SOLUTION BRIEF

# Leveraging FortiClient with Microsoft Defender: 6 Use Cases

## Executive Overview

**A compromised endpoint can quickly infect an entire enterprise network—which is why endpoint devices are now a favorite target for cyber criminals. More than an endpoint protection platform that provides automated, next-generation threat protection, FortiClient connects endpoints with the Security Fabric. It enables endpoint visibility and compliance throughout the Security Fabric architecture. Combining FortiClient with OS-embedded protection, such as Microsoft Defender or Microsoft Defender ATP, enhances these capabilities, providing an integrated endpoint and network security solution that reinforces enterprise defenses, reduces complexity, and enhances the end-user experience.**

## Improving Protection of Endpoint Devices

FortiClient provides automated threat protection and endpoint vulnerability scanning to help maintain endpoint security hygiene and deliver risk-based visibility across the Fortinet Security Fabric architecture. As a result, organizations can identify and remediate vulnerabilities or compromised hosts across the entire attack surface.

In some cases, customers may wish to take advantage of certain FortiClient features while leaving existing third-party protections in place. For example, in instances where there are policies in an organization that require two different antivirus (AV) vendors on an endpoint for governance or compliance reasons, the need for FortiClient alongside a third-party AV solution such as Microsoft Defender is necessitated.

Following are the primary use cases involving FortiClient and Microsoft Defender:

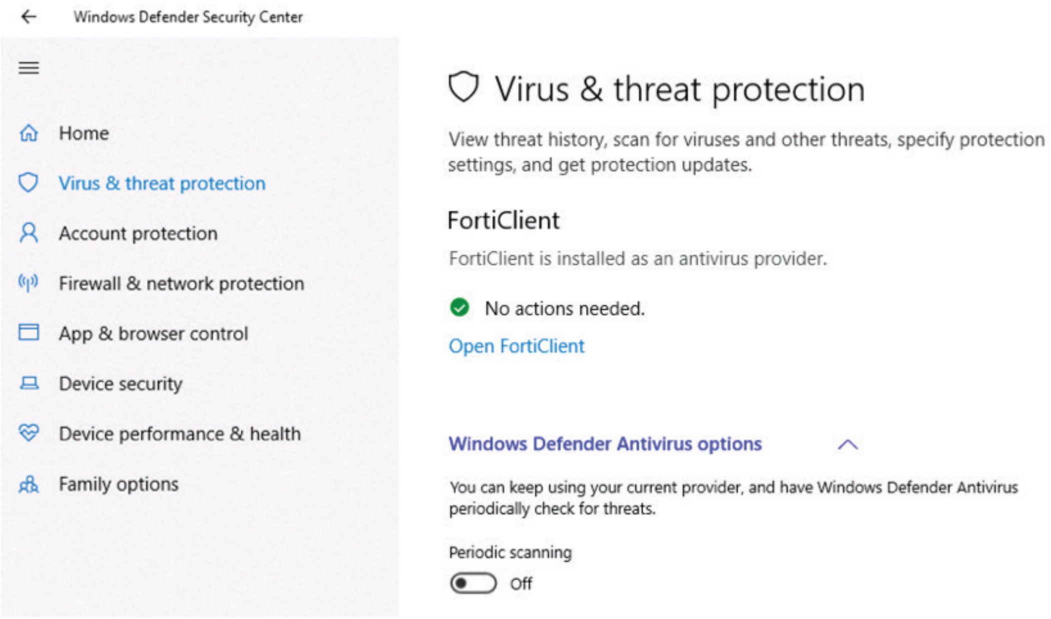
## Use Case: FortiClient with Microsoft Defender Antivirus as Backup

Microsoft Defender, unlike other AV products, is included in the operating system of Microsoft Windows endpoints. Defender is enabled automatically but will interoperate with other endpoint security products when they are installed. When FortiClient is installed and FortiClient real-time protection is enabled, Windows Defender will automatically disable its protection to avoid conflicts.[1]

In this configuration, FortiClient becomes the primary AV provider, but Defender can be used as a secondary provider in cases where the end-user must have two AV agents installed for regulatory compliance requirements. To do this, administrators need to turn on Windows Defender Periodic Scanning using Group Policy. This can also be achieved by manually using the selector in the Windows Defender Security Center (see Figure 1).

