JOINT SOLUTION BRIEF

Gigamon and Sentinel Intrusion Prevention Systems Shore Up Security for Resource-Strapped Teams

The Challenge

Lean IT teams find themselves overwhelmed defending their network, triaging alerts and differentiating between benign and actual threats.

Integrated Solution

When working with the Gigamon Visibility Fabric, Sentinel Outpost and Sentinel Internal Intelligence can enhance visibility into malicious traffic, detect network vulnerabilities and locate problem devices quickly, giving you more time to focus on the projects that drive revenue and add efficiencies to your operation.

Joint Solution Benefits

- Boosts visibility and access to traffic from physical, virtual and public cloud networks
- Supports failover protection and maintains traffic continuity in the event of a network outage or tool failure
- Blocks billions of known threats before they hit the firewall, reducing the firewall workload by 70 percent
- Masks sensitive or confidential data within packets before they're sent to other tools
- Splits too-large traffic flows across multiple tools, while keeping sessions together

Introduction

Many small businesses, state and local government entities, and companies with lean IT departments don't have the security expertise or time to manage increasingly sophisticated — and frequent — cyberattacks. So, they're turning to Sentinel Intrusion Prevention Systems to do the heavy lifting.

Sentinel, a network security services provider, has deflected billions of ransomware, malware and targeted brute force and exploit attempts. They're taking much of the burden off lean IT teams through enhanced protection, visibility and a 24/7 support team that assists with managing critical alerts, troubleshooting network issues and researching security events.

The Gigamon-Sentinel Joint Solution

Integrated with the Gigamon Visibility Fabric, the Sentinel Outpost and Internal Intelligence solutions offer greater visibility into malicious traffic traversing the network.

- Sentinel's Internal Intelligence locates problem devices quickly, scans the network for vulnerabilities, and monitors unique and interesting internal traffic
- Sentinel Outpost can reduce the firewall's workload by up to 70 percent and enhance visibility into malware, exploits and other malicious traffic

Key Gigamon Visibility Fabric features that enhance the value of Sentinel Outpost and Sentinel Internal Intelligence Unit to defend the network include:

- **Easy access to traffic from physical and virtual networks:** The Gigamon Visibility Fabric manages and delivers all network traffic — including east-west data center traffic and private and public cloud workloads — to tools so all traffic can be monitored and analyzed together, reducing blind spots and increasing the likelihood of spotting suspicious behavior.
- **Load balancing to spread traffic across multiple devices:** When traffic flows are larger than a single tool can cope with, the Visibility Fabric can split the flow across multiple tools, while ensuring sessions are kept together. Additionally, tool numbers can be incrementally grown by adding new devices to those already connected.
- **Easier control of asymmetric routing to ensure session information is kept together:** Most security devices require all the packets in a session to be inspected by the same device because incomplete sessions can be blocked. Gigamon's Visibility Fabric provides an intelligent and efficient way to ensure that happens in most architectures.
- **Traffic filtering:** The Visibility Fabric can be configured to only send relevant traffic — or relevant sessions — to the connected tools, so Sentinel tools don't become overloaded with irrelevant traffic.
- **Inline bypass for efficient and resilient deployment:** The inline bypass functionality of the Gigamon Visibility Fabric provides physical bypass traffic protection in the event of power loss and logical bypass traffic protection in the event of an inline tool failure.
- **SSL decryption:** The Visibility Fabric is used to decrypt SSL encrypted traffic for inspection by security tools and any other devices connected out of band.

- **Masking for security/compliance:** The Visibility Fabric is used to mask sensitive or confidential data within packets before they're sent to other tools, where they may be seen by unauthorized people.
- **Deduplication:** Pervasive visibility requires tapping or copying traffic from multiple points in the network, which in turn, means tools may see the same packet more than once. To avoid the unnecessary packet-processing overhead on Sentinel tools, the Visibility Fabric removes duplicates before they consume resources.

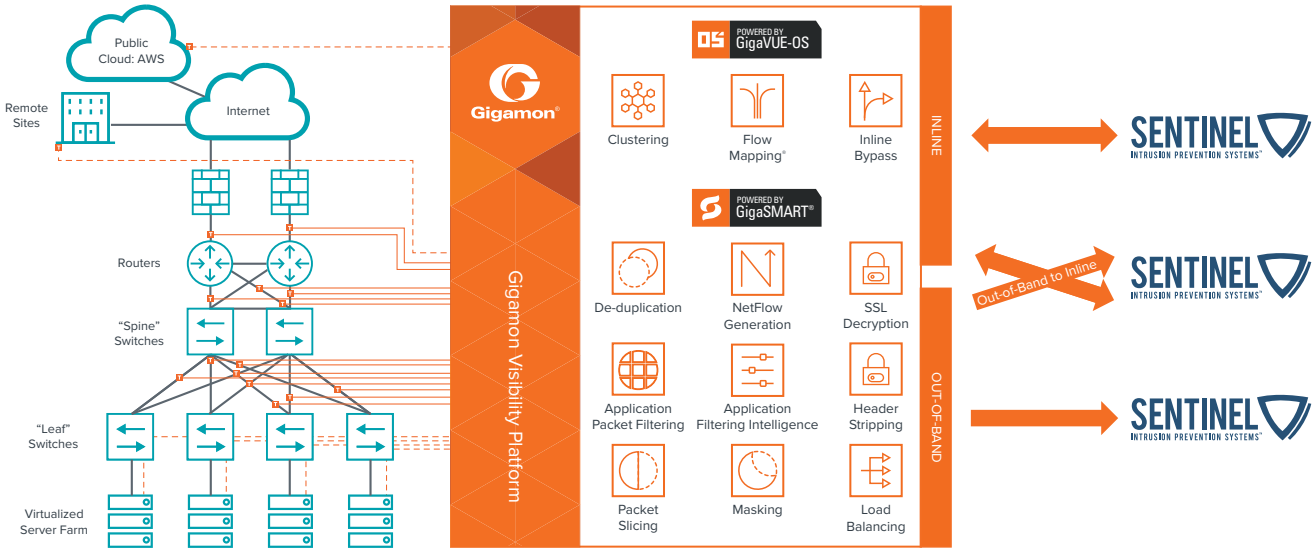

Figure 1: The Gigamon and Sentinel Joint Solution

For more information on Gigamon and Sentinel Intrusion Prevention Systems solutions, visit:
www.gigamon.com and https://sentinelips.com

Gigamon®
Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com