FORTINET

2022 Cybersecurity Skills Gap

Global Research Report

Contents

The impact of the cybersecurity skills gap

New cyber research on key concerns, recruitment, diversity, and security awareness

INTRODUCTION

Is the cybersecurity workforce growing fast enough to keep up with new threats?

During the last two years, IT teams were forced to rapidly adapt to remote and hybrid work models. While the effort was challenging, the ability to adapt was a safeguard for most organizations.

Unfortunately, increases in remote and hybrid work models resulted in the expansion of the threat landscape. IT teams had to act quickly to deal with an increasingly harsh reality.

"Cybercriminals are developing attacks faster than ever. They continue to exploit the expanding attack surface of hybrid workers and IT. And they're using advanced persistent cybercrime strategies that are more destructive and less predictable than those in the past."

—Derek Manky, Chief Security Strategist & VP Global Threat Intelligence, FortiGuard Labs

The sudden expansion of the corporate network, where millions of employees were logging in from their unsecured home offices, led to significant spikes in malicious cyber activity. In 2021, the Fortinet Global Threat Landscape Report revealed a tenfold increase in ransomware attacks alone.

According to a new Fortinet-sponsored survey, it's clear that many of the challenges organizations face in combating cybercrime are directly related to a lack of qualified cybersecurity professionals.

[1]Global Threat Landscape Report 2021, *Fortinet* | Fortinet Blog

Worldwide, 80% of organizations suffered one or more breaches that they could attribute to a lack of cybersecurity skills and/or awareness.

Here are a few examples:

The survey shows that 64% of organizations experienced breaches that resulted in lost revenue and/or cost them fines during the past year. A staggering 38% of organizations reported breaches that cost them more than a million dollars (USD).

A key factor is that organizations struggle to find and retain certified cybersecurity people. Global leaders indicate that:

- 60% struggle to recruit cybersecurity talent
- 52% struggle to retain qualified people
- 67% agree that the shortage of qualified cybersecurity candidates creates additional risks for their organizations

They're not wrong.

Organizations need qualified cybersecurity professionals now more than ever, which is why 76% of organizations indicate that their board of directors now recommends increases in IT and cybersecurity headcount.

In this report, we analyze the results from our survey to explore five central themes about why the current cybersecurity skills gap matters, and how organizations are attempting to fill it.

EXECUTIVE SUMMARY

How the cybersecurity workforce is growing

Cybersecurity affects every organization

80% of organizations experienced one or more breaches during the last 12 months.

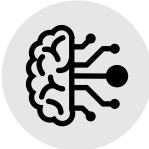
19% confirm five or more breaches.

Almost 40% suffered breaches that cost more than a million dollars USD to remediate.

Recruitment and retention of talent is a problem

67% of respondents agree that the skills shortage creates additional cyber risks for their organization. As such, 76% of organizations now have a board of directors who explicitly recommend increases in IT and cybersecurity headcount.

However, 60% of organizations struggle to recruit cybersecurity talent and 52% struggle to retain it.



Organizations are looking for individuals with certified skills

95% of decision-makers believe technology-focused certifications positively impact both their role and their team. As such, 81% of leaders prefer to hire people with certifications.

However, 78% indicate it's hard to find certified people, which is why 91% of organizations are willing to pay for the training and certification of their employees.

Organizations are looking for more diversity

7 out of 10 leaders worldwide say hiring women and new graduates are among their top three challenges.

61% say hiring minorities is also a top three challenge.

Despite the challenges, or perhaps because of it, 3 out of 4 organizations implemented formal processes to hire more women, and 9 out of 10 actively engaged women and new graduates during the last three years.

Raising cybersecurity awareness remains a key challenge

87% of organizations implemented a training program to increase cyber awareness. However, 52% of leaders continue to believe their employees still lack the necessary knowledge. This raises the question of the effectiveness of these programs.

66% of organizations that don't have a program intend to set one up.

About the research

The survey was conducted among 1223 IT and cybersecurity decision-makers located in:

Argentina
Australia
Brazil
Canada
Colombia
France
Germany
Hong Kong
India
Indonesia
Israel
Italy
Japan
Malaysia
Mexico
The Netherlands
People's Republic of China
The Philippines
New Zealand
Singapore
South Africa
South Korea
Spain
Sweden
Taiwan
Thailand
United Arab Emirates
United Kingdom
United States of America

Respondents came from organizations of various sizes:

100-499 employees: **22%**

500-999 employees: **24%**

1,000-2,499 employees: **23%**

2,500-4,999 employees: **16%**

5,000+ employees: **15%**

Respondents came from a range of industries. The best represented were technology (28%), manufacturing (12%), and financial services (10%).

