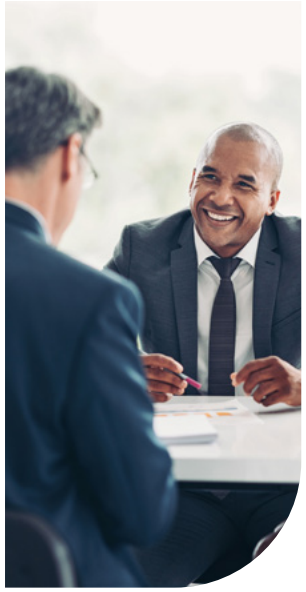


# Sustainability report 2021

FORTINET®

# About Fortinet

## Our vision is security-driven networking for a hyperconnected world

Fortinet, an American multinational corporation headquartered in Sunnyvale, California, empowers its customers with intelligent, seamless protection across their expanding attack surface combined with the power to take on the ever-increasing performance requirements of the borderless network—today and into the future. The Fortinet Security Fabric architecture delivers integrated, broad, automated security to address today's most critical security challenges, whether in network, application, cloud, or mobile environments. Fortinet has been awarded over 1,260 patents and owns the world's most extensive portfolio of network security technologies. Fortinet ranks number one in the most security appliances shipped worldwide, with more than 580,000 customers who trust Fortinet to protect their businesses.


Number of locations **90+**

Appearance in Gartner Magic Quadrants **8**

Market capitalization [As of Dec 31, 2021] **$58.2B**

| Year founded | Headquarters | Stock symbol | Customers | Units shipped to date | Global patents | Number of employees[1] | FY 2021 financial highlights |
|---|---|---|---|---|---|---|---|
| 2000 | Sunnyvale, California | FTNT<br>IPO: November 2009 | 580,000+ | 8.4M+ | 1,269 issued<br>260 pending | (As of December 31, 2021)<br>10,000+ | $3.34B in revenue<br>$4.18B in billings<br>$2.99B cash and investment[2] |

*1 - Excluding Alaxala and Linksys employees.*
*2 - Including cash, cash equivalents, short term and long term investments and marketable equity securities.*


# Table of contents

**Fortinet began its journey in 2000 with the belief that cybersecurity is a force for good and a commitment to making the internet a safe place for everyone. Today, we are even more driven to translate that vision into reality. Cybersecurity is no longer confined to the technology realm. It is now a broader sustainability issue due to the digitization of society, our growing digital economy, and the importance of digital information to geopolitics. It has also become essential to organizations and individuals—from a data and privacy standpoint—to maintain the sustainability of our society, now and in the future.**

The COVID-19 pandemic led to the rapid expansion of remote work, a trend that is expected to continue long after the pandemic ends. Today's hybrid workforce has increased global demand for our solutions—partly because we are faced with an escalating cybercrime landscape that includes advanced persistent threats and state-sponsored attacks. As a cybersecurity engineering company founded and led by engineers, we understand that because the threat landscape evolves rapidly, the industry must innovate at an even greater pace. That is why at Fortinet, innovation lies at the heart of everything we do.

Our commitment to that effort is reflected in our portfolio of patents and solutions, the largest in the industry, and FortiGuard Labs, our threat intelligence platform and research organization. But making the digital world safe for all must also include collaboration, which is why we are a founding member of the Cyber Threat Alliance (CTA) and the World Economic Forum (WEF) Center for Cybersecurity. Additionally, we work with public, private, and industry partners worldwide, including Europol, NATO, and INTERPOL, to share intelligence, stop threats, and combat cybercrime.

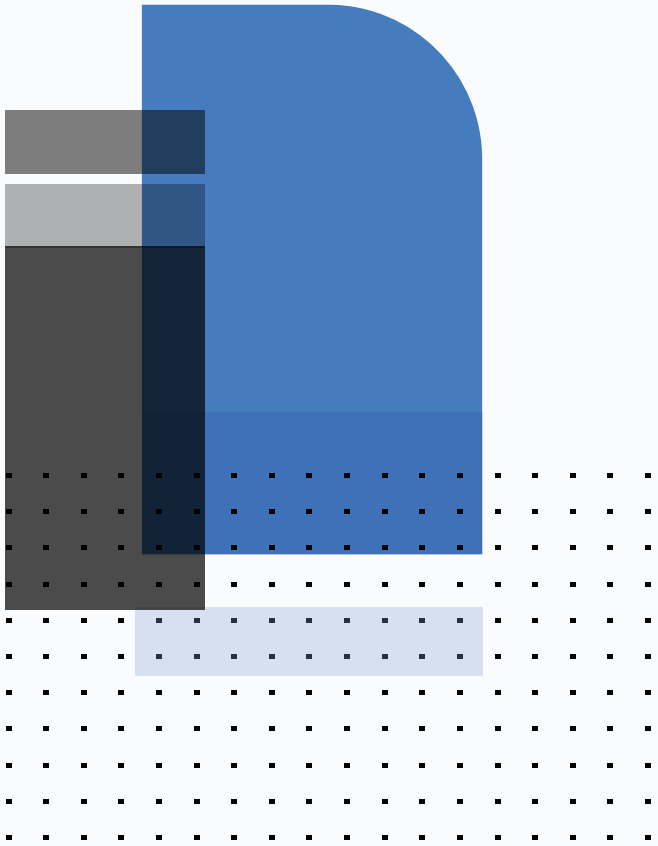
However, a significant worldwide shortage of skilled cybersecurity professionals has complicated the mission of protecting society from cyber risks. Many organizations are struggling to fill critical roles needed to help combat the increasing threat of cyberattacks. To this end, Fortinet has dedicated years to close the cybersecurity skills gap through our Fortinet Training Institute and partnerships with organizations such as WEF, Salesforce and IBM.

We are furthering our commitment to significantly reducing the cybersecurity skills gap with a pledge to train one million people by 2026. Reducing this shortage also requires us to consider ways to create a more diverse workforce and remove additional barriers to access for traditionally under-represented groups globally. We will then have access to cybersecurity professionals who come with diverse perspectives on doing business and problem-solving, and Fortinet will be stronger for it.

Integrating sustainability into our business model means conducting business responsibly, which is why we are focused on good governance and ethical practices. This includes a commitment to further reducing the environmental footprint of our solutions and adopting responsible approaches in our daily operations. In 2021, we announced our pledge to become carbon neutral by 2030. I am particularly proud of our newly completed corporate headquarters building, which is LEED-Gold Certified. Beyond our operations, we are focused on reducing the environmental footprint of our customers by innovating highly efficient, integrated appliances and cloud-based security solutions. Since the company began, it's always been a priority for me to deliver the highest level of computing power while reducing energy consumption and optimizing system deployment.

This inaugural Sustainability Report documents Fortinet's sustainability journey, the public goals we have set, progress toward our commitments, and our achievements. I am committed to ensuring that Fortinet fulfills its corporate social responsibility vision, but we cannot achieve our vision alone. It is only with the support of our employees, partners, customers, and suppliers that Fortinet can foster just and sustainable societies through a trustworthy digital world.

**Ken Xie**
*Fortinet Founder & CEO,*
*Chairman of the Board*



# About this report

Fortinet's 2021 Sustainability Report, our first, presents a balanced account of our sustainability performance across our priority material issues and allows our stakeholders – including customers, partners, employees, suppliers, shareholders, and communities - to better understand our corporate social responsibility approach and mission.

This report also outlines our approach to integrating sustainability into Fortinet and covers our performance throughout our operations and activities worldwide for the fiscal year 2021 (January 1, 2021 – December 31, 2021).

The report references the Global Reporting Initiative (GRI) Standards, Sustainability Accountability Standards Board (SASB) Standards and the United Nations Sustainable Development Goals (UN SDGs).

Limited assurance was performed on Fortinet's greenhouse gas emissions. The assurance statement can be found on page 48 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**

# Sustainability approach



## Sustainability data and policies

- CSR Committee Charter
- CSR website
- Social Responsibility Committee of the Board of Directors Charter

# Materiality and stakeholder engagement

A materiality assessment enables Fortinet to prioritize environmental, social and governance (ESG) issues most significant to its business and main stakeholders to achieve long-term sustainability performance.

In 2021, we engaged BSR, an external corporate sustainability consultancy, to conduct our first material assessment to ensure an unbiased appraisal using a methodology that can be assured to meet the requirements of ESG reporting standards and stakeholder expectations. The materiality assessment has helped us understand what matters most in the long term as a responsible and sustainable business and established a direction for prioritization and strategy development.

BSR conducted the assessment in four stages:

1

**IDENTIFIED**
potential material ESG issues in line with relevant reporting frameworks and standards (GRI, SASB, TCFD), initiatives (e.g., RBA, WEF metrics for Stakeholder Capitalism), and experience with materiality assessment in the technology sector.

2

**UNDERSTOOD**
internal and external stakeholder perspectives through interviews with a selected number of Fortinet employees and external stakeholders including customers, partners, suppliers, and investors. Polecat, an artificial intelligence tool, provided an independent assessment of which issues held the greatest interest to stakeholders across the technology sector.

3

**SCORED**
each potential material issue across criteria relevant to the business and stakeholders using insights gained through the stakeholder engagement step. The score indicated the issue's relative importance to business success and stakeholders.

4

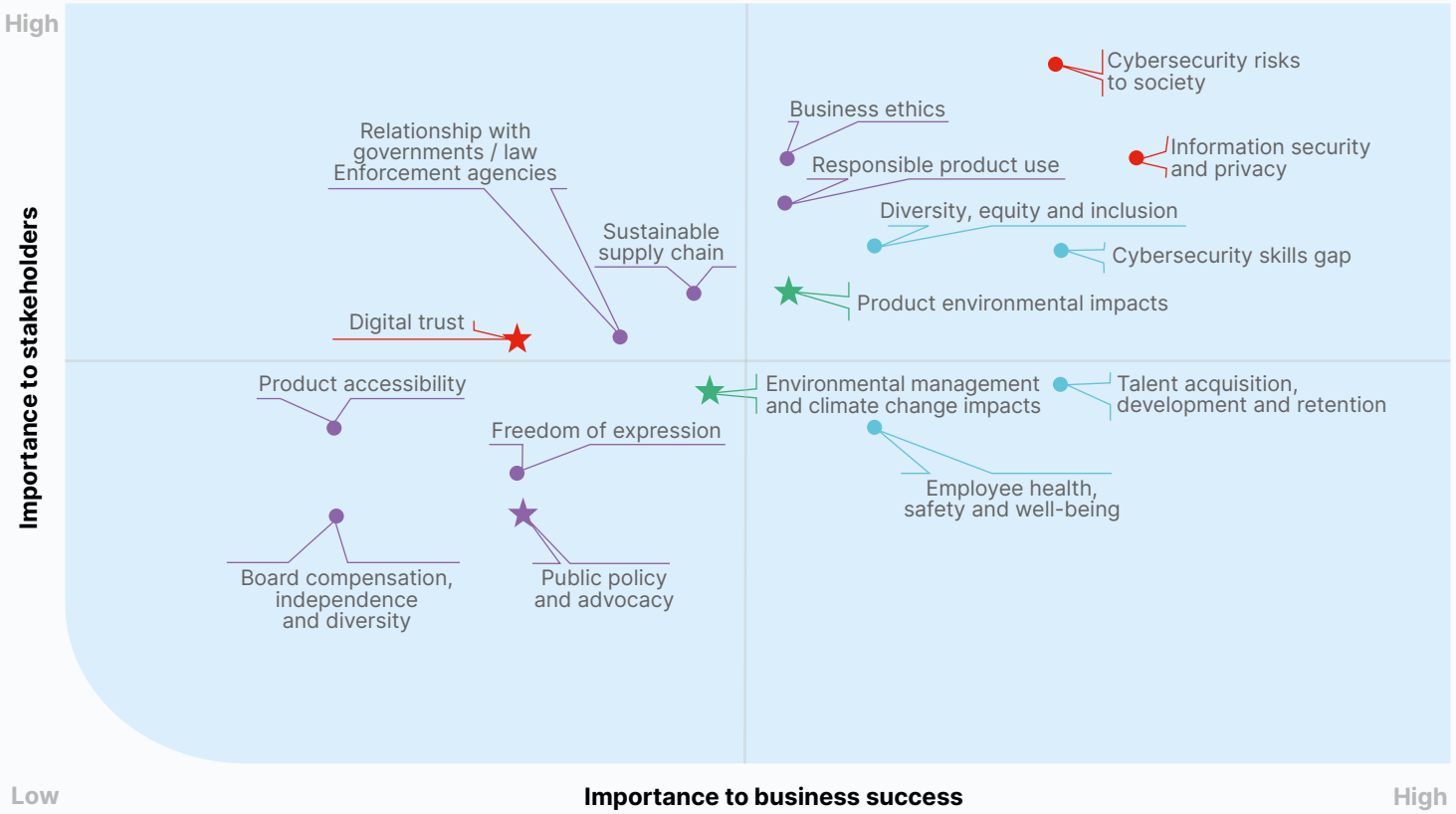
**PRIORITIZED**
the issues on the materiality map based on their relative importance to the business and stakeholders. The results were validated by Fortinet's internal Corporate Social Responsibility (CSR) Committee and the Social Responsibility Committee of the Board of Directors.[3]

The sustainability reporting landscape is evolving rapidly, and Fortinet will monitor developments, including those related to sustainability framework standardization and materiality assessments, and adapt its practices accordingly.



