FORTINET

REPORT

Enterprises Must Adapt to Address Telework Security Challenges

2020 Remote Workforce Cybersecurity Report

Table of Contents

Infographic: Key Findings

Almost 60% of enterprises are planning to spend more than $250,000 on secure telework investments over the next 24 months.

32% of respondents found secure connectivity to be the most challenging aspect of switching to telework.

About three-quarters of participants are planning to make investments in VPN, cloud security, and network access control technologies.

92% expect an increase in budget for telework technologies.

During the shift to telework:

The majority of enterprises reported that transitioning workers was challenging.

Nearly two-thirds of the respondents saw an increase in breach attempts.

34% of those surveyed experienced a breach.

Introduction

The COVID-19 pandemic has changed almost every aspect of the way we live and work. Organizations were required to shift to telework practically overnight as teams around the globe were told to stay home. Sixty-two percent of employed Americans say they have worked from home during the coronavirus crisis, doubling between March 13 and April 2.[1]

Typically, moving an entire workforce from offices with secure IT environments to remote setups with very little cybersecurity would take long-term IT planning and preparation. But that was not an option in 2020, and cyber criminals have been taking advantage of this widespread opportunity.

We decided to investigate how enterprises worldwide handled the sudden change to telework as the norm, and what their plans are for supporting and securing it in the future. A big decision-making factor for IT teams is always budget, so we also asked about unanticipated spending on telework and if other projects were impacted by it.

"Predictably, cyber criminals of all shades—from opportunistic phishers to scheming nation-state actors—found some way to exploit the pandemic for their benefit."
– Fortinet Global Threat Landscape Report, August 2020[2]

Methodology

This report was based on a survey conducted in June 2020. Participants are employed in 17 different countries, representing nearly all industries and the public sector. They are involved in the purchase or planning decision-making for networking, cybersecurity, remote working, financial planning, facilities, and human resources. The most common titles are IT director, CIO, head of IT, network architect, and director/VP/manager of network operations, IT infrastructure, or network engineering and operations.

This study sought to find out how enterprises are going about securing networks, devices, and applications during the sudden switch to telework. We were curious to know how they approached this daunting task, what the main challenges were, and if they are planning further changes in IT security to accommodate ongoing remote work.

We uncovered a number of interesting insights about the current state of telework and what the future might look like, which are shared in this report.

Telework Trends and Security

In this section, we will discuss the results and insights uncovered after examining the survey data.

Insight: Almost All Enterprises Will Invest More in Secure Telework in the Next Two Years

Almost 60% of enterprises are planning to spend more than $250,000 in secure telework investments over the next 24 months due to the pandemic. These investments were unplanned, but securing remote work has become a top priority.

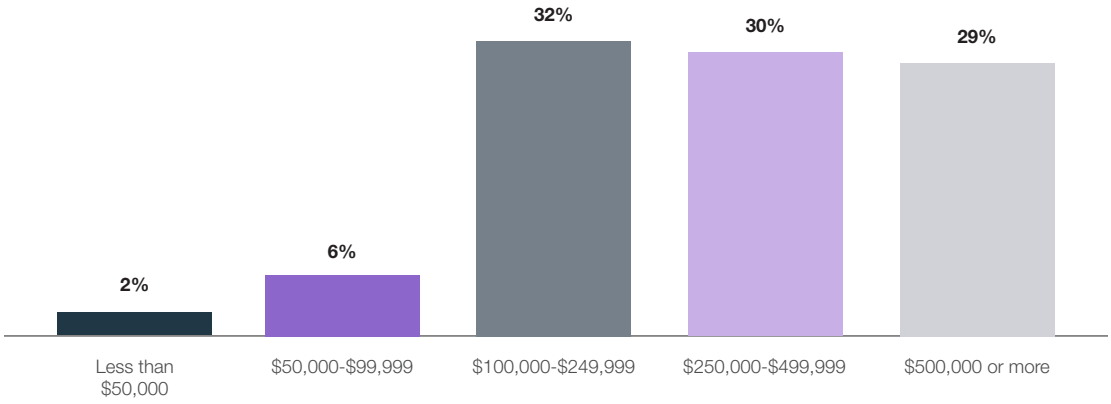

Figure 1: Secure telework investments over the next two years.

