling.

SUSTAINABLE OPERATIONS

ENERGY

Energy consumption is a key driver of GHG emissions in our facilities and represents a significant operational cost. We focus on improving energy efficiency and transitioning to lower-impact energy sources. In 2024, we formed an energy strategy sub-committee within the CSR Committee to guide and oversee these efforts. This group comprises Fortinet experts from operations, global real estate, CSR, facilities, and our energy broker.

In 2024, our owned facilities consumed 210,853 gigajoules (GJ) of energy, a 16% increase in usage per square foot compared to 2023, driven primarily by new data centers, in Piano (Texas) and Madrid (Spain).

Of this, 186,168 GJ—88.3% of our energy consumption—were sourced from renewable energy. The remaining usage was offset through the purchase of RECs. Sixty-five percent of our owned sites by square footage used 100% renewable electricity, including all facilities in California, Spain, and France.

With RECs, 100% of our owned sites achieved 100% renewable electricity usage. Throughout the year, we focused on ensuring access to renewable electricity for newly owned sites and leased data centers, adhering to Fortinet's Green Guidelines for site sourcing.

To continually expand the use of renewable electricity as we grow, we partnered in 2024 with a global energy broker that assists us in procuring all forms of renewable energy, from utility contracts to virtual power purchase agreements.

We are also decreasing our reliance on natural gas. In 2024, 62% of Fortinet's owned and occupied sites did not consume any natural gas.

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. We comply with global and regional waste management regulations and are committed to minimizing the generation of both non-hazardous and hazardous waste. Our ISO 14001-certified environmental management system covers all waste management. The only hazardous waste in our operations is universal waste (such as light bulbs, e-waste, and small amounts of chemicals like cleaners). These waste items are properly disposed of or recycled by qualified recyclers, in accordance with local environmental regulations.

Fortinet has been taking steps to improve waste tracking and continued its progress on waste reduction in 2024, with a particular focus on e-waste. We formalized our hardware donation program, collaborating with other organizations to provide select equipment for a second life, creating social value while reducing the environmental impact of our products. Learn more.

GOAL

Achieve

100%

renewable energy use across all owned Fortinet sites by 2030

*Some of the remaining sites use a combination of renewable and non-renewable electricity.

ELECTRICITY REDUCTION AT FORTINET TECHNICAL ASSISTANCE CENTERS LAB

In 2024, the Customer Support and Services team at our Sophia Antipolis office in France added a power-saving feature to their lab automation software. This new feature automatically powers down eligible equipment in the TAC lab every Friday evening, with devices only being powered up again by users when needed.

This simple yet effective solution reduced the lab's electricity consumption by approximately 40%, cutting overall site electricity use by 18%. It also lowered site-related GHG emissions by an estimated 40 metric tons of CO_2e annually while achieving cost savings of over €200,000 each year. To expand on these savings, we are implementing similar energy-saving measures across other Fortinet TAC labs worldwide.

EMPLOYEE AWARENESS AND ENGAGEMENT

Environmental sustainability has become increasingly important to our employees. We are committed to raising awareness internally while empowering everyone with the knowledge to engage in sustainability and take positive action.

We help employees expand their knowledge in the following ways:

- **Sustainability e-learning:** We have developed a series of e-learning modules on topics such as sustainability at Fortinet, product environmental impacts and ecolabels, to deepen employee knowledge and improve their ability to discuss sustainability with colleagues, prospects and customers. Beginning in 2024, we integrated these modules into Fortinet's onboarding trainings.
- **Company-wide awareness campaigns:** We conduct periodic awareness campaigns to educate Fortinet employees about critical environmental topics and events that impact Fortinet, our customers, and our communities. In 2024, campaigns focused on World Environment Day and plastics reduction.
- **Sustainability monthly digest:** Our monthly newsletter, available to all employees worldwide, summarizes Fortinet sustainability highlights, sustainability news headlines, various sustainability-related tools, and other information.

300
electronic goods donated to Emmaüs Connect

70
metric tons of CO_2e emissions prevented by this donation

FORTINET'S EMPLOYEE-LED SUSTAINABILITY ACTION TO SUPPORT DIGITAL INCLUSION

Initiated in 2023 by Fortinet's IT, CSR, and purchasing teams based in France, Fortinet donated over 300 used laptops and smartphones to Emmaüs Connect, an NGO that helps economically vulnerable individuals by providing access to technology, training, and support. This donation helped prevent approximately 70 metric tons of CO_2e emissions. Building on this success, IT teams worldwide implemented similar initiatives in 2024. For example, in the USA, over 100 laptops were donated to a locally based NGO to support educational programs, helping students and adults learn essential computer skills. In India, 50 laptops were donated to the United Way Bengaluru NGO to support flood-impacted students in Wayanad.

RESPONSIBLE EVENTS

Following a series of workshops about designing responsible events with global and regional event teams at Fortinet, we created educational materials in 2024 to support this initiative, including a checklist and best practices guide. We began implementing some of these practices with the EMEA marketing organization, focusing on hosting paper-free events and prioritizing the reuse or upcycling of event materials. We also work to reduce food waste by ensuring venues have food donation programs and offering seasonal, locally sourced menus with refilled buffets only as needed. We limit giveaways to high-use items made from at least 70% recycled materials and collect lanyards and badges for recycling at event's end.

PRODUCT ENVIRONMENTAL IMPACTS

With over 830,000 customers worldwide and more than 13.7 million appliances shipped in 2024, our products' environmental impact represents the majority of our carbon footprint. Product energy efficiency has always been a key focus at Fortinet, but we understand that our products' environmental impact goes beyond GHG emissions. For this reason, we focus on reducing our products' broader environmental impacts across their lifecycles.

ECO-DESIGN

The design phase largely determines the environmental impact of a product or service, so we work to consider sustainability from the early stages of product development. Fortinet complies with globally recognized product environmental regulations to ensure the responsible use of materials (see Product regulatory environmental compliance). Our commitment goes beyond compliance: we also strive to incorporate sustainable materials into product design.

We understand that using recycled, renewable, and low-carbon-emission materials in our products and packaging is integral to fostering a circular economy and mitigating the environmental impacts associated with typical hardware manufacturing. We also consider how design impacts energy efficiency in the use phase as well as factors that affect product lifespan, such as durability, repairability, and ease of disassembly.

Increasing our employees' understanding of sustainability and circularity is fundamental to designing and delivering products and packaging with reduced environmental impacts. In recent years, we have engaged our teams to deepen their knowledge in these areas and empower them to implement new ideas.

In 2024, we built on these efforts by collaborating with external subject matter experts to create and deliver circular economy workshops to employees in R&D, product management, and operations. These workshops explored key regulatory and other trends shaping the U.S. and EU markets, including the EU's new Circular Economy Action Plan and its Ecodesign for Sustainable Products Regulation, which emphasizes sustainability and eco-design principles. We assessed how sector-related requirements, such as implementing digital product passports and the need for product lifecycle transparency, impact Fortinet. We also envisioned how the company's value chain strategy might evolve to align with a circular economy, focusing on repurposing products and components to minimize waste. Lastly, we analyzed how these trends might impact product and service design, inventory management, and the integration of circularity principles throughout our operations.

SUPPLIER ENGAGEMENT

Engaging our suppliers is crucial to reducing emissions associated with the manufacturing of our products. We are prioritizing emission reductions within our supply chain and from the use of our products. A key first step is ensuring that our suppliers are equally committed to emission reductions and transparent tracking of their progress. For this reason, we have set a near-term target approved by the SBTi to have at least 60% of our suppliers—by spend—set public and science-based GHG emissions reduction targets by 2029.

LIFECYCLE ASSESSMENT

In 2024, Fortinet completed a full lifecycle assessment of the FortiGate 40F firewall appliance, aligned with ISO 14040, 14067, and 14044 standards. This analysis provided actionable insights into the product's environmental impact throughout its lifecycle, including raw materials, upstream production, manufacturing, distribution, product use, and end-of-life. The findings will serve as the foundation for developing an environmental product declaration for the FortiGate 40F, providing transparent environmental data to help customers make more informed and sustainable decisions.

SUSTAINABLE PACKAGING

Product packaging is another focus area. We recognize that packaging typically becomes waste once our products reach the customer. Our goal is to design packaging that not only protects our products during transportation but also optimizes materials use and space efficiency.

We strive to minimize unnecessary packaging and prioritize materials that are reusable, easily recyclable, or environmentally friendly. In 2024, we created 22 new models of product packaging with a variety of renewable materials, including corrugate paper. All of these new packaging models are certified by the Forest Stewardship Council® (FSC).

Wherever possible, we eliminate plastic from our packaging. For example, we have designed dedicated compartments for antennas and other accessories in our packaging, reducing or eliminating the need for plastic bags. In 2024, 86 models of our top-selling product lines were designed with eco-friendly packaging. Through eco-friendly packaging manufactured in 2024, we avoided approximately 387.5 metric tons of CO_2e emissions, primarily by removing an estimated 77.5 metric tons of plastics.

Building on the success of a 2023 pilot, we expanded a packaging initiative in 2024, replacing polyethylene foam with Korrvu®/SealedAir for many refurbished products shipped through our return merchandise authorization (RMA) service. Korrvu®/SealedAir provides superior protection with a resilient low-slip film that helps prevent damage from shock, vibration, and scratches during shipping. Its space-efficient design reduces packaging inventory. Environmentally, it removes up to 90% plastic, is easily recyclable, and can be reused for return shipments.

It is also easy to use, with quick assembly and flexibility to integrate into packaging lines. The Korrvu®/SealedAir will contribute to saving approximately 28 metric tons of CO_2e emissions annually and eliminating an estimated 5.7 metric tons of plastics.

ECO-FRIENDLY PACKAGING IN 2024

86
models of Fortinet's top-selling product lines designed with eco-friendly packaging

~387
metric tons of CO_2e emissions avoided through eco-friendly packaging manufactured

~77
metric tons of plastic removed from product packaging

22
product packaging models certified by the Forest Stewardship Council® (FSC)

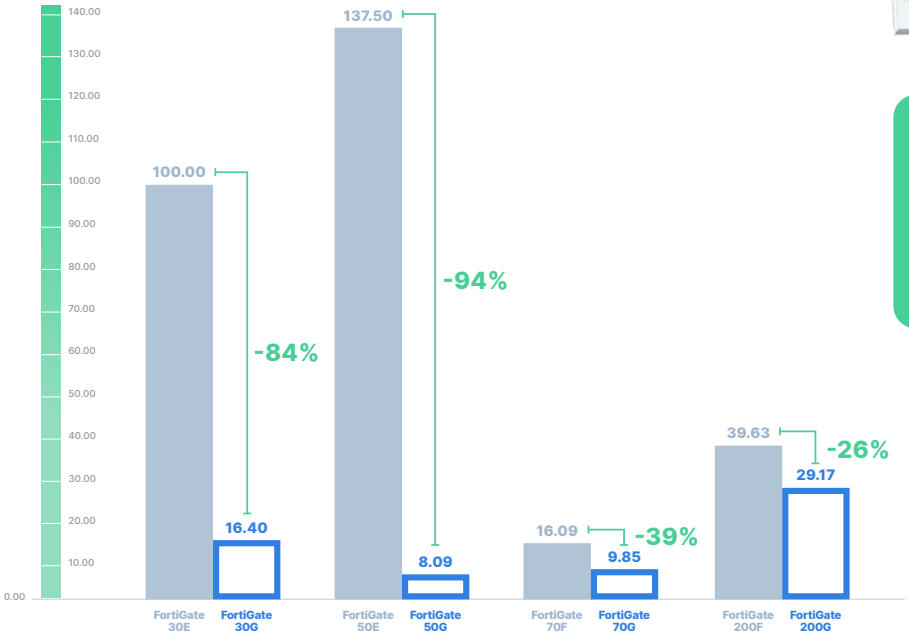
PRODUCT ENERGY EFFICIENCY

The energy consumed by our products in use is by far the main contributor to Fortinet's GHG emissions across our value chain. Since the company's inception, we have prioritized consolidating multiple functions into a single platform to reduce power, cooling, and space, helping customers minimize energy consumption and GHG emissions.

