Gigamon Application Metadata Intelligence for Superior Hybrid Cloud Security and Performance

NETWORK INTELLIGENCE EXTENDS CAPABILITIES OF EXISTING OBSERVABILITY AND SIEM TOOLS TO PROACTIVELY DETECT VULNERABILITIES AND ACCELERATE TROUBLESHOOTING

Gigamon Application Metadata Intelligence At-a-Glance

BENEFITS

+ Supercharge observability tools, SIEMs, and custom tools with more than 5,000 application attributes to identify vulnerabilities and unsanctioned activities, such as weak encryption ciphers, non-standard port usage, and crypto-mining activity
+ Improve application performance and uptime by equipping operations teams with the information needed to pinpoint the causes of bottlenecks and outages, such as slow TCP links, video frame rate changes, and network errors
+ Incorruptible network telemetry from AMI augments MELT and verifies potentially spoofed log data to give clarity around a security incident

RELATED GIGAMON PRODUCTS

+ GigaVUE® Cloud Suite
+ GigaVUE-FM
+ Gigamon Application Filtering Intelligence

A hybrid cloud environment, which encompasses one or more public clouds together with on-premises data centers, brings greater agility and cost savings. However, it also comes with challenges associated with decreased visibility. That's because traditional and native cloud tools that rely on MELT (metrics, events, logs, and traces) data are limited in what they can identify, and how deeply or broadly they can monitor today's complex infrastructure.

For example, legitimate applications are indistinguishable from rogue ones using native logging alone. The problem is further compounded when application data traverses, in a spider web-like fashion, between multiple public clouds, containers, and on-prem data centers. Or when you need to monitor unmanaged hosts, such as in the case of older applications or unknown APIs in production, and IOT devices. In these cases, pinpointing the source of an application performance issue or a security vulnerability is near impossible.

What is needed is deep observability from Gigamon that eliminates these hybrid-cloud blind spots, both East-West (such as between container nodes within VMs) and North-South (when application traffic transits between multiple environments). Furthermore, Gigamon Application Metadata Intelligence (AMI) augments MELT with the addition of application and network metadata. AMI sends a rich set of application and data-in-motion-derived intelligence to your tools, including:

+ **Application identification:** Application/file names, video titles, application types (crypto, audio/video streaming, chat, shadow IT)
+ **Protocol attributes:** Response codes, cyclic redundancy check (CRC) checksum failures, URLs, round-trip time (RTT), dropped packets, client/server software, resets, latency, and more for various protocols like HTTP, SIP, and FTP
+ **Mail protocols:** File attachments, email size, sender/recipients
+ **DNS parameters:** Request/response codes, queries, performance attributes, DNS tunneling, traffic volume, data exfiltration

AMI also makes available dozens of elements on mainstream applications such as YouTube, Facebook, and Gmail. (See the Gigamon AMI datasheet for more details on provided metadata attribute).

With AMI, you get increased visibility into application user-experience metrics and potential compliance or security risks:

+ Discover hosts, assets, and applications across your hybrid and multi-cloud environment, both known and unknown
+ Surface preventable vulnerabilities, such as deprecated ciphers and self-signed or expired SSL certificates
+ Detect unauthorized activities, including BitTorrent, crypto-mining, and shadow IT
+ Spot anomalies and nefarious acts, such as data exfiltration attempts and use of non-standard TCP ports (i.e., port spoofing)

And you would get this additional visibility through your existing tools. There's no need to buy new tools or change the monitoring processes that your teams know so well. Gigamon has pre-built integration with the most common security and observability tools, including Dynatrace, Datadog, New Relic, Splunk, QRadar, Elastic, and others. One of the top things on an operations team's wish list — to have a single-pane-of-class for unified visibility across all environments — is now a reality.

Security Use Cases: Stay Secure in Changing Times

Gigamon AMI makes sure your tools don't miss anything by sending application and network intelligence to security and observability tools for analysis and visualization. For example, tools can correlate application behavior from AMI together with MELT to get a full picture of a specific security incident. SecOps and CloudOps teams can automate detection of anomalies such as unusual activities and vulnerable applications to stop cyber risks that overcome perimeter or endpoint protection.

+ **Uncover suspicious remote connections.** AMI can help identify suspicious SSH, RDP (remote desktop protocol), and Telnet remote connections by looking for leading indicators like bandwidth use, connection longevity, IP reputation and geolocation. This helps detect unauthorized external remote connections used for data exfiltration.
+ **Detect rogue activities.** Whether intentional or unintentional, every IT infrastructure bears the cost of unsanctioned applications and activities. AMI identifies traffic from P2P activities, such as BitTorrent, and crypto mining.