In addition:

12% of respondents are owners

34% hold C-level executive positions

6% are vice presidents

14% are department heads

34% are directors

64% are male

35% are female

Cybersecurity affects every organization

When organizations don't have the qualified cybersecurity talent they need, they become more vulnerable to attacks. The data bears this out, with two-thirds of leaders (67%) worldwide expressing concern about the additional risks they face due to the skills gap within their organization.

Leaders on every continent share this concern

Leaders from France (81%), North America (77%), and Hong Kong (77%) show the highest level of concern and believe that skills shortages pose additional risks to their organization.

Whereas only half of the leaders from Indonesia (50%), Italy (50%), and Israel (47%) indicate concern.

Globally, 88% of organizations that have a board of directors report that their board now asks questions specifically about cybersecurity.

Cybersecurity is now a board-level priority

Given the increasing and tangible costs of breaches, cybersecurity is becoming a board-level priority. Globally, 88% of organizations that have a board of directors report that their board now asks questions specifically about cybersecurity.

As a result of these discussions, 76% of boards of directors globally are suggesting an increased headcount for IT and cybersecurity.

For example,

- USA (90%) organizations discuss cybersecurity with their board, and 77% of those boards recommend an increase in headcount in IT and security.
- Indian (100%) and Chinese (96%) organizations discuss cybersecurity with their boards. Given the high number of breaches in these countries, it is not surprising that 92% of Indian boards and 100% of Chinese boards recommend an increase in headcount in IT and security.

Recruitment and retention of talent is a problem

Hiring challenges

It is difficult to find and recruit qualified cybersecurity professionals. Globally, 60% of leaders admit their organizations struggle with recruitment.

Further analysis shows that it is a far bigger problem for some than for others:

- Brazil (97%), France (77%), and North America (69%) struggle with hiring.
- People's Republic of China (33%) and Spain (29%) report fewer issues.

This may be due to the number of qualified cybersecurity professionals available in these regions. It's likely also influenced by the maturity of the cybersecurity industry within each region.

Retention: the critical challenge

When there's a lack of qualified professionals in the pipeline, there's only so many things that organizations can do to grow their workforce. For companies to reliably protect themselves in the long run, the most important thing they can do is focus on retaining their best people.

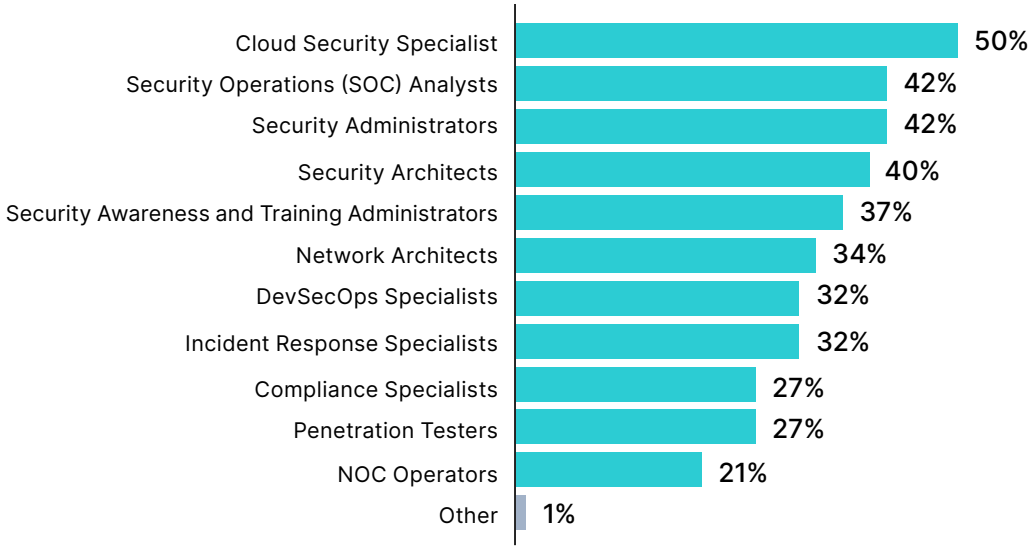
Globally, 52% of leaders admit their organization struggles to retain cybersecurity talent. However, there are significant regional differences:

- Thailand (91%), Brazil (84%), and Israel (80%) report significant issues with retention.
- Italy (30%), Mexico (28%), and People's Republic of China (25%) report fewer issues.

