2022 Sustainability Report

FORTINET

Who we are

Fortinet: making possible a digital world you can always trust.

Fortinet's mission is to protect people, organizations, devices, and data from today's growing cyberthreats—ensuring that everyone has reliable and secure access to the critical digital resources they rely on in their professional and personal lives.

Fortinet has been a driving force in the convergence of networking and security for over 20 years, delivering cybersecurity everywhere you need it with the largest integrated portfolio of over 50 products. Well over half a million customers trust our solutions. We are accelerating the evolution of cybersecurity through innovative solutions designed to increase visibility and control, reduce complexity, improve operational efficiency, and lower total cost of ownership.

This unique approach is why the world's largest enterprises, service providers, governments and public organizations choose Fortinet to enable their digital journey. We are uniquely able to provide consistent security for every endpoint, network, and cloud.

Corporate headquarters:
Sunnyvale
California, U.S.A

Number of locations:
90+

Year founded:
2000

Number of employees:
12,500+

Number of global patents issued:
1,285

Included in:
Nasdaq 100 and **S&P 500**

FY 2022 financial highlights:
$4.42B in revenue
$2.26B cash and investment
$512.4M spend in R&D

Number of customers:
635,000+

Market capitalization (as of December 31, 2022):
$38.2B

Table of contents

Letter from our CEO

Fortinet has been a cybersecurity leader for two decades. Over this time, cybersecurity has transitioned from a technology strategy to a sustainability issue—critical to the resilience of the digital society we all live in. This need for a secure digital world reinforces our commitment to innovating in the areas of networking and security. Our goal is to guarantee that critical infrastructure and applications remain protected amid the rapid evolution of digital transformation and cybercrime.

2022 was a year marked by new global challenges, ranging from the worldwide energy crisis to looming fears of a recession, massive layoffs across segments of the technology sector, supply chains recovering from the global pandemic, and the Ukraine war—events that impacted us all. Fortinet has been very responsive to the needs and demands of the market in these challenging times. We also understand that integrating sustainability into our business is not just a priority. It's a necessity.

We are actively implementing our sustainability strategy across our most material areas to fulfill our vision of making possible a digital world you can always trust. In this second Sustainability Report, we share the progress we have made along our journey. We have found that while there are areas in which we are leading, there are also areas where we can do even more. We continue to prioritize the security and privacy of individuals and organizations to enable digital progress and establish sound governance across our entire value chain. And we remain committed to the vital issues of climate change and resource scarcity that impact us and our stakeholders.

Our commitment to the environment and our efforts to curtail climate change are reflected in our product innovation and manufacturing standards, the eco-footprint of our facilities, and our support of environmental policies and regulations. As a further demonstration of our efforts to reduce our environmental impact and emissions, in 2022 we signed on to the Science-Based Target Initiative (SBTi).

Fortinet has also taken a leadership position in tackling the cybersecurity skills gap, which is critical to fulfilling our mission of protecting society from cyber risks. We have concentrated on skilling, upskilling, and reskilling individuals to create a larger and more diverse cybersecurity workforce. In 2022, at the White House National Cyber Workforce and Education Summit, we announced the expansion of our existing free training offerings, focusing on schools as part of our strategy to help reach our goal of training one million people in cybersecurity by 2026.

I am proud of our overall sustainability journey and the progress made in 2022. One evidence of this progress is that Fortinet is now a member of the Dow Jones Sustainability Indices (DJSI) — World and North America. Our inclusion is a testament to our ongoing action and dedication to building a more secure and sustainable world for all. We will continue to focus on our sustainability efforts in 2023 in partnership with our employees, partners, customers, and suppliers to realize our broader corporate vision of making possible a digital world you can always trust.

Ken Xie
Fortinet Founder & CEO, Chairman of the Board

> "We also understand that integrating sustainability into our business is not just a priority. It's a necessity."

Cybersecurity is a sustainability issue

Our society and its economy are increasingly dependent on digital data and applications. Digitization has taken over nearly every aspect of our lives, from communications and entertainment to running our households, purchasing goods and services, and even interacting with our colleagues, friends, and family. Likewise, nearly all the critical infrastructure and services our society depends on, whether energy, transportation, healthcare, communications, finance, or public services, are now digitized and connected to the internet. These changes have completely transformed how we work, live, and interact with others. Billions of people worldwide now rely on—and even take for granted—services and resources that didn't even exist a few years ago.

Key fact

$8.4T global **cost** of **cybercrime** in 2022

$11T predicted global **cost** of **cybercrime** in 2023

The critical need for cybersecurity

The flip side of this new digital world is that any disruption to these operations and services, including the loss or compromise of critical data, the interruption of critical services such as power plants or payment systems, and possible physical damage, all caused by cyberattacks, can place individuals, organizations, nations—and even the global economy—at risk. And that risk is more real than people realize. That's why cybersecurity is now as essential for society and its economy as healthcare is for humans. Shut down the internet, and our world comes to a standstill.

Cybersecurity is a necessary condition for the sustainability of our modern society because it is critical for protecting and maintaining the following **four foundational elements:**

— **Cybersecurity is a condition of digital privacy and individual protection:** Digital privacy is a human right. Cybercriminals who steal private and sensitive information such as—financial, medical, and employment records or government-issued information—can expose and disrupt the lives of individuals; a disruption from which it can take months or years to recover. Similarly, disruptions to critical infrastructure, like sanitation and clean water, or the compromise of safety measures at industrial facilities, can put people's lives in danger.

— **Cybersecurity is a condition of business resiliency:** The World Economic Forum's Global Risk Report 2022 ranks cyberattack as one of the world's top five risks. And according to Statista, the global cost of cybercrime, estimated at $8.4 trillion in 2022, is predicted to surpass $11 trillion in 2023. Attacks targeting infrastructure (such as power plants and supply chains), services (such as banks or web hosting), and connected devices have significant disruptive potential and can cause severe damage to business.

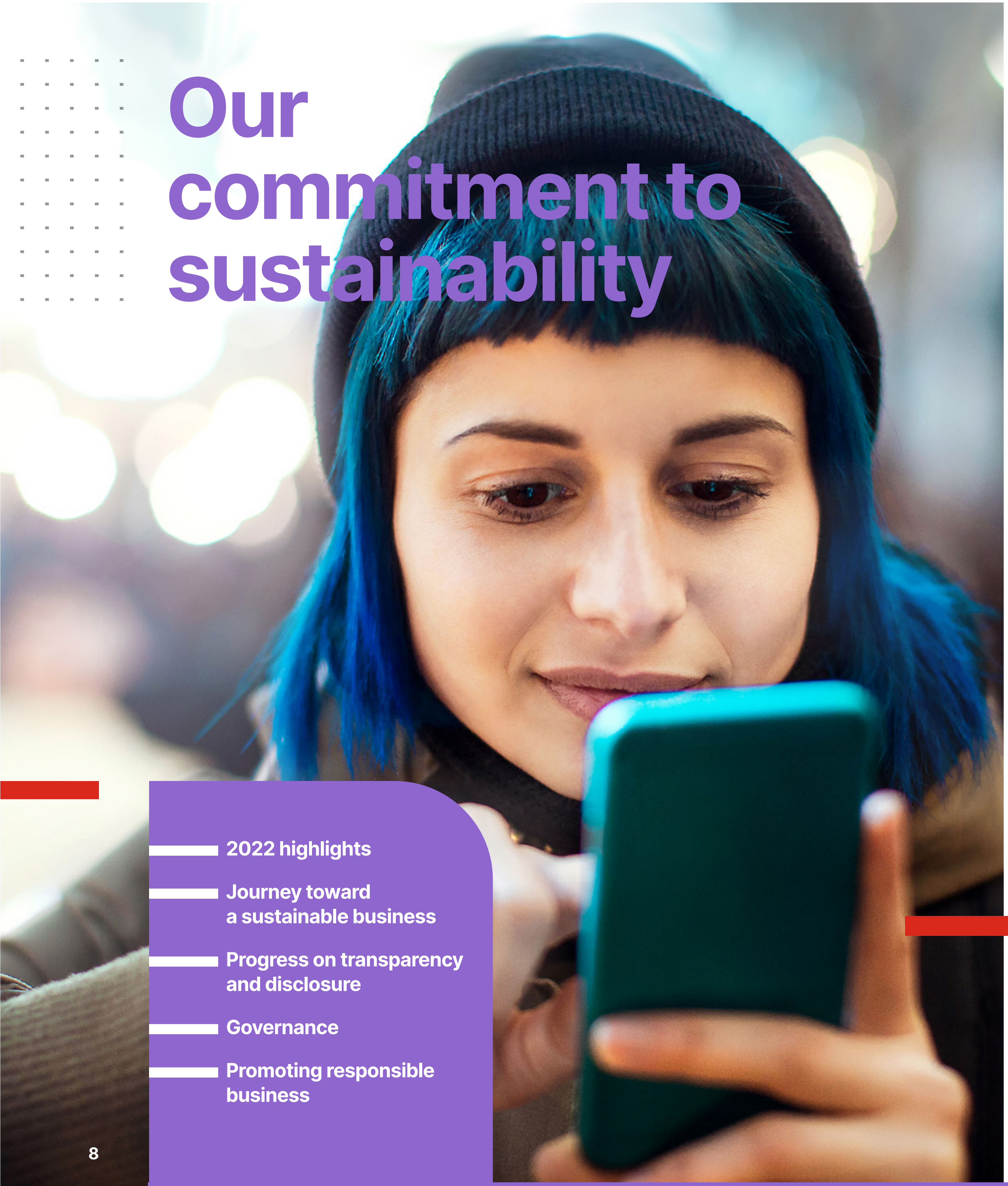
— **Cybersecurity is a condition of national security:** The vitality of today's societies and national economies depends on a secure cyberspace. Ensuring their safety and resiliency against hacktivists, nation-states, cyber threat actors, and cybercriminal organizations is paramount. Everything from political stability to protection from physical harm to economic health is at stake in the event of an attack on a country's cyberspace infrastructure.

— **Cybersecurity is a condition of digital trust:** Trust is an essential element of every transaction, whether buying goods and services online or international diplomacy. With the rapid evolution of digital technology and tools (deep fakes, data manipulation, etc), trust can be undermined. This is why it is imperative to have systems that ensure authentication and maintain data and system integrity to protect individual privacy, intellectual property, and digital transactions.

Because of its role in ensuring the future of our society, cybersecurity is no longer just a technology concern, it must be treated as a sustainability issue. Today, it is an essential element of business governance and data ethics.

Cybersecurity, like climate change, gender equality, diversity, and business ethics, must be part of every company's sustainability initiative. Every organization must put the proper measures, processes, and governance in place to ensure that the digital world we all rely on is safe, reliable, and sustainable.

Barbara Maigret
SVP, Global Head of Sustainability, Fortinet



Our commitment to sustainability

2022 highlights

Innovating for a safe internet

200,000+
pieces of malicious cyber infrastructure were disrupted as part of **INTERPOL's anti-cybercrime operation in Africa**

5
new product families and services designed to support security teams in the arms race against cybercrime

13
new information security certifications and assessments completed, including SOC2, HIPAA, TISAX

Respecting the environment

Committed to the Science-based Target Initiative (SBTi) and published for the first time our Scope 3 emissions

SCIENCE BASED TARGETS

66%
average reduction in **product energy consumption***

100%
biodegradable packaging for FortiGate-40/60/70F series

Based on new models of 2022 FortiGate F series (compared to equivalent models from previous generation).

Growing an inclusive cybersecurity workforce

219,465
people trained in cybersecurity as part of our goal to reach 1 million individuals trained in cybersecurity by 2026

Best Workplace
recognition from **Great Place to Work** and **Glassdoor**

+39%
year-on-year increase in **women hired**

Promoting responsible business

Training
on the impacts of Human Rights throughout the product lifecycle delivered to key business units

100%
of our key contract manufacturers*

>90%
of our distributors globally

completed Fortinet's training on compliance and business ethics

** Representing >90% of spend.*

Journey toward a sustainable business

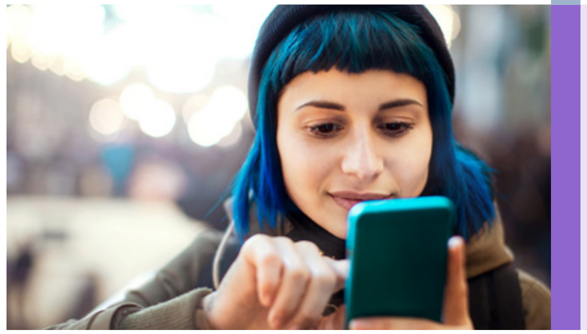
We are on a journey toward embedding sustainability into our business model and every aspect of our business operations. In 2021, Fortinet conducted a materiality assessment to prioritize the sustainability issues most significant to our business and primary stakeholders—those essential to achieving long-term sustainability performance. This materiality assessment helped us understand what matters most to Fortinet in order to continue to forge a path toward building a responsible and sustainable business. It has also allowed us to establish a direction for prioritization and strategy development.

The sustainability reporting landscape is evolving rapidly, including those related to sustainability framework standardization and materiality assessments. In 2022, the U.S. Securities and Exchange Commission (SEC) published for comment new climate-related disclosure requirements for public companies and proposed amendments to its rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting. The International Sustainability Standards Board (ISSB) also published for comment two exposure drafts on climate-related disclosures and sustainability-related financial information. The SEC and the ISSB are expected to finalize these drafts in 2023. Fortinet continues to closely monitor these developments and will adapt our reporting practices to conform to regulations and stakeholder expectations accordingly.