At the time of this survey, nearly half of respondents had already invested in their virtual private network (VPN) and cloud security. As the chart below reflects, the top areas respondents are planning to upgrade are:

- Cloud security (58%)
- VPN (55%)
- Network access control (NAC) (55%)
- Skilled IT workers (50%)
- Endpoint detection and response (EDR) (48%)
- Business continuity plan (48%)

The top areas they are planning to make new investments in are:

- Multi-factor authentication (MFA) (30%)
- Secure telephony/unified communications (27%)
- Software-defined wide-area networking (SD-WAN) for the enterprise (26%)
- SD-WAN for the employee's home (26%)
- Segmentation (26%)
- VPN (25%)
- SASE (24%)

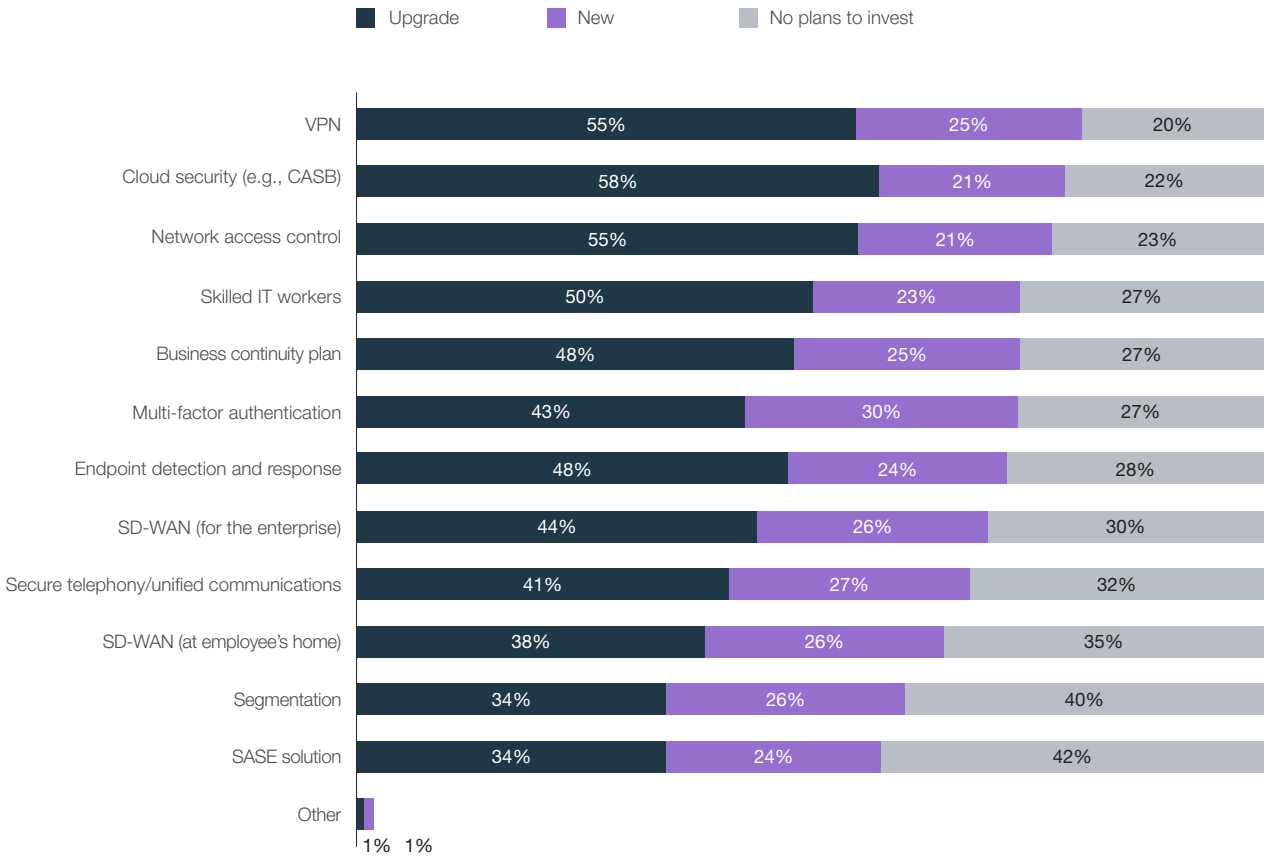

Figure 2: Investment plans due to pandemic.