*3 - More information on the CSR Committee and the Social Responsibility Committee can be found on p.10.*

## Materiality matrix



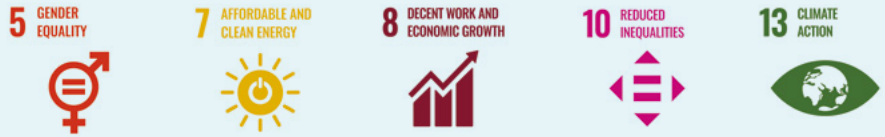

Note: Stars indicate fast moving issues that will likely increase in importance in the next 3-5 years.

- Innovating for a safe internet
- Respecting the environment
- Growing an inclusive cybersecurity workforce
- Promoting responsible business

# Strategic framework

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 that vision by innovating sustainable security technologies, diversifying cybersecurity talent, and promoting responsible business across our value chain.

Our objective is to promote long-term value for our stakeholders, including customers, partners, suppliers, employees, shareholders, and communities. Our strategic framework for sustainability – informed by the materiality assessment conducted in 2021 – is defined as follows:

| | | |
|---|---|---|
| **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**<br>• Cybersecurity risks to society<br>• 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**<br>• Product environmental impacts<br>• 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**<br>• Diversity, equity and inclusion<br>• Cybersecurity skills gap |
| **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**<br>• Business ethics<br>• Responsible product use |
| **United Nations Sustainable Development Goals (SDGs)** |  | |

We are on a sustainability journey. For Fortinet, 2021 was the year for assessing our sustainability status and strategically planning our journey for the medium- to long-term. We established ambition levels for each of our priority issues and developed initial roadmaps, engaging Fortinet's relevant business units in the process. We also improved transparency and disclosure by actively participating in sustainability assessments from selected rating agencies and bolstering our public CSR disclosures, including our public website. We are currently working on a broader set of goals aligned with our material issues to be published in the coming years.

We are publishing our first sustainability report this year and our reporting is guided by the GRI and SASB standards. Our sustainability strategy is also guided by five UN SDGs – 5, 7, 8, 10 and 13 – where we believe Fortinet can help make progress. In the coming years, we will continue to work towards embedding these goals into our strategy. The ESG reporting landscape is evolving at a rapid pace, with the U.S. Securities and Exchange Commission proposing mandatory climate disclosures and the recent formation of the International Sustainability Standards Board (ISSB), which was created with the express purpose of developing a global set of sustainability disclosure standards. Fortinet will continue to monitor the landscape and adapt to meet stakeholder expectations and regulatory requirements. As a next step, in 2022, we will work on aligning our climate strategy to the TCFD framework and submit our first CDP report.

# Governance

Our approach to corporate social responsibility is based on a strong corporate governance structure which starts with our Board of Directors. The Board of Directors is committed to meeting Fortinet's social responsibilities while promoting long-term value for our stakeholders.

Fortinet's Board of Directors formed the Social Responsibility Committee to bring the highest level of governance to corporate social responsibility issues. The Committee, comprised of at least two Board members, 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. As appropriate, the Committee collaborates with other Board committees on legal corporate governance matters and diversity, equity and inclusion (DEI) issues. The Board of Directors has reviewed and approved this 2021 Sustainability Report.

Fortinet's internal CSR Committee was created to assist the Social Responsibility Committee of the Board in overseeing Fortinet's corporate social responsibility, including ESG matters. The Committee comprises cross-functional management representatives from across Fortinet and is responsible for defining CSR priorities, objectives, and strategies and for overseeing and coordinating CSR initiatives. The Committee is chaired by Fortinet's Global Head of Sustainability & CSR and reports to the Social Responsibility Committee at least two times a year.

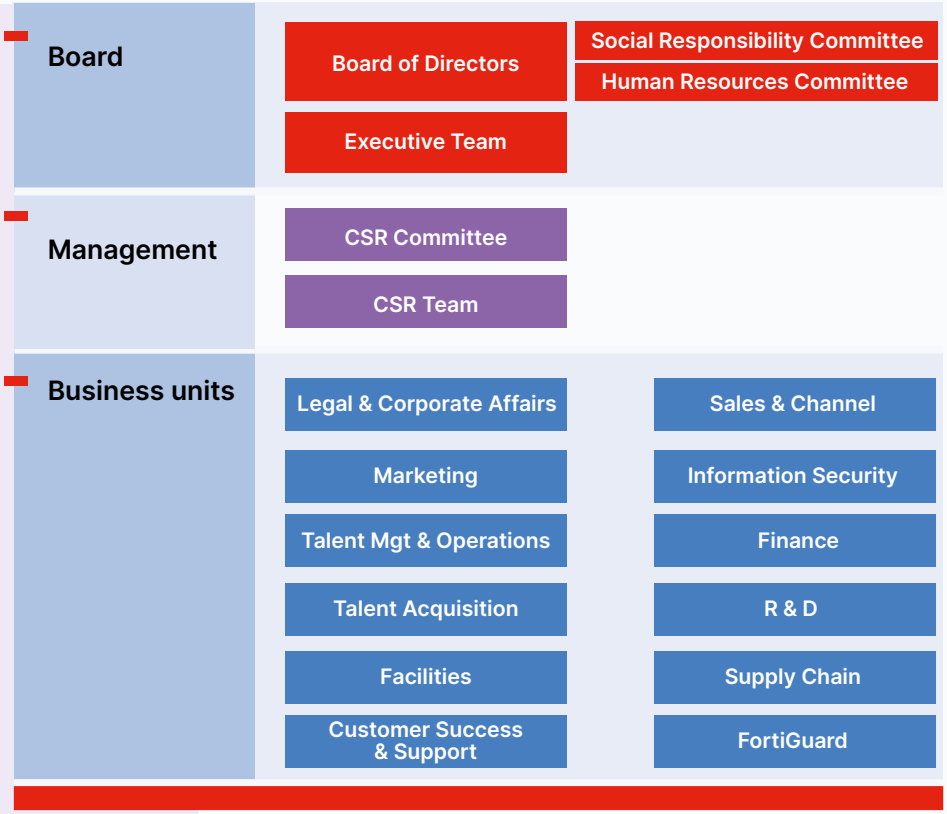
Fortinet's executive leadership sponsors corporate social responsibility integration throughout its business operations. The Global Head of Sustainability & CSR, together with her team and the internal CSR Committee, leads strategy development, and champions CSR execution and disclosures internally and externally, engaging with stakeholders. Each business unit within Fortinet has its own CSR Champions and CSR Ambassadors. CSR champions are accountable for CSR action plans and operational goals within their business units. CSR Ambassadors are volunteers who help engage Fortinet's workforce more broadly on CSR issues.

In 2021, to educate employees on sustainability, BSR conducted several trainings, including on DEI and climate change, for executives and managers. The consultancy partnered with Fortinet to create roadmaps for its material issues, define specific internal and external goals, targets, and develop action plans to achieve them.

*"At Fortinet, we understand the importance of making sustainability integral to our business model and believe in the power of collaboration and engagement to drive social responsibility and progress. We are working cross-functionally, across our value chain and with the broader industry to address the key expectations of our stakeholders. Throughout our journey, we are committed to acting transparently and leading with ambition towards a more sustainable world and safer internet."*

**Barbara Maigret,** Global Head of Sustainability & CSR, Fortinet.

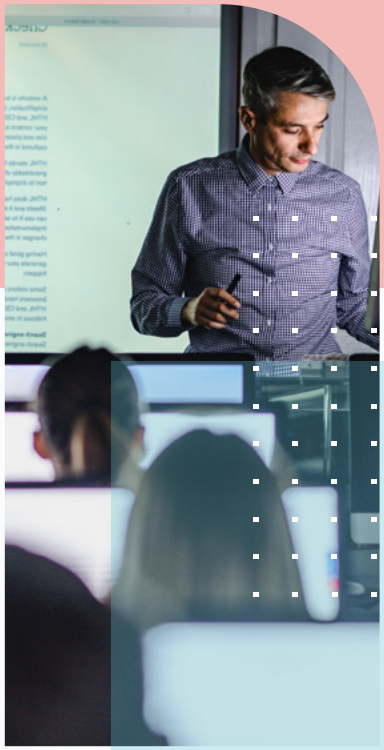
**Fortinet CSR governance structure**



# Goals

**1 million**

people trained in cybersecurity by 2026



**NET 0**

Become carbon neutral by 2030[4]



*4 - Target relative to Scope 1 and Scope 2 emissions resulting from our owned facilities worldwide, in alignment with the Science Based Target Initiative (SBTi).*

# Innovating for a safe internet

**Ensuring the digital security and data privacy of individuals and organizations enables digital progress. We strive to create value through security innovation, expertise, research, and cooperation.**

## Our approach

As our digital world advances, public, private sector, and personal environments are increasingly dependent on digital data and applications. Today, vital and critical infrastructure and services, including energy, transportation, healthcare and public service are often digitized and connected to the internet. As a result, the disruption of operations or services and the loss or compromise of data due to cyberattacks places every individual, organization, and even nation – at risk.

Given this context, cybersecurity is not just a technology concern but has become a broader sustainability issue. Fortinet is engaged in innovating for a safe internet for all, responsibly, and committed to driving progress and sustainability through cybersecurity. Ensuring the digital security and data privacy of individuals and organizations enables digital progress. Fortinet has a vital role to play here – through innovative cybersecurity technologies, strong customer adoption, expertise, research, and cooperation – in enabling digital progress and creating a trustworthy and safe digital world.

**Cybersecurity risks to society** ..... 13

**Information security & privacy** ..... 18

**Sustainability data and policies**

Cybersecurity innovation data ..... 36

Privacy Policy

Security Vulnerability Policy

# Cybersecurity risks to society

**Fortinet is committed to advancing cybersecurity to create a safer internet through innovation, community engagement, and partnerships. We aim to create digital trust for all and help communities avoid the potentially negative social impact of the misuse of digital technology, especially in terms of privacy and information security. We are also proactively working to effectively fight cybercriminals by partnering with vendors, governments, public and private sector entities to combine our threat intelligence research and capabilities. Innovative cybersecurity provides Fortinet with a transformative opportunity to be an industry leader, elevate the global cybersecurity ecosystem, disrupt the adversarial model of cybercrime, and make the internet safer.**

## Innovation at heart

The world of cybercrime is highly sophisticated and evolves rapidly, leveraging the latest techniques and technologies to target victims and thwart security measures. In this context, it is paramount for the industry to be at the forefront of innovation.

At Fortinet, innovation lies at the heart of everything we do and is rooted in over 20 years of prioritizing research and development in our company's culture which has resulted in the industry's broadest portfolio of cybersecurity solutions with over 50 security-related products. Most of our technology has been built from the ground up and is fully integrated into the Fortinet Security Fabric – a broad, integrated, and automated cybersecurity mesh platform that spans the extended digital attack cycle and enables self-healing security and networking to protect devices, data, and applications.

