Enhance Visibility and Security with Gigamon and Elastic

Deep Observability for Modern DevOps and API Security

Gigamon Deep Observability Pipeline combined with Elastic's AI-driven security analytics delivers unparalleled visibility and control over complex hybrid cloud environments. Together, they empower organizations to proactively secure their infrastructure, optimize application performance, and tackle API security challenges to help customers with OWASP compliance.

How It Works

Traffic Ingestion
Gigamon captures all network traffic across hybrid cloud infrastructures, including IoT devices, VMs, containers, and on-premises environments, through physical and virtual taps.

Gigamon Deep Observability Pipeline

- Performs deep packet inspection to extract actionable rich metadata.
- Filters and aggregates high-risk traffic to streamline insights.
- Sends traffic to Elastic for advanced analytics adding L2-L7 application aware context.

Elastic AI Security Analytics

- Provides dashboards with contextual intelligence for root cause analysis.
- Automates detection and remediation processes.

View integration details on elastic.co

Features

- **Unified Visibility**
  Monitor traffic across on-prem, virtual, cloud, and containerized environments.
- **Enhanced Metadata Extraction**
  Gain detailed insights into API behaviors, communication flows, and protocols.
- **Proactive Threat Detection**
  AI-driven identification of anomalies and lateral movements.
- **Scalable Delivery**
  Dynamically deliver filtered, context-rich data to multiple security tools.

Key Benefits

- **Eliminate Blind Spots**
  Detect lateral movement and expose blind spots in real-time.
- **Reduce False Positives**
  AI-powered analytics improve threat detection.
- **Streamline Security**
  Accelerate threat response with automated workflows.
- **Enhance Scalability**
  Scale seamlessly across hybrid environments without blind spots.

Key DevOps and API Security Use Cases

API Inventory Management

- Identify outdated API versions exposing sensitive data.
- Map API flows to detect and mitigate misuse or vulnerabilities.

Broken Access Control Prevention

- Pinpoint manipulated cookies or hidden fields elevating user privileges.
- Detect suspicious metadata manipulations indicative of privilege escalation attacks.

Infrastructure Monitoring and MTTR Optimization

- Analyze application and network round-trip times to isolate performance bottlenecks.
- Track application bandwidth and connection errors to maintain SLOs.
- Significantly reduce MTTD, MTTI and MTTR.

Threat Surface Reduction

- Detect unauthorized IoT device communications and rogue traffic.
- Identify non-standard port usage and protocol anomalies (e.g., crypto mining, SMBv1).

API Security Analysis

- Monitor user agents, response codes, and connections and maintain OWASP compliance.
- Analyze DNS queries for malicious domains and untrusted encryption certificates.

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.

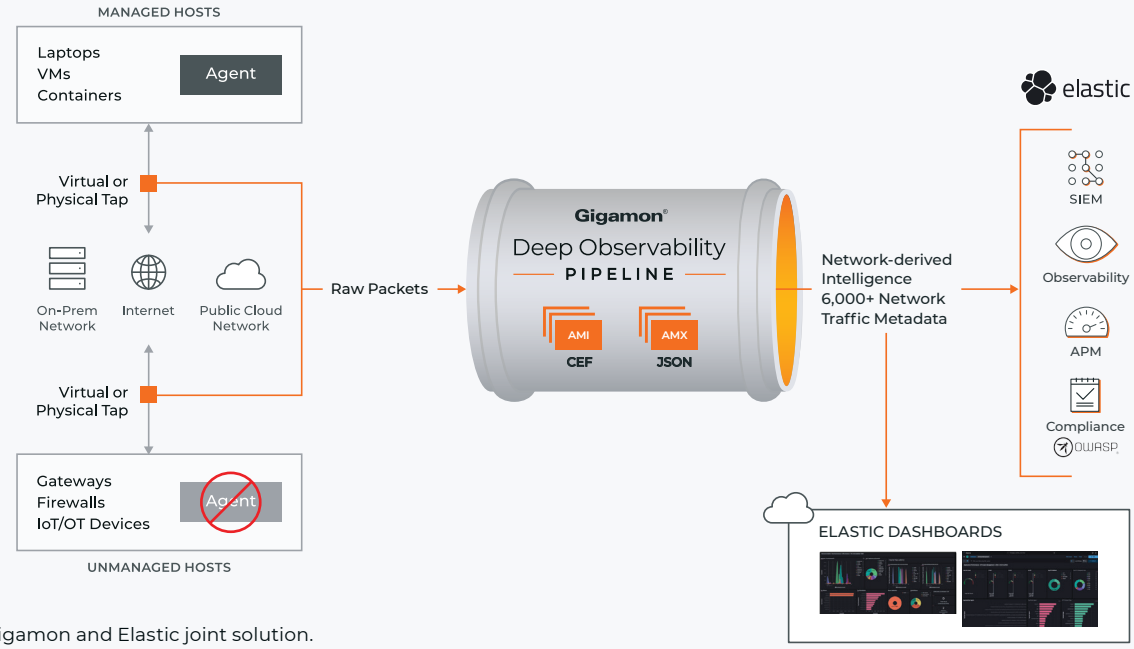

Figure 1. The Gigamon and Elastic joint solution.

Gigamon®

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

04.25_02