### FortiClient Features Include:

- **Security Fabric Connector.** Enables endpoint visibility and compliance throughout the Security Fabric architecture.
- **Vulnerability scanning.** Detects and patches endpoint vulnerabilities.
- **Anti-malware protection.** Employs machine learning (ML), artificial intelligence (AI), and cloud-based threat detection in addition to pattern-based malware detection.
- **Anti-exploit engine.** Uses signatureless, behavior-based protection against memory and fileless attacks; detects exploit kits and application attacks.
- **Sandboxing.** Integrates with FortiSandbox (on-premises or cloud-based).
- **Web filtering.** Institutes acceptable use policy enforcement for internet browsing.
- **Application firewall.** Blocks or allows application communication based on application signatures; backed by IPS signatures to block exploits of endpoint vulnerabilities.



Windows Defender Security Center

Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options

Virus & threat protection

View threat history, scan for viruses and other threats, specify protection settings, and get protection updates.

FortiClient

FortiClient is installed as an antivirus provider.

✓ No actions needed.

Open FortiClient

Windows Defender Antivirus options

You can keep using your current provider, and have Windows Defender Antivirus periodically check for threats.

Periodic scanning

○ Off

Figure 1: Windows Defender Security Center with FortiClient installed.

To avoid conflicts in scheduled or periodic scanning, one must ensure that FortiClient and Defender scanning schedules do not overlap.

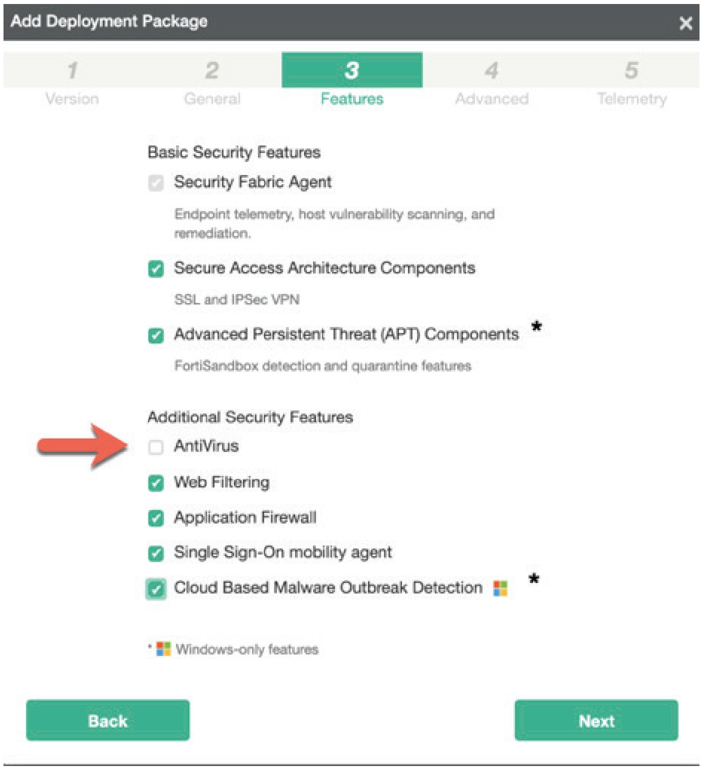
## Use Case: Windows Defender as Primary Protection

Organizations may also use Microsoft Windows Defender as their primary anti-malware protection, while using FortiClient for enhanced security, endpoint compliance controls, visibility, and broader security integration via the Fortinet Security Fabric. FortiClient modules that can be enabled to complement Windows Defender include:

- Endpoint telemetry
- Vulnerability scanning
- Application inventory
- Application firewall
- Web filtering
- Sandbox integration

**Technical considerations:** Because Microsoft Defender is sensitive to other anti-malware products with real-time scanning, Defender will disable its protection if another AV real-time protection product is installed—regardless of whether it is enabled or not.

FortiClient Endpoint Management Server (EMS) provides a solution to this problem. EMS contains an Installer Management feature, allowing customers to configure deployment packages with only the components they desire to be installed on the endpoint. In this use case, a FortiClient package would be created without the standard AV module, leaving Defender to act as the primary protection (see Figure 2).



Add Deployment Package

Basic Security Features

☑ Security Fabric Agent

Endpoint telemetry, host vulnerability scanning, and remediation.