The Fortinet R&D team is dedicated to improving the energy efficiency of our products. It works hard to ensure that each new generation of Fortinet products uses less energy, space, and cooling than its predecessors. Reducing product energy intensity while maximizing performance is critical to supporting our customers and helping them meet their climate goals. Although the U.S. Environmental Protection Agency (EPA) ENERGY STAR program doesn't currently include a cybersecurity category, the EPA accepted our proposal in 2024 to create that category in the coming years, and we are collaborating on that effort.

In 2024, we also continued to push the boundaries of energy efficiency by delivering maximum performance per watt, enabling our customers to consolidate their IT equipment and reduce energy and cooling needs. Our new products launched in 2024—including the FortiGate 30G, FortiGate 50G, FortiGate 70G, and FortiGate 200G—consume 84%, 94%, 39%, and 26% less power, respectively, than prior generation products. The FortiGate 200G is four times as energy efficient as the industry average.

FortiGate power consumption per throughput (Watts Max/Gbps)
New products launched in 2024 compared to prior generation products

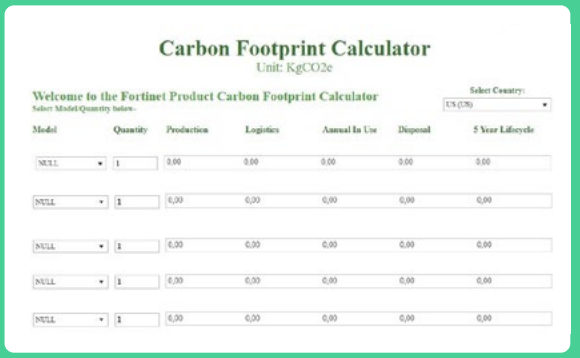


61%
average reduction in product energy consumption

** Based on comparison with equivalent product models from the previous generation.*

FORTINET CARBON FOOTPRINT CALCULATOR

Many Fortinet customers share our focus on reducing GHG emissions, including from their own operations and IT suppliers. The Fortinet carbon footprint calculator provides the carbon footprint of our products to support our customers' decision-making related to sustainability. This online tool, available exclusively to Fortinet employees, provides the carbon footprint of selected products across the lifecycle, based on the country of use. The methodology for GHG emissions from product use has been verified by third-party TÜV SÜD America and complies with the GHG Protocol. In 2024, Fortinet added about 300 new models to the calculator, for a total of more than 570 models in 56 countries.



CIRCULARITY

We are committed to embracing circular economy practices that increase repair and reconditioning, extend product lifespans, and enhance materials recycling. This requires strong collaboration with customers, suppliers, and partners to identify and implement best practices for reusing and recycling our solutions.

We've also implemented an internal refurbishing pilot program to return unused evaluation units for free and include them in a circular process for reuse. In 2024, 14,953 products were returned through this process, 22% more than the prior year. Over 88% of these units were successfully repaired for reuse. This program is now available in more than 30 countries.

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, it is our responsibility to minimize the environmental impact of our products. To ensure compliance with all new and evolving regulations, we continually monitor global legislative developments through multiple sources of information, such as BOMcheck, the ECHA, the SGS, and the Green Soft Technologies.
We regularly review and update policies, procedures, and reporting templates to adapt to changing requirements and ensure ongoing compliance with all current regulatory requirements.

Our Design for Compliance (DfC) approach integrates environmental considerations into our product development process. Fortinet compiles all applicable directives and regulations into its Restricted & Declarable Substances List, which serves as a key reference for our design teams and contract manufacturers to proactively address compliance requirements.

Fortinet's products comply with all applicable regulatory environmental directives and regulations worldwide. In addition, Fortinet complies with the Waste Framework Directive (WFD) by submitting its data to relevant databases and facilitating the proper disposal and recycling of its products.

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 Packaging Directive 94/62/EC as amended by EU Directive 2018/852

Waste management

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

FORTINET INTERNAL REFURBISHING PILOT PROGRAM

14,953
units returned

88%
success rate on return repair

GIVING A SECOND LIFE TO OUR PRODUCTS THROUGH DONATIONS

In 2024, we formalized our hardware donation program to repurpose some Fortinet products that would otherwise be recycled. Through this program, we donate excess inventory or repurposed equipment from our internal refurbishing pilot to NGOs and educational institutions, where it can support their missions and programs.

For example, in 2024, we donated excess equipment to Simon Fraser University in Canada and San José State University in California. These donations were used to build hands-on learning labs, helping students gain practical cybersecurity experience using Fortinet products.

We also donated repurposed FortiAP access points to the French NGO Laurette Fugain, which supports children with leukemia and blood cancers. These previously used devices, which underwent rigorous testing, wiping and software updates, were deployed in schools to facilitate the connection of medical monitoring machines for children undergoing treatment.

GROWING AN INCLUSIVE CYBERSECURITY WORKFORCE

Developing and maintaining strong cyber awareness, skills, and expertise is vital to ensuring a secure, reliable, and sustainable digital future. This challenge is too vast for any single organization, government, or individual to address alone—it requires collective action and collaboration.
Closing the cybersecurity skills gap and fostering greater diversity in the workforce are essential to strengthening defenses against the evolving threat landscape.
At Fortinet, we are committed to making a measurable global impact by empowering a broad and diverse range of individuals with the knowledge and skills needed.
By fostering an inclusive and diverse workforce both within Fortinet and across the broader cybersecurity industry, we aim to help people reach their full potential while shaping a safer, more secure digital world for all.

Cybersecurity skills pledges

1 million
people trained in cybersecurity globally (2022-2026)

New pledge
75,000
individuals trained in cybersecurity in the European Union (2024-2027)

2024 HIGHLIGHTS

630,859
people trained in cybersecurity since 2022

Joined Cybersecurity Skills Academy

6
recognitions as one of the best places to work

INCLUSION AND BELONGING IN OUR WORKFORCE

With more than 14,000 employees in over 100 countries, Fortinet is enriched by rich perspectives, backgrounds, and experiences of its global workforce. This diversity fuels our innovation and is a cornerstone of our success. We are committed to fostering an environment where everyone feels valued, empowered, and equipped to thrive.

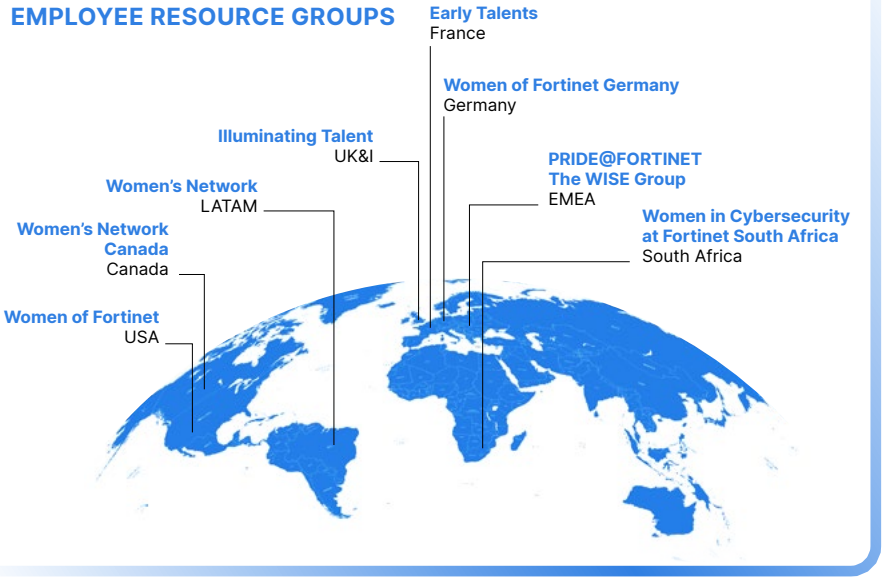
INCLUSIVE WORKPLACE

Our core values—Teamwork, Innovation, Openness—define who we are, how we work, and what we do. At the heart of it all are our people, who are essential to Fortinet's long-term success. These values also guide our efforts to foster a workplace where employees feel connected, engaged, and supported from day one. We focus on building connections through employee resource groups (ERGs), offering ongoing training and resources to empower our team members and encourage them to contribute to positively impact their communities.

Opportunities for employees' connection

At Fortinet, we encourage employees to connect and engage through our ERGs and initiatives led by Fortinet diversity ambassadors and allies.

EMPLOYEE RESOURCE GROUPS



RECOGNITIONS IN 2024

BEST PLACES TO WORK 2024 "GLASSDOOR"

Great Place To Work. Certificada Abr/2024 - Abr/2025 BRASIL

Great Place To Work. Certificada MAY 2024-MAY 2025 COL

Los Mejores Lugares para Trabajar™ para Mujeres Great Place To Work. COLOMBIA 2024

Great Place To Work. Certificada NOV 2024-NOV 2025 México

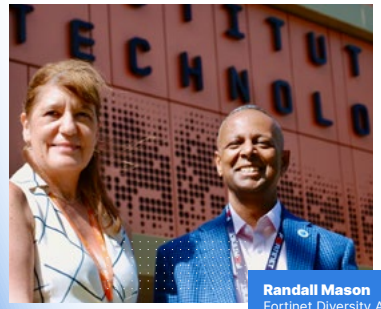
Los Mejores Lugares para Trabajar™ para Mujeres Great Place To Work. MÉXICO 2024

Employee Resource Groups

Fortinet's ERGs, founded and led by employees, promote inclusion and foster a sense of belonging by building supportive communities within the workplace. Employees are encouraged to join ERGs—regardless of their background and interests—to broaden awareness and develop relationships with colleagues from diverse perspectives and experiences.

In 2024, we launched four new ERGs—Women's Network Canada, Women in Cybersecurity at Fortinet South Africa, Women of Fortinet Germany, and WISE Group (Women in Systems Engineering and Consulting Systems Engineering). Through regular meetings and events, these groups create spaces for sharing experiences, learning from one another, and raising awareness about the unique opportunities and challenges in cybersecurity.

INCLUSION AND BELONGING IN OUR WORKFORCE



Randall Mason
Fortinet Diversity Ally

« I am passionate about inspiring interest in cybersecurity and STEAM (Science, Technology, Engineering, Arts, and Mathematics) for learners of all ages, from 11-year-old students to a 55-year-old person who wishes to learn new skills. In 2024, we hosted several events, like our Cyber Games, designed by our Systems Engineering team to teach online safety in an engaging way. These games include a Capture-the-Flag challenge, where students solve hacking puzzles, and a Digital Autopsy game, where they decrypt a cybercriminal's laptop to uncover evidence. »

Fortinet diversity ambassadors and allies

Fortinet diversity ambassadors and allies amplify efforts to strengthen Fortinet's inclusive workplace culture. In 2024, the group consisted of six ambassadors and 12 allies from different business units and seniority levels across the EMEA region. These employees serve as role models who inspire, mentor, and empower others within Fortinet and the broader community.

Employee awareness

In 2024, we recognized key global awareness events—International Women's Day, Pride Month, World Mental Health Day, and the International Day of Persons with Disabilities—as opportunities to reflect and foster an inclusive workplace. Through global initiatives, regional events, and educational resources, we encouraged engagement, learning, and inspiration among our team members worldwide.

Learning programs and training

In 2024, we enhanced our internal development programs to empower our leaders with the skills and knowledge needed to champion inclusion. This included integrating content focused on fostering inclusivity into our flagship Leadership Signature Programs and hosting a series of webinars.

Our Fundamentals e-learning introduces core concepts related to inclusive workplace to Fortinet's people managers globally and became a key development opportunity in 2024, with 82% completing it by year-end. This course provides foundational knowledge on recognizing unconscious bias and leveraging diverse perspectives to enhance innovation and teamwork.

We also expanded our Inclusive Leadership Workshops globally, reaching 81 leaders across the organization. Building on the success of last year's pilot, this interactive workshop helps leaders identify personal biases, and provides practical strategies to enhance psychological safety within teams and foster a culture of inclusion.

