Gigamon Hawk Cloud Visibility and Analytics Fabric

Unified network monitoring and security for all infrastructures

As network operations move from monolithic physical appliance deployments to self-managed virtual private hosts, and as application developers move from on-prem self-hosted implementations to public cloud, the ability to sufficiently manage and secure the networks and applications becomes harder and harder. Just as operators of physical networks learned in the 1990s and 2000s, simply relying on log files and other data from the network functions and applications themselves is unreliable and requires constant development as functions and apps change or are upgraded. This is where Gigamon Hawk comes in.

The first true network visibility fabric for hybrid physical, private and public clouds. (See Figure 1)

KEY FEATURES

- Traffic acquisition from any virtual machine, container and physical network infrastructure
- Core intelligence for aggregating, replicating, tagging, filtering and distributing traffic to monitoring and security tools
- Unified orchestration via DevOps approaches and single-pane-of-glass fabric management
- RESTful APIs for integration with tools and cloud infrastructures

KEY BENEFITS

- Full visibility into network traffic across your hybrid cloud and monolithic hardware environments
- Reduced complexity and cost, and improved efficacy, of your monitoring and security solution without sacrificing coverage
- Reduction in application downtime
- Discovery of new workloads, proper directing of traffic and adjustment of the visibility tier – all without manual intervention

Successful Cloud Operations Means Covering All Networks

In the face of digital transformation that's occurring at an increasing rate, network and security operations face significant challenges. How can you, for example, maintain continuous operations and ensure security of your networks, services and applications across the hybrid mix of public cloud-hosted applications and on-prem infrastructure and applications?

Whether it's workloads in the public cloud, a self-managed private cloud datacenter or a physical datacenter, continued operation, security and compliance of network data and applications rests on IT teams who must ensure that it is all deployed securely and performs as required. To automatically and proactively identify and remediate security and performance limitations, you must have accurate and comprehensive visibility into all network environments.

CRUCIAL CONSIDERATIONS

IT, cloud and security architects need to address the following questions when planning any network migrations or expansions:

+ How do I assure that everyone in the enterprise uses the network and applications securely?
+ How do I migrate applications to the public cloud while meeting the needs for compliance and security controls?
+ If zero-day security vulnerabilities are exploited in unpatched software, what mechanisms do I have to detect them?
+ How do I detect and respond to security or network anomalies while deploying new applications or upgrading existing applications?
+ How can I get a consolidated view across all infrastructures with my monitoring and security tools?
+ Are there effective methods to reduce the cost of backhauling traffic when the tools monitoring traffic in the cloud are on-premises vs. part of a tool tier in the cloud?
+ How do I overcome limitations of public cloud traffic mirroring and peering, particularly in the face of high data-egress charges?

Not addressing these considerations slows the migration of applications and services to private and public clouds — and leaves you vulnerable to potential security breaches.

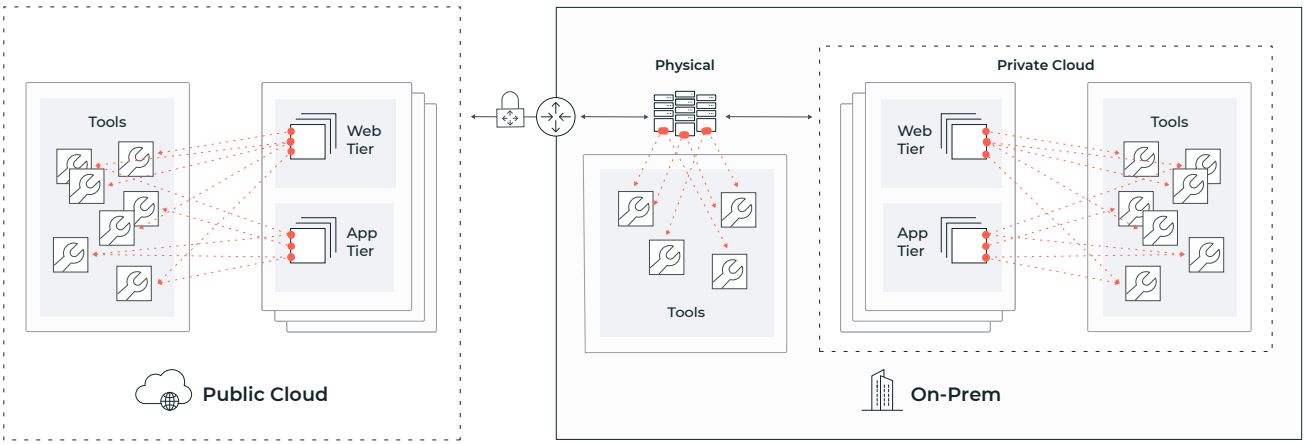

Figure 1. An enterprise hybrid network without Gigamon Hawk.

The Solution

Gigamon Hawk offers intelligent packet and flow brokering capabilities, via a simple business model, to help increase security, operational efficiency and scale across hybrid network infrastructures. It enables NetOps and InfoSec teams to maximize visibility for network monitoring and security and to get the most out of their new and existing tools, where even existing physical tools can be used for on-prem private cloud.

