FORTINET

WHITE PAPER

FortiClient and the Fortinet Security Fabric Deliver Integrated, Advanced Endpoint Protection

Executive Summary

The number of endpoints connecting to the network is expanding exponentially. These pose serious risk to an enterprise, where a single compromised endpoint can quickly infect an entire network, compromise credentials, and expose critical data to exfiltration by cyberattackers. FortiClient integrates endpoint and network security to improve endpoint security and help organizations reduce their risk exposure by coordinating security and threat intelligence across and between security elements. This seamless integration facilitates transparent visibility to each endpoint while automating security workflows, allowing IT infrastructure leaders to proactively manage endpoint risk. It also embraces zero-trust access, ensuring that endpoint devices for remote and mobile workers are not only protected but also continuously assessed and reverified before allowed to access critical assets.

Traditional Endpoint Security Fails

IT infrastructure leaders are under considerable pressure to secure their endpoints against the full range of malicious threats. Unfortunately, most traditional endpoint security solutions still operate in silos, separated from more robust network security defenses. This separation hinders visibility and slows threat responses. A new approach to endpoint security is required.

FortiClient is much more than a traditional endpoint security solution, offering advanced protection with features such as telemetry-based risk awareness, conditional access, web filtering, and machine learning. FortiClient can also be deployed as an essential and integral component of the Fortinet Security Fabric, delivering endpoint visibility, network access control (NAC), and proactive threat response.

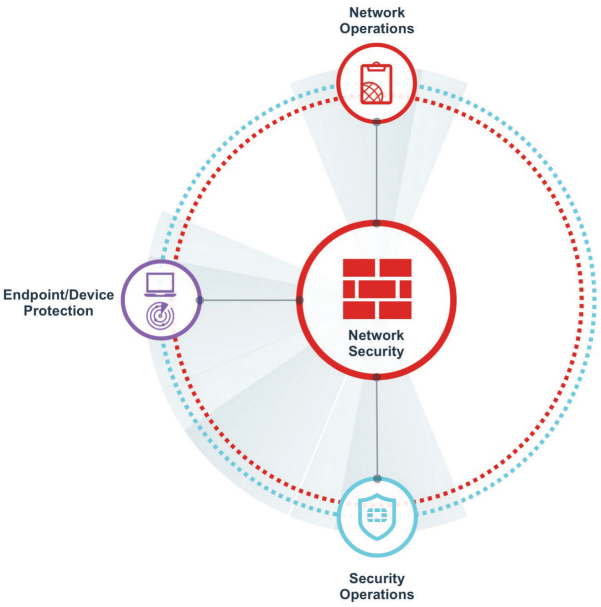

Figure 1: When deployed as part of the Fortinet Security Fabric, FortiClient can take advantage of threat-intelligence sharing to expand network visibility, detect attacks in real time, and coordinate threat response.

FortiClient enhances endpoint security in three key areas:

- Endpoint visibility and management
- Secure remote access
- Automated threat response

Independent testing shows FortiClient's superior protection and low total cost of ownership (TCO).

The NSS Labs 2019 Advanced Endpoint Protection (AEP) Group Test demonstrates that FortiClient delivers superior endpoint protection, with results that include:[1]

- 100% block rate on exploits
- 100% block rate for web-borne malware
- 100% detection rate for evasions
- Zero false positives

NSS Labs also found that FortiClient costs less than $100 per protected endpoint, placing FortiClient in the top quadrant for low TCO.[2]

Integrated Endpoint and Network Security Open Ecosystem

A critical starting point to integrating endpoint and network security is an integrated, open ecosystem of security solutions. Woven together to scale and adapt as business demands change, the Security Fabric enables companies to address the full spectrum of challenges across the expanding attack surface. Accordingly, part of the Fortinet Security Fabric, FortiClient works alongside common antivirus (AV) and endpoint detection and response (EDR) solutions. For example, users of Microsoft Windows Defender can augment their endpoint protection with FortiClient capabilities such as sandbox integration and VPN support.

Endpoint Visibility and Management

FortiClient integrates endpoint and network security, providing seamless visibility and control across and between all endpoints, enforcing conditional access, and delivering automated threat response. It provides end-to-end visibility for both hosts and endpoint devices to help organizations harden endpoints and boost their security posture. Specifically, FortiClient simplifies endpoint management by centralizing key security tasks, identifying vulnerabilities, and correlating events to improve incident reporting. Following are the ways FortiClient integrates endpoint and network security to provide transparent visibility and management:

Telemetry-based risk awareness

FortiClient establishes risk awareness by sharing real-time endpoint telemetry with network security through the Fortinet Security Fabric. As part of this process, FortiAnalyzer collects logs from FortiClient and other network components and incorporates global threat intelligence from FortiGuard Labs into a single pane of glass.