WELLNESS

We are committed to supporting the wellness of our workforce globally through programs designed to promote physical, mental, and emotional well-being. Fortinet's Wellness Assistance Program aims to help employees balance their personal and professional responsibilities. The program provides employees, their families, and their partners with access to resources and counseling on a wide range of topics, such as improving relationships, managing stress and life changes, coping with loss, building confidence, and navigating workplace challenges. Available 24×7, 365 days a year, this confidential service is available in more than 100 languages and at no cost to employees.

Employee community engagement

Supporting a sense of community and belonging goes beyond the workplace. We encourage our employees to give back by matching donations to eligible non-profit organizations—up to $1,000 per employee annually— and by volunteering to contribute to community projects.

Highlights of employee-led community projects in 2024

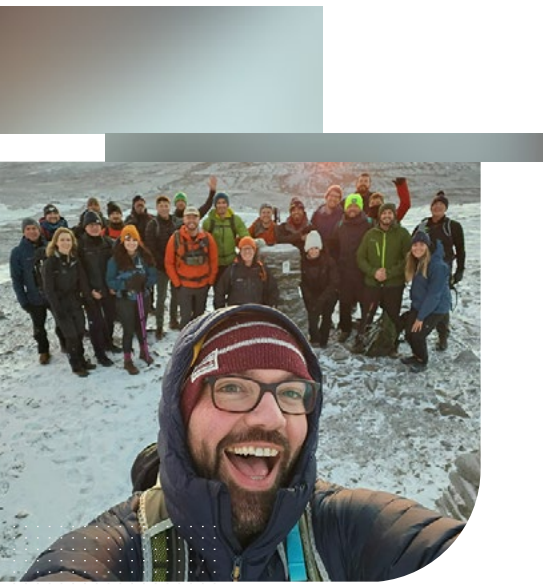
- **Brazil:** In partnership with Paróquia Nossa Senhora do Rosário de Fátima in São Bernardo do Campo, our employees brought joy to 80 children aged 0-12 in vulnerable situations. By donating clothing, footwear, and toys, the team helped create a memorable and festive holiday season.
- **Canada:** Throughout the year, over 100 employees contributed to HR-organized donation drives to support a variety of NGOs, including the BC Cancer Foundation, Qmunity (a queer, trans, and two-spirit resource center), MOSAIC (settlement and employment services), BC Mental Health Foundation, and Dixon Transition Society (supporting women and children impacted by domestic violence).
- **Colombia:** Our team supported the Contributing to a Promising Future initiative with the Surcos Foundation, which assists girls and adolescents in vulnerable situations. Volunteers donated hygiene kits to over 60 girls aged 10-18 and conducted a cybersecurity awareness session, equipping them with knowledge to safely navigate the digital world.
- **France:** Employees came together to support Les Restos du Cœur, an NGO dedicated to providing food and hot meals to homeless people and those in need. In total, 63 kg of nonperishable food items were collected for distribution.
- **India:** Employees supported multiple NGO projects by providing education and community development resources. Their contributions ranged from funding education scholarships to providing nutritious meals, safe drinking water, and digital infrastructure for individuals with disabilities, improving the quality of life and promoting inclusion across various communities.
- **South Africa:** Employees led two fundraisers to support underprivileged children during the holiday season. In Cape Town, they partnered with Tomorrow Trust to provide Santa Magic Boxes for 8-year-old students. In Johannesburg, they collaborated with the NGO Santa Shoebox Project to provide Virtual Santa Shoeboxes. Through these initiatives, 55 children received boxes filled with clothing, toiletries, school supplies, sweets, and toys to brighten Christmas.
- **UK&I:** Our employees supported several initiatives throughout the year. Through the UK&I Channel Charity Initiative, they helped raise £40,555 for Sands, an NGO supporting those affected by baby loss, with activities like a marathon walk and a 300-mile cycling challenge. They also partnered with The Felix Project, preparing and distributing 4,900 hot meals for individuals and families in need.
- **United States:** In Florida, our team volunteered at the Broward Outreach Center in Hollywood, serving Thanksgiving dinner to individuals and families facing challenges such as poverty, unemployment, addiction, domestic violence, and health issues.

SKILLED AND INCLUSIVE WORKFORCE

Attracting, developing, and retaining a highly skilled workforce is key to innovation and success. We are committed to broadening our reach to engage individuals with various experiences, backgrounds, and perspectives—across age, professional and academic disciplines, as well as global and cultural viewpoints. Our efforts focus on sourcing talent through several pathways, hiring high-performing talents inclusively, and supporting individuals early in their careers. We are also committed to empowering all our employees by providing opportunities for growth, development, and learning.

Talent recruitment and hiring

We are committed to broadening our talent-sourcing strategies to attract individuals from different backgrounds, ensuring our workforce reflects a variety of perspectives and experiences to drive innovation and success.



Inclusive hiring practices

To strengthen representation across our workforce, our trained recruiters actively engage with a wide range of candidates. Leveraging AI-driven tool, we enhance our outreach, run tailored online campaigns, and improve employer branding to attract top talent. In 2024, we developed a global inclusive hiring framework to ensure fair, consistent and accessible recruitment processes, and prioritize an inclusive candidate experience.

Our recruitment efforts are supported by multiple channels to connect with talents, including targeted job fairs, internship programs to develop early-career talent, university partnerships to engage students from various academic disciplines, and collaborations with industry associations to reach underrepresented candidates.

The Early Talent program

Our Early Talent program offers internships and graduate roles in a variety of technical and non-technical roles. It is complemented by training, mentorship by seasoned Fortinet professionals, and exposure to our cybersecurity technology. In 2024, the six-month program in India enabled interns to earn Fortinet certifications including Fortinet Certified Fundamentals (FCF), Fortinet Certified Associate (FCA), and Fortinet Certified Professional (FCP). Interns gained hands-on experience, and some transitioned into full-time roles at Fortinet.

Leadership development

At Fortinet, we are committed to supporting both current and aspiring leaders by providing them with the tools and development opportunities needed to inspire and empower our employees while helping them thrive professionally.

Through Manage for Success, Fortinet's signature leadership development program, we equip managers worldwide with the knowledge and skills to be effective leaders. This program offers a well-rounded, forward-thinking approach to leadership development, covering topics such as change management, courageous conversations, inclusion, self-management, and strategic leadership. In 2024, 287 leaders in four cohorts completed the program.

Ignite Your Potential, another global program, builds and strengthens management foundations for emerging and new leaders. After completing a leadership self-assessment, participants focus on practices that are essential for leading a team. Graduates of Ignite Your Potential walk away with a leader's mindset and the ability to set others up for success and leading teams through change. In 2024, 143 leaders participated in this program.

In collaboration with various business functions, we also hosted nine leadership summits in 2024, bringing together 226 managers worldwide to enhance leadership skills and drive performance. We also offered a series of webinars for current and emerging managers globally, with 902 attendees, focusing on topics such as maximizing team potential and leading behavior change through feedback.

CYBERSECURITY SKILLS GAP

In an increasingly digital world where cyberattacks are growing in scale and sophistication, cybersecurity has become essential for safeguarding citizens and ensuring economic stability. All individuals have a role to play in staying cyber-aware to protect themselves and contribute to our collective safety. Cybersecurity professionals are essential to this effort. However, a significant talent shortage persists, with over 4.7 million unfilled cybersecurity jobs globally in 2024—a 19.1% increase from 2023[1]— making the skills gap an urgent priority that threatens global economic resilience.

As a leader in cybersecurity, Fortinet is committed to breaking down financial, geographic, and technological barriers to high-quality cybersecurity education. Through our Fortinet Training Institute, we provide industry-focused training on job roles, skills and best practices to close the skills gap and promote cyber awareness.

We work with cybersecurity professionals, educational institutions, NGOs, governments, policymakers, and partners to advance the industry and society by building a sustainable and diverse talent pipeline, upskilling and re-skilling today's workforce, and empowering individuals of all ages to stay safe online.

CYBERSECURITY SKILLS PLEDGES	FORTINET ON TRACK
1 million people trained in cybersecurity by 2026 (2022 base year)	630,859 people trained since 2022
75,000 individuals trained in cybersecurity in Europe (2024-2027)	63% of our 5-year goal

FORTINET CYBERSECURITY RESEARCH AND THE SKILLS GAP

In 2024, Fortinet released two key cybersecurity reports:

The 2024 Cybersecurity Skills Gap Global Research Report highlighted the top causes of breaches, including insufficient IT/security training (58%), lack of security awareness (56%), and inadequate cybersecurity products (54%). Nearly 90% of organizations experienced a breach in 2023, with 53% incurring costs exceeding $1 million. Seventy percent of IT leaders agreed the skills shortage increases organizational risk, particularly due to challenges in finding network security expertise.

The 2024 Security Awareness and Training Global Research Report emphasized the critical role of a cyber-aware workforce, with 67% of leaders expressing concerns over employee security awareness. A high 97% agreed that increased training could reduce cyberattacks.

2024 FORTINET TRAINING INSTITUTE AWARDS

SC Awards

WINNER: Best Professional Certification Program

Cybersecurity Breakthrough Awards

WINNER: Professional Certification Program of the Year

Cybersecurity Excellence Awards

WINNER: Cybersecurity Training
WINNER: Security Awareness Program

Global InfoSec Awards

MOST INNOVATIVE: Cybersecurity Training and Certification
MOST INNOVATIVE: Security Awareness and Training Service

Globee Awards

WINNER: Cybersecurity Education and Training
WINNER: Security Awareness & Training

1. According to 2024 ISC2 Cybersecurity Workforce Study, https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study.

INDUSTRY ADVANCEMENT THROUGH PARTNERSHIPS

Fortinet is committed to advancing global cybersecurity training and education by working with a diverse network of stakeholders. These collaborations aim to shape effective cybersecurity policies, expand educational opportunities, and define best practices for public-private partnerships worldwide.

In 2024, the Fortinet Training Institute strengthened its commitment to addressing the cybersecurity talent gap by entering into a strategic partnership with the European Commission and working on additional initiatives with the WEF. These partnerships are an essential way for Fortinet to help advance the industry, by sharing expertise with our peers and collaborating to tackle the common issues we face.

European Commission's Cybersecurity Skills Academy

In 2024, Fortinet joined the European Commission's Cybersecurity Skills Academy initiative to support efforts to close the cybersecurity skills gap in Europe. Through this initiative, Fortinet is helping to expand the cybersecurity talent pool by offering free, industry-recognized cybersecurity training, certifications, and an awareness-raising curriculum through the Fortinet Training Institute. Fortinet has pledged to train 75,000 individuals in the EU over three years (February 2024–January 2027).

Our contribution to this initiative targets three key groups:

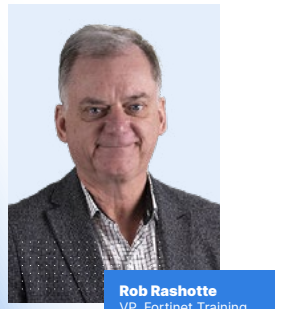
- **60,000 cybersecurity professionals** and ICT workers will have free access to Fortinet's self-paced Network Security Expert (NSE) certification program to re-skill.
- **5,000 students** will gain access to our cybersecurity curriculum, labs, self-paced training and certifications through the Fortinet Academic Partner program in partnership with 30 academic institutions that joined as partners in 2024.
- **10,000 EU students** aged 5–18 will receive cybersecurity and digital safety awareness education through our security awareness curriculum to promote early learning.

Since joining this initiative, Fortinet began offering its certification program through the Cybersecurity Skills Academy and expanding learning opportunities for individuals across all 27 EU countries, helping develop critical cyber skills in the region. In 2024, we trained more than 19,500 EU citizens through this initiative and worked with 186 academic institutions in the EU, including 37 new partnerships in 14 countries.

EU CITIZENS TRAINED

19,789
EU citizens trained in cybersecurity in 2024

186
academic institutions



Rob Rashotte
VP, Fortinet Training Institute and Member of the CSR Committee at Fortinet

« Cybersecurity remains a significant global challenge, posing threats to organizations, individuals, and the broader economy. The growing demand for cybersecurity professionals far outpaces the current supply of trained and certified talent. At Fortinet, we support initiatives like the EU Pledge and the WEF's Bridging the Cyber Skills Gap initiative to expand access to cybersecurity training and equip individuals with the skills necessary to thrive in today's digital world. Cybersecurity skills are essential not just for IT professionals, but for everyone, and through programs like the EU Cybersecurity Skills Academy, we are making critical learning opportunities accessible across all EU member states—empowering people and strengthening the region's cyber resilience. »

World Economic Forum Strategic Cybersecurity Talent Framework collaboration

Another key example of our commitment is Fortinet Training Institute's collaboration with the WEF, which focuses on addressing the cybersecurity skills gap, fostering public-private partnerships, and supporting global capacity building and workforce development.