The core of our innovation lays with our FortiOS, Fortinet's unique operating system, which spans much of our product line and includes many innovative features. And our purpose-built ASIC processors, the first in the industry, deliver unrivaled performance and efficiency. We also foster innovation through our Fortinet Open Fabric Ecosystem, allowing the integration of more than 280 third-party fabric-ready partners with over 500 technology integrations into our operating system.

Beyond technology, we deliver innovation through breakthrough threat intelligence and services. We have experienced threat hunters, researchers, analysts, engineers, and data scientists operating in FortiGuard Labs around the globe. This team provides our customers with the industry's best-applied threat research, intelligence information and analytics to protect them from the latest cyberattacks. We are particularly proactive in detecting and protecting against zero-day threats.[5] Fortinet is also committed to a responsible disclosure process that allows impacted companies to fix identified issues while also increasing consumer protection by blocking threats against unpatched security vulnerabilities. We began working with a single vendor for our zero-day program back in 2006, and since then have reported to over 135 companies. Our progress showcases our innovative approach and our commitment to building healthy relationships with a wide range of companies.

*5 - A 'zero-day' threat is a newly discovered software vulnerability or security flaw. Because it is new, it is a window of opportunity for hackers.*

## Highlights in 2021

Fortinet delivered significant innovative solutions, including launching the industry's first integrated Zero Trust Network Access to support the increased number of customer employees working from home due to COVID-19. To help close the cybersecurity skills gap, Fortinet also launched multiple managed services, including Security Operations Center (SOC) as-a-Service, Managed Detection and Response, and Incident Response services.

To keep up with the volume, sophistication, and speed of today's cyber threats and to offer a modern approach to security, Fortinet has further leveraged the latest technologies, such as Artificial Intelligence (AI), Machine Learning (ML) and Deep Learning technologies in the design and development of its cybersecurity solutions and services. These technologies have led to the development of products and services that analyze millions of malware samples per day with near-perfect accuracy and improve real-time threat hunting and intelligent threat detection.

Following the industry's pervasive SolarWinds vulnerability, Fortinet delivered The FortiGuard Outbreak Alerts system. This system allows customers to quickly hunt for cyber threats when an incident, affecting numerous organizations and with significant ramifications to the cybersecurity industry occurs. This system has been critically important over the past year, given the issues with major global security impacts, such as Log4J, Microsoft Exchange, and Spring4Shell.

**998**

**zero-day threats discovered by FortiGuard Labs**

**1,269**

**global patents issued and 260 pending**

**500+**

**technology integrations**

## Driving innovation

Digital innovation and acceleration are now core priorities for all industries and sectors worldwide, and it is our mission to safely enable such innovation.

One of our areas of focus is supporting innovation in Operational Technology (OT).[6] We do this by protecting critical infrastructures such as energy utility plants, healthcare and manufacturing from cyber threats and attacks to keep systems and services safe and operational. To that end, Fortinet has formed a strategic partnership with Schneider Electric to provide cybersecurity solutions to address the unique needs of OT networks. Together, we are working to harden security on OT equipment, close security holes, and research attack metrics. We also collaborate on zero-day research and as a result were able to report the discovery of eight new vulnerabilities to Schneider Electric in 2021.

With the ongoing OT-IT convergence, assets digitization, and digital transformation initiatives, the introduction of 5G into industrial environments represents a complex technology that significantly expands the potential attack surface. Fortinet encapsulates IT, OT, Industrial internet of Things (IIoT), and 5G security to empower 5G providers, industrial enterprises, and system integrators to secure private, public, and hybrid 5G networks and services. In 2021, Fortinet launched products for security gateway deployments, 5G connectivity solutions, and reconnaissance detection in OT and IIoT networks.

The digitization of our society also has impacts at the individual level, and we are proud of our innovative solutions to help ensure a safe internet for everyone:

- Fortinet has partnered with Linksys to help companies create a safe digital workspace with enterprise-class network security for their work-from-home employees in the U.S.
- The Linksys HomeWRK for education secured by Fortinet solution helps schools bridge the homework gap so that students can stay current in their learning requirements and achieve better academic performance. This solution delivers secure broadband access with nationwide coverage in the U.S.
- To anticipate threats resulting from the advent of quantum computing, we have also partnered with ID Quantique (IDQ), a quantum cybersecurity company, to help protect today's data from tomorrow's cyber threats.

## Contributing to industry innovation

As an industry leader, we have the responsibility to help advance the cybersecurity world through contributions to standardization and interoperability to enable further innovations. As a result, we actively participate in numerous industry associations and groups.

| Partnerships / Initiatives | Description |
|---|---|
| **5GACIA** | 5GACIA is a consortium of companies that facilitates industrial 5G adoption and specific use cases. They fuse OT / Industrial Internet of Things and 5G and deliver thought leadership through recommendations, white papers, and frameworks. |
| **European Telco Standards Institute (ETSI)** | ETSI produces globally applicable standards for ICT-enabled ETSI produces globally applicable standards for ICT-enabled systems, applications and services deployed across industry sectors and society. Fortinet collaborated with ETSI to enable 5G innovation and implemented ETSI standards for Quantum Key Distribution. |
| **International Society of Automation (ISA)** | The ISA is a non-profit technical society for engineers, technicians, business people, educators, and students, who work, study or are interested in automation and related pursuits, such as instrumentation. |
| **MEF** | MEF is a global industry association of network, cloud, and technology providers driving network transformation to power the digital economy. Fortinet contributed to the MEF-coordinated industry standardization SASE Services Framework white paper. |
| **Wi-Fi Alliance** | Wi-Fi Alliance drives global Wi-Fi adoption and evolution through thought leadership, spectrum advocacy, and industry-wide collaboration. |



*6 - Operational Technology is the use of hardware and software to monitor and control physical processes, devices, and the infrastructure.*

## Partnerships and initiatives for the Greater Good

Disrupting cybercriminals and dismantling the attack infrastructure is a joint responsibility that requires strong, trusted relationships with other public and private organizations. Cybercriminals operate like a business, and if we keep forcing them to start over, rebuild, and shift tactics, it is costly for their organizations and better for the digital world. For Fortinet, sharing actionable threat intelligence between organizations and helping shape the future of mitigation against cyber threats is vital. Our key partnerships and joint initiatives include:

| Partnerships / Initiatives | Description |
|---|---|
| **Cyber Threat Alliance** | Fortinet is a founding member of the CTA, an independent non-profit organization composed of cybersecurity providers and practitioners dedicated to sharing critical threat intelligence to raise the level of security for organizations globally. See below for additional details, including the game changing Magellan platform. |
| **Exploit Prediction Scoring System (EPSS)** | Fortinet contributes to the EPSS, an effort that uses data to estimate the probability of vulnerability in software and network systems. This is used to provide early warnings and evaluate dynamic risk over time. |
| **FIRST** | Fortinet is a member of FIRST, a consortium of incident response and security teams from every country to ensure a safe internet for everyone. Through FIRST, Fortinet works with national CERTs (Computer Emergency Response Teams) across the world. |
| **INTERPOL Gateway** | Fortinet's partnership with the Interpol Gateway includes sharing threat information generated by the Fortinet FortiGuard Labs global threat research team with INTERPOL. FortiGuard Labs routinely responds to breaking RFIs (Request for Intelligence) as new cases emerge. |
| **MITRE Engenuity Center for Threat Informed Defense (CTID)** | The CTID, a research and development hub, serves as a focal point for the Threat-Informed Defense Community, driving applied research and advanced development to improve cyber defense at scale for the global community. Fortinet has been engaged in several new and innovative projects with MITRE to help the industry make advances in threat detection, visibility, and reporting. |
| **NATO – NATO Industry Cyber Partnership (NICP)** | Fortinet entered a partnership with NATO – the NICP – to collaborate on intelligence sharing on cyber threats. This partnership enables the proactive identification and stopping of advanced persistent threat and cybercriminals that threaten national security, delivering greater security for all our customers and all organizations. |
| **WEF Partnership against Cybercrime (PAC)** | Fortinet is a founding member of the WEF PAC, an initiative formed with the goal of building trusted public & private sectors threat sharing relationships. In 2021, the PAC created the Cybercrime ATLAS project to map all major global cybercrime syndicates and develop a hub to link cybersecurity experts and allow them to share knowledge on analysis techniques, new tools, new adversary behavior, and strategic insights. |

## Focus on threat intelligence collaboration

### CTA: Magellan platform

Fortinet, one of the original two founding members of the CTA, co-engineered Magellan, the most extensive collaborative Structured Threat Information Expression (STIXv2TM) platform in the industry. All industry members have been actively using Magellan and over 200 million observations on threat intelligence have been shared across the platform.

### Fortinet - INTERPOL partnership

Fortinet has provided INTERPOL with cyber threat intelligence since 2015 as an active member of an expert working group. The information provided by Fortinet has helped INTERPOL discover and identify multiple cybercrime operations, including the first arrests we contributed to in 2016 that leveraged Fortinet intelligence. More recently, in 2021, Fortinet, along with several other private sector companies supported an INTERPOL-led operation targeting cybercrime across the ASEAN region. This operation led to the identification of approximately 9,000 command-and-control servers and hundreds of compromised websites including government portals. In previous years, in cooperation with INTERPOL and other private sector partners, Fortinet has helped uncover the online fraudsters behind thousands of online scams that cost hundreds of victims globally over $500 million.

## In 2022, we will focus on the following initiatives to advance cybersecurity internally and externally:

- Integrate more third-party technology into the Fortinet Open Fabric Ecosystem.
- Expand Fortinet's products and services to further cover the attack surface, including more early-stage reconnaissance capabilities and the expansion of AI / ML-driven threat detection capabilities.
- Initiate an internal organization-wide innovation project to allow employees to further dedicate time outside their core job function, to innovate and solve cyber problems.
- Create a cybercrime hub in partnership with the WEF with the capability launching disruption campaigns against cybercrime.
- Implement tools to track customer satisfaction and customer challenges related to the direct use of our products. And develop strategic initiatives to help customers with product knowledge-sharing and maximizing their use.

# Information security & privacy

**Fortinet provides organizations with the advanced technologies and solutions they need 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. We protect data from unauthorized access by unwanted parties and cyber threats, and at the same time, allow authorized users to securely access data while conforming to globally recognized standards.**

## Protecting our products

Fortinet implements organizational, administrative, and technical measures based on industry-standard information security measures prescribed by the National Institute of Standards and Technology (NIST) and aligned with the ISO/IEC 27000 series of standards to safeguard the confidentiality, integrity, availability, privacy and resiliency of Fortinet's IT infrastructure and data.

Fortinet operates a Secure Product Development Lifecycle policy within the scope of our ISO 9001 Quality Management System to mitigate the risk of software, hardware and supply chain vulnerabilities. Fortinet also adheres to ISO/IEC policies for vulnerability disclosure and handling processes when working with Fortinet customers, independent security researchers, consultants, industry organizations, and other vendors to identify possible security vulnerabilities and issues with Fortinet products, services, and networks. We operate a proactive and fully transparent vulnerability management process with a continual code audit and all internally discovered vulnerabilities are published through the public notification process. Additional details of our security vulnerability policies can be found in our Product Security Vulnerability Management Policy.

## Protecting our data

Our information security policies protect the confidentiality, integrity, availability, privacy, and resiliency of the Fortinet system as well as the employee and customer data stored within the network. Our Privacy Policy details how Fortinet handles information provided by our partners and customers and the purposes of using such personal data (outside of human resources and recruiting).

Fortinet has received ISO 27001 information security certification (limited scope) and several SOC2 examinations for its data centers and primary cloud services. The ISO 27001 certification and SOC2 reports provide our customers with assurances and transparency about Fortinet's information security program and the security measures that protect customer data.

Information security is overseen by the Audit Committee of the Board of Directors. We conduct management review of these policies either annually or when significant changes occur, so policies remain suitable, adequate, and effective. We also communicate any changes to these policies to our employees.

Fortinet IT and Information Security teams leverage the company's own products and solutions to prevent, detect and respond to cyber threats and protect customer data under a Fortinet on Fortinet program, providing early feedback to product development.

**Fortinet on Fortinet**

We adopt and implement our own technology for our internal information security.