Vision and Corporate Social Responsibility (CSR) pillars

Our company vision, a digital world you can always trust, is essential to achieving just and sustainable societies. At Fortinet, we believe it is our corporate social responsibility to deliver on this vision by innovating sustainable security technologies, diversifying cybersecurity talent, and promoting responsible business across our value chain.

Our CSR pillars and priority issues are outlined below:



Promoting responsible business

We are committed to doing business ethically in respect with human rights and in compliance with all laws. Our corporate governance practices aim to ensure accountability to meet our responsibilities across our entire value chain.

PRIORITY ISSUES
— Business ethics
— Responsible product use

Innovating for a safe internet

We believe that ensuring the digital security and privacy of individuals and organizations enables digital progress, and we strive to create value through security innovation, expertise, research, and cooperation.

PRIORITY ISSUES
— Cybersecurity risks to society
— Information security and privacy

Respecting the environment

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

PRIORITY ISSUES
— Product environmental impacts
— Environmental management and climate change impacts

Growing an inclusive cybersecurity workforce

We are committed to building an inclusive, equitable, and diverse workforce within our organization and across the industry to help empower individuals to reach their full potential.

PRIORITY ISSUES
— Diversity, equity and inclusion
— Cybersecurity skills gap

Stakeholder engagement

We understand the importance of listening and engaging with our stakeholders across our value chain and using the feedback we receive to further our sustainability journey. We engage our stakeholders proactively and throughout the year. The chart indicates some of the ways we engage with stakeholders, the nature of these engagements and the relevant areas where stakeholders weigh in on our strategy.

STAKEHOLDER GROUP	HOW WE ENGAGE	TOPICS
Customers	— Request for proposals (RFPs) — Customer meetings — Sustainability assessments — Customer forums and events — Digital marketing and communications	— Greenhouse Gas (GHG) emissions — Carbon footprint — Product lifecycle — Products and solutions environmental impacts — Human rights — Data privacy and security
Employees	— Internal communications — Employee engagement—challenges, virtual events, mentoring, and workshops — Employee resource groups (ERGs) — Onboarding — Company policies — Trainings	— Women in cybersecurity and women in leadership positions — Diversity and inclusion — Environmental management and eco-friendly initiatives — Product sustainability — Sustainability strategy — Compliance and business ethics — Cybersecurity awareness
Industry associations	— Collaboration with TSIA, ETSI, MEF, WiFI Alliance, 5G-ACIA and ISA — Information sharing with government security agencies, INTERPOL, and regional computer emergency response teams (CERT)	— Adoption of standards and interoperability across the industry — Coordination of investigation of global security incidents — Threat intelligence sharing — Peer group benchmarking in support service and customer success
Communities and NGOs	— Partnerships with education outreach organizations — Supporting academia and governments on cybersecurity awareness and curriculum — Programs and partnerships focused on upskilling, mentoring, and donations	— Cybersecurity education — Talent diversity with focus on under-represented groups — Women in Science, Technology, Engineering and Mathematics (STEM) — Cybersecurity skills gap — Digital divide
Partners	— RFPs — Meetings — Marketing/communication campaigns — Trainings — Partner Code of Conduct — Vendor risk assessment	— Sustainability approach — Compliance and business ethics — Product environmental compliance — Carbon footprint of product in use — e-waste — Human rights
Shareholders and investors	— Sustainability reporting — 1:1 engagement with shareholders — Investor calls — Analyst calls — 10K — Proxy	— Sustainability strategy and progress — Climate change — Environmental management — Governance — Diversity, equity and inclusion (DEI)
Suppliers	— New product introductions — Trainings — Supplier Code of Conduct — Supplier assessments / reviews	— Sustainable product design and manufacturing — Ethical practices — Human rights — Regulatory and compliance

Progress on transparency and disclosure

We are committed to improving the transparency of our sustainability efforts. In 2022, Fortinet published its inaugural sustainability report, continued to improve disclosure on its public website and actively engaged with sustainability assessments from rating agencies most relevant to its business and primary stakeholders. Our efforts to further align with global reporting frameworks helps improve the communication and quality of the sustainability information we share with our key stakeholders.

ESG rating agency scores

Dow Jones Sustainability Indices

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

S&P Global

Fortinet, Inc.
Software

Industry Mover
S&P Global ESG Score 2022

57 /100

As of February 7, 2023.
Position and Score are industry specific and reflect exclusion screening criteria. Learn more at spglobal.com/esg/yearbook

S&P Global Sustainable1

EcoVadis

BRONZE
2022
ecovadis
Sustainability Rating

MSCI

MSCI
ESG RATINGS
A

CCC	B	BB	BBB	A	AA	AAA

Progress on environmental disclosure

CDP

Fortinet submitted its CDP report for the first time in 2022 and received a B- score.

CDP
DRIVING SUSTAINABLE ECONOMIES

Alignment to TCFD

In 2022, we began aligning our climate strategy and disclosures to the TCFD framework (see our TCFD index on page 58 for more information).

TCFD
TASK FORCE ON CLIMATE-RELATED FINANCIAL DISCLOSURES

— **Governance:** The board's Social Responsibility Committee (SRC) oversees climate-related risks and opportunities as part of its responsibilities overseeing Fortinet's objectives, strategy, and risks related to sustainability.

— **Strategy:** Through its participation in the CDP assessment, Fortinet provided a detailed qualitative description of specific climate-related issues with impact on the organization covering short-, medium-, and long-term time horizons. Work has been done to qualitatively describe scenarios associated with transition and physical risks to address specific requirements of the TCFD framework.

— **Risk management:** As part of 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 management priorities.

— **Metrics and targets:** In 2021, Fortinet publicly disclosed Scope 1 and Scope 2 emissions and committed to future disclosure of Scope 3 emissions. In 2022, we fulfilled this commitment by conducting the inventory and measurement of our Scope 3 emissions and identifying those categories most significant to our business. Scope 3 emissions are disclosed on page 53 of this report.

United Nations Sustainable Development Goals (UN SDGs)

Last year, Fortinet conducted a prioritization exercise to assess the tangible impact we can create through our various initiatives to contribute to the achievement of the UN SDGs. In an assessment facilitated by our sustainable business partner BSR, we chose the five UN SDGs—Gender Equality (5), Affordable and Clean Energy (7), Decent Work and Economic Growth (8), Reduced Inequalities (10) and Climate Action (13)—where we can have the maximum impact. In 2022, due to the significance of the cybersecurity skills gap and our public goal of training 1 million people in cybersecurity by 2026, we added Quality Education (4) to our reporting.

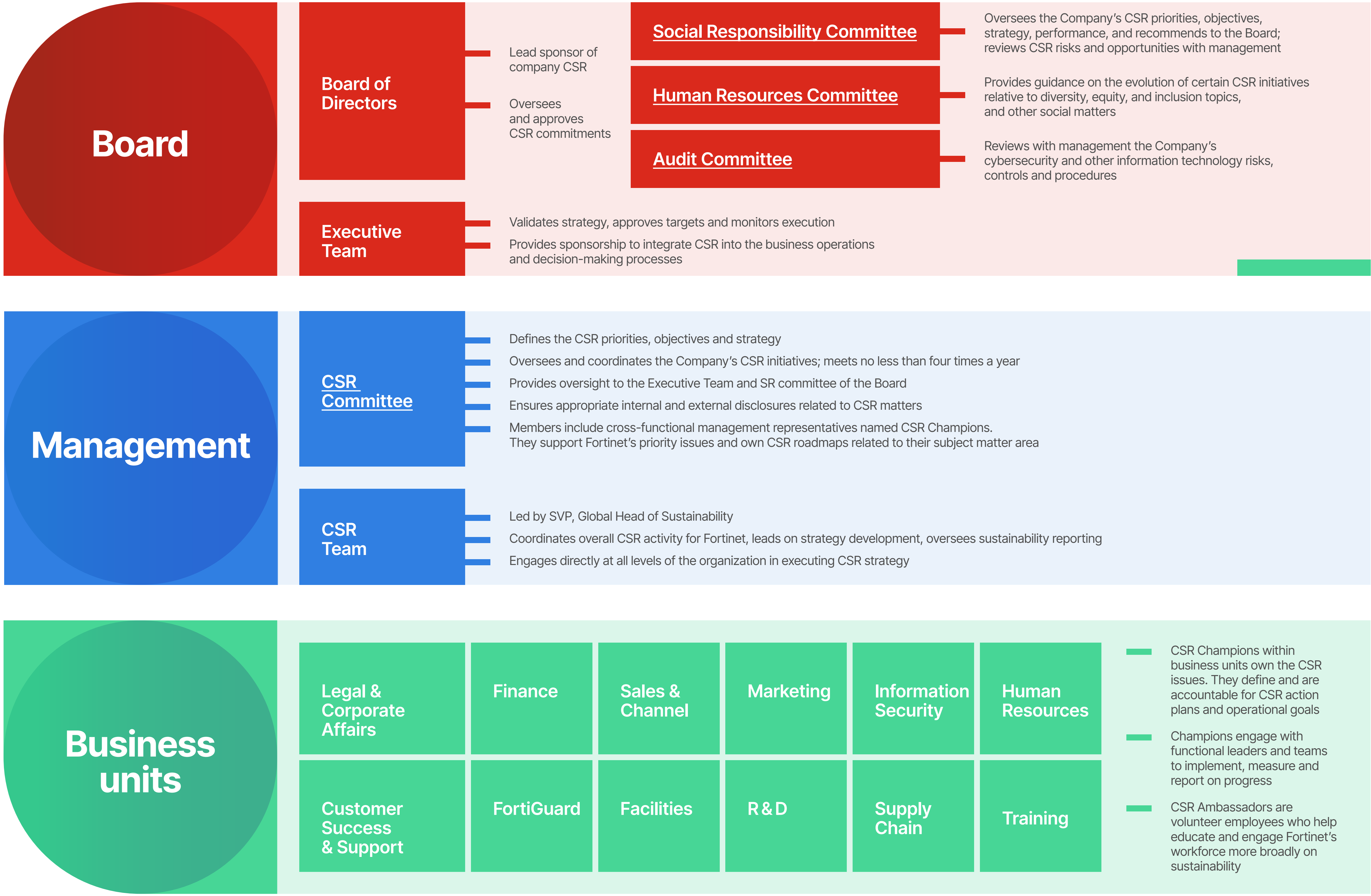
SUSTAINABLE DEVELOPMENT GOALS
13 CLIMATE ACTION
4 QUALITY EDUCATION
5 GENDER EQUALITY
7 AFFORDABLE AND CLEAN ENERGY
10 REDUCED INEQUALITIES
8 DECENT WORK AND ECONOMIC GROWTH

GRI and SASB

In addition to the TCFD recommendations, we align our disclosures with the GRI and SASB reporting standards. These disclosures ensure we can highlight our year-over-year progress and publish standardized data that enables benchmarking across businesses and sectors. Our indices are available at the end of this report on pages 62-67.

Governance

Our approach to corporate social responsibility is based on a strong corporate governance structure, starting with our Board of Directors. The Fortinet Board's Social Responsibility Committee (SRC) oversees Fortinet's sustainability programs, including environmental, social, and governance (ESG) matters every quarter. The SRC is supported by the management-level Corporate Social Responsibility Committee, which defines our CSR strategy, priorities, and objectives, and drives CSR initiatives across the value chain. As appropriate, the SRC collaborates with other Board committees, such as the HR Committee, which oversees DEI-related issues, and the Audit Committee, which oversees information security. In 2022, Fortinet's Board participated in a training session dedicated to climate change. With this training, board members deepened their understanding of climate risks, future climate-related financial disclosures, and integration of climate risks into enterprise risk management processes in the context of evolving expectations of boards to provide climate oversight.



Board

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

Social Responsibility Committee – Oversees the Company's CSR priorities, objectives, strategy, performance, and recommends to the Board; reviews CSR risks and opportunities with management

Human Resources Committee – Provides guidance on the evolution of certain CSR initiatives relative to diversity, equity, and inclusion topics, and other social matters

Audit Committee – Reviews with management the Company's cybersecurity and other information technology risks, controls and procedures

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 the CSR priorities, objectives and strategy
- Oversees and coordinates the Company's CSR initiatives; meets no less than four times a year
- 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 named CSR Champions. They support Fortinet's priority issues and own CSR roadmaps related to their subject matter area

CSR Team
- Led by SVP, Global Head of Sustainability
- Coordinates overall CSR activity for Fortinet, leads on strategy development, oversees sustainability reporting
- Engages directly 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 within business units own the CSR issues. They define and are accountable for CSR action plans and operational goals
- Champions engage with functional leaders and teams to implement, measure and report on progress
- CSR Ambassadors are volunteer employees who help educate and engage Fortinet's workforce more broadly on sustainability

Promoting responsible business

We are committed to conducting business ethically and in compliance with all laws. Our approach to responsible business is based on strong corporate governance practices that aim to ensure accountability while meeting our responsibilities across our value chain. Being a responsible business is our social license to operate and core to our business, as is protecting human rights. It is important for Fortinet to design, develop, deploy, sell, and manage products and services in ways that are both ethical and respect human rights. We firmly believe and are driven by the fact that our business and the products and solutions we produce are a force for good.