Vulnerability management

FortiClient includes vulnerability scanning that allows IT infrastructure teams to discover and prioritize unpatched vulnerabilities. FortiClient also creates an applications inventory. This not only provides visibility into software license utilization but also helps identify potentially unwanted applications and outdated applications for which patching support may not be available. All of this results in a reduced endpoint attack surface.

Centralized provisioning and monitoring

FortiClient allows IT infrastructure teams to deploy endpoint security software and perform controlled upgrades to thousands of clients in just minutes, avoiding the time drain associated with manual deployment and minimizing human error. This seamless process is aided by FortiClient API integration with Microsoft Active Directory.

Alert verification

Integration between FortiClient and other security elements across the Security Fabric enables cross-referencing of events with network traffic. This feature helps to verify and triage alerts, enhancing the "signal-to-noise" ratio for incident reporting. As a result, IT infrastructure teams spend less time investigating false positives and are able to focus on identifying actual threats more accurately.

Proactive risk management

Organizations can augment their FortiClient endpoint security with an optional subscription to the FortiGuard Security Rating Service. The Security Rating Service helps IT infrastructure leaders improve their security in measurable ways and report their risk posture to executive management, boards of directors, and auditors. The Security Rating Service helps organizations understand where they stand in relation to peer organizations and accepted standards and provides actionable insights that IT infrastructure leaders can take to improve the organization's risk posture.

Cyberattacks are profitable even at low success rates.

Modern cyberattacks, such as sophisticated phishing techniques utilizing phony emails that look quite real, can be profitable, even with a seemingly low success rate around 1%.[3]

Configuration Errors Increase Endpoint Vulnerability

By 2025, more than 85% of successful attacks against endpoints will exploit configuration and user errors rather than make use of advanced malware.[4]

Secure Remote Access

FortiClient offers IT infrastructure teams a powerful toolset for securing access by remote users, including conditional access empowered through endpoint and network integration and streamlined virtual private network (VPN 0 access) (Figure 2).