Insight: Budgets Need to Accommodate Spending on Telework

92% of enterprises expect an increase in their telework budget, while 11% anticipate an increase in their on-premises technology budget. 64% expect essentially no change in their on-premises technology budget.

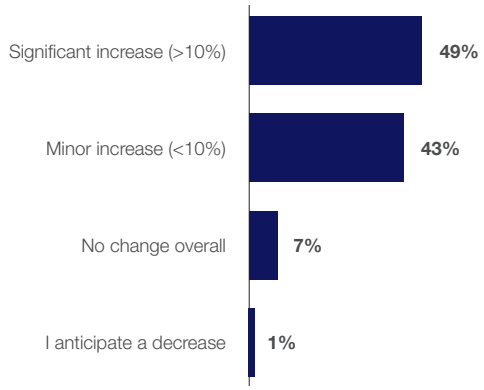

Figure 3: Anticipated telework technology spend.

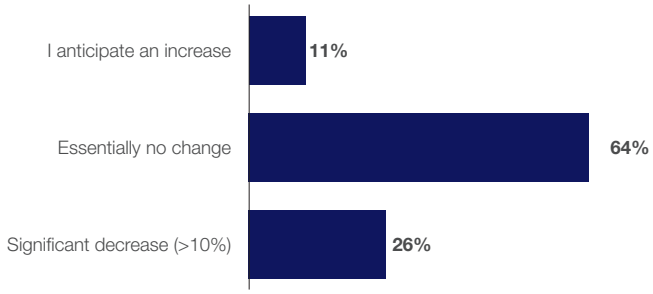

Figure 4: Anticipated on-premises technology spend.

Insight: A Long-term Shift to Telework Is Anticipated

Nearly two-thirds of firms surveyed needed to transition more than half of their workforces to telework. And, they are expecting more of their workforce to continue to work remotely in the future. In fact, 29% of organizations expect more than 50% of employees to continue teleworking after the pandemic.

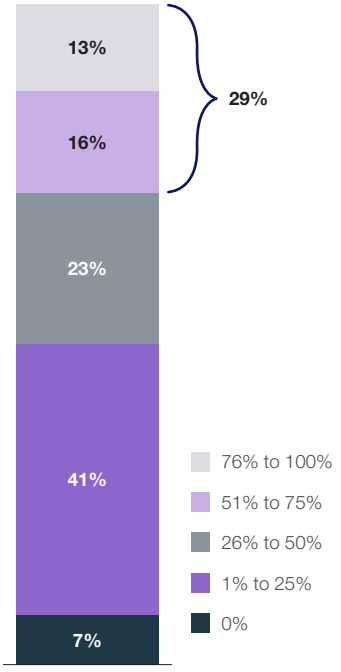

Figure 5: Full-time telework pre-pandemic.

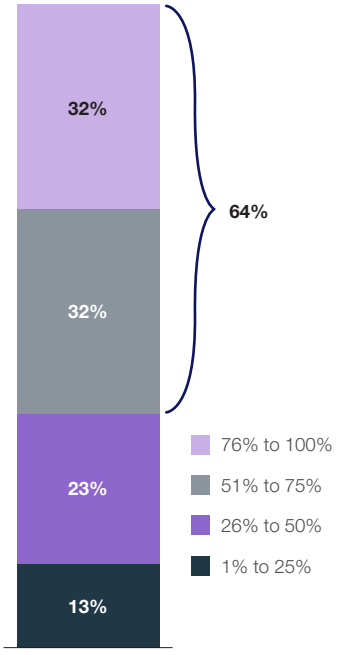

Figure 6: Additional % shifted to telework due to pandemic.

