REPORT

2023 Work-from-Anywhere Global Study

The Hybrid Workforce Is Here, There, and Everywhere for Good

TABLE OF CONTENTS

Executive Summary

Fortinet commissioned a global research study to get a better understanding of companies' current work-from-anywhere (WFA) policies and their cybersecurity issues. Five hundred seventy organizations from around the world with at least 100 employees were surveyed in early January 2023.

The survey questions were constructed to uncover the level of commitment organizations have in protecting their networks, data, and remote employees—and what specific areas of cybersecurity concerns have the highest priority. Additional survey objectives included quantifying the number of security breaches that have occurred due to WFA vulnerabilities and identifying the best ways of securing them.

Another key goal of the research study was to get visibility into the current security solutions that organizations have deployed in response to the massive increase in the number of WFA employees. Also of interest was knowing how receptive organizations are to working with multiple security vendors. The final key purpose of the survey was to get a better idea of cybersecurity budget priorities.

The survey results provided three primary takeaways: 1) WFA is clearly here to stay; 2) organizations consider the insecurity of home networks a major concern; and 3) companies are planning significant spending on cybersecurity—but there is no consensus on which solutions they are prioritizing.

WFA Is Here, There, and Everywhere for Good

Propelled by the 2020 global pandemic, the dispersion of people from their workplaces led to the explosive expansion of the hybrid workforce and the need for updating existing WFA policies and creating new ones. The survey this report is based on was conducted almost exactly three years after that major global event occurred. Our aim was to dig deep into the current state of affairs of organizations that had to respond to the many significant cybersecurity challenges since then.

What does your company's remote work policy look like currently? (n=570)

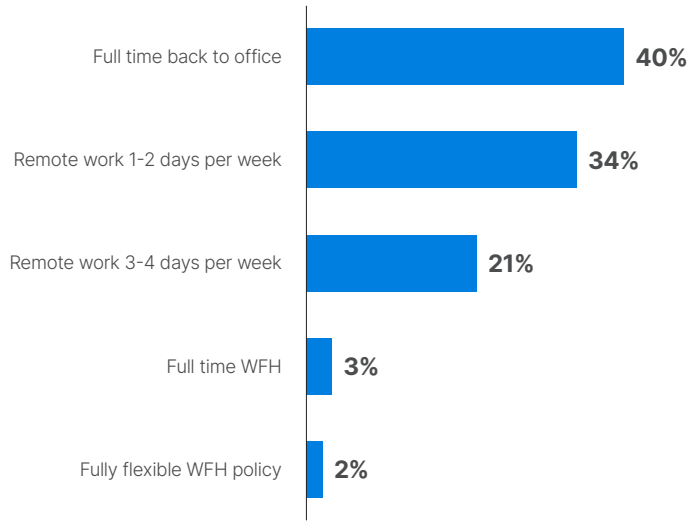

Figure 1: Current remote work policies

The responses to one of the primary survey questions—*What does your company's remote work policy look like currently?*—reveal that 60% of the 570 companies in the study are still accommodating employees working from home or other off-site locations, with 55% of companies embracing a hybrid work strategy for their employees. Unsurprisingly, hospitality and healthcare are the industries most likely to go back to the office full-time based on the nature of their job function.

Even with several industries that have the fundamental requirement to be on-site and in-person to operate effectively, we conclude that WFA is here to stay. Prime example: In the Asia-Pacific-Japan (APJ) region—the most restrictive for hybrid workers—more than 47% of the organizations surveyed are still accommodating WFA employees.

What does your company's remote work policy look like currently? (By region: NA=140; EMEA=130; APJ=230; LATAM=70)