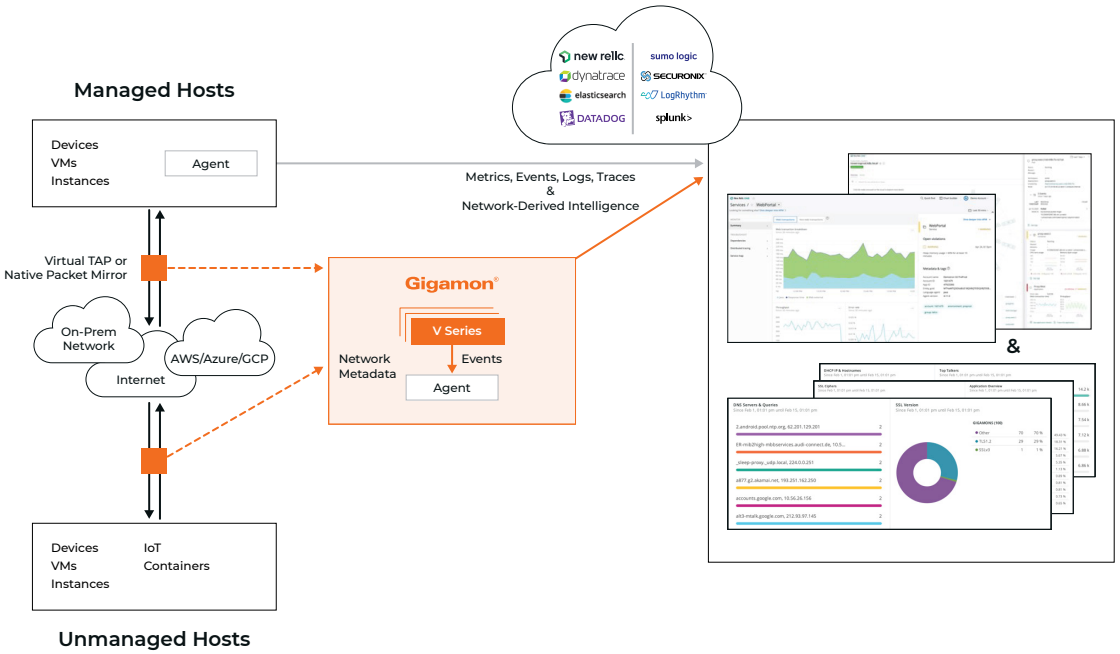

Figure 1. AMI augments MELT with network-derived intelligence from both managed and unmanaged hosts. AMI data is ingested, analyzed, and visualized through our partner ecosystem tools.

+ **Recognize dubious end-user activity.** Highly privileged users logging in from unauthorized systems could represent a brute force attack on your network via compromised user credentials. Multiple logins by the same user from different locations may represent a similar attack. AMI surfaces these unusual login attempts and high login activities.
+ **Monitor and control file access.** Monitor data in motion involving FTP, SCP, SMB, and CFS protocols for applications from various file sharing service vendors. It is imperative that IT obtain insights into which clients are obtaining specified files. Otherwise, malicious activity, such as unauthorized user or machine accounts moving data without being disclosed or uploading files containing malware, will occur without detection. Tools can use AMI attributes to generate lists of files involved, source and destination IP addresses of the end-users, and other information and be displayed in a dashboard. Thus, determining who is accessing what files for forensic purposes.
+ **Analyze HTTP client errors.** With AMI, you can analyze HTTP client errors, including the number of HTTP response-code errors relative to the total number of codes, to spot suspicious activity. The distribution of these errors and the clients seeing these codes may also provide further insight. AMI can provide details on a client IP address and the number of errors it has encountered, which can help you spot a hacker trying a brute force attack and getting 401 errors.
+ **Identify expired SSL/TLS certificates.** TLS certificates enable encryption and authentication and are effectively mandatory for web servers; without them, visitors will quickly move on. But the windows during which these certificates are valid are shrinking — some are only good for a few weeks, for example — so it is imperative to find those on your servers that are defunct. You can use several attributes to spot these and create real-time alerts. AMI provides certificate expiry dates, as well as notices of any revoked or expired certificates, along with the application servers using them for compliance reasons. You also can detect SSL-decrypted traffic that uses non-trusted or self-signed certificates, which could indicate nefarious activity.
+ **Identify data exfiltration.** AMI can help evaluate the volume and type of DNS requests you're receiving, including those on non-standard ports, at various domain levels, including DNS queries involving entropy, statistics, outliers, and record types. This data can reveal DNS tunneling in the network and help establish the legitimacy of domains.
+ **Locate weak ciphers.** Ideally, clients and servers should only employ the strongest cipher suites available and negotiate to one of these during the TLS handshake, but this is not always the case. AMI can provide metadata that reveals all TLS connections with weak ciphers, along with the applications and systems hosting those applications, helping you ensure security compliance.
+ **Analyze target time windows.** AMI allows IT to derive an end-to-end picture of various security events by leveraging metadata to look at Kerberos, SMB, DNS, and HTTP use. By isolating protocol activities that led up to and followed an incident, you can track down the origins of a security breach or get the details of the activities of a particular host within a given timeframe.
+ **Detect rogue DNS and on-prem DHCP servers.** Attackers can host shadow IT within your network for diverting traffic and launching man-in-the-middle attacks. AMI provides details that help you list the total number of DNS and DHCP for on-premises environments in your network, distinguishing rogue servers from those that are trusted or publicly known servers.
+ **Profile client experience.** Obtain metadata from customers and locations worldwide to granularly identify what each of their clients are doing on the internet. This helps ensure security, compliance, and SLA goals. Metadata gathered from clients include which applications are in play, their bandwidth utilization, SSL/TLS ciphers, DNS transactions, DHCP insights, and HTTP details.

