Gigamon® | Trellix

Boosting Threat Detection with Gigamon and Trellix

Overview

Today's cyber threats are stealthy, persistent, and increasingly leveraging lateral movement within hybrid environments. Traditional prevention mechanisms—NGFWs, IDS/IPS, and malware sandboxes—remain critical, but they are no longer sufficient on their own. Organizations require advanced detection and response that leverages real-time network intelligence and adaptive security analytics.

Together, Gigamon and Trellix offer a joint solution that enhances threat detection and response. By uniting Gigamon Deep Observability Pipeline and the Trellix AI-powered Security Platform, security teams can uncover threats hidden in encrypted traffic, understand attack context, and respond rapidly to incidents.

The Challenges

Security and visibility teams face several common challenges:

- Blind spots across lateral (East-West) traffic, IoT/OT, segmented networks, and hybrid environments
- Lack of incident context and impact due limited insight into network traffic
- High alert fatigue and false positives from siloed tools
- Difficulty detecting unknown threats or zero-days
- Delays in incident response due to fragmented telemetry
- Incomplete visibility into encrypted or containerized traffic
- Limited SOC resources stretched across disconnected workflows

The Solution

The Gigamon Deep Observability Pipeline captures and filters network traffic across physical, virtual, and cloud infrastructure. Using taps and visibility nodes, Gigamon provides comprehensive L2-L7 visibility, extracts essential network metadata, decrypts TLS traffic, and delivers enriched streams of intelligence to Trellix.

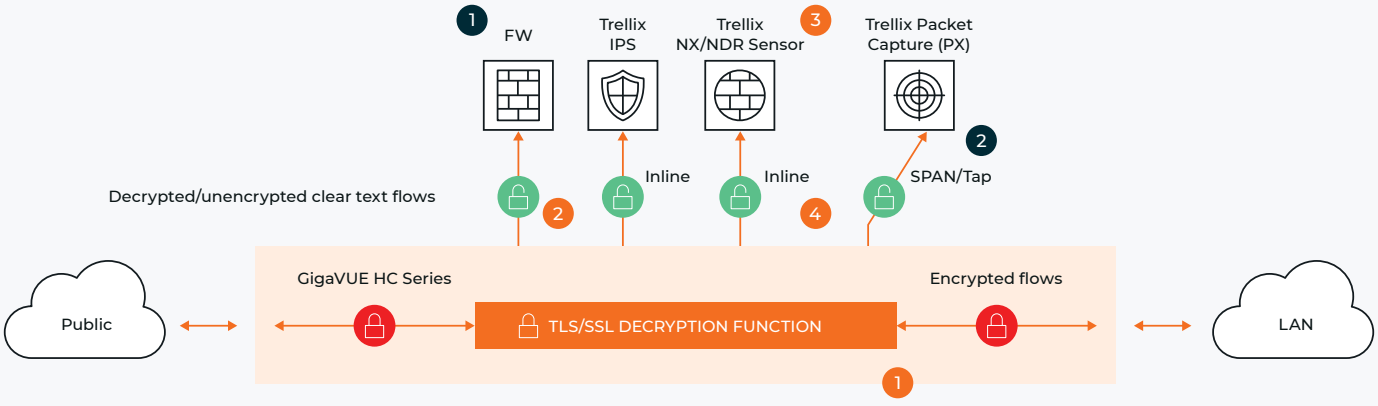
Trellix solutions receive this enhanced metadata and correlate indicators from various telemetry sources, including endpoint, network, email, and cloud sources to provide timely and precise threat detection. It applies machine learning and behaviour analytics to detect offensive tactics like lateral movement, privilege escalation, exfiltration, and other attack techniques. Trellix then prioritizes and visualizes threats for rapid analyst action—building resilience, reducing risk, and protecting against the latest cyber threats.

Key Features

- **Comprehensive Lateral (East-West) Visibility:** Enhance observability across cloud workloads, data centres, and container environments
- **Traffic Intelligence at Scale:** Extract close to 6,000 metadata attributes, including app protocols, user identities, and encryption states
- **Integrated Threat Detection:** Trellix correlates Gigamon network-derived telemetry and metadata with endpoint, perimeter security controls, IoT/OT, and cloud telemetry for high-fidelity detection and context
- **Encrypted Traffic Analysis:** Decrypt and analyse TLS/SSL traffic to detect concealed attacks without sacrificing privacy policies
- **Behavioural Analytics and Automation:** Trellix accelerates threat investigation and response using AI-driven prioritization

Key Benefits

- **Accelerated and Scalable Threat Detection:** Identify threats in real time—precise and timely detection across hybrid cloud, virtual machines, containers, IoT/OT environments, by leveraging network telemetry and metadata in encrypted and clear text traffic traversing in all directions (lateral, North-South, and Egress-Ingress)
- **Reduced Alert Fatigue:** Filter low-risk traffic before it reaches detection tools, enabling analysts to focus on critical threats
- **Faster Response Time:** Use automated, contextual insights to empower faster remediation and eliminate redundant traffic



TLS Challenges

1. Decrypting TLS traffic on each tool is prohibitively expensive and adds significant latency with inline tools
2. Passive TLS 1.3 decryption is not possible

Gigamon Delivers TLS Value

1. Decrypt once and feed different Trellix Sensors (NX/NDR/IPS/PX) with centralized decryption
2. Selectively decrypt inbound and outbound TLS flows
3. Increase efficiency, effectiveness, and coverage of security tools
4. Feed both inline and out-of-band tools, including security and application performance

Figure 1. Addressing the challenges of encrypted traffic using Gigamon and Trellix

- **Inspects Encrypted Traffic:** Decrypt SSL traffic for out-of-band inspection and analysis surfacing concealed C2 and exfiltration channels.
- **Protects against network outages:** Utilize inline bypass protection to maintain traffic continuity and minimize maintenance windows.
- **Cloud-Native Flexibility:** Support for multi-cloud, hybrid, and containerized deployments

Summary

- **Lower Total Cost of Ownership:** Ensure optimal performance and longevity of devices through load balancing across multiple devices, link consolidation, and filtering.
- **Reduce Noise:** Filter out traffic that doesn't need inspection for greater efficiency from your tool stack.
- **Avoid SPAN port contention:** Replicate a feed from the SPAN port or a tap to multiple tools using Gigamon, while also filtering feeds to only include relevant traffic for each tool.
- **Complete integration:** Integrate Gigamon and Trellix easily and scale quickly.

By adopting this joint solution, teams can overcome key obstacles to build an effective security posture. With comprehensive visibility, deep contextual understanding, and AI-driven automation, this partnership empowers organizations to proactively detect and respond to threats—even as IT environments grow more complex and adversaries become more advanced.

About Trellix

Trellix is redefining the future of cybersecurity and soulful work with its industry-leading products built on the broadest AI-powered security platform, securing organizations from advanced threats and strengthening operational resilience. Along with an extensive partner ecosystem, Trellix accelerates technology innovation through artificial intelligence, automation, and analytics, empowering over 53,000 customers with responsibly architected security solutions.

About Gigamon

Gigamon® offers a deep observability pipeline that efficiently delivers network-derived telemetry 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, 9 of the 10 largest mobile network providers, and hundreds of governments and educational organizations. To learn more, please visit gigamon.com.

For more information on Gigamon and Trellix please visit
gigamon.com | trellix.com

Gigamon®

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

08.25_01