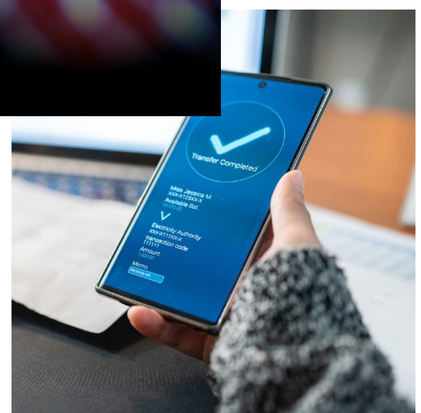
2023 Sustainability Report



FORTINET®

Table of contents

Letter from our CEO

As we reflect on 2023, it's clear that the world continues to evolve at an unprecedented pace. New opportunities are accompanied by a myriad of issues that could put our future at stake. The acceleration of the adoption of generative AI offers innovative prospects but also raises concerns about data privacy, cybersecurity, and inclusivity. Geopolitical instability underscores the urgent need for global cooperation to combat cyber warfare and espionage. Continued inequality and disillusionment among workers and citizens emphasize the need to foster inclusive workplaces and communities, address socio-economic disparities, and promote equitable opportunities. Finally, climate change and the transition to sustainable energy, pressured by rapidly evolving regulations and increased stakeholder demands, compel organizations to decarbonize their businesses and operations.

A commitment to sustainability is critical to overcoming these challenges and any organization's long-term success and resilience. And now, given our transition to a globally connected digital economy, cybersecurity has become essential for our society and its economy, making it the defender of sustainability.

Fortinet's sustainability strategy is built on core priorities: talent development, diversity, equity, and inclusion (DEI), industry collaboration, technology innovation, and decarbonization. These priorities are central to our social responsibility and help us pursue our vision of making a digital world you can always trust.

Throughout this report, we address Fortinet's objectives and progress achieved in 2023, validated by Fortinet again being named a member of the Dow Jones Sustainability Indices. I am also proud to share that we are now a member of the UN Global Compact, adhering to its principles in the areas of human rights, labor, environment, and anti-corruption. This membership further strengthens our commitment to sustainability and the Sustainable Development Goals (SDGs).

This past year, we have continued focusing on reducing cybersecurity risks to our society while reducing our products' environmental impacts. This includes continuously improving the energy efficiency of Fortinet products while maximizing performance. These efforts are critical to helping protect our customers' businesses while meeting their climate goals. We also helped drive industry innovation through additional crowdsourcing initiatives, empowering individuals to contribute to our innovation efforts while working with industry pioneers to address future and emerging opportunities and threats, such as quantum computing.

Partnering with international, regional, and national law enforcement agencies and our cybersecurity peers is another priority we have pursued to ensure a safe digital world. In 2023, we forged partnerships with private and public entities and expanded our efforts to combat cybercrime through collaborations such as the Joint Cyber Defense Collaborative (JCDC) and the WEF Cybercrime Atlas Project. As part of those efforts, we contributed to the arrest of 15 cybercriminal groups.

We have also continued to address the need for more cyber awareness among the general public and the growing cybersecurity talent gap, which represent significant obstacles to ensuring a secure, reliable and sustainable digital future. We expanded our support to educational institutions last year by providing free access to a variety of curricula, fostering online safety awareness, and nurturing future cybersecurity professionals among students. I am pleased to share that we now stand at 43% of our goal to train one million people in cybersecurity by 2026.

We have also increased our efforts to promote diversity and inclusion, teamwork, and continuous learning within our organization. These efforts have earned us awards from Great Place to Work and Glassdoor and the Diversity, Equity, and Inclusion Excellence Award from the HR Miami organization.

We value the trust of our stakeholders and continue to foster a business environment characterized by integrity, compliance, privacy, and respect for human rights. The launch of the Fortinet Trusted Center last year testifies to our transparency and accountability, providing our customers with visibility into our information security and data privacy programs.

Finally, we remain committed to our ambitious environmental sustainability goals, which consist of achieving net zero greenhouse gas emissions across our owned operations by 2030, and across our entire value chain by 2050. Our focus on renewable electricity led to important investments in green energy sources, as shown by the opening of our new garage space in Sunnyvale, whose solar panels will cover the power needs of our headquarters and nearby sites.

"A commitment to sustainability is critical to overcoming these challenges and any organization's long-term success and resilience."

Later this year, we will submit our decarbonization plan to the Science-based Targets Initiative (SBTi) for validation.

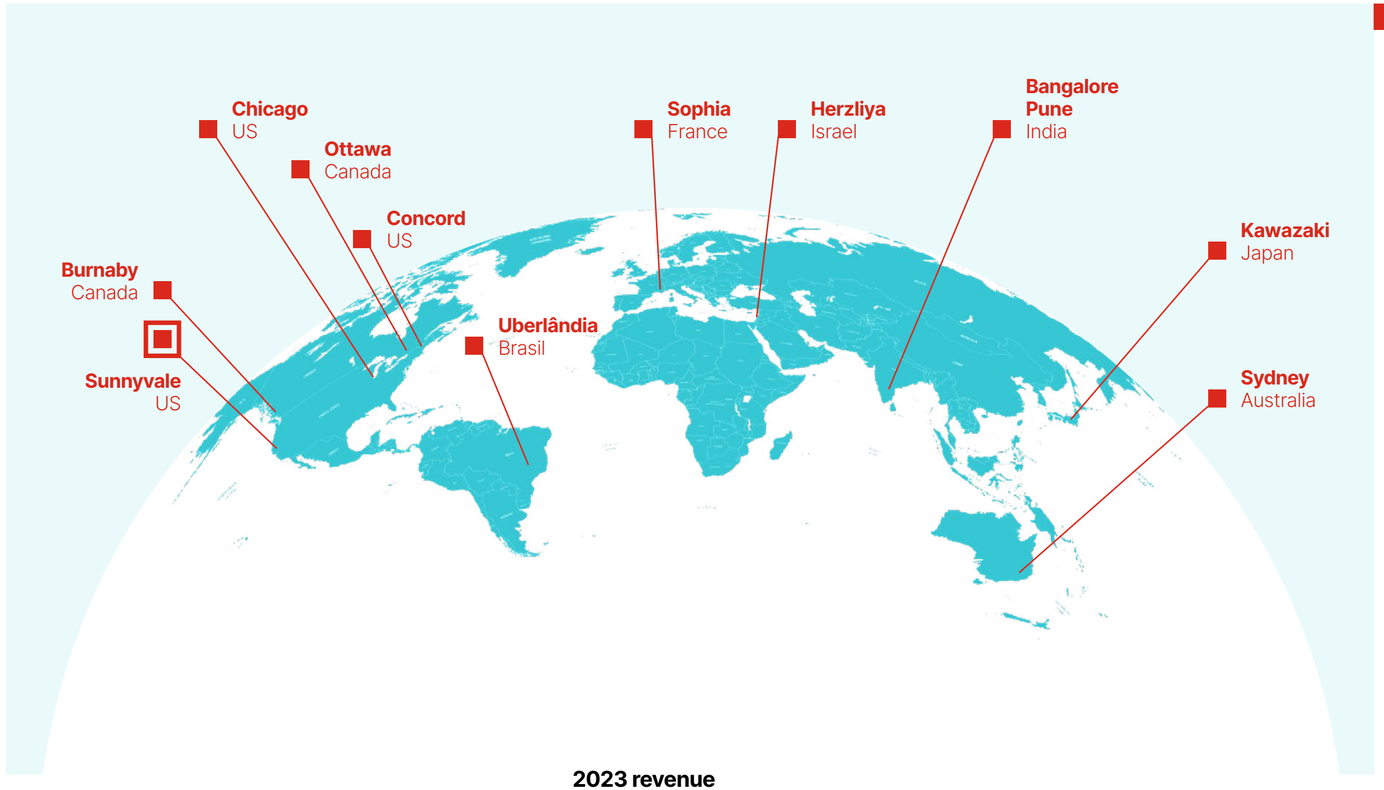
Moving forward into 2024, we remain steadfast in our commitment to sustainability, knowing that our continued collaboration with our employees, partners, customers, and suppliers is necessary to achieve our shared ambitions and to effectively tackle the world's most critical challenges.

Ken Xie
Fortinet Founder, CEO and Chairman of the Board

Who we are

Making possible a digital world you can always trust.

For over 20 years, Fortinet has been a driving force in the evolution of cybersecurity and its convergence with networking. We deliver cybersecurity everywhere our customers need it, and we are committed to addressing cybersecurity risks to society, diversifying cybersecurity talent, respecting the environment, and promoting responsible business across our value chain.



Corporate headquarters:

Sunnyvale
California, U.S.A

Number of locations:
90+

Founded:
OCTOBER
2000

Included in:

Nasdaq
NASDAQ-100 INDEX

STANDARD &POOR'S 500

Member of
Dow Jones Sustainability Indices
Powered by the S&P Global CSA

Fortinet employees in FY23:
13,568

Global customer base:
730,000+

Active channel partners:
100,000+

2023 revenue (as of Dec 31, 2023):
$5.30B

Cash and investment:
$2.44B

Market capitalization (as of Dec 31, 2023):
$44.5B

R&D investment in FY23:
$613.8M

Patents:
1,299

Sustainability impact

Building a reliable digital world you can trust every day is the cornerstone of contributing to just and sustainable societies. We believe it is our corporate social responsibility to turn this vision into reality. That's why we act on developing sustainable and innovative cybersecurity solutions while ensuring positive social impact and responsible business practices.

Promoting responsible business

47
information security certifications and examinations
(30 renewed and 17 new ones completed)

100%
of distributors and key contract manufacturers
completed Fortinet's training on compliance and business ethics

1
Trust Resource Center for customers to learn more about our privacy and information security practices

Addressing cybersecurity risks to society

11
new products
and cloud-hosted services introduced

2 **new memberships:**
Network Resilience Coalition — Making Networks Stronger, Together
JCDC

$40M
prevented
in financial losses

15
cybercriminal groups arrested through **the INTERPOL Gateway program**

Respecting the environment

100%
renewable electricity in 80% of our owned sites

62%
average **reduction** in product energy consumption

~455
tons of CO_2 emissions **avoided** through eco-friendly packaging manufactured

CLIMATE CHANGE PLEDEGE

Net zero by 2030
Scope 1 & Scope 2 emissions

SBTi committed

Growing an inclusive cybersecurity workforce

CYBERSECURITY SKILLS PLEDGE

1 million people
trained in cybersecurity (2022-2026)

213,440
people trained in cybersecurity in 2023

340+
of our leaders trained on **fostering inclusion**

6
recognitions as one of **the best places to work**

CSR governance

Fortinet CSR governance is a robust, guiding strategy that tracks progress and swiftly implements projects and training across all levels. It ensures the cohesive and collaborative deployment of our sustainability strategy, engaging our entire organization throughout the process.

Board

Board of Directors

- Lead sponsor of company CSR
- Oversees and approves CSR commitments

Social Responsibility Committee
- Oversees sustainability strategy, covering environmental, social and governance (ESG) aspects, on a quarterly basis

Human Resources Committee
- Oversees Diversity, Equity, and Inclusion (DEI) matters

Audit Committee
- Oversees information security

Executive Team

- Validates strategy, approves targets, and monitors execution
- Provides sponsorship to integrate CSR into the business operations and decision-making processes

Management

CSR Committee

- Defines CSR priorities, objectives, and strategy
- Drives and oversees the company's CSR initiatives
- Provides oversight to the Executive Team and SR committee of the Board
- Ensures appropriate internal and external disclosures related to CSR matters
- Members include cross-functional management representatives – CSR Champions. They champion Fortinet's priority issues and take ownership of CSR roadmaps specific to their respective subject matter areas

CSR Team

- Organizes overall CSR activity for Fortinet, leads strategy development, and oversees sustainability reporting
- Directly engages at all levels of the organization in executing CSR strategy

Business units

- Legal & Corporate Affairs
- Finance
- Sales & Channel
- Marketing
- Information Security
- Human Resources
- Customer Success & Support
- FortiGuard
- Facilities
- R & D
- Supply Chain
- Training

CSR Champions own specific CSR issues. They define and are accountable for CSR action plans and operational goals

They collaborate with functional leaders and teams to implement, measure and report progress

CSR Ambassadors – volunteer employees – play a role in educating and engaging Fortinet's broader workforce on sustainability

Stakeholder engagement

At Fortinet, we are determined to implement a sustainability strategy in line with the expectations of our stakeholders, integrating their valuable input to deploy a relevant and effective sustainability approach. In 2021, we conducted a materiality assessment to identify the most important topics to our stakeholders, laying the foundations for our approach. For this assessment, we consulted a broad range of stakeholders, including Fortinet employees, investors, suppliers, partners and customers. Signed off by the Fortinet Board of Directors, we aim to refresh this analysis approximately every three years as it guides our long-term sustainability roadmap and helps define key performance indicators to track progress.

	Customers	Employees	Industry associations and government	Communities and NGOs	Partners	Shareholders & investors	Suppliers
HOW WE ENGAGE	— Request for proposals (RFPs) — Customer meetings — Sustainability assessments: cyber risk, data privacy, environmental, compliance, etc. — Digital marketing and communications — Annual Fortinet conference — Fortinet and third-party-led events — Training and certification programs — MoUs and partnerships — Service delivery and support	— Quarterly employee all hands — Awareness campaigns — Fortinet intranet and portals — Mentoring — Employee Resource Groups (ERGs) — Onboarding — Company policies and relative training — Leadership training & workshops — Department and manager-employee meetings and trainings	— Collaboration with TSIA, ETSI, MEF, WiFi Alliance, 5G-ACIA, and ISA — Driving industry best practices through founding membership such as the Network Resilience Coalition and participation in NIST National Cybersecurity Center of Excellence (NCCoE) — Founder of Cyber Threat Alliance and driving daily trusted sharing of threat intelligence with the private sector — Research partner with MITRE Engenuity working on industry projects and frameworks for threat informed defense — Collaboration with third-party vendors and industry peers on zero-day threat research and responsible disclosure — Information sharing with government security agencies e.g., INTERPOL — Information sharing and incident coordination with agencies such as CISA JCDC, and regional computer emergency response teams (CERTs) — Engagement with schools — Engagement with industry analysts and product validation/verification organizations	— Partnerships with education outreach organizations — Supporting academia and governments on cybersecurity awareness and curriculum — Programs and partnerships focused on upskilling, mentoring, donations, and volunteering activities/ employee giving — UN Global Compact membership — Global initiatives with the World Economic Forum Center for Cybersecurity, Partnership against Cybercrime and Cybercrime Atlas — Social initiatives such as volunteer time off, donations	— RFPs — Meetings — Marketing/communication campaigns — Trainings — Partner code of conduct — Vendor risk assessment — Events: Partner-led events and Fortinet conferences and Fortinet-led events — Partner review performance	— Sustainability reporting — 1:1 engagement with shareholders — Analyst calls — 10K — Proxy — Sustainability assessments	— Training — Supplier code of conduct — Supplier assessments/ reviews — Supplier meetings — Cyber risk and data privacy assessments
TOPICS OF INTEREST	— Climate change and greenhouse gas (GHG) emissions — Product carbon footprint and product lifecycle — Product environmental impacts — Human rights — Data privacy and security — Cybersecurity skills gap/ awareness culture — Sustainable supply chain, including supply chain risk management, compliance, and certifications — Product adoption and issue resolution	— Women in cybersecurity and women in leadership positions — Diversity and inclusion with a focus on women, LGBTQIA+, and people with disabilities — Mental health — Climate change — Environmental management and eco-friendly initiatives — Product sustainability — Sustainability strategy and awareness — Compliance — Ethical behavior — Cybersecurity awareness	— Adoption of standards and interoperability across the industry — Investigation of global security incidents — Threat intelligence — Cybersecurity education — Product security and best practices	— Cybersecurity education and hands-on training — Talent diversity with a focus on under-represented groups — Women in Science, Technology, Engineering, and Mathematics (STEM) — Cybersecurity skills gap — Digital divide — SDGs	— Sustainability approach and goals — Compliance and business ethics — Product environmental compliance — Carbon footprint of products in use — E-waste — Human rights — Quality and compliance to various program levels	— Sustainability strategy and progress — Climate change — Environmental management — Governance — DEI (Diversity, Equity and Inclusion) — Human rights — Innovation — Business ethics	— Sustainability approach and goals — Sustainable product design and manufacturing — Business ethics — Human rights — Regulatory and compliance — Sustainable supply chain, including supply chain risk management, compliance, and certifications

Reporting frameworks

Fortinet is continually working to enhance its reporting practices by adopting globally recognized frameworks for performance disclosure. Those include the Global Reporting Initiative (GRI) standards, the Sustainability Accounting Standards Board (SASB) standards, the Taskforce on Climate-related Financial Disclosures (TCFD) and CDP. Our GRI, SASB and TCFD indexes can be found in the Appendix of this report.

In anticipation of the increasing prevalence of mandated ESG (Environmental, Social, and Governance) disclosures, Fortinet takes a proactive stance, diligently anticipating future regulations. This dynamic approach aligns with industry trends and showcases Fortinet's commitment to upholding the highest standards of transparency in its operations and sustainability reporting.

United Nations reporting frameworks

United Nations Global Compact (UNGC)

In 2023, Fortinet joined the globally recognized voluntary leadership platform for developing, implementing, and disclosing responsible practices. By doing so, Fortinet further pledges to drive sustainable business practices by following the UNGC's ten principles in the areas of human rights, labor, environment, and anti-corruption. Participation in the UN Global Compact requires companies to report yearly on their commitment to the universal sustainability principles and development goals. Launched in 2000, the UN Global Compact is the world's largest corporate sustainability initiative, with over 15,000 organizations and 3,000 non-business signatories based in over 160 countries.

United Nations Sustainable Development Goals SDGs

The United Nations Sustainable Development Goals (UN SDGs) provide an essential global framework to drive social, environmental, and economic progress. Fortinet has identified six UN SDGs where it can have a positive impact: Quality Education (4), Gender Equality (5), Affordable and Clean Energy (7), Decent Work and Economic Growth (8), Reduced Inequalities (10), and Climate Action (13). In this report, UN SDG icons help refer to how Fortinet's sustainability actions contribute towards SDGs.

ESG RATING AGENCY SCORES

Dow Jones Sustainability Indices

Member of
Dow Jones Sustainability Indices
Powered by the S&P Global CSA

2023 DJSI World & North America

Ecovadis

SILVER 2023 ecovadis Sustainability Rating

CDP

CDP
DRIVING SUSTAINABLE ECONOMIES

Score B-

MSCI

MSCI ESG RATINGS BBB
CCC | B | BB | BBB | A | AA | AAA

Sustainalytics

Rated MORNINGSTAR | SUSTAINALYTICS

ESG risk rating of 18.9

Sustainability in our business operations

Since embarking on our sustainability journey three years ago, we have looked ahead to understand where and how we can contribute to broader societal challenges while bolstering the resilience and longevity of our business and creating value for our stakeholders. Fortinet's sustainability approach was defined through a formal materiality assessment, reflecting the priority issues that matter most to our business and stakeholders: addressing cybersecurity risks to society, diversifying cybersecurity talent, respecting the environment, and promoting responsible business across our value chain.