Network and Application Performance Monitoring Use Cases

Whether your applications and workloads are in cloud or on-prem (or a mix of both), AMI can help ensure an optimal user experience. AMI gets critical performance data and indicators to your NPM and cloud APM tools without flooding them with irrelevant data.

Example use cases include:

+ **Maintain network and application health in an on-prem environment.** Leverage application visibility to evaluate network health by looking at application broadcast and multicast control packets. For example, you can observe where in the communication chain response times are slow or having problems. Also, understand if the delay is related to a specific piece of compute or due to long round-trip time to other regions or on-prem.

  Applications send these packets at regular intervals and, by analyzing them over time, you can determine the average interval between them and their timing. If the interval between control packets changes over time, that may indicate device malfunction, network congestion, or network traffic storms. You can also monitor SNMP, UPNP, and any broadcast packets to pinpoint root causes of network problems.

+ **Maintain application health in the public cloud.** In a public cloud or multi-cloud scenario, AMI give you visibility into degraded digital experiences. Get application performance metrics, such as response time and error codes, to evaluate health and user experiences. By monitoring when a query is received by the application and the length of time for a response to take place, over time you can determine and map out performance norms and when abnormal behavior is occurring without relying on the application to report these problems.

+ **Improve video experiences.** You can use metadata attributes in a video embedded in an application to optimize the user experience for work-at-home employees collaborating via video chat. These attributes include:

  - Frame-per-second rate at the beginning of the video and changes over time
  - Bitrate changes over time
  - Drop from HD to standard video quality
  - Video length
  - When the user stops a video

  Your application and network performance monitoring tools can use this information to determine the user's true video viewing experience and find potential causes of service degradation.

+ **Analyze poor application response times.** Application-level metadata can export attributes related to SNMP, SMTP, HTTP, ICMP, and IPMI, which you can feed to network monitoring tools to detect and report failures of devices or connections, network bandwidth utilization of links, round trip times, and other aspects of network operations. Slowing DNS servers and other application servers can cause latency and an overall undesirable user experience, and you can use average and top response times detected by AMI to track down these trouble spots.

+ **Identity bandwidth hogs.** To properly monitor and manage performance levels and end-user experiences, IT needs to understand what the top applications and users are present, what their usage levels are, server error codes such as 404, and actual latency from RTT metrics. Gigamon Application Metadata Intelligence (AMI) and Application Filtering Intelligence (AFI) work together to enable a SIEM dashboard to highlight 'top talkers' and application performance, among other APM/NPM use cases.

Empowering Your Current Set of Tools

The Gigamon Application Metadata Intelligence solution works out of the box with New Relic, Splunk, QRadar, Dynatrace, Sumo Logic, Datadog, LogRhythm, and other SIEM and observability tools. In fact, any security tool can benefit from AMI as long as it has an adaptor to parse CEF or IPFIX.

Reports and accompanying dashboards are fully customizable.

Use Case: Adaptive Response Application for Splunk

If you're an AMI customer who uses Splunk, you can do more than look at forensic data retroactively, isolating, and remediating lapses in security. Splunk Base interacts with Gigamon Adaptive Response Application for Splunk and GigaVUE-FM fabric manager to make changes to traffic flows based on any detected anomaly. With this application, you can automate the use of metadata to boost security, selecting attributes to proactively implement corrective action in real time. For instance, you can:

+ Correlate file names and usernames, and automatically generate and send an alert to a security tool to block or temporarily quarantine specific downloaded files or links, based on those attributes.