☑ Secure Access Architecture Components

SSL and IPSec VPN

☑ Advanced Persistent Threat (APT) Components *

FortiSandbox detection and quarantine features

Additional Security Features

☐ AntiVirus

☑ Web Filtering

☑ Application Firewall

☑ Single Sign-On mobility agent

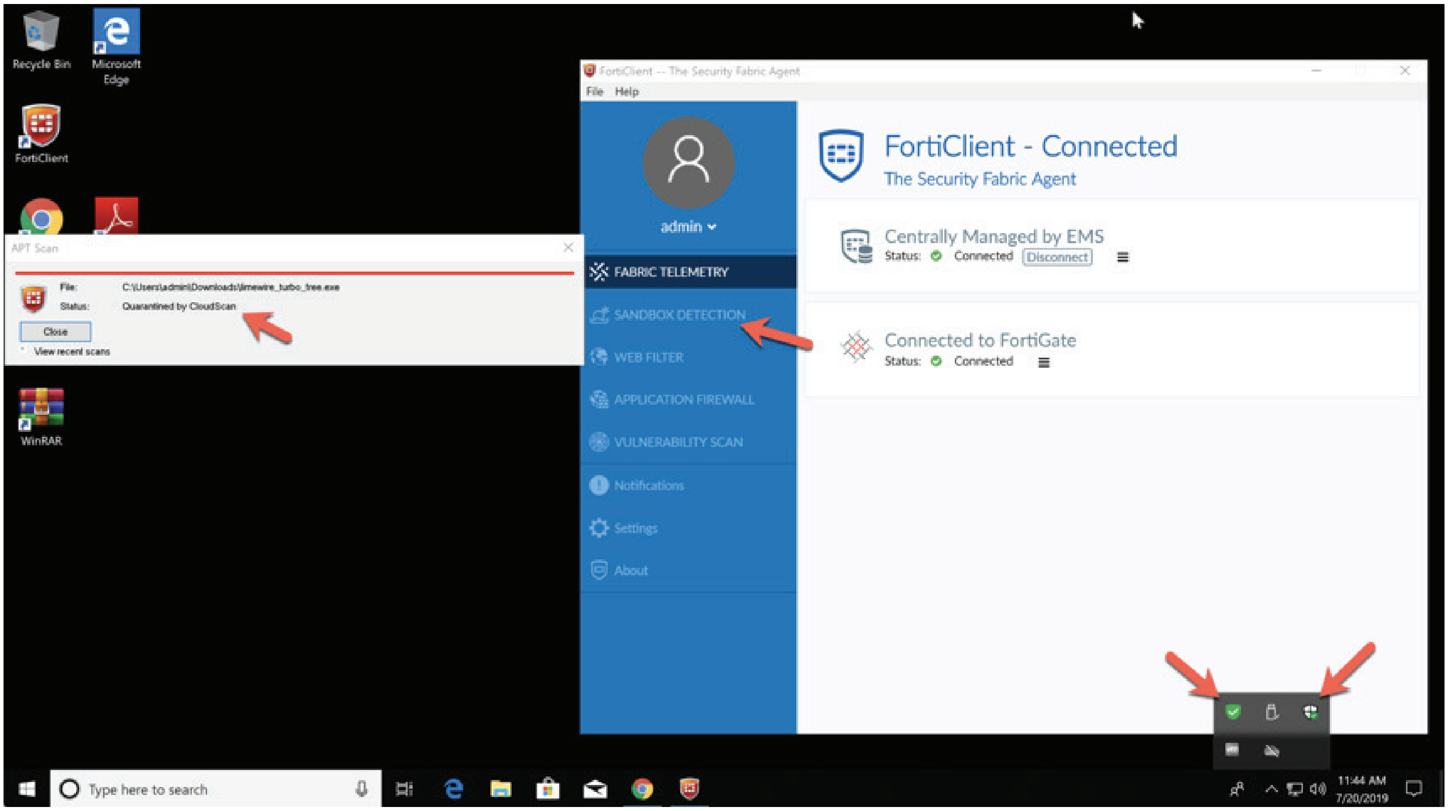
☑ Cloud Based Malware Outbreak Detection *

* Windows-only features

Figure 2: When using Windows Defender for primary antivirus protection, users can select to add FortiClient for enhanced security.

In this use case, note that the “AntiVirus” module is deselected, but “Advanced Persistent Threat (APT) Components” are enabled as well as “Cloud Based Malware Outbreak Detection.” Both of these components augment the protection that Defender provides by adding sandboxing and cloud-based emerging threat-detection capabilities.

Once deployed, both FortiClient and Defender will coexist and provide dual-vendor threat protection. When both Defender and FortiClient are enabled with FortiSandbox and FortiClient cloud-based outbreak detection, a file can be downloaded and detected by FortiClient (see Figure 3).