At Fortinet, we believe fostering collaboration for a sustainable future must start from within. That's why, in 2023, we intensified our efforts to embed sustainability practices into our operations further and engage every business unit. For instance, we conducted workshops for our R&D and marketing departments to educate our teams and develop action plans for integrating sustainable practices into our products and events. We also introduced e-module training on sustainability for all employees.

These modules raise awareness about driving sustainable business in the cybersecurity industry, covering key issues such as climate change and other environmental challenges, along with our company's sustainability approach and strategy.

Sustainability at Fortinet is gradually becoming a transformational force that engages every department, drives our innovation, reinforces our commitment to business ethics, and fosters a culture of engagement within the company.

Q&A

Michael Xie

Fortinet co-founder, president & CTO. Chairman of the Social Responsibility Committee of the Board

What is Fortinet's approach to embedding sustainability in technology today?

Fortinet firewalls are the most deployed in the world. Our mission is to secure people, devices, and data everywhere. And along with that, we hold an important responsibility to reduce the environmental impact of our products, including their carbon footprint, especially in the customer use phase. That's why our focus on delivering more sustainable products is a priority. Through over 20 years of processor innovation and development, we have integrated multiple security and networking functions into a single, highly energy-efficient platform. Our engineering team works hard to ensure that each new generation of our products uses less energy, space, and cooling to reduce our GHG emissions and help our customers meet their broader sustainability goals.

While energy efficiency is at the core of Fortinet's product design, we're committed to doing more. That's why, in 2023, we trained our engineering teams on product lifecycle and eco-design principles to further embed sustainability into technology innovation. This includes considering pathways for reusability, recyclability, waste reduction, responsible sourcing, and the use of renewable materials in products and packaging.

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. Our corporate governance practices aim to ensure accountability to meet our responsibilities across our entire value chain. Trust with our stakeholders is of paramount importance to us. We are committed to implementing the best practices internally for information security and privacy to protect our own systems and the data of our employees and customers.

2023 highlights

1

Trust Resource Center for customers to learn more about our privacy and information security practices

47

information security certifications and examinations

100%

of our distributors and key contract manufacturers completed Fortinet's training on compliance and business ethics

SDGs

Business ethics and human rights

Committed to ethical business practices and legal compliance, we prioritize responsible business through robust governance. Our commitment spans our entire value chain, underscoring our social responsibility and emphasis on human rights protection. By designing and delivering products ethically, we firmly believe in our ability to make a positive impact and thrive as a force for good.

Setting a robust framework

Fortinet strives to foster a business environment characterized by integrity, compliance, and respect for human rights. Our comprehensive approach to governance, codes of conduct, and engagement with employees, partners, and suppliers reflect our dedication to promoting ethical business practices in the cybersecurity industry.

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

In 2023, we established a risk management steering committee to enhance our anti-corruption program. This committee plays a vital role in identifying and mitigating risks associated with third parties and aligning the organization's efforts to maintain the highest ethical standards wherever it operates.

Audits and accountability
Fortinet employs focused audits as systematic and proactive measures to ensure compliance with its ethical standards. In FY23, Fortinet conducted several audits, notably for its Global Trade Compliance program and supply chain, covering company governance, import/export standards, conflict material standards, employee conditions, returns, and product safety. These evaluations testify Fortinet's commitment to accountability and continuous improvement.

Responsible minerals sourcing policy

In line with the Responsible Minerals Initiative (RMI), which aims to establish industry-wide governance standards for responsible minerals, Fortinet reviewed its sourcing policy in 2023 to align with global standards and regulations. Additionally, a new statement on modern slavery for suppliers in Australia has been introduced to comply with recent regulations.

Fostering a strong business ethics culture

Central to this commitment is the prioritization of compliance and ethics training, serving as a fundamental lever both internally and with third parties. This multifaceted strategy ensures that Fortinet's entire collaborative ecosystem remains well-versed in ethical and regulatory obligations, thereby contributing to the overall integrity and resilience of its business ethics culture.

Fortinet employees must complete annual ethics and compliance training as part of this ambition. We have additional requirements for our sales team to complete additional sales compliance training every six months and provide a quarterly compliance certification.

We also closely collaborate with our suppliers and vendors to ensure they fully meet our business ethics standards, reinforcing a comprehensive approach to ethical business practices across our value chain. In 2023, Fortinet's top contract manufacturers, representing >90% of our spend, completed the Fortinet Vendor/Supplier Compliance Training. This was complemented with 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 export/import compliance regulations.

All our distributors and channel partners are also integral to this effort, engaging in mandatory compliance and ethics training.

We ensure that our employees and third parties take compliance training seriously, as evidenced by our current 98% employee and 100% distributor completion rates. To achieve this, we continuously enhance our training methods, incorporating elements such as gamification, quizzes, videos, and checks on learning.

FY23 compliance and business ethics training completed by:

100% of Fortinet **key contract manufacturers***

100% of Fortinet **distributors globally**

Making our training as immersive as possible is vital to empowering our stakeholders on these issues. Our responsibility is also to make sure everyone knows where to go for support and how to report a concern.

Reporting concerns
Our ambition to promote a strong culture of integrity means ensuring that every individual is not only expected to act ethically but also empowered to voice concerns without fear of retaliation. Any employee or third-party who suspects or is aware of a violation of Fortinet's code or policies may raise a concern through various avenues outlined in the Fortinet Whistleblower policy. This includes the option to report concerns confidentially and, if desired, anonymously, to our third-party whistleblower hotline. A dedicated team promptly investigates allegations, taking necessary actions to mitigate and remediate any adverse impacts.

To enhance accessibility, we upgraded our telephony options in 2023, ensuring that local languages are available in our larger offices along with direct phone numbers for reporting incidents. This improvement streamlines the reporting process, offering live telephone language interpretation in over 150 languages.

This comprehensive approach underscores our dedication to maintaining a workplace where concerns are addressed with diligence and fairness.

* Representing >90% of spend.

Business ethics and human rights

Respecting human rights

We are dedicated to ensuring that the fundamental rights of people involved in our operations throughout the value chain are not violated. Fortinet's Global Human Rights policy outlines the company's commitment to respecting the human rights of all stakeholders, including the users of our products and services. The policy applies to all employees, partners, and suppliers globally and 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.

Fortinet also comprehensively incorporates human rights language into key documents such as license agreements, product datasheet templates, and codes of conduct for partners and suppliers. This thorough integration extends to our educational initiatives, where human rights are incorporated into mandatory training programs. This demonstrates our commitment to raising awareness and understanding throughout our organization and value chain. Fortinet also updates and enhances its Global Human Rights policy, adapting to the evolving landscape of human rights risks.

Ensuring responsible product use

Designing, developing, selling, and managing products and services in ways that respect human rights is paramount for us. That is why Fortinet fully adheres to the guidance as set out by the UN's Guiding Principles on Business and Human Rights and is also aligned with the laws of the countries in which it operates. Doing so ensures a responsible and respectful approach to our activities throughout our entire organization. Our Global Human Rights policy holds a global scope, exemplifying Fortinet's commitment to upholding the rights of various stakeholders within our value chain.

Evaluating and managing risks

Fortinet prioritizes robust risk management by implementing a meticulous screening process for its partners and suppliers. This involves two-step verification, sophisticated third-party diligence tools, and continuous monitoring in high-risk areas. Criteria such as human rights, the U.S. Foreign Corrupt Practices Act, and sanctions lists are applied to assess direct suppliers and vendors. In 2023, Fortinet conducted a proactive anti-corruption evaluation of top distributors to ensure adherence to ethical practices, with close collaboration in addressing any reported non-compliance. Fortinet's commitment to risk mitigation includes an agile response and resolution process, reinforcing its dedication to maintaining ethical standards worldwide.

Diego Hernandez

Senior Director, Global Trade Compliance and Member of the CSR committee at Fortinet

"Fortinet champions ethical practices at every level, enforcing compliance through contractual agreements, comprehensive training with our suppliers and partners, a continuous engagement with them to ensure they comply, and a robust reporting system."

Sharing higher human rights expectations

Vendors/suppliers 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) signed on Dec. 23, 2021. Fortinet commits to investigating and rectifying non-compliance with disciplinary actions, including termination when necessary.

Information security and privacy

Privacy and information security are not only an integral part of our business but also vital to our stakeholders' continued trust. Our commitment to data privacy and Information security is embedded in every part of our business and every phase of our product development, manufacturing, and delivery processes.

Keeping the data of Fortinet, its employees, and customers safe

Our Information Security Management System (ISMS) undergoes continuous enhancements, helping ensure the confidentiality, integrity, and availability of Fortinet systems and our customers' data. This commitment is reflected in Fortinet's robust oversight, processes, and procedures.

Fortinet's governance structure, led by our Board of Directors, actively oversees and emphasizes cybersecurity as a critical 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.

Our comprehensive and robust ISMS incorporates policies, programs, standards, procedures, and controls aligned with industry standards such as the ISO 27001/2 and the NIST 800-53/161 frameworks and data privacy laws such as GDPR (General Data Protection Regulation) and CCPA (California's Consumer Privacy Act). Other standards may be adopted to augment these to satisfy unique requirements 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 continuous suitability, adequacy, and effectiveness. Changes in policies are communicated to all employees.

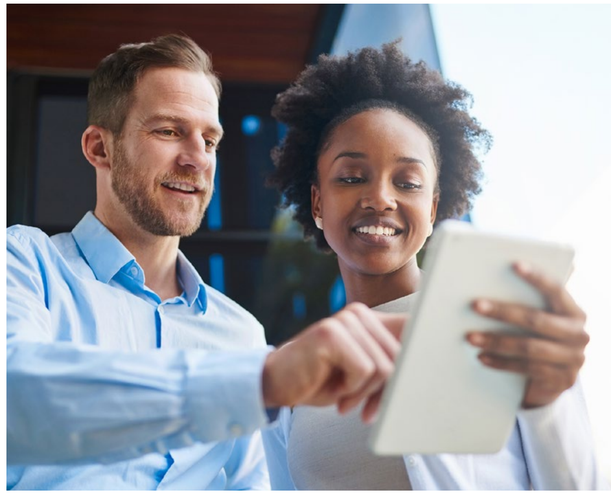
As an early adopter of its own technology, in 2023, Fortinet continued to expand the implementation of its products and solutions and adopted new capabilities and features to protect its network while providing early feedback to the R&D organization that can help further strengthen Fortinet's cybersecurity solutions. In addition, Fortinet applies security best practices in the product development process by adhering to leading standards such as NIST 800-53, NIST 800-160, NIST 800-218, US EO 14028, UK TSB. We also have robust product scrutiny—internally and externally—at all stages of our product development lifecycle, from design through end of life. When issues occur, Fortinet promptly remediates them following a comprehensive response plan.

The company's proactive approach to fostering cyber awareness among its employees is also evident in initiatives like the 2023 Information Security Awareness Compliance training and periodic phishing simulation campaigns.

We provide customer assurance concerning our information security and data privacy practices through certifications and independent assessments based on internationally recognized standards. In 2023, Fortinet reaffirmed its commitment to cybersecurity by renewing and expanding the ISO 27001 certificate and the scope of SOC2 and HIPAA examinations.

Employee training

Fortinet requires successfully completing mandatory security awareness training at the time of hiring and at least annually thereafter. This training includes videos, gamification, quizzes, and additional techniques. Periodic phishing campaigns are conducted to educate Fortinet employees about various attack techniques, including social engineering. Developers are also required to complete secure code development training, and specialized training is required from employees in IT and information security roles.



2023 information security and privacy measures

- CSA STAR
- GDPR
- HIPAA
- ISO 27001
- ISO 27001 SoA
- ISO 9001
- SOC 2
- ISMAP
- TISAX
- VPAT

Information security certifications and examinations:

30 renewed

17 new ones completed

Information security and privacy

Protecting our customers with supply chain cybersecurity

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

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

- **Identify**: Identify potential risks to the supply chain
- **Protect**: Build controls to help protect the supply chain from risks
- **Detect**: Detect issues early, giving more time and options to respond
- **Respond**: Respond as quickly as possible to mitigate the vulnerability or threat
- **Recover**: Recover with minimal impact to customers.

Q&A

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

How does Fortinet identify and address information security risks?

We have implemented a comprehensive cybersecurity risk management approach to identify new and evolving threats and vulnerabilities in our infrastructure and digital assets and drive mitigation efforts and best practices. This approach is consistently applied throughout the organization. It leverages various techniques, including proactive threat intelligence gathering and threat hunting exercises, secure design and architecture reviews, scans to identify vulnerabilities and misconfigurations, penetration tests, and internal audits. All employees and contractors undergo information security awareness training, ongoing phishing campaigns, and exercises to test the organization's readiness to detect and respond to security threats. Fortinet has also completed preparations to comply with the new SEC regulation, showcasing its commitment to compliance with new regulatory requirements.

Fortinet Trusted Supplier Program

In 2023, Fortinet extended its Trusted Supplier Program to additional supply chain partners. The 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 United States Government for securing the Information and Communication Technology Services (ICTS) supply chain. This program was also 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 United States Government directives. Fortinet conducts a thorough security assessment of its TSP partners to ensure they satisfactorily comply with applicable controls established by NIST SP 800-161 and work side-by-side with them to remediate gaps and monitor their security posture.

Fortinet Trust Resource Center

This innovative platform, launched in 2023, offers our customers transparency regarding our information security and data privacy programs. Customers can easily access a wealth of 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. Learn more at:
↗ **https://trust.fortinet.com**

Protecting 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 Fortinet's privacy team, we have established a cross-functional committee consisting of Fortinet privacy champions across different business units, including R&D, product management, sales, marketing, etc., who meet regularly to review privacy practices and policies, stay informed of any legislative developments, keep our processes updated, and address privacy, comments, and questions seamlessly to help ensure our employees remain updated and aware of data privacy matters.

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 with it (you can read Fortinet's GDPR approach).

Our employees are required to complete mandatory privacy training at the time of hiring and at least annually thereafter. We also conduct privacy review of our third-party vendors and incorporate 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.

Addressing cybersecurity risks to society

As digitization takes over 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. At Fortinet, we are committed to advancing the industry through security innovation, public-private cooperation, and customer success to strengthen the collective defense against cyber adversaries and contribute to a more secure and sustainable society.

2023 highlights

11
new products and cloud-hosted services introduced

2
New memberships

Network Resilience Coalition
Making Networks Stronger, Together

JCDC

Contributed to the arrest of
15
cybercriminal groups

and **the prevention of**
$40M
in financial losses through the INTERPOL Gateway program

SDGs

8 DECENT WORK AND ECONOMIC GROWTH

Securing the digital world, a global priority

Billions of people around the world use digital services every day. In fact, in our modern world, everything and everyone is digitally connected to apps, data, purchases, services, communications, and more. Digital transformation, accompanied by the widespread adoption of artificial intelligence, has become an integral part of every company's journey, regardless of its size or industry. Critical infrastructures and services, such as finance, telecommunications, emergency response, energy, healthcare, transportation, water supply, and food systems, have all embraced digitization.

While digital transformation brings many benefits, it also introduces new risks. These include new forms of disruptive cybercrime, additional vulnerabilities due to the expanded attack surface, the increasing complexity of managing and securing modern infrastructures, and a threat landscape that shows no signs of slowing in terms of sophistication, frequency, and complexity. Daily news on data breaches, ransomware, and malware attacks underscore that every individual and organization is a potential cybercrime victim. Any disruption or failure in an organization or service can result in economic hardship and the loss of essential services and safety.

The World Economic Forum's Global Risks for 2024 revealed that cyber insecurity ranks among the top five short-term risks for the first time in a decade. For 39% of respondents, cyberattacks remain a major concern in the overall outlook, emerging as a top-three concern for both government and private-sector respondents. In light of these challenges, securing the digital world is paramount and positions cybersecurity as a societal issue, which requires innovation, agility, and collaboration to counter today's escalating cyber risks.

Global risks ranked by severity
(over the next two years)

WORLD ECONOMIC FORUM

1	Misinformation and disinformation
2	Extreme weather events
3	Societal polarization
4	Cyber insecurity
5	Interstate armed conflict

Source: World Economic Forum Global Risks/Perception Survey 2023-2024.

Innovating for a safe internet

Innovation within cybersecurity is the only way to keep up with the ever-evolving threat landscape. Throughout its more than 20-year history, Fortinet's commitment to remaining at the forefront of innovation has been a driving force in helping organizations digitally protect themselves. Our innovation has been based on the founding principles of the convergence of networking and security and the consolidation of point products into an integrated platform. Our continued focus on consolidation, automation, orchestration, scalability, and threat intelligence sharing has helped advance the industry and reduce complexity for all our customers.

Deeply committed to innovation

$613.8M
investment in R&D in 2023

1,299
patents

6
new products and

5
new cloud-hosted services introduced in 2023

Reducing complexity is a priority

Fortinet integrates a comprehensive suite of networking and security technologies into its Security Fabric platform to reduce the complexity of disparate security solutions. This integration spans a vast ecosystem of technologies and vendors, reducing operational complexity and ensuring compliance. Worldwide, FortiGuard acts as a driving force to ensure the industry is effectively collaborating to fight emerging global security risks.

700+
tech integrations

380+
Fabric-Ready partners (one of the industry's largest ecosystems)

Fortinet fuels its industry-leading innovation engine through a company culture that encourages and rewards innovative thinking. The success of this approach is evident in our 1,299 patents and 252 patents pending, demonstrating that our innovation continues unabated. In 2023 alone, Fortinet's R&D investments resulted in the introduction of six new products and five new cloud-hosted services to the market.

2023 major product launches and enhancements:

- **Secure networking:**
  Fortinet made significant strides in network security and secure connectivity innovation, particularly in the evolution of next-generation firewalls to a Hybrid Mesh Firewall framework and the development of the industry's most comprehensive security and networking platform. Fortinet also launched its Security Processor 5 (SP5) ASIC to accelerate networking and security convergence across network edges, along with the introduction of new, higher-performance FortiGate G-series appliances. ASICs continue to showcase Fortinet's dedication to sustainability, providing customers with power-efficient products with a smaller footprint to minimize environmental impact.
- **Unified SASE:**
  Fortinet introduced innovations across SD-WAN and SASE to ensure secure access for hybrid workforces across the internet, SaaS, and private applications. The company expanded its network reach to over 100 global locations through investments in its own SASE datacenter locations and strategic partnerships with providers such as Google Cloud. These innovations prioritize unified management and end-to-end digital experiences, enabling automated operations and network visibility for Fortinet customers. In addition, Fortinet expanded its flexible consumption model using FortiFlex to extend AI-powered security services across today's hybrid environments.
- **Security operations:**
  Fortinet announced enhancements across its security operations portfolio to improve its ability to automate detection and response thereby reducing the time to remediate security issues. Significant updates included new AI and Machine Learning capabilities and additional real-time response and automation capabilities to improve efficacy, increase effectiveness, and accelerate time to resolution of sophisticated attacks. In addition to technology, an expanded set of FortiGuard expert services, including SOC-as-a-Service, were introduced to uplevel the skill and efficiency of SecOps teamsand processes.