In 2024, the WEF published its Strategic Cybersecurity Talent Framework, a critical resource for public and private sector decision-makers that offers actionable strategies for tackling workforce shortages and developing sustainable cybersecurity talent pipelines.

Fortinet's early engagement and leadership in the WEF's Bridging the Cyber Skills Gap initiative, along with other company experts, produced insights that contributed to the framework's development and implementation. Learn more.

DIVERSE AND SUSTAINABLE CYBERSECURITY TALENT PIPELINE

Fortinet is committed to improving access to cyber education and training for diverse pools of talent to help address digital and cyber inequities worldwide. By engaging women, veterans, students, and people of all backgrounds and life experiences, Fortinet helps build more sustainable cyber talent pipelines.

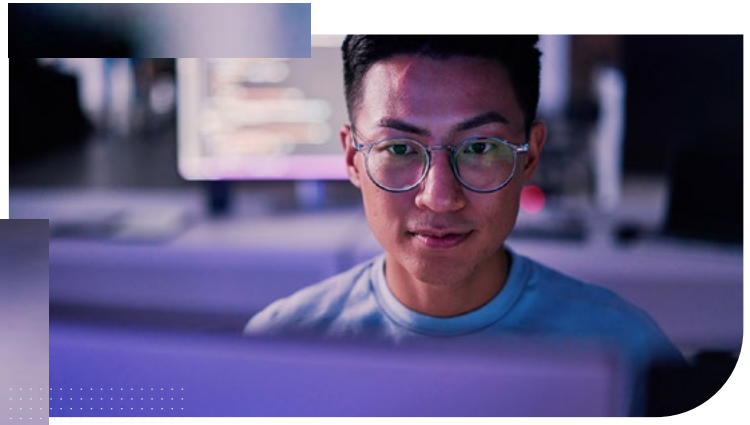
Fortinet Education Outreach program

Through the Fortinet Education Outreach program, part of the Fortinet Training Institute, we collaborate with NGOs to reach underrepresented populations, including veterans and spouses, and women. By providing access to training, certifications, and Fortinet's employer ecosystem, we create pathways to cybersecurity careers, fostering inclusivity and equipping individuals with the skills needed for success in the industry. To date, we have over 10,000 participants in this program, including more than 4,500 added in 2024.

Fortinet Veterans program

A core component of our Education Outreach program, the Fortinet Veterans program supports the military community—including military service members, veterans, and spouses—looking to transition to civilian careers in cybersecurity. Since its launch in 2018, the program has provided free training and certification to over 3,000 veterans and their spouses, equipping them with the technical skills needed to succeed in cybersecurity. The program offers a structured learning path, starting with foundational courses like Networking Fundamentals and progressing to specialized cybersecurity certifications. Fortinet also works with partners who provide tailored career development services for veterans. To date, over 9,500 courses have been completed by veterans and military spouses.

In 2024, more than 290 military veterans and spouses joined the program, contributing to the completion of over 950 courses and workshops by all Veterans program members. We also launched a pilot in Australia that included retired police officers. This pilot has shown benefits, as retired police officers bring similar security mindsets and skills to the cybersecurity field as military veterans.



The Veterans Program Advisory Council—which includes representatives from the Five Eyes countries (Australia, Canada, New Zealand, the United Kingdom, and the United States)—provides the Fortinet Veterans program with strategic guidance to support ongoing improvement. In 2024, the Council continued to share valuable insights on expanding opportunities for military veterans and their spouses to transition into cybersecurity roles or advance their careers.

Other key Fortinet initiatives in 2024 included:

- **Partnership with Women in Cybersecurity (WiCyS) Military Affiliate:** collaborating to support women veterans transitioning into cybersecurity roles, highlighting their unique skills and contributions to the industry.
- **BCIT Cyber Catalyst Bootcamp:** sponsoring and supporting an intensive training program for Canadian veterans at the British Columbia Institute of Technology (BCIT), a Fortinet Academic Partner. Fortinet covered travel, room, and board expenses, donated lab equipment, provided expert-led training, and hosted a networking event to connect participants with Fortinet HR executives. Learn more.
- **VetSecCon'24 sponsorship:** participating in the virtual conference to share insights on the Fortinet Veterans Program and NSE certification opportunities, helping veterans pave their path to cybersecurity careers.

FORTINET'S VETERANS PARTNERS

Blue Star Families
CERCO a Fortinet Education Outreach Partner
CYBER Catalyst.io
FORGE
ONWARD to OPPORTUNITY
VETJOBS
SOLDIER ON
US VALOR
VETERANS TRANSITION SUPPORT
VetSec
Tech Vets Canada
Helping Heroes Rehabilitation Service

Women in cybersecurity

Women have historically been underrepresented in cybersecurity, currently making up only 20%–25% of the workforce[1]. As part of the Fortinet Education Outreach program, we collaborate with women's associations worldwide, including WOMCY in Latin America, WiCyS in the United States, and Women4Cyber and Women in Tech in Europe. These partnerships enable us to support women at all stages of their cybersecurity careers by participating in conferences and webinars, providing mentoring, offering Fortinet training and certification, and connecting them to potential job opportunities.

FORTINET NETWORKING FUNDAMENTALS BOOTCAMP

In 2024, Fortinet ran two 12-week Networking Fundamentals Bootcamps, a new initiative designed to empower underrepresented talent pools with access to cybersecurity education and training. Developed by the Fortinet Training Institute, the bootcamp was offered to all Fortinet Education Outreach program partners. Organizations participating included WiCyS, Siyafunda, Blacks in Technology, the Jamaica Technology & Digital Alliance, and Fortinet Veterans program partners like TechVets and VetSec.

More than 700 individuals worldwide participated in these bootcamps, which combined a mix of self-paced training with live, weekly, instructor-led sessions across multiple time zones. The program provided foundational knowledge in data communication and computer networking, preparing attendees for careers in IT, infrastructure, and cybersecurity and helping to build a more diverse workforce.
Learn more.

"The Networking Fundamentals Bootcamp provides essential knowledge critical for understanding advanced cybersecurity concepts. This preparation is particularly valuable for obtaining cybersecurity certifications, which require a solid grasp of networking principles. By mastering these fundamentals, I'll be equipped to pass these certification exams and advance my career in cybersecurity."
Networking Fundamentals Bootcamp participant

Fortinet Academic Partner Program

Fortinet works with educational institutions globally through the Fortinet Academic Partner Program, equipping the next generation of cybersecurity professionals with the skills needed to address evolving cybersecurity challenges. By integrating Fortinet's NSE training, hands-on labs, and certifications into academic curricula, these partnerships aim to enhance students' technical capabilities while preparing them for high-demand roles in the workforce.

In 2024, the Fortinet Academic Partner Program expanded its global reach, forming partnerships with 153 new academic institutions, including Politecnico di Torino in Italy, the University of Southern Queensland in Australia, and Metro State University in the United States, which incorporated Fortinet training into their graduate programs, equipping students for careers in computer security, IT security, and other related fields. In India, through our collaboration with the EduSkills program—which provides quality education and vocational training in high-demand sectors such as cybersecurity—we have trained over 22,500 students since 2023, including more than 8,200 in 2024. In addition, more than 385 students received Fortinet certifications through CareerTiQ, and over 40 were placed successfully in cybersecurity roles.

Fortinet also supports academic institutions by donating its technology to enhance hands-on learning experiences. In 2024, we donated Fortinet solutions to the BCIT in Canada to equip school labs and contributed to the cyber-physical lab at Simon Fraser University's Surrey Campus. This lab trains mechatronics systems engineering students in smart manufacturing programs, combining Siemens Digital Industries Software with Fortinet cybersecurity solutions to prepare students and provide hands-on experience in OT security.

In 2024, Fortinet introduced new resources to enhance the experience for academic institutions and instructors. These include monthly onboarding sessions to help new partners seamlessly integrate Fortinet training into their curricula. Additionally, live train-the-trainer sessions provide instructors with direct access to Fortinet experts, helping them effectively deliver our content to their students and ultimately enhancing the overall quality of the training experience.

The Fortinet Academic Partner Program includes

790+
colleges and universities across

104
countries (as of December 31, 2024)

1. According to https://www.isc2.org/Insights/2024/04/Women-in-Cybersecurity-Report-Inclusion-Advancement-Pay-Equity.

CYBERSECURITY SKILLS GAP

A NEW GENERATION OF RESPONSIBLE AND SAFE DIGITAL CITIZENS

Ensuring a sustainable and safe cyberspace and society requires ongoing engagement from governments, organizations, and individuals. As a global leader in cybersecurity, we are ideally positioned to help the current and next generations of digital citizens become more cyber-informed and improve their skills to identify and avoid breaches at school, at home, and anywhere they go. Fortinet supports cybersecurity education in primary and secondary schools globally, focusing on staff and students.

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 when confronted with cyberattacks. Available at no cost and in local languages in Australia, Brazil, Canada, Saudi Arabia (added in 2024), the United Kingdom, and the United States, the service reaches approximately 12 million education staff. Learn more.

> « Fortinet's Security Awareness Curriculum provides an opportunity for educators and educational stakeholders to build their own capacity and understanding of topics related to digital safety and well-being. Building this capacity is important so that educators are better equipped to provide meaningful learning experiences for students. The lesson plans, background information, and suggested activities are thorough, and provide practical "dos", as opposed to "do nots", to help anyone living in the digital age make informed decisions to protect themselves from cyber risks. »
>
> **Tineke,**
> Digital Instruction and Assessment Facilitator, Simcoe County, United States

OUR CONTRIBUTION TO PROTECTING CHILDREN IN THE DIGITAL WORLD

As children increasingly engage with digital technologies, they become more vulnerable to online threats, such as phishing, password attacks, cyberbullying, theft of personally identifiable information, and other harmful behaviors that exploit their lack of experience and awareness. To address this growing challenge, Fortinet has programs and resources specifically designed to protect children in the digital world.

Fortinet Security Awareness Curriculum
Through our Security Awareness Curriculum, we help to provide students aged 4–18 with the cybersecurity education they need for a safer digital life experience. The curriculum is available at no cost to elementary schools in Canada, Saudi Arabia (added in 2024), the United Kingdom, and the United States, where it is available to over 70 million K-12 students. The curriculum is divided into age groups: Rookies (ages 4–7), Novices (ages 8–11), Specialists (ages 12–14), Leaders (ages 15–18), and Future Professionals (elective courses for ages 15–18). Each group covers online presence, digital safety, secure privacy, ethical integrity, digital impact, cybersecurity landscape, and online information.

Cyber Safe: A Dog's Guide to Internet Security
Cyber Safe: A Dog's Guide to Internet Security is a Fortinet children's book designed to raise cyber awareness among elementary and middle school students. It takes readers on a journey to learn how to stay secure online. The book is available in several languages.

Fortinet employee volunteers
In 2024, Fortinet launched a global employee engagement initiative that aligns with our commitments to community engagement and cybersecurity education. As part of this effort, we provide Fortinet employee volunteers with training and essential materials—such as instructional videos, presentations, and interactive exercises—to deliver security awareness sessions to students aged 12–14.

CYBERSECURITY PROFESSIONAL UPSKILLING

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

Fortinet Network Security Expert Certification program

Fortinet established the NSE Certification program in 2015 as part of its long-standing dedication to addressing the cybersecurity skills gap. To date, the program has issued over 1.7 million certifications.

The NSE Certification program offers a wide range of free self-paced and instructor-led courses, tailored with a role-based approach to align training with in-demand cybersecurity careers. This enables security professionals to continually enhance their skills, stay ahead of evolving threat methods, and deepen their knowledge of the latest security technologies. By completing these certifications, cybersecurity professionals are better equipped to bolster their organization's security posture and effectively defend against the ever-changing threat landscape. Participants can also access on-demand labs at a cost, providing hands-on exercises to develop practical, real-world experience.