Business ethics

We are focused on good governance and ethical practices throughout our business. Our Board of Directors frequently reviews our governance practices to ensure that they are appropriate and reflect our company's maturity. Our cross-functional Ethics Committee meets quarterly, helps set the proper tone at the top, and takes specific action to ensure a culture of ethics and integrity.

To promote ethical business practices, we have adopted policies that set out a Business Code of Conduct for all employees, partners, suppliers, and vendors. We also have trainings and controls designed to prevent corruption in our business. These trainings cover a wide range of business ethics issues including anti-corruption, anti-bribery, and conflict of interest. In addition, our Employee Handbook sets out Fortinet's core values and mission to our employees and details procedures for our work environment.

Fortinet expects all employees to take business ethics seriously and requires them to complete mandatory annual ethics and compliance training.

We have more stringent requirements for our sales staff and executives, requiring them to complete special compliance training every six months and get certified in compliance every quarter. We hold our employees, teams, partners, and end customers to the highest ethical standards. In 2022, Fortinet introduced two mandatory Compliance and Business Ethics trainings: one for our key contract manufacturers (representing >90% of spend) and one for our distributors globally.

Integrating human rights into our operations

We work closely with our suppliers and vendors to ensure they understand our expectations concerning business ethics. All our core policies are reviewed and updated, if necessary, each year to make sure they are relevant and keep pace with developments in this space. To that end, in 2022, we expanded the human rights language in all compliance and business ethics training. We also updated our supplier and partner codes of conduct to include explicit references to our environmental and human rights policies.

We are making progress year-over-year in ensuring due diligence throughout our value chain. New direct suppliers added into our enterprise resource planning system must be processed through a two-step verification process, including a screening in high-risk areas. Our direct suppliers and vendors are screened against several criteria, including human rights, U.S. Foreign Corrupt Practices Act, and sanctions lists. In 2022, Fortinet selected five of its top contract manufacturers (representing approximately 80% of spend) to participate in EcoVadis's supply chain assessment. Also, in 2022, as part of Fortinet's ongoing due diligence and commitment to compliance, we conducted an internal audit to assess the different controls for Third Party Risk Management.

Lastly, we continue to encourage any Fortinet stakeholder, including our employees, to report any known or suspected violations of Fortinet policies or the law as per our Whistleblower policy. This policy describes the avenues, including the whistleblower hotline operated by third-party NAVEX, through which employees and business partners can report any unethical practice without fear of reprisal.

Compliance and Business Ethics trainings:

100% completion by our key contract manufacturers

91% completion by our distributors globally

Responsible product use

We are committed to ethically designing, developing, selling, and managing products and services in ways that respect human rights. Fortinet respects human rights as set out by the UN Guiding Principles on Business and Human Rights. We have set organizational standards, principles, values, and norms that govern the actions and behavior of individuals and organizations within our value chain.

In 2022, Fortinet embedded human rights clauses in its service agreements. We also updated existing clauses on human rights and ethical business in our agreements with contract manufacturers, including human rights language in our product license agreement, product datasheet template, and in our partner and supplier codes of conduct. Additionally, we expanded coverage of human rights in our various mandatory trainings on compliance and business ethics.

Our Human Rights policy applies to our broader value chain globally. We are committed to respecting the human rights of all our stakeholders including the users of our products and services. We will continue to update and enhance this policy by including aspects of human rights risks most relevant to our business and stakeholders as they evolve.

To continue in our efforts to integrate human rights and responsible product use aspects into our operations and make them actionable, employees in key business units at Fortinet attended a human rights training conducted by BSR. The training emphasized how employees must consider human rights throughout the product lifecycle, from design and development to licensing and use.

Innovating for a safe internet

Cybersecurity risks to society

Information security and privacy

Cybersecurity risks to society

Globally, we are rapidly transitioning to a digital economy. Vital and critical infrastructure and services, as well as our work and personal lives, all operate within a digitized environment. As a result, the disruption of operations or services or the loss or compromise of data due to cyberattacks places every individual, organization, and even nation—at risk. In this context, Fortinet strives to provide its customers with the best digital protection through innovation, anti-cybercrime partnerships and customer success services.

Driving innovation

We are deeply committed to innovation as evidenced by our nearly 1,300 patents, with hundreds more pending. What sets us apart further, allowing us to advance the cybersecurity industry, is the cadence at which we introduce innovations into the market combined with the vast number of solutions they encompass.

In 2022, for example, Fortinet launched five new offerings designed to support security teams in the arms race against cybercrime. Innovation is centered on our commitment to providing organizations with a broad, integrated, and automated solution strategy designed to span and adapt to today's highly dynamic hybrid networks.

PROGRESS

Goal: create a safer internet for all and advance cybersecurity

200,000+ pieces of malicious cyber infrastructure were disrupted as part of INTERPOL's anti-cybercrime operation in Africa

32,639 points mapped and analyzed for disruption opportunities in the cybercriminal ecosystem through WEF's Cybercrime ATLAS

5 new product families and services designed to support security teams in the arms race against cybercrime

Broad protection of the ever-expanding attack surface to better manage risk

Fortinet is innovating to deliver the broadest portfolio of security technologies in the industry, with solutions designed to cover the entire attack surface. Central to that innovation—and the core of our security fabric—is FortiOS, an operating system that consolidates a vast portfolio of network and security technologies into a single solution.

1,285 patents issued and 255 patents pending

In 2022, Fortinet released a new version of its operating system that included over 300 new features to further enable the convergence of networking and security for consistent, coordinated security across any network edge at scale.

Because our customers increasingly rely on flexible, hybrid environments, Fortinet security solutions remains agile, ensuring they remain protected even as their networks evolve. This unified approach spans remote employees, applications deployed across multiple clouds, virtual and physical data centers, and distributed networks.

FOCUS

Journey to the cloud

As organizations continue to go through digital acceleration, their information technology (IT) environments sprawl across multiple private and public clouds and services. This results in operational complexity, loss of visibility, potential misconfigurations, and increased cyber risk.
Fortinet continues to innovate to protect its customers in the different phases of their cloud journey by introducing enhanced and new solutions, services, and partnerships. In 2022, we launched a new cloud-native protection platform across Microsoft Azure, Google Cloud, and AWS cloud services. The solution is based on patented technology that produces context-rich, actionable insights, so security teams can prioritize the remediation and mitigation of risks that have the highest potential impact on cloud workload security, without slowing down business.

5G

5G is starting to deliver new and exciting use cases in areas such as Industry 4.0, smart cities, smart healthcare, to name a few. These are enabled and driven by advanced 5G networks, edge compute site deployments, and the creation of value-add ecosystems. To accelerate the adoption of 5G in critical use cases, Fortinet launched in 2022 a new series of hyperscale firewalls that set new standards for security, scale, performance, and latency. These firewalls empower telco operators and managed service providers to secure their 5G networks and services to drive value and growth in the marketplace.

Operational Technology (OT)

As organizations digitize their operational processes, they expose their OT networks to cyber threats while facing potential major disruptions of their operations that can seriously impact their business and the broader society.
Fortinet leads on delivering cybersecurity solutions that address the specific requirements of OT critical infrastructure. In 2022, Fortinet further enhanced its OT-specific capabilities by providing real-time industrial threat intelligence updates, introducing new ruggedized products for harsh operating environments, further integrating within global system integrators ecosystems, and offering specialized training programs to OT engineers.

Integrated protection to reduce complexity

Organizations are overwhelmed by the volume of security and networking solutions they have in place that do not interoperate. They struggle to share and correlate threat intelligence, detect threats, and deliver a coordinated response. To address this issue, Fortinet not only integrates the most extensive suite of networking and security technologies into its Security Fabric platform but extends this integration to a broad ecosystem of technologies and vendors, one of the largest in the industry.

Such an open ecosystem matters because it reduces operational complexity while ensuring compliance enabling interoperability, analytics, threat intelligence, centralized management, and automation*. In 2022, we reached a new milestone with over 500 tech integrations performed with 300 of our Fabric-Ready partners.

FOCUS

FortiGuard Outbreak Alerts

Chief Information Officer and Chief Information Security Officer teams must overcome significant challenges as they manage business-critical initiatives such as securing work-from-anywhere, enabling digital acceleration, and staying ahead of increasingly sophisticated cyber threats—all this while facing a shortage of skilled cybersecurity personnel globally.
To help these teams in their daily tasks, in 2022 we introduced a new service to our customers and partners: FortiGuard Outbreak Alerts. These alerts deliver important information when a cybersecurity incident/attack/event with large ramifications to the cybersecurity industry and affects numerous organizations occurs. They help organizations understand what happened, the technical details of the attack and provide timely steps to mitigate these breaking cybersecurity events. Last year we issued 30 Outbreak Alerts.

"Fortinet were the pioneers of using AI and ML to enhance Fortinet's security solutions by automating the analysis of malware and detect anomalous network activity. Fortinet has taken this further with the introduction of AI to simplify the day to day operations of the network and security in order to reduce the complexity for our customers."

Carl Windsor. SVP Product Technology & Solutions at Fortinet

500+ tech integrations

30 Outbreak alerts issued

* Fortinet Fabric-Ready Partner Program provides and incentivizes partners with program infrastructure, resources, and tools to integrate with the Security Fabric and develop joint solutions as part of the Fortinet Open Ecosystem.

Automated with AI-driven security for faster and stronger defense

To keep up with the volume, sophistication, and speed of today's cyber threats, security approaches and solutions must be enhanced with advanced technologies that enable automation, including Artificial Intelligence (AI) and Machine Learning (ML). Fortinet and its threat intelligence and research organization, FortiGuard Labs, have been at the forefront of AI and ML innovation for over a decade. These advanced technologies use deep learning and artificial neural networks to power our products and security services, enabling a faster, stronger, and more accurate defense. Such innovation not only allows organizations to mitigate risks brought on by automated cyberattacks with near-real-time coordinated protection, but also helps them stay ahead of emerging cyber threats by using advanced predictive capabilities.

THREAT RESEARCH IN NUMBERS

500+
dedicated threat researchers

609,000
hours of research into our AI/ML technologies

100+
billion global security events analyzed per day

Over one billion
daily security updates pushed to Fortinet's products

In 2022, Fortinet further pushed cyber automation by launching, among others:

— **A new network detection and response offering** powered by AI and other advanced analytics capabilities to help security operations teams quickly identify anomalies that may indicate a security incident in progress, analyze emerging threats in real-time, and automate responses to stop an attack and mitigate its impact.

— **A new network operations tool** that applies AI and ML to all network layers to bring visibility to network operations centers, improve response times to anomalies, and reduce ticket volume by proactively remediating network issues. This new solution not only identifies problems, but also provides recommended resolutions.

— **A new threat intelligence AI-powered security service** supported by our in-house global team of cybersecurity researchers that provides our customers and the cybersecurity community with timely actionable threat intelligence and real-time protection.

— **A SOC-as-a-Service** that detects network threats, identifies when a system is compromised, and provides information on malicious activities on the Dark Web directed at the organization. The service also works to fill in cybersecurity skills gaps by providing resources capable of monitoring the entire attack surface.

Partnering against cybercrime

Fortinet is committed to anticipating, analyzing, and disrupting cybercrime. But technology alone is not enough. We strongly believe that disrupting cybercriminals and dismantling the attack infrastructure requires solid and trusted relationships and partnerships with other public and private organizations. For us, sharing actionable threat intelligence between organizations and helping shape the future of mitigation against cyber threats is also vital.
Our key partnerships and joint initiatives in 2022 included:

— **MITRE Engenuity Centre for Threat-Information Defense:** as a research partner, Fortinet was a key contributor to several MITRE publications, which provide new threat intelligence frameworks and models on how attackers are conducting their criminal activity. This includes the Sightings Ecosystem and Attack Flow projects and the 2021 ATT&CK Sightings report. In the aforementioned report, we detail how FortiGuard Labs researchers helped analyze over one million attacks collected over 28 months using the MITRE ATT&CK framework, to provide contextual and actionable intelligence through threat informed defense.

FOCUS

World Economic Forum (WEF) Cybercrime Atlas

Fortinet is a founding member of the WEF Centre for Cybersecurity and an active contributor to Partnership Against Cybercrime (PAC), an initiative formed with the goal of building trusted public and private sector threat sharing relationships. In 2021, PAC created the Cybercrime ATLAS project, to map all major global cybercrime syndicates and develop a hub to link cybersecurity experts from the private sector to law enforcement and policy experts from the public sector. This hub allows experts to collaborate across sectors to identify strategic points of disruption and communicate on analysis techniques, new tools, new adversary behavior, tactical insights, and shared infrastructure. In 2022, the partnership, through deep dive analysis that spanned over 1,000 hours and involving over 20 members, identified 13 cybercrime syndicates, and mapped and analyzed 32,639 points for disruption opportunities in the cybercriminal ecosystem.

"Holistic disruption of cybercrime requires a global multi-stakeholder approach at scale. WEF Cybercrime ATLAS exemplifies public-private collaboration. As a founding grantor, Fortinet is committed to disrupting the cybercriminal ecosystem. Such initiative benefits us all by effectively creating a safer internet and mitigating cybersecurity risks to society."

Derek Manky, Chief Security Strategist & Global VP Threat Intelligence at Fortinet

.

