Mitigate Threats Faster with Gigamon and Splunk

Overview

Organizations today face the daunting task of securing hybrid cloud infrastructure against an increasingly sophisticated threat landscape. New applications, IoT and OT devices, and rapidly evolving technologies expand the attack surface, yet current monitoring tools are limited in their ability to detect evolving threats.

Gigamon and Splunk together address this challenge by delivering deep observability into all data in motion. This joint solution provides complete visibility across hybrid cloud infrastructure, enabling faster detection, investigation, and response to changing security threats while reducing operational complexity and cost.

The Gigamon Deep Observability Pipeline acquires and processes network traffic, efficiently delivering network-derived telemetry such as packet, flow, and application metadata to security and observability tools. This enriched telemetry data helps organizations to eliminate blind spots, accelerate threat detection, and strengthen performance monitoring while reducing cost and complexity.

Gigamon uses deep packet inspection to extract rich metadata from network traffic across hybrid cloud infrastructure. Security and operations teams can leverage this network and application metadata (L2–L7) to add critical intelligence to their monitoring and security tools. With Gigamon Application Metadata Intelligence (AMI), organizations gain visibility into the applications communicating within lateral, East-West traffic, uncovering hidden risks and performance issues. This added layer of intelligence delivers insights that provide a deeper understanding of what is happening across the environment.

With Gigamon deep observability and Splunk advanced analytics, security teams can detect threats earlier, investigate faster, and respond with greater precision. The joint solution delivers actionable intelligence from both network and non-network sources, breaking down data silos to accelerate investigations and strengthen resilience. Customers also benefit from automated alerting, customizable investigations, and streamlined workflows that enhance compliance and audit readiness while driving greater business value from their security operations.

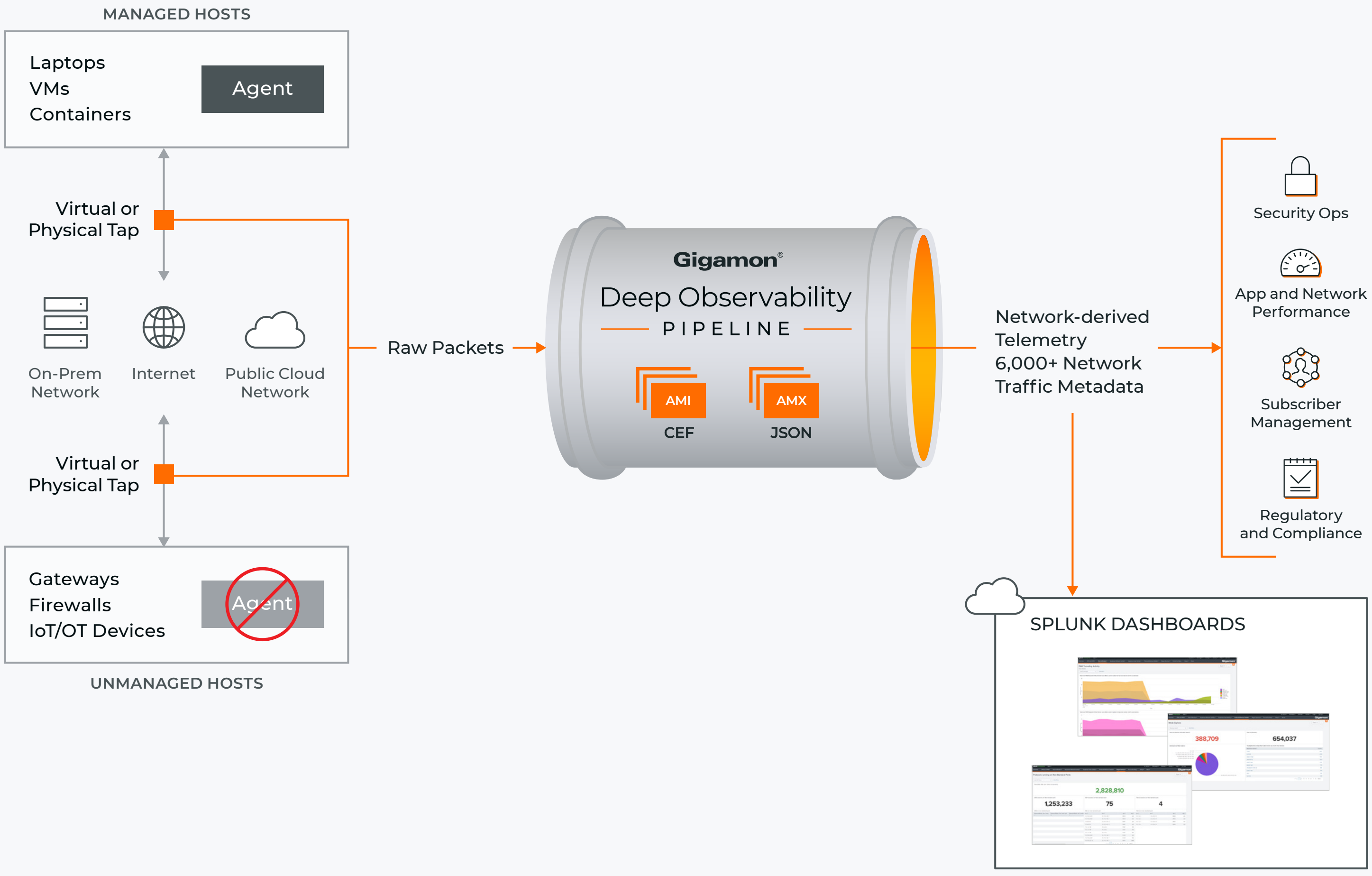
Challenges

Security teams are challenged by a myriad of different obstacles, including:

- Continuously changing hybrid cloud infrastructure creates network visibility blind spots.
- Noisy dashboards can result in information overload
- An inability to effectively secure lateral East-West traffic
- New risks and methods of attack from a threat landscape that is changing by the day
- Network logs that can't identify applications
- Reliance on outdated security systems, due to limited resources to invest in new solutions

The Solution

The Gigamon Deep Observability Pipeline delivers complete visibility across hybrid cloud infrastructure and adds critical intelligence to strengthen security posture. Splunk amplifies these capabilities with advanced analytics, enabling organizations to aggregate, analyze, and correlate network-derived telemetry from Gigamon with insights from diverse sources. Together, this unified approach empowers security teams to detect threats earlier, accelerate investigations, and make data-driven decisions that improve resilience and maximize business value.



Key Features

- Extract metadata from traffic based on application-related attributes to gain a deeper contextual view into what is occurring across your infrastructure
- Centralized observability into all lateral East-West traffic across on-premises, virtual, public cloud, and container environments
- Efficient delivery of network-derived telemetry to tools
- Visibility into the applications currently communicating across your network
- Centralized decryption to strengthen security posture with visibility into encrypted data
- Optimized telemetry data fed into Splunk to control information overload

Key Benefits

Here are a few examples of security use cases enabled by the joint Gigamon and Splunk solution:

- **Address DNS:** Monitor DNS traffic, identify rogue DNS servers, and assess external DNS server queries
- **Make logs application aware:** Combine intelligence received from logs with metadata extracted from network traffic to create dashboards that deliver deeper insights
- **Pinpoint applications and protocols:** Gain an understanding of known and unknown applications and protocols currently communicating across your infrastructure, like crypto mining, nonstandard port usage, FTP, SMBv1, and NTP
- **Compliance monitoring:** Continuous compliance monitoring, including detection of non-encrypted network traffic, non-compliant certificates, weak encryption, unauthorized users and applications, and more
- **Take control of decryption:** Enhance dashboards with access to decrypted traffic and identification of expired TLS/SSL certificates and any anomalous traffic
- **Secure IoT/OT devices:** Access and identify security risks in traffic going to and coming from IoT/OT devices
- **Fortify secure posture:** Enhance log-based monitoring with application intelligence to uncover lateral movement, identify source and destination locations, and expose vulnerable systems and compute resources targeted by malware

Supercharge Splunk Common Information Model (CIM)

Gigamon makes network log attributes application aware. This add-on facilitates the mapping of Gigamon-specific fields to the corresponding CIM data model, enhancing the overall visibility and comprehension of Gigamon-generated telemetry data within the Splunk platform. Examples of what can be mapped include:

- Certificate information, including expiry date
- TLS ciphers in use
- Applications and protocols
- Standard and nonstandard port usage

The Gigamon CIM data model enables organizations to achieve greater interoperability, reduce costs, improve data quality, and streamline operations, making it a crucial asset in complex and data-driven industries.

Leveraging Splunk Unified Data Management

By combining the Gigamon Deep Observability Pipeline with Splunk Edge Processor/Ingest Processor and Federated Search, organizations gain a unified data management architecture. This approach maximizes visibility, minimizes unnecessary data movement, enhances compliance, and ensures every team has access to the intelligence they need — wherever the data resides.

Summary

Gigamon and Splunk together give organizations deep observability and advanced analytics to eliminate blind spots, detect threats earlier, and respond with speed and precision. As hybrid cloud environments expand and threat actors grow more sophisticated, this joint solution strengthens security posture and puts organizations back in control.

Discover in Splunkbase

- Gigamon Deep Observability App (JSON)
- Gigamon Deep Observability App (CEF)
- Gigamon CIM

About Splunk

Splunk was founded in 2003 to solve problems in complex digital infrastructures. From the beginning, we've helped organizations explore the vast depths of their data like spelunkers in a cave (hence, "Splunk"). In 2024, Splunk was acquired by Cisco to help customers continue to build resilience across their entire digital footprint. Our purpose is to build a safer and more resilient digital world. Every day, we live this purpose by helping security, IT, and DevOps teams keep their organizations securely up and running. When organizations have resilient digital systems, they can adapt, innovate, and deliver for their customers. Resilience is a team effort. Let's build it together.

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 Splunk please visit Gigamon.com | Splunk.com

Gigamon®

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