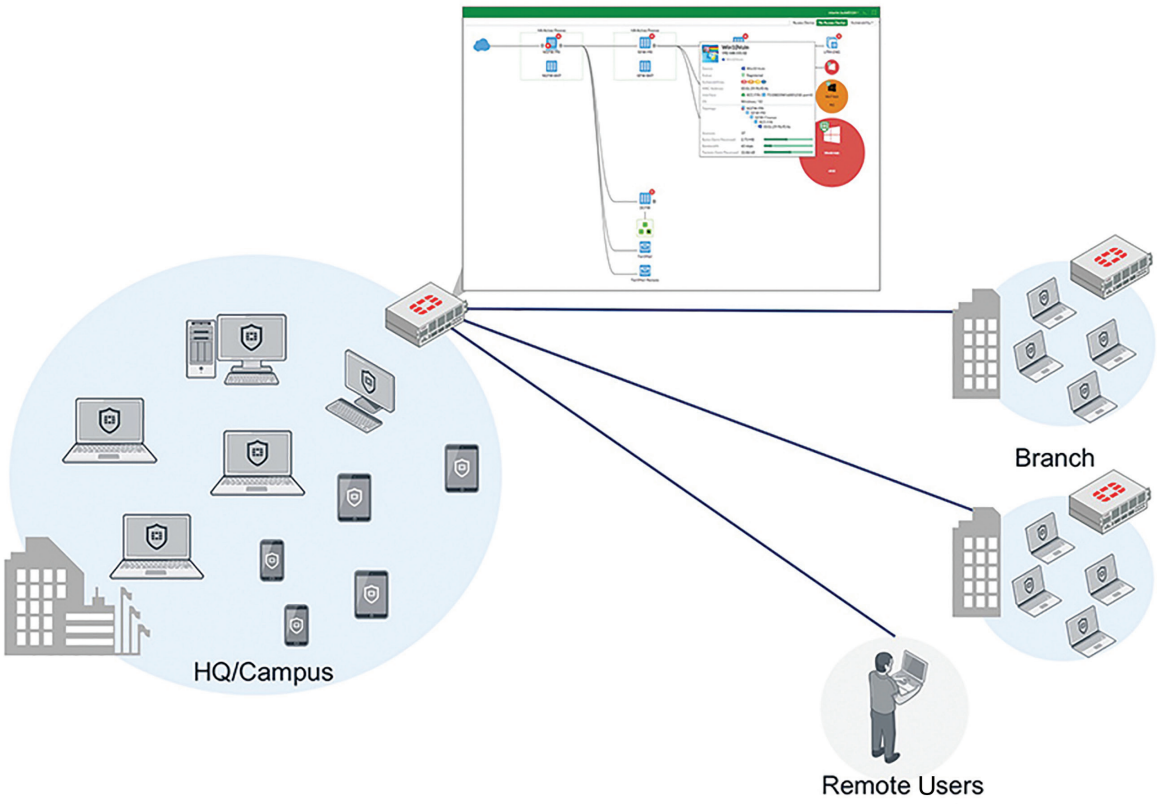

Figure 2: FortiClient supports both IPsec and SSL VPN connections to provide secure remote access to remote users and branch offices.
The FortiClient console allows administrators to provision VPN configurations and endpoint users to set up new VPN connections, saving time and reducing configuration errors.

Conditional access empowered through endpoint and network integration

Leveraging conditional access capabilities in FortiClient, the IT infrastructure team is able to control endpoint access dynamically through virtual groups to determine access rights. Thus, as an example, only users in a finance group can retrieve information from the organization's financial database. Yet, users in sales or engineering groups are unable to do so. Accordingly, FortiGate next-generation firewalls (NGFWs) retrieve and use FortiClient virtual groups to create firewall policies that enforce conditional access. This process is automatable since FortiGate NGFWs and FortiClient are integrated within the Security Fabric.

Security enforcement also extends beyond virtual group access by automating conditional access: If an endpoint is out of compliance according to a preset condition (e.g., the device lacks a critical iOS or Android patch for a specified timeframe), FortiClient will assign the user to a security-risk virtual group. By virtue of this designation, FortiGate NGFWs deny access to all resources except for internet connectivity. Once a user installs the required patch, FortiClient removes the user from the security-risk group, thereby restoring previous access rights.

Streamlined VPN access

Secure sockets layer (SSL)/transport layer security (TLS) and IPsec VPN features in FortiClient provide secure and reliable access to corporate networks and applications from virtually any internet-connected remote location. FortiClient simplifies the remote user experience with built-in auto-connect and always-up VPN capability. Integration with FortiAuthenticator allows network teams to add two-factor authentication for additional access security. In addition, FortiClient integrates with Microsoft Active Directory to facilitate authentication and VPN logins using Active Directory credentials.

Proactive Threat Response

FortiClient leverages machine learning (ML)-based anti-malware, exploit prevention, web filtering, and sandbox integration to proactively protect endpoint devices. Here, FortiClient shares real-time threat intelligence across and between all endpoints and network security components to enable enterprisewide protection, regardless of where the threat is first discovered. Threat-intelligence sharing facilitates automated responses, containing outbreaks in near real time—thereby reducing time to containment and resolution.

Automated remediation

FortiClient automatically quarantines suspect devices to limit the spread of infection to other parts of the network. It also supports automatic patching for software applications and operating systems, even when the endpoint is offline. These features help IT infrastructure leaders to ensure compliance with increasingly strict data privacy standards and industry regulations.

Web filtering

FortiClient delivers web security, web content filtering, and granular Software-as-a-Service (SaaS) control. In this case, it monitors browser and web application activity and enforces policies. FortiClient web filtering supports a variety of user devices, including Windows, Mac, iOS, Android, and Chromebook. Additionally, with FortiClient, IT infrastructure 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.

Sandbox integration

FortiClient submits unknown or suspicious objects to FortiSandbox for detailed analysis. Once FortiSandbox identifies the threat, it notifies all FortiClient-protected endpoints and other security elements within the Security Fabric (Figure 3). This proactive approach allows IT infrastructure leaders to pinpoint and block unknown and zero-day threats quickly and easily.

Automated Threat Detection Is a Critical Requirement

43% of security decision-makers consider automated detection a critical requirement, but only 30% feel their current solutions completely meet their needs in this area.[5]

Hackers Have Motives Other Than Financial Gain

Many—perhaps most—cyberattacks are motivated by the prospect of monetizing stolen information. However, hackers have other reasons to launch exploits, including:

- Extortion and blackmail
- Taunting and shaming
- Experimenting with new methods
- Credibility and bragging rights
- Advertising their services[6]

Conclusion

FortiClient facilitates deep integration between endpoint security and network security, especially when deployed as part of the Fortinet Security Fabric. This integration strengthens not only endpoint security but also network security. At the same time, automation of endpoint security workflows and threat-intelligence sharing enables IT infrastructure leaders to streamline operations. This helps them deal with the cybersecurity skills shortage.

