SOLUTION BRIEF

Fortinet Endpoint and Remote User Protection for Small and Midsize Businesses

Executive Summary

Small and midsize businesses (SMBs) are supporting large remote workforces, many for the first time. Currently, 70% of SMBs have at least one employee working from home—and 62% expect to continue supporting remote workers in the future.[1] Security in the corporate office is under the control of the organization, but many home offices don't have security at all. This means that users connecting to the network via consumer-grade wireless routers and potentially infected devices may unknowingly infect the corporate network. Fortinet endpoint and remote user protection provides complete protection, everywhere remote employees need it.

Fortinet delivers:

- Always-on, auto-connect virtual private network (VPN) capabilities with split tunneling to improve performance
- Automated endpoint hygiene scanning and remediation to provide application security
- 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 and machine learning and shares this intelligence across all solutions in the Fortinet Security Fabric. This integrated approach helps overwhelmed SMBs to deliver robust protection more efficiently.

Secure Access With Managed VPN

FortiClient gives organizations the secure access and visibility they need to keep their business secure as employees work remotely. VPNs have long been used to ensure that traffic from remote home offices to headquarters or to critical Software-as-a-Service (SaaS) applications is safe. Legacy VPN solutions came with two well-known deficiencies. First, users simply forget to turn it on. Second, limited firewall bandwidth and the additional decryption needed created performance issues. Fortinet addresses these issues with:

- **Free, auto-connect, always-on, managed VPN.** Managed VPN is included with your investment in FortiClient, allowing you to simplify the remote user experience with built-in auto-connect and always-on VPN capabilities. These provide secure and reliable access to corporate networks and applications from virtually any internet-connected remote location. There is no need to purchase

Components of the Fortinet Endpoint and User Protection Framework

- **FortiClient** remote VPN 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 standalone VPN solution and further complicate the security architecture. In addition, FortiClient integrates with Microsoft Active Directory (AD) to facilitate authentication and VPN logins using AD credentials.

- **Less latency with split tunneling.** Even the smallest businesses often use multiple cloud-based services these days. Organizations have historically directed all remote traffic to headquarters first using the VPN tunnel. Those accessing SaaS and other resources in the cloud would then access the public internet from there. But does all traffic really need to be routed through headquarters first before again leaving the organization on its way to its final destination?

FortiClient includes managed VPN with auto-connect, always-on, and split tunneling at no additional cost.

The split tunneling feature in FortiClient enables VPN traffic to be used solely for traffic that needs to go back to the head office, enabling other traffic to proceed directly to the internet. This enables administrators to take significant load off the VPN tunnel—which is especially useful when dealing with a large number of remote users.

In a hybrid workforce scenario, split tunneling significantly improves the user experience and reduces complaints about slow performance. Without it, the next-generation firewall (NGFW) can become a bottleneck and degrade performance.

Endpoint Hygiene With Vulnerability Scanning, Auto-patching, and Network Access Controls

FortiClient was purposely built to natively integrate with the larger 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 give the administrator the ability to control network access, including VPN access based on patching and updates. It can also create an application's inventory that not only provides visibility into software license utilization but also helps identify potentially unwanted or outdated application's 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 when they are 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 cyber criminals, 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 allowing users to 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 stop breaches, data exfiltration, and ransomware attacks automatically, without disrupting business operations. In the event of 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 that have affected endpoints. Key capabilities include:

- **Advanced Endpoint Detection and Response.** SMBs are being increasingly targeted with more sophisticated attacks as their digital attack surfaces expand. To combat these threats, FortiEDR brings multi-layer detection and prevention technology such as machine learning, patented code-tracing technology, and automated response and remediate procedures.
- **Post-infection Protection.** FortiEDR is the only solution that can protect your assets in real time even on already infected computers to contain 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 prior to 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 (PaaS) solution powered by dual machine learning models that not only helps detect unknown attacks but also automates threat intelligence and sharing across the Fortinet Security Fabric. Unlike other sandbox SaaS solutions, FortiSandbox Cloud offers unlimited submissions and scalability. It is able to 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 (IOCs).

Achieve Maximum Value With Fortinet Endpoint and Remote User Solutions

As the past year has proven, SMBs must be in a constant state of adaptation to stay ahead of the competition—and even to stay 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 that it does not impede progress. Fortinet is engineered for complete protection and enables growing organizations to get the security they need—across their entire ecosystem, within their budgets and operating cycles, and scalable for future growth.

[1] "Small business statistics during COVID-19," ZenBusiness, June 10, 2020.

FORTINET

www.fortinet.com

May 21, 2021 11:52 PM
863430-A-1-EN