What is the most significant skills gap?

A key challenge for organizations seeking cybersecurity talent is that they need to hire people for a broad range of security and IT network-related roles and specializations.

What roles are organizations looking for?

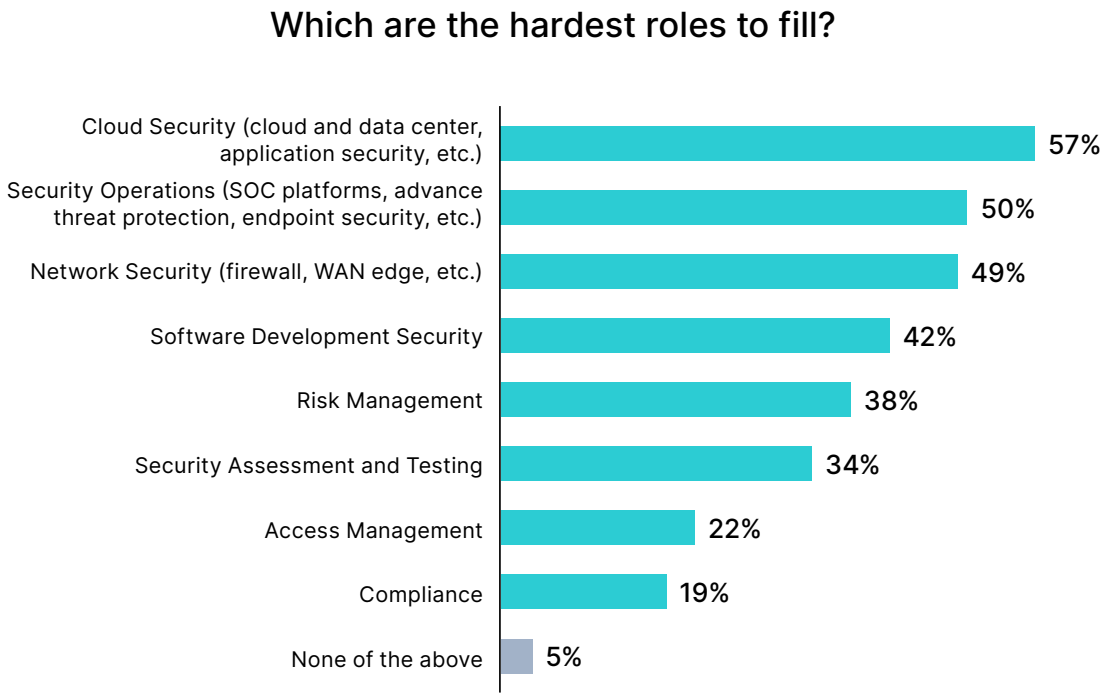


The challenge is finding the right people

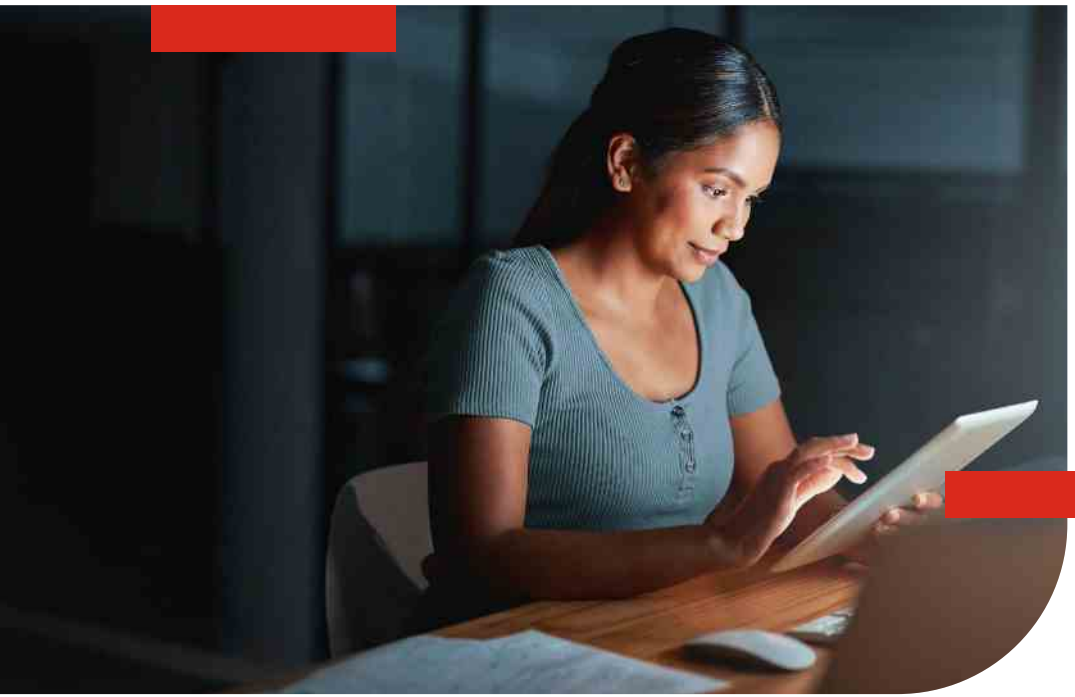
Cloud security specialists and security operations (SOC) analysts remain among the most sought-after roles in cybersecurity, followed closely by security administrators and architects. But organizations aren't just looking to ramp up hires arbitrarily. They're deliberately trying to build teams of specialized talent who are equipped to handle an increasingly complex threat landscape.

