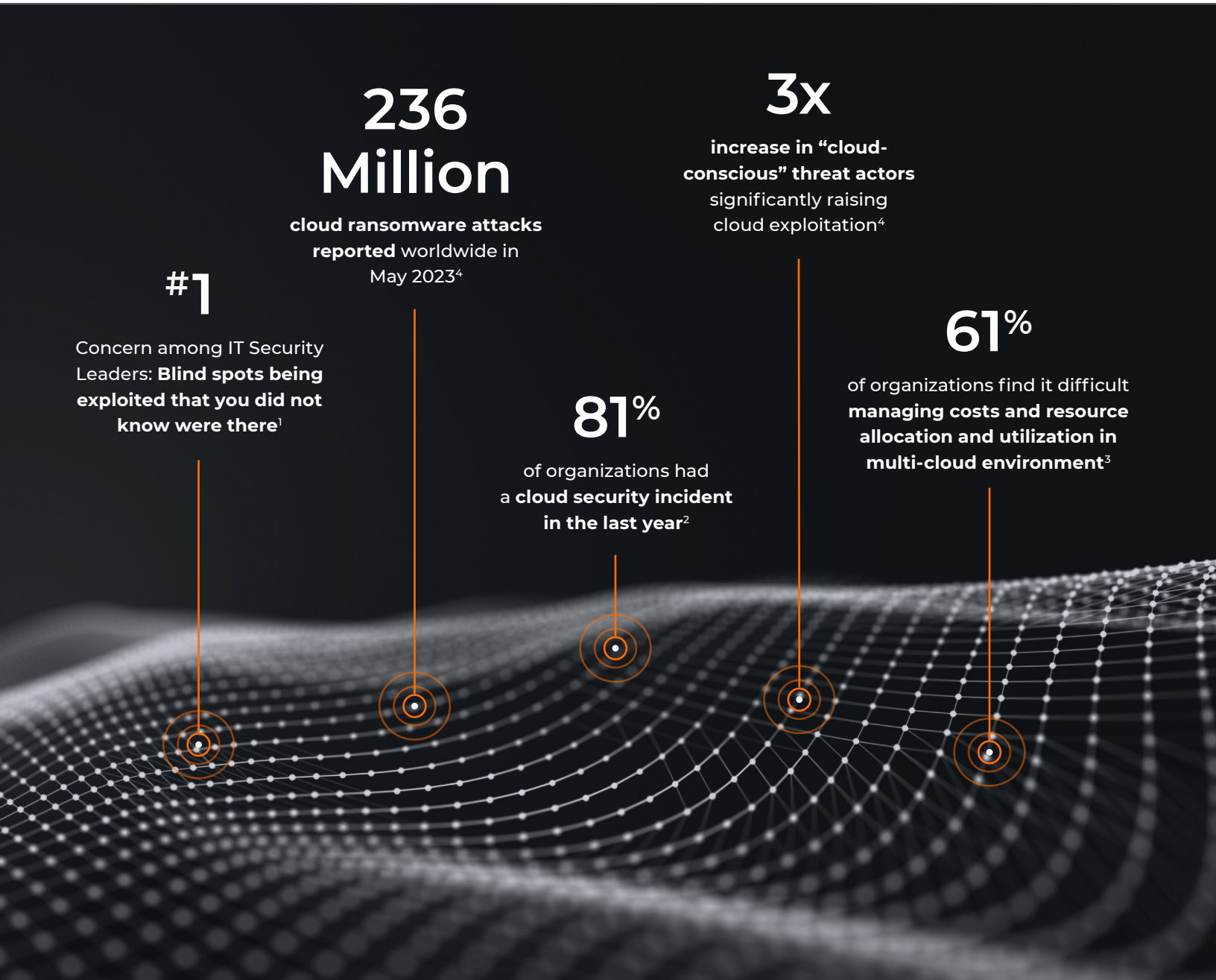
GigaVUE Enriched Metadata for Cloud Workloads

Bring hidden threats into focus with clarity and speed, improving threat detection and incident response using network telemetry enrichment.