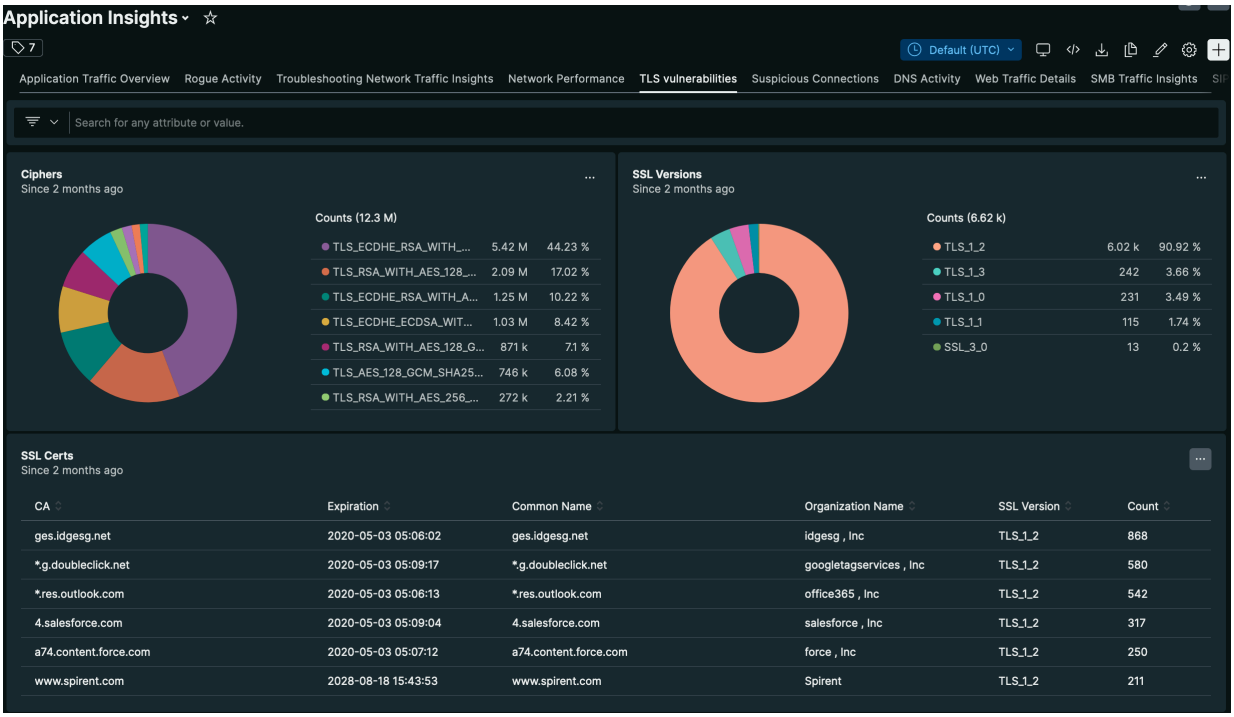

Figure 2. Gigamon Application Metadata Intelligence dashboard within New Relic showing TLS vulnerabilities.

+ Use metadata about specific file types to automatically generate alerts when emails including an attachment arrive, ensuring that the file is sent to a sandboxing tool for analysis before it's opened.

Gigamon Adaptive Response Application for Splunk provides you with alert actions you can take on the GigaVUE® HC Series visibility nodes via GigaVUE-FM and can redirect certain applications or flows to specific security tools, such as advanced threat protection or secure email gateways. These actions can be bound to correlation searches on Splunk Enterprise Security for automated response or executed on an ad hoc basis with notable events. This application leverages Splunk's Adaptive Response framework and uses a RESTful API to integrate with GigaVUE-FM.

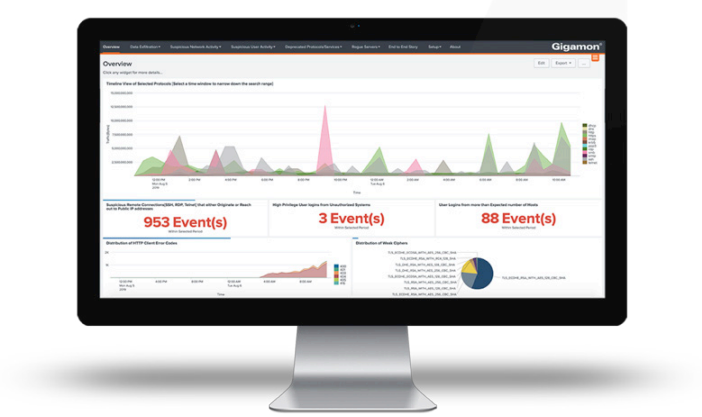

Figure 3. Gigamon Application Metadata Intelligence dashboard within Splunk, showing suspicious connections, unusual login activity, HTTP error codes, and more.