Carl Windsor

SVP - Product, Technology & Solutions, and Member of the CSR Committee at Fortinet

"Innovation is the lifeblood of Fortinet and we achieve this through empowerment of our employees to help drive the company forward on the journey towards a safer digital future, where each breakthrough is a shield against emerging threats."

Innovating for a safe internet

Fostering a strong innovation culture

Fortinet champions a culture of innovation by actively engaging everyone within the company through its crowdsourcing initiatives. These include:

- **FortiHours program**
  Specific to our research and development team, the FortiHours program dedicates time (generally on Friday afternoons) for crafting new ideas or tooling, with support and guidance from management.
- **FortiIdeas initiative**
  Open to all, this project facilitates the submission of broad product concepts and company suggestions, which are then submitted to Fortinet's Innovations Council.
- **Patent submission system**
  Fortinet enables the submission of potentially patentable innovations to a specific patent review board. This system is open to every Fortinet employee.
- **Feature request tool**
  This system allows anyone within the organization, from field personnel to customer feedback handlers, to propose new product features through the New Feature Request (NFR) process. This inclusive approach democratizes innovation, ensuring valuable insights and ideas come from all corners of the company. The system employs a unique mechanism where CTO dollars are used to crowdsource ideas, emphasizing the significance of contributions. This approach not only elevates noteworthy ideas but also encourages a diverse range of perspectives.
- **Customer Advisory Boards (CAB) & Xperts Academy**
  Fortinet invites VIP customers from major verticals (OT, Finance, Healthcare, etc.) to generate ideas, identify new perspectives, and ensure direct feedback to the company's CTO.

FortiQuest program

This program was designed to add value to existing products and solutions by encouraging Fortinet's R&D staff to deliver better customer outcomes. From troubleshooting to new product ideas, FortiQuest aims to improve product quality and faster go-to-market timelines.
A pilot was conducted as a two-day hackathon in 2023, involving more than 120 Fortinet engineers from various R&D business units in India. From these two days, 31 PoCs were submitted for evaluation, eight PoC were planned for production in the next quarter, and three research papers were developed.

Advancing the cybersecurity industry

While cybersecurity enables innovation in every sector of the modern digital economy, innovative technologies also enable cybersecurity to better secure networks, people, organizations, and data worldwide. One notable aspect of Fortinet's innovation journey is its embrace of disruptive technologies to advance the cybersecurity industry.

Redefining boundaries with AI
Fortinet has been at the forefront of Artificial Intelligence (AI) and Machine Learning (ML) innovation for over a decade, harnessing their power to deal with a plethora of threats and threat actors. The sheer size and growing sophistication of risks are met with AI-driven tools and capabilities available to Fortinet and to its customers. ML and AI engines are embedded in our products and solutions to maximize efficiency and remediation. In 2023, we launched GenAI-based tools to guide, simplify, and automate security, helping to increase the operational efficiency of organizations in dealing with cyberthreats, despite the cybersecurity skill shortage.

Teaming up to ensure a secure future

- **Quantum computing**
  Quantum computing has the potential to disrupt encryption. Fortinet is at the forefront of quantum-safe solutions to protect today's data against the potential threat of tomorrow's quantum computing. In 2023, Arqit, BT and Fortinet worked together to launch commercially available quantum-safe encryption. In addition, LTIMindtree, QuantumExchange and Fortinet collaborated to deliver a secure communication infrastructure with data security that is ready for the quantum era.

Fortinet joined the Network Resilience Coalition

Use of misconfigured, outdated, and end-of-life products can lead to massive vulnerabilities in the security of the global network infrastructure, disrupting both businesses and consumers. To help tackle this issue, Fortinet joined the Network Resilience Coalition, an alliance of technology vendors, security experts, and network operators, in 2023 to develop a white paper with recommendations on how network product vendors and users can work together to improve the overall security of networks.

- **GSMA Open Gateway initiative**
  The GSMA Open Gateway harmonizes revenue-generating interactions by introducing open and standardized APIs and simplifies developer access across mobile network operators. Fortinet's Security Fabric platform provides the entire scope of "security in depth" components required to ensure safe and profitable consumption of the Open Gateway—protecting Telco's assets and driving trust with application developers.

Disrupting cybercrime together

Fortinet is committed to proactively staying ahead of and thwarting cybercrime. We firmly believe that effectively dismantling cybercriminal organizations requires robust, trusted relationships and collaborations with public and private entities. To this end, we have been cooperating with international, regional, and national law enforcement agencies and cybersecurity companies for more than a decade, providing our expertise and sharing actionable threat intelligence to ensure the effective investigation and disruption of cybercriminal organizations.

FortiGuard Labs

Founded in 2002, FortiGuard Labs is Fortinet's elite cybersecurity threat intelligence and research organization. A pioneer and security industry innovator, FortiGuard Labs develops and utilizes leading edge Machine Learning and AI technologies to provide timely and top-rated protection and actionable threat intelligence. Partnering with law enforcement agencies, government organizations, and security vendor alliances worldwide, FortiGuard acts as a driving force to ensure the industry is effectively collaborating to fight emerging global security risks.

FortiGuard Labs in numbers:

Trillions
of events are processed daily

Hundreds
of issued patents from FortiGuard Labs & Threat Detection

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

41
Outbreak alerts issued in 2023

Derek Manky

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

"Disrupting cybercriminals and dismantling their attack infrastructure is a joint responsibility that requires strong, trusted relationships with other public and private organizations. Cybercriminals operate like a business, and forcing them to constantly start over, rebuild, and shift tactics is costly for their organizations and better for the digital world. Fortinet is committed to helping shape the future of cyberthreat mitigation and strengthening public - private partnerships through actionable threat intelligence."

Disrupting cybercrime together

A long history of collaboration

Cooperation with international, regional, and national law enforcement agencies and our cybersecurity peers is a priority for us to ensure a safe digital world. Our first collaboration to jointly fight cybercrime started with Microsoft in 2006. Since then, we have been actively engaging with the industry, CERTs, government agencies, and academia to establish new collaborations and expand the scope of our existing partnerships.

2006 — Microsoft MAPP Zero-Day Program

Member of the Microsoft MAPP Zero-Day program. Since then, Fortinet's contribution to industry has resulted in 1,020+ zero-day discoveries working to harden Infrastructure through responsible disclosure.

2012 — FIRST.org

Member of the Forum of Incident Response and Security Teams (FIRST), collaborating with national CERTs worldwide.

Fortinet contribution project: EPSS to enhance software and network system security through dynamic risk evaluation and early warning systems. The official Special Interest Group (SIG) was launched in 2020.

2013 — MITRE

Partnership with MITRE.

Fortinet contribution projects: STIX & TAXII 1.0 development before ratification.

2014 — Cyber Threat Alliance (CTA)

Original founding member of the CTA, an independent non-profit organization composed of cybersecurity providers and practitioners dedicated to sharing critical threat intelligence and raising the level of security for organizations globally.

2015 — INTERPOL

Officially joined INTERPOL through its Global Cybercrime Expert Group, working on active investigations, resulting in a first arrest in 2016.

2016 — NATO

Partnership with the NATO NCI Agency—the NICP—fostering intelligence sharing on cyber threats and cybercriminals to enhance national security.

2018 — INTERPOL Gateway

Officially joined the INTERPOL Gateway project. It includes weekly sharing of threat information from the Fortinet FortiGuard Labs global threat research team and routinely responding to breaking RFIs (Request for Intelligence) as new cases emerge. Fortinet also participated in Cyber Surge campaigns for Law Enforcement education and training.

2019 — World Economic Forum Center for Cybersecurity (C4C)

First cybersecurity founding partner of the WEF Centre for Cybersecurity (C4C).

2020 — WEF Partnership Against Cybercrime (PAC)

A founding member of the WEF PAC, an initiative aiming to build trusted public & private sector threat sharing relationships. Fortinet is a key contributor to the Partnership Against Cybercrime report, which provides recommended first steps towards establishing a global architecture for cooperation.

2021 — MITRE Engenuity Center for Threat Informed Defense

A research partner with the MITRE Engenuity Center for Threat Informed Defense (CTID). Fortinet's contribution projects:

- Sightings Ecosystem in 2021: 353 unique attack techniques were observed in 198 countries and 1.6M sightings (Period: August 2021 - November 2023)
- Attack Flow & Attack Flow II in 2022,
- ATT&CK Workbench and Summitting the Pyramid in 2023.

2023

An inaugural founding grantor of the **Cybercrime Atlas project** initiated by the PAC.

UC Berkeley Center for Long-Term Cybersecurity (CLTC).
Fortinet contribution project: Cybersecurity Futures 2030

Joint Cyber Defense Collaborative (JCDC).
Fortinet contribution project: OSS initiative.

Disrupting cybercrime together

Key contributions in 2023

Advancing Threat Informed Defense Globally with MITRE Engenuity CTID
As a MITRE Engenuity CTID research partner, Fortinet participated in two major projects in 2023: *ATT&CK Workbench* and *Summitting the Pyramid*.

The ATT&CK Workbench is an open-source software tool developed in partnership with AttackIQ, Inc., Fortinet, HCA—Information Technology & Services, Inc., Health ISAC, Inc., and Verizon Business, that reduces the barriers for defenders to ensure their threat intelligence is aligned with the public ATT&CK knowledge base. It helps protect organizations with precision against evolving threats through collaborative threat intelligence.

Summiting the Pyramid is a research project focused on engineering cyber analytics to make adversary evasion more difficult. In partnership with CrowdStrike, Inc., Fortinet, Fujitsu, IBM Security, Microsoft Corporation, and Verizon Business, the Center's project has created a methodology, approaches, and tips for organizations to make their analytics less evadable.

MITRE ENGENUITY™
A Foundation for Public Good

INTERPOL

Fortinet and INTERPOL

Since 2015, Fortinet has actively contributed to INTERPOL's mission to fight crime and create a safer world for communities. In 2023, INTERPOL and its partners, including Fortinet, achieved several significant milestones:

- FortiGuard threat intelligence was shared with law enforcement in 25 countries through the Gateway program
- 15 arrests were made through INTERPOL operations as part of the Gateway program
- $40M prevented in financial losses
- First-time leadership role in INTERPOL's Global Cybercrime Conference

JCDC

Member of the Joint Cyber Defense Collaborative

In April 2023, Fortinet proudly became a member of the Joint Cyber Defense Collaborative (JCDC), deepening our commitment to strengthening the United States' security posture and cybersecurity resilience. By collaborating with the JCDC, Fortinet is sharing expertise, broad threat visibility, and actionable intelligence, bolstering the Cybersecurity and Infrastructure Security Agency's (CISA) mission to unite public and private entities in the defense against cyber threats.
Fortinet also contributed to a new fact sheet on improving the security of open -source software in operational technology (OT) and industrial control systems (ICS), released by JDCD in collaboration with CISA, the NSA, the Department of the Treasury, and the FBI. FortiGuard Labs tracks attacks on Open Source Software (OSS) and provides insightful learnings and protection guidance into what happened, the technical details of an attack, and how an organization can protect itself. This fact sheet promotes a deeper understanding of OT security and highlights best practices and considerations for the secure use of OSS in OT and ICS environments.

Disrupting cybercrime together

Fortinet joins UC Berkeley Center for Long-Term Cybersecurity (CLTC)
Cybersecurity Futures 2030 is a project led by experts at the University of California Berkeley's Center for Long-Term Cybersecurity (CLTC), with participation from the WEF, Fortinet, and other strategic partners. This initiative is designed to help public and private sector leaders critically examine future-focused scenarios and consider how digital security will evolve over the next several years. Through ongoing scenario planning and workshops, the Cybersecurity Futures 2030 initiative produces policy and planning recommendations along with reports to help decision-makers worldwide and across all industries anticipate and effectively address the cybersecurity challenges that lie ahead.

CLTC
Center for Long-Term Cybersecurity
UC Berkeley

Cybersecurity Futures 2030's inaugural report, *Cybersecurity Futures 2030: New Foundations*, released in January 2024, includes insights from six global workshops featuring discussions focused on how technological, political, economic, and environmental changes will impact the future of cybersecurity for governments and organizations, and how leaders should begin addressing these issues now.

In 2023, Fortinet participated in the discussions as a part of the Washington, D.C. working session, which consisted of a hands-on workshop that included analysis between different geographies and scenario planning for 2030. The intent of that dialogue and engagement was to translate collective expertise into future proactive actions, especially considering the speed of technology and innovation in the industry and for cyber adversaries.

WORLD ECONOMIC FORUM

Fortinet and the World Economic Forum

Established six years ago with Fortinet as a founding partner, The World Economic Forum (WEF) Centre for Cybersecurity brings together global leaders from private and public sectors, academia, and law enforcement to develop research, share critical insights, and identify and respond to current and future cyber risks.

One of its key initiatives was the creation of the Partnership Against Cybercrime (PAC) group in 2020, which was formed to build trusted threat-sharing relationships between the public and private sectors.

In 2021, the PAC began the Cybercrime Atlas project to map all major global cybercrime syndicates and develop an interactive platform. Launched at the WEF Annual Meeting in January 2023, Fortinet is a founding partner of the Cybercrime Atlas initiative along with Microsoft, PayPal, and Santander. The objective of this project is to help national and international law enforcement agencies, cybercrime investigators, and global businesses collect and share global threat information, generate policy recommendations, and identify opportunities for coordinated action to fight cyberthreats and disrupt cybercrime.

What we accomplished together with the WEF in 2023:

- Publicly launched the Cybercrime Atlas project and established governance
- Identified and analyzed 13 cybercrime syndicates,
- Delivered 3 completed research packages (2023)
- Mapped 8,584 actionable data points on targeted cybercrime actors and their infrastructure (2023)
- Participated at the 2023 WEF Annual Meeting and Annual Meeting on Cybersecurity
- Actively contributed to the global CISO Community, and helped reduce the cybersecurity skills gap.

Enabling customer success

Fortinet prioritizes trusted service quality, accessibility, and expertise to maximize the value of its solutions for its customers and improve their security posture. In 2023, we focused on channeling feedback for continuous improvement while expanding service for deployment and implementation to ensure successful customer outcomes.

Key initiatives included:

Feature request tool

The revamp of our **feature request tool** now provides a direct avenue to suggest new service features in addition to product features. It serves as an interactive platform to submit customer requirements and contribute to the evolution of Fortinet's services.

Community platform

The significant improvement of Fortinet's **Community platform,** with the creation and publication of 3,100 knowledge articles, fosters a collaborative environment for sharing insights and expertise within the Fortinet community, which now exceeds 100,000 members.

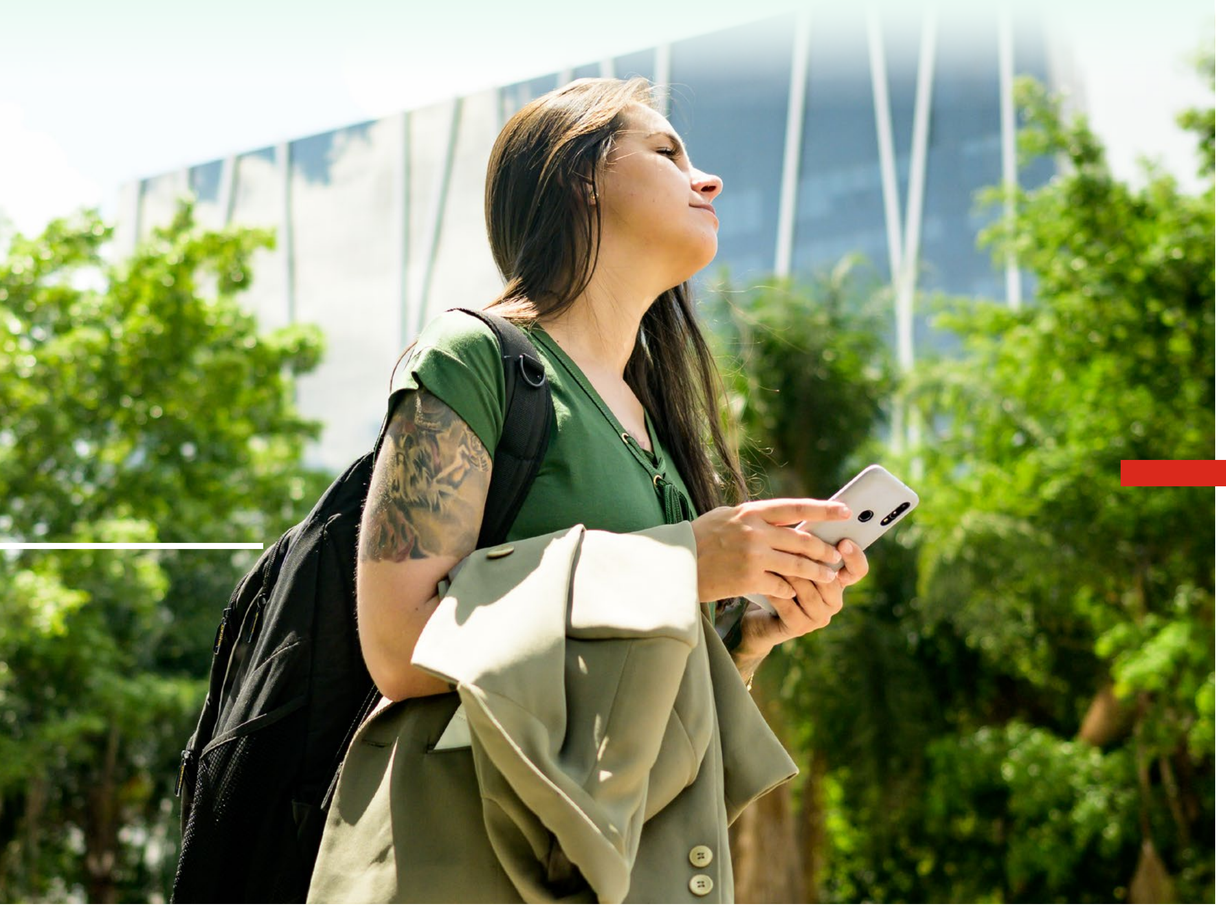
QuickStart program

The expansion of our **QuickStart program**, a consulting service that helps customers get started with Fortinet's solutions. Two new QuickStart packages were introduced for smaller organizations and technology novices. They complement existing professional services options ranging from one-day engagement to multi-year resource alignment for comprehensive customer support.

Two new certifications

The launch of **two new certifications** in 2023 as part of the Fortinet Engage Partner program: Engage Technical Support Partner (ETSP) and Engage Preferred Service Partner (EPSP). Both reflect the partner's level of expertise and experience in technical support or professional services, giving our customers confidence in working with them.

Respecting the environment



Climate change, the scarcity of natural resources, and the energy crisis are some of the biggest threats to business and society today and in the future. Addressing these issues is everyone's responsibility. Fortinet prioritizes its environmental responsibility by addressing the impacts of climate change and minimizing the environmental footprint of its solutions, operations, and broader value chain. To do our part on decarbonization, we have committed to achieving net zero greenhouse gas emissions by 2030 from our owned facilities worldwide (Scope 1 and Scope 2 emissions) and by no later than 2050 across all Scopes, in alignment with the latest criteria established by the Science Based Targets initiative (SBTi). We are actively working on our decarbonization roadmap and adopting sustainable practices internally.