## Highlights in 2021

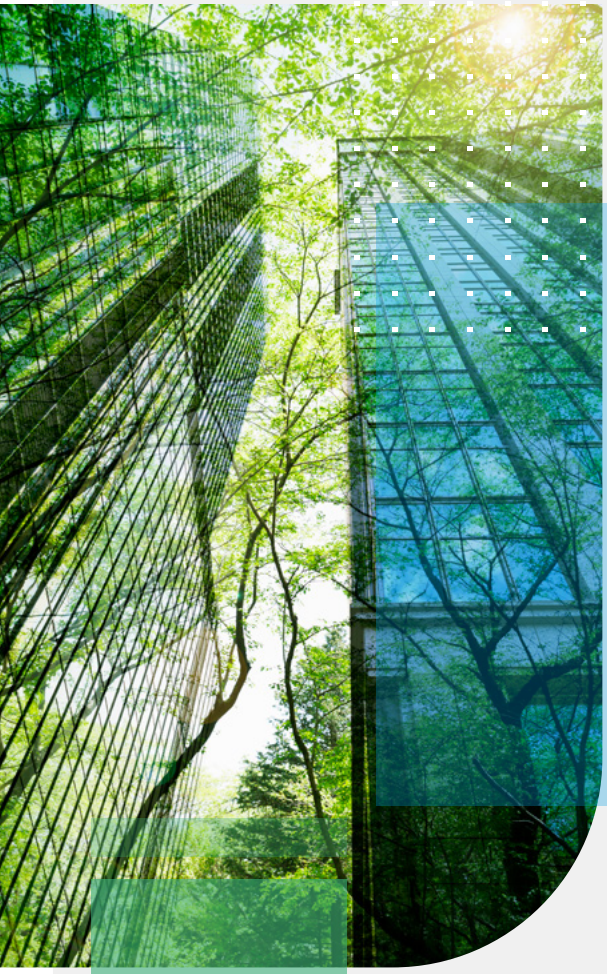
Fortinet provides employees with mandatory annual information security awareness and compliance trainings. Fortinet's Data Privacy Awareness Training provides employees with a more detailed overview of global data privacy laws, principles, data security and the processes and procedures governing data privacy and security.

We developed a procurement program for our internal business teams that work closely with external vendors. The program entails providing internal business teams with additional guidance, so they fully understand the privacy concepts and requirements involving the use, collection, or disclosure of personal information. We also require vendors who work with personal data to comply with applicable privacy laws, implement data security measures, and follow any additional and relevant data privacy requirements.

**87%** **of employees completed the 2021 Infosec-Awareness Compliance training**

## In 2022, we will continue to strengthen the information security program by:

- Extending the scope of the ISO 27001 certification to encompass additional functions.
- Obtaining SOC2 certifications for additional products/services.
- Enhancing our products and services to cover new security and privacy regulations, and ensure compliance with applicable security and privacy regulations.
- Continuously expanding our existing privacy training to account for regional differences in privacy laws across jurisdictions arising from our global presence.



# Respecting the environment

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



## Our approach

Environmental considerations such as climate change, resource scarcity, and the energy crisis are a top priority for the future of our planet. Most nations have signed the Paris Agreement to limit global warming, preferably to 1.5 degrees Celsius. But governments alone cannot reverse the effects of climate change, and partnerships with the private sector are a critical path forward for accelerating the transition to a sustainable future and low-carbon economy.

The 2021 United Nations Climate Change Conference (COP26) has called on nations and businesses to take concrete, united actions to reduce potential environmental impacts and preserve our planet for future generations. Fortinet is committed to doing its part in respecting the environment and ensuring the future of our planet. We demonstrate our commitment to environmentally responsible behavior by reducing the footprint of our products and solutions, adopting responsible approaches to our daily business operations, and helping our broader value chain progress toward circularity.

### Sustainability data and policies



Form 10-K

Environmental Policy

Pledge to the environment

# Product environmental impacts

**Environmental sustainability remains at the core of all Fortinet products throughout the entire product lifecycle. This includes design, manufacturing, product energy use and efficiency at customer sites, and recycling and proper disposal at the end of life. All our products comply with all globally recognized product environmental compliance directives and regulations.**

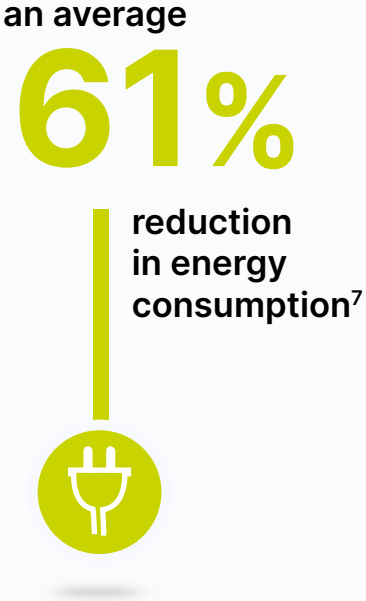
## Highlights in 2021

We formed a taskforce to drive research and development (R&D) on corporate social responsibility topics, including product environmental impacts. The purpose of this group is two-pronged–first to make the R&D team aware of sustainability and its importance and embed it into product development, and secondly, to allow the CSR team to understand the various product inputs to calculate carbon emissions, develop biodegradable packaging, and generate other sustainability initiatives.

Fortinet products use less energy compared to peer products, as per a Fortinet R&D study conducted in 2021. Our years of dedicated innovation and the development of the industry's only security-focused processors have allowed us to integrate multiple security and networking functions into a single, energy-efficient platform. As a result, each new generation of products, uses less power, space, and cooling. On average, our solutions consume 3X fewer resources than traditional appliances while delivering up to 15X more performance. Our power consumption technology also ensures that each generation of Fortinet products consumes less energy than the prior generation.

In 2021, we spent time assessing the environmental impact of our products and developed action plans to address adverse effects while putting into place internal controls. As a result, we have developed a methodology based on the GHG protocol and ISO 14064 to calculate carbon emissions of products in use. We are looking at the circular economy concept and looking to reducing the environmental impact of product packaging. As such, we have measured and implemented biodegradable packaging for our 1st class of products.[8]

In partnership with third-party vendors including Wistron Green-Tech, Fortinet has begun tracking the amount of e-waste being collected and disposed in the company's warehouse located in Union City, California - our largest warehouse in North America. While we are only at the beginning of the process, we have already reduced our waste by 21% in 2021. Fortinet also requires its distributors and resellers worldwide to perform an environmentally friendly, WEEE-compliant collection of discarded products at no charge to the user.




## In 2022, to make our products more sustainable, we will:

- Pursue the assessment of the design process and materials used when creating products. We will work to reuse as much packaging as possible and investigate potential reconditioning options. And we will engage with our distributors to understand their detailed process of disposing packaging.
- Enhance our engagement with component vendors from which our products are created to ensure they are aware of their environmental impact.
- Look into packaging for the 2nd class of products[9] and calculate carbon emissions for the entire product lifecycle.

*7 - Improvements in maximum power consumption use in models (FortiGate E and FortiGate F Series) released in the past 2 years.*
*8 - 1st class of products refers to small-size desktops.*
*9 - 2nd class of products refers to medium-size desktops.*

# Environmental management and climate change

**We have approached this material topic by focusing on our own operations and developed overarching climate goals that we will move toward. From an operational standpoint, we are committed to driving an environmentally low impact business across our globally distributed offices, facilities, and data centers. We also monitor and manage our impact on the climate from our owned operations and supply chains. In alignment with the Science-Based Target Initiative (SBTi) methodology, we publicly committed to a target of carbon neutrality on our Scope 1 and 2 emissions by 2030 and pledged to increase our climate disclosures.**

## Highlights in 2021

Fortinet understands its responsibility to respect the planet and contribute to the efforts to curtail against climate change. We published our first Environmental Policy to establish a global standard for Fortinet's approach to managing environmental impacts. We also initiated an analysis of the risks and opportunities of climate change to our business and published them for the first time in our 2021 10-K filing. We strive to identify and manage environmental sustainability impacts in all our business areas.

Fortinet invests in renewable electricity and sustainable projects around the world. All our owned facilities run on 100% renewable electricity, including our headquarters[10]. We ensure that most, if not all, of our new sites will only use 100% renewable electricity and that new construction meets LEED/BREAM or other green building certifications. To that end, we use solar panels in our owned facilities across North America and Europe.

Fortinet has publicly announced its commitment to carbon neutrality by 2030 using renewable energy, energy and carbon efficiency methodologies, and emission offset programs across its owned operations globally. This target is relative to our Scope 1 and Scope 2 emissions resulting from our owned facilities worldwide, in alignment with the SBTi. Our newly created climate roadmap will help us reach our goals. We have also defined internal targets and key performance metrics and are working on action plans to mitigate and minimize our environmental impact.

In 2021, we started to track water usage and waste in our sites. We expect to understand these measures better once our Environmental Management System is in place in 2022. The radiant cooling system used in Fortinet's new headquarters, for example, saves 76,800 gallons per year compared to a standard cooling tower. We also plan to inform our suppliers, contract manufacturers, and other stakeholders of our climate goals and work with them to ensure that we have their support and cooperation so we can meet our public goals.

## In 2022, we will make progress toward our goals and targets by:

- Maturing our sustainability reporting by beginning to align with the TCFD recommendations and participating in CDP reporting to increase the transparency of our environmental disclosures.
- Capturing the inventory of our Scope 3 emissions and committing to aligning our targets with the Science Based Targets initiative (SBTi) methodology.
- Continuing the work around water and waste management.
- Developing guidelines for green (renewable energy) leasing options for the facilities group.
- Improving our environmental performance by beginning the process for ISO 14001 certification.



*10 - If a new facility cannot obtain renewable electricity due to its location, Fortinet ensures the purchase of renewable energy credits to offset carbon emissions until renewable energy is available via the local utility.*

## Fortinet's energy efficient headquarters facilities

Fortinet's flagship project is our brand-new headquarters facilities in Sunnyvale, California. Our recent headquarters expansion is a state-of-the-art 172,000-square-foot building and LEED-Gold certified. This all-electric, net-zero facility has implemented multiple energy efficiency measures including solar panels and radiant cooling, which uses 30% less energy than a standard building and conserves 76,800 gallons of water annually. Fortinet also incentivizes employees at its headquarters to reduce their environmental footprint by providing onsite solar-powered electric vehicle charging stations, preferred parking spaces for sustainable energy vehicles, and installed bike racks. And the solar panel installation will not only make the headquarters fully energy self-sufficient but generate enough additional power to offset much of the energy consumption of our other facilities across North America.

# Growing an inclusive cybersecurity workforce

**Building an inclusive, equitable, and diverse workforce within our organization and across the industry will help empower individuals to reach their full potential.**

## Our approach

The cybersecurity industry faces a significant skills gap of over 2.7 million cybersecurity professionals worldwide. This shortage affects not only cybersecurity companies like Fortinet, but also all our customers and partners. There is also a need for a more diverse representation within the workforce to enable different perspectives that can propel innovation and propose new ways of combating cybercrime.

No individual, institution, organization, or government can address those issues alone. It will take a collaborative effort to close the cybersecurity skills gap while diversifying talents. Fortinet is focusing on growing an inclusive and diverse workforce and contributing to a broader awareness of the benefits of a career in cybersecurity. We are also committed to helping reduce the cybersecurity skills gap across a wide and diverse range of audiences and improving opportunities for those seeking a career in cybersecurity.


**Diversity, equity and inclusion** ..... 25

**Cybersecurity skills gap** ..... 28


**Sustainability data and policies**


DEI data ..... 38

Cyber skills gap data ..... 41

Fortinet NSE

# Diversity, equity and inclusion

**Fortinet is building an inclusive and diverse workplace that rewards collaboration and innovation and empowers everyone to reach their full potential. Fortinet's success is tied to our ability to attract and retain skilled global talent and build an inclusive culture so our employees can thrive in a pleasant work environment. We are committed to the global representation of all genders, races, ethnicities, nationalities, ages, and sexual orientations in our workforce. We also support a diverse workforce by ensuring all our employees have equal opportunity, fair recruitment, and equitable remuneration.**

## Fortinet – Who we are

Fortinet is a global company with operations in over 90 countries and is proud to be highly diverse in culture and age. We are also aware that we have more to do to achieve diversity, in particular, when it comes to gender diversity.