— **NATO:** Fortinet participated in NATO Locked Shields. This breach and attack simulation exercise aimed at reducing risk by conducting realistic simulation attacks with defensive and offensive teams.

— **FIRST:** as a member of FIRST, a consortium of incident response and security teams from every country, Fortinet actively participated in discussions on industry collaboration, including during their annual conference in Dublin. At the conference, we were part of the keynote panel presenting to global and national computer emergency response teams and were featured in the post-conference report.

FOCUS

INTERPOL

Fortinet's partnership with Interpol Gateway includes sharing threat information generated by Fortinet's FortiGuard Labs global threat research team. In 2022, Fortinet participated in a capacity development campaign for law enforcement in Africa–Cyber SURGE–to counter cybercrime across the continent. Fortinet provided support and guidance to the campaign through curated threat intelligence for training exercises organized by INTERPOL for law enforcement teams from 27 countries across Africa.

Enabling customer success

Fortinet is focused on enabling and empowering its customers by providing them with the solutions, services, and threat intelligence that best protect their organizations. The key to enabling customer success lies in driving customer adoption, dedicated expertise and providing organizations with advanced services. To further help our customers optimize their cybersecurity implementation and reduce exposure to cyber threats and potential downtime, we introduced new services in 2022, including:

— **FortiCare Elite** is a new device-based service that provides a consolidated view of cybersecurity events experienced on FortiGate devices along with associated recommendations for those events.

— **Advanced Support portfolio** includes dedicated resources to be leveraged for consultancy and collaboration to optimize customer cyber implementation success and effectiveness.

— **'Community' Platform** on which customers can collaborate, share insights and experiences, and engage with their peers to receive advice and feedback.

Fortinet leverages data analytics to proactively address areas of weakness raised by the community, allowing the rapid resolution of issues and ongoing improvement of customer skills through knowledge sharing.

Information security & privacy

Fortinet provides organizations with advanced technologies and solutions to protect their IT infrastructure and data against evolving threats and assist them with their security compliance requirements. The same technology and solutions we provide to our customers are used to keep our own IT infrastructure and data secure. Our information security and privacy policies protect the confidentiality, integrity, availability, privacy, and resiliency of the Fortinet systems and the employee and customer data stored within the network.

What we do

Fortinet is constantly upgrading and improving its information security system to be best prepared to prevent and mitigate IT system failures and major cybersecurity incidents. We adopt and implement our own technology across our hybrid networks as well as organizational, administrative, and technical measures and processes based on industry standards. Those include National Institute of Standards and Technology (NIST) SP 800-161/53, ISO 270001/2, and other similar standards. We operate a Secure Product Development Lifecycle policy aligned with NIST 800-53 and 800-160 standards. Fortinet also adheres to ISO/IEC policies for vulnerability disclosure and handling processes.

In 2022, Fortinet completed SOC2 audits for several of its products. We also assessed two of our products for U.S. Health Insurance and Portability Accountability Act (HIPAA) compliance and completed the Trusted Information Security Assessment Exchange (TISAX)*audit.

PROGRESS

Goal: adopt innovative practices for infosec & data privacy, in line with globally recognized standards

13 new information security certifications and assessments completed, including SOC2, HIPAA, TISAX

Mandatory infosec & privacy training rolled out to 100% of Fortinet employees

Year-long global employee awareness campaign against phishing

* *TISAX is an automotive industry information security standard.*

FOCUS

Fortinet on Fortinet

In 2022, we continued to expand the implementation of Fortinet products and solutions. We also adopted new capabilities and features to protect our network and provide our R&D team with early feedback that will help further strengthen our cybersecurity solutions.

How we are building awareness

We aim to protect our brand, reputation, and resources by educating employees on vulnerabilities, escalating cyber threats, and enhancing digital self-defense actions. We have implemented a Security Champions Program to empower product development teams to embed security best practices into all levels of the product development lifecycle.

We also conduct annual internal campaigns, including ones focused on vigilance, training, and phishing, to ensure our workforce is educated on information security. In addition, we require all employees, including contractors and temporary workers, to complete mandatory annual information security and privacy compliance training. And we ensure that employees in select workforce roles and responsibilities have access to additional focused training on information security and privacy.

FOCUS

Fortinet employee awareness campaign against phishing

In 2022, Fortinet implemented a comprehensive, company-wide training awareness program on phishing to help its employees understand the importance of becoming a "human firewall," strengthen cyber resilience, and influence a security-forward culture.
We have continually tested employee readiness across the company by launching intermittent, targeted, and simulated attacks that reflect real world threats. Educational testing is meant to reinforce behavior modification, such as looking for red flags, emails that are out-of-the ordinary way of communicating, and/or spoofed email addresses to help employees identify true phishing attacks that may slip through email security filters.
Fortinet's phish alert button and reporting guidance empowers employees to take an active role in managing the ubiquitous problem of malicious emails and to always pause before clicking, hover over all hyperlinks to determine the true URL destination path and report any suspicious messages.

Phish Alert Report

How we respond to information security and privacy incidents

Fortinet security analysts and engineers leverage a "follow-the-sun model" to monitor, detect and provide rapid response to security incidents in adherence with NIST and other standards. They apply a systematic approach that includes the following steps: detect and analyze the threat; contain the impact; eradicate the threat; recover operations; remediate to prevent any reoccurrence. In parallel, Fortinet has a formal outreach process to collaborate with law enforcement and regulatory bodies, and industry vendors to address major global cybersecurity events that may affect our customers. We also have an established reporting procedure in the event of a data or customer privacy breach.

Respecting the environment

- Product environmental impacts
- Environmental management and climate change impacts

Product environmental impacts

Product environmental impacts are driven by two converging forces: the increasing pressure on businesses to reduce their impact on the environment and the global energy crisis that accelerated in 2022 and has resulted in resource scarcity and price inflation, putting the global economy at risk. Within this operating context, it has become critical for businesses to choose technologies that have the least impact on the environment. Since Fortinet's founding, it has been a strategic priority to consolidate multiple functionalities into a product to reduce its footprint. We are now focused on reducing the environmental impacts of our products throughout their entire product lifecycle. This includes design, manufacturing, product energy use and efficiency, and end of life. Every Fortinet product complies with all globally recognized product environmental compliance directives and regulations.

Minimizing product environmental impacts

Minimizing our environmental footprint has always been integral to Fortinet's DNA, not just at an operational level but also from a technological standpoint. Energy consumed by our products in use is largely contributing to our carbon emissions. Fortinet has combined innovation with environmental sustainability to reduce the use of energy, cooling, and space required for its solutions, helping customers minimize power consumption and GHG emissions. Today, we lead in power efficiency and are committed to further innovating to reduce the footprint of our solutions.

Goal: mitigating our product environmental impacts and support circularity

PROGRESS

66% average reduction on product energy consumption*

33% reduction on FortiGate 4200/4400F series size vs E series

100% biodegradable packaging for FortiGate-40/60/70F series

** Based on new models of 2022 FortiGate F series (compared to equivalent models from previous generation).*

FOCUS

Energy efficiency

Fortinet has leveraged a culture of innovation to not just develop effective security solutions but ones that also address environmental requirements. Our ability to consolidate multiple security technologies into a single appliance and have it powered by the industry's only custom-designed security processors (Fortinet ASICs) means that our customers benefit from strong security performance with a smaller footprint. Replacing multiple standalone solutions with a single integrated platform saves energy, cooling, and space. For example, the new FortiGate 1000F launched in 2022 consumes 80% less power than similar industry solutions. It also requires less cooling as it generates only 15% of the BTU/h per Gbps of firewall throughput compared to competitive firewalls.

Carbon calculator

To address increasing demand from customers for information on the carbon footprint of their solutions, Fortinet has developed a carbon footprint calculator for over 120 product models to help customers estimate the emissions of products in use. This calculator, whose methodology has been independently verified, is a testament to Fortinet's commitment to transparency on the environmental impacts of its products.

Space occupation

Fortinet's years of dedicated innovation means that each new generation of products uses less power and less space. By deploying one appliance instead of several, Fortinet reduces the space to host a product at a customer site while positively impacting transportation overhead by reducing shipping weight and volume. For example, we have reduced the size of our FortiGate 4200F and FortiGate 4400F appliances by 33% compared to the previous generation.

Meeting product environmental compliance

Fortinet is committed to meeting or exceeding all applicable environmental laws and regulations related to protecting 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 the materials we use and our waste management.

We comply with all environmental directives and regulations related to materials 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 WEEE Directive (Waste of Electrical and Electronic Equipment)

Improving product sustainability

Product packaging has been the first area we decided to focus on to improve product sustainability as it immediately becomes waste once a product is received at a customer site. To reduce our environmental impact, in 2021 we started using biodegradable packaging for our first-tier product models, engaging with our contract manufacturers. We have replaced plastics with biodegradable paper, cardboard, or recycled by-products. We have also designed specific compartments in our packaging to reduce or eliminate additional plastics bag for things like antennas and other accessories.

Since implementing this program, we estimate that nearly 424,000 boxes have been shipped in 2022 using this new eco-friendly (no-plastic) packaging on first-tier products. Building on this work, last year, we began redesigning the packaging for our second-tier products in collaboration with one of our key contract manufacturers. We now use 100% bio-degradable packaging for the estimated 500,000+ packaging boxes–equivalent to 50+ tons in weight–shipped in 2022 for our both first-tier products and second-tier FortiGate 40F/60F/70F appliances.

500,000+
boxes shipped with 100% eco-friendly packaging

Another priority area we started to work on in 2022 is product end-of-life. Our objective is to increase the repair or reconditioning to extend the product lifespan and improve material recycling. This echoes a growing interest from our customers. In 2022, we conducted a technical feasibility assessment on our top-shipped product lines to identify potential models that could be leveraged for reconditioning. We subsequently launched an internal pilot program (see below).

FOCUS

Refurbishing pilot program

Through our internal refurbishing pilot program launched in 2022, we have highlighted the power of the circular economy by taking back products and repairing for reuse and/or recycling. This program is helping us reduce e-waste and consequently, the carbon footprint typically generated at the end of a product lifecycle. In under three months, the pilot program has revived 1,901 eval units returned from employees in 30+ countries, with 508 units repaired for re-use.

Environmental management and climate change

Businesses are increasingly under pressure to address their climate change impacts and environmental management practices to ensure the sustainability of our planet. This pressure has already resulted in a surge of regulations and compliance requirements related to climate. Fortinet is committed to developing and implementing a robust climate change strategy in accordance with globally recognized reporting frameworks such as the TCFD.

Tracking our GHG emissions

In 2021, we reported for the first time on our Scope 1 and Scope 2 emissions, and we publicly committed to becoming carbon neutral by 2030, in alignment with the Science-Based Target Initiative. We also pledged to increase our climate disclosures and begin an inventory of our Scope 3 emissions to identify the emission categories that are most significant to our business. In 2022, we began and completed the inventory of our Scope 3 emissions, capturing the 12 categories relevant to our company as defined by the GHG Protocol (see page 53 for our comprehensive Scope 3 emissions data).

We consider two of these categories–purchased goods and services; and use of sold products–to be significant. To further engage on our path to carbon neutrality in alignment with the Paris Agreement, we formally signed on to the SBTi commitment in September 2022. We will develop a comprehensive decarbonization plan that will be vetted by SBTi and implemented by 2024.

SCIENCE BASED TARGETS

PROGRESS

Goal: reach Net 0 by 2030 across Scope 1 & Scope 2 emissions

Obtained **LEED-Gold certification** for our new HQ

Completed implementation of our **Environmental Management System**

Committed to the **Science-based Target Initiative** (SBTi)

FOCUS

Fortinet Act4Environment Challenge

Environmental considerations such as climate change, resource scarcity, and the energy crisis are top priorities for the future of our planet and society. Addressing these issues is everyone's responsibility, and Fortinet is committed to mobilizing its workforce by raising employee awareness of environmental issues. In 2022, for the first time, Fortinet organized the Fortinet Act4Environment Challenge–a one-month internal awareness campaign. During this campaign, we engaged with our employees to broaden their knowledge of environmental issues and understand how to reduce their personal carbon footprint through physical and eco-friendly activities. We estimate their collective impact during this one-month challenge at 2.24 tons of CO_2 saved.

> ***"I wanted to share that this challenge really opened my eyes to not only my own impact on the environment but also what Fortinet is doing to make a difference."***
>
> **Employee on environmental awareness campaign.**

Measuring our operational data

In 2022, we implemented an Environmental Management Systems (EMS) platform to track our energy, water, and waste impact (see pages 52-53 for our resource use data). The platform also calculates the carbon emissions from each of our owned facilities and estimates the energy use and subsequent carbon emissions for our 20 largest leased facilities. This EMS platform will allow us to track any additional sustainability projects and metrics related to our operational data.

Initiating decarbonization

To meet our ambitious net-zero commitment by 2030 and as part of our decarbonization plan, we are working cross-functionally to mitigate Scope 1 and Scope 2 emissions in owned facilities. Measures we have begun to adopt in 2022 include: ensuring that all our newly owned and leased sites can obtain renewable electricity; following green guidelines and checklists when sourcing locations; minimizing the use of natural gas in new construction; investing in renewable energy; and purchasing renewable energy certificates. As we integrate our Scope 3 emissions into our decarbonization plan, we will begin collaborating with suppliers and vendors to ensure alignment between their climate action plans and ours, to ensure that we are partners in achieving our net-zero goals.

