SOLUTION BRIEF

Fortinet and Symantec Provide Comprehensive Security for Endpoints and Network Infrastructure

Executive Summary

With the adoption of a digital business model, applications, data, and services must flow faster across an increasingly diverse landscape of users, domains, and devices. As data moves freely between locations—including virtualized networks and public cloud environments—organizations find it increasingly difficult to track and secure their infrastructure. The isolated point security solutions that most organizations have deployed over the past decade are simply not designed to solve today's cybersecurity challenges. Security administrators need greater visibility and control across their entire end-to-end deployment—including physical, cloud, and virtualized network infrastructure, as well as endpoints. In this regard, the combination of Symantec Endpoint Protection and the Fortinet Security Fabric provides an ideal solution.

Endpoint Devices Expand the Network Attack Surface

Defending highly dynamic and distributed environments requires tightly integrated security and network technologies that share intelligence and collaborate to detect potential issues, isolate threats, and synchronize automated responses in real time across the entire connected infrastructure.

Symantec Endpoint Protection is designed to address today's threat landscape with a comprehensive approach to endpoint device security. Symantec Endpoint Protection spans the attack chain and provides in-depth defenses. Fortinet provides best-in-class network security through its award-winning **FortiGate** network security platform and the integrated **Fortinet Security Fabric** architecture. The Security Fabric allows security components to share intelligence between devices and systems. This integration also enables unified security management as well as automates threat responses that can be synchronized across the organization. This open architecture of connected defenses allows organizations to scale and adapt their security as business demands change while addressing the full spectrum of cyber threats across an ever-expanding attack surface.

A Joint Solution for Shared Endpoint Intelligence

The diagram below illustrates how Symantec and Fortinet work together to provide end-to-end security across endpoints and network infrastructure.

The joint Symantec and Fortinet solution combines Symantec's endpoint protection with Fortinet's best-in-class network security and Security Fabric architecture to deliver unparalleled protection. This pairing enables customers to use Symantec Endpoint Protection for advanced endpoint device security while leveraging the Fortinet Security Fabric to gain end-to-end visibility of endpoints and network infrastructure.

Joint Solution Components

- Fortinet FortiGate Next-generation Firewall (NGFW)
- Symantec Endpoint Protection

Joint Solution Benefits

- Comprehensive endpoint protection against advanced threats
- Consistent compliance policy enforcement
- End-to-end visibility and security

FORTINET FABRIC-READY

According to the Ponemon Institute, the frequency of attacks against endpoints is increasing—as is the cost, with the average successful attack now causing $7.1 million in damages.[1]