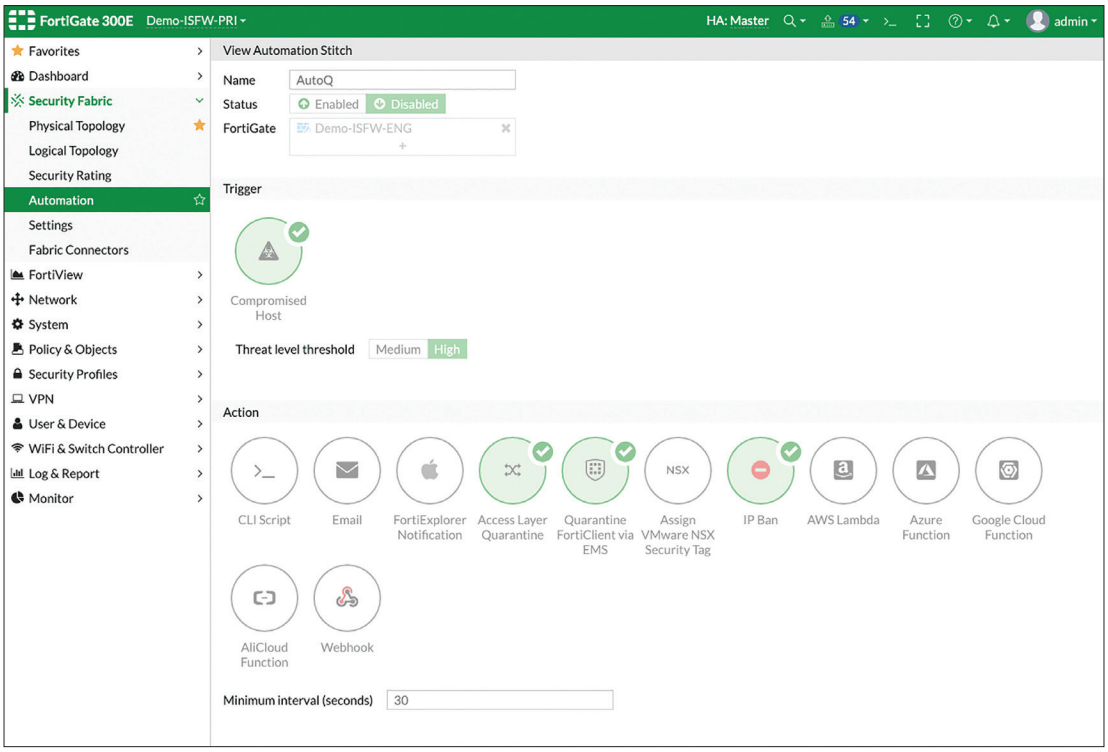

Figure 3: By integrating with the Security Fabric, FortiClient automates the process of quarantining suspicious or compromised endpoints.

In addition to the above, FortiClient gives IT infrastructure teams **end-to-end risk visibility** based on threat-intelligence sharing and full control of security policies and responses. At the same time, it offers **flexible, powerful remote access security** with conditional admission and VPN support. Finally, FortiClient delivers **proactive threat response** with integrated, automated remediation, sandbox integration, web filtering, and interoperability with common AV and EDR solutions.

[1] James Hasty, et al., "Advanced Endpoint Protection Test Report," NSS Labs, March 5, 2019.

[2] "Security Value Map: Advanced Endpoint Protection (AEP)," NSS Labs, March 2019.

[3] Jim Parise, "Heads Up: Cybercriminals Are Businesspeople," CFO, August 2, 2019.

[4] Dionisio Zumerle, "The Long-Term Evolution of Endpoints Will Reshape Enterprise Security," Gartner, May 1, 2019.

[5] "Empower Security Analysts Through Guided EDR Investigation: Bridging The Gap Between Detection And Response," Forrester, May 2019.

[6] Navanwita Sachdev, "The many motives of hackers and how much your data is worth to them," The Sociable, July 1, 2019.

October 18, 2019 12:47 AM

446978-0-0-EN