APT Scan

File: C:\Users\admin\Downloads\limewire_turbo_free.exe

Status: Quarantined by CloudScan

Close

View recent scans

FortiClient -- The Security Fabric Agent

FortiClient - Connected

The Security Fabric Agent

Centrally Managed by EMS

Status: Connected Disconnect

Connected to FortiGate

Status: Connected

Figure 3: The Windows Defender administrative panel shows what additional third-party elements have been activated and their status.

## Use Case: Endpoint Visibility and Compliance Control

Organizations need full awareness of endpoints when they are on and off the organization’s network. Security must be able to see all users and devices and be able to assess inherent risks—including potential compliance issues; only endpoints that meet all compliance and security standards should be granted access to the network. Automating endpoint detection and response solutions is the top priority for IT professionals trying to put actionable controls around their endpoints.[2]

### Endpoint telemetry for visibility

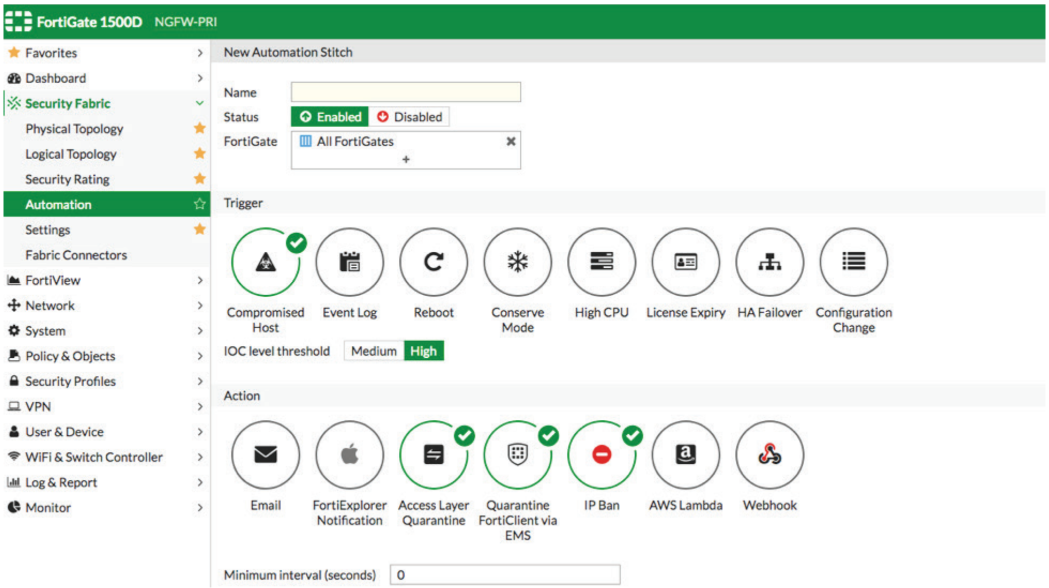
FortiClient shares endpoint telemetry with the Security Fabric to ensure unified endpoint awareness and delivers integrated endpoint and network security. Shared endpoint information includes device information, OS, security status, vulnerabilities, events, and user ID.

### Dynamic access control for compliance enforcement

EMS creates virtual groups based on endpoint security posture. These virtual groups are then retrieved by FortiGate and used in firewall policy for dynamic access control. Dynamic groups help automate and simplify compliance for security policies.

### Automation/host quarantine

The Fortinet Security Fabric features automated responses that include automated host quarantine. For example, with the IOC (indicator of compromise) service, the Security Fabric can identify suspicious or potentially compromised hosts, and then automatically trigger a policy-based response to quarantine the endpoint in order to contain incidents and prevent outbreaks. Thanks to native endpoint and network integration, there are multiple options for quarantining endpoints (see Figure 4).



Name

Status: [✓ Enabled] Disabled

FortiGate: All FortiGates

IOC level threshold: Medium [✓ High]

Minimum interval (seconds): 0

Figure 4: FortiGate NGFW dashboard includes the ability to automate specified endpoint security workflows.

## Use Case: Endpoint Hardening

Organizations must identify, install, and configure effective security solutions to harden their endpoint devices against attack—as well as to establish baseline readings. Key success factors in this pursuit include ease of data collection (49%), correlation of data into usable information (47%), skilled operators (46%), and automation/tool interoperability (43%).[3]

### Vulnerability scanning and patching

Most successfully exploited vulnerabilities are known by the IT security team at the time of the attack with patches available. FortiClient provides endpoint vulnerability scanning capabilities for detecting unpatched vulnerabilities (including endpoints that may have installed patches but are pending restart) with detailed information (such as severity of the issue) in order to pinpoint specific devices that need attention. FortiClient's flexible patching options include:

- Detect unpatched vulnerabilities
- Prioritize
- Link to additional information
- Share endpoint vulnerability information with Security Fabric components (e.g., FortiGate, FortiAnalyzer, Security Rating Service)

Vulnerability scanning results are also shared across the Security Fabric as part of endpoint telemetry, providing real-time, risk-based visibility. This allows the network security operations team to take additional measures to help secure the broader organization. For example, a company can set up conditional network admissions that restrict access to sensitive information from endpoints that have severe vulnerabilities.

