FORTINET

INTERCONNECTING BUSINESS & CYBERSECURITY

By John Maddison

SEP 13, 2021 2:29 PM PDT

About

CISOs today face an expanding attack surface, increasingly threats, and a cybersecurity skills gap. An integrated and automated approach to security is needed to protect across the infrastructure.

OPINION

Completing the Journey from BYOD to a Hybrid WFA Workforce

While the recent transition to a work-from-anywhere (WFA) business model may have been sudden, it certainly shouldn't have caught anyone off guard. Organizations have been moving in this direction for a long time, starting with the advent of BYOD more than a decade ago. This was followed by roaming technologies that allowed mobile devices to move seamlessly across campus and even handoff an open session to a 3G/4G or WiFi connection when a user that is on a call or using an application moves off-network. Applications began moving to the cloud to further support remote and mobile workers, followed by SD-WAN and SASE technologies to further enhance remote connectivity.

What did catch everyone off-guard was the speed and scale at which the transition took place. While the trend towards remote and mobile work was clearly on track, the pandemic shortened the development cycle by several years. Organizations went from 20,000 employees in 5 offices to 20,000 employees in 20,000 offices almost overnight. IT teams worldwide had to scramble to ensure that every worker had access to essential applications and resources from a remote location, which was usually their home office. And that's where the trouble began.

Home networks are notoriously undersecured. They are often filled with vulnerable

devices, such as entertainment and gaming systems, unprotected personal devices, and consumer-grade routers that may be several years old and never updated or patched. So, while end-user devices and cloud-based applications, and connectivity tools for remote branches were mainly in place, the home network became a critical security issue for many organizations.

Tweets by @Fortinet

Cybercriminals were quick to respond. Almost overnight, they launched COVID-19 phishing attacks and switched their attack strategies to target vulnerable home networks. Unfortunately, their goal was quite successful. It was to compromise a home network, move laterally to the endpoint device used by the WFA employee, and then connect back into the corporate network to launch attacks and spread malware. Between July 2020 and June 2021, organizations saw an over 1,000% increase in ransomware attacks. Organizations have also reported that one in five successful data breaches originated from a remote worker.

This is all because the last mile of this thread of digital innovation had not been completed when the pandemic hit. This caused IT teams everywhere to build workarounds and deploy temporary solutions to keep their businesses up and running. And when a choice had to be made between security and keeping their doors open, they tended to cross their fingers and reassure themselves that this was only temporary.

But, of course, it’s not. And it never was going to be. We were already well down this road when the crisis struck, and there is no turning back. The fact is, productivity numbers for remote workers are way up, as is worker satisfaction. And business overhead costs are down. So now, most organizations are looking at a hybrid workforce, where employees work from home at least a couple of days a week—which means those “temporary fixes” aren’t temporary at all.

Fixing the home office problem should be a top priority for many organizations. New technologies are needed that combine enterprise-grade protection, reliable high-speed connectivity, secure access to essential resources, and remote management—without compromising the privacy of the home network. Corporate and personal networks need to be fully separated, with no visibility or access to

personal information granted to corporate IT teams, allowing remote workers to enjoy the benefits of a secure corporate work environment while maintaining privacy for the rest of the home network.

Using enterprise-grade technology to create entirely separate networks, a home office can become a true extension of the corporate WAN. Critical business applications can be prioritized to eliminate lag and jitter and to optimize user experience. IT teams can keep track of remote devices, manage access to applications and critical resources using tools like ZTNA, and maintain a consistent security framework that encompasses the entire distributed network. And at the same time, other users and devices, including other home workers, remote learners, and home entertainment and gaming systems, can continue to enjoy the benefits—and privacy—of a separate home network.

We are witnessing the beginning of an entirely new market, one that closes the final connectivity and security gap in the WFA journey that began over a decade ago. Effectively creating, managing, and securing a hybrid workforce, and the hybrid networks they require, is essential for the next stage of digital innovation. Organizations that can effectively make temporary strategies permanent will be able to effectively reap the benefits of increased productivity and profitability, while their workers will enjoy the flexibility and work-life balance that a hybrid work environment provides. All while meeting the strictest standards for reliable connectivity, user experience, and comprehensive security.

***

To help organizations ensure enterprise-grade security and high-performance connectivity for remote and hybrid workers at home, check out the new joint enterprise solution from Fortinet and Linksys: Linksys HomeWRK for Business | Secured by Fortinet.

Copyright © 2021 IDG Communications, Inc.