

Gigamon Hawk Deep Observability Pipeline

Get a Higher Level of Security and Compliance Assurance for Your Hybrid Cloud

Enterprises are shifting to hybrid cloud deployments as they march towards modernizing applications and infrastructures. While more applications are migrated to various public clouds, many will remain on-premises for the foreseeable future. Unfortunately, a distributed multi-vendor architecture also brings complexity. IT teams may struggle to maintain a consistent security and compliance posture. Troubleshooting and resolving issues takes that much longer.

That's where the Gigamon Hawk deep observability pipeline comes in. We simplify complex network environments, so you can regain control. Now you can extend the value of familiar cloud or on-premises tools, processes, and procedures to secure your cloud workloads, plus set up common policies no matter where workloads reside.

Gigamon helps secure your hybrid environment by eliminating network blind spots and complementing metrics, events, logs, and traces (MELT) with actionable network-level intelligence. By providing information extracted through deep packet inspection, Gigamon Hawk brings additional security use cases to your current set of SIEM, APM, and observability tools. These include 1) discovering assets and API communications over the network, 2) identifying managed or unmanaged hosts using weak ciphers or expiring TLS certificates, and 3) detecting unauthorized activities such as crypto mining.

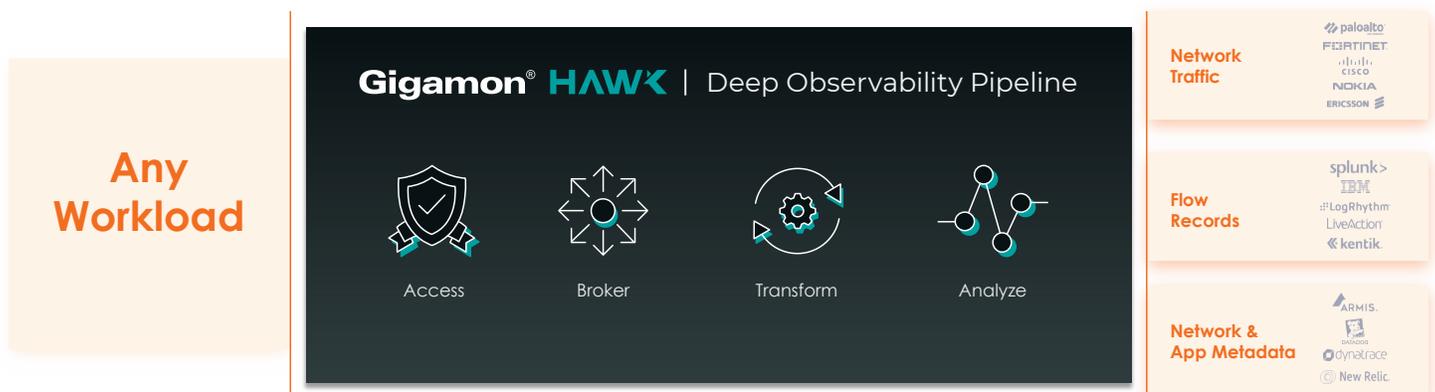


Figure 1: Gigamon Hawk deep observability pipeline acquires data-in-motion from any source and sends actionable network-level intelligence to any security or observability tool.

	FEATURES	BENEFITS
Access	Traffic acquisition from any VM, container, or physical network infrastructure; Gigamon Automatic Target Selection dynamically adapts to changes in VM or container instances and locations	Easily obtain full visibility into East-West, North-South, and container traffic across your hybrid cloud environments, and ensure continued visibility as cloud deployments scale up or down
Broker	Send network traffic packets or metadata to any security, observability, or monitoring tool running on any platform	Gain on-prem level of security and compliance governance, and accelerate migration to clouds by reusing existing monitoring and security infrastructure
Transform	Filtering, packet de-duplication, advanced flow slicing, load balancing, and NetFlow generation	Significantly reduce tool costs while boosting tool efficiency and effectiveness
Analyze	Application Metadata Intelligence, with more than 5,000 traffic-protocol and application-related metadata attributes, for your SIEM and observability tools	Detect anomalies faster and speed root-cause analysis of security incidents and performance bottlenecks
Manage	Unified visibility management and orchestration via GigaVUE-FM fabric manager or native DevOps approaches	Reduce operational overhead associated with managing hybrid and multi-cloud infrastructures

Accelerating Your Cloud Adoption

How can you ensure that your applications and services stay secure as you ramp up cloud migration? For security assurance and effective security governance, you need consistent visibility across all environments.

