

#### **CHECKLIST**

# Five Keys to a Secure Work-From-Anywhere Solution

As organizations adopt hybrid work, they need to extend security to employees no matter where they may be located. The work-from-anywhere (WFA) model presents security risks, so it's critical for organizations to provide enterprise-level security everywhere they work, whether at home, in the office, or on the road.

In addition to the next-generation firewall (NGFW) in the office, these five key technologies keep employees productive and secure wherever they happen to be working.

#### **Endpoint Protection**

Employees take devices such as laptops with them as they move from the office to home and the airport, often connecting through unsecured public access points to access corporate resources. The increase in sophisticated malware means devices can be attacked in virtually any location. Organizations need an endpoint detection and response (EDR) solution that combines cloud-based artificial intelligence with automated playbooks to keep devices and their associated employees productive and safe. Fortinet FortiEDR provides advanced endpoint protection that detects advanced threats and stops breaches and ransomware damage in real time.

#### **✓** Application Access Control

Organizations need an access policy engine that can provide appropriate access for users in any location based on user and device identity, location, device type, and posture to establish secure access. Fortinet offers Zero Trust Network Access (ZTNA) as a feature of the FortiGate NGFW and FortiClient Fabric Agent.

#### Mome Network Security and Control

Enterprise-class security needs to extend to home networks, which are a vulnerable and potentially congested environment. Solutions should enable a corporate-controlled and secure network in the home that optimizes bandwidth for videoconferences while also ensuring privacy for the family. Fortinet has partnered with Linksys to create the Linksys HomeWRK for Business | Secured by Fortinet product, which combines the enterprise security of Fortinet with the home wireless coverage of Linksys.

## **✓** Cloud-based Security Services

Securing the network is especially challenging when employees are on the road. EDR and ZTNA can secure the endpoint and control application access, but access to the internet should be protected by a cloud-based secure web gateway (SWG) and Firewall-as-a-Service (FWaaS) services for secure connectivity while traveling. Fortinet FortiSASE is a cloud-delivered security service that protects employees whether they're working in a coffee shop or an airport.

## ✓ A Unifying Platform for Integrated Security

Trying to secure a WFA environment using a dozen or more vendors or non-compatible solutions for endpoint protection, EDR, identity, and firewall is nearly impossible. The Fortinet Security Fabric unifies Fortinet's broad portfolio of zero trust, endpoint, and network security solutions to deliver fully integrated security, services, and threat intelligence that seamlessly follow users whether they're on the road, at home, or in the office.

#### **Work From Anywhere Requires Security Everywhere**

Protecting employees as they shift between office, home, coffee shop, airport, and everywhere in between has been a challenge for many IT teams, especially as attacks have increased on remote workers. Fortinet offers integrated, comprehensive security, so organizations can secure and connect their WFA employees and devices to critical applications and resources no matter where they are located.



www.fortinet.com

Copyright © 2022 Fortinet, Inc., all rights reserved. Fortinet\*, FortiGate\*, FortiGate\*, FortiGate\*, and cartain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinets' General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinets' internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.