Build a Stronger Security Posture Today with Deep Observability and AI

Member of Microsoft Intelligent Security Association

Microsoft Security

Introduction

Organizations face a series of obstacles in securing hybrid cloud infrastructure from today's ever-evolving landscape of cyberthreats. Threat actors continue to gain in sophistication as hybrid cloud infrastructure becomes increasingly complex as new applications and IoT/OT devices are introduced. A lack of consistent investment in modernizing monitoring and security tools has left organizations in a precarious position in the battle to secure their infrastructure and organization.

Gigamon and Microsoft Sentinel provide a joint solution that enables IT teams to strengthen their security posture by leveraging deep observability and AI.

The Gigamon Deep Observability Pipeline accesses network traffic across hybrid cloud infrastructure, including lateral and encrypted traffic, and efficiently delivers network-derived intelligence and insights to an organization's cloud, security, and observability tools.

This centralized approach to accessing traffic provides organizations with the deep observability they need to efficiently monitor and secure network traffic.

Gigamon also uses deep packet inspection to extract insightful metadata from the accessed traffic. Teams use these capabilities to understand the applications currently communicating laterally within an organization and filter out duplicate and low-risk traffic from the stream sent to tools. This contextual level of intelligence is extracted from traffic and integrated with metric, event, log, and trace data to provide organizations with a complete picture. This powerful combination is what Gigamon refers to as 'deep observability.'

This creates the opportunity for organizations to strengthen their security posture by simplifying access to critical intelligence, limiting the creation of blind spots, and focusing resources on high-risk traffic.

Microsoft Sentinel receives this network-derived intelligence from Gigamon and incorporates built-in AI to analyze large volumes of data from many different sources to produce behavioral analytics that help organizations gain the upper hand and stay ahead of evolving threats. With Microsoft Sentinel, you can now accelerate proactive threat hunting with pre-built queries, investigate threats, hunt suspicious activities at scale leveraging decades of cybersecurity work at Microsoft, accelerate threat response with integrated automation of common tasks, and simplify workflows.

Challenges

IT teams are challenged by a myriad of different obstacles including:

- Continuously evolving infrastructures that create visibility blind spots
- Noisy dashboards that make you struggle with information overload
- Escalating cost and complexity of supporting traditional SIEMs
- Inability to scale visibility and security postures fluidly
- Overreliance on log-based data exposes teams to false results as traditional logs can be manipulated
- Usage of systems that lack automation and orchestration

The Solution

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

Once lateral traffic is acquired by taps, a copy of the traffic is efficiently delivered to either 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 tool stack.

Once Microsoft Sentinel receives its customized stream of network-derived intelligence from Gigamon, it is collected along with other data to detect, investigate, and respond to incidents rapidly before and after they have occurred.

Key Features

- Extract metadata from traffic based on application-related attributes to gain a deeper contextual view into what is occurring across your hybrid cloud infrastructure
- Centralized visibility into all lateral and encrypted traffic across on-premises, virtual, public cloud, and container environments
- Efficient and scalable delivery of network-derived intelligence to tools
- Visibility into the applications currently communicating across your network
- Proactive threat detection, investigation, and response
- Visibility into Layer 7 application protocols currently running that 5-tuple log analysis does not provide