Climate change pledge

Net zero
by 2030
Scope 1 & Scope 2 emissions

SBTi committed

2023 highlights

100%
renewable electricity in 80% of our owned sites

62%
average reduction in product energy consumption

~455
tons of CO_2 emissions avoided through eco-friendly packaging manufactured

SDGs

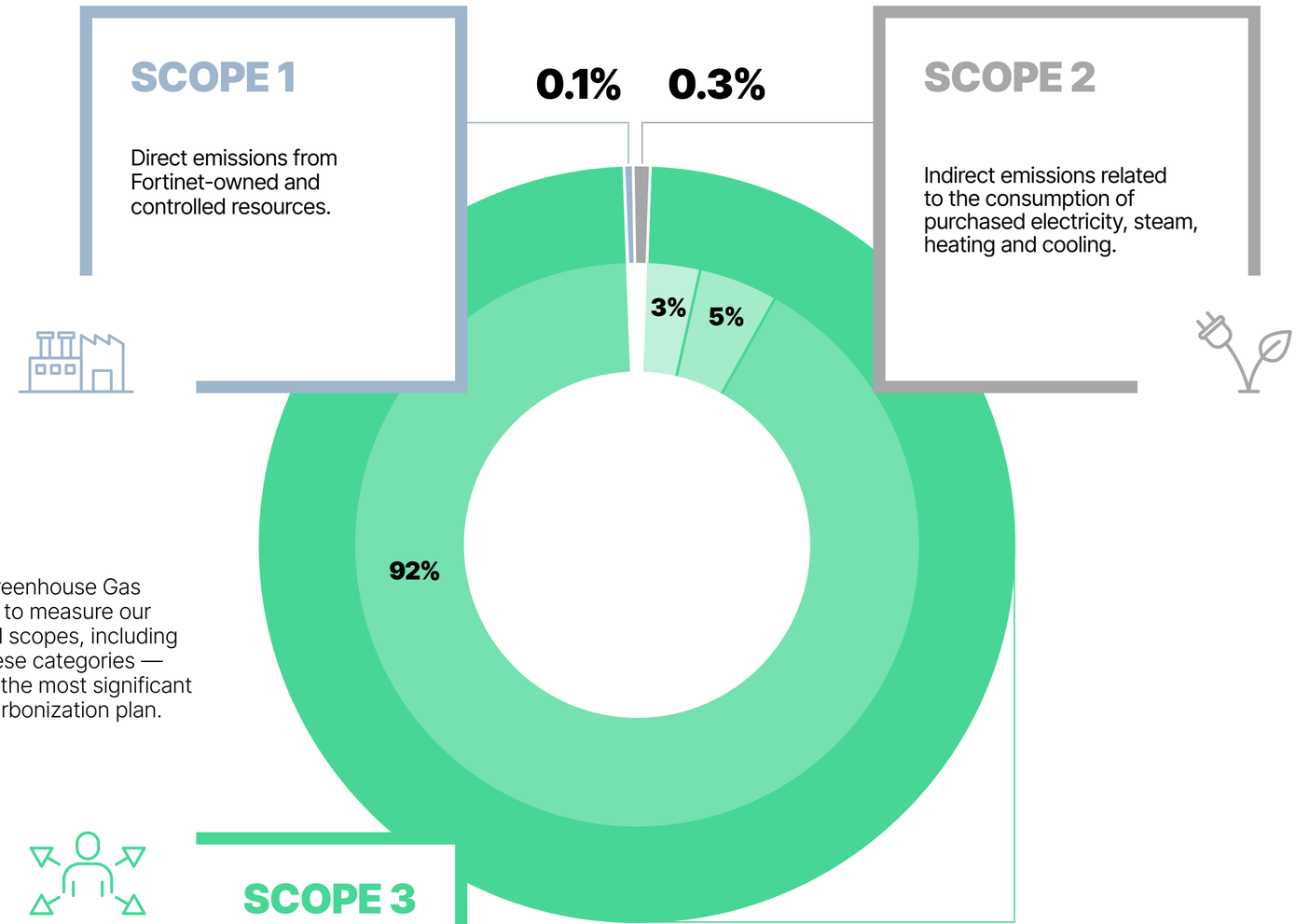
Mitigating our impact on climate change

Achieving net zero impact requires a deep understanding of our carbon footprint and the implementation of an ambitious decarbonization plan.

Fortinet's FY23 carbon footprint — FY23

We use globally recognized standards and methodologies, such as the Greenhouse Gas Protocol Corporate Accounting and Reporting Standard (revised version), to measure our GHG emissions. We have been measuring our carbon emissions across all scopes, including the 12 categories of Scope 3 that are relevant to our company. Two of these categories — the use of sold products and purchased goods and services — are by far the most significant and have been identified as the key ones to neutralize as part of our decarbonization plan.

TOTAL
2,030,699 $mtCO_2e$



Mitigating our impact on climate change

Our path to net zero

Our net zero GHG emissions targets align with the latest criteria established by the Science Based Targets initiative (SBTi). SBTi is a global body that enables companies to set ambitious emissions reduction targets in line with the latest climate science. It is focused on accelerating the decarbonization of companies worldwide to halve emissions by 2030 and achieve net zero emissions by 2050. Specifically, Fortinet's commitment adheres to the near-term 1.5C criteria (version 5.1, released in April 2023) and net zero criteria (version 1.1, released in April 2023) set forth by SBTi.

In 2023, we updated our decarbonization plan for Scope 1 and Scope 2 emissions to take into account Fortinet's strategy in the short- and long-term acquisition of data centers, which significantly impact the baseline for our sustainable efforts. We have also started to work on our broader decarbonization plan in view of submitting our emissions reduction targets across all scopes to SBTi for validation by the fall of 2024.

Q&A

Meera Ramanathan

Director, Environmental Sustainability at Fortinet Member of the CSR Committee

How is Fortinet approaching its net zero ambitions?

In 2023, Fortinet decided to massively invest in its own data centers. This was key to making sustainability central to our site development strategy. Collaboration and innovation took center stage in allowing us to execute on that strategy. Large data center purchases required cooperation among different teams such as Facilities, Corporate Real Estate, CSR, and IT to ensure 100% renewable energy availability and the selection of energy partners that would assist us in our commitment to decarbonization. Only strong partnerships among the different teams in Fortinet will move us forward for a sustainable net zero future.

Goal	Net zero by 2030	Net zero by no later than 2050
Scope 1 **Direct emissions**	**Elimination** of natural gas usage **Electrification** of buildings Alternative **refrigerant** usage **and cooling** mechanisms	
Scope 2 **Indirect emissions**	Usage of **100% renewable electricity** for both owned and leased sites **On-site** (solar panels, etc.) and **off-site** (VPPAs, etc.) investments	
Scope 3		
Purchased goods and services Emissions from manufacturing Fortinet components and products	Ensure that all suppliers and vendors **climate programs align with ours** Work with vendors that have **a clear climate plan**	
Product in use Emissions from the use of Fortinet products at customer sites	Reduce energy usage via **continuous efficiency improvement** **Increase recyclability and reusability** of components	

Mitigating our impact on climate change

Ambition #1:
Net zero for our owned operations (Scopes 1 and Scope 2 emissions) by 2030

Reducing GHG emissions from our facilities starts with procuring renewable energy, combining on-site renewable electricity, purchasing utility green power, and receiving energy attribute certificates in alignment with the stringent technical criteria outlined in version 4.1 of RE100 (released on December 12, 2022). It is also about driving operational efficiency, reducing the use of natural gas, and introducing alternative cooling technologies in our buildings and data centers.

Our goal? Achieving 100% renewable energy usage across all sites, leased and owned.

In 2023, 80% of our overall owned sites by square footage used 100% renewable electricity. 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 guarantee that we will expand the use of green electricity as we grow, we have chosen a global energy broker that will assist us in procuring all forms of green energy, from utility contracts to virtual power purchase agreements (VPPAs).

As part of our investment in green energy, in 2023 we completed a new parking garage at our headquarters in Sunnyvale, CA, with a roof fully covered by solar panels. The renewable solar energy generated by these panels (starting in 2024) will cover the electricity consumption for our entire HQ campus and nearby owned facilities.

While increasing our green electricity usage, we are also decreasing our natural gas reliance: in 2023, sixty-two percent (62%) of Fortinet's owned and occupied sites did not consume natural gas. New sites that are being constructed will be powered entirely by renewable electricity, similar to our HQ site in Sunnyvale.

And lastly, we purchase energy attribute certificates (EACs) to compensate for the remainder of the carbon emissions we generate across our owned sites.

100%
renewable electricity usage

↗ **80%**
of owned sites by square footage

Purchase of RECs

↗ **The remaining 20%**
of sites that do not have green energy

0%
natural gas usage

↗ **62%**
of Fortinet's owned and occupied sites

Number of 100% fully electrified sites

↗ **2 including**
our headquarters in Sunnyvale, CA

Fortinet's real-estate green guidelines

Fortinet developed a comprehensive set of green guidelines for both its data centers and offices, based on the LEED and BREEAM green building rating systems, including the assessment of renewable energy availability, green certifications, alternative transportation accessibility, and waste and management, amongst other building efficiencies. This helps us align new real-estate investment with our decarbonization goals. These guidelines also help identify corrective actions for continuous improvement.

Ambition #2:
Net zero across our value chain (Scope 1, Scope 2, and Scope 3 emissions) by 2050

Because Scope 3 emissions account for the majority of our GHG emissions, we have the greatest opportunity to achieve net zero by 2050 through a combination of upstream and downstream initiatives in our value chain. To achieve this, we are working to:

- **Reduce total GHG emissions at every stage of our product lifecycle,** from material sourcing, design, manufacturing, packaging, and transportation to recovering products when they are no longer in use to maximize recycling and refurbishing.
- **Reduce the energy footprint of our products** while continuing to maximize performance.

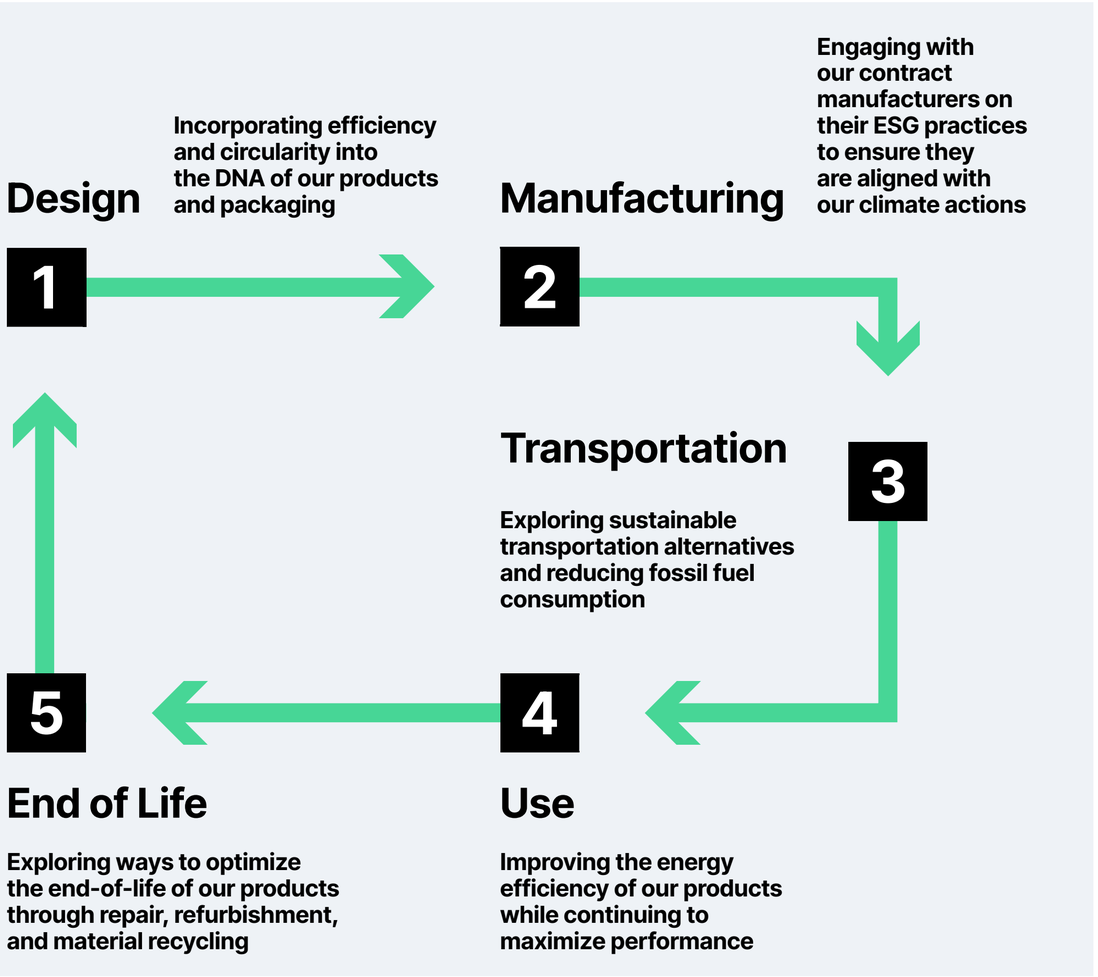
We have started to work on our Scope 3 decarbonization roadmap, assessing discrete actions to assess decarbonization potential within Category 1: Purchased Goods & Services and Category 11: Use of Sold Products. The goal is to identify reduction pathways internally and through supply chain and customer engagement.

Reducing the environmental impact of our products

With 730,000+ customers worldwide and 11.8+ million appliances shipped in 2023, we recognize that the energy consumed by our products in use is by far the major contributor to our carbon emissions. Since the company's inception, it has been a priority to consolidate multiple functions into a single platform to reduce power, cooling, and space, helping customers minimize energy consumption and GHG emissions.
Today, we lead in energy efficiency, but we understand that the impact of our products on the environment goes beyond their carbon emissions.
That's why we focus on reducing our solutions' broader environmental impact throughout their lifecycle. This means being more sustainable at the design, manufacturing, distribution, use, and end-of-life stages.

Streamlined life cycle assessment

As part of our efforts to understand and address our products' environmental impact, in 2023, we worked with a third-party environmental expert to conduct a streamlined life cycle assessment (LCA) for selected FortiGate firewall models, following ISO 14040, 14067 and 14044 standards. We limited the analysis to carbon intensity across the various stages of the value chain, including raw materials, upstream production processes, manufacturing, distribution, customer use, and end-of-life. This information has helped us identify opportunities for improvement and confirmed that products in use are by far our highest GHG emission category.



Fortinet carbon footprint calculator

Many Fortinet customers share our focus on reducing GHG emissions, including those generated by their own operations and their IT suppliers.
In 2022, Fortinet created the Fortinet carbon footprint calculator.
This tool shows the estimated carbon footprint of our most sold products to help inform our customers and facilitate their sustainable decision-making. This online tool, available exclusively to Fortinet employees, provides the carbon footprint of the product in use, based on the country of deployment, and its entire lifecycle. The methodology for product in use has been verified by third-party TÜV SÜD America, and complies with the GHG protocols.

In 2023, Fortinet has added **150 new models** to its carbon footprint calculator, for a total of 270+ models as of December 31, 2023.

Reducing the environmental impact of our products

Energy efficiency

The Fortinet R&D team places a strong emphasis on improving the energy efficiency of our products and works hard to ensure that each new generation of Fortinet products uses less energy, space, and cooling than its predecessors. Reducing the energy intensity of our products while continuing to maximize performance is critical to supporting our customers' businesses and meeting their climate goals.

In 2023, we continued to push the boundaries by delivering maximum performance per watt, enabling our customers to consolidate their IT equipment and reduce energy and cooling needs. Our new security processing unit 5 (SP5) ASIC achieves industry-leading performance per watt and boasts an 88% reduction in power consumption compared to industry-standard CPUs. Another major milestone was the launch of our new FortiGate 90G, which remarkably consumes 89% less power than the previous generation.

FY23 improvements in numbers

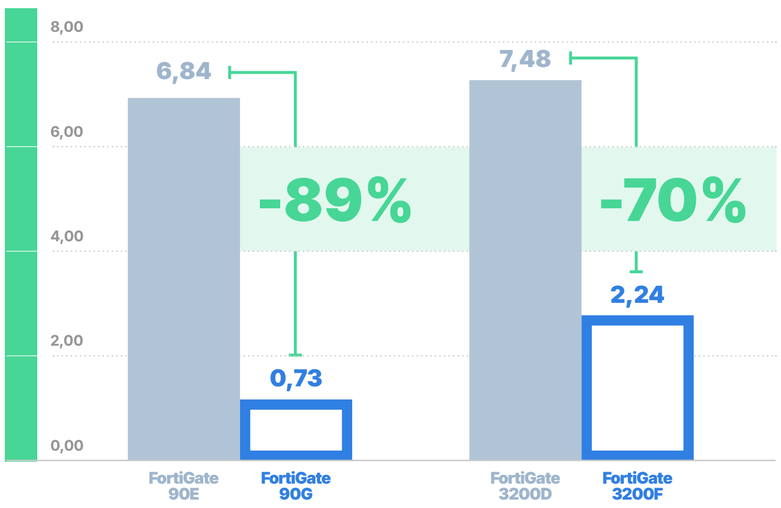
New Fortinet SP5:

88%
power reduction compared to industry-standard CPUs

62%
average reduction in product energy consumption*

FortiGate power consumption per throughput

(Watts Max/Gbps)



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

Eco-design

Today, Fortinet complies with globally recognized product environmental regulations to ensure the responsible use of materials. Our commitment goes beyond compliance—we 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 traditional hardware manufacturing.

In 2023, we trained 75+ employees from R&D, Product Management, Operations, and Quality Management teams with eco-design principles through a series of workshops with external subject matter experts. We aim to create products that are not only resource-efficient but also easily reusable, repairable, and recyclable.

We also focused our efforts on product packaging, recognizing that it quickly becomes waste once it reaches the customer. Working with an external consultant in industrial packaging, our engineers have been exploring packaging made from biodegradable materials that can adapt to our extensive range of product models. By making our packaging plastic-free and recyclable, we facilitate disposal at the end-user level. In 2023, we have launched a new packaging pilot relative to its refurbished shipment, replacing PE foam with Korrvu®/ SealedAir. Production will begin in 2024 with an estimated 18,630 $KgCO_2e$ reduction in carbon footprint.

Eco-friendly packaging in 2023

61
models of Fortinet's top-sold product lines designed with eco-friendly packaging

~455
tons of CO_2 emissions avoided through eco-friendly packaging manufactured (based on an estimated 91 tons of plastic removed)

Fortinet refurbishing pilot program

12,242
units returned in 2023

81%
success rate on return repair

Exploring circularity

We are committed to embracing circular economy practices that encourage increased repair and reconditioning, extended product lifespans, and enhanced material recycling. We can achieve this by fostering strong collaboration with customers, suppliers, and partners to identify and implement best practices for the reuse and recycling of our solutions. In line with the EU Electronics Policies and our environmental sustainability goals, Fortinet launched an internal refurbishing pilot program in 2022 to return unused eval units and engage them in a circular process for reuse and/or recycling.