## 2021 key metrics[11]

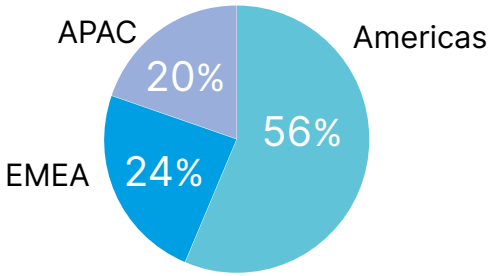
**Board of Directors:**

≃56%

under-represented groups;

1/3 female

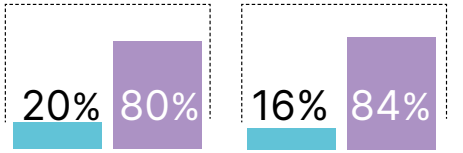
**Region**




**Number of employees**

10,005

**Gender**



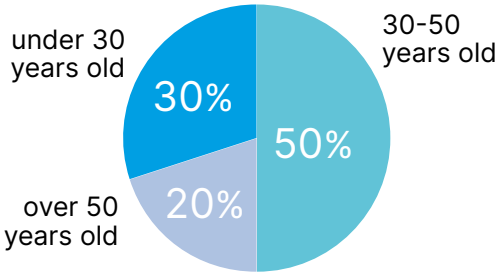

All employees | Management

**Female new hires**

71.6%

YoY increase

**Age**






*11 - Excluding Alaxala and Linksys employees (as of December 31, 2021).*

## Highlights in 2021

Because diversity is key to an innovative and successful organization, we strive to be inclusive and equitable, ensuring that all voices are represented at every level of the organization. To that end, we are focused on recruiting, developing, and retaining high-performing, innovative talent with diverse backgrounds. This starts with drawing from a wide pool of potential candidates to work in all areas of our organization. We have also begun to incentivize diversity in recruitment, with a particular focus on women and minorities. In 2021, the percentage of women in our total workforce increased by 26%. Our recruiters now have diversity targets, and diversity goals are key performance metrics for recruitment teams globally. In addition, senior management from R&D, sales and support service teams now have gender diversity reports to track progress.

### Recruitment

To help meet our diversity goals, we reviewed job descriptions to ensure the language is gender-neutral and educated our hiring managers on DEI principles through inclusive team-building workshops. We have also expanded our job postings to sites that focus on women and minorities and collaborated with universities to develop a pipeline of diverse talent. Our partners include a Canadian university whose students are recruited for R&D and universities in the U.S. and Latin America for students for non-R&D positions. In the Latin America region, we delivered cybersecurity training to students in over 15 universities. And in 2021, we increased our female new hires by 71.6% compared to 2020.

### Retention

Inclusion has always been part of our culture and starts from day one for each employee with our newcomer welcome and onboarding programs. Our workforce culture ensures that our employees know that no matter where they may come from, at Fortinet, they are not only welcome, but their voices are heard and valued. Building an environment of collaboration requires valuing different perspectives and voices because every employee plays a crucial role in team decision-making and meeting critical business objectives.

We provide our employees with a pleasant work environment, designed with comfort in mind including ergonomic equipment, and offering safety, sports facilities, breakout areas, nap rooms and other services. We offer competitive salaries, benefits and equity programs that reflect how much we value our employees.  Benefits vary based on each country where we operate and include health benefits, retirement plans and allowances. Our FortiChamp program is a peer recognition program that every quarter recognizes and rewards individual employees who exemplify the company's values through their outstanding work. A similar FortiChamp award is delivered to an entire functional team once a year.

Great Place To Work.

Recognized as 'Best Workplaces' by Great Place to Work*

* In Colombia, Brazil, and Mexico for the sixth consecutive year

To maintain our inclusive culture, Fortinet offers the following set of talent programs and initiatives across the world:

- **Fortinet conversations** – are the levers with which Fortinet builds key relationships, develops business, and accelerates performance. These management practices and shared organizational leadership frameworks help drive employee engagement, development, and performance.
- **Manage for success** – equips managers to be effective people leaders for a diverse and ever-evolving workforce. This program is comprised of three modules that guide a participant from transitioning to management, to managing people and eventually to leading and accelerating performance.
- **Unconscious bias training** – stimulates critical self-reflection and personal ownership for growth and generates actionable insights to help employees improve their decision-making. This is part of our commitment to ensuring an inclusive environment where all employees thrive while achieving their personal and career goals.
- **Inclusive leadership guide** – has been published internally and targeted toward helping people leaders at Fortinet commit to enabling performance and realizing the potential of all our employees. The guide reaffirms our belief that managing at Fortinet is an ongoing and deliberate act of supporting employees to perform at their best.

## Equitable pay

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

### Mentor Me program in Latin America

Mentorship programs are effective in helping further the careers of new employees and interns, particularly when they are from under-represented programs. Fortinet understands this and as part of its Mentor Me program in Latin America, focuses on providing mentorship and ensuring mentors are equipped to provide the guidance mentees need. In 2021, over 22 leaders were trained to become new mentors and develop the future leaders of Fortinet.

## In 2022, we will continue our DEI journey by:

- Strengthening diversity in non-traditional lines of businesses such as sales and R&D and across regions. We will institute gender diversity targets to increase the representation of women in Sales and R&D and create a Diversity Employee Resource Group in EMEA to complement the ones in Americas.
- Developing a diverse management talent pipeline by launching talent management conversations – conversations that identify roles critical to business operations and growth and proactively plan to fill these roles.
- Engaging our employees through sustainability education, including on DEI-related topics, by conducting employee pulse surveys.

# Cybersecurity skills gap

Fortinet is committed to achieving a sustained and measurable global impact on closing the skills gap across diverse audiences through the Fortinet NSE Training Institute. It provides cybersecurity training and certifications, career growth resources and hiring opportunities to make a career in cybersecurity attainable for all – including students in colleges and universities, adults looking for a new career path, and cybersecurity professionals looking to enrich their skills. In 2021, Fortinet bolstered its commitment to address the cybersecurity skills gap by pledging to train one million people globally across the next five years.

These programs include a wide range of self-paced, instructor-led, and virtual instructor-led training, as well as practical, experiential exercises to demonstrate mastery of complex network security concepts. To ensure we are reaching a diverse set of individuals and that there are no barriers to access, our expert-level training is delivered in local languages through an extensive network of Fortinet Authorized Training Centers.

Fortinet will reduce the cybersecurity skills gap and reach its target of training one million people globally by:

**Educating the professionals of tomorrow:** Through the Academy Partner Program, we offer official training materials, technology, and exam vouchers to over 400 academic institutions and NGOs in 90 countries, thereby providing students with the opportunity to receive industry-recognized certification. This allows participants, including those who serve underrepresented groups, to integrate high-quality technical cybersecurity training into their curriculum to encourage, enable, and accelerate the next generation of cybersecurity professionals.

**Diversifying the cybersecurity workforce:** Fortinet is committed to helping build an inclusive and diverse security workforce through its *Education Outreach Program*. We partner with local and global organizations to create career pathways in cyber for all under-represented or disadvantaged individuals.

- Fortinet partners with active associations focused on driving gender diversity including Women in Cybersecurity (WiCYS) in the U.S., and WOMCY in Latin America to promote Fortinet's certification program among their members. To help women improve their skills and advance their cybersecurity careers at all levels through mentorship programs, we also collaborate with Women4Cyber in Europe.
- The Fortinet Veterans Program facilitates the transition of military service members, veterans, and military spouses into cybersecurity careers. The program has been expanded outside the U.S. to include the U.K., Canada, and Australia.
- Fortinet drives global collaboration. We have partnered with IBM to include our cybersecurity curriculum into the SkillsBuild platform to help create new cybersecurity career pathways for job seekers, including those struggling with long-term unemployment, refugees, asylum seekers, veterans, and students. Another joint initiative is the Cybersecurity Learning Hub, resulting from a partnership between Fortinet, Salesforce, and the WEF.

**Upskilling cybersecurity professionals:** Fortinet is helping cybersecurity professionals, including Fortinet employees, learn new skills, reskill, or upskill through the NSE Certification Program. This eight-level training and certification program provides technical professionals with independent validation of network security skills and experience.

Fortinet created a set of Fortinet Education Pathways mapping extensive training catalogs to NIST Education Pathways. NIST developed the project as part of the National Initiative for Cybersecurity Education to help students and those in career transition navigate the complexity of cyber careers.

In 2021, we introduced a new OT education pathway to serve as a roadmap on training and certifications necessary for careers in OT security. And we launched a new OT security course as part of our NSE Certification Program to expand technical skills for protecting OT environments, increasingly prone to cyberattacks.

## 2021 key metrics

| People completing Security Awareness Training: | Companies signing up for Security Awareness Training service: | Total # people trained: | Certifications issued: |
|---|---|---|---|
| 41,000+ | 1,150+ | 164,982 | 226,258 |

# Growing an inclusive cybersecurity workforce

## Cybersecurity skills gap

**Closing the digital divide by driving broader awareness on cybersecurity:**
People are the weakest link for cybercriminals. The cybersecurity fundamentals training is a critical line of defense for any company, government or individual, and is something we are committed to addressing through:

- Fortinet free training to all cybersecurity professionals, IT professionals, and teleworkers through a complete self-paced curriculum of cybersecurity training courses. These courses range from basic cybersecurity awareness training to more advanced training.
- Fortinet Security Awareness and Training service for organizations of all sizes and suitable for the entire workforce, from technical to non-technical employees and contractors. It offers industry-leading cybersecurity awareness components to educate people about today's cyber threats, such as phishing, social engineering, and ransomware attacks, and how to protect against them.
- Various initiatives to drive awareness among young people: to increase cyber awareness among children ranging from 7 to 12 years old, we published "Cyber Safe: A Dog's Guide to Internet Security", a book co-authored by Renée Tarun, Deputy CISO/Vice President Information Security at Fortinet.

## In 2022, to reduce the cybersecurity skills gap, we will:

- Enhance the Security Awareness and Training service as a SaaS-based offering to help IT, security, and compliance leaders build a cyber-aware culture among our customers and employees.
- Introduce cybersecurity to students at an early age by developing additional cybersecurity training programs for K-12 students and a career jumpstart program for at-risk youth.

# Promoting responsible business

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

## Our approach

Our approach to responsible business is based on a strong corporate governance structure and high ethical standards promoted throughout our value chain. Protecting human rights is core to our business, and we are committed to respecting them. Stakeholders are increasingly paying attention to ethical product use in the technology sector. The consequence of the digitization of our global society is that companies must consider the human rights implications of the products and services they produce, both from an upstream and downstream perspective. It is important for them to design, develop, deploy, sell, and manage products and services in ways that are both ethical and respect human rights. Fortinet firmly believes that our business and the products and solutions we produce are a force for good, and we are committed to being a responsible business.



### Sustainability data and policies



- Code of Business Conduct and Ethics
- Partner Code of Conduct
- Vendor/Supplier Code of Conduct
- Conflict Minerals Policy
- End-User License Agreement
- Anti-Corruption Policy
- Human Rights Policy
- Modern Slavery Statement
- Privacy Policy
- Whistleblower Policy

# 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 and 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 also adopted a set of policies that set out a Code of Conduct for all employees, partners, and vendors, and we have training, policies and controls designed to prevent corruption in our business. We require all employees to complete regular compliance training and offer additional training to specific functional groups. We also work closely with our suppliers and vendors to ensure they understand our expectations in relation to business ethics.