Authorized Training Centers

Fortinet also increases security professionals' access to upskilling through its ATC program, a network of accredited training organizations across 150 countries and territories worldwide. More than 110 ATCs deliver cybersecurity training in 26 local languages using the Fortinet NSE Certification program curriculum. In 2024, new partners that joined the ATC program included IT QAN Hub in Egypt and Fast Lane in Mexico.

FORTINET CERTIFIED EXPERT
- Cybersecurity

FORTINET CERTIFIED PROFESSIONAL
- Network Security
- Security Operations
- Public Cloud Security

FORTINET CERTIFIED ASSOCIATE
- Cybersecurity

FORTINET CERTIFIED SOLUTION SPECIALIST
- Security Operations
- Public Cloud Security
- Network Security
- Zero Trust Access
- OT Security
- Secure Access Service Edge

FORTINET CERTIFIED FUNDAMENTALS
- Cybersecurity

110+
ATCs in 150 countries and territories teaching in 26 languages

2
new ATCs in 2024 (Egypt, Mexico)

950+
courses delivered and

6,000+
people trained through ATCs in 2024

PROMOTING RESPONSIBLE BUSINESS

Responsible and sustainable practices are essential to business. As a global cybersecurity leader, Fortinet is committed to conducting business ethically, respecting human rights, and complying with all laws and regulations. Stakeholder trust is of paramount importance to us, and our corporate governance practices aim to ensure accountability to meet our responsibilities across our entire value chain. We are committed to implementing best practices internally for information security and privacy to protect our own systems and the data of our employees and customers. We advocate for public policies that advance cybersecurity with proper controls, transparency, and oversight at the highest levels.

2024 HIGHLIGHTS

81
information security certifications and examinations

Board-level
cybersecurity committee

Fortinet's training on compliance and business ethics completed by

100%
of our distributors

100%
of our top contract manufacturers*

** Representing >90% of spend.*

BUSINESS ETHICS

We are committed to upholding ethical business practices and ensuring legal compliance, fostering a culture built on integrity, accountability, and trust. Our comprehensive approach to governance, codes of conduct, and engagement with employees, partners, suppliers, and customers reflect our dedication to promoting responsible business across our entire value chain. We also conduct third-party audits to assess compliance with ethical standards, both for our operations and those of our key contract manufacturers, driving continuous improvement.

ETHICS GOVERNANCE

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

Our risk management steering committee plays a vital role in identifying and mitigating risks associated with third parties 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 a broad range of areas such as general standards of conduct, avoiding conflicts of interest, 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 for all employees applies to all directors, officers, and employees of Fortinet and its subsidiaries. Agents and contractors of Fortinet are also expected to read, understand, and abide by the Code.

Our partners, suppliers and vendors are extensions of our business and, therefore, our reputation. We hold them 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.

COMPLIANCE AND ETHICS TRAINING AND AWARENESS

Compliance and ethics training are central to our commitment in this area, both internally and with third parties. Our multifaceted strategy ensures that people throughout Fortinet's ecosystem remain well-informed about ethical and regulatory obligations. This enables everyone to contribute to the integrity and resilience of our business ethics culture.

Fortinet employees must complete annual trust and compliance training, and 98% achieved this in 2024. We have additional requirements for our sales team to complete sales compliance training every six months, complemented by a quarterly compliance certification. In 2024, we also created a compliance toolkit designed to equip all employees with the resources needed to effectively foster awareness and understanding of Fortinet's business ethics and compliance program.

We also collaborate closely with our suppliers and vendors to ensure they fully meet our business ethics standards. In 2024, 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 2024, 100% of distributors completed the Partner Compliance training.

Making business ethics and compliance training as engaging as possible is essential to empowering our stakeholders on these topics. We continually enhance our training methods, incorporating elements such as gamification, quizzes, videos, and checks on learning.

BUSINESS ETHICS

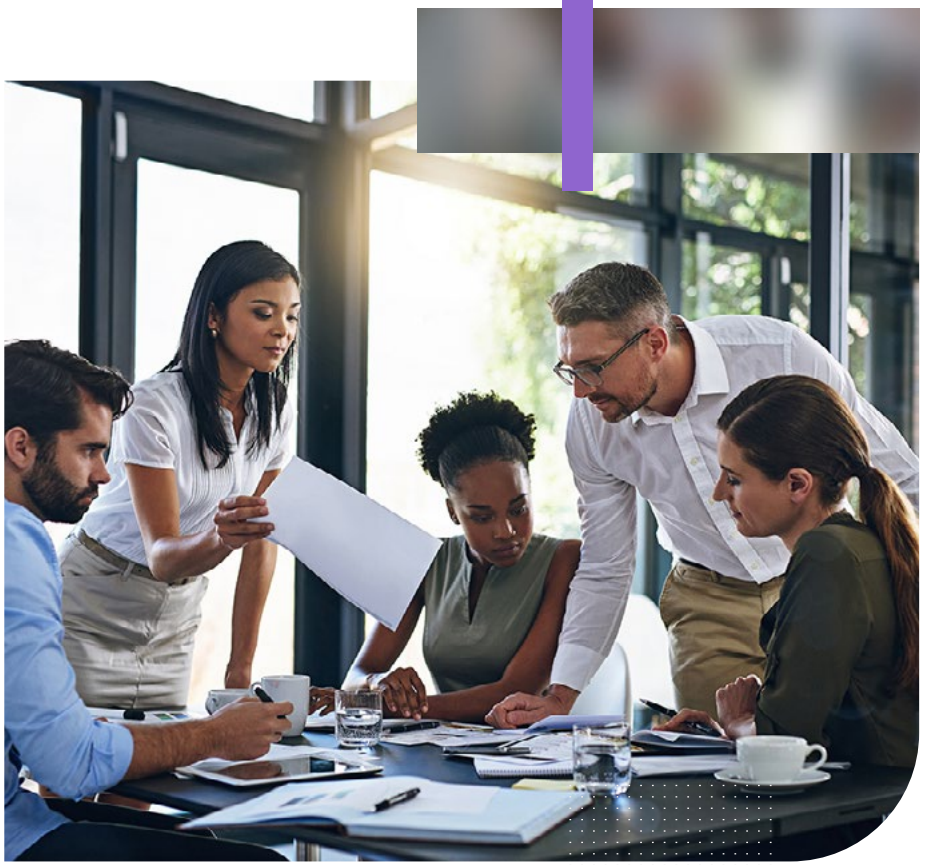
REPORTING CONCERNS

Fundamental to our culture of integrity, 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 through various avenues outlined in the Fortinet Whistleblower Policy without fear of retaliation. This includes the option to report concerns confidentially and, if desired, anonymously to our third-party whistleblower hotline. A dedicated team promptly investigates all relevant allegations and takes necessary actions to mitigate and remediate any adverse impacts.

To enhance accessibility, 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. In 2024, we updated our compliance posters and distributed copies to all major offices worldwide. These posters include a QR code with detailed information about 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.

AUDITS AND ACCOUNTABILITY

Fortinet employs focused audits as systematic and proactive measures to ensure compliance with its ethical standards. In 2024, 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 collect feedback about our programs to identify opportunities for improvement. In our 2024 employee compliance survey:

100%
of respondents stated they know where to go to report a concern

99%
of respondents stated they are confident their concern will be addressed

100%
of respondents stated they are confident that Fortinet executive leadership operates with ethics and integrity

HUMAN RIGHTS

Our Global Human Rights Policy outlines Fortinet's commitment to respecting the human rights of stakeholders across our value chain, including workers in our supply chain, our employees, the users of our products and services, and others. This policy provides a baseline for furthering our human rights program and due diligence process while anchoring Fortinet's engagement with stakeholders on human rights-related topics. We are committed to conducting business ethically and taking reasonable steps to ensure respect for internationally recognized human rights as expressed in the International Bill of Human Rights and adopting responsible business practices consistent with the UN Guiding Principles on Business and Human Rights.

Fortinet incorporates human rights language into key documents such as End-Users License agreements, product datasheet templates, and codes of conduct for partners and suppliers. We also incorporate human rights information into mandatory training programs, reflecting our commitment to raising awareness and understanding throughout our organization and value chain. Fortinet periodically reviews its Global Human Rights Policy to ensure it addresses the evolving landscape of human rights risks.

As a cybersecurity leader, we advance technological innovation that protects the sensitive data and property of individuals and businesses, combating cybercrime and safeguarding individual freedoms. Learn more. Through our efforts to close the cybersecurity skills gap, we are also helping to build an inclusive cybersecurity workforce. Learn more.

HUMAN RIGHTS IN OUR VALUE CHAIN

Fortinet considers the following potential human rights impacts in our value chain:

Responsible minerals sourcing

Fortinet expects its suppliers to comply with the Responsible Business Alliance Code of Conduct and conduct their business in alignment with Fortinet's Supplier Code of Conduct, including policies such as Fortinet's Responsible Minerals Sourcing Policy. If a supplier does not meet Fortinet's expectations, Fortinet reserves the right to engage with them to address the issue appropriately, which may involve corrective actions or reevaluation of the partnership.

Third-party diligence

Fortinet prioritizes robust risk management by implementing a meticulous screening process for its partners and suppliers. This process involves two-step verification, sophisticated third-party diligence tools, and continuous monitoring in high-risk areas. To assess direct suppliers and vendors, we apply criteria such as human rights, the U.S. Foreign Corrupt Practices Act, and sanctions lists.

Suppliers and vendors must adhere to human rights principles, including the Trafficking Victims Protection Act, the UK Modern Slavery Act, and the Uyghur Forced Labor Prevention Act (UFLPA). We request compliance certifications from contract manufacturers for high-risk regulations in our industry and continually screen contract manufacturers and partners in high-risk regions. Fortinet commits to investigating and rectifying non-compliance with disciplinary actions, including termination when necessary.

In 2024, Fortinet continued conducting proactive anti-corruption evaluations of third parties to ensure adherence to ethical practices and collaborated closely to address any reported non-compliance. Our commitment to risk mitigation includes an agile response and resolution process.

Modern slavery

As made clear in Fortinet's Statement on Modern Slavery, we are fully committed to ensuring that our business practices, human resources procedures and selection of staff and those with whom we do business align with good faith efforts to combat slavery and human trafficking.

Responsible product use

Designing, developing, selling, and managing products and services in ways that respect human rights is paramount for us. Fortinet adheres fully to the relevant guidance of the UN Guiding Principles on Business and Human Rights, and we comply with the laws of the countries where we operate. We have a team dedicated to ensuring compliance with trade compliance laws, such as laws prohibiting the sale of our products to certain countries, some of which have poor human rights records. We contractually commit our end-customers, through our End-User License Agreement, to agree that Fortinet's products and services cannot be used to engage in or support in any way 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.

Diego Hernandez
Senior Director,
Global Trade Compliance
and Member of the
CSR Committee at Fortinet

What steps is Fortinet taking toward its supply chain sustainability program?

« In 2024, we engaged an external expert to assess the current state of our supply chain sustainability program. This assessment focused specifically on managing contract manufacturers and identifying related best practices. It covered internal elements—such as supply chain strategies, processes, governance, and management—and external elements like supplier engagement and reporting. We are working to advance our supply chain sustainability program in several ways over the coming years. These include engaging with contract manufacturers to develop strategies that align with sustainability goals, providing them training on Fortinet's sustainability initiatives, and educating internal teams on best practices for selecting suppliers that support our broader sustainability objectives. »

INFORMATION SECURITY AND DATA PRIVACY

Information security and privacy are integral to our business and vital to our stakeholders' ongoing trust. Our commitment in this area is embedded in every part of our business and every phase of our product development, manufacturing, and delivery processes.

GOVERNANCE

Fortinet's governance structure, led by our Board of Directors, actively oversees and emphasizes cybersecurity as an essential component of the company's overall approach to enterprise risk management. Fortinet's Board of Directors recognizes the critical importance of maintaining the trust and confidence of our customers, business partners, and employees. In 2024, the Board of Directors established a new Cybersecurity Committee to focus on this topic.