Strengthening environmental management

In line with our Environmental policy, we are committed to reducing our environmental impact by driving operational excellence. We identify and control environmental impacts related to energy, water, and waste and continuously improve our performance through a comprehensive Environmental Management System (EMS) certified in May 2023 to ISO 14 001, which covers our largest owned warehouse and overflow warehouse, located 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 in Union City.

In FY23, Fortinet took several steps to improve waste tracking and continued its progress on waste reduction, with a particular focus on e-waste. A pilot program is underway in Union City, CA, and Burnaby, Canada, involving a single vendor to improve data tracking and assess circularity by optimizing the final disposition of e-waste. Fortinet is also actively looking for options to reduce its e-waste, including through donations. From a solid waste perspective, California locations, including our headquarters, have proactively complied with SB1383 mandates to divert food waste from landfills since January 1, 2024, through employee communication and training.

New California climate regulation: AB1305

As a California-based company, Fortinet is subject to comply with California's new Climate Regulation, AB1305, designed to prevent greenwashing. In compliance with this regulation, Fortinet issued a public statement on January 1, 2024.

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 impact of our products in terms of materials used and waste management.

We comply with all environmental directives and regulations related to material restrictions. In addition, we support waste management directives, submit our data to relevant databases, and facilitate proper disposal and recycling of our products.

Product regulatory environmental compliance (related to restriction of use of certain hazardous substances in the EEE type of product):

- **EU RoHS directive**
- **EU REACH regulation**
- **U.S. SEC conflict minerals rule**
- **EU packaging directive**

Waste management:

- **EU waste framework directive – Waste prevention and recycling**
- **EU Waste of Electrical and Electronic Equipment (WEEE) directive**

Q&A

Andrew Rybacha
Compliance Manager and Member of the CSR Committee at Fortinet

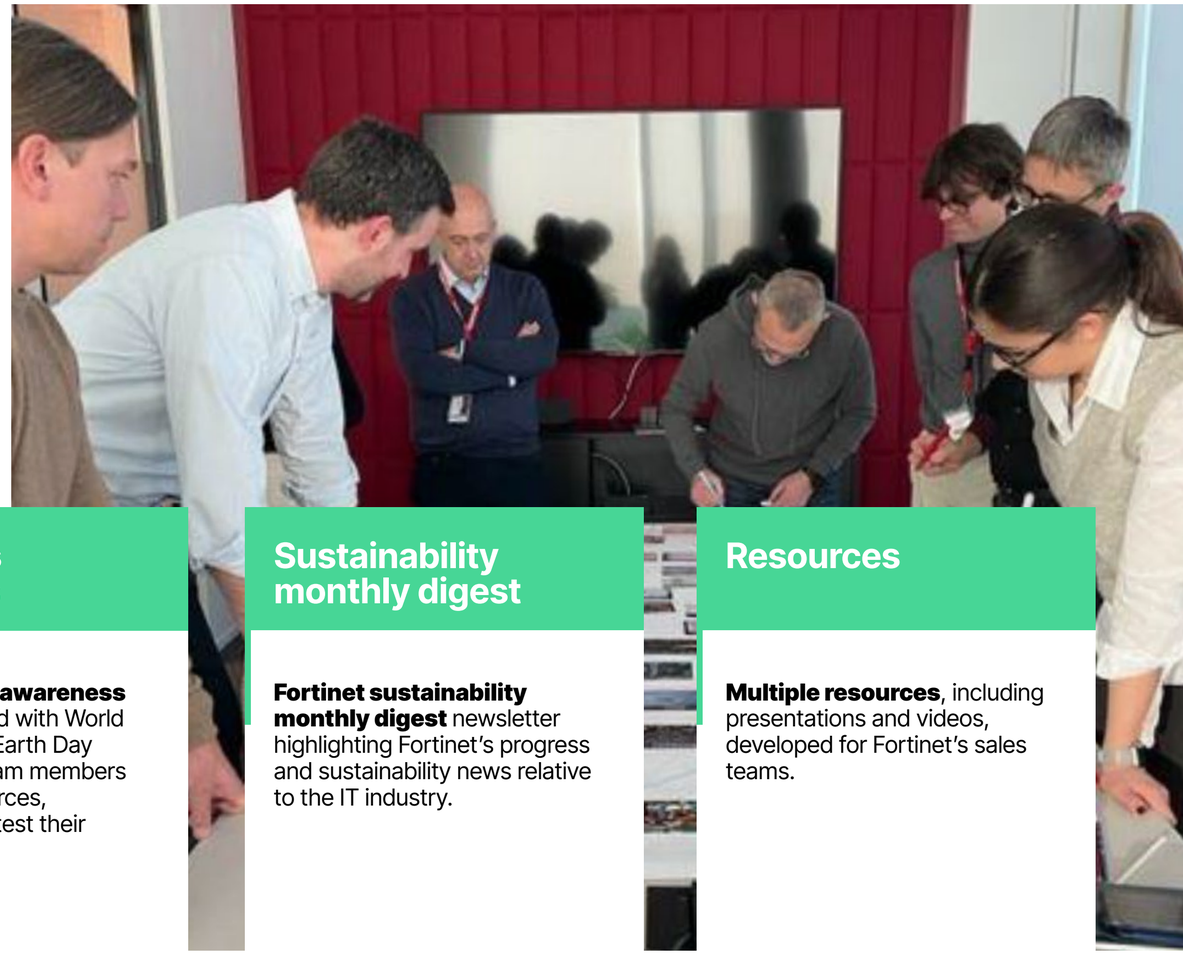
What steps has Fortinet taken to align its product manufacturing with environmental directives?

Fortinet has implemented a comprehensive approach, including the elimination of parts and materials claiming RoHS exemptions as soon as reliable alternative technology is available regardless of whether the given exemption is still valid, a measure which was included in the Manufacturing Purchase Agreement. These measures ensure compliance with environmental objectives and directives such as EU RoHS, EU REACH regulation, US SEC conflict minerals rule, and EU packaging directive.

Fortinet ensures compliance by utilizing multiple sources of information, including BOMcheck, the ECHA website, SGS, and Green Soft Technologies. Regular reviews of evolving requirements prompt adjustments to policies, procedures, and reporting templates to ensure ongoing compliance with current and future regulatory standards.

Engaging our employees on environmental sustainability

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 contribute by taking positive action.



Key initiatives introduced in 2023 include:

Sustainability e-learning

Sustainability e-learning modules developed in house and available to all employees. These modules are also part of Fortinet's onboarding programs, ensuring that new hires are immediately immersed in our sustainability journey.

In-person workshops

In-person workshops to help Fortinet employees better understand climate change, including its causes and consequences. During the sessions, we also discussed how we can individually and collectively reduce our environmental impact. As a result, Fortinet participants formulated more than 150 suggestions that are being reviewed and considered to improve our environmental management. It has been exciting to see employee awareness translate directly into concrete operational initiatives worldwide, such as in the UAE, where the Dubai team decided to eliminate all single-use plastic items.

Awareness campaigns

Company-wide awareness campaigns timed with World Climate Day and Earth Day through which team members can access resources, get inspired, and test their knowledge.

Sustainability monthly digest

Fortinet sustainability monthly digest newsletter highlighting Fortinet's progress and sustainability news relative to the IT industry.

Resources

Multiple resources, including presentations and videos, developed for Fortinet's sales teams.

Growing an inclusive cybersecurity workforce

The lack of cyber awareness among the general public and the continued cybersecurity talent gap represent major obstacles to ensuring a secure, reliable and sustainable digital future. To address these issues, we are committed to achieving a sustained and measurable global impact on closing the skills gap across a broad and diverse range of audiences and building an inclusive, equitable, and diverse workforce within our organization and across the industry to help empower individuals to reach their full potential.

Cybersecurity skills pledge

1 million

people trained in cybersecurity (2022-2026)

2023 highlights

213,440

people trained in cybersecurity

340+

of our leaders trained on fostering inclusion

6

recognitions as one of the best places to work

SDGs

Diversity, equity, and inclusion

Our people are essential to who we are, what we do, and how we innovate. Driving innovation, advancing the industry, and understanding our stakeholders' needs require diverse perspectives. As such, diversity is a central business imperative at Fortinet. We are focused on increasing diverse representation in our workforce and inspiring our teams to thrive in engaging and inclusive work environments.

Fortinet's global workforce in 2023

With a global workforce of +13,500 employees across +90 countries, our diverse team enables collaboration, encourages sharing across borders, and helps drive innovation.
To fulfill our commitment to increasing representation in our workforce, we hire with the intent of developing a full spectrum of talent. This includes early-in-career talent, those representing racial and gender diversity, underrepresented groups, and people from diverse areas of study or background.
The work of DEI has always been complex yet, 2023 presented additional challenges in gender diversity progress due to flat attrition and slowed hiring at Fortinet. Despite this, we remained committed to making representation progress and strengthening inclusion through inclusive leadership and management practices, career opportunities for early talents, and initiatives that foster employee engagement and awareness.

Our goals

- **Increasing** diversity among Fortinet's workforce
- **Further promoting** a culture of inclusion and belonging

Recognitions in 2023

BEST PLACES TO WORK 2024 'GLASSDOOR'

Great Place To Work.

Los Mejores Lugares para Trabajar™ para Mujeres
Great Place To Work. México 2023

HR MIAMI

DEI in numbers

Women representation

GLOBAL WORKFORCE 20.2%

NEW HIRES 18.6%

Age

<30 13%
30-50 64%
>50 23%

Region

EMEA 25%
APAC 20%
AMERICAS 55%

DEI embedded into our organizational governance

2023 was the first full year with Fortinet's organizational governance around DEI in place. It reflects a robust commitment from leadership, emphasizes cross-functional collaboration, and strategically promotes diversity and inclusion across the organization.
In 2023, we held quarterly DEI Council meetings to enhance our DEI strategy and efforts to make the Fortinet experience more inclusive. To that end, we focused on creating inclusive job descriptions globally, developing DEI training for employees, embedding DEI principles into existing internal programs, and increasing organizational awareness of DEI.

Diversity, equity, and inclusion

Reaching diverse talents

At Fortinet, our targeted recruitment programs aim to attract talents from diverse backgrounds. In 2023, we focused our efforts on early talent from underrepresented groups and women. These efforts included the Early Talent program, university sponsorships, scholarships, and inclusive hiring practices.

The Early Talent program
Fortinet provides a supportive and inspiring work environment for interns and recent graduates who can gain real-world experience in the field of cybersecurity. The Early Talent program offers a variety of technical and non-technical roles across multiple functions. It includes training and mentorship from senior staff, exposure to cutting-edge technology, and networking opportunities with industry experts. Our goal? Make Fortinet an ideal place for anybody seeking a meaningful career in cybersecurity.

Inclusive hiring practices
With targeted incentives for gender diversity, our DEI-trained recruiters actively source women and candidates from underrepresented groups. We broadened our recruitment channels by exploring internship programs and job fairs and engaging with several women's associations worldwide to help skill and upskill their communities. Leveraging AI allowed us to better connect with female candidates, run online campaigns, and tailor branding efforts to attract a more diverse range of candidates.

Equitable pay

Fortinet is committed to fair and equitable pay practices throughout all levels of the organization, and continuously review and refine its job architecture and compensation structure.
We continued our work with external consultants to align salary ranges to job function and grade in line with industry best practices to improve equity in pay. We also measure, monitor and report on employee compensation to address local regulatory guidelines in jurisdictions where required.

University sponsorships and scholarships

Fortinet is privileged to welcome exceptional talent to our R&D and Support teams, notably recent graduates from Canadian and U.S. institutions. Strengthening university partnerships is an area of focus for Fortinet, exemplified in part by multi-year scholarships in collaboration with the University of British Columbia (UBC) and Simon Fraser University (SFU).

A culture of learning

We prioritize inclusiveness through global self-learning and inclusive leadership programs. Our commitment extends to empowering employees wherever they operate, enabling them to drive positive impact within the entire organization.

Fostering inclusive leadership
Aligned with our commitment to fostering an inclusive workplace, in 2023 we further strengthened our internal leadership development solutions to empower our leaders with inclusive leadership skills and an in-depth understanding of inclusiveness. This includes DEI-related learning in the company's flagship Signature program, webinars, and a workshop pilot focused on inclusion.

343
of our leaders trained on fostering inclusion in 2023

Fortinet's manager development programs
Fortinet's Signature leadership development program, Manage for Success, supported by HR leadership, Sales Enablement, and the Training Institute teams, stands as a pivotal initiative for developing existing managers.
In 2023, we introduced Ignite Your Potential: our newest signature initiative for emerging and developing leaders to gain the knowledge and skills needed to effectively lead a team. Through a leadership assessment tool, attendees can enhance their self-awareness and self-mastery. Following this, participants delved into best practices of leading others while gaining insights on how to integrate these practices into their day-to-day leadership responsibilities.
153 leaders attended this pilot in 2023.

Manage for Success
Designed to align management practices and bolster leadership acumen throughout Fortinet, three cohorts of Manage for Success ran in 2023 to provide leadership training. 328 employees completed the modules covering awareness of distinct leader accountabilities across the organization, skill building, and capability enhancement. In the area of DEI, in particular, the Manage for Success' curriculum encompasses thought leadership, addresses unconscious bias, and offers insights into inclusive leadership and "diversity 101", ensuring a well-rounded, forward-thinking approach to leadership development.

Inclusive leadership workshops

Fortinet's commitment was demonstrated in 2023 by successfully implementing an inclusive leadership workshop pilot in the EMEA region that targeted 38 leaders. This interactive workshop was designed to promote conscious reflection in inclusive leadership. It focused on raising awareness and enabling conscious change to inclusively improve employee engagement, relationships, team dynamics, and performance. Noteworthy impacts included leaders adopting a more introspective approach, actively seeking feedback on their leadership behaviors, and embracing vulnerability as a basis for team trust. Additionally, leaders recognized the direct correlation between a culture of inclusion and enhanced individual and team performance.

Diversity, equity, and inclusion

A community of inclusion and belonging

Beyond encouraging diverse perspectives, backgrounds, and knowledge, Fortinet cares about fostering an environment of inclusion and belonging where our employees feel welcomed, respected, supported, and valued from day one. We're fostering an inclusive community within and beyond our workplace through our diversity ambassadors and allies, Employee Resource Groups, DEI awareness campaigns and community donations.

In 2023, Fortinet leveraged several international celebration days and months such as International Women's Day, Pride Month, World Mental Health Day, and International Day of Persons with Disabilities, to raise awareness of diversity and inclusion among its employees. Our internal communication campaigns included educational resources, external subject matter expert webinars, employee and leader interviews, and inspiring videos.

Fortinet diversity ambassadors and allies
We are also amplifying our diversity and inclusion culture through the dedicated efforts of our most engaged employees - the Fortinet diversity ambassadors and allies. Today, the group consists of 18 employees from different business units and levels of seniority. They put their beliefs into action by standing as role models who inspire, mentor, and empower across our organization and externally to foster a diverse and inclusive workplace and attract more diverse candidates to join our industry. As a result, we launched DEI&B Coffee Chats in 2023: monthly open get-togethers encouraging discussions about DEI matters, with updates from Fortinet diversity ambassadors and Employee Resource Groups (ERGs).

LGBTQIA+ inclusion

In June 2023, Fortinet offices worldwide, including Florida, Brazil, Mexico, Israel, and France, celebrated Pride Month, reflecting Fortinet's support for LGBTQIA+ inclusion.
In the EMEA region, discussion about creating a dedicated Employee Resource Group (ERG) was initiated following the success of the Pride Month celebration. In LATAM, Fortinet signed the Pride Connection charter. By doing so, the company is taking a step further to create a safe and supportive environment for the LGBTQIA+ community through awareness and training actions, increased recruitment, affinity group support, and collaboration with local and national public bodies.

Portrait of Christina Baeck, Fortinet diversity ally

Christina joined Fortinet in 2014 and is now managing the Austrian Fortinet channel. A founding member of Women4Cyber in Austria, she helps promote and celebrate women across the industry. Christina said, *"The decision to become a founding member was motivated by a proactive desire to 'be the change you want to see' in addressing the gender gap in cybersecurity. We established the Austrian chapter not just to identify challenges but to embody the change we envisioned."*
A Fortinet diversity ally, Christina is also actively engaged in building a more gender-inclusive cyber community, regularly contributing to discussions about security awareness and the cyber skills gap. She explained, *"By actively participating in external networks, I bring in best practices from outside our organization, fostering a continuous exchange of insights and contributing to a more dynamic and inclusive cybersecurity community."*

Diversity, equity, and inclusion

Employee Resource Groups
Fortinet's Employee Resource Groups (ERGs) led by employee volunteers, continue to grow, providing a valuable resource for members dedicated to fostering a sense of inclusion and belonging in the workplace.

Here's a panorama of Fortinet ERGs:

- **Women of Fortinet – US:** Launched in 2022, this group in the United States actively champions women's progress in cybersecurity. With 250 members and allies, the group fosters networking and support through webinars and events. Initiatives include hosting the inaugural Women in Tech conference, networking events at LPGA golf tournaments, a mentor program empowering female leaders, and a Women in Cyber blog series showcasing successful and inspiring women thriving in the cybersecurity landscape.
- **Women's Network – LATAM:** Created in 2019, this supportive networking community of over 260 members promotes the professional development of the many women who make up Fortinet LATAM while providing the space to support other women pursuing a professional career in cybersecurity. In 2023, four general meetings were held addressing topics such as Artificial Intelligence and Leading Crucial Conversations. The ERG also organized four topical Happy Hours and five focus groups this year.
- **Illuminating Talent – UKI:** The primary focus of this ERG is to bring together a community of people who support all aspects of DEI within the UK and Ireland. The group focuses on illuminating talent both internally and externally. In its early adoption phase, the ERG held its first meeting in January 2023. The aim is to meet every 6 to 8 weeks with an occasional guest speaker on a specific topic and to foster a safe environment to share, learn, and raise awareness combined with access to mentoring support.
- **Early Talents – France:** Created in 2023, this group is dedicated to fostering intergenerational inclusion and building connections within Fortinet. Through organized in-person gatherings, including breakfast and lunch events, the group creates opportunities for individuals to meet and connect with colleagues across the organization, emphasizing the importance of collaboration and a supportive community within Fortinet France.
- **LGBTQIA+ – EMEA:** Following the success of its June Pride Month event, the LGBTQIA+ ERG was initiated late in 2023. This group fosters inclusivity and strives to amplify diverse voices. Still in its early days, this ERG aims to create a supportive space for dialogue, collaboration, and advocacy.

Employee community engagement
Contributing to act for good has become increasingly important to our employees. Here are some examples of how our employees are engaged and have made an impact:

- **300+ laptops donated to Emmaüs Connect:** In 2023, Fortinet teamed up with Emmaüs Connect, a French NGO that contributes to social and digital inclusion among underserved communities. This initiative saw the IT and Facilities teams give over 300 unused Fortinet laptops a second life.

