# Modernize Security, Observability, and APM with AI-Driven Security Analytics Powered by Deep Observability

## Overview

Organizations face the challenge of securing their complex hybrid cloud infrastructure from an ever-changing threat landscape. While dealing with this complexity, teams are forced to use outdated methods of understanding what is occurring in an infrastructure. Security solutions that lack the ability to provide actionable insights, complete visibility, environment-wide correlations, integrated threat intelligence, and real-time investigative capabilities all threaten an organization's ability to effectively address security issues.

Gigamon deep observability and Elastic's extensive machine learning (ML) capabilities together deliver enhanced AIOps while reducing false positives.

The Gigamon Deep Observability Pipeline accesses lateral network traffic across hybrid cloud infrastructure and sends copies of traffic simultaneously to all tools. This centralized approach to visibility lets you efficiently monitor and secure lateral traffic.

Gigamon also uses deep packet inspection to extract insightful metadata from network traffic. Teams use these capabilities to understand the applications currently communicating in lateral traffic and filter out low-risk traffic from the stream sent to tools. The contextual level of intelligence that can be extracted from traffic is what Gigamon refers to as deep observability.

This creates the opportunity to establish modernized security postures that simplify access to critical intelligence, limit the creation of blind spots, and focus resources on only high-risk traffic.

Elastic receives intelligence from Gigamon to help you detect threats, investigate the issue, and respond using AI-driven security analytics — giving you an unfair advantage against even the most sophisticated cyber threats. Strengthen the defenses of your security posture with a SIEM solution that provides real-time insights, expert-built detection rules, contextual dashboards, and AI. Teams can use AI provided by Elastic to explain alerts, suggest next steps, craft inquiries, and augment a group's expertise to address threats faster.

## The Challenge

Teams are challenged by a myriad of obstacles including:

- Constantly evolving infrastructures that create visibility blind spots
- Noisy dashboards that make you struggle with information overload
- Cost and complexity associated with supporting traditional SIEMs
- Inability to scale visibility and security postures fluidly
- Sole dependence on logs, which provides a limited view into what is occurring
- Use of systems that lack automation and orchestration

## The Solution

The Gigamon Deep Observability Pipeline communicates with taps sitting across a hybrid cloud infrastructure to access lateral traffic. Physical taps are used within physical data centers. Virtual taps are used in virtual environments like private cloud, public cloud, and containers.

Once lateral traffic is accessed by taps, a copy of the traffic is sent to GigaVUE® HC Series appliances in physical data centers or mirrored to GigaVUE Visibility Nodes in virtual environments for aggregation, deep packet inspection, and traffic filtering.

The GigaVUE HC Series and Visibility Nodes are then programmed to simultaneously present customized, filtered streams of intelligence to each tool being used for monitoring and security in a team's stack.

Once Elastic receives its customized stream of intelligence from Gigamon, it uses AI-driven security analytics to detect, investigate, and respond to security issues.

## Key Features

- Extract metadata from traffic based on application-related attributes to gain a deeper contextual view into what is occurring in your infrastructure
- Centralized visibility into all lateral traffic across on-premises, virtual, public cloud, and container environments