Organizations are exposed to proliferating cyber threats with threat actors capitalizing on blind spots created from siloed security and disparate tool architectures used to secure and manage hybrid cloud infrastructure. These security blind spots lead to a lack of awareness of malicious actors who seek to exploit misconfigurations and vulnerabilities and move laterally to exfiltrate sensitive data.

Fortunately, GigaVUE® Enriched Metadata (GEM) for Cloud Workloads delivers a powerful solution by leveraging network-derived intelligence to provide deep observability into all cloud traffic, enabling organizations to identify and resolve security and performance challenges with greater situational awareness. With deeper context about host and environment details, organizations can significantly reduce Mean-Time-To-Detect (MTTD) and Mean-Time-To-Respond (MTTR) and better secure and manage their hybrid cloud infrastructure.

Key Features

GEM for Cloud Workloads enables you to organize your monitoring needs in alignment with your corporate structure, operations, risk assessment, security policies and compliance enforcement. This level of deep observability provides clarity that can help Ops teams derive actionable insights to reduce MTTD and MTTR.

GEM for Cloud Workloads makes this possible by extracting network and application metadata from private and public cloud workload traffic and enriching it with corresponding host environment details.

The enriched records can be seamlessly ingested into data lake, SIEM, and observability tools using JSON format over HTTPS/Kafka.

Key Benefits

- **Gain faster incident response** by providing context to metadata in Gigamon Application Metadata Intelligence to isolate issues such as the resulting impact from policy changes, network/application latency, and security policy enforcement
- **Improve threat detection** through anomaly identification by baselining traffic patterns based on criticality, ownership, department, cost center, location, security group mappings, and the IAM instance profile of the workloads
- **Reduce cloud compute consumption costs** through centralized monitoring and end-to-end visibility for better resource usage supervision and capacity planning
- **Simplify tools integration** with enriched contextual correlated data feed, resulting in reduced MTTR, remediation time, and time spent managing disparate tools

Supported cloud environments include:

Type of Information	Private Cloud (VMware ESXi and NSX-T)	Public Cloud (AWS and Azure)
Platform	Platform Type Datacenter Name	Platform Type Account ID
Workloads (Virtual Machines)	Cluster Name DNS Host Name VM Name Guest OS Tags	Instance Type and ID DNS Host Name Guest OS Tags Security Group* IAM Instance Profile*
Virtual Network	Virtual Network Name	Virtual Network ID

* Information applies to AWS only.

Challenges

The shift to multi-cloud architecture continues to accelerate, bringing with it an increased risk of cyber threats that could compromise sensitive data, systems, and networks. Cybercriminals continue to target the cloud to gain access to sensitive information. This could include customer data, financial records, and proprietary business intelligence. Looking ahead, it's clear that cloud security threats will continue to evolve and become more complex. By adopting a proactive approach to security that includes regular compliance audits, vulnerability assessments, pen testing, and robust incident response planning, you can protect your hybrid cloud infrastructure and organization from cyber threats.

In addition, digital transformation has disaggregated applications and services and underlying enterprise networks as they have expanded from on-premises to hybrid and multi-cloud environments. The complexity of these distributed systems is one of the top challenges facing the CloudOps, CloudSecOps, Cloud Security Operations Center (Cloud SOC), and DevOps teams today.

These are some of the threat detection and incident response (TDIR) challenges for CloudSecOps and Cloud SOC teams:

- Advanced persistent threats (APTs) stay undetected due to lack of visibility into lateral traffic, allowing ransomware and malware attacks to establish command-and-control channels to exfiltrate sensitive data
- Limited visibility not only hampers effective threat detection and investigation but also complicates the response process, making it harder to mitigate risks and respond to incidents in real time
- Data breaches can occur without timely detection, resulting in financial loss, reputational damage, and regulatory penalties
- Insider threats can go overlooked, allowing rogue or disgruntled employees or contractors to steal sensitive information or disrupt operations

CloudOps and DevOps face these operational challenges when troubleshooting applications and managing the cost of the cloud environment:

- Ensuring comprehensive and effective monitoring and logging across all services can be challenging with dynamic and ephemeral cloud resources. Inconsistent logging practices and insufficient monitoring can complicate issue tracking and correlating logs over time.
- Managing and optimizing resource allocation to avoid over-provisioning or under-provisioning is critical and remains challenging.
- Understanding cost implications and optimizing cost efficiency can be painful, as troubleshooting often involves scaling resources up and down, which can lead to unexpected costs if not managed properly.
- Identifying performance bottlenecks in a distributed cloud environment requires detailed performance metrics and insights, which can be challenging to gather and analyze.
- Ensuring that the cloud environment complies with security policies and regulatory requirements can add yet another layer of complexity to trouble shooting.

Why GEM for Cloud Workloads?

GigaVUE Enriched Metadata for Cloud Workloads enables CloudOps, DevOps, CloudSecOps, and Cloud SOC teams to drive their TDIR to become operationally efficient, enhancing security policy enforcement and capacity planning in their virtual environments. They will also be able to quickly identify, troubleshoot, isolate, and remediate the compromised workloads by augmenting application metadata with additional context from host environments.

Gigamon Application Metadata Intelligence (AMI) is one of the most popular deployable solutions for providing L2–L7 information for workload traffic. The GEM for Cloud Workloads solution provides additional context to L2–L7 network metadata, enriching it with cloud host environment and security details in an easily consumable JSON format. This enables organizations to use a single source of data for faster incident response. The GEM solution, which is available for AWS, Azure, VMware ESXi, and NSX-T platforms, enriches the AMI data path flow metadata for many use cases.

- 99 percent volume reduction
- Over-the-top app detection
- Near real-time metadata generation with configurable export periodicity