- **Intimate Dignity program in Brazil:** The Secretary of Education in São Paulo initiated this program to address menstrual poverty in public schools. Providing hygiene products to vulnerable students, the program aids around 1.3 million girls. Our Brazil team led a successful awareness and donation campaign, ensuring the delivery of essential personal hygiene items.
- **UK&I raises thousands for the Alzheimer's Society:** Since 2017, a team of volunteers from the UK and Ireland has undertaken impressive feats for the Fortinet Channel Charity Initiative. This includes scaling the 2,930ft Cader Idris mountain in Wales, a mighty 5,500-mile team cycle, and more. The initiative has raised thousands of pounds for a different charity every year.
- **A back-to-school drive in Florida:** With the Caring Place, a non-profit based in Florida that supports homeless and low-income individuals, our Sunrise team initiated a back-to-school drive in 2023 by collecting and donating supplies, backpacks, and shoes to aid students in need.
- **Recycling rally in Mexico:** In September and October 2023, our Mexico team conducted a successful recycling rally, collecting 103kg of cardboard, 25.2kg of aluminum, and 95kg of plastic. The initiative served to raise environmental awareness and improve recycling habits. It culminated in a rewarding ceremony recognizing the best team, with donations benefiting local ECOCE and Banco de Tapitas associations.

Closing the cybersecurity skills gap

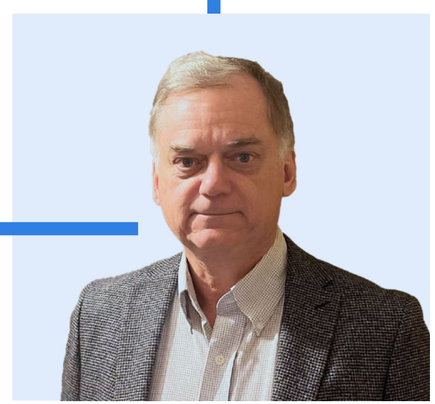
As our societies become increasingly digitized, cybersecurity has become essential for safeguarding citizens and ensuring the stability of our economy. Cybersecurity professionals are the guardians of the complex cyberspace we all share, playing a critical role in protecting and upholding the backbone of the modern digital world. With roughly 4 million unfilled jobs in cybersecurity globally, addressing the talent gap is crucial to supporting today's global economy. Through our various free training and certification programs, we are committed to effectively bridging this ongoing skills shortage by upskilling and diversifying today's workforce while making youth cyber-aware and preparing them to consider and pursue careers in cybersecurity.

Q&A

Rob Rashotte
VP, Global Training & Technical Field Enablement and Member of the CSR Committee at Fortinet

How does Fortinet address the cyber divide?

Fortinet proactively addresses accessibility barriers in its training approach. The company offers online, self-paced training and hands-on labs for all, allowing learners to engage with material at their convenience. Additionally, Fortinet removes financial barriers by providing its self-paced training at no cost and eliminates language barriers by offering instructor-led training in local languages through partners in over 150 countries and territories. This approach ensures that cybersecurity education is accessible to a diverse audience around the globe.



Cybersecurity skills pledge

↗ Train
1 million
people in cybersecurity by 2026
(FY22 base year)

Fortinet on track

↗ **Since 2022, we have trained**
432,905
people

↗ **This means we are at**
43%
of our 5-year goal
+213,440
new people trained in 2023

Closing the cybersecurity skills gap

Diversifying the cybersecurity talent pool

Fortinet acknowledges digital and cyber inequities around the world, and is committed to reaching diverse pools of talent to access cyber education and training. Talent can be found everywhere. By empowering women, veterans, students, and people of all ages, backgrounds, and life experiences, Fortinet expands access to the cybersecurity industry, helping to create employment opportunities and shrinking the skills gap.

One of our key education programs is the Fortinet Education Outreach program. As part of the Fortinet Training Institute, this program reflects our commitment to inclusivity by collaborating with Non-Governmental Organizations (NGOs) to reach underrepresented populations, including women, veterans, and disadvantaged individuals.

Veterans Program Advisory Council

In 2023, Fortinet established the Veterans Program Advisory Council to provide more cybersecurity opportunities for the military veteran community. Council members from across the Five Eyes countries provide insights and guidance on how the Fortinet Veterans program can further help military veterans transition into cybersecurity and/or advance in their careers. The newly established council ensures a voice and representation of veterans, offering insights to ways Fortinet can further support the community.

By offering training and certifications and connecting individuals with the Fortinet employer ecosystem, the Education Outreach program actively creates cyber career pathways, contributing to closing the cybersecurity skills gap and creating professional opportunities.

The 5th anniversary of the Fortinet Veterans program
A core component of our Education Outreach program, the Fortinet Veterans program helps transition the military community—including military service members, veterans, and spouses—to civilian careers in cybersecurity. Since its inception, Fortinet has trained and offered free certification opportunities to over 3,000 veterans and their spouses. This training and certifications help bridge the required technical experience to make a career transition outside the military and enter the industry.

In 2023, the Veterans program expanded to provide additional benefits to veterans and their spouses. This includes introducing a progressive pathway to Fortinet Certified Professional certification, providing access to Fortinet's new Networking Fundamentals course, and working more closely with partners who offer career development services for veterans. In 2023, 448 veterans were trained.

Fortinet's Veterans partners

Blue Star Families
CERCO
CyberCatalyst Talent Solutions
Hire Heroes USA
FORGE
Onward to Opportunity
RSA
Soldier On
Forces Employment Charity
TechVets
US Valor
Veterans Transition Support
VetSec
Vets in Cyber
Tech Vets Canada
Helping Heroes Rehabilitation Service

Women in cybersecurity
As part of our Education Outreach program, we partner with women's associations around the world working to build a gender equality cybersecurity workforce, such as WOMCY in LATAM, Women in Cybersecurity (WiCyS) in the US, and Women4Cyber in Europe. Through these partnerships we provide mentoring and Fortinet training and certification to members at all stages of their cybersecurity career journey, and participate in their virtual and in-person conferences and webinars.

WOMEN 4CYBER
EUROPEAN CYBER SECURITY ORGANISATION

Women4Cyber in Europe

In 2023, Fortinet partnered with Women4Cyber (W4C) in Europe on different initiatives. The Mentorship program supports women entering the cybersecurity job market, with Fortinet providing nine mentors (both from technical and non-technical backgrounds) for personal and professional guidance. Our training team also partnered with the W4C to include our Fortinet NSE certification training in the W4C Academy launched in 2023, making cybersecurity training and certification accessible to their members. Additionally, Fortinet contributes to webinars and posts job opportunities in the W4C newsletter. Our home speakers also engage in events like the W4C Conference, advocating for "Cyber for All" and addressing the cybersecurity workforce gap in Europe.

Closing the cybersecurity skills gap

Making next generations a force for a safe digital world

Ensuring a more sustainable and safer digital world can be achieved when everyone contributes —governments, nations, organizations and individuals. As a global leader in cybersecurity, we feel we are best positioned to demystify cybersecurity for the current and next generations of digital citizens and inspire the next generations of workers to consider and pursue future careers in cybersecurity.

Nurturing cyber talents for tomorrow

Through the Fortinet Academic Partner program, we aim to shape the next generation of cybersecurity professionals by adding our NSE training and certification technical content into academic curricula. In 2023, we partnered with additional academic institutions, including Ecole 2600, a cybersecurity school in France, which incorporates Fortinet's training into its Hybrid Lab for practical learning. The EduSkills program in India further exemplifies Fortinet's commitment, actively training 6,000 students in cybersecurity to support their integration into the workforce.

650+
colleges and universities across

99
countries

Championing cybersecurity education for K-12

Fortinet is actively shaping a cyber-aware culture by taking significant strides in global cybersecurity education for K-12, focusing on both staff and students in the United States. In 2023, we expanded our free cybersecurity awareness training for educators in Canada, Australia, the UK, and Brazil. The service is now available to 11.8 million education staff across the US, Canada, Australia, the UK, and Brazil.

As part of this service, in 2023 we launched a new free curriculum on cybersecurity awareness for kids aged 4 to 18 in the US and UK. To build this, we partnered with teachers from the US, Australia, Canada, France, and the UK to ensure an engaging and meaningful interaction in the classroom. Our goal is to provide kids with the cybersecurity education they need for a safer digital life experience.

Impact

64
million K-12 students potentially

"I welcome Fortinet's initiative to provide free security awareness and training to Australian primary and secondary school educators. As part of the Albanese Government's commitment to make Australia the most cyber-secure country in the world by 2030, we see the value in working in partnership with companies such as Fortinet to help improve cyber skills at every level. This significant and important initiative will support teachers and staff across all Australian schools."

The Hon Clare O'Neil MP, Minister for Cybersecurity

2023 Cyber Security Excellence Award Winner for Best Cybersecurity Training Program and Security Awareness Program

2023 Global Infosec Award Winner for Best Cybersecurity Training and Cutting-Edge Security Awareness Training

2023 Cybersecurity Breakthrough Award Winner for Best Security Awareness Training Platform

Closing the cybersecurity skills gap

Upskilling cybersecurity professionals

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

New NSE certifications

Fortinet NSE certification
Fortinet established the NSE Certification program in 2015 as part of its longstanding dedication to addressing the cybersecurity skills gap. With over 1.5 million certifications issued to date, the Fortinet Certification program includes a wide range of self-paced (no cost) and instructor-led courses and practical, hands-on exercises that are designed to demonstrate mastery of complex cybersecurity concepts.

In 2023, we revamped our certification program, focusing on more role-based training aligned to careers in demand. These changes further enable security professionals to sharpen their skill sets to stay ahead of new threat methods and learn about the latest security technologies to help strengthen their organization's security posture.

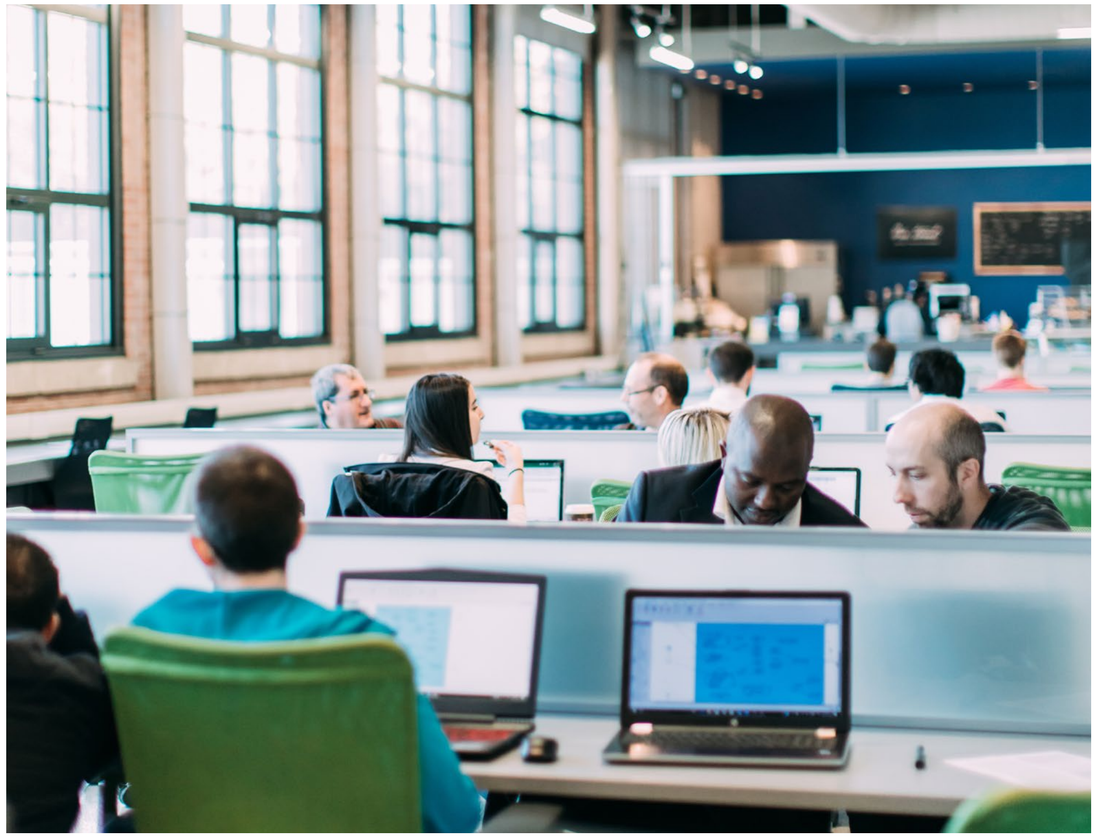
Authorized Training Centers
Fortinet is also increasing security professionals' access to upskilling through its Authorized Training Center (ATC) program, a network of accredited training organizations in over 150 countries and territories around the world teaching in 26 languages. These ATCs deliver cybersecurity training in local languages using the Fortinet NSE Certification curriculum.
In 2023, new partners joined the ATC program including Computer Gross in Italy and DNS based in the Czech Republic.

The ATCs are a network of accredited training organizations in over

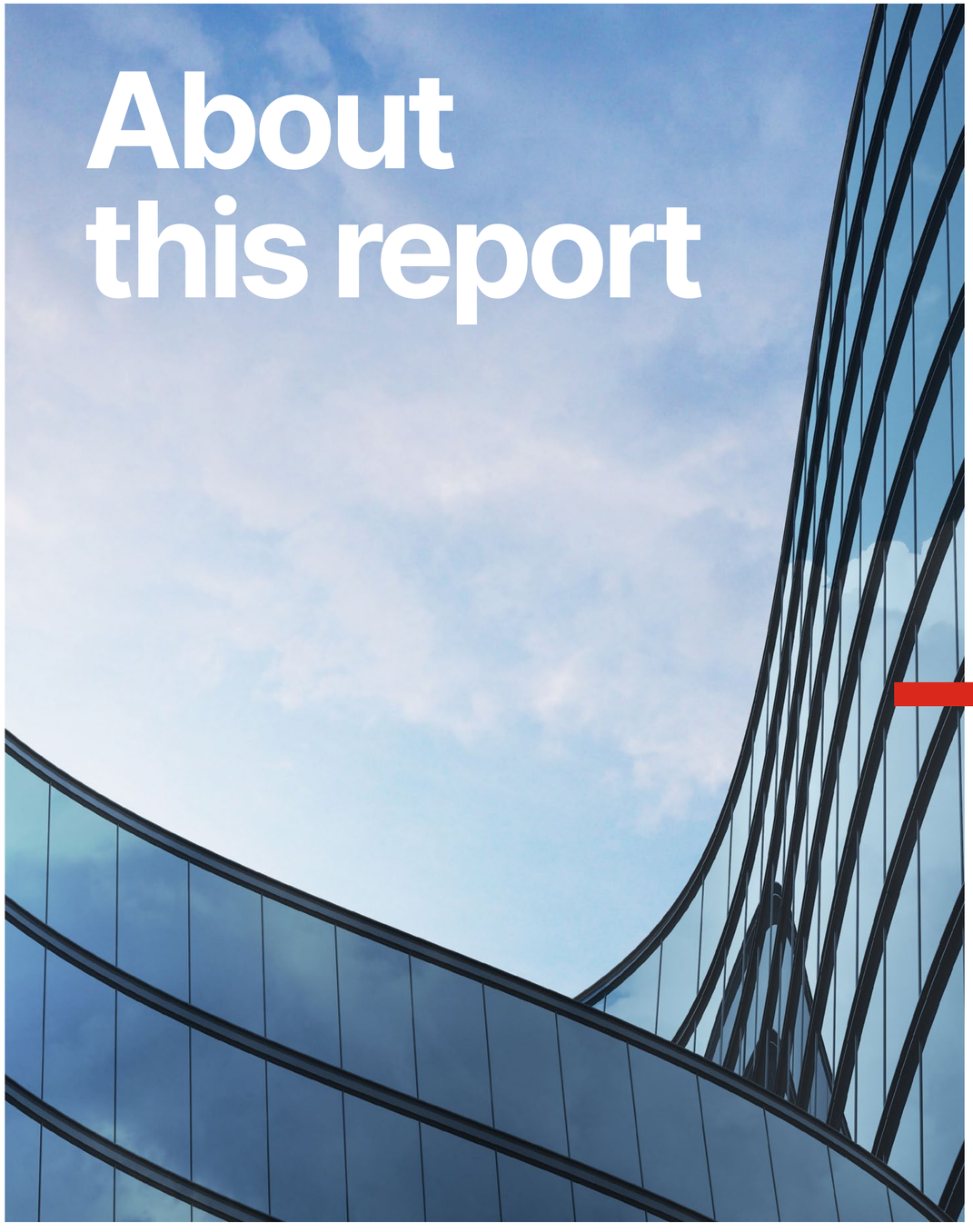
150
countries teaching in

26
languages

4
new ATCs in 2023 (US, Cyprus, Japan, India)



About this report



Fortinet's 2023 Sustainability Report presents a balanced account of our sustainability performance across our priority issues. It allows our stakeholders–including customers, partners, employees, suppliers, shareholders, and communities–to better understand our corporate social responsibility approach and mission. Since 2021, we have reported annually on our sustainability progress and provided in-depth information to our stakeholders on our sustainability commitments and progress across our key pillars and priority issues.

This report also outlines our approach to integrating sustainability into Fortinet. It covers our sustainability journey and performance for our operations and activities worldwide, unless stated otherwise, for the fiscal year 2023 (January 1, 2023–December 31, 2023).