The Cybersecurity Committee is responsible for reviewing our cybersecurity and other information technology risks, controls, and processes with management, including the processes used to prevent or mitigate cybersecurity risks and respond to cybersecurity events. Fortinet executives responsible for cybersecurity provide quarterly reports to the Cybersecurity Committee, the Chief Executive Officer and other members of our senior management, as appropriate. These reports include updates on our cybersecurity risks and threats, the status of projects to strengthen our information security posture, assessments of our information security program, and summaries of the emerging threat landscape.

ROBUST INFORMATION SECURITY MEASURES

We are committed to continuously enhancing our Information Security Management System (ISMS), helping ensure the confidentiality, integrity, and availability of Fortinet systems and our customers' data.

Our comprehensive and robust ISMS incorporates policies, programs, standards, procedures, and controls aligned with industry standards such as the ISO 27001/2, ISO 27017, ISO 27018, and NIST 800-53/161 frameworks as well as data privacy laws such as the European Union General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Other standards may be adopted to augment these to satisfy unique requirements, such as NIS2 and DORA (see box), in some regions or industry verticals.

Management reviews of security policies are conducted at least annually or when significant changes occur to help ensure their continued suitability, adequacy, and effectiveness. We communicate changes in policies to all employees.

As an early adopter of Fortinet technology, we rely heavily on our security solutions and services to manage and mitigate cybersecurity risks. In 2024, Fortinet continued to expand the implementation of its products and solutions and adopted new capabilities and features to protect its network. We also provided early feedback to the R&D organization that can help further strengthen Fortinet's cybersecurity solutions. We conduct regular risk assessments and engage internal experts and third-party auditors to validate that our practices align with industry standards and best practices. In addition, Fortinet applies security best practices in the product development process, adhering to leading standards such as NIST 800-53, NIST 800-160, NIST 800-218, U.S. EO 14028, and the UK TSA.

We also have robust internal and external product scrutiny at all stages of our product development lifecycle, from design through end-of-life. When issues occur, Fortinet remediates them promptly, following a comprehensive response plan. See Secure by design, secure by default.

We provide customer assurances concerning our information security and data privacy practices through certifications and independent assessments based on internationally recognized standards. In 2024, Fortinet reaffirmed its commitment to cybersecurity by renewing and expanding the scope of its ISO 27001/17/18 certifications and SOC2 Type II examinations.

81
information security certifications and examinations

2024 INFORMATION SECURITY AND PRIVACY CERTIFICATIONS

- COMMON CRITERIA
- CSA STAR
- ENS
- GDPR
- HIPAA
- ISMAP
- ISO 27001
- ISO 27001 SOA
- ISO 27017
- ISO 27018
- ISO 9001
- SOC 2
- TISAX
- VPAT

COMPLYING WITH NEW REGULATIONS AND REQUIREMENTS

New cybersecurity regulations, such as the EU NIS2 Directive and the EU Cyber Resilience Act (CRA), introduce a more holistic framework and stricter requirements for global cybersecurity providers like Fortinet. In addition, sector-specific regulations, including the EU Digital Operational Resilience Act (DORA) and the UK Telecom Security Act (TSA), require a higher level of resilience against cyber risks for our customers. In response, Fortinet is strengthening its policies, processes and controls to ensure compliance with these evolving regulations while also helping our customers in adapting their own compliance programs.

INFORMATION SECURITY AWARENESS AND TRAINING FOR EMPLOYEES

Fortinet fosters cyber awareness among its employees through initiatives, including our annual Information Security Awareness Compliance training, which was completed by over 96% of our employees in 2024. This training includes videos, gamification, quizzes, and additional techniques. We also conduct periodic phishing campaigns to educate 100% of Fortinet employees about various attack techniques, including social engineering. In addition, developers are required to complete secure code development training, and specialized training is required from employees in IT and information security roles.

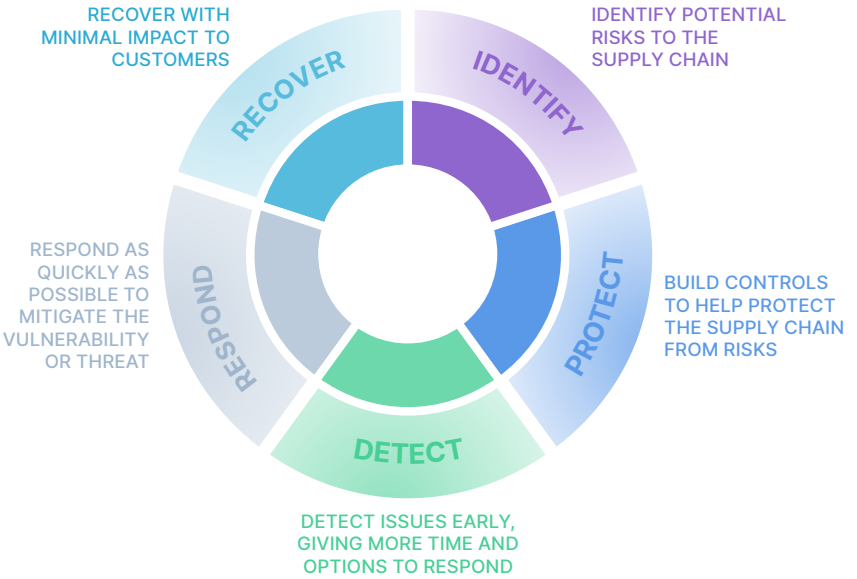
The information security team publishes alerts about new and emerging threats and provides security tips to all employees on its internal website. Fortinet promotes the ethical and responsible use of AI solutions and provides guidance to employees to ensure the security and privacy of our data.

SUPPLY CHAIN SECURITY RISK MANAGEMENT PROGRAM

Fortinet's supply chain plays a critical role in providing customers assurance about the security and integrity of Fortinet products. Supply chain security management begins with establishing control over a qualified supplier base, which can in turn provide qualified and trusted components for design, development, and manufacturing services, as well as post-sale product support.

The Fortinet Trusted Supplier Program (TSP) is aligned with the requirements defined in NIST SP 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations and other directives, as periodically established by the U.S. government for securing the information and communication technology services supply chain. This program was developed in response to increasing customer demand for transparency in the security of the hardware, firmware, and software included in Fortinet's products and to comply with US government directives. Fortinet conducts a thorough security assessment of its TSP partners to ensure they comply satisfactorily with applicable controls established by NIST SP 800-161, and works side-by-side with them to remediate gaps and monitor their security postures.

The Fortinet TSP covers security risk management for the entire breadth of the supply chain and implements five key steps for managing supply chain risks:



Rafi Brenner
VP Information Security and Member of the CSR Committee at Fortinet

« Supply chain risk management is a cornerstone of ensuring trust in Fortinet's products. Through our Trusted Supplier Program, we methodically implement processes and controls aligned with rigorous standards, such as NIST SP 800-161, to identify threats, protect our products, and respond to and recover from adversarial events. This commitment not only addresses evolving customer demands for transparency but also fortifies the security and integrity of the hardware, firmware, and software in our products. »

DATA PRIVACY

Ensuring the trust and confidence of our employees, business partners, and customers is vital. Our governance structure includes a dedicated privacy team that oversees the Fortinet privacy program and all privacy initiatives. Under the guidance of this team, we have established a cross-functional committee consisting of Fortinet privacy champions across different business units—including R&D, product management, sales, marketing, and others—who meet regularly to review privacy practices and policies, stay informed of legislative developments, keep our processes updated, and seamlessly address privacy questions and comments to help ensure our employees remain updated and aware of data privacy matters. In 2024, we established Fortinet Data Protection Officers in Mexico, Singapore, and Spain to ensure compliance with regional data privacy laws, guide local initiatives, and uphold our privacy compliance.

Fortinet's practices for processing personal data are detailed in the Fortinet Privacy Policy, which aligns with various data privacy protection laws and principles, providing a globally consistent standard applicable to all stakeholders. For example, we comply with GDPR and support our customers and partners in their efforts to comply (see detail about Fortinet's GDPR approach). Our Fortinet Data Privacy Practices document highlights how personal information is handled by our products and services, including in the areas of communication between Fortinet products and services, FortiGuard information collection, and information storage and protection on cloud services.

We continually enhance our approach to align with emerging regulations and stakeholder expectations worldwide. In 2024, we updated our Privacy Policy to reflect Fortinet's participation in the EU–US Data Privacy Framework. To inform our employees, customers, and others, we also increased the amount of privacy-related content and data available on our public Fortinet Trust Resource Center, such as regarding data protection officers, data subject access requests, and privacy-by-design.

The Fortinet Trust Resource Center offers customers transparency regarding our information security and data privacy programs. Customers can easily access extensive information, including statements regarding data privacy, data processing agreements, certifications, and detailed audit reports, empowering them with a deeper understanding of our commitment to safeguarding their data.

All of our employees are required to complete mandatory privacy training upon hiring and at least annually thereafter. We also conduct privacy reviews of our third-party vendors and impose additional privacy obligations on vendors where appropriate.

Fortinet's holistic approach ensures that our privacy program remains aligned with industry standards while fostering a culture of transparency, education, awareness, and accountability across the organization.

PUBLIC POLICY

We engage in public policy advocacy to advance the interests of our company, our customers, and other stakeholders. Our advocacy is primarily focused on smart government policies that ensure or enable strong cyber resilience across all sectors of the economy. We also advocate for policies that promote a strong and growing cybersecurity workforce and that bolster cyber awareness in all communities.

Fortinet is committed to ensuring proper controls and transparency related to its public policy engagements through oversight at the highest levels. Our Chief Operating Officer and VP of Corporate & Government Affairs lead these efforts, overseeing high-level government engagements, developing our public policy strategy, and ensuring compliance with related laws and regulations, including proper disclosure.

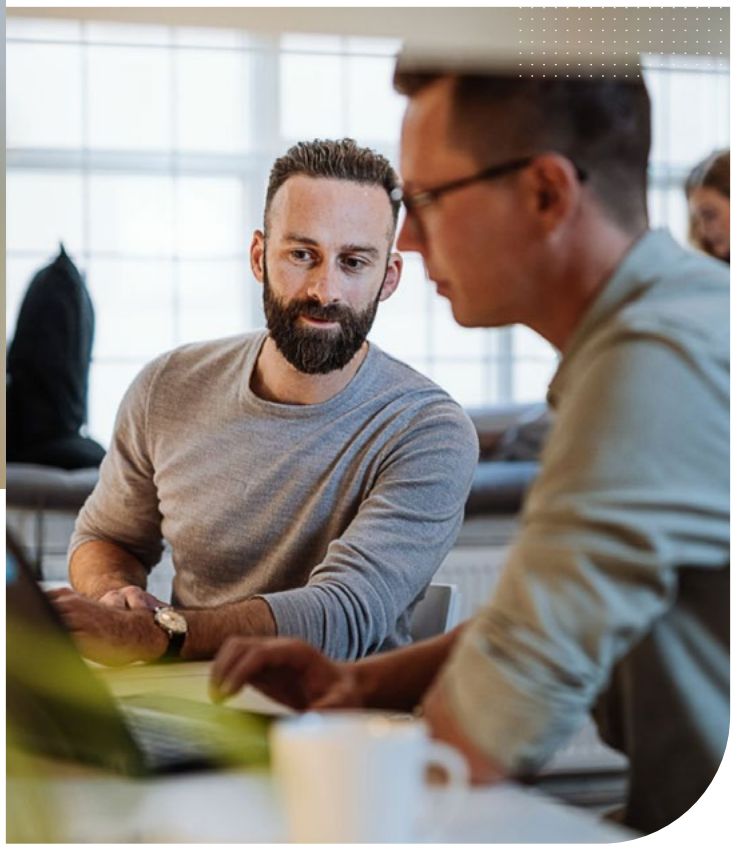
Collaboration with the public sector and industry has been fundamental to Fortinet's strategy for many years. We partner with industry peers, computer emergency response teams (CERTs), and government entities to proactively exchange threat information and enhance cyber resilience globally. Learn more about our international partnerships and engagements with key government and trade associations.