Modernizing infrastructure and applications also entails big changes that require IT organizations to adapt. However, change management takes time. We buy you time because teams no longer need to refactor security and monitoring infrastructure for new cloud deployments on day one. Instead, they can rely on familiar, proven datacenter tools, processes, and procedures. Using existing tools not only saves time and money, but helps you achieve a consistent security and compliance posture.

With Gigamon Hawk, you can realize the full transformational promise of the cloud. Address security and operational issues that slow digital initiatives and leave your organization vulnerable to threats and breaches.

With Gigamon, you can:

- + Confidently migrate applications to the public cloud while meeting stringent compliance and security requirements
- + Consolidate your security and observability tool stack with solutions of your choice
- + Move to a proactive security posture in the cloud that isn't possible with current MELT approaches
- + Monitor unmanaged hosts/endpoints and IoT devices, which don't produce logs
- + Speed root-cause analysis and troubleshooting by getting a bigger picture of what happened
- + Unify visibility management across all infrastructures and easily map and filter traffic to tools

The Solution

Gigamon Hawk deep observability pipeline extends the value of your existing cloud security and observability tools with real-time network intelligence derived from packets, flows, and application metadata. For the first time, you can add a new layer in your defense-in-depth with full packet visibility and the ability to feed network-level intelligence to your current security and observability tools.

The solution consists of:

- + GigaVUE® Cloud Suite with GigaVUE V Series visibility nodes and virtual G-vTAPs for traffic acquisition, processing, and forwarding within virtual and container infrastructures
- + GigaVUE HC/TA physical appliances and physical G-TAPs for traffic acquisition, processing, and forwarding within physical infrastructures
- + GigaVUE-FM fabric manager for unified management of Gigamon Hawk across hybrid and multi-cloud infrastructures
- + GigaSMART® applications — such as SSL/TLS decryption, de-duplication, and Application Metadata Intelligence — improve tool efficiency and visibility

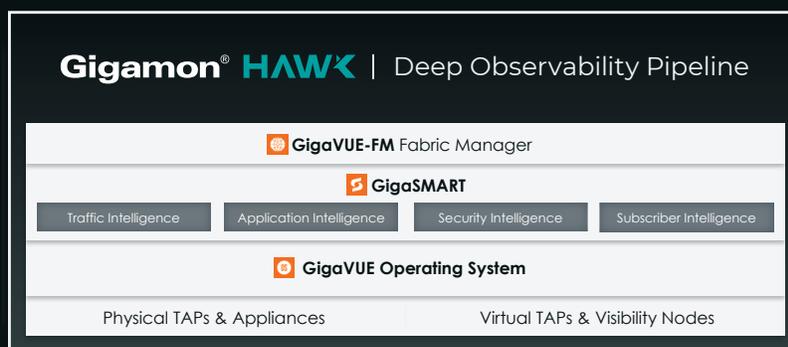


Figure 2: Gigamon Hawk components for both physical and cloud infrastructures.