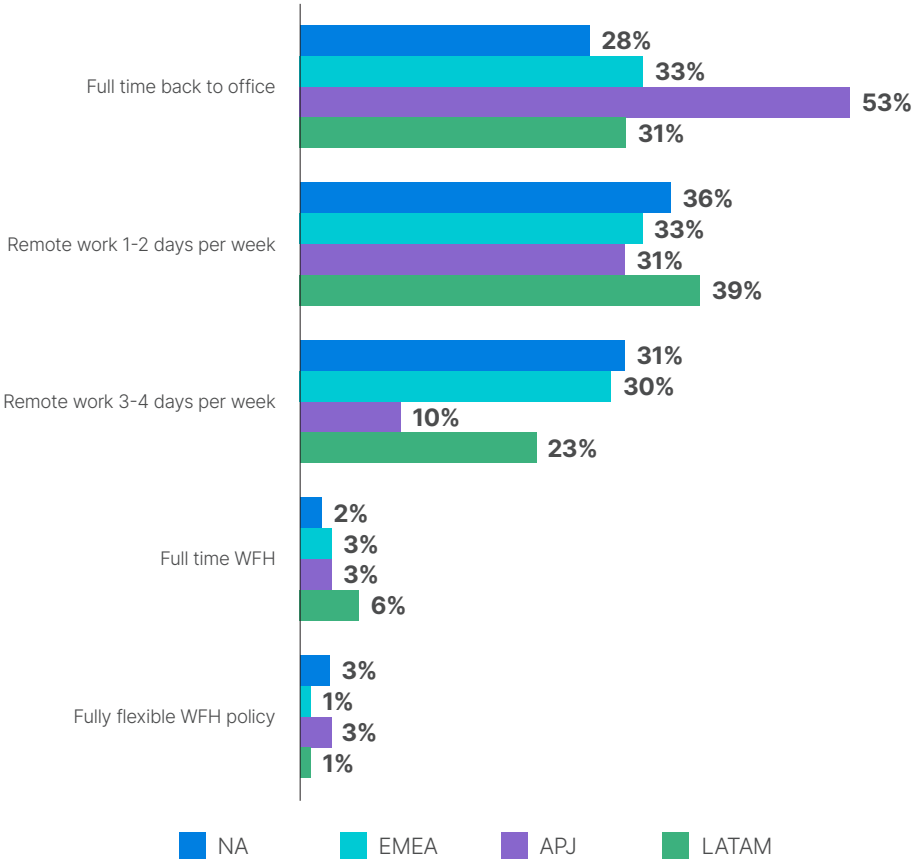

Figure 2: Current remote work policies by region

The survey reveals a third of employees expect to stay working off-site 80% of the time, while more than half expect to continue working off-site 51-80% of the time.

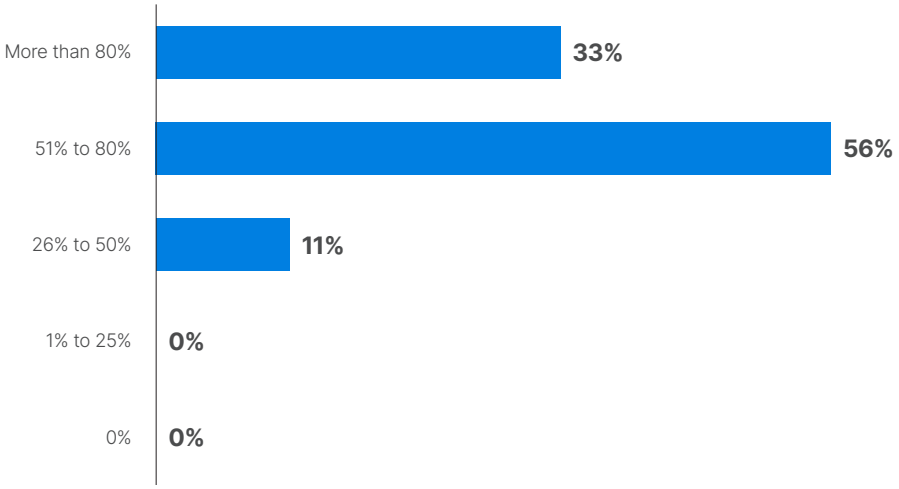

Figure 3: % Employees staying full-time remote

Do some jobs WFA more than others? (n=570)

The survey also reveals that WFA participation does not appear to be limited by job function or title.

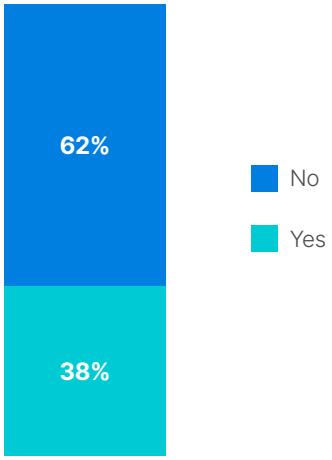

Figure 4: Some job functions WFA more than others

Security Concerns Still the Most Critical Hurdle for WFA Adoption

There are several other data points from the survey that most cybersecurity analysts would expect to find. Organizations that required employees to return to the office as soon as pandemic fears waned are the most concerned about data breaches due to remote workers.