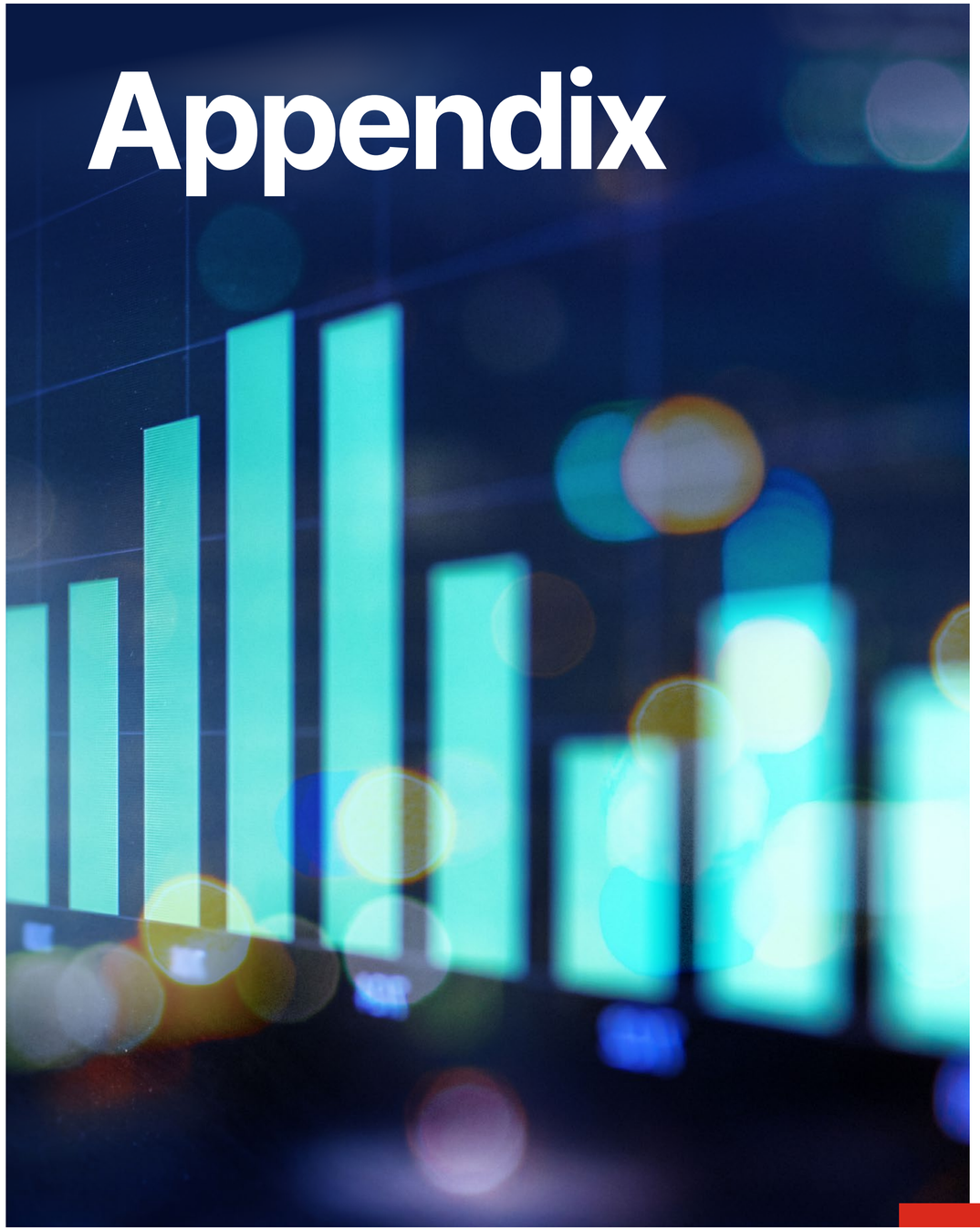
The report references reporting frameworks and standards such as GRI, SASB, TCFD and the UN SDGs. These indices can be found on pages 47-51 and our detailed year-over-year performance metrics can be found on pages 42-46.

Limited assurance was performed on Fortinet's greenhouse gas emissions. The assurance statement can be found on page 52 of this report.

All financial figures are reported in United States Dollars unless otherwise noted.
Additional information on key cybersecurity terms is available here.

CONTACT US

If you would like to connect, please reach us at **sustainability@fortinet.com**



Performance data

PROMOTING RESPONSIBLE BUSINESS

Business ethics

	2023	2022	2021
% of employees who were communicated Fortinet's Code of Business Conduct and Ethics	100%	100%	100%
% of eligible employees who have completed the quarterly Sales Compliance Training[1]	100%	100%	100%
% Fortinet's new direct supplier that were screened using human rights criteria, FCPA, sanction lists, embargoed countries	100%	100%	100%
% of distributors globally who completed Fortinet's Compliance and Business Ethics training	100%	91%	Not applicable
% key contract manufacturers[2] who completed Fortinet's Compliance and Business Ethics training	100%	100%	Not applicable

1. Based on Q4 2023 sales compliance certification.
2. Represents > 90% of total contract manufacturing spend.

ADDRESSING CYBERSECURITY RISKS TO SOCIETY

Innovation

	2023	2022	2021
% of revenue generated from innovation[3]	38.3%	49.5%	Not reported
Number of new product families introductions	6	5	8
R&D investment (USD in millions)	613.8	512.4	424.4
Number of issued and pending global patents (cumulative)	1,551	1,540	1,529

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

Partnership against cybercrime

	2023	2022	2021
WEF's Cybercrime ATLAS - Number of actionable data points mapped and analyzed for disruption opportunities in the cybercriminal ecosystem[4]	8,584	Not applicable	Not applicable
CTA - Number of early discovery shares on threat campaigns	223	197	195

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

RESPECTING THE ENVIRONMENT

Product environment impacts

% of improvement in power efficiency per throughput for top 5 products	2023[5]	% of improvement in power efficiency per throughput for top 5 products	2022[5]	% of improvement in power efficiency per throughput for top 5 products	2020-2021[5]
FortiGate-90G	89%	FortiGate-70F	72%	FortiGate-40F	88%
FortiGate-120G	30%	FortiGate-400F	64%	FortiGate-60F	73%
FortiGate-900G	57%	FortiGate-600F	73%	FortiGate-80F	75%
FortiGate-3200F	70%	FortiGate-1000F	51%	FortiGate-100F	50%
		FortiGate-3000F	68%	FortiGate-200F	20%
Average	62%	Average	66%	Average	61%

5. Improvements in maximum power consumption use in top 4 products sold (FortiGate F Series versus FortiGate E Series) released in 2023, 5 products sold in 2022 and in 2020-2021 (FortiGate F Series versus FortiGate E Series).

Waste

	2023	2022	2021
E-waste (in tonnes)[6]	42.1	67.1	30.8
Recyclable waste (in tonnes)[7]	12.8	11.2	Not reported

6. Data represents e-waste removed during the year from the largest warehouses and RMA centers (Union City - US, Burnaby - Canada and Sophia Antipolis - France).
7. 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

	2023	2022	2021
Water (m^3)[8]	29,188[8]	Not reported	Not reported

8. Data presented here is from owned sites.

Environmental management and climate change impacts

	2023	2022	2021
Scope 1 ($mtCO_2$ e)	1,328.3	1,205.6	1,209.4
Scope 2 - Location based ($mtCO_2$ e)	5,422.2	4,589.6	3,253.9
Scope 2 - Market based ($mtCO_2$ e)	792	163.7	242.9
GHG emission intensity	1,27E-06	1,31E-06	1,35E-06
Reduction of GHG emissions intensity	7%	6%	3%
Energy consumption (GJ)	182,280	142,316	127,878
Energy intensity	3,44E-05	3,22E-05	3,83E-05
Reduction of energy intensity	6%	16%	18%

9. Scope 1 and Scope 2 emissions are calculated for sites under Fortinet's operational control. Data presented here is from owned sites.
10. Increase in Scope 2 emissions from 2021 to 2022 is due to an increase in Fortinet's real estate.

Scope 3 emissions by category ($mtCO_2e$)

	2023	2022	2021
Purchased goods and services	94,208	103,356	Not applicable
Capital goods	6,180	7, 278	
Fuel- and energy-related activities	5,246	4,586	
Upstream Transport and Distribution	7,541	9,983	
Waste generated in operations	622	562	
Business travel	7,842	5,762	
Employee commuting	5,250	4,587	
Upstream leased assets	6,432	6,533	
Downstream transportation and distribution	15,747	12	
Use of sold products[11]	1,874,729	3,669,454	
End of life treatment of sold products	150	255	

11. Use of Sold products total decreased due to the use of more accurate raw data and less estimation in 2023.

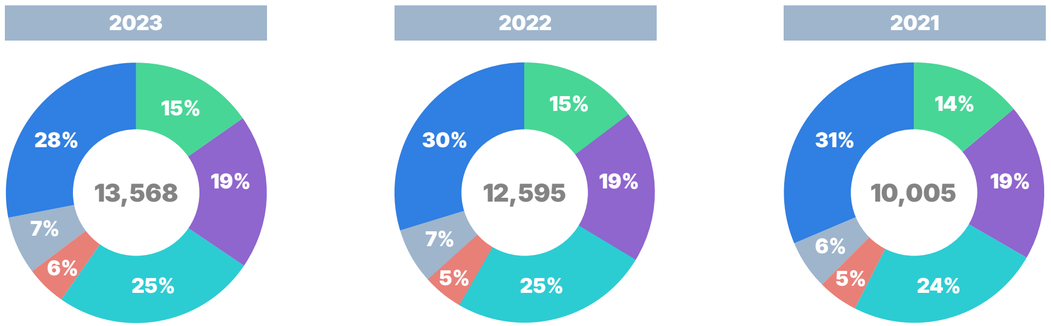
GROWING AN INCLUSIVE CYBERSECURITY WORKFORCE

Diversity, equity, and inclusion

Percentage of individuals within organization's governance bodies by diversity categories

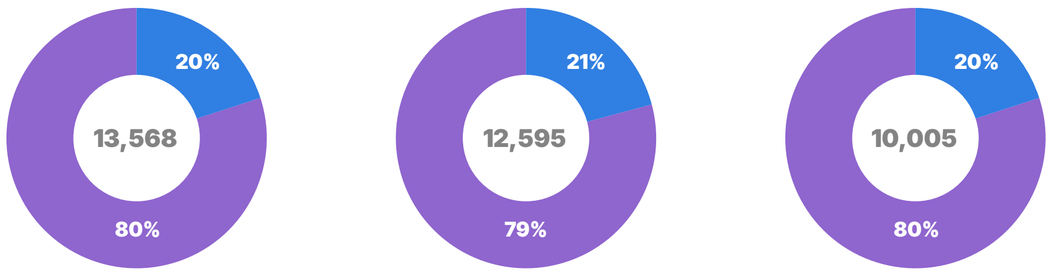
	2023			2022			2021		
	Total	Female	Male	Total	Female	Male	Total	Female	Male
Board of Directors	**8**	25%	75%	**8**	25%	75%	**9**	33%	67%

Total number of employees by region



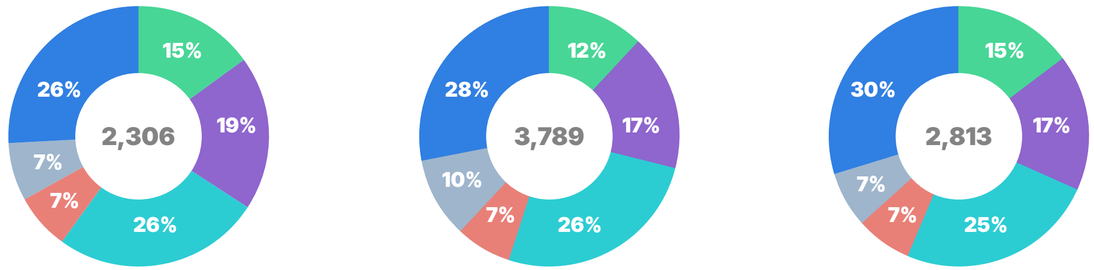
	2023	2022	2021
US	3,826	3,756	3,080
EMEA	3,426	3,095	2,417
CANADA	2,594	2,340	1,930
APAC	1,997	1,835	1,401
LATAM	987	913	632
INDIA	738	656	545

Total number of employees by gender



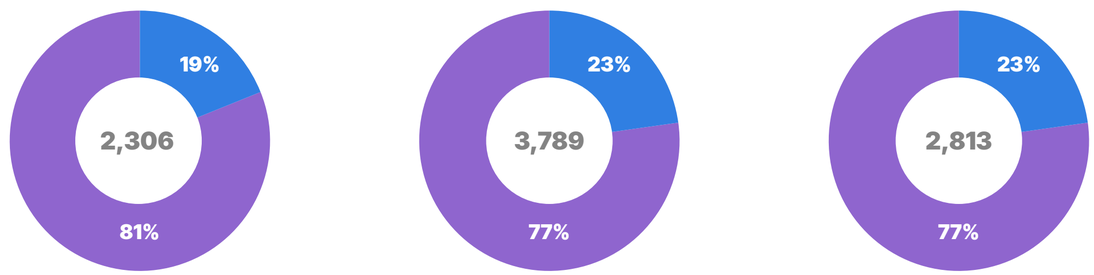
	2023	2022	2021
FEMALE	2,735	2,590	1,963
MALE	10,833	10,005	8,042

Total number and rate of new employee hires by region



	2023	2022	2021
US	606	1,067	837
EMEA	606	987	698
CANADA	432	655	471
APAC	341	460	419
LATAM	162	369	195
INDIA	159	251	193

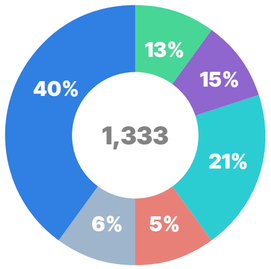
Total number and rate of new employee hires by gender



	2023	2022	2021
FEMALE	429	888	640
MALE	1, 877	2,901	2,173

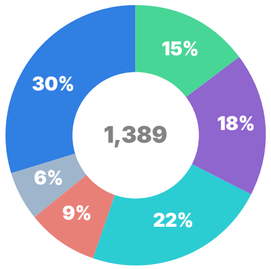
Total number and rate of employee turnover by region

2023



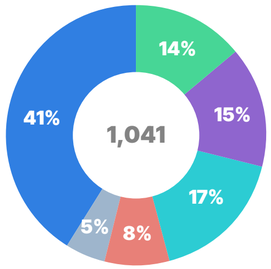
US	535
EMEA	278
CANADA	191
APAC	177
LATAM	82
INDIA	70

2022



US	410
EMEA	312
CANADA	245
APAC	213
LATAM	80
INDIA	129

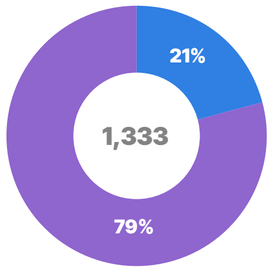
2021



US	429
EMEA	177
CANADA	155
APAC	149
LATAM	50
INDIA	81

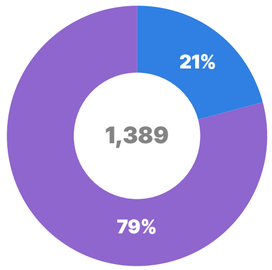
Total number and rate of employee turnover by gender

2023



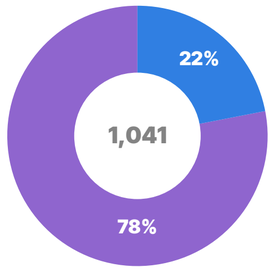
FEMALE	284
MALE	1,049

2022



FEMALE	288
MALE	1,101

2021

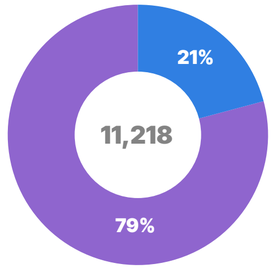


FEMALE	232
MALE	809

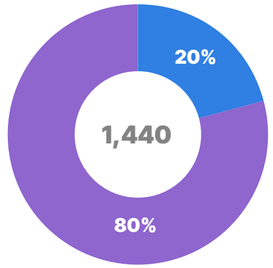
Percentage of employees per employee category by diversity categories

2023

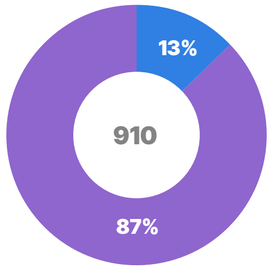
INDIVIDUAL CONTRIBUTOR



MANAGER

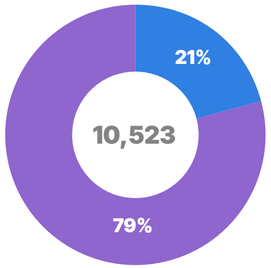


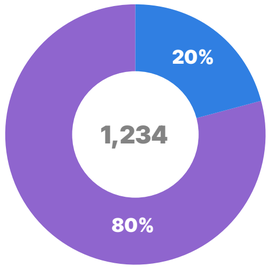
DIRECTOR & ABOVE

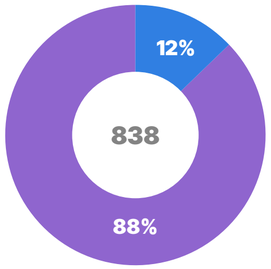


FEMALE	
MALE	

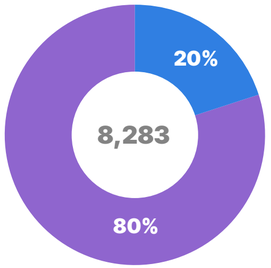
2022

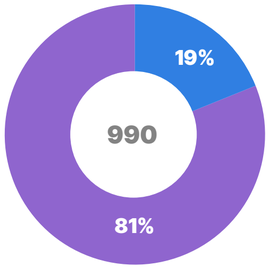


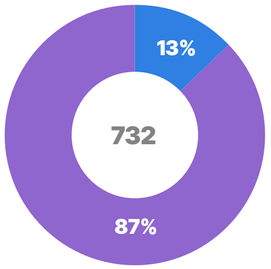




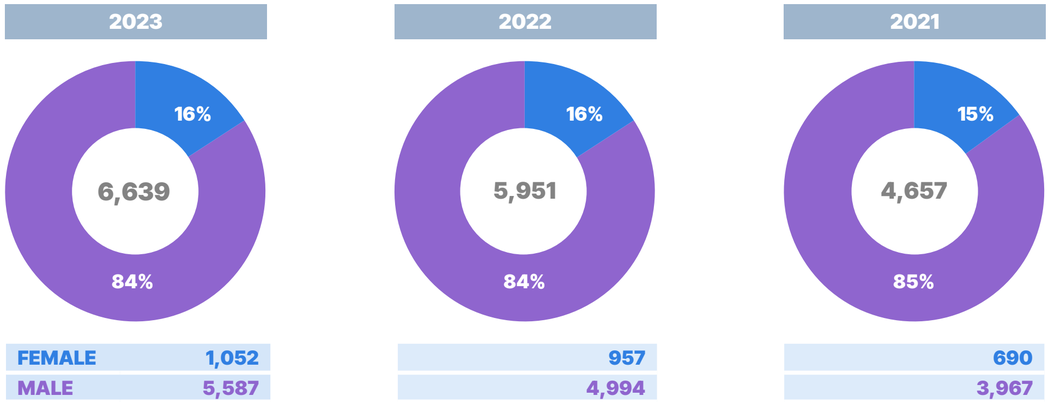
2021





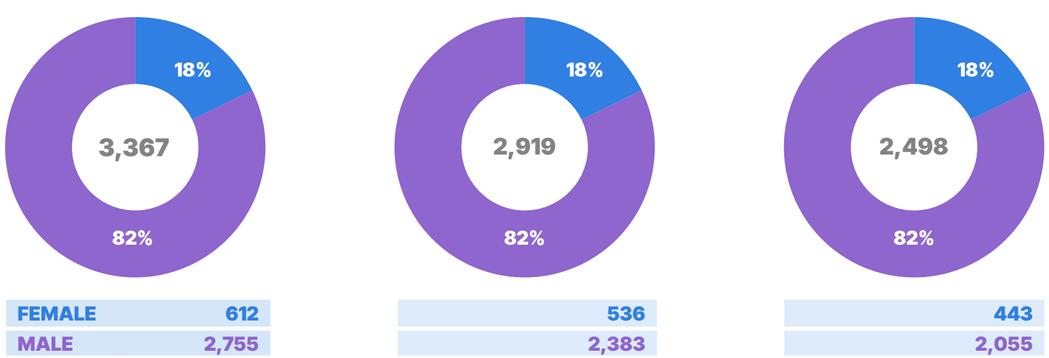


Gender diversity within Global Sales Organization



	2023	2022	2021
FEMALE	1,052	957	690
MALE	5,587	4,994	3,967

Gender diversity within Global R&D Organization



	2023	2022	2021
FEMALE	612	536	443
MALE	2,755	2,383	2,055

EEO-1 Data (U.S. only) / Percentage of gender and racial/ethnic group representation for management, technical staff, and all other employees

2023

Gender	Management	Technical staff[12]	Other	Total
Female	17%	20%	24%	22%
Male	83%	80%	76%	78%

2022

Gender	Management	Technical staff[12]	Other	Total
Female	17%	12%	33%	22%
Male	83%	88%	67%	78%

2021

Gender	Management	Technical staff[12]	Other	Total
Female	16%	18%	24%	21%
Male	84%	82%	76%	79%

ETHNICITY	2023	2022	2021
White	49.5%	49.9%	48.1%
Asian	35.9%	35.2%	37.2%
Latinx	9.6%	9.5%	9.6%
Black	2.9%	2.9%	2.6%
Two or more races	1.7%	1.7%	1.7%
Pacific Islander	0.3%	0.3%	0.2%
Native american	0.1%	0.2%	0.2%
Not disclosed	0.0%	0.2%	0.2%

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

Cybersecurity skills gap

	2023	2022	2021
Total individual people trained[13]	213,440	219,465	Not applicable
Certifications obtained from the learning platform	334,429	315,239	226,258

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 January 1st 2022 and is targeted to be completed by December 31st, 2026.