Traffic Intelligence

Key benefits:

- + Reduce traffic by more than 50 percent by removing duplicate packets that result from network switch mirror/SPAN ports, multiple TAP points, or multiple virtual mirroring sources
- + Remove or truncate packets or flows, resulting in 75 percent or more reduction in traffic forwarded to tools
- + Gain visibility into SSL/TLS encrypted traffic, including TLS 1.3 encrypted flows
- + Comply with data privacy rules with data masking
- + Remove unwanted tagging and encapsulation, increasing effectiveness and efficiency of your tools
- + Tunneling support for virtual traffic sources, multi-site interconnection, and forwarding to virtual tools

Application Intelligence

Key benefits:

- + Identify all applications running in your cloud and physical infrastructures — including shadow IT and other unauthorized apps
- + Filter out or focus on specific applications within user traffic, making your monitoring and security more effective and efficient
- + Generate rich application metadata to feed monitoring and security tools that can't ingest raw packets
- + Create video data records for video analytics tools (e.g., Nokia AVA's PVA) without the need for separate probes

Subscriber Intelligence

Key benefits:

- + Filter, safelist, and/or sample 3G, 4G, and 5G control and user-plane sessions, focusing on only the traffic of importance
- + Balance 3G, 4G, and 5G loads across multiple instances of the same tool
- + Filter, safelist, and/or sample SIP signaling and RTP data sessions, focusing on only the traffic of importance
- + Balance SIP and RTP loads across multiple instances of the same tool

Security Intelligence

Key benefit:

- + Generate threat metadata intelligence for Gigamon ThreatINSIGHT™ network detection and response (NDR)

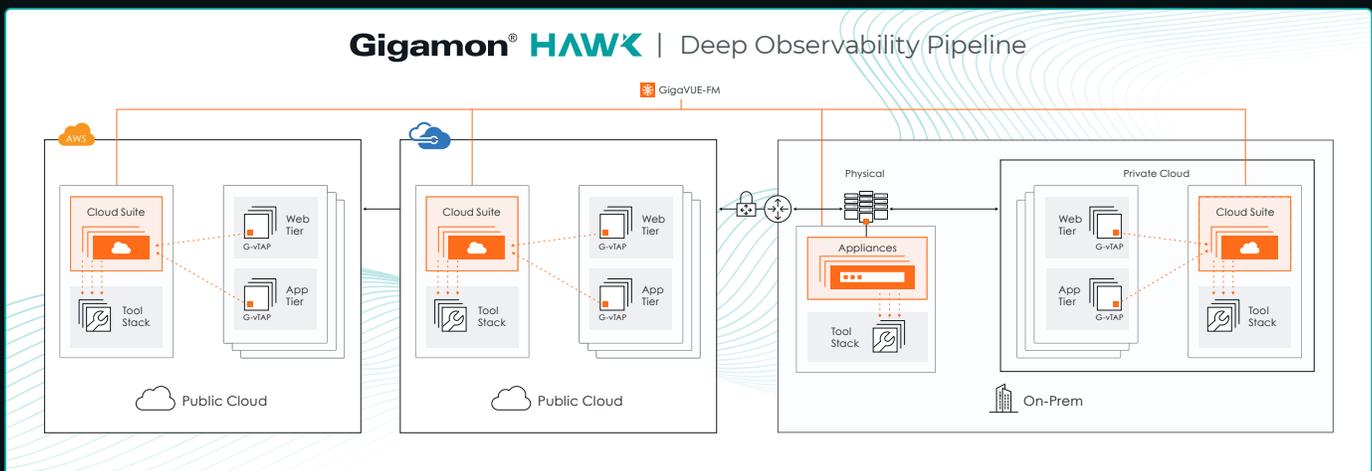


Figure 3: Hybrid cloud deployment with Gigamon Hawk

Conclusion

Gigamon Hawk lets you enjoy the agility and resiliency benefits of hybrid and multi-cloud infrastructures while driving down security and non-compliance risks. Our deep observability pipeline harnesses network-level intelligence to amplify the capabilities of observability tools. This powerful combination of network intelligence with MELT data enables IT organizations to assure security and compliance governance, speed root-cause analysis, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures. The result: Your organization realizes the full transformational promise of the cloud.



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

© 2022 Gigamon. All rights reserved. Gigamon and the Gigamon logo are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners. Gigamon reserves the right to change, modify, transfer, or otherwise revise this publication without notice.