FORTINET®

WHITE PAPER

Work From Anywhere Doesn't Have To Be Complicated

Provide Consistent Security No Matter Where Users Are Located

Executive Summary

Over the past decade or so, technology has been steadily evolving to give workers more flexibility in the devices they use, the locations they can work from, and the resources they can access. Bring your own device (BYOD) and cloud application access were the first steps toward enabling flexible work.

Although organizations were on track to embrace a true work-from-anywhere (WFA) strategy sometime in the next few years, the COVID-19 pandemic accelerated the need. And now more workers are demanding that employers provide a WFA option. The challenge is in how to deliver a hybrid work experience that keeps workers both productive and secure.

Securing a Hybrid Workforce

When the pandemic hit, few organizations were prepared to support remote work. Workers were suddenly dialing into the office from poorly secured home networks. Access controls were inadequate, and endpoint devices were vulnerable. Not surprisingly, cyber criminals were quick to exploit those weaknesses. In fact, Forrester recently noted that 67% of organizations had suffered a business-impacting cyberattack attributed to remote work vulnerabilities.[2]

According to the Global Threat Landscape Report, ransomware incidents increased nearly 1100% from June 2020 to June 2021.[1]

As organizations look to the future, many of them are planning to let a significant number of their employees continue to work remotely at least part of the time. Because they have already invested in tools and solutions to help their employees remain productive, there’s no reason to deny those employees who prefer remote work the ability to keep doing it.

Hybrid workers may be in the office a few days a week and working from home or remotely the rest of the time. These workers and their devices need to move seamlessly between those environments. No matter where they are located, they need to be able to securely access applications and resources in the cloud or data center.

To support work from anywhere, organizations need to think about security and deploy solutions that are capable of following, enabling, and protecting users no matter where they are located. They need security on the endpoint combined with zero-trust access (ZTA) and zero-trust network access (ZTNA). They also need secure software-defined wide-area networking (SD-WAN) and secure access service edge (SASE) for secure connectivity. Access policy engines need to provide appropriate access based on user and device identity, location, device type, and posture to establish secure access.

The challenge most organizations face is trying to support WFA using products from a dozen or more independent vendors. One vendor might provide endpoint protection (EPP), another provides endpoint detection and response (EDR), another does identity, and so on. There may even be different firewall vendors deployed in the data center, the branch, and on the various cloud platforms being used. Creating a cohesive and reliable solution with that many vendors is nearly impossible. Ultimately, organizations end up creating complex workarounds to get solutions to even sort of work together. And maintaining those systems takes up significant amounts of IT overhead.

A better approach is to deploy solutions as part of a fully integrated cybersecurity mesh platform architecture. This platform approach provides stronger security, easier management and orchestration, and better total cost of ownership than solutions operating in isolation.

Protection Everywhere

Supporting WFA requires security that works whether the user is working from the corporate office, a home office, or while they're traveling and not in either the corporate or home office. Each of these locations poses challenges and requires certain security technology for complete protection.

In the Fortinet Global Ransomware Survey, 67% of organizations report having been a ransomware target.[3]

Work from the office

Because organizations rely on applications to conduct business, securing access to those applications, the networks to connect to those applications, and the devices that run those applications remains an essential component of a layered defense even when an employee is working from a traditional corporate office location. Most corporate offices have the customer data, servers, applications, identity information, user credentials, and source code that hackers want to access. Securing users, devices, and servers in the office starts with next-generation firewalls (NGFWs) as the first of many defenses for this critical repository of information. Organizations need to complement those NGFWs with an integrated combination of endpoint security, zero trust, and identity management:

- NGFWs secure external access by proving advanced and consistent security in campus, data center, branch, and cloud environments.
- ZTNA agents and identity services control and secure access to applications and other resources. ZTNA provides internal control by controlling access to applications, encrypted tunnels in the office, and user verifications.
- Endpoint security such as EDR for user and device security. EDR provides the means for securing the user devices and interacts with the critical data.

Office environments also should include networking and security solutions, such as Secure SD-WAN, that offer advanced networking tools that are designed to operate from a unified security platform that optimizes WAN connectivity between data centers, clouds, branches, and campus locations with application-aware intelligence.

Work from home

Remote and hybrid employees typically log in from a home office environment with a laptop, monitor, and external webcam. However, those home networks are often poorly secured with retail wireless routers and could contain vulnerable Internet-of-Things (IoT) devices that can act as a pathway for hackers to gain access. Employees using home networks also face challenges when it comes to videoconferences and other bandwidth-intensive activities. Worker productivity can be affected if other members of the household, such as family members or roommates, are consuming bandwidth with videostreaming or online gaming activities. Home users need:

- Endpoint security such as EDR to secure the worker and the devices
- ZTNA agents and identity services to control and secure access to applications and other resources
- Enterprise-class security for home networks to ensure secure access to the corporate network as well as applications in the cloud and data center. It should include traffic management to prioritize business traffic over videostreaming or gaming.

A home office solution needs to extend the corporate firewall protections to the entire home network. It also should segment the home network to provide corporate IT visibility of corporate traffic and optimize bandwidth for business applications, while ensuring employee privacy for the non-work section of the network.

Work while traveling

Users traveling or working outside the corporate office or their primary remote space are often exposed to unique threat environments. When mobile users connect to the applications and resources they need to do their jobs, they may use unknown and unsecured networks and access points, which can potentially be used to compromise the network. Mobile users need:

- Endpoint security such as EDR for the user and devices
- ZTNA agents and identity services to control and secure access to applications and other resources
- Remote network security SASE solutions for cloud-based firewalling capabilities to secure employees that are away from the office or home network

A mobile network solution should include multi-factor authentication, a cloud-based secure web gateway (SWG), and a cloud access security broker (CASB).

Integrated WFA Security Enhanced With Threat Intelligence

To support WFA, organizations should identify a cybersecurity mesh platform with solutions that are designed to work as an integrated system with actionable threat intelligence to keep the security products informed and prepared with threat identification and protection information across all of the types of locations. This type of platform approach means zero trust, endpoint, and network security can all be unified by a common set of application programming interfaces (APIs) and integration points to ensure users can seamlessly shift from one location to another with a consistent and secure experience. And on the IT side, the cybersecurity mesh simplifies policy creation and enforcement, ensures uniform configurations, centralizes management, and makes it possible to monitor and control users, devices, data, applications, and workflows.

Work from anywhere has become more important due to the recent pandemic, but the pandemic has only accelerated a trend that was in progress. The hybrid work environment is here to stay and organizations need to ensure they are ready to safely use that work model.

[1] "Global Threat Landscape Report: A Semiannual Report by FortiGuard Labs," Fortinet, August 2021.

[2] "Beyond Boundaries: The Future Of Cybersecurity In The New World Of Work," Forrester, 2021

[3] "The 2021 Ransomware Survey Report," Fortinet, November 3, 2021.

January 6, 2022 5:56 AM
1400814-0-0-EN