Mitigating climate risks

Fortinet is in the process of identifying our owned and leased facility locations with the most climate, financial, and reputational risks in view of creating environmental management systems as appropriate. In 2022, Fortinet started the ISO 14001 certification process for its largest owned warehouse located in Union City, California.

Growing an inclusive cybersecurity workforce

- Diversity, equity, and inclusion
- Cybersecurity skills gap

Diversity, equity, and inclusion

Fortinet is building an inclusive workplace that empowers talent of diverse backgrounds to reach their full potential. We are committed to a diverse workforce with a global representation of all genders, races, ethnicities, nationalities, ages, and sexual orientations. We also ensure that all our employees have equal opportunity, fair recruitment, and equitable remuneration. Our offices are designed with employee needs and comfort at the core, with our owned offices offering ergonomic equipment, sports facilities, and other services to all employees. Fortinet's success is tied to our ability to attract and retain skilled talent and have our employees thrive in an engaging and inclusive work environment.

Where we stand on DEI

Fortinet is comprised of 12,500+ employees operating in over 90 countries. This diverse workforce contributes to and enriches our innovative culture. Beyond encouraging diverse perspectives, backgrounds, and knowledge, Fortinet cares about fostering an inclusive environment where our employees feel welcomed, respected, supported, and valued from day one. We believe that diversifying our workforce is critical to our future. Therefore, we are looking ahead to the work we still must do to improve organizational diversity, equity, and inclusion.

PROGRESS

Goal: increase diversity among workforce and promote a culture of inclusion and belonging

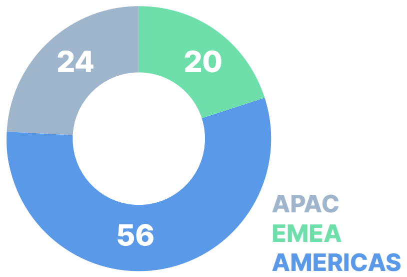
21% women in our workforce

+39% year-on-year increase in women hired

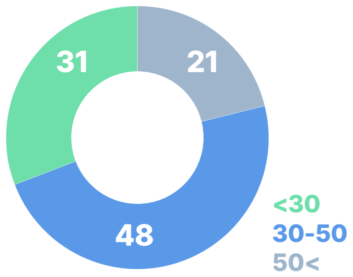
Best Workplace recognition from Great Place to Work and Glassdor

2022 KEY METRICS

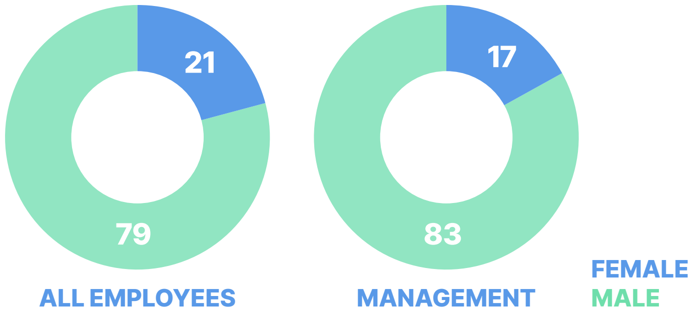
REGION (%)



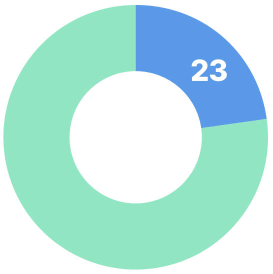
AGE (%)



GENDER (%)



FEMALE NEW HIRES (%)



FOCUS

Organizational governance

We have taken significant steps to improve and establish organizational governance around DEI, including developing a DEI strategy. These steps start with our top leadership levels. The Board of Directors' Human Resources Committee specifically provides oversight of Fortinet's organization and human resources activities, including DEI initiatives. In addition, we formed a global DEI Organizing Committee with members from the Human Resources and the Corporate Social Responsibility teams. In August 2022, we started to identify the DEI sponsors and council members. We held our first DEI Council meeting in October.

— **DEI sponsors:** we identified three DEI sponsors from our executive team. These sponsors are committed to promoting DEI as a business imperative to drive innovation and success.

— **DEI Council:** we convened a DEI Council comprised of a team of senior leaders selected for two years from across the organization. This DEI Council is part of a more extensive network of leaders, employees, and employee resource groups all directed toward elevating organizational DEI.

— **DEI strategy:** Fortinet's DEI strategy is co-created by the DEI Organizing Committee and DEI Council. It provides Fortinet with a shared direction and commitment to recruiting and valuing a diverse workforce, fostering a culture of teamwork and openness, and building a more inclusive workplace.

Progressing along our DEI journey

We are committed to fostering a diverse, equitable, and inclusive workplace. We work hard to create and maintain an environment in which employees feel welcomed, respected, supported, and valued across every stage of their journey at Fortinet, including:

Talent acquisition

We are focused on recruiting high-performing, innovative talent with diverse backgrounds. This starts by drawing from a vast pool of potential candidates to work in all areas of our organization.

— **Diverse recruitment:** we have specific incentivized targets for gender diversity and train our in-house recruiters to source female and other candidates from under-represented groups. We are diversifying the avenues through which we hire by considering internship programs, job fairs, delivering presentations to NGOs serving women, and training women in cybersecurity. We are also leveraging AI technology to reach out to female candidates and creating specific online campaigns and branding to recruit diverse candidates.

glassdoor BEST PLACES TO WORK 2022

Great Place To Work®

— **University recruitment:** we leverage Fortinet role models to promote careers in cybersecurity in schools and universities that cater to a more diverse student pool to attract more diverse candidates.

Onboarding

We work to ensure that every employee is set up for success from day one, beginning with our onboarding process that provides a seamless transition into a culture of teamwork, openness, and innovation. In addition to the company-wide onboarding program, some business units across Fortinet offer additional programs to help employees settle into the company. For example, in Latin America (LATAM), new system engineers during their first six months at Fortinet take part in a mentoring program that is part of their onboarding process.

Leadership development

At Fortinet, we have developed a leadership development curriculum to equip managers with the right tools and practices to be effective people leaders. We train our managers through targeted programs, self-directed learning, and coaching to support a diverse and ever-evolving workforce.

— Fortinet's flagship leadership development program is **Manage for Success**. This program aims to align management practices and build leadership acumen across Fortinet. This quarterly management foundations program trains participants in awareness, skill building, and capabilities enhancing components spanning multiple leadership areas. The program also includes thought leadership, instruction around unconscious bias, inclusive leadership, and "diversity 101."

— We hold **DEI trainings and workshops** as part of our commitment to ensure an inclusive environment. These include:
- DEI workshops for specific lines of business across Fortinet, including sales, consultant system engineering, customer success and support teams
- Unconscious bias training, available to all managers, to stimulate critical self-reflection and personal ownership for growth and generate actionable insights to help them improve their decision-making.

— We have implemented **leadership dashboards on gender diversity** to track our workforce composition. These dashboards are shared every quarter with Fortinet's senior leadership. They track female representation, hiring and retention within our workforce. And every six months, we report on our gender diversity goals and progress to-date to the Human Resources Committee of the Board of Directors.

Employee training and engagement

To maintain our inclusive culture and foster diversity, Fortinet offers trainings to all employees to help them increase their knowledge of DEI. Beyond formal training programs, we have introduced several initiatives to engage employees and celebrate diversity at Fortinet.

— **Employee resource groups (ERGs):** Fortinet's ERGs are voluntary, employee-led groups that serve as a resource for members by fostering a diverse, inclusive workplace. One example is Fortinet WEMS, an ERG launched in the U.S. in 2022 with the aim of uplifting women at Fortinet by providing them with opportunities to connect and support each other so that they are set up for success. The WEMS ERG promotes inclusion, collaboration, development, and career growth through mentoring and networking. Over 200 women accessed this newly formed ERG community last year, with the ERG holding six talks featuring guest speakers and panel discussions on topics relevant to women.

— **Regional programs:** to actively foster a culture of diversity and inclusion, we encourage our employees to define DEI programs at the regional level. This ensures that despite Fortinet's global footprint, we are respectful of local cultures and priorities. Therefore, we have many initiatives and programs activated at the local or regional levels to help our employees understand the impact of DEI and attract diverse candidates in our industry.

For example, in 2022, in Europe, Middle East and Africa region, we launched the following:
- The Fortinet Diversity Ambassadors & Allies program to promote a DEI culture internally and externally.
- A series of webinars to educate employees on understanding and promoting unconscious bias and promoting DEI in the workplace.
- Women4Cyber mentoring program in Europe to empower more women to join or further their careers in cybersecurity.
- Presentations at various graduate events and fairs to promote cybersecurity as a career to a diverse student body.

FOCUS

LATAM initiatives

We continue to expand our DEI initiatives across the region in 2022, working on our Women's LATAM network agenda through general meetings, happy hours, and focus groups. To increase the diversity of the cybersecurity workforce and encourage more women to participate in the industry, we are partnering with academic institutions in the region. In 2022, we deepened our partnership with Politécnico Grancolombiano (Colombia), FATEC (Guatemala), Galileo University (Honduras), Universidad Tecnológica Centroamericana UNITEC (Puerto Rico), and Universidad Politécnica de Puerto Rico (Mexico). We also conducted a few DEI-related workshops/presentations in the region, including a presentation on hacker girls in Colombia, and a master class with WOMCY conducted in Spanish and Portuguese in LATAM countries. The events led to the issuance of 775+ Network Security Expert (NSE) certifications.

"A truly diverse and inclusive culture is one in which every employee feels a sense of belonging, has opportunities to grow, express oneself, exchange ideas, and feel heard. In this culture, each one of us can improve the workplace with our individual words and behaviors. Everyone has the opportunity and holds the responsibility to make a difference every single day, even if it is just listening to and engaging with others."

Patel CHITTIMELLA, Fortinet EMEA Diversity Ambassador

200+

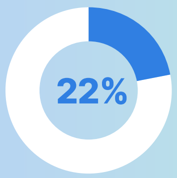
female employees joined the new US WEMS ERG

Cybersecurity skills gap

The cybersecurity industry faces a significant skills gap of 3.4 million professionals worldwide. This number has increased by 25% in just one year according to the 2022 Cybersecurity Workforce Study by (ISC)^2. This shortage affects all organizations worldwide. A recent global study from Fortinet demonstrates multiple risks resulting from the cybersecurity skills gap, including the prevalence of additional cyber risks for an organization. Most notably, 84% of organizations surveyed have suffered at least one breach they could attribute to a lack of cybersecurity skills or awareness. Through the Fortinet Training Institute, we are committed to empowering untapped talent pools, including women, students, veterans, and more, to reskill or expand their skills for a career in cybersecurity, helping to address the industry talent shortage.

PROGRESS

Goal: train 1 million people in cybersecurity by 2026 (FY22 base year)



As of December 2022, we have exceeded our goal for 2022, training over 210,000 people through various initiatives sponsored by the Fortinet Training Institute.

Driving broader cybersecurity awareness

Fortinet is narrowing the cyber skills gap by providing learning opportunities and educating more people from all walks of life in cybersecurity. Individuals remain the weakest link in the cybersecurity chain. Therefore, we consider it vital to educate all of society on cybersecurity fundamentals, beginning with schools.

FOCUS

Free cyber training in K-12 schools districts

Fortinet participated in the 2022 White House Cyber Workforce and Education Summit and shared its perspective on closing the cybersecurity skills gap through global cross-industry collaboration and dialogue. Tied to the Summit, Fortinet announced a free education-focused version of its Security Awareness and Training service for all K-12 school districts in the U.S. This service is designed to help administrators build a cyber-informed culture, through comprehensive training, a robust training platform and deployment guidance provided by Fortinet. With content incorporating threat intelligence insights from FortiGuard Labs, this service arms faculty and staff with the latest knowledge, guidance, and tips needed to make smarter choices when confronted with cyberattacks. Since September 2022, this free offering has been adopted by more than 100 school districts in 27 states, potentially helping over 143,000 staff and faculty members in U.S. schools become more cyber-informed and improve their skill sets to avoid breaches at educational institutions.

Fortinet free cyber training adopted by

100+

U.S. school districts

School districts (K-12) in the U.S. are increasingly focused on cybersecurity as they continue to adapt to the rapid digitization of the learning environment, transforming their networks to facilitate e-learning and other digital programs to enhance student curricula.

This digital transformation places data privacy and cybersecurity responsibilities on them. These districts must now provide a fundamental level of cyber awareness and training to their faculty and staff to ensure that the personally identifiable information stored on their networks remains secure. To address these needs in 2022 and beyond, Fortinet announced a new tailored version of its Security Awareness and Training service free of charge for all K-12 school districts in the U.S. This service has been updated to ensure it is education-focused and aligned with the NIST 800-50 and NIST 800-16 guidelines (see above for more information).

Fortinet has also enhanced its enterprise-grade Security Awareness and Training service as a new SaaS-based offering to help IT, security, and compliance leaders build a cyber-aware culture within their organizations. With this offering, employees can recognize and avoid cyberattacks, and organizations can satisfy their regulatory/industry compliance training requirements.

