SOLUTION BRIEF

Fortinet and Gigamon Security Solution

Pervasive Visibility Enabling Pervasive Security with Fortinet and Gigamon

Executive Summary

The Fortinet and Gigamon Security Solution combines the power of Fortinet's secure networking and security operations capabilities with the Gigamon Deep Observability Pipeline, provides network-based threat detection capabilities that improve SOC teams' ability to rapidly identify and respond to sophisticated threats.

Fortinet's award-winning FortiGate Next-Generation Firewalls (NGFWs) provide top-rated protection, high performance, and advanced security services such as secure sockets layer (SSL) inspection and ultra-low latency for protecting mission-critical environments. Through awareness of applications, users, and content within network traffic, FortiGate NGFWs offer comprehensive protection against known and unknown threats, including ransomware, malicious botnets, zero-day attacks, and encrypted malware. As an integral part of the Fortinet Security Fabric, FortiGate NGFWs communicate within Fortinet's comprehensive security portfolio and third-party security solutions to share threat intelligence and improve security posture.

Fortinet Network Detection and Response (NDR) and SIEM solutions provide visibility into your environments allowing your security team to detect, prioritize, investigate, hunt, and respond to attacks across your network. Using AI-based detections and expert analysis, security teams can spot evidence of attacker behavior early, enabling effective responses across your IT/OT/IoT environments.

The **Gigamon Deep Observability Pipeline** provides good visibility to FortiGate firewalls and Fortinet NDR solutions. Accessing, optimizing, decrypting, and extracting metadata enhances these tools' visibility and intelligence. This ensures that FortiGate firewalls and Fortinet NDR solutions have comprehensive insight into network traffic across all environments. These capabilities also ensure maximum visibility and prioritize resources for the traffic most at risk for attacker activity, thereby strengthening security posture.

Joint Solution

The Fortinet Security Fabric and the Gigamon Deep Observability Pipeline provide the pervasive, scalable, high-performance security solution needed to address the demands of today's business world. The award-winning FortiGate network security platform has core, edge, and access solutions. Network detection and response combines AI-based, human, and behavioral network traffic analysis to look at and trace evidence of malicious activity without installing agents.

Fortinet NDR solutions enables security professionals to coordinate threat-hunting and investigation efforts across their global SOC teams. Team members can view existing queries and investigation results. They can also pivot to predesigned queries with results already ready for review. All detections are mapped to the MITRE ATT&CK framework, ensuring global alignment regarding attacker behavior.

Pairing any of these Fortinet solutions with the Gigamon Deep Observability Pipeline gives SOC and NOC teams the confidence that all traffic from anywhere can be inspected promptly and efficiently. This also ensures a deeper understanding of what is occurring across the hybrid cloud infrastructure.

Solution Components

- Fortinet FortiGate Next-Generation Firewall
- Fortinet Network Detection and Response (NDR) Solutions
- Fortinet Security Information and Event Management (SIEM)
- Gigamon Deep Observability Pipeline

Solution Benefits

- Proven protection of assets and users, without limiting the speed or capacity of network operations
- Protection from threats, even if they are in encrypted traffic
- Highly resilient and operationally robust deployment that minimizes planned and unplanned service outages
- Automatically identify anomalous and malicious behavior, with relevant risk scores, and threat intelligence to assist security teams in prioritizing response efforts
- Maximize protection while achieving maximum efficiency from deployed assets
- Leverage global threat intelligence with Fortinet FortiGuard Security Subscription Services to protect individual customers