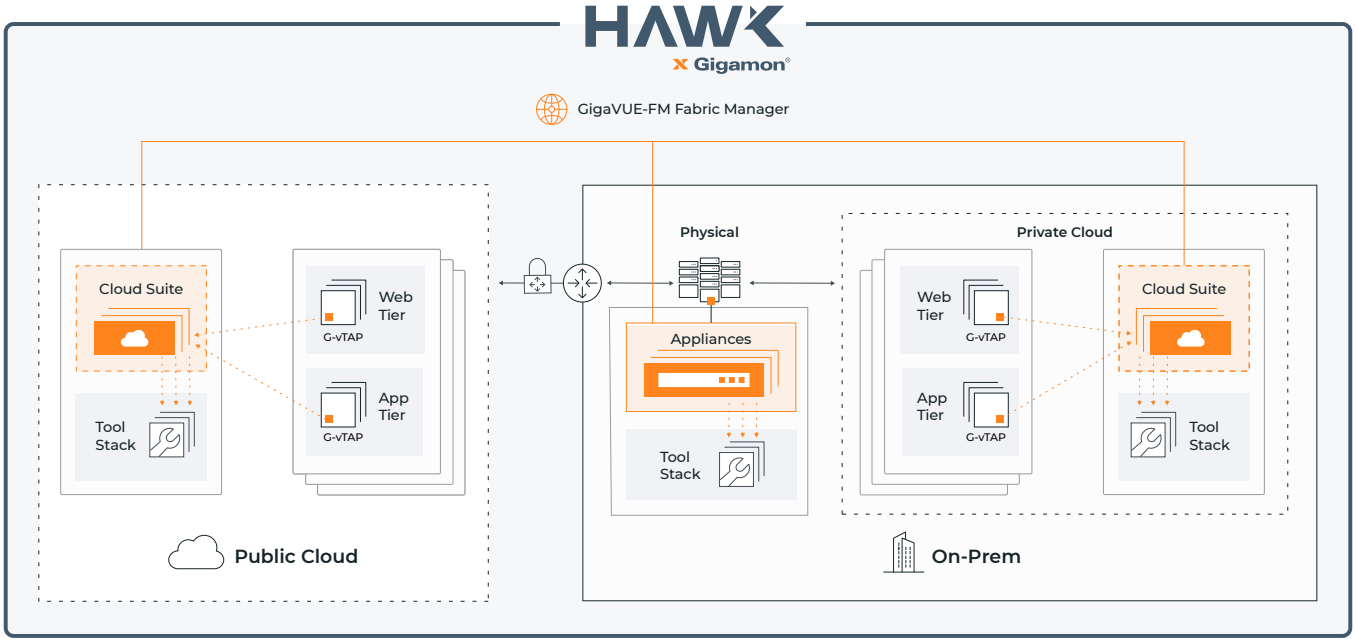

Figure 2: An enterprise hybrid network with Gigamon Hawk.

The solution consists of:

+ GigaVUE® Cloud Suite, with GigaVUE V Series visibility nodes and G-vTAPs, to provide traffic acquisition, processing and forwarding within virtual and container infrastructures
+ GigaVUE physical appliances, with GigaVUE HC/TA Series and G-TAPs, to provide traffic acquisition, processing and forwarding within physical infrastructure
+ GigaVUE-FM to provide single-pane-of-glass unified management of the visibility and analytics fabric across all infrastructures

TRAFFIC INTELLIGENCE

Key benefits:

+ Remove duplicate packets that result from network switch mirror/SPAN ports, multiple TAP points or multiple virtual mirroring sources, which can reduce monitoring traffic by more than 50 percent
+ 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,
+ thereby 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:

+ Ignore or focus on specific applications within user traffic, making your monitoring and security more effective and efficient
+ Generate rich metadata for applications to feed monitoring and security tools (e.g. SIEMs) that don't ingest actual raw packets
+ Generate video data records for video analytics tools (e.g. Nokia AVA's PVA), without the need for separate probes

SUBSCRIBER INTELLIGENCE

Key benefits:

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

SECURITY INTELLIGENCE

Key benefit:

Generate threat intelligent metadata for the Gigamon ThreatINSIGHT™ network detection and response (NDR) tool.

Conclusion

Whether your organization's operations are predominantly in the cloud, on-prem or an even mix of both, Gigamon Hawk provides intelligent network traffic visibility for applications and services running across your hybrid cloud. Unified management streamlines deployment of an all-encompassing visibility tier that aggregates traffic and applies advanced intelligence prior to sending selected traffic to monitoring and security tools. With Gigamon Hawk, you can finally obtain consistent insight into your infrastructure across public clouds and on-premises environment.

CSPi Technology Solutions

CSPi Technology Solutions, a Gigamon Authorized Reseller, provides the expertise and service scope - including Managed IT Services, Professional Services, and Cloud Services - to help our clients architect and manage a high-performance, highly available, and highly secure IT infrastructure.

For more information on Gigamon Hawk, visit cspitechsolutions.com.

Gigamon®

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

07.21_02