Diversifying the cybersecurity workforce

Fortinet is committed to closing the cybersecurity skills gap and providing access to a diverse audience through the following programs and partnerships:

— **The Academic Partner Program:** with more than 500 Authorized Academic Partners, Fortinet makes its award-winning curriculum available to students worldwide through partnerships with academic institutions. We continued to expand our partnerships with educational institutions in 2022 by adding partners from Spain, New Zealand, Morocco, Singapore and more. Our academic partner program operates in more than 90 different countries and territories.

— **The Education Outreach Program:** we partner with local and global non-profit organizations to create cyber career pathways for underrepresented populations, including women, veterans, and disadvantaged individuals. By providing training and certification opportunities and connecting individuals with the Fortinet employer ecosystem, we are working to help close the cybersecurity skills gap.

Partnering with
500+
educational institutions in
90+ countries

- **The Fortinet Veterans Program:** to meet the growing needs of veterans and military spouses and better transition them into the cybersecurity field, we introduced a new course entitled Networking Fundamentals in 2022. This course, which builds on to our existing free certification training and hands-on labs, offers a broader foundation for veterans entering the IT field or interested in continuing to the Fortinet NSE Certification program. We also initiated new partnerships with Cerco IT and Forge Institute to expand our applicant pool and provide participants with access to job boards and soft skills training.

- Fortinet expanded its partnership with **Women in Cybersecurity (WiCyS)** to develop cybersecurity knowledge and skills, and drive gender diversity within its membership. In 2022, we became a WiCyS Tier 1 sponsor and a VIP sponsor for their annual conference. In addition to offering WiCyS's 5,000+ members our free training initiative and free exam vouchers for certification, we also ran a dedicated NSE 4 Certification bootcamp for 100 members. In this bootcamp, participants gained technical knowledge through coursework, labs and one-on-one support from Fortinet Certified Trainers. Fortinet is also considering bootcamp participants for employment.

Upskilling cybersecurity professionals

Fortinet continues to help cybersecurity professionals, including Fortinet employees, develop, reskill, or upskill through the NSE Certification Program. Our globally recognized eight-level NSE Certification program offers users, including cyber professionals, a structured pathway designed to teach the necessary real-world skills required for both fundamental cyber awareness and a successful career in cybersecurity. In 2022, Fortinet announced that its NSE level 8 certification is now being offered online, making it accessible to more users and cyber professionals worldwide looking to achieve or maintain their certification.

The Fortinet Training Institute also helps combat cybercrime by offering free training–free access to all self-paced training courses from the certification program–to anyone interested in learning new cyber skills. The initiative offers 30+ technical courses (300 hours of curriculum) on critical topics ranging from secure SD-WAN to operational technology to cloud security.

Fortinet's cybersecurity training is delivered in local languages worldwide through **Fortinet's Authorized Training Centers (ATCs).** The ATCs are a network of accredited training organizations in 148 countries/ territories teaching in 26 different languages. In 2022, we added 10 new ATCs and one new teaching language–Hungarian.

About this report

Fortinet's 2022 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 in the footnotes, for the fiscal year 2022 (January 1, 2022–December 31, 2022).

The report references the GRI Standards, SASB Standards and the UN SDGs. This year, we are aligning our disclosures to the TCFD recommendations for the first time. The GRI, SASB and TCFD indices can be found on pages 58-67 and our detailed year-over-year performance metrics can be found on pages 51-57.

Limited assurance was performed on Fortinet's greenhouse gas emissions. The assurance statement can be found on pages 68-69 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**

Appendix

Performance data*

Promoting responsible business

Business ethics

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

1. Based on Q4 2022 sales compliance certification.
2. Represents > 90% of total contract manufacturing spend.

Innovating for a safe internet

Innovation

	2022	2021	2020
% of revenue generated from innovation[3]	49.5%	Not reported	Not reported
Number of new product families introductions	5	8	6
R&D investment (USD in millions)	512.4	424.4	341.4
Number of issued and pending global patents (cumulative)	1,540	1,529	910
Number zero-day threats discovered by FortiGuard Labs	109	108	120

3. Represents percentage of newly commercialized hardware models, product families and cloud-based services launched during the previous two years. In 2021, this metric was calculated using a different methodology, and is therefore not comparable with 2022 data. 2021 data could not be restated.

Partnership against cybercrime

	2022	2021
WEF's Cybercrime ATLAS - Number of points mapped and analyzed for disruption opportunities in the cybercriminal ecosystem	32,639	Not applicable
CTA - Number of early discovery shares on threat campaigns	197	195

**Data refers to fiscal year unless otherwise indicated. Fortinet's fiscal year runs from January 1st - December 31st. Data refers to global operations unless stated otherwise in the footnotes.*

Respecting the environment

Product environmental impacts

% of improvement in power efficiency per throughput for top 5 products	2022[4]	% of improvement in power efficiency per throughput for top 5 products	2019-2021[4]
FortiGate-70F	72%	FortiGate-40F	88%
FortiGate-400F	64%	FortiGate-60F	73%
FortiGate-600F	73%	FortiGate-80F	75%
FortiGate-1000F	51%	FortiGate-100F	50%
FortiGate-3000F	68%	FortiGate-200F	20%
Average	**66%**	**Average**	**61%**

[4] *Improvements in maximum power consumption use in top 5 products sold (FortiGate F Series versus FortiGate E Series). For 2022, relates to models released during the year, and, for 2019-2021, relates to models released in the past 2 years.*

	2022	2021	2020
E-waste (in tonnes)	67.1 [5]	30.8	38.8
Recyclable waste (in tonnes)	11.2 [6]	Not reported	

[5] *Data represents e-waste from the largest warehouses and RMA centers (Union City - US, Burnaby - Canada and Sophia Antipolis - France).*
[6] *Data represents recyclable waste from all sites where waste is diverted from landfill which includes the large owned sites and one leased site in London. More sites will be added as the program is expanded.*

Environmental management and climate change impacts

	2022	2021	2020
Scope 1 (mtCO$_2$e)[7]	1,205.6	1,269.4	1,016.1
Scope 2 - Location based (mtCO$_2$e)[7,8]	4,589.6	3,253.9	2,411
GHG emission intensity	1.31E-06	1.35E-06	1.31E-06
Reduction of GHG emissions intensity	6%	3%	28%[9]
Energy consumption (GJ)	142,316	127,878	121,711
Energy intensity	3.22E-05	3.83E-05	4.69E-05
Reduction of energy intensity	16%	18%	16%[8]

[7] *Scope 1 and Scope 2 emissions are calculated for sites under Fortinet's operational control. Data presented here is from owned sites.*
[8] *Increase in Scope 2 emissions from 2021 to 2022 is due to an increase in Fortinet's real estate.*
[9] *Values result from the impact of COVID-19 on operations and the continued growth in our business.*

Scope 3 emissions by category (mtCO$_2$e)

	2022	2021
Purchased goods and services	103,356	Not applicable
Capital goods	7,278	
Fuel- and energy-related activities	4,586	
Transportation and distribution (upstream and downstream)	9,995	
Waste generated in operations	562	
Business travel	5,762	
Employee commuting	4,587	
Leased assets (upstream and downstream)	6,533	
Use of sold products	3,669,454	
End of life treatment of sold products	255	

Growing an inclusive cybersecurity workforce

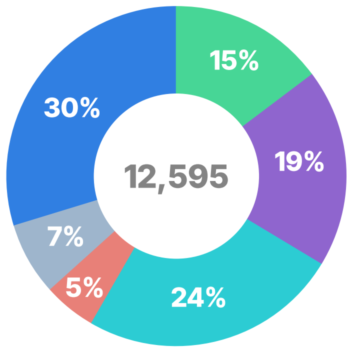
Diversity, equity, and inclusion

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

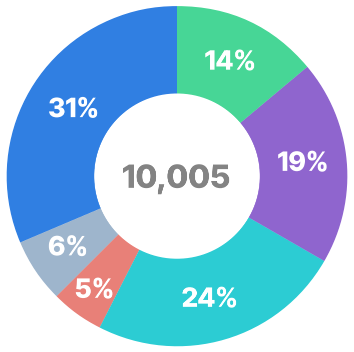
	2022			2021			2020		
	Total	Female	Male	Total	Female	Male	Total	Female	Male
Board of Directors	8	25%	75%	9	33%	67%	8	37%	63%

Total number of permanent employees by region

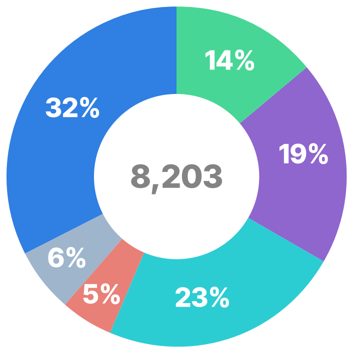
2022



2021



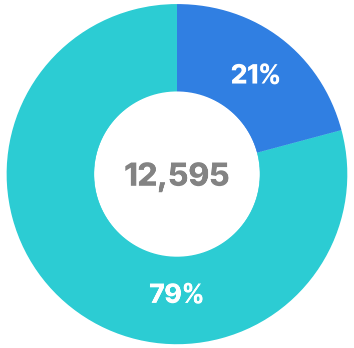
2020



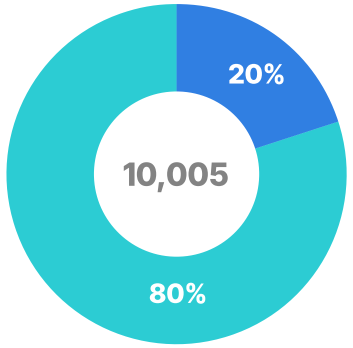
	2022	2021	2020
US	3,756	3,080	2,645
EMEA	3,095	2,417	1,903
CANADA	2,340	1,930	1,565
APAC	1,835	1,401	1,159
LATAM	913	632	490
INDIA	656	545	441

Total number of permanent employees by gender

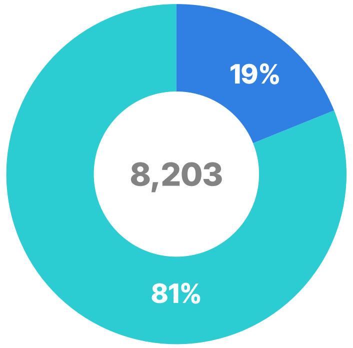
2022



2021

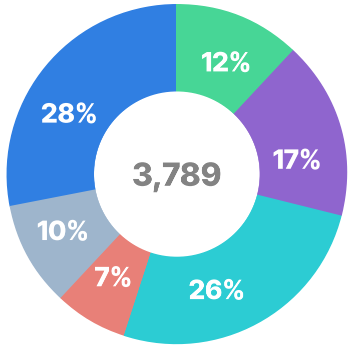


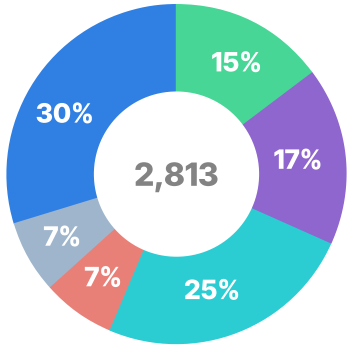
2020

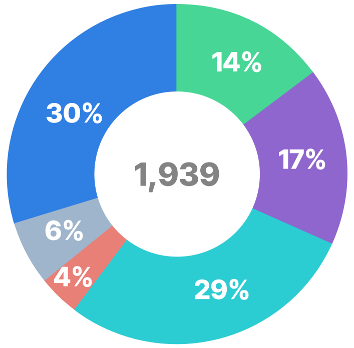


	2022	2021	2020
FEMALE	2,590	1,963	1,518
MALE	10,005	8,042	6,685

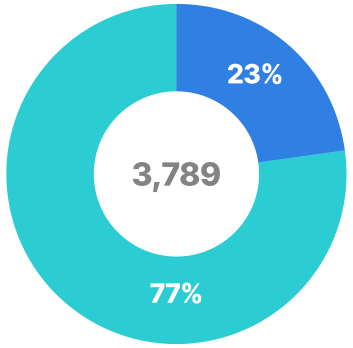
Total number and rate of new employee hires, by gender and region

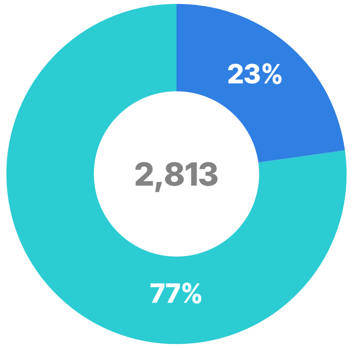


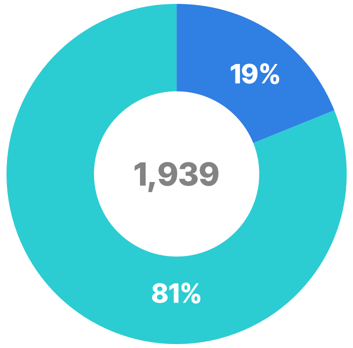




	2022	2021	2020
US	1,067	837	574
EMEA	987	698	562
CANADA	655	471	330
APAC	460	419	279
LATAM	369	195	121
INDIA	251	193	73



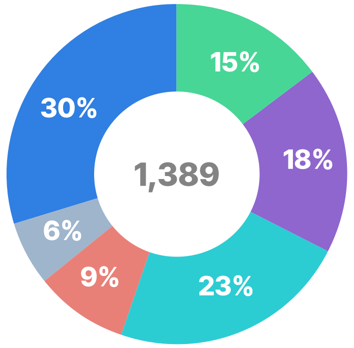




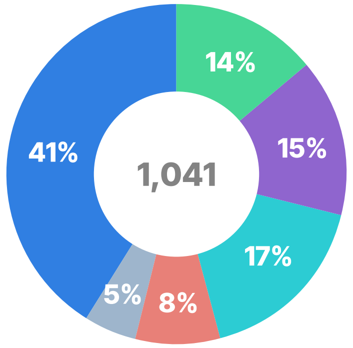
	2022	2021	2020
FEMALE	888	640	373
MALE	2,901	2,173	1,566