Security Breaches Due to WFA

Perhaps the most startling finding from the survey is learning that nearly two-thirds of the companies have experienced a data breach due to their WFA vulnerabilities.

Did you experience a security breach during the past two to three years that could be at least partially attributed to an employee working remotely?

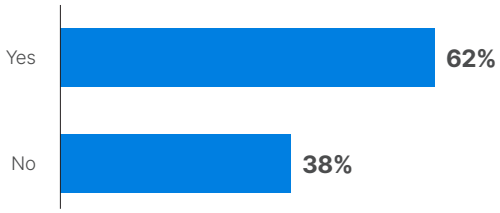

Figure 5: Security breach from WFA

Organizations cite a lack of cybersecurity training as their top concern for hybrid workers. The second top concern is how best to extend corporate security to home offices and remote locations. And the third top concern (which is also outlined in the Fortinet 2021 Ransomware Report) is that organizations are still unsure about protecting themselves from ransomware attacks.

Rank the top five most significant challenges for your organization in preventing cyberattacks in relation to WFA, where 1 is the most challenging. (n=570)

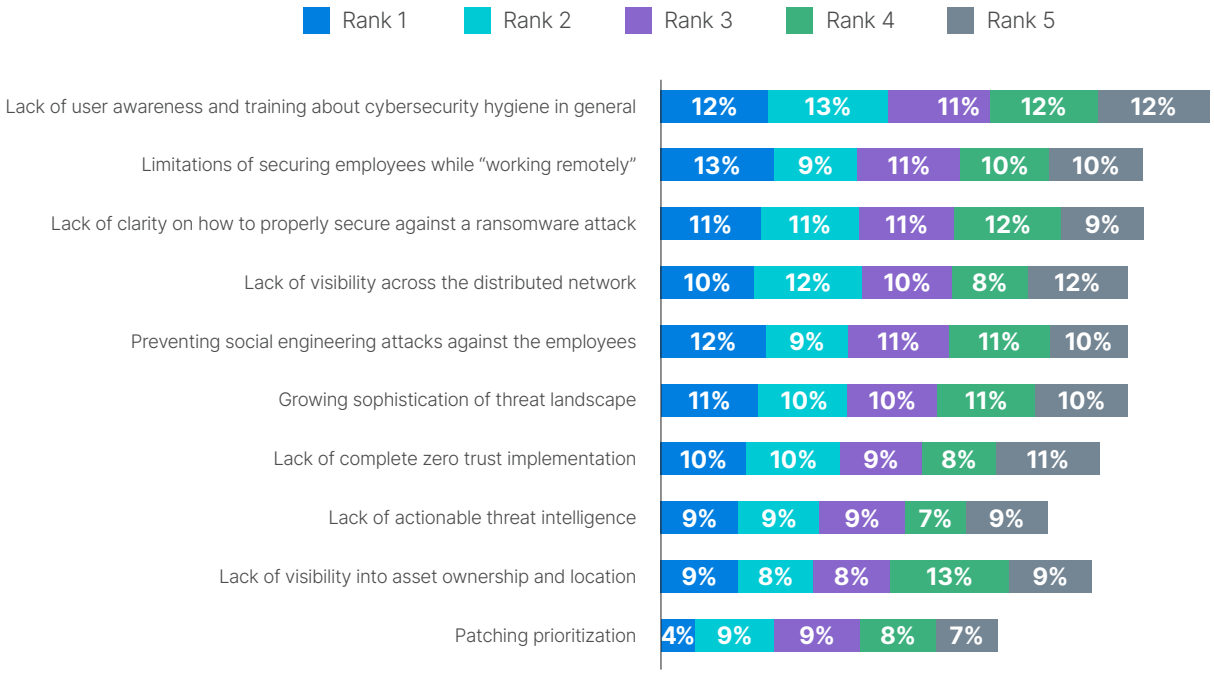

Figure 6: Most significant challenges preventing cyber attacks

Also, a prominent concern is the lack of visibility across distributed networks that include employee homes, branch offices, and other off-site locations. Most of the rest of the cybersecurity concerns are related to fundamental security issues, such as lacking zero-trust access (ZTA), actionable threat intelligence, visibility into asset ownership, and an effective patching protocol—combined with the growing sophistication of the threat landscape. In short, the challenges to prevent cyberattacks due to WFA are many and diverse.