Users that already rely on Microsoft System Center Configuration Manager for patching can continue to do so. As a complementary tool, FortiClient can patch applications that CCM or Windows Server Update Services (WSUS) do not. FortiClient provides real-time visibility and control across endpoint and network security operations.

### Application inventory

Another key aspect of endpoint hardening is application visibility. Potentially unwanted applications (PUA) and end-of-life (EOL) applications can increase security risks. FortiClient's application inventory capabilities provide administrator-level visibility of all installed software and version numbers across the organization—which can improve overall security hygiene. Administrators can leverage inventory information to detect and remove unwanted or outdated applications in order to reduce the organization's attack surface.

## Use Case: Unified Policy Enforcement

Endpoint security should enforce policies and controls across all devices. FortiClient web filtering and application firewall functions follow the same policy protocols as FortiGate next-generation firewalls (NGFWs) to ensure consistent enforcement as well as simplified management.

### Web filtering and web security

By enabling FortiClient's web-filtering function, users can enforce acceptable web usage across all platforms—including Windows, Mac, Android, iOS, and Chromebook devices. Users can also import and sync web-filtering policies between FortiGate and FortiClient EMS to ensure unified enforcement both on and off network.[4] The addition of FortiAnalyzer enables logging of the browsing history to satisfy compliance requirements (such as in K-12 environments).

### Application/SaaS control

By enabling FortiClient's application firewall function, users can enable control of applications—including Software-as-a-Service (SaaS) subscriptions. The application firewall includes anti-botnet and IPS signatures that can block exploits. As with FortiClient web filtering, the application category is the same as FortiGate—allowing the implementation of a consistent application control policy.

## Use Case: Advanced Threat Protection

As a next-generation endpoint protection solution, FortiClient helps connect endpoints to real-time security tools and research-based services within the Security Fabric to help organizations repel unknown threats and zero-day attacks.

### Sandboxing for zero-day threats

FortiClient natively integrates with FortiSandbox sandboxing solutions. FortiClient can block execution of never-before-seen files (including scripts) and then automatically submit files to the sandbox for immediate analysis. Real-time threat intelligence from FortiSandbox is then instantly shared across the enterprise—including all deployed endpoints. For example, if an unknown object submitted from FortiGate or FortiMail is determined to be malicious, the information is then disseminated to all FortiClient-protected endpoints in near real time. FortiClient also offers an optional FortiSandbox Cloud subscription. Licensed endpoints running FortiClient 6.2.0 can now use the FortiSandbox Cloud service for deep inspection of zero-day threats.

### IOC service

Customers that subscribe to the FortiAnalyzer IOC service can also leverage FortiClient's integration with the Security Fabric. With the IOC service, FortiAnalyzer can identify endpoints that are potentially compromised and then automatically quarantine the suspicious endpoint (as an optional configuration using EMS) for further investigation.

## FortiClient and Microsoft Defender Simplify Endpoint Security

With an ever-increasing number of endpoint devices (including workstations, servers, laptops, tablets, and smartphones) across most organizations, management of IT assets has become a constant challenge. The combined capabilities of FortiClient and Microsoft Defender can help organizations consolidate point security solutions for endpoint protection—including AV, endpoint detection and response (EDR), vulnerability scanning, virtual private network (VPN), and proxy client. With broader integration with Fortinet Security Fabric controls, FortiClient and Defender help provide an effective dual-vendor security solution for comprehensive visibility, control, and protection of endpoint devices.

[1] "Windows Defender Antivirus compatibility," Microsoft, September 2, 2018.

[2] Lee Neely, "Endpoint Protection and Response: A SANS Survey," SANS Institute, June 12, 2018.

[3] Ibid.

[4] Please note: While Windows Smart Screen Filter provides web security, it does not offer policy enforcement and only works with the Windows Edge Browser.

September 17, 2019 3:44 PM

Macintosh HD:Users:ckluck:Documents:FORTINET_ck:2019:sb-Leveraging-FortiClient-w-Microsoft-Defender-6-Use-Cases:sb-Leveraging-FortiClient-w-Microsoft-Defender-6-Use-Cases