

SOLUTION BRIEF

Securely Work From Anywhere With the Fortinet Security Fabric

Executive Summary

The way people work has fundamentally evolved, and organizations need to be able to keep workers productive from multiple locations. They need to make it possible for employees to work safely and securely whether they are located in the office, at home, or on the road. The Fortinet Security Fabric platform delivers endpoint, network, and remote access security that is required for employees to work from anywhere (WFA). Its enterprise-class security provides a consistent user experience in all locations with comprehensive management and reporting.

The Changing Work Environment

Workforce security is constantly changing. Sometimes that change comes gradually, but sometimes it happens almost overnight. Organizations have supported remote working for decades, but only a small percentage of the workforce routinely worked outside of an office. Even though videoconferencing was available, management concerns kept the growth of remote work low; it was generally the exception, not the norm. The pandemic of 2020 changed everything, as the vast majority of workers that could work remotely were pushed out of the office. Now that companies have seen productivity levels remain high and employees have experienced the benefits of remote work, going forward, more organizations need to support workers who routinely work in an office, at home, and on the road. However, doing so expands the attack surface, so it's mandatory for organizations to provide consistent, enterprise-class protection in all of those areas.

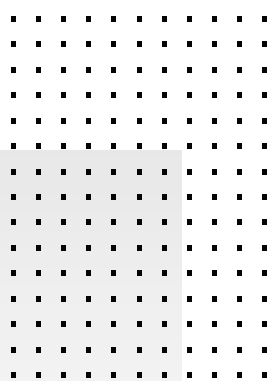
Consistent Security Everywhere

Fortinet is uniquely positioned to provide the necessary security for employees working in the office, from home, or on the road because the Fortinet Security Fabric offers enterprise-class protection for endpoint, network, and remote access. This platform approach solves the issue of managing and coordinating separate, point products with different policies for each location. The Fortinet Security Fabric offers consistent policy and enforcement, as well as reporting to help support hybrid work.

Working from home

The massive transition of the workforce to the home revealed both the benefits and the shortcomings of people working where they live. Although the reduced commute and flexible work hours increased productivity, the reduced protections had a negative impact on organizations. FortiGuard Labs saw a spike in attacks on home-based workers as literally millions of remote workers and their vulnerable home networks and devices and unprotected browsers expanded the attack surface almost overnight.²

To improve security for remote access, organizations should shift from using virtual private networks (VPNs) to using zero-trust network access (ZTNA). ZTNA provides more verification and authentication of users and devices than a VPN. It also automates the encrypted tunnels and provides granular application access, which improves both security and the user experience. Fortinet offers ZTNA as a free feature in the FortiClient Fabric Agent and the FortiGate operating system. The FortiClient Fabric Agent includes the ZTNA agent, which enables the endpoint to create encrypted tunnels to the ZTNA application gateway, which is located in a FortiGate. The ZTNA application gateway authenticates both the user and the device. It checks for the appropriate device posture and the user's rights to access a particular application.



Sixty-seven percent of business-impacting cyberattacks targeted remote workers.¹

Bad actors have targeted laptops that are located away from the layers of protection in the office, which has contributed to a surge in ransomware. Organizations should protect laptops with endpoint detection and response (EDR) solutions that can automatically detect malware as it starts to work, stop it, and restore the laptop to its pre-infected state. FortiEDR provides these features; it combines artificial intelligence with predefined playbooks for automated response. Unlike many EDR solutions that burden IT teams with too many false positives that can delay an effective response, FortiEDR uses cloud-based analysis and kernel-level actions to prevent potential malware from spreading while IT staff work to determine what is happening. Safe programs are restored and malware is removed with any changes rolled back to a pre-infection state.

Organizations must embrace hybrid work, with 75% of workers saying their expectations for working flexibly have increased.³

For organizations, home networks present difficult security challenges because they need to protect workers in an uncontrolled and unsecured network. Home networks are usually secured using retail wireless routers. The consumer-grade security and bandwidth sharing endanger corporate devices on a home network. To provide the same protections as when they are working in an office behind a FortiGate NGFW, workers at home should use cloud-based FortiSASE, which includes the same next generation firewall capabilities as a FortiGate since it is running the same operating system. FortiSASE is a firewall in the cloud, as well as adding other security features such as Secure Web Gateway (SWG), DLP, sand-boxing, and CASB so home-base employees are protected as they surf the Internet or connect back to the office.