Total number and rate of employee turnover, by gender and region

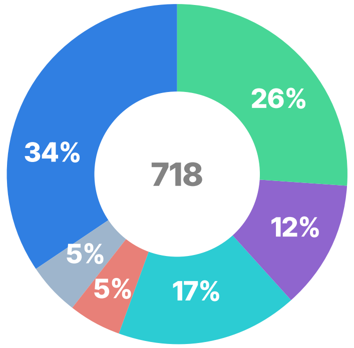
2022



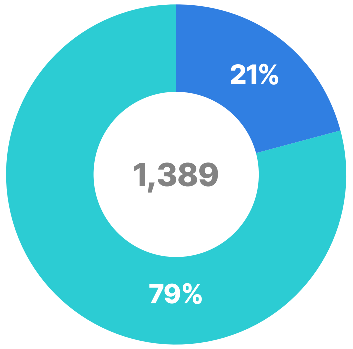
2021

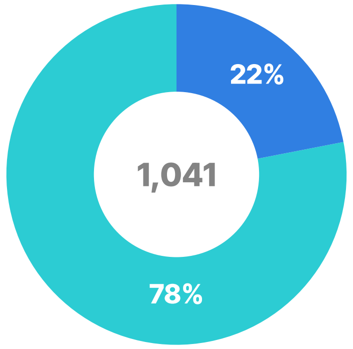


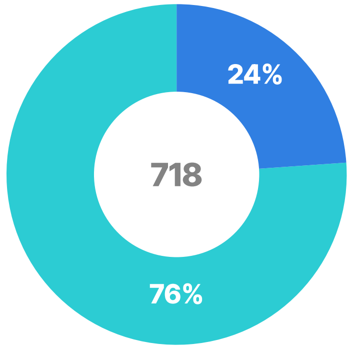
2020



	2022	2021	2020
US	410	429	242
EMEA	312	177	124
CANADA	245	155	89
APAC	213	149	185
INDIA	129	81	39
LATAM	80	50	39

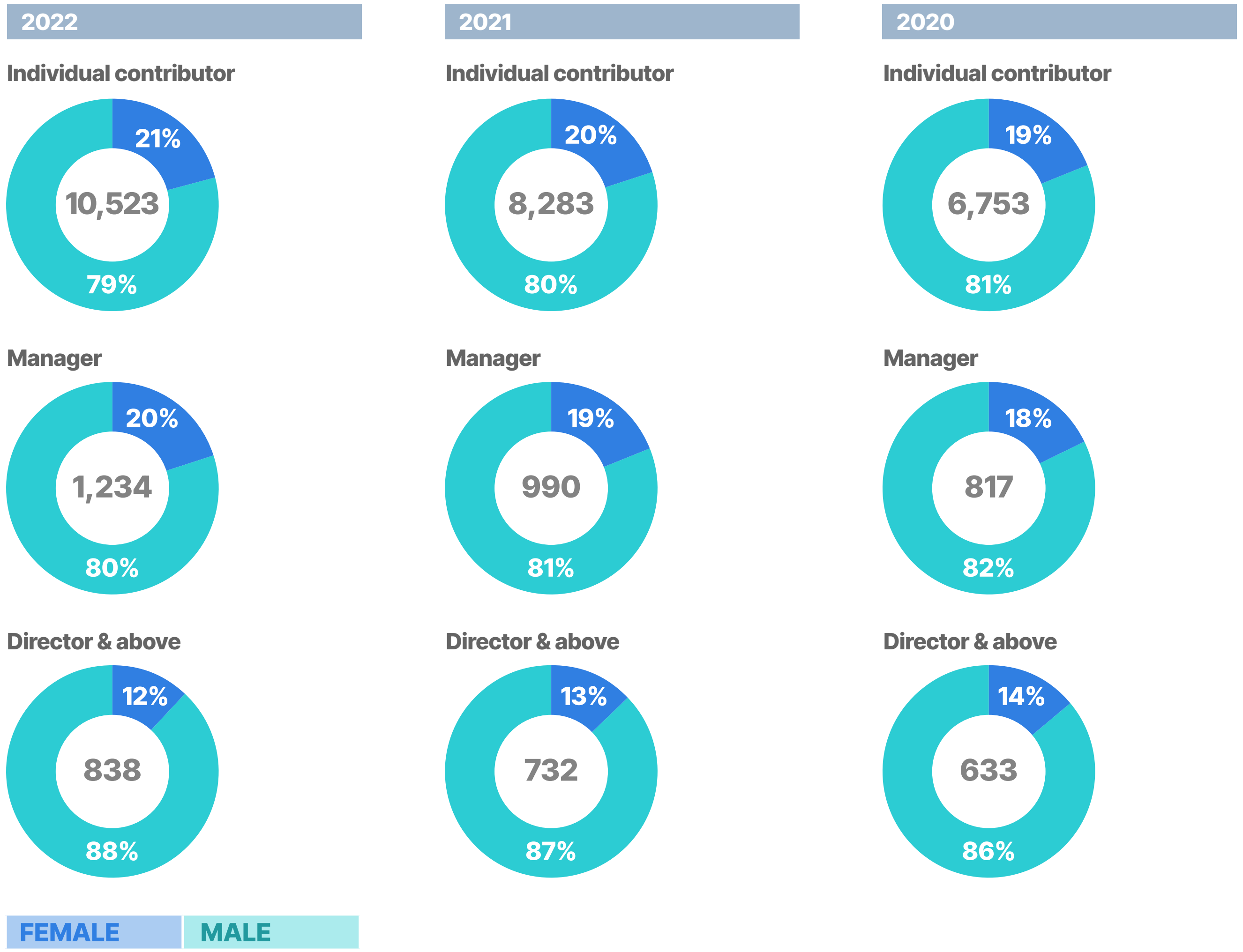






	2022	2021	2020
FEMALE	288	232	170
MALE	1,101	809	548

Percentage of employees per employee category by diversity categories



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

2022				
Gender	Management	Technical staff[10]	Other	Total
Female	17%	12%	33%	22%
Male	83%	88%	67%	78%

2021				
Gender	Management	Technical staff[10]	Other	Total
Female	16%	12%	33%	21%
Male	84%	88%	67%	79%

2020				
Gender	Management	Technical staff[10]	Other	Total
Female	17%	12%	34%	21%
Male	83%	88%	66%	79%

Ethnicity	2022	2021	2020
White	49.9%	47.3%	46.8%
Asian	35.2%	36.7%	37.8%
Latinx	9.5%	9.5%	9.1%
Black	2.9%	2.6%	2.4%
Two or more races	1.7%	1.8%	1.6%
Pacific Islander	0.3%	0.3%	0.3%
Native American	0.2%	0.2%	0.2%
Not disclosed	0.2%	1.5%	1.9%

[10] Technical staff is the EEO-1 Category/Job group of Professional/Technical Professional.

Cybersecurity skills gap

	2022	2021	2020
Total individual people trained[11]	219,465	164,982	183,452
Certifications obtained from the learning platform	315,239	226,258	271,327

[11] 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. The SR Committee, chaired by Fortinet's Co-Founder, President, and CTO, is informed about our plans, projects, and initiatives relative to environmental management, climate change and product environmental impacts on a quarterly basis. *For more information see SR p. 18-19 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 and CSR, 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. *For more information see SR p. 18-19 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	In 2022, we conducted 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 become carbon-neutral (relative to Scope 1 and Scope 2 emissions) by 2030 - in alignment with the SBTi - and is planning to develop a transition plan within the next two years. We are also working to engage our channel distributors, resellers, and contract manufacturers on our climate journey, and are focusing on R&D product innovation to decrease overall power usage of our products with every new generation. **Operations:** Climate-related opportunities across our operations include reducing environmental impacts at our global facilities, and within our supply chain. All our owned facilities in 2021 run on 100% renewable electricity, including our headquarters. 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. **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, through a methodology based on the GHG protocol and ISO 14064. *For more information see SR p. 15 and 33-37*
	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	Fortinet has a specific climate-related risk management process. 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.
	B. Organization's processes for managing climate-related risks	Fortinet began the process of understanding its impact on the climate in 2021 through several steps, including identifying the materiality of its environmental impact and climate change from both operations and technology levels. This analysis offered us a path to comprehensively manage environmental and climate aspects. 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 become carbon neutral 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. *For more information see SR p. 15 and 2022 Form 10-K p.47*
	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 management 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 began its journey to mitigate its impacts on climate change in 2021. We track metrics to assess climate-related risks and opportunities including total GHG emissions, energy consumption, purchased and on-site renewable electricity, and green building certifications. In 2022, we started to track water usage and waste in our sites. *For more information see SR p. 37*
	B. Disclosure of Scope 1, Scope 2, and Scope 3 greenhouse gas (GHG) emissions	In 2021, Fortinet reported for the first time on our Scope 1 and Scope 2 emissions, and we publicly committed to becoming carbon neutral by 2030, in alignment with the Science-Based Target Initiative (SBTi). In 2022, we began and completed the inventory of our Scope 3 emissions. We track and disclose our Scopes 1, 2, 3 GHG emissions, as well as GHG emission intensity metrics on an annual basis. Emissions are calculated in alignment with the Greenhouse Gas Protocol and the ISO14064-1 Standard. To progress towards our goal of carbon neutrality, 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 performance data see p. 52*
	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. We also formally committed to the Science Based Targets Initiative (SBTi) to set goals aligned with limiting global warming to 1.5°C in 2022. *For more information see SR p. 36*

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, 2022- December 31, 2022
GRI 1 used	GRI 1: Foundation 2021
Applicable GRI Sector Standard(s)	None developed yet

GRI Standard	Description	Reference/Disclosure	Alignment to the SDGs*
General disclosures			
GRI 2: General disclosures 2021	2-1 Organizational details	2022 Sustainability Report / Who we are p. 2-3 2022 Form 10-K p. 3-11	
	2-2 Entities included in the organization's sustainability reporting	2022 Sustainability Report / About this report p. 49	
	2-3 Reporting period, frequency and contact point	2022 Sustainability Report / About this report p. 49	
	2-4 Restatement of information	There are no restatements.	
	2-5 External Assurance	2022 Sustainability Report / Limited assurance statement p. 68-69	
	2-6 Activities, value chain and other business relationships	2022 Sustainability Report / Who we are p. 2-3	
	2-7 Employees	2022 Sustainability Report / Diversity, equity and inclusion p. 38-43 2022 Sustainability Report / Performance data p. 51-57	*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	
	2-10 Nomination and selection of the highest governance body	Social Responsibility Committee Charter Governance Committee Charter 2022 Proxy Statement p. 33	
	2-11 Chair of the highest governance body	Ken Xie, CEO and Chairman 2022 Proxy Statement p. 30-31	
	2-12 Role of the highest governance body in overseeing the management of impacts	Social Responsibility Committee Charter Governance Committee Charter 2022 Proxy Statement p. 32	

GRI Standard	Description	Reference/Disclosure	Alignment to the SDGs*
General disclosures			
GRI 2: General disclosures 2021	2-13 Delegation of responsibility for managing impacts	Social Responsibility Committee Charter CSR Committee Charter 2022 Sustainability Report / Governance p. 18-19	
	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	16
	2-16 Communication of critical concerns	2022 Proxy Statement p. 34	16
	2-17 Collective knowledge of highest governance body	2022 Sustainability Report / Governance p. 18-19	
	2-18 Evaluation of the performance of the highest governance body	2022 Proxy Statement p. 16	
	2-19 Remuneration policies	2022 Proxy Statement p. 37-42	
	2-20 Process to determine remuneration	2022 Proxy Statement p. 36-37 Human Resources Committee Charter	
	2-22 Statement on sustainable development	2022 Sustainability Report / Letter from our CEO p. 4-5	
	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 2022 Sustainability Report / Business ethics p. 20 2022 Sustainability Report / Integrating human rights into our operations p. 20 2022 Sustainability Report / Responsible product use p. 21 2022 Sustainability Report / Performance data p. 51-57	
	2-26 Mechanisms for seeking advice and raising concerns	2022 Sustainability Report / Business ethics p. 21 Whistleblower Policy	16
	2-28 Membership associations	2022 Sustainability Report / Cybersecurity risks to society p. 27	16
	2-29 Approach to stakeholder engagement	2022 Sustainability Report / Stakeholder engagement p. 12-13	