## Foundational policies

Business ethics at Fortinet are guided by the foundational policies outlined hereinafter. We expect our employees to understand and comply with all policies and do their part in helping us build a highly ethical and reputable business.

| Policy | Description |
|---|---|
| **Anti-Corruption Policy** | • Applies to all Fortinet employees worldwide, including individuals employed by or acting on behalf of Fortinet or its subsidiaries.<br>• Highlights the expectation that Fortinet does not tolerate corruption in any form worldwide. |
| **Code of Business Conduct and Ethics** | • Details the expectations and standards that will guide employees to conduct business ethically.<br>• Applies to all directors, officers, and employees of Fortinet. |
| **Codes of Conduct for Partners and Vendors/ Suppliers** | • Allows our partners, vendors and suppliers to understand our expectations regarding business ethics.<br>• Ensure our products and services are built in workplaces that are safe and respectful of individuals' rights. |
| **Conflict Minerals Policy** | • Refers to the policies associated with the extraction, trading, handling, and exporting of minerals from conflict-afflicted and high-risk areas.<br>• Outlines the conflict minerals-related governance policies, processes, and controls we have adopted in our business. |
| **Employee Handbook** | • Communicates Fortinet's core values and mission to our employees.<br>• Sets the expectation for our employees and details procedures for the work environment. |
| **End-User License Agreement (EULA)** | • Includes human rights language so that our products and services are not used to violate human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force.<br>• Applies to dealings with Fortinet and distributors, resellers, partners and end-users. It specifies the terms and conditions governing Fortinet products and services. |
| **Human Rights Policy** | • Applies to all Fortinet employees, partners, and suppliers globally and is our commitment to respecting the human rights of all our stakeholders including the users of our products and services.<br>• Provides a baseline for furthering our human rights program and due diligence process, while grounding our engagement with stakeholders on human rights-related topics. |
| **Modern Slavery Statement** | • States that Fortinet business practices, human resources procedures and staff selection are aligned with good faith efforts to combat slavery and human trafficking.<br>• Aims to prevent modern Slavery and Human Trafficking in Fortinet´s business and supply chain. |
| **Privacy Policy** | • Covers personal data that partners and customers ask Fortinet to process on their behalf.<br>• Handles personal data for Fortinet business, other than for human resources and recruiting operations. |
| **Whistleblower Policy** | • Requires every Fortinet employee to report any known or suspected violations of Fortinet policies or the law.<br>• Describes the avenues, including the whistleblower hotline operated by third-party Ethical Points, through which employees can report any unethical practice without fear of reprisal. |

**100%** of employees were communicated Fortinet's Code of Business Conduct and Ethics

**100%** of direct suppliers screened

## Highlights in 2021

Fortinet expects all employees to take business ethics seriously and requires them to complete mandatory annual ethics and compliance training. We have additional, more stringent requirements for our sales staff and executives 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.

Fortinet uses third-party screening software for suppliers and vendors. We enhanced this process in 2021 and now require new direct suppliers to be processed through a two-step verification process, including a screening in high-risk areas. Our suppliers and vendors are screened against several criteria including human rights, FCPA, and sanctions lists.

We have adopted policies supporting the protection of human rights. As an example, in 2022, we were an early company to take a public stance regarding Russia's invasion of Ukraine by publicly announcing our suspension of business in Russia. Our stance for responsible business practices was acknowledged by the Yale School of Management, which listed Fortinet as one of the early companies receiving an "A" grade for halting engagement in Russia, distinguishing us from others in the cybersecurity industry.

## In 2022, we will maintain our high ethical standards by:

- Implementing a mandatory Supplier Compliance training for our top contract manufacturers (those from whom we buy 80% of products).
- Enhancing the human rights language within the Vendor/Supplier and Partner Codes of Conduct.
- Having our worldwide distributors take mandatory training on the Partner Code of Conduct and compliance materials.

# 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.

## Highlights in 2021

Fortinet has embedded human rights clauses in its service agreements. Beyond updating existing clauses on human rights and ethical business in our agreements with contract manufacturers, we have included human rights language in our product license agreement as well in our partner and supplier codes of conduct. We have also included human rights in the mandatory employee compliance training.

We seek to avoid, prevent, and mitigate potential harm related to the use of our products and services by conducting due diligence throughout the product lifecycle. We integrate data security and privacy principles in our products and services to help our customers protect their data. Our EULA clearly states that our products and services cannot be used to engage in, or support in any way, violations, or abuses of human rights. The Partner Code of Conduct sets out expectations for our sales partners to respect human rights and labor standards.

**100%** of Manufacturing Purchase Agreement and Product License Agreement (EULA) templates were updated with human rights language

**100%** of Fortinet sales transactions were screened against U.S. embargoed countries and sanctioned/ restricted lists to ensure compliance with export and applicable regulations

## In 2022, we will strengthen our commitment to responsible product use by:

- Updating new Fortinet product datasheets template with human rights language.
- Extending the scope of our mandatory compliance and responsible product use training, which includes human rights, to partners and suppliers.
- Start assessing the application of human rights dimensions into product development, in collaboration with R&D.

# Appendix

# Performance data[1]

## Innovating for a safe internet

### Innovation

| | 2021 | 2020 |
|---|---|---|
| **Percentage of revenue generated from innovation[2]** | 41.6% | Not reported |
| **Number of new product families introductions** | 8 | 6 |
| **R&D investment[3] ($ in millions)** | 424.2 | 341.4 |

*1 - 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.*
*2 - Revenue resulting from products that include firmware versions introduced in the last two years.*
*3 - GAAP research and development expense.*

# Respecting the environment

## Product environmental impacts

| % Improvement in power efficiency per throughput for top 5 products sold[4] | 2019-2021 |
|---|---|
| FortiGate-40F | 88% |
| FortiGate-60F | 73% |
| FortiGate-80F | 75% |
| FortiGate-100F | 50% |
| FortiGate-200F | 20% |
| **Average** | **61%** |

| | 2021 | 2020 | 2019 |
|---|---|---|---|
| E-waste (in tonnes)[5] | 30.76 | 38.81 | 35.44 |

## Environmental management and climate change impacts

| | 2021 | 2020 | 2019 |
|---|---|---|---|
| Scope 1 (mtCO2e)[6] | 1,269.4 | 1,016.1 | 1,159.3 |
| Scope 2 - Location based (mtCO2e)[6] | 3,253.9 | 2,411 | 2,775.2 |
| GHG emission intensity | 1.35E-06 | 1.32E-06 | 1.82E-06 |
| Reduction of GHG emissions | 3% | 28%[7] | Not reported |
| Energy consumption (GJ) | 127,878 | 121,711 | 120,487 |
| Energy intensity | 3.83E-05 | 4.69E-05 | 5.57E-05 |
| Reduction of energy consumption | 18% | 16%[7] | Not reported |

*4 - This metric looks at improvements in maximum power consumption use in models (FortiGate E Series and FortiGate F Series) released in the past 2 years.*
*5 - Data represents e-waste from the largest warehouse in North America.*
*6 - Scope 1 and Scope 2 emissions are calculated for sites under Fortinet's operational control. Data presented here is from owned sites.*
*7 - Values result from the impacts of COVID-19 on operations and the continued growth in our business.*

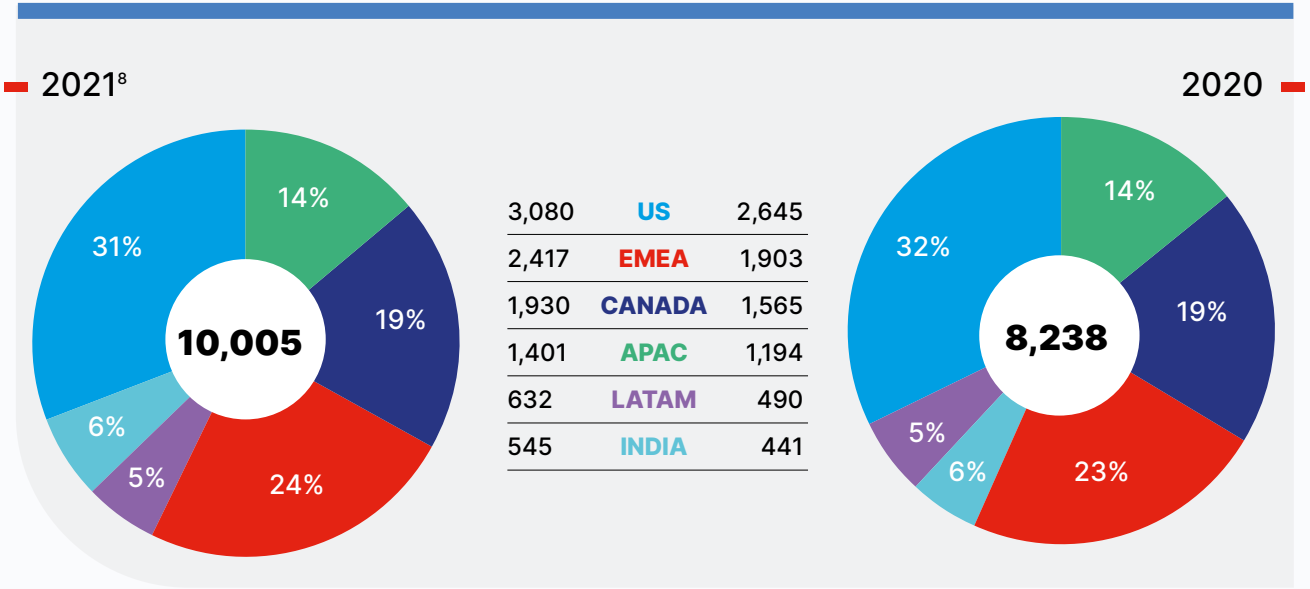
# Growing an inclusive cybersecurity workforce

## Diversity, equity and inclusion

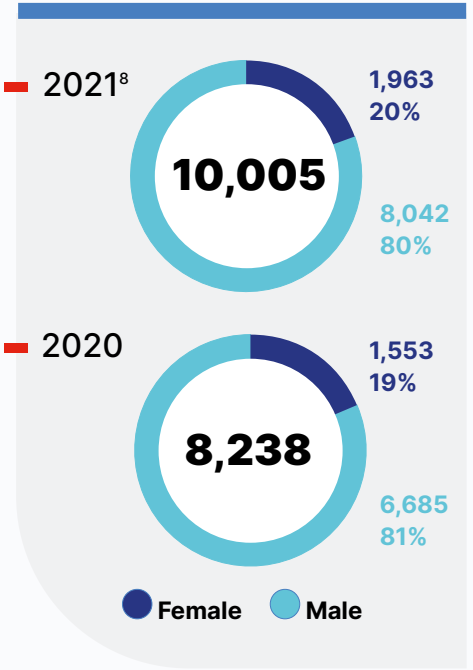
**Percentage of individuals within organization's governance bodies by diversity categories**

| | 2021 | | | 2020 | | |
|---|---|---|---|---|---|---|
| | Total | Female | Male | Total | Female | Male |
| Board of Directors | 9 | 33% | 67% | 8 | 37% | 63% |