Fortinet engages with third-party strategic allies and industry associations to expand our positive influence on public policy focused on strengthening cyber resilience across the economy, supporting a strong cybersecurity workforce, improving general security awareness, and helping ensure infrastructure policies address the evolving cyber threat landscape.

Fortinet also engages in discussions with policymakers at different levels of government, as permitted, and files related required reports and disclosures, including reports required by the Lobbying Disclosure Act, along with those required by other jurisdictions.

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 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 appropriate compliance and the required disclosure and reporting of these activities.



APPENDIX

ABOUT THIS REPORT

Fortinet's 2024 Sustainability Report presents a balanced and transparent account of our sustainability performance across our priority topics during the year. It enables our stakeholders to better understand our approach in this area and how we integrate sustainability across the company. Since 2021, we have reported annually on Fortinet's sustainability performance and provided in-depth information on our commitments and progress across the company's sustainability pillars and priority topics. See our historical sustainability reports.

The data summary includes extensive performance metrics and data. Limited assurance was performed on Fortinet's GHG emissions. See the assurance statement.

This report references reporting frameworks and standards, including GRI (Global Reporting Initiative) Standards, Sustainability Accounting Standards Board (SASB) Standards, Task Force on Climate-related Financial Disclosures (TCFD), United Nations Global Compact (UNGC), and CDP. Fortinet's GRI, SASB, and TCFD indices are included in the Appendix.

Unless stated otherwise, this report covers Fortinet's operations and activities worldwide for the fiscal year 2024 (Jan. 1, 2024–Dec. 31, 2024). All financial figures are reported in U.S. dollars unless noted otherwise. See additional information on key cybersecurity terms.

CONTACT US

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

PERFORMANCE DATA

ADDRESSING CYBERSECURITY RISKS TO SOCIETY

Innovation

	2024	2023	2022
% of revenue generated from innovation [1]	**30.6%**	38.3%	49.5%
Number of new product families introduced	**3**	6	5
R&D investment (USD in millions)	**716.8**	613.8	512.4
Number of issued and pending patents globally	**1,829**	1,551	1,540

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

Partnership against cybercrime

	2024	2023	2022
WEF's Cybercrime Atlas — number of actionable data points mapped and analyzed for disruption opportunities in the cybercriminal ecosystem [2]	**10,000+**	8,584	Not applicable
Cyber Threat Alliance — number of early discovery shares on threat campaigns	**207**	223	197

2. In 2022, this metric was calculated using a different methodology, and is therefore not comparable with 2023 data. 2022 data could not be restated.

PROMOTING RESPONSIBLE BUSINESS

Business ethics

	2024	2023	2022
% of employees who received communication about Fortinet's Code of Business Conduct and Ethics	**100%**	100%	100%
% of Fortinet's new direct suppliers screened using human rights criteria, Foreign Corrupt Practices Act (FCPA), sanction lists, embargoed countries	**100%**	100%	100%
% of distributors globally who completed Fortinet's Partner Ethics and Compliance training	**100%**	100%	91%
% of key contract manufacturers [3] who completed Fortinet's Vendor/Supplier Compliance training	**100%**	100%	100%

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

RESPECTING THE ENVIRONMENT

Product environmental impacts

% improvement in power efficiency per throughput for top four products	2024[4]
FortiGate-30G	**84%**
FortiGate-50G	**94%**
FortiGate-70G	**39%**
FortiGate-200G	**26%**
Average	**61%**

4. Improvements in maximum power consumption use in top four products (FortiGate G series versus equivalent product models from previous generations) released in 2024.

Waste

	2024	2023	2022
E-waste (in metric tons) [5]	**12.0**	42.1	67.1
Recyclable waste (in metric tons)[6]	**83.1**	12.8	11.2
Total waste	**95.1**	54.9	78.3

5. Data represents e-waste removed during the year from the largest warehouses and RMA centers (Union City, USA, Burnaby, Canada and Sophia Antipolis, France).
6. 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.

Water

	2024	2023	2022
Water (cubic meter) [7]	**60,313**	29,188	Not Reported

7. Data presented here is from owned sites. Increase from between 2023 and 2024 is due to better tracking.

GHG emissions and energy consumption

	2024	2023	2022
Scope 1 emissions ($MTCO_2e$) [8]	**1,606.4**	1,328.3	1,205.6
Scope 2 emissions—Location based ($MTCO_2e$) [8]	**9,838.8**	5,422.2	4,589.6
Scope 2 emissions—Market based ($MTCO_2e$) [9]	**0**	792	163.7
GHG emissions intensity ($MTCO_2e$)/$billion revenue	**1.92E-06**	1.27E-06	1.31E-06
Energy consumption (GJ) [10]	**210,853**	182,280	142,316
Energy intensity (GJ)/$billion revenue	**3.54E-05**	3.44E-05	3.22E-05

8. Scope 2 emissions - Location based increased due to addition new sites and two datacenters.
9. Scope 2 emissions—Market based (MTCO2e) is 0 due to a combination of renewable electricity and purchase of RECs.
10. Energy consumption increased due to addition new sites and two datacenters.

GHG emissions and energy consumption (cont.)

	2024	2023	2022
Purchased goods and services	**110,259**	94,208	103,356
Capital goods	**3,689**	6,180	7,278
Fuel and energy-related activities	**5,300**	5,246	4,586
Upstream transportation and distribution	**8,475**	7,541	9,983
Waste generated in operations	**843**	622	562
Business travel	**14,131**	7,842	5,762
Employee commuting	**16,936**	5,250	4,587
Upstream leased assets	**4,768**	6,432	6,533
Downstream transportation and distribution	**14**	15,747	12
Use of sold products [11]	**1,690,540**	1,874,729	3,669,454
End-of-life treatment of sold products	**461**	150	255

11. Use of sold products total decreased in 2023 due to the use of more accurate raw data and less estimation. Total Scope 1, 2 and 3.

GROWING AN INCLUSIVE CYBERSECURITY WORKFORCE

Board of Directors

	2024	2023	2022
Size of the Board	**10**	8	8
Women on the Board	**40%**	25%	25%

Number of employees

	2024	2023	2022
Total	**14,138**	13,568	12,595
Americas	**7,665**	7,407	7,009
APAC	**2,725**	2,735	2,491
EMEA	**3,748**	3,426	3,095

Number of new hires

	2024	2023	2022
Total	**2,199**	2,306	3,789
Americas	**1,185**	1,200	2,091
APAC	**329**	500	711
EMEA	**685**	606	987

Employee turnover

	2024	2023	2022
Total	**1,628**	1,333	1,389
Americas	**926**	808	735
APAC	**336**	247	342
EMEA	**366**	278	312

Representation of women

	2024	2023	2022
All	**20%**	20%	21%
Management	**17%**	17%	17%
Technical [12]	**17%**	20%	12%
Other	**23%**	24%	33%
Sales	**16%**	16%	16%
R&D	**18%**	18%	18%
New hires	**21%**	19%	23%
Turnover	**20%**	21%	21%

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

Ethnicity—US only

	2024	2023	2022
White	**48.5%**	49.5%	49.9%
Asian	**37.2%**	35.9%	35.2%
Latinx	**9.4%**	9.6%	9.5%
Black	**2.7%**	2.9%	2.9%
Two or more races	**1.8%**	1.7%	1.7%
Pacific Islander	**0.3%**	0.3%	0.3%
Native American	**0.1%**	0.1%	0.2%
Not disclosed	**0.0%**	0.0%	0.2%

Cybersecurity skills gap

	2024	2023	2022
Total individual people trained [13]	**630,859**	432,905	219,465
Certifications obtained from the learning platform	**203,062**	334,429	315,239
EU Pledge	**19,789**	Not Applicable	Not Applicable

13.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.

REPORTING FRAMEWORKS INDICES

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 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 and CSR Director, with the occasional assistance of specialized consulting firms, conducts quarterly presentations to the Board to review ESG-related strategy, risks and opportunities, share information about the evolution of climate-related regulations, report progress in sustainability and issue recommendations for ongoing improvement. At the end of 2022, Fortinet's Board members participated in a training session to deepen their understanding of climate-related risks and opportunities. **Learn more** about CSR governance at Fortinet and see our Board of Directors Governance and Social Responsibility Committee Charter.
	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 provides sponsorship to integrate sustainability 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 strategy, and oversees related initiatives and programs. It assists the GSR Committee of the Board of Directors in overseeing Fortinet's CSR, including climate-related issues. The CSR Committee meets at least four times a year, and shares progress and recommendations with Fortinet's Executive Team and the Board of Directors' GSR Committee once a quarter. The CSR team and the internal CSR Committee, both led by Fortinet's Global Sustainability and 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, and other stakeholders to implement the solutions agreed upon. Fortinet has also integrated a dedicated incentives scheme for the CSR team and Global Sustainability and CSR Director regarding sustainability-related issues via the achievement of quarterly business goals. **Learn more** about CSR 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	**Transition risks and opportunities:** We assessed risks and opportunities related to regulations, public policy, technology, the marketplace and the company's reputation. Developing new, more energy-efficient products and services through R&D and innovation is a key opportunity related to these risks and may have financial or strategic impacts on our business. Learn more. Use of renewable energy sources is another important opportunity. We have developed a comprehensive strategy for renewable energy purchasing and generation. We have also developed energy-efficiency optimization of our data centers and offices and real estate investment, through a set of green guidelines. Learn more. **Physical risks and opportunities:** We evaluated potential acute and chronic risks and opportunities associated with the physical impacts of climate change on key operations. Risks included extreme weather, such as hurricanes, fires and floods, especially in locations where Fortinet has a large presence.
	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. Guiding our overall efforts, 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, were validated by SBTi in 2024. Learn more. Our decarbonization plan, developed in 2024, 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. Sixty-five percent of our owned facilities by square footage used 100% renewable electricity in 2024, and this is 100% of facilities when we include the purchase of renewable energy credits (RECs) or energy attribute certificates (EACs). 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 working to engage 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 work to enhance product designs to reduce power, cooling and space, helping customers minimize energy consumption and GHG emissions. To support our customers' decision-making related to sustainability, we have developed the Fortinet carbon footprint calculator, which provides the carbon footprint of many of our products. To reduce overall environmental footprint, we also focus on sustainable packaging and embracing circular economy practices that increase repair and reconditioning, extend product lifespans and enhance materials recycling. Learn more.
	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 will enhance our resilience against climate change. Energy consumption is a key driver of GHG emissions in our facilities and represents a significant operational cost. We focus on improving energy efficiency and transitioning to lower-impact energy sources, which will save resources, decrease GHG emissions and support resilience in our operations. We anticipate that customers will increasingly value energy efficiency and other aspects of environmental performance in our products. Our ongoing focus on innovation in this area will help us to capitalize on this opportunity.

Topic	Required disclosure	Reference/disclosure
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	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 take into account factors such as disruptions to our operations and potential damage to our brand. We leverage scenarios from the International Energy Agency (IEA) (see below) to inform the climate-related risk-identification process. Climate-related risks are also assessed as a part of Fortinet's periodic materiality assessment process. The climate-related risks that Fortinet has identified are aligned with the risks included in Tables 1 and 2 of the 2021 TCFD Report Implementing the Recommendations of the Task Force on Climate-related Financial Disclosures. Several analyses have informed our understanding of climate-related risks and opportunities, including the following: • In 2022, Fortinet conducted a qualitative analysis of current and potential climate-related transition and physical risks and opportunities with impact on our company. The analysis evaluated three scenarios from the IEA: IEA NZE 2050, IEA APS and IEA STEPS (previously IEA NPS). • We conducted a Scope 3 and product carbon footprint analysis in 2023 to help us understand the impacts of our supply chain partners and vendors on climate change. • In 2024, Fortinet completed a full life cycle 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 life cycle.
	B. Describe the organization's processes for managing climate-related risks	CSR issues, including climate-related risks, are managed through Fortinet's CSR 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. In recent years, we have engaged our teams to deepen their knowledge in these areas and empower them to implement new ideas, including through circular economy workshops that employees in R&D, product management and operations participated in during 2024. Learn more. To increase organizational capacity in this area, we inform internal teams about climate-related issues through a monthly sustainability digest, training modules on sustainability, e-learning modules and other resources available to specific teams.
	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 (which includes Finance) have begun to collaborate on defining the best approach to integrating climate risk into the company's broader risk management priorities.
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) • % improvement in power efficiency per throughput for top four products • E-waste • Recyclable waste • Total waste • Water 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 Greenhouse Gas Protocol Corporate Accounting and Reporting Standard (revised version), to calculate our GHG emissions. We calculate our GHG emissions across all Scopes, including the 12 Scope 3 categories that are relevant to our company. 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. Learn more.