Giving Visibility Back to Organizations Worldwide

Gigamon Application Metadata Intelligence (AMI) is deployed by cloud, network, and security operations teams to provide the additional visibility needed for today's hybrid cloud environment. Here are some examples of government entities, communication service providers, and major enterprises using AMI:

+ A major worldwide satellite communications provider used AMI to identify ultra-granular details on what internet activities were taking place at the client and location level to ensure quality end-user experiences.
+ A government institution with more than 10,000 employees leveraged a multi-vendor architecture to identify security events and immediately link them to the traffic responsible to accelerate troubleshooting and remediation.
+ A large credit union was able to identify the principal clients and their bandwidth levels to improve the application experiences and ensure SLAs.
+ A medical provider helped obtain compliance by ensuring only compliant applications, ciphers, and TLS versions were being used.

We're Here to Help Navigate What's Next for Your Organization

Gigamon Application Metadata Intelligence gives you deep observability to all corners of your hybrid cloud infrastructure. Armed with that knowledge, your teams can more efficiently manage and monitor your infrastructure — using the tools you already have, without a need for costly network or tooling upgrades.

To see how Gigamon Application Metadata Intelligence can work with your business, contact our sales team or visit Gigamon.com to request a demo.

Appendix

Various use cases for AMI are listed below with the associated dashboards to view and their implications.

CATEGORY AND NAME OF USE CASE	DASHBOARDS	WHAT TO INFER
Data Exfiltration: DNS Tunneling	Volume of DNS Requests at Top Domain Level Volume of DNS Requests at Subdomain Level DNS Query Entropy DNS Query Statistics DNS Query Outlier DNS Record Types	+ Presence of DNS tunneling in the network + Legitimacy of the domains
Suspicious Network Activity: Detecting Command-and-Control Attacks Using Machine Learning	Total Unique Domains Seen on Network Total Domains Predicted to Be Generated by DGA List of Domains Predicted to Be Legit List of Domains Predicted to Be DGA History of Manual Adjustments Test Data	+ Command-and-control attacks in the network + Check whether a domain is legit or generated using a domain generating algorithm (DGA) + Verify domain authenticity by leveraging external sources such as Virus Total
Suspicious Network Activity: Suspicious Remote Connections	Total Number of SSH Sessions Total Number of RDP Sessions Total Number of Telnet Sessions Total Number of Suspicious Remote Connections List of Suspicious Remote Sessions	+ Detection of unauthorized external remote connections + Look for bandwidth usage by external remote connections, which can be used for data exfiltration + Longevity of remote connections
End-to-End Story: Time Analysis of an Event	Prior Kerberos Protocol Activity Post Kerberos Protocol Activity Prior SMB Protocol Activity Post SMB Protocol Activity Prior DNS Protocol Activity Post DNS Protocol Activity Prior HTTP Protocol Activity Post HTTP Protocol Activity	+ Isolate prior and post protocol activities that lead to an incident + Find all activities of a particular host in a given time range
Suspicious User Activity: High-Privilege User Activity	High-Privilege Use Logins from Unauthorized Systems	+ High-privilege user credentials may have been compromised + Someone is trying brute force attack using the login ID of a privileged user

CATEGORY AND NAME OF USE CASE	DASHBOARDS	WHAT TO INFER
Suspicious User Activity: Abnormal User Login Activity	Total Number of Login Sessions Seen Multiple Logins by Same User	+ User credentials may have been compromised, therefore the same user is seen logging in from more than two hosts + Someone is trying a brute force attack using a false login ID
Suspicious User Activity: HTTP Client Error Analysis	Number of HTTP Response Code Errors Number of HTTP Response Codes Distribution of HTTP Error Codes List of Clients Seeing Error Codes	+ List of Clients Seeing Error Codes provides details about client IP and the number of errors it has encountered + Someone is trying a brute force attack and getting 401 errors
Deprecated Protocols and Services: Weak Ciphers	Total Connections with Weak Ciphers Total TLS Connections Distribution of Connections with Weak Ciphers Top Applications Using Weak Ciphers	+ Whether weak ciphers are seen in the live network + List of applications using the weak cipher list and systems hosting those applications + Network security compliance
Rogue Servers: Rogue DNS and DHCP Servers	Rogue DNS Servers Rogue DHCP Servers Trusted/Known Servers	+ Man-in-the-middle activities + Unauthorized servers in the network

Gigamon®

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