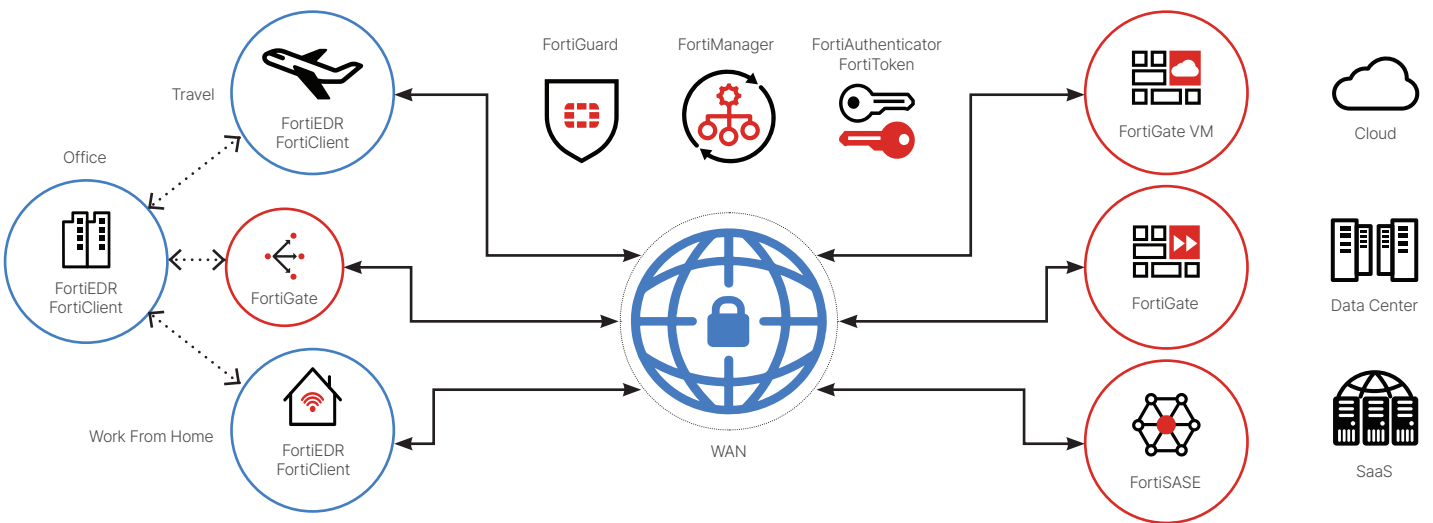


Figure 1: Fortinet enables secure work from anywhere.

Working from the road

In addition to working from a set remote location, employees also work from other non-office settings, such as airports, hotel rooms, and coffee shops. In these settings, employees need to connect back to organizational assets over untrusted networks. When users are working from the road, the Fortinet ZTNA and EDR technologies provide the same benefits as they do for a home network. The solutions control the safe access to applications and ensure the endpoint stays safe from malware. ZTNA provides the encrypted tunnel to keep the communication private and authenticates the user and device, just as it does for a user working from home. FortiEDR monitors the programs and sessions on the laptop and can step in and take action when it detects suspicious activity. The main difference between the home environment and the traveling environment is the network. When an employee is connecting from a home network, additional hardware can be deployed to control and protect the laptop, but that isn't possible while traveling. For the traveling remote worker, security solutions such as FortiSASE offer the best protection. The encrypted ZTNA tunnel can connect to a point of presence (POP) where security services such as firewalling, secure web gateway, DLP, ZTNA proxy, and CASB can be applied to protect the user and traffic. FortiSASE remote cloud-based security delivers the benefits of the Fortinet FortiGate operating system from a Fortinet-managed cloud instance.

Working from the office

The office setting has traditionally been the most protected, with layers of security for employees and company-hosted assets. Offices often have critical company information such as process secrets, customer lists, and financial records. Most companies go to great lengths to secure the offices and data centers that contain their high-value digital assets with multiple next-generation firewalls deployed for segmentation that include policies for application control, user access, and traffic inspection. Fortinet FortiGate Next-Generation Firewalls are the most widely deployed in the world and provide extensive visibility and protection to customers of all types and sizes. Even with these advanced security appliances, organizations still need to protect and control application access and the laptops used at the office. For this reason, ZTNA and EDR should also be deployed in the office to provide consistent security policies in all locations and layered protections against attacks.

Key Supporting Technologies

To secure networks, endpoints, and application access, products must be supported by certain key technologies. Identity and access management (IAM) tools such as FortiAuthenticator and FortiToken are required to enable the proper authentication of users with multi-factor authentication (MFA) and federating identity services. Organizations need FortiGuard Services to provide updated threat information to FortiGate Next-Generation Firewalls so they can use their IPS engines and signature matching to identify known threats and attacks. And management tools such as FortiManager and FortiAnalyzer, which can provide the single-pane-of-glass visibility and control across the entire platform, are also key to successfully deploying security to users when they are at home, in the office, or on the road.

New Requirements Need New Solutions

The need to support employees working from multiple locations has placed more pressure on networking and security teams. The technologies of the past, such as VPN, are being replaced by more advanced solutions that improve both security and the user experience. Fortinet is uniquely capable of providing all the networking and security technologies to support WFA. The solutions draw upon the Fortinet Security Fabric to deliver a broad, integrated, and automated solution to secure endpoints, networks, and application access.

¹ ["Beyond Boundaries: The Future Of Cybersecurity In The New World Of Work,"](#) Forrester, September 2021.

² Lakhani, Amir. ["Bad Actors are Maximizing Remote Everything,"](#) ThreatPost, May 2, 2022.

³ ["Future of Work Reinvented: Returning to the Workplace — Differently,"](#) Gartner, 2021.



www.fortinet.com