The Biggest WFA Security Risks

The insecurity of home networks, employees using company laptops for personal use, and compromised family devices infecting an employee's work PC are considered by most organizations to be their top WFA security risks. These all pointed to vulnerabilities of home networks and the lateral movement for malware to enter the corporate network. This is a big issue largely due to the inability to extend corporate security to a non-owned environment. Other risks include failure to follow security protocols when not in the office and unknown users sharing the home network.

What organizations want is the ability to establish consistent policies across all locations, including those where workers connect to the network remotely. The challenge is finding vendors that can implement solutions and enforce consistent security protocols on the corporate network and in home offices. This is likely why nearly half (42%) end up using different vendors.

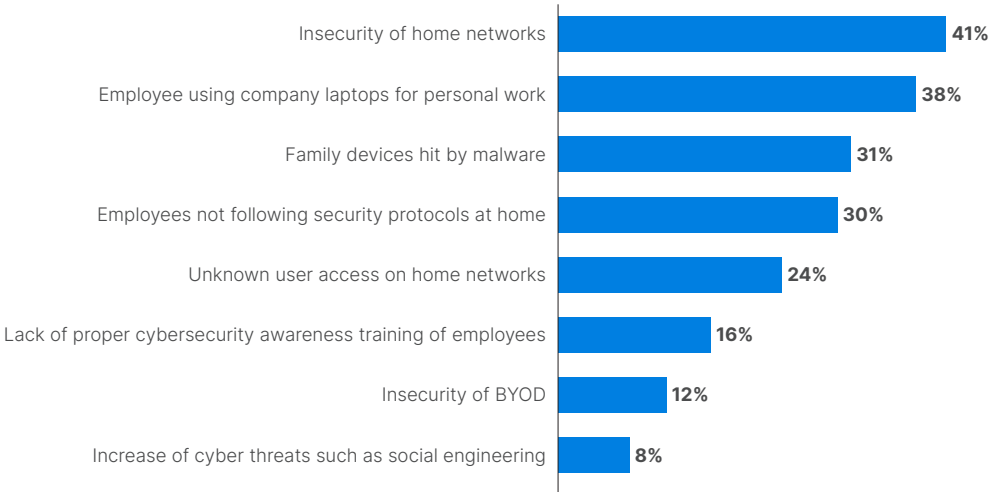

Figure 7: Biggest WFA security risk

Where do you think your two biggest security risks from WFA are coming from? (n=570)

Do you have a consistent security policy across employee homes, HQ offices, and branch offices? (n=570)

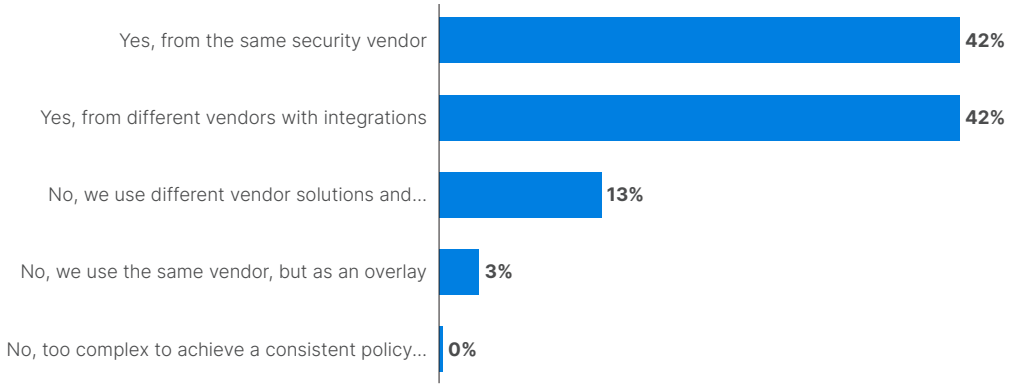

Figure 8: Consistent security policy across locations

Companies place high importance on delivering a consistent security policy across employee homes, HQ, and branch offices.