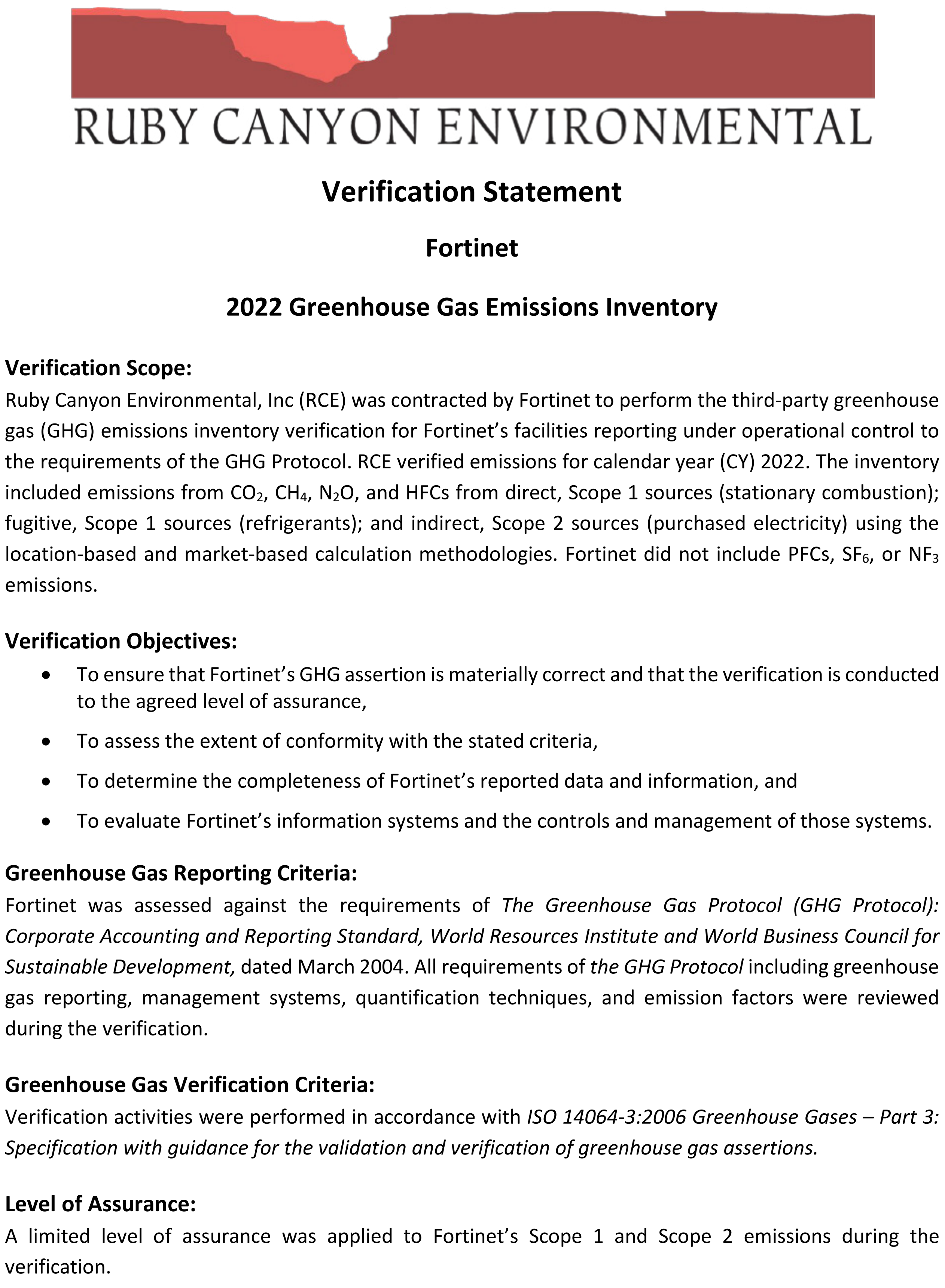
GRI Standard	Description	Reference/Disclosure	Alignment to the SDGs*
Material topics			
GRI 3: Material topics 2021	3-1 Process to determine material topics	2022 Sustainability Report / Journey toward a sustainable business p. 10-11	
	3-2 List of material topics	2022 Sustainability Report / Journey toward a sustainable business p. 11	
	3-3 Management of material topics	2022 Sustainability Report / Cybersecurity risks to society p. 22-28 2022 Sustainability Report / Information security and privacy p. 29-31 2022 Sustainability Report / Product environmental impacts p. 32-35 2022 Sustainability Report / Environmental management and climate change impacts p. 36-37 2022 Sustainability Report / Cybersecurity skills gap p. 44-47 2022 Sustainability Report / Diversity, equity and inclusion p. 38-41 2022 Sustainability Report / Promoting responsible business p. 20-21	7.2, 7.3, 7.a, 13.1, 13.2 16
Indirect economic impact			
GRI 203: Indirect economic impacts 2016	203-2 Significant indirect economic impacts	2022 Sustainability Report / Cybersecurity risks to society p. 22-28	16
Anti-corruption			
GRI 205: Anti-corruption 2016	205-2 Communication and training about anti-corruption policies and procedures	Anti-corruption Policy 2022 Sustainability Report / Promoting responsible business p. 20-21 2022 Sustainability Report / Performance data p. 51	16
Energy			
GRI 302: Energy 2016	302-1 Energy consumption within the organization	2022 Sustainability Report / Performance data p. 52	7.2, 7.3, 7.a, 13.1, 13.2
	302-3 Energy intensity	2022 Sustainability Report / Performance data p. 52	13.1, 13.2
	302-4 Reduction of energy consumption	2022 Sustainability Report / Performance data p. 52	13.1, 13.2
	302-5 Reductions in energy requirements of products and services	2022 Sustainability Report / Product environmental impacts p.34 2022 Sustainability Report / Performance data p. 52	7.2, 7.3, 7.a, 13.1, 13.2
Emissions			
GRI 305: Emissions 2016	305-1 Direct (Scope 1) GHG emissions	2022 Sustainability Report / Performance data p. 52-53	13.1, 13.2
	305-2 Energy indirect (Scope 2) GHG emissions		
	305-3 Other indirect (Scope 3) GHG emissions		
	305-4 GHG emissions intensity		
	305-5 Reduction of GHG emissions		
Waste			
GRI 306: Waste 2020	306-2 Management of significant waste-related impacts	2022 Sustainability Report / Performance data p. 52 2022 Sustainability Report / Product environmental impacts p. 35	12
Employment			
GRI 401: Employment 2016	GRI 401-1 New employee hires and employee turnover	2022 Sustainability Report / Performance data p. 54-55	5.1, 5.5, 8.5, 10.2, 10.3, 10.4
Training and education			
GRI 404: Training and education 2016	404-1 Average hours of training per year per employee	14 hours per employee. Data only encompasses cybersecurity training.	4.3, 4.4, 4.5
	404-2 Programs for upgrading employee skills and transition assistance programs	2022 Sustainability Report / Cybersecurity skills gap p. 53	
Diversity and equal opportunity			
GRI 405: Diversity and equal opportunity 2016	405-1 Diversity of governance bodies and employees	2022 Sustainability Report / Performance data p. 53 2022 Proxy Statement p. 15-16	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	2022 Sustainability Report / Performance data p. 51	16

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**	2022 Sustainability Report / Performance data p. 52
	Discussion of the integration of environmental considerations into strategic planning for data center needs	**TC-SI-130a.3**	2022 Sustainability Report / Product environmental impacts p. 33-35 2022 Sustainability Report / Environmental management and climate change p. 36-37 2022 Sustainability Report / Performance data p. 52-53
Data privacy & freedom of expression	Description of policies and practices relating to behavioral advertising and user privacy	**TC-SI-220a.1**	Privacy Policy
Data security	Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards	**TC-SI-230a.2**	2022 Sustainability Report / Information security and privacy p. 29 SOC2 certification ISO 27001 certification TISAX certification HIPAA 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**	2022 Sustainability Report / Performance data p. 57
Managing systemic risks from technology disruptions	Description of business continuity risks related to disruptions of operations	**TC-SI-550a.2**	2022 Sustainability Report / Cybersecurity risks to society p. 26-28



RUBY CANYON ENVIRONMENTAL

Verification Statement

Fortinet

2022 Greenhouse Gas Emissions Inventory

Verification Scope:
Ruby Canyon Environmental, Inc (RCE) was contracted by Fortinet to perform the third-party greenhouse gas (GHG) emissions inventory verification for Fortinet's facilities reporting under operational control to the requirements of the GHG Protocol. RCE verified emissions for calendar year (CY) 2022. The inventory included emissions from CO_2, CH_4, N_2O, and HFCs from direct, Scope 1 sources (stationary combustion); fugitive, Scope 1 sources (refrigerants); and indirect, Scope 2 sources (purchased electricity) using the location-based and market-based calculation methodologies. Fortinet did not include PFCs, SF_6, or NF_3 emissions.

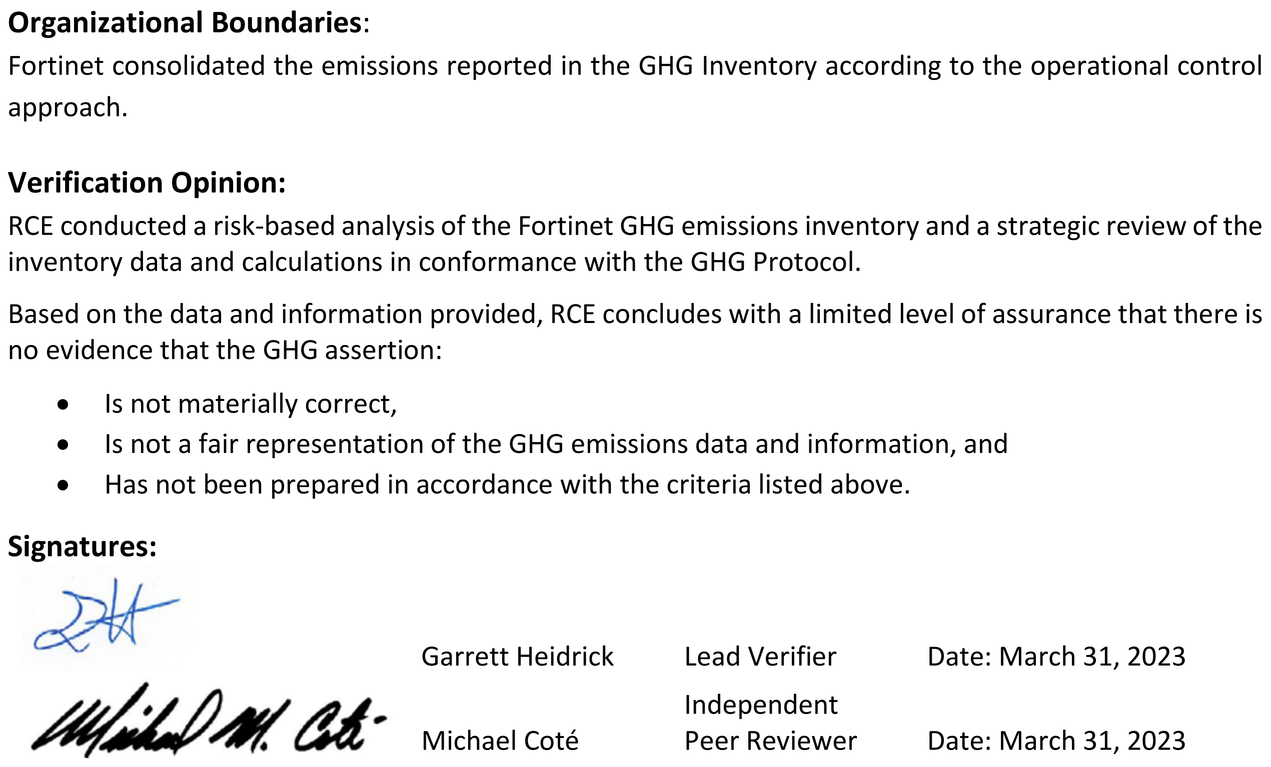
Verification Objectives:

- To ensure that Fortinet's GHG assertion is materially correct and that the verification is conducted to the agreed level of assurance,
- To assess the extent of conformity with the stated criteria,
- To determine the completeness of Fortinet's reported data and information, and
- To evaluate Fortinet's information systems and the controls and management of those systems.

Greenhouse Gas Reporting Criteria:
Fortinet was assessed against the requirements of *The Greenhouse Gas Protocol (GHG Protocol): Corporate Accounting and Reporting Standard, World Resources Institute and World Business Council for Sustainable Development,* dated March 2004. All requirements of *the GHG Protocol* including greenhouse gas reporting, management systems, quantification techniques, and emission factors were reviewed during the verification.

Greenhouse Gas Verification Criteria:
Verification activities were performed in accordance with *ISO 14064-3:2006 Greenhouse Gases – Part 3: Specification with guidance for the validation and verification of greenhouse gas assertions.*

Level of Assurance:
A limited level of assurance was applied to Fortinet's Scope 1 and Scope 2 emissions during the verification.



Organizational Boundaries:
Fortinet consolidated the emissions reported in the GHG Inventory according to the operational control approach.

Verification Opinion:
RCE conducted a risk-based analysis of the Fortinet GHG emissions inventory and a strategic review of the inventory data and calculations in conformance with the GHG Protocol.

Based on the data and information provided, RCE concludes with a limited level of assurance that there is no evidence that the GHG assertion:

- Is not materially correct,
- Is not a fair representation of the GHG emissions data and information, and
- Has not been prepared in accordance with the criteria listed above.

Signatures:

	Garrett Heidrick	Lead Verifier	Date: March 31, 2023
Michael M. Coté	Michael Coté	Independent Peer Reviewer	Date: March 31, 2023

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®

www.fortinet.com

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

Photo credits: Getty Images – Graphic design: osidièse.