Globally, 50% of organizations seek cloud security specialists, a priority that's likely informed by how rapidly companies moved their operations to the cloud during the pandemic.

The challenge is finding the right people.



Globally, cloud security (57%) and security operations (50%) are the most challenging areas to recruit into, followed by technical roles in network and software development–related security.



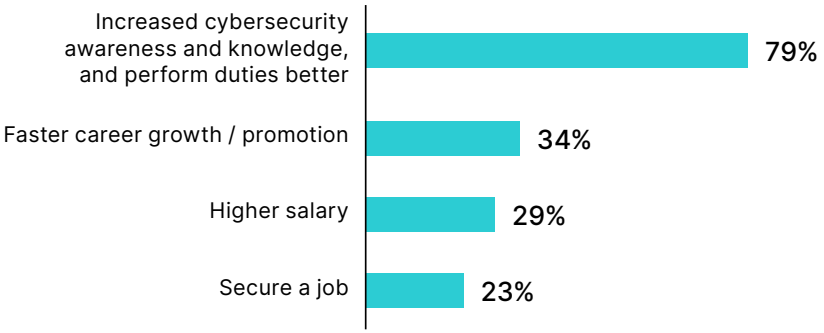
In North America, it was slightly higher, with 63% and 57% of leaders respectively listing cloud security and security operations as the two most challenging roles to fill. The greatest struggles came from Thailand (87%), People's Republic of China (79%), and Indonesia (73%).

Organizations are looking for individuals with certified skills

Central to the challenge of recruiting and retaining cybersecurity talent is the importance of certification. Certified professionals are universally sought after. Globally, 91% of organizations claim they are willing to pay for an employee to achieve a cybersecurity certification.

In India and People's Republic of China, certifications are especially sought after with 100% of leaders looking for certified people when hiring. In North America, 85% of organizations are reporting a preference to hire certified people.

What impacts have certifications made?



It is no surprise that 81% look for people with certifications when hiring.

The preference to hire certified people may be because organization leaders followed that same path themselves:

- 86% of decision-makers report having earned technology-focused certifications.
- 88% report having other people with certifications on their team.

For companies with fewer than 499 employees, 78% of decision-makers are certified in some way, while at companies with more than 1,000 employees, 89% of leaders have certifications. It is no surprise that 81% look for people with certifications when hiring.

However, finding certified professionals is not the same for each region.

For example:

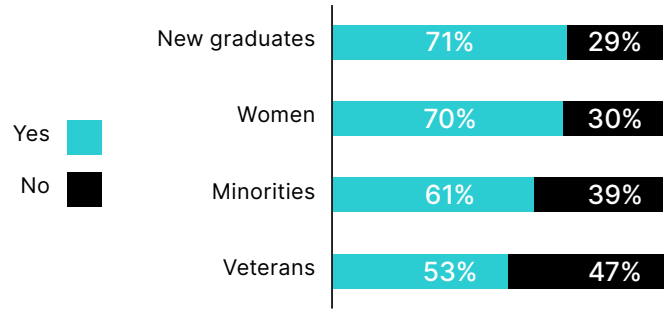
- Argentine (95%), Japanese (88%), and Brazilian (87%) organizations report having difficulty finding certified talent.
- Whereas Australian (62%) and Hong Kong (68%) leaders have fewer difficulties.

Organizations are looking for more diversity

The challenge isn't just hiring more people, but also building more capable and more diverse teams. While enterprises need qualified talent for a range of different roles, 89% of global companies also have explicit diversity goals as part of their hiring plan.