Did you experience an increase in support calls from WFA employees on access and security issues in the last two years? (n=570)

Support calls regarding access and security issues have increased substantially due to WFA. In fact, according to the survey, 72% of those surveyed saw an increase in WFA support calls in the last two years. Clearly, supporting WFA employees is

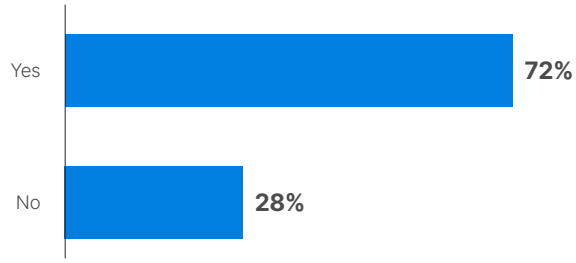

Figure 9: Increase in WFA support calls in last 2 years

consuming too much time and too many resources for an IT team to keep pace. To sustain WFA, thin IT organizations must have better management and support solutions.

Almost 75% of respondents believe that such a solution can help reduce security risks for their businesses. Nearly half (48%) believe that home security only reduces their risk by 50% or less, and another third (36%) believe it can only reduce risk between 50% and 75%. Only 16% of survey respondents believe that a current WFA cybersecurity solution can fix the problem of home network security risks. Those who have experienced a WFA breach are the least confident that such risk can be reduced.

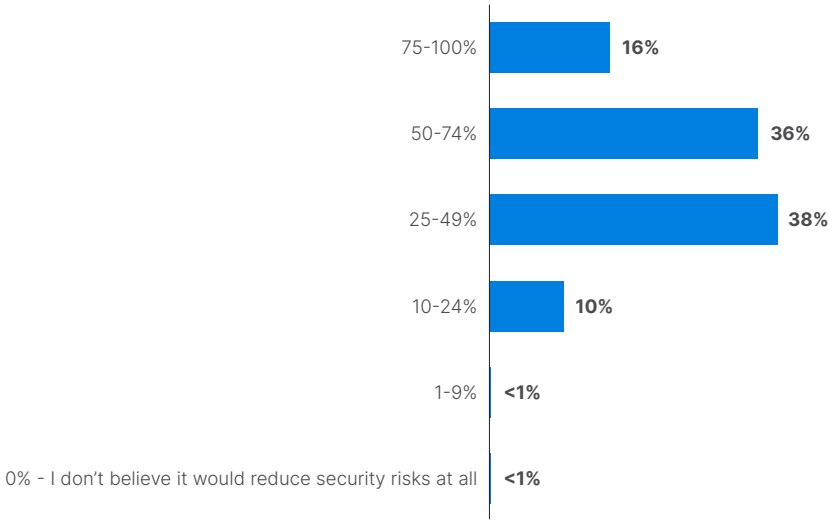

Figure 10: How much home network solutions reduce security risks

At what percentage do you think a business solution specifically designed to protect the home networks of your employees would help reduce security risks to your business? (n=570)

Providing WFA Security

The onus for protecting home offices, according to most survey respondents (71%), falls squarely on the shoulders of both the corporation and service providers. As a result, 94% anticipate an increase in their security budget to accommodate WFA policies, with over a third (37%) expecting an increase of 10% or more.

How are you planning to adjust your security budget in response to supporting your company's long-term WFA policy? (n=570)

Companies have already deployed solutions to address risks to some extent, but planned investments in security solutions are broad—especially for laptop antivirus and VPN. What's more, those who have had a breach tied to WFA are more likely than those who have not to invest in laptop antivirus, VPN, secure access service edge (SASE), SD-WAN, and zero-trust network access (ZTNA).

- **What security solutions do you believe are the most important to secure WFA employees? (Check up to 4 that are most important [n=570])**
- **What security solutions have you deployed to improve your organization's security posture specifically in response to employees working from home? (Check all that apply [n=570])**
- **Thinking about the next 24 months, how has the shift to remote work over the last two years impacted your investment plans? Which of the following areas do you plan to invest in? (n=570)**

	Most important	Already deployed	Plan to invest
Network access control	38%	58%	85%
Antivirus on company laptop	37%	62%	94%
Multifactor authentication (MFA)	35%	59%	77%
Cloud security (e.g. CASB)	31%	57%	85%
Secure access service edge (SASE)	30%	48%	81%
Secure Web Gateway (SWG)	29%	53%	85%
Firewall at employee home	28%	48%	85%
Security service offered by Telco or MSP	24%	42%	78%
VPN	23%	51%	92%
Enterprise Access Point at employee home	22%	46%	82%
SD-WAN	22%	40%	79%
Endpoint detection and response (EDR	18%	52%	82%
Email security	16%	51%	81%
Cybersecurity training/awareness service	7%	29%	80%
Wi-fi router w/ security managed by employer	5%	35%	81%
ZTNA	4%	29%	72%
Extended detection and response (XDR)	4%	38%	79%

Table 1: Areas to invest in

Interestingly, while the top priority for securing remote workers cited is network access control (NAC), with 58% reporting having already deployed such a solution, only 4% list ZTNA as their most important investment despite its ability to limit access to network resources. Ironically, VPN, which provides broad access to the network, is in the top 10 of the most important investments.