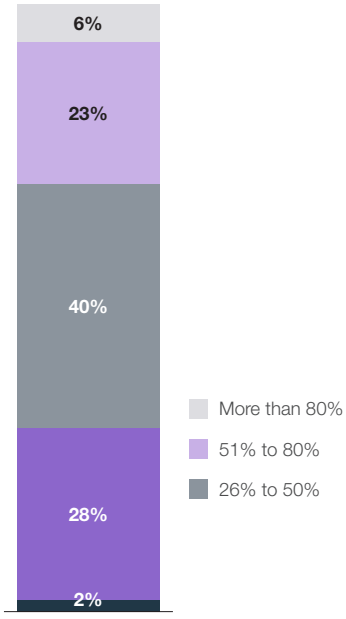

Figure 7: To remain full-time telework post-pandemic.

Insight: The Sudden Shift to Telework Was Challenging for Most Enterprises

Not surprisingly, given the focus on telework investments post-change, most survey respondents said they were challenged by the rapid change. 83% cited it as moderately, very, or extremely challenging. Another 14% said it was slightly challenging and therefore only 3% were not at all challenged.

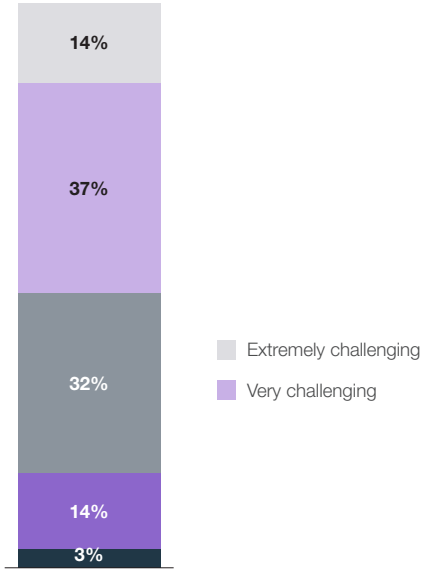

Figure 8: Degree of challenge of shift to telework.

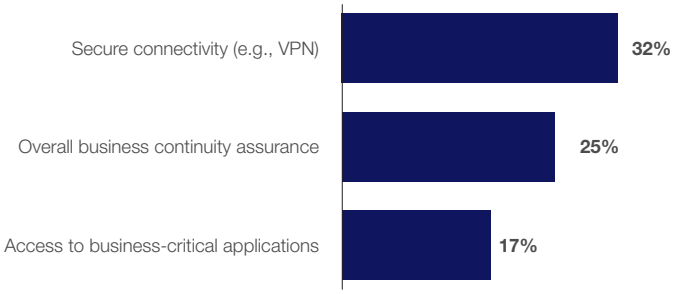

Figure 9: Top most-challenging aspects of shift to telework.

The most challenging aspects of the shift were secure connectivity, employee productivity, business continuity assurance, and access to business-critical applications.

Insight: Enterprises Are Experiencing More Breaches and Breach Attempts

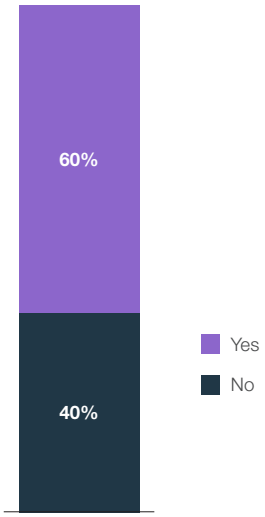

Figure 10: Respondents were asked if they noticed an increase in attempts to breach their network.

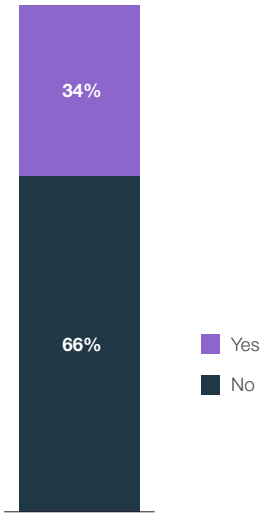

Figure 11: Respondents were asked if they experienced a security breach during shift to telework.

Insight: About Half of Respondents Are Considering Alternative Security Vendors

As a result of security issues encountered during the pandemic, 43% of those surveyed are looking to change vendors. Only 23% are planning to reduce the number of security vendors they use.