Globally, 70% of IT managers see the recruitment of women and new graduates as a top three challenge. Organizations in Latin America (93%) and North America (90%) are more likely to have diversity goals in place, likely as a result of bigger struggles recruiting from these populations.

Is hiring from these populations one of your organization's top three challenges?



Hiring a diverse team is more than just intent. Organizations are actively and strategically changing their hiring structures to promote more diverse talent. For example, 75% of organizations report having formal structures to recruit more women, and 89% have intentionally set diversity goals when hiring new graduates.

While fewer organizations report having hiring processes designed to attract more minorities and veterans, they are still present in most organizations:

- 59% of companies have structures in place to hire minorities, and 51% for hiring more veterans.
- 64% and 52% of organizations in North America have put structures in place to hire minorities and veterans respectively, while in EMEA, 56% and 48% have these structures in place.

There are challenges

New graduates are the easiest to hire, with only 24% of decision-makers reporting that they've found it difficult. By comparison, 33%, so exactly one-third, of North American organizations say they have difficulties hiring minorities, which is considerably lower than 43% of organizations in Asia Pacific.

However, 45% of organizations report that it's challenging to find qualified veterans, with 18% going so far as to say it's very difficult.

Decision-makers also feel that hiring individuals from these groups is just as difficult now as before the pandemic, with some noteworthy distinctions. For example, more women seem to be joining the ranks of the cybersecurity workforce, with 24% of organizations reporting they've found it easier to hire women since the pandemic.

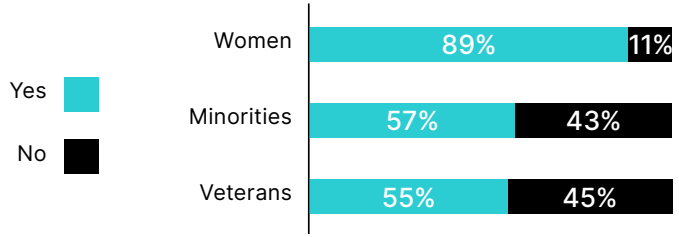
Nonetheless, companies are continuing their efforts to hire more diverse teams

Over the last three years:

- 88% of organizations report having actively hired more women
- 87% actively seek to meet diversity goals when hiring new graduates
- 67% have actively hired minorities
- 53% have deliberately sought out veterans

Most importantly, most of these companies report having members of these groups in their C-suite team.

Population in C-suite team



In addition:

- 89% of executive teams include women
- 57% include minorities
- 55% have veterans on their executive teams
- 72% of women performing these roles have been doing so for more than five years, with 26% doing so for more than 10
- 80% of veterans have been in C-suite roles for more than five years
- 18% of veterans in C-suite roles only began in the last five years

Unsurprisingly, the larger an organization is, the likelier it is to have women, minorities, and veterans represented in the C-suite.

24% of organizations report they've found it easier to hire women since the pandemic.

Raising cybersecurity awareness remains a key challenge

Even though the recruitment, retention, and certification of a cybersecurity team is vital, companies cannot realistically protect themselves until they also raise the cyber awareness of all employees. That requires ensuring that all employees, at all levels and all roles within the organization, have the knowledge and awareness to protect themselves and their organization's data. Until they do, breaches will always be likely.

Asian (56%) leaders feel employees lack the necessary awareness. Worryingly, federal governments (69%) and state-level government organizations (61%) feel the same way. Interestingly, local and state government organizations (28%) and media organizations (25%) are the most likely to not have cybersecurity awareness programs in place.

On the other hand, Sweden (63%) and South Africa (60%) believe their employees do have the necessary level of cybersecurity awareness.

The value of awareness programs

Interestingly, 87% of organizations implemented a training program to increase cyber awareness. However, 52% of leaders continue to believe their employees still lack the necessary knowledge. This raises the question of the effectiveness of programs currently in place.

For those that don't have a program in place, 66% report they are currently looking for a program that would suit their needs.

CONCLUSION

The power of people

Cybersecurity can sometimes feel like a purely technological domain. But when you look past the technology that organizations rely on, cybersecurity is all about how well your employees work together to protect the organization.

The challenge for organizations is multi-faceted

Organizations need to:

- find and recruit people who are qualified, skilled, and certified for a variety of network- and security-related roles
- expand their search and focus on diversity to create the specialized teams they're aiming to build
- improve their ability to retain people by making it possible for employees to improve their skills, get certified, and continue their professional development
- provide all employees, both technical and non-technical, with cybersecurity awareness training so they can develop critical cyber-hygiene skills

Fortunately, organizations are making deliberate efforts to improve on all these fronts. However, it is imperative to remember that the cyber battle isn't won on any one front. Cybersecurity requires an entire system of people and technology working together to protect an organization.