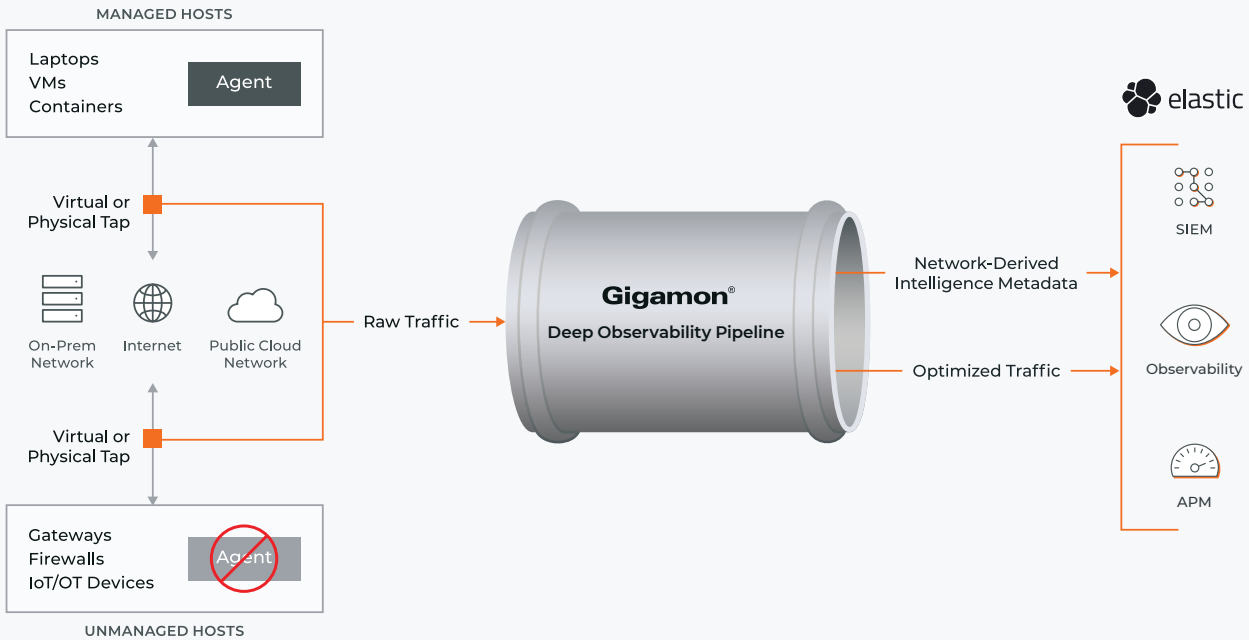


**Figure 1.** The Gigamon and Elastic joint solution.

- Simplified and scalable delivery of network-derived intelligence to tools
- Visibility into the applications currently communicating in your network
- Proactive threat detection, investigation, and response

## Key Benefits

The joint Gigamon–Elastic solution enable organizations to:

- **Complement log usage:** Combine intelligence received from logs with metadata extracted from network traffic to create dashboards that provide deep insights.
- **Enhance your API security:** Improper inventory management is on the list of top ten OWASP API security risks. Document all aspects of your APIs, such as user agents and response codes. Identify flows with old, unprotected API versions that could expose personal identifiable information (PII).
- **Prevent broken access control:** Broken access control remains the top concern on the OWASP top ten. Quickly identify broken access controls in your network and look out for metadata manipulation, such as cookies or hidden fields manipulated to elevate privilege, by gaining insights into the entire API Statistics.
- **Minimize mean time to resolution (MTTR):** Gain valuable network-related insights such as application round-trip time, network round-trip time, application bandwidth, and CRCs to minimize (MTTR), increase uptime, and enhance performance metrics while keeping your SLOs in mind.
- **Pinpoint applications and protocols:** Gain an understanding of known and unknown applications and protocols currently communicating in your infrastructure, including crypto mining, non-standard port usage, FTP, SMBv1, and NTP.
- **Analyze DNS with depth:** Identify DNS servers, response times of queries between client and servers, connections between client and server, and domain names being queried.
- **Take control of encryption:** Quickly identify expired TLS/SSL certs, monitor for untrusted certificates, efficiently identify their legitimacy, and understand if certificates were issued by a trusted Certificate Authority (CAs).
- **Simplify DHCP Monitoring:** Gain information to help you troubleshoot DHCP servers that are not responding. Understand how long a request is valid along with information on the messages being passed between the client and DHCP server.
- **Gain coverage in complex areas:** Gain visibility into unmanaged hosts like IoT devices, container-to-container communications, non-standard port usage, and suspicious traffic that is outside the norms.
- **Fortify secure posture:** Strengthen your existing security posture by complementing your current use of logs with application intelligence use cases, such as observation of lateral movement, geographic location of source and destination of traffic, vulnerable systems, and compute that can be targeted by malware.

## Gigamon Deep Observability Package on Elastic

To learn more about the integration between Gigamon and Elastic, visit the following website for more information: https://www.elastic.co/docs/current/integrations/gigamon

## Summary

Gigamon deep observability and Elastic's extensive ML capabilities together deliver enhanced AIOps while reducing false positives.

Teams can now adequately address current challenges that impede them from creating an effective security posture by implementing a joint solution that gives them complete visibility, a deeper understanding of what is occurring, and the ability to identify issues faster through the power of AI.

Put your organization in control even as infrastructures become more complex and threat actors become more sophisticated.

## About Elastic

Elastic is the leading platform for search-powered solutions, and they help everyone — organizations, their employees, and their customers — find what they need faster, while keeping applications running smoothly, and protecting against cyber threats.

When you tap into the power of Elastic Enterprise Search, Observability, and Security solutions, you're in good company with brands like Uber, Slack, Microsoft, and thousands of others who rely on them to accelerate results that matter.

## 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, 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 Elastic please visit

**gigamon.com | elastic.co**

Gigamon®

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



11.24_02