When it comes to WFA, many companies are still in the early stages of security implementations. Even though some (58%) already cover the fundamentals, such as NAC deployment. There are still some organizations that haven't used VPN, let alone advanced into ZTNA and other technologies. We still have a long way to go in securing WFA users.

Survey Specifics

The survey was conducted by InMoment, a customer-feedback management company, from January 4, 2023, to January 10, 2023. The survey had 570 respondents from organizations in various industries with 100 or more employees.

Global Reach

Argentina, Australia/New Zealand, Brazil, Canada, Colombia, Denmark, France, Germany, Hong Kong SAR, India, Indonesia, Israel, Italy, Japan, Mainland China, Malaysia, Mexico, Philippines, Poland, Portugal, Singapore, South Africa, South Korea, Spain, Sweden, Taiwan, Thailand, UAE, United Kingdom, the United States, and Vietnam

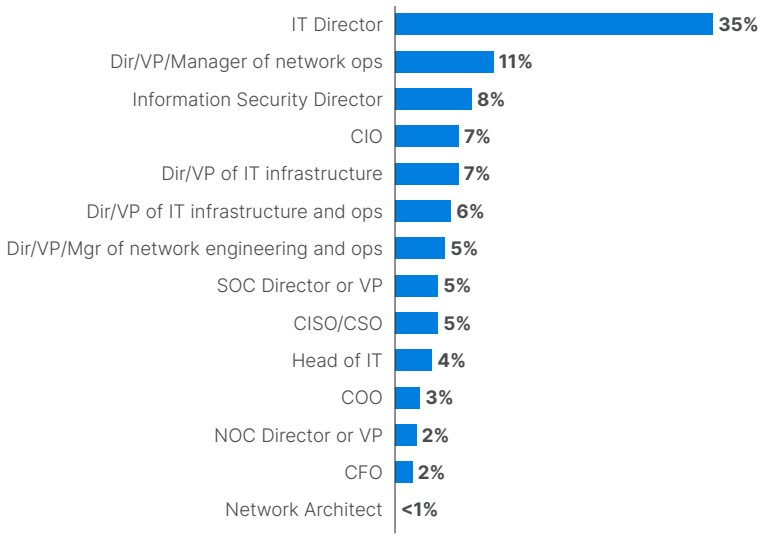

Figure 11: Job title

Respondent Demographics

IT Directors comprise the largest group of respondents, and nearly all are involved in cybersecurity and networking decision-making.

What best describes your title? (n= 570)

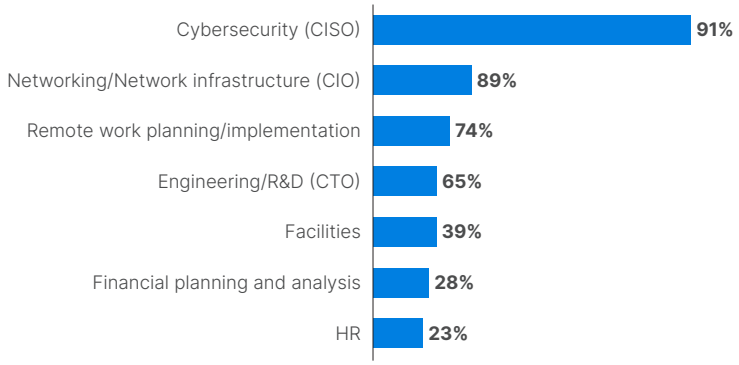

Figure 12: Decision making

The individuals surveyed were involved in purchase or planning decisions in at least remote work planning/implementation, cybersecurity, or networking/network infrastructure.

Indicate if you are involved in purchasing or planning decisions for any of the following areas. (n=570)

Resources

If you think a cybersecurity threat has impacted your organization, get a Fortinet Cyber Threat Assessment.

Learn about Fortinet FortiGuard Labs threat research and intelligence organization and the FortiGuard AI-powered security services portfolio.

March 7, 2023 9:16 AM

2013485-0-0-EN