TCFD INDEX

Fortinet supports the recommendations of the Task Force on Climate-related Financial Disclosures (TCFD). As part of our commitment to climate action, we are publishing a TCFD Index for the first time this year. The information below summarizes our approach to the 11 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. Executive Board's oversight of climate-related risks and opportunities	Fortinet's Board, through its Social Responsibility (SR) Committee, oversees our objectives, strategy and risks relating to sustainability and corporate social responsibility, including climate-related risks. The Committee itself is responsible to review, assess, and oversee Fortinet's ongoing execution versus those objectives. Presentations are done by the Global Head of Sustainability, with the occasional intervention of specialized consulting firms, to periodically review ESG risks and strategy, share on the evolution of regulations, report sustainability progress and issue recommendations. At the end of 2022, Fortinet's Board members also participated in a training session dedicated to climate change in order to deepen their understanding of climate risks. The Board of Directors has adopted a written charter about its SR Committee, which is available on Fortinet's public website. **For more information on CSR governance see SR p. 6 and our Social Responsibility Committee Charter**
	B. Management's role in assessing and managing climate-related risks and opportunities	Executive leadership at Fortinet is directly involved in our sustainability strategy, which includes the management of climate-related risks and opportunities. The Social Responsibility (SR) Committee, chaired by Fortinet's Co-Founder, President, and CTO, oversees Fortinet's sustainability programs, including ESG matters, and reviews and assesses management performance, risks, controls, and procedures related to corporate social responsibility and sustainability. The internal CSR Committee, comprising cross-functional management representatives from across Fortinet, assists the Social Responsibility (SR) Committee of the Board in overseeing Fortinet's corporate social responsibility, including climate-related issues. The CSR team and the internal CSR Committee, both led by the Global Head of Sustainability, 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 for guidance. The CSR Team then works closely with business units, such as Finance, Facilities, R&D, Supply Chain and other stakeholders, to implement the solutions agreed upon. Fortinet has also integrated dedicated incentives scheme for the CSR team and Global Head of Sustainability regarding sustainability-related issues via the achievement of quarterly business goals (MBO). **For more information see SR p. 6 and our CSR Committee Charter.**
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. Description of climate-related opportunities and risks	Fortinet conducted in 2022 a qualitative analysis of current and potential climate-related physical and transition risks and opportunities with impact on our organization, and we intend to perform a quantitative analysis in the next two years, to address the specific requirements of the TCFD. We evaluated potential acute and chronic risks and opportunities associated with the physical impacts of climate change on key operations. The potential physical risks included earthquakes, fire, and floods, especially in key business centers. The qualitative climate-related transition risk analysis evaluated three scenarios from the International Energy Agency (IEA). We assessed transition risks and opportunities associated with legal and policy risks, technology risks, and market and reputational risks. We also identified climate-related opportunities that may have financial or strategic impacts on our business, including developing new, more energy-efficient products or services through R&D and innovation.
	B. Impact of climate-related risks on the organization's businesses, strategy, and financial planning	Climate-related risks inform our strategy across our operations and products and services. As a first step on our climate journey, Fortinet has committed to be net zero (relative to Scope 1 and Scope 2 emissions) by 2030 - in alignment with the Science-based Targets Initiative (SBTi). In 2023, Fortinet updated the decarbonization plan for Scope 1 and Scope 2 emissions to take into account Fortinet's strategy in the short- and long-term acquisition of data centers, which significantly impact the baseline for our sustainable efforts. Fortinet also started to work on its broader decarbonization plan in view of submitting its emissions reduction targets across all scopes to SBTi for validation by the fall of 2024. Fortinet has defined three key strategic focus areas: Operations: Climate-related opportunities across our operations include reducing environmental impacts at our global facilities, and within our supply chain with the ambition to be net zero across our owned sites by 2030. 80% of our owned facilities run on 100% renewable electricity, 100% with purchase of RECs (Renewable Energy Credits)/EACs (Energy Attribute Certificates). We also ensure that our new owned and leased sites can obtain renewable electricity, follow green guidelines and checklists when sourcing locations, minimize the use of natural gas in new construction, and invest in renewable energy and purchasing renewable energy certificates. Value chain: Fortinet is also working to engage its channel distributors, resellers, and contract manufacturers on its climate journey, and is focusing on R&D product innovation to decrease overall power usage of its products with every new generation. Products and services: To respond to consumer requests' regarding Fortinet's climate strategy and product environmental impacts, we have developed and further defined our climate and environmental management strategy from publicly committing to carbon neutrality to quantifying the carbon emissions of our products. We have been calculating the carbon footprint of our main product models, and conducted a streamlined life cycle assessment, a methodology based on the GHG protocol and ISO 14064. In 2023, Fortinet took several steps to improve waste tracking and continued its progress on waste reduction, with a particular focus on e-waste. **For more information on SBTi commitments, path to net zero and strategic action plan see SR p. 24-30**
	C. Resilience of the organizational strategy	Fortinet's climate roadmap, qualitative climate risk scenario analysis, and new climate-related goal demonstrate our continued commitment and progress to strengthen climate risk management across our organization. We leverage science-based frameworks including the IEA to inform our climate-related risk identification process, and we are committed to net zero emissions by 2030 in alignment with the Science Based Targets initiative (SBTi).

Topic	Required disclosure	Reference/disclosure
Risk management Disclosure of how the organization identifies, assesses, and manages climate-related risks	A. Organization's processes for identifying and assessing climate-related risks	The internal CSR Committee and the CSR team assess specific items with reputational, strategic impact and financial risks. For climate-related risks, we consider current and emerging regulations, technology, legal, market, reputational, and acute and chronic physical risks, and included qualitative factors such as disruptions to our operations, and potential damage to our brand. Looking ahead, we plan to conduct a quantitative climate-related scenario analysis to manage climate-related risks. More generally, internal teams are also made aware of climate issues through a monthly sustainability digest, training modules on sustainability, and other resources available for specific teams. In 2023, key initiatives were launched such as e-learning and in-person workshops to engage employees in sustainability. **For more information on employees training see SR p. 31.**
	B. Organization's processes for managing climate-related risks	Fortinet began the process of understanding its impact on climate in 2021 through several steps, including identifying the materiality of its environmental impact and climate change from both operations and technology levels. In order to manage and minimize those risks, we certified our largest owned warehouse and overflow warehouse under ISO 14001. Climate and CSR issues are prioritized by the internal CSR Committee and the CSR team. These governing bodies ensured the calculation of Scope 1 and Scope 2 emissions, and a public commitment to be net zero by 2030, in alignment with the SBTi. In 2022, we also conducted the inventory and measurement of our Scope 3 emissions and identified those categories most significant to our business. The climate-related risks identified by Fortinet are fully aligned with the risks included in Table 1 and 2 of the 2021 TCFD Report: Implementing the Recommendations of the Task Force on Climate-related Financial Disclosures.
	C. Integration of processes for identifying, assessing, and managing climate-related risks into the organization's overall risk management	As part of our efforts on climate change oversight, our corporate social responsibility and risk management teams have begun to collaborate on defining the best approach to integrating climate risk into the company's broader risk managem ent priorities.
Metrics and targets Disclosure the metrics and targets used to assess and manage relevant climate-related risks and opportunities where such information is material	A. Metrics used by the organization to assess climate-related risks and opportunities	Fortinet track metrics to assess climate-related risks and opportunities including total GHG emissions, energy consumption, purchased and on-site renewable electricity, waste, product environmental impacts and green building certifications. We started to track water usage in 2022, and to report on water consumption of our owned sites in 2023 as a first step. By next year, we will begin development of water conservation goals. **For more information on environmental performance data see SR p. 43.**
	B. Disclosure of Scope 1, Scope 2, and Scope 3 greenhouse gas (GHG) emissions	Fortinet reported for the first time on our Scope 1 and Scope 2 emissions in 2021, and we publicly committed to be net zero by 2030, in alignment with the Science-Based Target Initiative (SBTi). Fortinet uses globally recognized standards and methodologies, such as the Greenhouse Gas Protocol Corporate Accounting and Reporting Standard (revised version), to measure our GHG emissions. We have been measuring our carbon emissions across all scopes, including the 12 categories of Scope 3 that are relevant to our company. To progress towards our goal, we are working cross-functionally to mitigate Scope 1 and Scope 2 emissions in owned facilities and Scope 3 energy usage and electricity emissions in leased facilities. As we integrate our Scope 3 emissions into our decarbonization plan, we will start to collaborate with suppliers and vendors to ensure alignment between their climate action plans and ours, so we partner toward achieving our net zero goals. **For FY23 carbon footprint see p. 25.**
	C. Targets used by the organization to manage climate-related risks and opportunities and performance against targets	We aim to minimize the impact of our operations on the environment and climate. In 2022, we implemented an Environmental Management Systems (EMS) platform to track our energy, water, and waste impact. Additionally, to meet our net zero commitment by 2030, we continue to invest in renewable electricity. In 2022, we also formally committed to the Science Based Targets Initiative (SBTi) to set goals aligned with limiting global warming to 1.5°C. **For more information on FY23 carbon footprint see p.25 / on environmental performance data see SR p. 43.**

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 January 1st, 2023- December 31, 2023**		
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	2023 Sustainability Report / Who we are p. 4 2023 Form 10-K p. 3-11	
	2-2 Entities included in the organization's sustainability reporting	2023 Sustainability Report / About this report p. 41	
	2-3 Reporting period, frequency and contact point	2023 Sustainability Report / About this report p. 41	
	2-4 Restatement of information	There are no restatements.	
	2-5 External Assurance	2023 Sustainability Report / Limited assurance statement p. 52	
	2-6 Activities, value chain and other business relationships	2023 Sustainability Report / Who we are p. 4	
	2-7 Employees	2023 Sustainability Report / Diversity, equity and inclusion p. 32-40 2023 Sustainability Report / Performance data p. 42-46	*5.1, 5.5, 8.5, 10.2, 10.3, 10.4*
	2-9 Governance structure and composition	Social Responsibility Committee Charter Governance Committee Charter Human Resources Committee Charter Audit Committee Charter 2023 Sustainability Report / CSR governance p.6	
	2-10 Nomination and selection of the highest governance body	Social Responsibility Committee Charter Governance Committee Charter 2023 Proxy Statement p.38	
	2-11 Chair of the highest governance body	Ken Xie, CEO and Chairman 2023 Proxy Statement p. 35-38	
	2-12 Role of the highest governance body in overseeing the management of impacts	Social Responsibility Committee Charter Governance Committee Charter 2023 Proxy Statement p. 35	
	2-13 Delegation of responsibility for managing impacts	Social Responsibility Committee Charter CSR Committee Charter 2023 Sustainability Report / CSR governance p.6	
	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	2023 Proxy Statement p. 39	
	2-17 Collective knowledge of highest governance body	2023 Sustainability Report / Governance p. 18-19	
	2-18 Evaluation of the performance of the highest governance body	2023 Proxy Statement p. 19-20	
	2-19 Remuneration policies	2023 Proxy Statement p. 41-46	
	2-20 Process to determine remuneration	2023 Proxy Statement p. 44-46 Human Resources Committee Charter	
	2-22 Statement on sustainable development	2023 Sustainability Report / Letter from our CEO p. 3	
	2-23 Policy commitments	Human Rights Policy Vendor/Supplier Code of Conduct Partner Code of Conduct Codes of Business Conduct and Ethics Conflict Minerals Policy	
	2-24 Embedding policy commitments	Codes of Business Conduct and Ethics Vendor/Supplier Code of Conduct Partner Code of Conduct Human Rights Policy 2023 Sustainability Report / Business ethics and human rights p. 11 2023 Sustainability Report / Ensuring responsible product use p. 12 2023 Sustainability Report / Performance data p. 42-46	
	2-26 Mechanisms for seeking advice and raising concerns	2023 Sustainability Report / Business ethics and human rights p. 11 Whistleblower Policy	
	2-28 Membership associations	2023 Sustainability Report / Disrupting cybercrime together p. 19	
	2-29 Approach to stakeholder engagement	2023 Sustainability Report / Stakeholder engagement p. 7	

GRI Standard	Description	Reference/Disclosure	Alignment to the SDGs[14]
Material topics			
GRI 3: Material topics 2021	3-1 Process to determine material topics	2023 Sustainability Report / Sustainability impact p. 5	
	3-2 List of material topics	2023 Sustainability Report / Sustainability impact p. 5	
	3-3 Management of material topics	2023 Sustainability Report / Business ethics and human rights p. 11-12 2023 Sustainability Report / Infosecurity and privcy p. 13-14 2023 Sustainability Report / Securing the digital world, a global priority p. 16 2023 Sustainability Report / Innovating for a safe internet p. 17-18 2023 Sustainability Report / Disrupting cybercrime together p. 19-22 2023 Sustainability Report / Mitigating our impact on climate change p. 25-27 2023 Sustainability Report / Reducing the environmental impact of our products p. 28-29 2023 Sustainability Report / Strengthening environmental management p. 30 2023 Sustainability Report / Diversity, equity and inclusion p. 33-36 2023 Sustainability Report / Closing the cybersecurity skills gap p. 37-40	7.2, 7.3, 7.a, 13.1, 13.2
Indirect economic impact			
GRI 203: Indirect economic impacts 2016	203-2 Significant indirect economic impacts	2023 Sustainability Report / Addressing cybersecurity risks to society p. 15-23	
Anti-corruption			
GRI 205: Anti-corruption 2016	205-2 Communication and training about anti-corruption policies and procedures	Anti-corruption Policy 2023 Sustainability Report / Business ethics and human rights p. 11 2023 Sustainability Report / Performance data p. 42	
Energy			
GRI 302: Energy 2016	302-1 Energy consumption within the organization	2023 Sustainability Report / Performance data p. 43	7.2, 7.3, 7.a, 13.1, 13.2
	302-3 Energy intensity	2023 Sustainability Report / Performance data p. 43	13.1, 13.2
	302-4 Reduction of energy consumption	2023 Sustainability Report / Performance data p. 43	13.1, 13.2
	302-5 Reductions in energy requirements of products and services	2023 Sustainability Report / Reducing the environmental impact of our products p. 28-29 2023 Sustainability Report / Performance data p. 43	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	2023 Sustainability Report / Performance data p. 43	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	2023 Sustainability Report / Performance data p. 43 2023 Sustainability Report / Reducing the environmental impact of our products p. 28-29	12
Employment			
GRI 401: Employment 2016	GRI 401-1 New employee hires and employee turnover	2023 Sustainability Report / Performance data p. 44-46	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	2023 Sustainability Report / Cybersecurity skills gap p. 37-40 2023 Sustainability Report / Engaging our employees on environmental sustainability p. 31	
Diversity and equal opportunity			
GRI 405: Diversity and equal opportunity 2016	405-1 Diversity of governance bodies and employees	2023 Sustainability Report/ Performance data p. 44 2023 Proxy Statement p. 19	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	2023 Sustainability Report/ Performance data p. 42	

14. The GRI Index includes alignment with both priority SDGs for Fortinet, as well as tier 2 and 3 SDGs, which are indirectly aligned with Fortinet's priority issues.

SASB INDEX

The following Index maps our disclosures to the 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**	2023 Sustainability Report/ Performance data p.43
	Discussion of the integration of environmental considerations into strategic planning for data center needs	**TC-SI-130a.3**	2023 Sustainability Report / Reducing the environmental impact of our products p. 28-29 2023 Sustainability Report / Strengthening environmental management p. 30 2023 Sustainability Report / Performance data p. 42-43
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**	2023 Sustainability Report / Infosecurity and privacy p. 14-15 Certifications list: ISO27001 certification SOC2 Type II examination HIPAA examination TISAX certification ISMAP 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 & 2 (FOS 6.2) FIPS 140-2 Level 2 (FSA 3.1) FIPS 140-2 Level 2 (WLM 8.5) FIPS 140-2 Level 2 (FPX 1.0) FIPS 140-2 Level 1 & 2 (FAZ 5.2) FIPS 140-2 Level 1 & 2 (FMG 5.2) FIPS 140-2 Level 1 & 2 (FCT 5.0) FIPS 140-2 Level 1 & 2 (FML 6.0) FIPS 140-2 Level 1 & 2 (FWB 5.6) **Network Device collaborative Protection Profile (NDcPP):** NDcPP + FWcPP + IPS +VPN (FOS 6.2) CC EAL4+ (FOS 6.2) NDcPP (FPX 1.0) NDcPP (FMG 5.2) NDcPP (FAZ 5.2) NDcPP (FML 6.0) NDcPP (FWB 5.2)
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**	2023 Sustainability Report / Performance data p. 46
Managing systemic risks from technology disruptions	Description of business continuity risks related to disruptions of operations	**TC-SI-550a.2**	2023 Sustainability Report / Addressing cybersecurity risks to society p. 15-23

Verification Opinion

Submitted to:	Fortinet
Verification Body:	TÜV SÜD America, Inc. - Ruby Canyon 743 Horizon Court, Suite 385 Grand Junction, CO 81506 (970) 241-9298
Lead Verifier:	Garrett Heidrick garrett.heidrick@tuvsud.com
Submitted:	4/3/2024

TÜV SÜD America, Inc. - Ruby Canyon conducted the verification of Fortinet's 2023 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 2023
- 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 RCE's attention which gives cause to believe that the GHG statement is not a fair representation of GHG data and information.

RCE 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 RCE's verification opinion without RCE's prior authorization, as long as the verification opinion is reproduced in its entirety, including the date.

Lead Validator/Verifier Signature

Garrett Heidrick

Independent Reviewer Signature

Michael Coté

Looking-forward 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