Gigamon® | Google SecOps

Unleash Deep Observability and Proactive Security with Gigamon and Google SecOps

Overview

Organizations struggle to secure hybrid cloud infrastructure as threat actors continue to grow more sophisticated and infrastructures expand to include new applications and IoT/OT devices. 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 Google SecOps provide a joint solution that allows teams to build a next-generation security posture based on deep observability and AI.

Experience complete visibility and advanced threat detection across your hybrid and multi cloud environments. The integration between Gigamon and Google SecOps empowers your security teams with actionable network telemetry, real-time analytics, and automated response—eliminating blind spots and accelerating incident resolution for a stronger, more resilient security posture.

The Gigamon Deep Observability Pipeline accesses ingress, egress, and lateral traffic across hybrid cloud infrastructure and sends copies of traffic simultaneously to all tools. This centralized approach to accessing visibility lets you efficiently monitor and secure traffic in any direction.

Gigamon also uses deep packet inspection to extract insightful metadata from accessed traffic. Teams use these capabilities to understand the workloads currently communicating in all directions, specifically in lateral traffic where attackers typically move into more valuable cloud resources once the initial access stage has been achieved. In addition, Gigamon can filter out low-risk traffic from the data sent to tools enhancing their threat detection capabilities and performance. 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 security postures that simplify access to critical intelligence, limit the creation of blind spots, and focus resources on only high-risk traffic.

As organizations accelerate their adoption of hybrid and multicloud environments, the complexity and scale of security operations grow exponentially. Google SecOps, as a cloud-native security operations platform, empowers security teams to detect, investigate, and respond to threats with speed and precision. By integrating with the Gigamon Deep Observability Pipeline, Google SecOps customers gain complete visibility into all network traffic—across on-premises, cloud, and containerized workloads—enabling more effective threat detection, compliance, and operational efficiency.

The Solution

Google SecOps delivers a unified security operations experience, combining SIEM, SOAR, and threat intelligence for streamlined detection, investigation, and automated response. The platform features curated and continuously updated detections, AI-powered search and playbook creation, and orchestration across hundreds of security tools. The Gigamon Deep Observability Pipeline extends Google SecOps' reach by acquiring, processing, and optimizing network-derived telemetry from any environment. This integration ensures that Google SecOps receives comprehensive, real-time visibility into all data-in-motion, including encrypted, egress, ingress, lateral and container traffic, without the need for additional agents or tool sprawl.

Key Benefits

1. Eliminate Blind Spots in Hybrid and Multicloud

- Gigamon enables Google SecOps to access full packet, flow, and application-level visibility across GCP, other clouds, and on-premises environments.
- Visibility extends to encrypted and lateral traffic, ensuring threats cannot hide in lateral or containerized communications.

2. Accelerate Threat Detection and Response

- Actionable, network-derived telemetry feeds directly into Google SecOps, empowering faster, more accurate detections, and investigations.
- Google SecOps' SOAR capabilities automate response actions, leveraging enriched Gigamon data to reduce mean time to respond (MTTR).

3. Consistent Security and Compliance

- Use familiar Google SecOps workflows and tools to monitor all workloads, ensuring a unified security and compliance posture across hybrid and multicloud deployments.
- Get context and plaintext visibility for compliance and support all stages of all incident response frameworks with Gigamon Application Metadata Intelligence and Gigamon Precryption™.

4. Operational Efficiency and Scalability

- Gigamon optimizes and filters traffic before it reaches Google SecOps, reducing unnecessary data and improving tool efficiency by up to 90 percent.
- Elastic scalability and automated workload discovery ensure security coverage keeps pace with dynamic cloud environments.

Solution Architecture

Component	Role in the Solution
Google SecOps	SIEM, SOAR, and threat intelligence for detection, investigation, and response
Gigamon Deep Observability	Performs Deep Packet Inspection and delivers optimized network intelligence to SecOps
Gigamon and GigaVUE Cloud Suite™	Ensures visibility across GCP, other clouds, and on-premises infrastructure

Use Cases

- **Unified Threat Detection:** Detect advanced threats and lateral movement across hybrid and multi-cloud with enriched network intelligence.
- **Compliance Monitoring:** Ensure continuous compliance by providing deep, auditable visibility into all network activity.
- **Operational Agility:** Accelerate cloud migration and scale security operations without adding tool complexity or overhead.

Why Google SecOps and Gigamon?

- **Complete Visibility:** See every packet, flow, and application—across all environments—for truly proactive security.
- **Efficient, Automated Response:** Leverage Google SecOps' automation and playbook capabilities with Gigamon network-derived telemetry and insights.
- **Scalable Security for Dynamic Workloads:** Support for dynamic, containerized, and hybrid workloads ensures your security operations are ready for tomorrow's challenges.

Summary

By integrating the Gigamon Deep Observability Pipeline with Google SecOps, organizations gain real-time, actionable visibility across hybrid and multi-cloud environments. This integration improves threat detection, accelerates response, and simplifies compliance all while reducing operational complexity.

Security teams are empowered to act faster, focus on high-risk traffic, and support dynamic cloud environments with confidence.

About Google Cloud

Google Cloud is the new way to the cloud, providing AI, infrastructure, developer, data, security, and collaboration tools built for today and tomorrow. Google Cloud offers a powerful, fully integrated, and optimized AI stack with its own planet-scale infrastructure, custom-built chips, generative AI models and development platform, as well as AI-powered applications, to help organizations transform. Customers in more than 200 countries and territories turn to Google Cloud as their trusted technology partner.

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 Google SecOps, please visit gigamon.com | cloud.google.com

Gigamon®

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

07.25_01