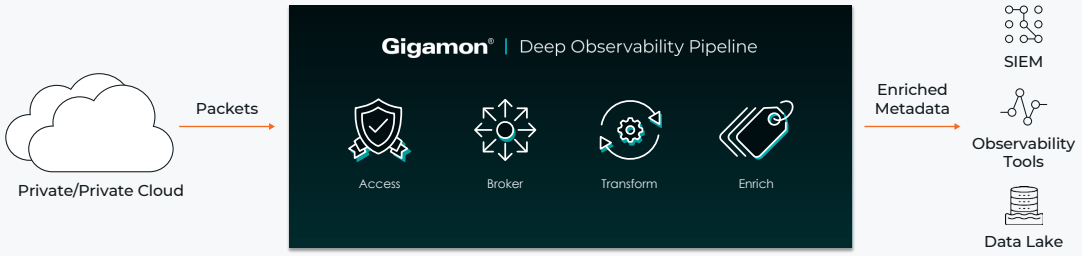


Figure 1. Packets in -> Enriched Metadata out with GEM for Cloud Workloads

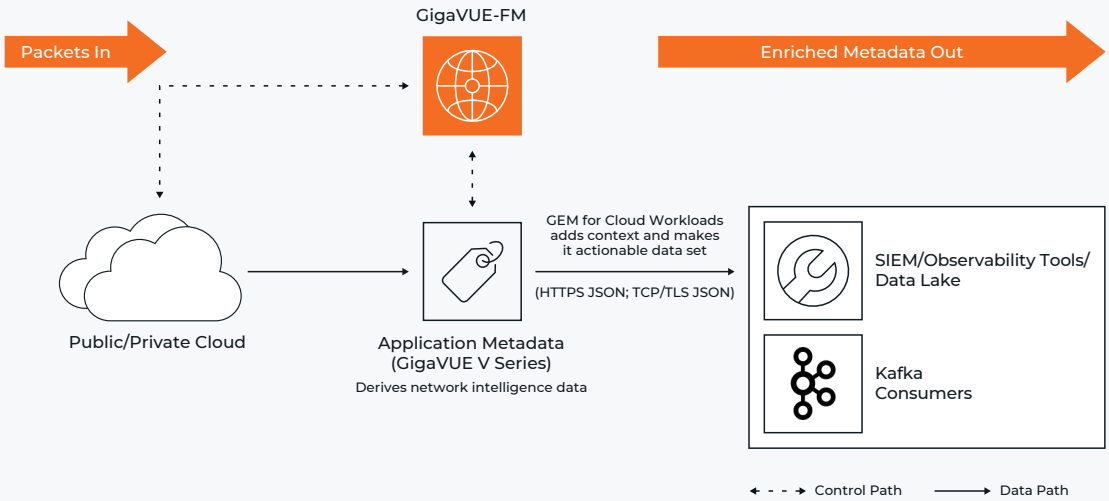


Figure 2. GEM for Cloud Workloads provides additional situational awareness to application metadata.

Mapping of Cloud Attack Vectors with GEM for Cloud Workloads Benefits

The Cloud Security Alliance (CSA) organization promotes the use of best practices for providing security assurance within the cloud computing industry. Based on their research on common cloud attack vectors, GEM for Cloud Workloads offers following benefits:

Attack Vector	Description	Impact	GEM for Cloud Workloads Benefits
Exploitable Workloads	Details an attacker's ability to exploit a workload's vulnerabilities (well-known or zero-day) (misconfigs, CVEs and app vulnerabilities, etc.) and gain initial footholds into the cloud environment.	• Running crypto miners or ransomware. • Attackers can achieve persistence, data access, or privilege escalation in the cloud environment. The attacker can then leverage this asset to strengthen access and control to perform lateral movements in search of additional assets.	• Monitor for traffic to/from domains with higher Domain Generation Algorithm (DGA) score (i.e. ephemeral domains) providing detailed information such as: – Account ID (AWS)/Subscription ID (Azure)/Data Center (VMware) – VPCs (AWS)/VNETs (Azure) – Tags (AWS/Azure/VMware) associated with services, accounts, environments, etc. Note: HTTP, SSL, and DNS support exporting dga_score. • Monitor for uniform enforcement of security groups (AWS only) among all business-critical workloads. Similarly, guest OS type and version VMware/Image ID (AWS and Azure), and Client and Server User Agents can be monitored for latest version/patches as required by an organization's security policy. • Security groups (AWS) can be profiled based on their active ports to detect any misconfigurations or compromises. • Traffic patterns can be profiled between security groups and between security groups and accounts, tags and/or VPCs to detect any abnormalities.
Workloads with Excessive Permissions	• Workloads are generally created to run several jobs or tasks, with different access patterns and authentication complexities, requiring different permissions for multiple services (e.g., access to cloud storage). These permissions are assigned to the workload as a policy or role. • This complexity creates challenges in managing access to specific services and resources, leading to bad security practices such as granting excessive permissions.	The attacker usually gains first access with low-level permissions, so access to the workload with excessive permissions can result in the elevation of privileges and the attacker gaining better persistence and the ability to create more damage.	• Monitor for uniform enforcement of IAM profiles (AWS only) among all business-critical workloads. • Monitor traffic patterns by correlating IAM profiles with other attributes such as accounts, VPCs, security groups and/or HTTP error codes to detect any abnormalities.
Unauthorized Access to Object Storage	Details the existence of cloud-hosted storage with public objects that don't require user authentication or authorization, usually by mistake.	Suppose those cloud storages are misconfigured to be publicly reachable without additional authorization. In that case, attackers can use readily available utilities to compromise the datastore and/or the data within, with a high likelihood of attacking without detection.	• Monitor for uniform enforcement of IAM profiles across all workloads hosting object storage. • Monitor traffic anomalies. • Monitor associated security groups.
Compromised Images	Images that have been maliciously modified to exploit vulnerabilities and allow attackers to gain access to cloud resources. This is usually done by creating a backdoor in the image or obfuscating malware inside the image.	Images that have been compromised can be used to launch cloud-based attacks, such as cloud malware injection, mining cryptocurrency, data exfiltration, or account takeover.	• Monitor guest OS and Type VMware or Image ID (AWS and Azure) of key workloads and their internal and external traffic patterns per account/environment.

