SOLUTION BRIEF

Protect SMB Remote Users with Fortinet Endpoint Protection

Executive Summary

Small and midsize businesses (SMBs) support large hybrid workforces, many for the first time. Hybrid work demands comprehensive security controls that work coherently across the modern IT infrastructure. Security in the corporate office is under the organization's control, but many home offices are not properly secure. Users connecting to the network via consumer-grade wireless routers and potentially infected devices may unknowingly infect the corporate network. Fortinet endpoint and work-from-anywhere (WFA) user protection provides complete security everywhere employees need it.

Fortinet delivers:

- Simplified and secure access to applications from any location with zero-trust network access (ZTNA)
- Automated endpoint hygiene scanning and remediation to improve the security posture
- Off-network web filtering to prevent users from traveling to malicious sites
- Two-factor authentication to protect against credential theft
- Real-time protection to stop breaches and ransomware
- Automated threat sharing and intelligence

Fortinet leverages advanced threat protection using artificial intelligence (AI) and machine learning (ML) and shares this intelligence across all solutions in the Fortinet Security Fabric. This integrated approach helps overwhelmed organizations deliver robust protection more efficiently.

Secure Access with ZTNA

FortiClient gives organizations the secure access and visibility they need to keep their business secure as employees work from anywhere. VPNs have long been used to ensure that traffic from off-site locations to headquarters or critical Software-as-a-Service (SaaS) applications is safe.

While VPNs provide secure connectivity, they are limited to preventing lateral movement of malware and ransomware. The risks associated with malware lateral movement become even more critical in a hybrid workforce, where WFA employees seamlessly switch between working remotely and on-site. ZTNA provides a modern solution for remote access with:

- **Improved security posture:** ZTNA uses a "never trust, always verify" philosophy, authenticating users and devices per session, continuously validating device posture, and granting access only to the specific application or resource needed. This least-privilege approach significantly reduces the attack surface and minimizes the potential impact of breaches. It also ensures that only authorized and trusted users can access sensitive data, and access can be removed in real time if they are compromised.

Components of the Fortinet Endpoint and User Protection Framework

- FortiClient ZTNA and VPN remote access, endpoint visibility, and hygiene
- FortiToken Cloud two-factor authentication
- FortiEDR real-time breach and ransomware protection
- FortiSandbox Cloud automated threat sharing and intelligence
- FortiGate Next-Generation Firewall (NGFW)

- **A more seamless, simplified user experience:** From a user perspective, ZTNA offers a more seamless and efficient experience. It eliminates manual VPN configuration, allowing users to access applications quickly and easily from any device. User experience is simplified and consistent with single sign-on access to applications from any location without logging in to every application. Additionally, ZTNA does not require backhauling all traffic through a central VPN server, which can significantly improve performance, especially for geographically dispersed users.

FortiClient unified agent integrates endpoint protection and secure access to applications to provide a comprehensive solution at a cost-effective price point for small and midsize businesses.

Endpoint Hygiene with Vulnerability Scanning, Auto-Patching, and Network Access Controls

FortiClient was purposely built to natively integrate with the Fortinet Security Fabric and, thanks to deep fabric integration, can be largely managed directly from the FortiGate NGFW or separately from the FortiClient Endpoint Management Server (EMS). FortiClient delivers:

- **Endpoint visibility and control:** Endpoint telemetry to the FortiGate gives administrators visibility, including logged-in user ID, applications, and unpatched vulnerabilities. Risk-based (conditional) access rules allow the administrator to control network access, including VPN access, based on patching and updates. It can also create an application's inventory that provides visibility into software license utilization and helps identify potentially unwanted or outdated applications where patching may not be available. Vulnerability scanning with automated patching ensures users are staying up to date, even when the endpoint is offline.
- **Centralized web filtering policies:** Even when users are offline, FortiClient delivers web security on its own or as directed from previously configured settings on the FortiGate NGFW. This ensures proper web use with web filtering and SaaS control (via the application firewall). With the latter approach, IT teams can set a consistent policy for devices on and off the network. This enables them to avoid the time and expense needed to deploy and manage a third-party web-filtering solution or web proxy tools.

Two-Factor Authentication

Theft of login credentials remains one of the most common attack vectors for cybercriminals, and hybrid work environments make this even more risky. Use of stolen credentials can be prevented with two-factor authentication using FortiToken Cloud, which makes it easy and cost-effective to validate users who log in from outside the network. From provisioning to revocation, administrators can easily manage their implementations from anywhere the internet is available—with physical tokens or push technology. Users can validate themselves with a quick swipe and click from mobile devices.

Real-Time Breach Protection and Ransomware

FortiEDR provides advanced endpoint protection, detection, and response. It helps organizations block exploits and automatically stop breaches, data exfiltration, and ransomware attacks without disrupting business operations. In a security incident, FortiEDR can protect data on compromised devices and defuse threats in real time to prevent data exfiltration and ransomware encryption. Further, automated incident response and remediation capabilities can roll back any malicious changes affecting endpoints. Key capabilities include:

- **Advanced endpoint detection and response:** SMBs are increasingly targeted with more sophisticated attacks as their digital attack surfaces expand. FortiEDR brings multi-layered detection and prevention technology such as ML, patented code-tracing technology, and automated response and remediate procedures to combat these threats.
- **Post-infection protection:** FortiEDR is the only solution that can protect your assets in real time, even on already infected computers, to keep the threats from spreading. The defusing post-infection protection layer controls outbound communications and file system modifications to prevent data exfiltration, lateral movement, and C2 communications, as well as file tampering and ransomware.
- **Backup and recovery:** FortiEDR enables administrators to roll back malicious changes and restore systems to a state before attack, eliminating the need to re-image infected systems.

Integration and Automation

When time and resources are limited, integration and automation across your security ecosystem help regain valuable cycles and build a more secure, unified solution. FortiSandbox Cloud is a dedicated, turnkey Platform-as-a-Service solution powered by dual ML models that helps detect unknown attacks and automates threat intelligence and sharing across the Fortinet Security Fabric. Unlike other sandbox SaaS solutions, FortiSandbox Cloud offers unlimited submissions and scalability. It can update Fortinet products with the latest threat information in minutes, not hours or days, with detailed analysis that maps malware techniques to the MITRE ATT&CK framework and STIX 2.0 compliant indicators of compromise.

Achieve Maximum Value with Fortinet Endpoint and Remote User Solutions

As the past year has proven, SMBs must be constantly adapting to stay ahead of the competition and even in business at all. No one predicted the massive shift to remote working, but small organizations had to support it on the fly, just as larger ones did. The future will bring new technologies that must be secured, new regulations that must be followed, and new ways of working that may upend things again.

Whatever changes occur in the future, it is critical that security continues to work and does not impede progress. Fortinet is engineered for complete protection. It enables growing organizations to get the security they need across their entire ecosystem, within their budgets and operating cycles, and scalable for future growth.

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 Fortinet's SVP Legal and above, 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 Fortinet's 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.

August 17, 2024 7:38 PM / 863430-B-0-EN