That starts with people who are empowered, qualified, and certified to protect the organization.

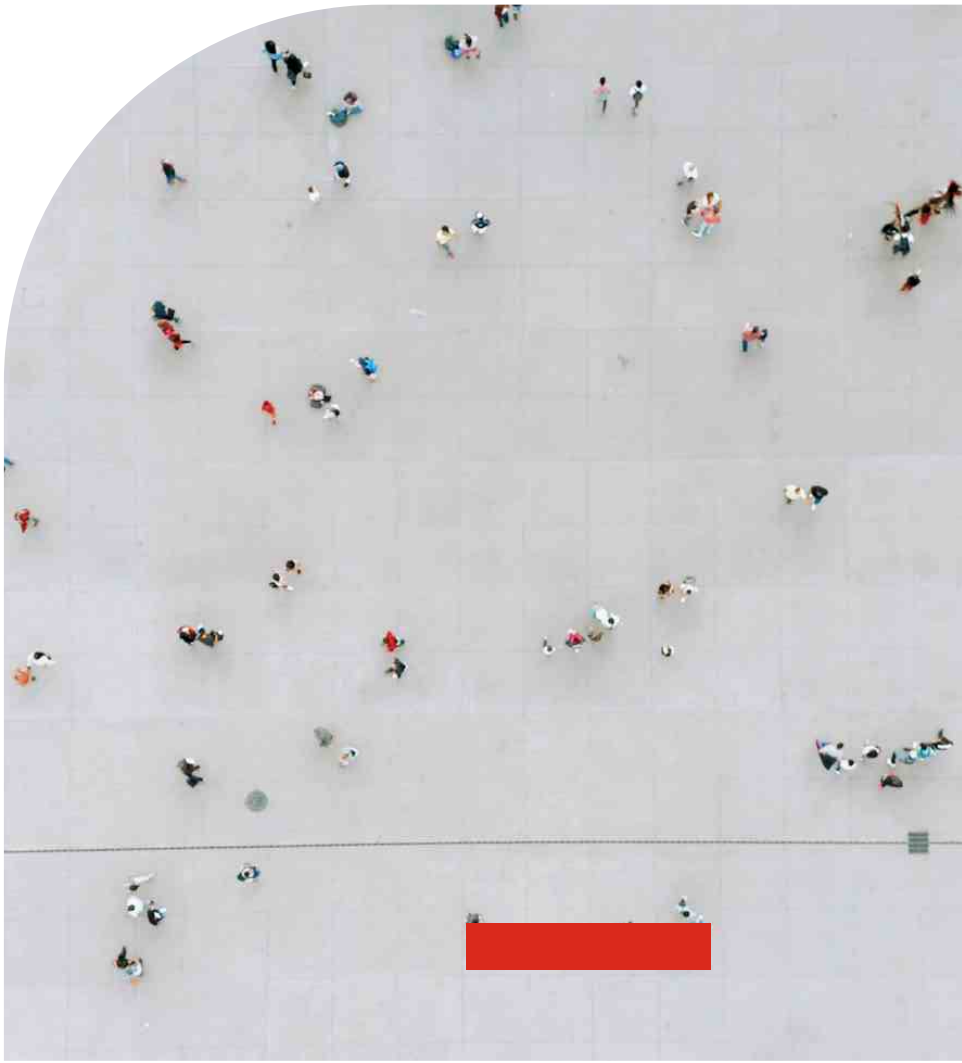
About Fortinet

Fortinet (NASDAQ: FTNT) makes possible a digital world that we can always trust through its mission to protect people, devices, and data everywhere.

The world's largest enterprises, service providers, and government organizations choose Fortinet to securely accelerate their digital journey.

The Fortinet Security Fabric platform delivers broad, integrated, and automated protections across the entire digital attack surface, securing critical devices, data, applications, and connections from the data center to the cloud to the home office. Ranking #1 in the most security appliances shipped worldwide, more than 550,000 customers trust Fortinet to protect their businesses.

The Fortinet Training Institute, an initiative of Fortinet's Training Advancement Agenda (TAA), provides one of the largest and broadest training programs in the industry to make cyber training and new career opportunities available to everyone. Learn more at https://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.



FORTINET

www.fortinet.com

April 2022