GRI INDEX

Fortinet's sustainability reporting has been prepared with reference to the Global Reporting Initiative (GRI) Standards.

Statement of use	Fortinet has reported with reference to the GRI Standards for the period Jan.1-Dec 31, 2024		
GRI 1 used	GRI 1: Foundation 2021		
Applicable GRI Sector Standard(s)	None developed yet		
GRI Standard	**Description**	**Reference/Disclosure**	**Alignment to the SDGs[14]**
General disclosures			
GRI 2: General disclosures 2021	2-1 Organizational details	2024 Sustainability Report / Who we are p. 3 2024 Form 10-K pp. 3-8	
	2-2 Entities included in the organization's sustainability reporting	2024 Sustainability Report / About this report p. 52	
	2-3 Reporting period, frequency and contact point	2024 Sustainability Report / About this report p. 51	
	2-4 Restatement of information	There are no restatements.	
	2-5 External Assurance	2024 Sustainability Report / Limited assurance statement p. 60	
	2-6 Activities, value chain and other business relationships	2024 Sustainability Report / Who we are p. 3	
	2-7 Employees	2024 Sustainability Report / Inclusion and belonging in our workforce pp. 37-38 2024 Sustainability Report / Performance data p. 54	*5.1, 5.5, 8.5, 8.8, 10.2, 10.3, 10.4*
	2-9 Governance structure and composition	Governance and Social Responsibility Committee Charter Human Resources Committee Charter Audit Committee Charter 2024 Sustainability Report / CSR governance p. 11	
	2-10 Nomination and selection of the highest governance body	Governance and Social Responsibility Committee Charter 2024 Proxy Statement pp. 31-32	
	2-11 Chair of the highest governance body	Ken Xie, CEO and Chairman 2024 Proxy Statement pp. 28-29	
	2-12 Role of the highest governance body in overseeing the management of impacts	Governance and Social Responsibility Committee Charter 2024 Proxy Statement pp. 29-30	

GRI Standard	Description	Reference/Disclosure	Alignment to the SDGs[14]
General disclosures			
GRI 2: General disclosures 2021	2-13 Delegation of responsibility for managing impacts	Governance and Social Responsibility Committee Charter CSR Committee Charter 2024 Sustainability Report / CSR governance p. 11	
	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	
	2-16 Communication of critical concerns	2024 Proxy Statement pp. 32-33	
	2-17 Collective knowledge of highest governance body	2024 Sustainability Report / CSR Governance p. 11	
	2-18 Evaluation of the performance of the highest governance body	2024 Proxy Statement p. 19	
	2-19 Remuneration policies	2024 Proxy Statement pp. 35-39	
	2-20 Process to determine remuneration	2024 Proxy Statement pp. 39-43 Human Resources Committee Charter	
	2-22 Statement on sustainable development	2024 Sustainability Report / Letter from our CEO p. 4	
	2-23 Policy commitments	Codes of Business Conduct and Ethics Responsible Minerals Sourcing Environmental Policy Global Health and Safety Policy Human Rights Policy Partner Code of Conduct Privacy policy Secure Product Development Lifecycle Policy Vendor/Supplier Code of Conduct	
	2-24 Embedding policy commitments	2024 Sustainability Report / Business ethics pp. 44–45 2024 Sustainability Report / Human rights p. 46 2024 Sustainability Report / Performance data pp. 52-54	
	2-26 Mechanisms for seeking advice and raising concerns	2024 Sustainability Report / Business ethics and human rights p. 45-47 Whistleblower Policy	
	2-28 Membership associations	2024 Sustainability Report / Update to Cybercrime disruption p. 18	
	2-29 Approach to stakeholder engagement	2024 Sustainability Report / Stakeholder engagement p. 10	

GRI Standard	Description	Reference/Disclosure	Alignment to the SDGs[14]
Material topics			
GRI 3: Material topics 2021	3-1 Process to determine material topics	2024 Sustainability Report / Sustainability materiality p. 9	
	3-2 List of material topics	2024 Sustainability Report /Sustainability impact p. 7	
	3-3 Management of material topics	2024 Sustainability Report / Business ethics pp. 44–45 2024 Sustainability Report / Human rights p. 46 2024 Sustainability Report / Information Security and data privacy pp. 47-49 2024 Sustainability Report / Cyber risks: A growing threat to society p. 13 2024 Sustainability Report / Secure by design, secure by default p. 14 2024 Sustainability Report / Security innovation pp. 15-16 2024 Sustainability Report / Cybercrime disruption pp. 17-20 2024 Sustainability Report / Climate strategy pp. 23-24 2024 Sustainability Report / Product environmental impacts pp. 28-31 2024 Sustainability Report / Inclusion and belonging in our workforce pp. 33-36 2024 Sustainability Report / Cybersecurity skills gap pp. 37-42	7.2, 7.3, 7.a, 13.1, 13.2 8.5, 8.8, 16.3, 16.4
Indirect economic impact			
GRI 203: Indirect economic impacts 2016	203-2 Significant indirect economic impacts	2024 Sustainability Report / Addressing cybersecurity risks to society pp. 20-21	16.3
Anti-corruption			
GRI 205: Anti-corruption 2016	205-2 Communication and training about anti-corruption policies and procedures	Anti-Corruption Policy 2024 Sustainability Report / Business ethics pp. 44–45 2024 Sustainability Report / Human rights p. 46 2024 Sustainability Report / Performance data p. 52	16.5
Energy			
GRI 302: Energy 2016	302-1 Energy consumption within the organization	2024 Sustainability Report / Performance data p. 53	7.2, 7.3, 7.a, 13.1, 13.2
	302-3 Energy intensity	2024 Sustainability Report / Performance data p. 53	13.1, 13.2
	302-4 Reduction of energy consumption	2024 Sustainability Report / Performance data p. 53	13.1, 13.2
	302-5 Reductions in energy requirements of products and services	2024 Sustainability Report / Product environmental impacts pp. 28–31 2024 Sustainability Report / Performance data p. 53	7.2, 7.3, 7.a, 13.1, 13.2

GRI Standard	Description	Reference/Disclosure	Alignment to the SDGs[14]
Emissions			
GRI 305: Emissions 2016	305-1 Direct (Scope 1) GHG emissions	2024 Sustainability Report / Performance data p. 53	13.1, 13.2
	305-2 Energy indirect (Scope 2) GHG emissions		
	305-3 Other indirect (Scope 3) GHG emissions		
	305-4 GHG emissions intensity		
	305-5 Reduction of GHG emissions		
Waste			
GRI 306: Waste 2020	306-2 Management of significant waste-related impacts	2024 Sustainability Report / Performance data p. 53 2024 Sustainability Report / Product environmental impacts pp. 28–31	12
Employment			
GRI 401: Employment 2016	GRI 401-1 New employee hires and employee turnover	2024 Sustainability Report / Performance data p. 54	5.1, 5.5, 8.5, 10.2, 10.3, 10.4
Training and education			
GRI 404: Training and education 2016	404-2 Programs for upgrading employee skills and transition assistance programs	2024 Sustainability Report / Cybersecurity skills gap pp. 37-42 2024 Sustainability Report / Employee awareness and engagement p. 27	8.6, 8.8
Diversity and equal opportunity			
GRI 405: Diversity and equal opportunity 2016	405-1 Diversity of governance bodies and employees	2024 Sustainability Report / Performance data p. 54 2024 Proxy Statement p. 18	5.1, 5.5, 8.5
Supplier social assessment			
GRI 414: Supplier social assessment 2016	414-1 New suppliers that were screened using social criteria	2024 Sustainability Report / Performance data p. 52	
GRI 415: Public policy 2016	415-1 Political contributions	Public policy p. 50	

14. This GRI index references SDGs that directly and indirectly align with Fortinet's priority topics.

SASB INDEX

The following index maps our disclosures to the Sustainability Accounting Standards Board (SASB) indicators in the 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**	2024 Sustainability Report / Performance data p. 53
	Discussion of the integration of environmental considerations into strategic planning for data center needs	**TC-SI-130a.3**	2024 Sustainability Report / Product environmental impacts pp. 28–31 2024 Sustainability Report / Climate strategy pp. 25–27 2024 Sustainability Report / Sustainable operations pp. 25–27 2024 Sustainability Report / Performance data p. 53
Data privacy & freedom of expression	Description of policies and practices relating to behavioral advertising and user privacy	**TC-SI-220a.1**	Privacy Policy
Data security	Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards	**TC-SI-230a.2**	2024 Sustainability Report / Information security and data privacy pp. 47 – 49 Certifications list: ISO 27001 certification SOC2 Type II examination HIPAA examination TISAX certification ISMAP certification ENS certification Up to date certifications can be found here **Fortinet PSIRT Policy** based on recognized industry standards including ISO 29147 (Vulnerability Disclosure) and ISO 30111 (Vulnerability Handling). For product compliance, Fortinet is currently auditing compliance to the controls within the following standards: NIST ST.SP.800-53 NIST ST.SP.800-160 NIST ST.SP.800-218 **Federal Information Processing Standard (FIPS):** FIPS 140-2 Level 1 (FortiOS 6.4 / 7.0) FIPS 140-2 Level 1 (FortiOS VM 6.4/ 7.0) FIPS 140-2 Level 1 (FortiManager 6.2) FIPS 140-2 Level 1 (FortiAnalyzer 6.2) FIPS 140-2 Level 2 (FortiOS 6.4/7.0) FIPS 140-3 Level 1 (FortiClient 7.0) **Network Device collaborative Protection Profile (NDcPP):** NDcPPv2.2e (FortiMail 7.4) NDcPPv2.2e (FortiAnalyzer 6.2) NDcPPv2.2e (FortiManager 6.2) NDcPPv2.2e + Firewall + VPN (FortiOS 6.4/ 7.0) **IPv6 Ready Logo Phase-2:** IPv6 (FortiOS 7.4) IPv6 (FortiSwitch 6.2) **USGv6 Program (Compliant to ISO/IEC 17025):** USGv6 (FortiOS 7.6.0) USGv6 (FortiOS 7.4.4) USGv6 (FortiOS 7.4.0) USGv6 (FortiOS 7.2.4) USGv6 (FortiOS 7.0.6) USGv6 (FortiOS 6.4)
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**	2024 Sustainability Report / Performance data p. 54
Managing systemic risks from technology disruptions	Description of business continuity risks related to disruptions of operations	**TC-SI-550a.2**	2024 Sustainability Report / Addressing cybersecurity risks to society pp. 12-21

Verification Opinion

Submitted to:	Fortinet
Verification Body:	TÜV SÜD America, Inc. 743 Horizon Court, Suite 385 Grand Junction, CO 81506 (970) 241-9298
Lead Verifier:	Pilar Gutierrez Pilar.Gutierrez@tuvsud.com
Submitted:	4/1/25

TÜV SÜD America, Inc. (TÜV SÜD) conducted the verification of the Fortinet's 2024 GHG inventory according to the requirements found in ISO 14064-3:2019, 14065:2020, & 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 and global operations.
- GHG statement: Calendar Year 2024
- 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
  - Other supplemental GHG methodologies including the US EPA Center for Corporate Leadership GHG Inventory Guidance and The Climate Registry's General Reporting Protocol

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.

In compliance with the requirements of ISO 14065:2020, the client may reproduce and distribute TÜV SÜD's verification opinion without TÜV SÜD's prior authorization, as long as the verification opinion is reproduced in its entirety, including the date.

Lead Verifier

Pilar Gutierrez

Independent Reviewer

Garrett Heidrick

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, among others: 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 manmade 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.

FORTINET

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

www.fortinet.com