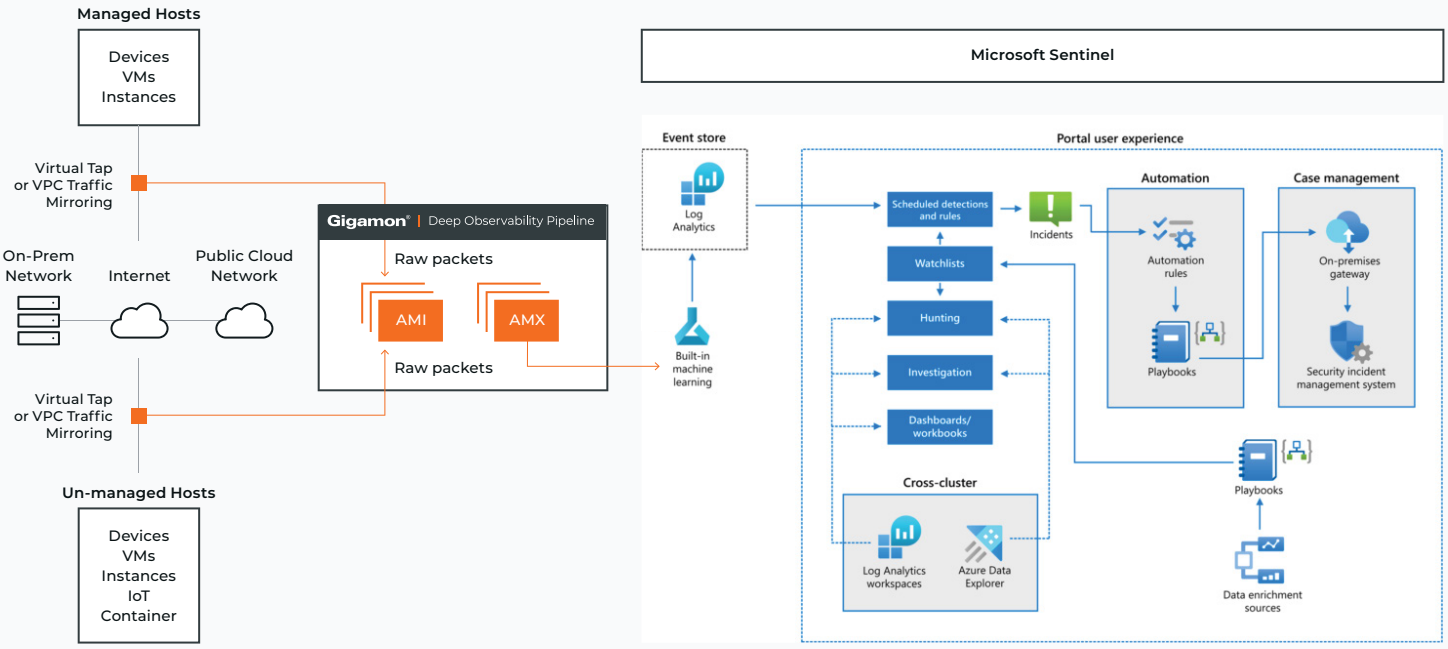

Figure 1. Gigamon accesses network traffic from all sources, extracts network-derived attributes, and sends Microsoft Sentinel for further analysis, exploration, and enrichments.

Key Benefits

Here are a few security use cases enabled by the joint Gigamon–Microsoft Sentinel solution:

- **Secure past 5-tuple analysis:** Combine existing 5-tuple based security analysis (source/destination ip, source/destination port, and network protocols) with layer 7 application protocol visibility provided by Gigamon network-derived intelligence
- **Pinpoint applications and protocols:** Gain an understanding of known and unknown applications and protocols currently communicating across your hybrid cloud infrastructure, including crypto mining, non-standard port usage, FTP, SMBv1, and NTP
- **Leverage years of knowledge:** Take advantage of data compiled over decades at Microsoft to expedite identification of threats and their severity.
- **Take control of encryption:** Quickly identify expired SSL/TLS certificates, monitor for non-trusted certificates, efficiently identify and validate their legitimacy, and understand if certificates were issued by a trusted Certificate Authority (CAs)
- **Gain coverage in complex areas:** Gain visibility into unmanaged hosts like IoT devices, container-to-container communications, non-standard port usage, and unusual or suspicious traffic
- **Proactively secure your infrastructure:** Leverage AI to quickly identify anomalous traffic to identify threats and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft
- **Strengthen your security posture:** Strengthen your existing security posture by complementing your current use of logs with network and 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

Start Securing Now

The Gigamon and Microsoft Sentinel joint solution comes with the ready-for-use Gigamon Data Connector for Microsoft Sentinel. With this integration, teams can focus their time on proactively identifying security issues and less on dealing with the traditional headaches associated with integration.

Summary

Gigamon plus Microsoft Sentinel helps you strengthen your security posture today with deep observability and AI.

IT teams can now proactively address current challenges that impede them from creating an effective security posture by implementing a joint solution that provides complete visibility, a deeper understanding of what is occurring, and the ability to proactively identify and respond to threats before they take down an organization or its hybrid cloud infrastructure.

Put your organization in control even as hybrid cloud infrastructure becomes more complex and threat actors become more sophisticated.

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 Microsoft Sentinel please visit Gigamon.com or search Gigamon Data Connector in the Azure Marketplace.

Gigamon®

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

10.24_01