**Total number and rate of permanent employees per region**



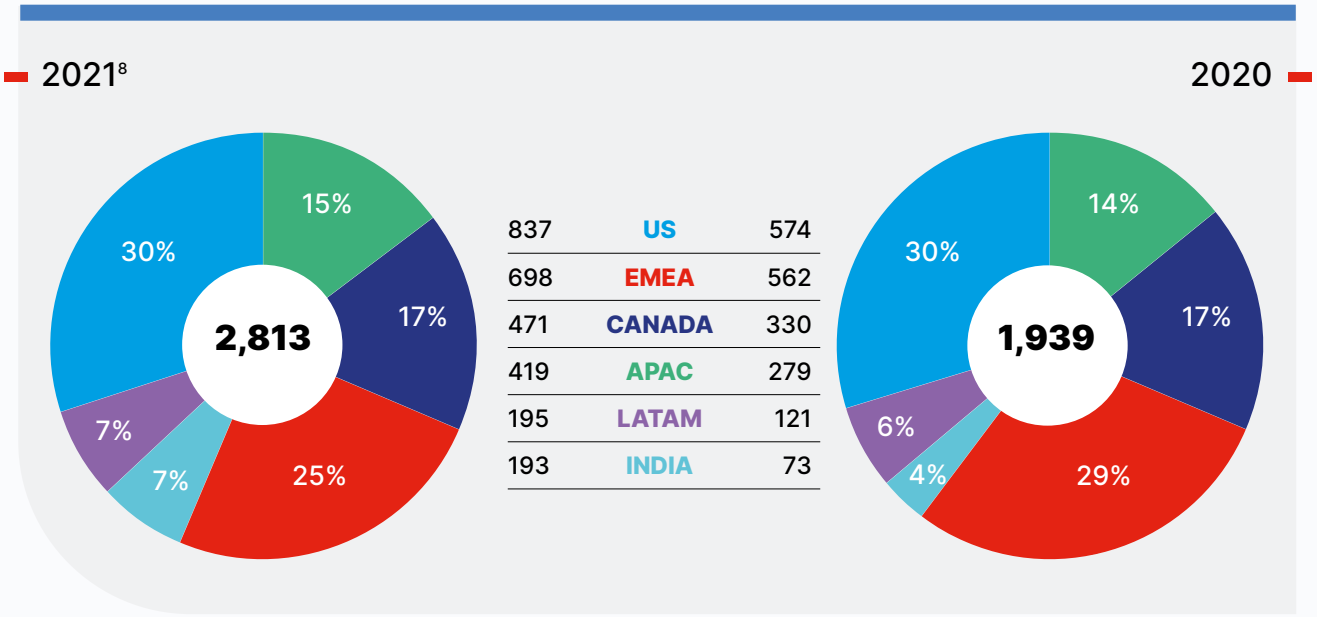

**Total number and rate of permanent employees per gender**





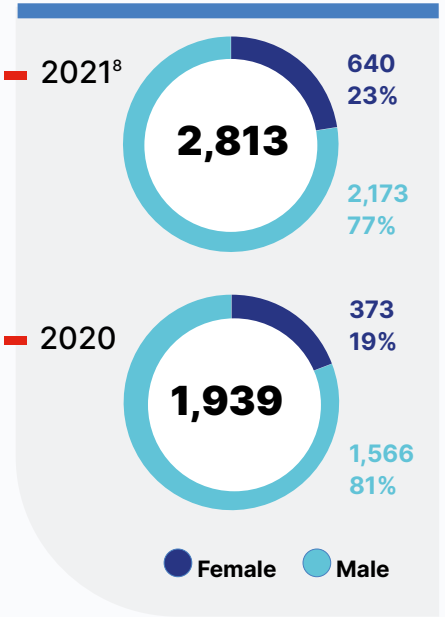

*8 - Excluding Alaxala and Linksys employees (as of December 31, 2021).*

## Total number and rate of new employee hires by region

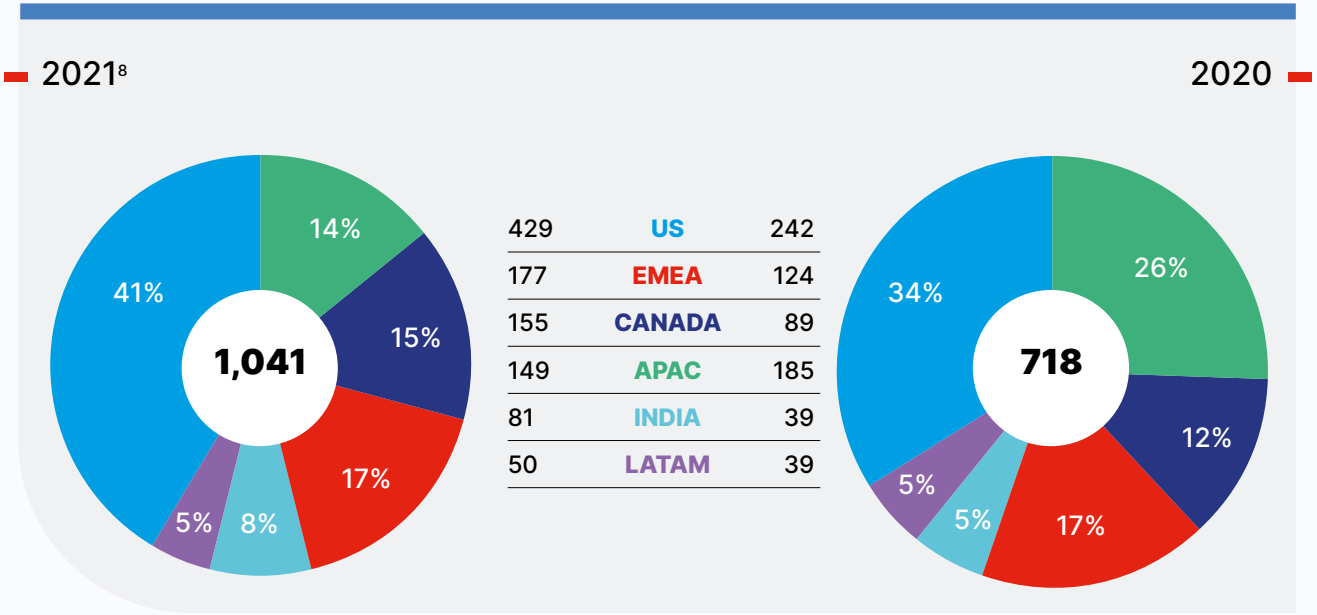



| 2021[8] | | 2020 |
|---|---|---|
| 837 | US | 574 |
| 698 | EMEA | 562 |
| 471 | CANADA | 330 |
| 419 | APAC | 279 |
| 195 | LATAM | 121 |
| 193 | INDIA | 73 |

## Total number and rate of new employee hires by gender

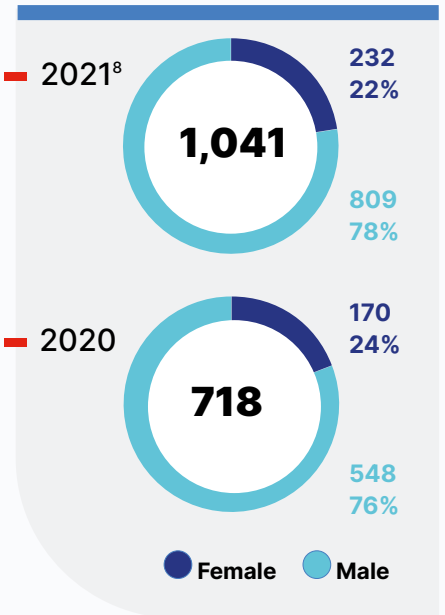



## Total number and rate of employee turnover by region



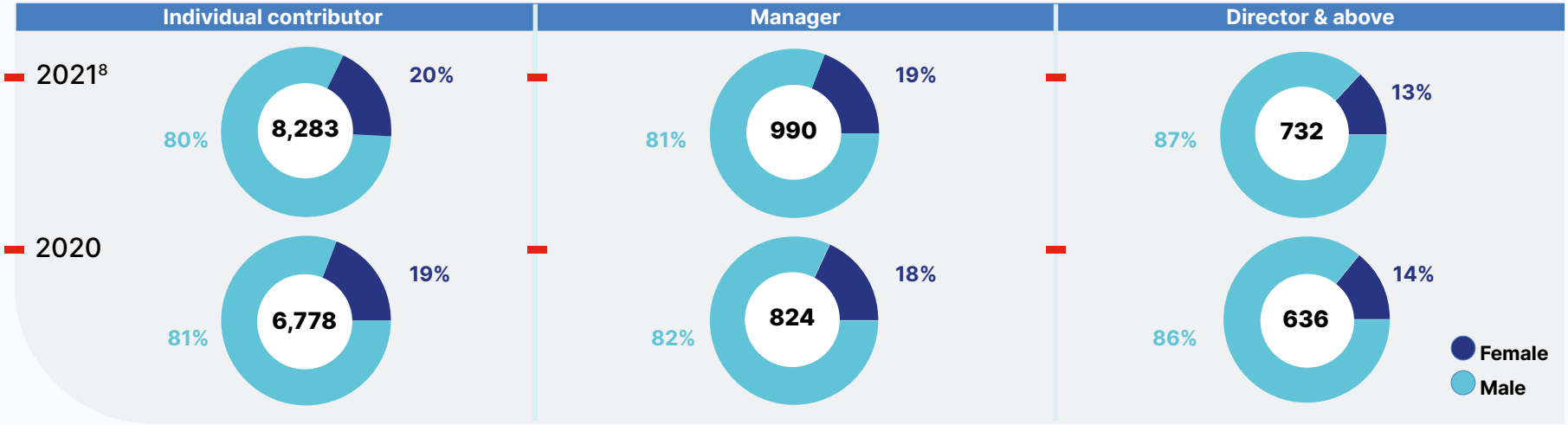

| 2021[8] | | 2020 |
|---|---|---|
| 429 | US | 242 |
| 177 | EMEA | 124 |
| 155 | CANADA | 89 |
| 149 | APAC | 185 |
| 81 | INDIA | 39 |
| 50 | LATAM | 39 |

## Total number and rate of employee turnover by gender



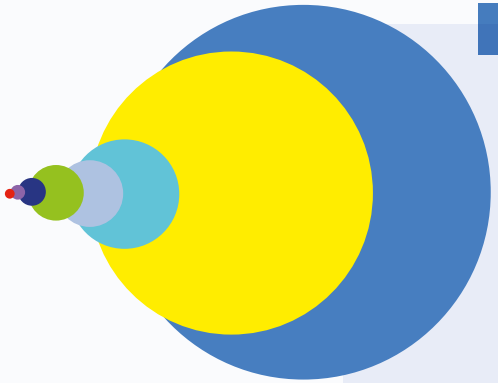

*8 - Excluding Alaxala and Linksys employees (as of December 31, 2021).*

**Total number and rate of employees per employee category per diversity categories**

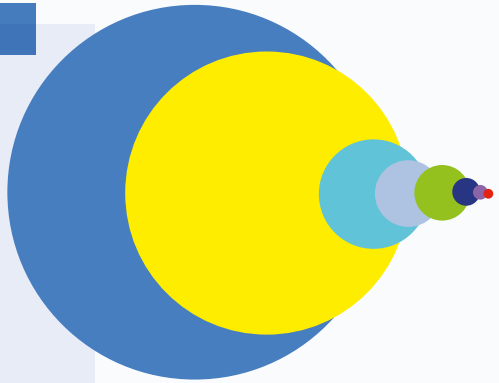



**EEO-1 Data (U.S. only) / Percentage of gender and racial/ethnic group representation for management, technical staff, and all other employees**

| | 2021 | | | | 2020 | | | |
|---|---|---|---|---|---|---|---|---|
| **Gender** | **Management** | **Technical Staff[9]** | **Other** | **Total** | **Management** | **Technical Staff[9]** | **Other** | **Total** |
| **Female** | 16% | 18% | 25% | 21% | 17% | 18% | 24% | 21% |
| **Male** | 84% | 82% | 75% | 79% | 83% | 82% | 76% | 79% |



| 2021 | | 2020 |
|---|---|---|
| 46.9% | White | 46.8% |
| 36.0% | Asian | 37.9% |
| 9.3% | Hispanic or Latino | 9.0% |
| 3.2% | Not disclosed | 1.9% |
| 2.7% | Black or African American | 2.4% |
| 1.5% | Two or more races | 1.5% |
| 0.3% | Native Hawaiian or other Pacific Islander | 0.3% |
| 0.2% | American Indian or Alaska Native | 0.2% |



*8 - Excluding Alaxala and Linksys employees (as of December 31, 2021).*
*9 - Technical Staff is the EEO-1 Category/Job group of Professional/Technical Professional.*

## Cybersecurity skills gap

| | 2021 | 2020[10] | 2019 |
|---|---|---|---|
| **Total individual people trained[11]** | 164,982 | 183,452 | 68,259 |
| **Certifications obtained from the learning platform** | 226,258 | 271,327 | 109,667 |

# Promoting responsible business

## Business ethics and responsible product use

| | 2021 |
|---|---|
| **% of employees who were communicated Fortinet's Code of Business Conduct and Ethics which refers to our Anti-Corruption policy and procedures** | 100% |
| **% Completion of Fortinet's 2021 Infosec-Awareness Compliance training** | 87% |
| **% of eligible employees who completed the quarterly sales compliance certification[12]** | 100% |
| **% Fortinet's new direct supplier that were screened using human rights criteria, FCPA, sanction lists, embargoed countries[13]** | 100% |
| **% of Fortinet sales transactions screened against U.S. embargoed countries[13] and sanctioned/restricted lists** | 100% |