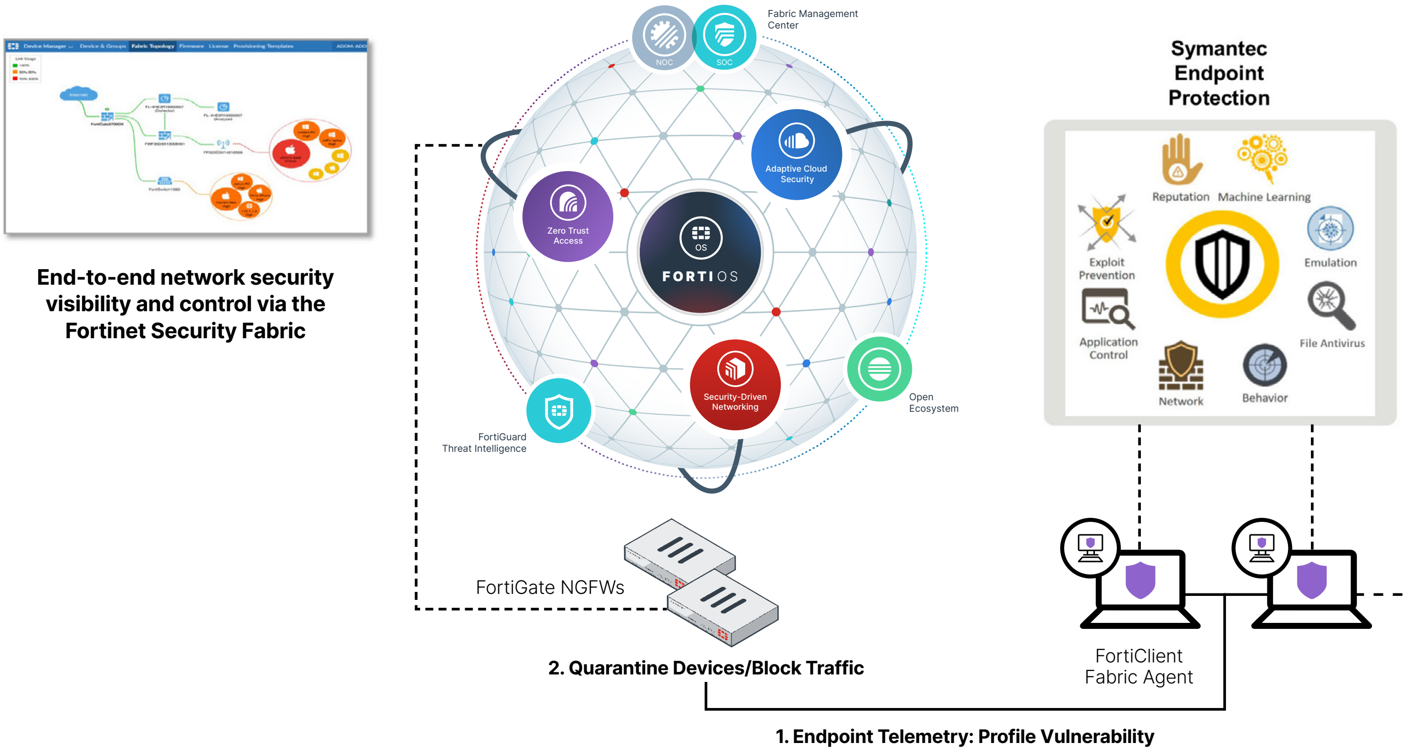
End-to-end network security visibility and control via the Fortinet Security Fabric
NOC
SOC
Fabric Management Center
Adaptive Cloud Security
Zero Trust Access
OS
FORTIOS
Security-Driven Networking
Open Ecosystem
FortiGuard Threat Intelligence
FortiGate NGFWs
2. Quarantine Devices/Block Traffic
Symantec Endpoint Protection
Reputation
Machine Learning
Exploit Prevention
Emulation
Application Control
File Antivirus
Network
Behavior
FortiClient Fabric Agent
1. Endpoint Telemetry: Profile Vulnerability

Figure 1: Symantec Endpoint Protection and the Fortinet Security Fabric.

Endpoint security compliance rules are defined by security administrators in a FortiGate security profile, which contains the requirements that devices must satisfy prior to accessing the network (such as software/OS version updates and current security patches). Policy enforcement, which is enabled by FortiGate next-generation firewalls (NGFWs) and FortiClient, enables security administrators to ensure that connecting devices comply with all defined criteria, thus limiting risk exposure and reducing organizational attack surface.

In addition, the FortiClient Fabric Agent module feeds FortiGate NGFWs telemetry, profile, and vulnerability data—enabling automatic updates from the endpoints to the Security Fabric. This provides comprehensive visibility across all connected endpoints and network infrastructure.

These actions are complemented by Symantec Endpoint Protection, which blocks viruses, malware, and other threats from infecting endpoint devices. Symantec Endpoint Protection effectively stops advanced threats using advanced machine learning (ML), file reputation analysis, and real-time behavioral monitoring.

Visibility, Control, and Security Across the Network

This partnership combines Symantec's endpoint protection leadership with Fortinet's best-in-class network security and Security Fabric integration to deliver unparalleled protection. The joint benefits of Symantec Endpoint Protection and the Fortinet Security Fabric include:

- Providing comprehensive endpoint security with powerful, layered protection that minimizes risk across the network attack surface while preventing a variety of sophisticated threats
- Enforcing consistent compliance policies across the organization
- Delivering end-to-end visibility without compromise across the entire security deployment

[1] "2018 State of Endpoint Security Risk," Ponemon Institute, October 2018.

March 30, 2021 9:01 AM
D:\Fortinet\2021 Rebranded templates\Marketing or Comms Request\March\Branding Refresh\913517 - Update Connecting SBs\sb-FA-fortinet-and-symantec-3302021\sb-FA-fortinet-and-symantec-3302021
472273-A-0-EN