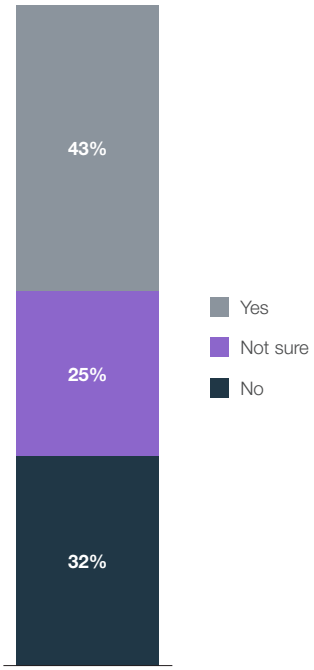

Figure 12: Respondents considering alternative security vendors.

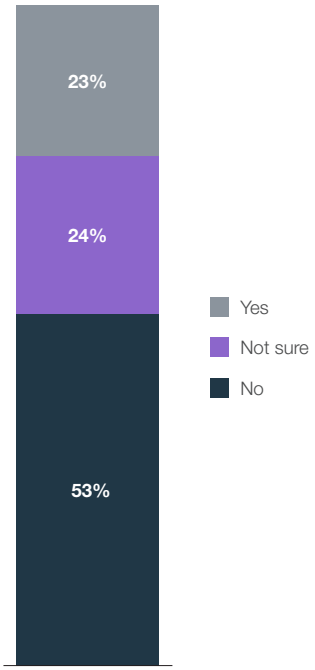

Figure 13: Respondents reducing number of security vendors.

Conclusion

The COVID-19 pandemic is going to have lasting results on secure telework and how organizations invest in security. Organizations understand that and are planning to increase spending on telework security initiatives. Given the high numbers of both attempted and successful breaches, IT decision-makers need to carefully consider what technologies and approaches are needed to secure telework. Many of the firms surveyed are focusing on the obvious areas, like VPN, cloud security, and skilled IT security personnel. However, there are some other key areas that should be given more attention to effectively shore up network security.

Things to consider for more secure telework

Organizations will be best prepared for sustained periods of telework by taking a secure access service edge (SASE) approach with secure SD-WAN. In addition, the following list of technologies and considerations may help enterprises prioritize telework cybersecurity initiatives.

"Based on our studies, your account is more than 99.9% less likely to be compromised if you use MFA." – Alex Weinert, Group Program Manager for Identity Security and Protection at Microsoft[3]

MFA. While using VPNs is necessary, it doesn't address the inherent insecurity of simple username/password logins. To access critical information and applications, MFA should be required. This eliminates the risk from stolen or weak passwords, preventing hackers from validating credentials and entering the network.

NAC. IT teams can't secure what they can't see. An advanced NAC product will profile devices as they connect, to control what devices are given access. They also provide visibility across all connections to the network. And, they include network monitoring—continuously watching for new connections and changes in connection status, taking automated action against suspicious events.

EDR. Remote user devices must be secure without impacting productivity. Advanced, real-time threat detection and mitigation for endpoints is a key tool. It proactively reduces the attack surface, prevents malware infection, detects and blocks malicious activities in real time, and can automate response and remediation procedures.

Business continuity. An organization should be capable of maintaining normal levels of productivity and security even with a remote workforce. Accomplishing this requires securing the endpoint and ensuring high-speed, reliable access to vital Software-as-a-Service (SaaS) applications. All organizations should have a business continuity plan that includes prevention and recovery systems to ensure business is not impacted even in the event of a breach or disaster.

Security complexity. Adding disparate security tools can create security gaps and management and configuration issues. A fabric solution with security controls that are seamlessly integrated with consolidated management, orchestration, and reporting tools reduces the overhead associated with telework security deployment, configuration, and troubleshooting. Further, when security devices share threat intelligence, response to threats can be automated for faster and more effective response.

[1] Megan Brenan, "U.S. Workers Discovering Affinity for Remote Work," Gallup, April 3, 2020.

[2] "Global Threat Landscape Report: A Semiannual Report by FortiGuard Labs," Fortinet, August 2020.

[3] Catalin Cimpanu, "Microsoft: Using multi-factor authentication blocks 99.9% of account hacks," ZDNet, August 27, 2019.

www.fortinet.com

August 14, 2020 11:19 PM

D:\Fortinet\Work\2020\August\081420\report-teleworker-security

740776-0-0-EN