*10 - The spike from 2019 to 2020 was due to the introduction of free online training.*
*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 31, 2026.*
*12 - Based on Q4 2021 sales compliance certification.*
*13 - Fortinet products and services are not authorized to be exported to U.S. embargoed countries and Fortinet does not transact business with parties in U.S. embargoed countries.*

# 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, 2021- December 31, 2021] | |
|---|---|---|
| GRI 1 used | GRI 1: Foundation 2021 | |
| Applicable GRI sector standard(s) | None developed yet | |
| **GRI standard** | **Description** | **Reference/Disclosure** |
| **General disclosures** | | |
| GRI 2: General disclosures 2021 | 2-1 Organizational details | 2021 Sustainability Report / About Fortinet p.2 |
| | 2-2 Entities included in the organization's sustainability reporting | 2021 Sustainability Report / About this report p.5 |
| | 2-3 Reporting period, frequency and contact point | 2021 Sustainability Report / About this report p.5 |
| | 2-4 Restatement of information | This is Fortinet's first sustainability report, as such, there are no restatements. |
| | 2-5 External assurance | 2021 Sustainability Report / Limited assurance statement p.48 |
| | 2-6 Activities, value chain and other business relationships | 2021 Sustainability Report / About Fortinet p.2 |
| | 2-7 Employees | 2021 Sustainability Report / Diversity, equity and inclusion p.24-27<br>2021 Sustainability Report / Performance data p.38-40<br>- 9,984 full time employees and 21 part time employees in 2021<br>- 8,225 full time employees and 13 part time employees in 2020 |
| | 2-9 Governance structure and composition | Social Responsibility Committee Charter<br>Governance Committee Charter<br>Human Resources Committee Charter<br>Audit Committee Charter |
| | 2-10 Nomination and selection of the highest governance body | Social Responsibility Committee Charter<br>Governance Committee Charter<br>2022 Proxy Statement p.33 |
| | 2-11 Chair of the highest governance body | Ken Xie, CEO and Chairman<br>2022 Proxy Statement p.30-31 |
| | 2-12 Role of the highest governance body in overseeing the management of impacts | Social Responsibility Committee Charter<br>Governance Committee Charter<br>2022 Proxy Statement p.32 |

| | | |
|---|---|---|
| | 2-13 Delegation of responsibility for managing impacts | Social Responsibility Committee Charter<br>CSR Committee Charter<br>2021 Sustainability Report / Governance p.10 |
| | 2-14 Role of the highest governance body in sustainability reporting | The board has approved this inaugural Sustainability Report. |
| | 2-15 Conflicts of interest | Audit Committee Charter<br>Governance Guidelines |
| | 2-16 Communication of critical concerns | 2022 Proxy Statement p.34 |
| | 2-17 Collective knowledge of highest governance body | 2021 Sustainability Report / Governance p.10 |
| | 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<br>Human Resources Committee Charter |
| | 2-22 Statement on sustainable development | 2021 Sustainability Report / CEO letter p.4 |
| | 2-23 Policy commitments | Human Rights Policy<br>Vendor/Supplier Code of Conduct<br>Partner Code of Conduct<br>Code of Business Conduct and Ethics<br>Conflict Minerals Policy |
| | 2-24 Embedding policy commitments | Code of Business Conduct and Ethics<br>Vendor/Supplier Code of Conduct<br>Partner Code of Conduct<br>Human Rights Policy<br>2021 Sustainability Report / Business ethics p.31-33<br>2021 Sustainability Report / Responsible product use p.34<br>2021 Sustainability Report / Performance data p.41 |
| | 2-26 Mechanisms for seeking advice and raising concerns | 2021 Sustainability Report / Business ethics p.31-33<br>Whistleblower Policy |
| | 2-28 Membership associations | 2021 Sustainability Report / Cybersecurity risks to society p.13-17 |
| | 2-29 Approach to stakeholder engagement | 2021 Sustainability Report / Materiality and stakeholder engagement p.7-8 |
| **Material topics** | | |
| GRI 3: Material topics 2021 | 3-1 Process to determine material topics | 2021 Sustainability Report / Materiality and stakeholder engagement p.7-8 |
| | 3-2 List of material topics | 2021 Sustainability Report / Materiality and stakeholder engagement p.7-8<br>2021 Sustainability Report / Strategic framework p.9 |

| | | |
|---|---|---|
| | 3-3 Management of material topics | 2021 Sustainability Report / Cybersecurity risks to society p.13-17<br>2021 Sustainability Report / Information security and privacy p.18-19<br>2021 Sustainability Report / Product environmental impacts p.21<br>2021 Sustainability Report / Environmental management and climate change p.22-23<br>2021 Sustainability Report / Cybersecurity skills gap p.28-30<br>2021 Sustainability Report / Diversity, equity and inclusion p.24-27<br>2021 Sustainability Report / Business ethics p.31-33<br>2021 Sustainability Report / Responsible product use p.34 |
| **Indirect economic impact** | | |
| GRI 203: Indirect economic impacts 2016 | 203-2 Significant indirect economic impacts | 2021 Sustainability Report / Cybersecurity risks to society p.13-17 |
| **Anti-corruption** | | |
| GRI 205: Anti-corruption 2016 | 205-2 Communication and training about anti-corruption policies and procedures | Anti-corruption Policy<br>2021 Sustainability Report / Business ethics p.31-33 |
| **Energy** | | |
| GRI 302: Energy 2016 | 302-1 Energy consumption within the organization<br>302-3 Energy intensity<br>302-4 Reduction of energy consumption<br>302-5 Reductions in energy requirements of products and services | 2021 Sustainability Report / Performance data p.37<br>2021 Sustainability Report / Performance data p.37<br>2021 Sustainability Report / Performance data p.37<br>2021 Sustainability Report / Product environmental impacts p.21<br>2021 Sustainability Report / Performance data p.37 |
| **Emissions** | | |
| GRI 305: Emissions 2016 | 305-1 Direct (Scope 1) GHG emissions<br>305-2 Energy indirect (Scope 2) GHG emissions<br>305-3 Other indirect (Scope 3) GHG emissions<br>305-4 GHG emissions intensity<br>305-5 Reduction of GHG emissions | 2021 Sustainability Report / Performance data p.37 |
| **Waste** | | |
| GRI 306: Waste 2020 | 306-2 Management of significant waste-related impacts | 2021 Sustainability Report / Product environmental impacts p.21 |

| | | |
|---|---|---|
| **Employment** | | |
| GRI 401: Employment 2016 | 401-1 New employee hires and employee turnover | 2021 Sustainability Report / Performance data p.39 |
| **Training and education** | | |
| GRI 404: Training and education 2016 | 404-1 Average hours of training per year per employee | 7.46 hours per employee.<br>2021 was the first year this data was collected, and it only encompasses cybersecurity training. |
| | 404-2 Programs for upgrading employee skills and transition assistance programs | 2021 Sustainability Report / Cybersecurity skills gap p.28-30 |
| **Diversity and equal opportunity** | | |
| GRI 405: Diversity and equal opportunity 2016 | 405-1 Diversity of governance bodies and employees | 2021 Sustainability Report / Performance data p.40<br>2022 Proxy Statement p.15-16 |
| **Supplier social assessment** | | |
| GRI 414: Supplier social assessment 2016 | 414-1 New suppliers that were screened using social criteria | 2021 Sustainability Report / Performance data p.41 |
| **Customer privacy** | | |
| GRI 418: Customer privacy 2016 | 418-1 Substantiated complaints concerning breaches of customer privacy and losses of customer data | Fortinet did not experience any personal data incidents that required reporting to global data protection authorities during fiscal 2021.<br>In addition, there were no personal data protection incidents causing exposure to high risk or material harm during this period. |

# 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,<br>(2) percentage grid electricity,<br>(3) percentage renewable<br>Unit: GJ, percentage | **TC-SI-130a.1** | 2021 Sustainability Report / Performance data p.37 |
| **Environmental footprint of hardware infrastructure** | Discussion of the integration of environmental considerations into strategic planning for data center needs | **TC-SI-130a.3** | 2021 Sustainability Report / Product environmental impacts p.21<br>2021 Sustainability Report / Environmental management and climate change p.22-23 |
| **Data privacy & freedom of expression** | Description of policies and practices relating to behavioral advertising and user privacy | **TC-SI-220a.1** | Privacy Policy |

| | | | |
|---|---|---|---|
| **Data privacy & freedom of expression** | Number of users whose information is used for secondary purposes | **TC-SI-220a.2** | None in which the secondary purposes were unrelated to the primary purpose or purposes described in the privacy policy. Encompasses customer contacts data; marketing contacts data; HR personal data.<br>Privacy Policy |
| **Data security** | (1) number of data breaches,<br>(2) percentage involving personally identifiable information (PII),<br>(3) number of users affected | **TC-SI-230a.1** | Fortinet did not experience any personal data incidents that required reporting to global data protection authorities during fiscal 2021.<br>In addition, there were no personal data protection incidents causing exposure to high risk or materialharm during this period.<br>No breach in which PII was subject to the data breach that required notification. |
| **Data security** | Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards | **TC-SI-230a.2** | 2021 Sustainability Report / Information security and privacy p.18-19<br>**SOC2 Certification** for key cloud delivered products.<br>**ISO 27001 Certification**<br>Fortinet PSIRT Policy based on recognized industry standards including ISO 29147 (Vulnerability Disclosure) and ISO 30111 (Vulnerability Handling).<br>For product compliance, Fortinet is currently auditing compliance to the controls within the following standards:<br>NIST ST.SP.800-53<br>NIST ST.SP.800-160<br>NIST ST.SP.800-218<br>**Federal Information Processing Standard (FIPS):**<br>FIPS 140-2 Level 1 & 2 (FOS 6.2)<br>FIPS 140-2 Level 2 (FSA 3.1)<br>FIPS 140-2 Level 2 (WLM 8.5)<br>FIPS 140-2 Level 2 (FPX 1.0)<br>FIPS 140-2 Level 1 & 2 (FAZ 5.2)<br>FIPS 140-2 Level 1 & 2 (FMG 5.2)<br>FIPS 140-2 Level 1 & 2 (FCT 5.0)<br>FIPS 140-2 Level 1 & 2 (FML 6.0)<br>FIPS 140-2 Level 1 & 2 (FWB 5.6) |

| | | | |
|---|---|---|---|
| | | | **Network Device Collaborative Protection Profile (NDcPP):**<br>NDcPP + FWcPP + IPS +VPN (FOS 6.2)<br>CC EAL4+ (FOS 6.2)<br>NDcPP (FPX 1.0)<br>NDcPP (FMG 5.2)<br>NDcPP (FAZ 5.2)<br>NDcPP (FML 6.0)<br>NDcPP (FWB 5.2) |
| **Recruiting & managing a global, diverse & skilled workforce** | Percentage of gender and racial/ethnic group representation for:<br>(1) management,<br>(2) technical staff, and<br>(3) all other employees | **TC-SI-330a.3/ TC-HW-330a.1** | 2021 Sustainability Report / Performance data p.40 |
| **Managing systemic risks from technology disruptions** | Description of business continuity risks related to disruptions of operations | **TC-SI-550a.2** | 2021 Sustainability Report / Cybersecurity risks to society p.13-17 |

Verification Statement - Fortinet

# 2019 – 2021 Greenhouse Gas Emissions Inventory

RUBY CANYON ENVIRONMENTAL
743 Horizon Court, Suite 385 - Grand Junction, CO 81506

**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 years (CY) 2019 – 2021. The inventory included emissions of CO2, CH4, and N2O from direct, Scope 1 sources (stationary and mobile fuel 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 PFC, SF6, or NF3 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.

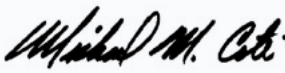
**Organizational Boundaries:**
Fortinet consolidated the emissions reported in the GHG Inventory according to the operational control approach.

**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
- Is not prepared in accordance with the criteria listed above.

**Signatures :**

**Garrett Heidrick, Lead Verifier**
**Date: June 1, 2022**



**Michael Coté, Independent Peer Reviewer**
**Date: June 1, 2022**

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

www.fortinet.com



## Forward-Looking information

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