FORTINET FABRIC-READY

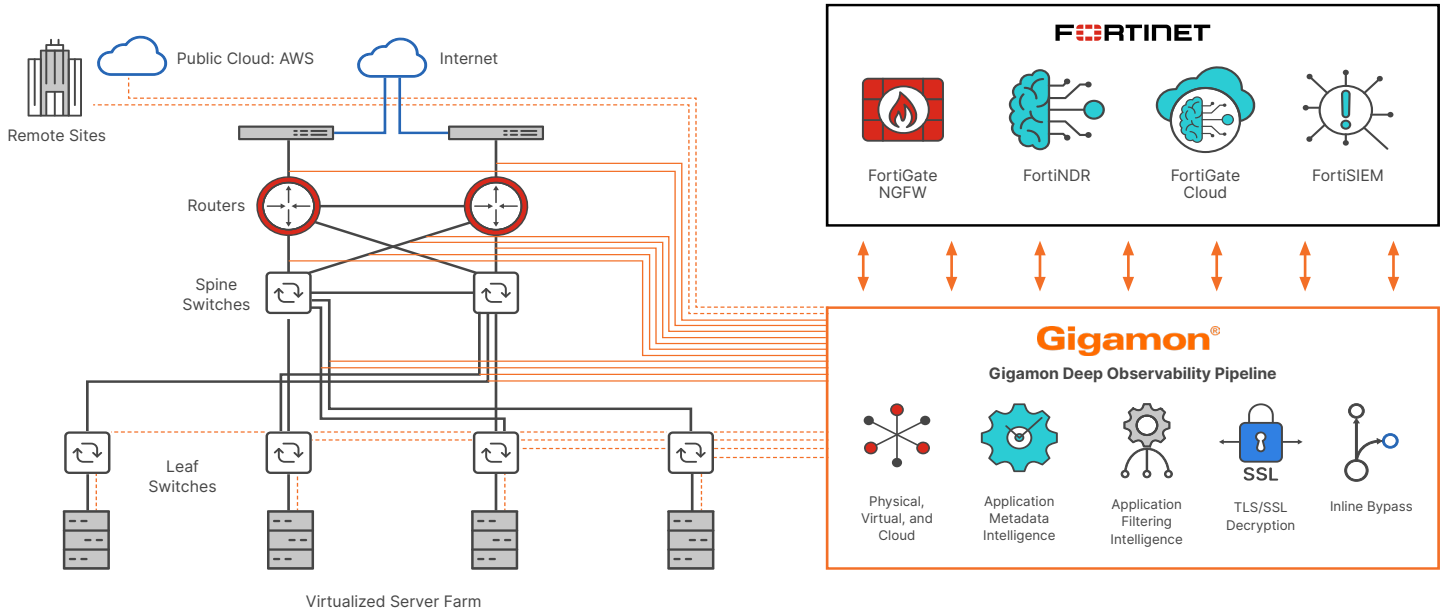

Figure 1: Joint solution composed of Fortinet Solutions with the Gigamon Deep Observability Pipeline

Joint Use Cases

Traffic distribution for load sharing: Improve the scalability of inline security by distributing traffic across multiple FortiGate NGFW appliances. This allows them to share loads and inspect more traffic, matching traffic volumes to the scale and number of security appliances deployed rather than having to match the number of network links protected.

Visibility into all your data: Gain visibility, network-derived intelligence, and control of all the traffic in motion on your network. Understand what applications are on your network, use filtering to eliminate unnecessary tool traffic, and gain insight into application and user behavior with Fortinet Security Fabric and Gigamon TLS/SSL decryption capabilities.

Agile deployment: FortiGate NGFW appliances can be added, removed, or upgraded without disrupting network traffic. They can also be converted from out-of-band monitoring to inline inspection on the fly without rewiring. Devices can be moved inline automatically or at the touch of a button without a network outage.

Consolidated IT/OT security: FortiSIEM and Fortinet NDR solutions support various OT-specific functions that enable customers to protect OT assets using standard IT security operations technologies and processes. For example, FortiSIEM and FortiNDR include OT asset discovery and monitoring and CMDB support. Both products feature Purdue and MITRE ATT&CK ICS mapping and integration with leading OT security products.

Real-time network detection: Fortinet NDR solutions leverage ML and AI to detect anomalous and malicious activity on the network, such as encrypted attacks via JA3 hashes, malware-based behaviors such as ransomware, downloaders, and coin miners, and attack origins such as worm infections.

About Gigamon

Gigamon offers a deep observability pipeline that efficiently delivers network-derived intelligence to cloud, security, and observability tools. This helps eliminate security blind spots and reduce tool costs, enabling you to better secure and manage your hybrid cloud infrastructure. Gigamon has served more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, nine of the ten largest mobile network providers, and hundreds of governments and educational organizations. To learn more, please visit gigamon.com.

February 21, 2025 3:55 PM / MKTG-278-0-0-EN