Key GEM for Cloud Workloads Use Cases

The enriched metadata solution offers broad support for the following use cases:

Use Cases for CloudOps and DevOps

Capacity Utilization
Enables monitoring consumption of cloud compute resources (number and type of instances) and bandwidth usage per:

- Key virtual networks
- Business critical applications/functions/environments

Troubleshooting
Enables identifying and troubleshooting performance and latency issues based on the criticality of workloads and their instance types and virtual networks.

- Workloads supporting business critical applications
- Workloads belonging to key business functions (e.g., HR, Finance, Sales, and more)
- Workloads supporting key environments (e.g., Production, Demo, UAT, and more)

Use Cases for CloudSecOps and Cloud SOC

Threat Detection
- Enables baselining traffic patterns based on virtual networks and their associations (such as accounts, tags, and security groups) to detect abnormalities caused by lateral movement techniques
- Enables profiling security groups based on their active ports to detect misconfigurations or compromises
- Enables monitoring uniform enforcement of tagging, security groups, and IAM instance profiles to identify access misconfigurations
- Enables monitoring guest operating systems to identify unpatched vulnerable workloads
- Enables monitoring suspicious communications to identify supply chain compromises

Incident Response
- Enables faster identification of security groups involved in an incident reducing the time to detection and analysis of incident management programs
- Aids threat detection and post-incident review (PIR) to determine root cause analysis of a security incident with detailed forensics information. Compare network and workload statuses before and after an incident, even after a workload is deleted, such as in cryptojacking attacks

Anomalous Traffic
- Enables monitoring the TLS security posture of key business functions and environments
- Enables monitoring compliance of HTTP version and server agents with enterprise security policy and monitoring anomalous HTTP traffic, based on the criticality of workloads
- Enables monitoring abnormal DNS traffic that may reveal threats such as ransomware, malware, phishing in key business functions and environments or security groups

Suspicious Connections
- Enables monitoring of unknown out of compliance services and unsanctioned applications commonly leveraged by attackers (P2P, SMB, FTP, RDP) in key business functions and environments

Conclusion

GEM for Cloud Workloads provides additional context enrichment to the AMI L2 to L7 network traffic metadata. CloudOps and DevOps teams have common goals for monitoring and troubleshooting performance and latency issues and monitoring the cost of their environments. GEM for Cloud Workloads can help to provide deep observability not only with reference to the various applications they monitor, but also with reference to the various environments and locations they manage. Finally, it also enables organizations to share data and rapidly triage issues.

GEM for Cloud Workloads helps CloudOps and Cloud SOC teams to eliminate blind spots, providing deep observability into lateral network traffic. This enhanced visibility exposes previously hidden lateral movement techniques, enabling faster, more effective threat detection and response with reduced Mean-Time-To-Response (MTTR) and Mean-Time-To-Detect (MTTD).

About Gigamon

Gigamon® offers a deep observability pipeline that efficiently delivers network-derived intelligence to your cloud, security, and observability tools, helping organizations eliminate security blind spots, reduce tool costs, and better secure and manage your hybrid cloud infrastructure. Gigamon goes beyond security and observability log-based approaches by extracting real-time network intelligence derived from packets, flows, and application metadata to deliver defense-in-depth and complete performance management. 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.

1. 2023 Hybrid Cloud Security Survey: Perception vs. Reality. Gigamon, 2023. https://www.gigamon.com/content/dam/gated/wp-gigamon-survey-hybrid-cloud-security-2023.pdf.
2. Shelley Boose. 81% of Companies Have Had a Cloud Security Incident in the Last Year. Venafi, September 28, 2022. https://venafi.com/blog/81-companies-have-had-had-cloud-security-incident-last-year-venafi-research.
3. https://expel.com/wp-content/uploads/2023/08/Security-Enabled-Innovation-Survey-Report.pdf
4. https://cloudsecurityalliance.org/blog/2023/06/29/cloud-security-threats-to-watch-out-for-in-2023-predictions-and-mitigation-strategies

Gigamon®

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

10.24_03