Keep Networks Responsive and Secure with Gigamon Application Metadata Intelligence

UNDERSTAND APPLICATION BEHAVIOR AND IMPROVE THE USER EXPERIENCE

Gigamon AMI at a Glance

BENEFITS

+ Ensures that the new wave of north-south traffic doesn't overwhelm performance monitoring and security tools by generating and sending relevant metadata
+ Improves visibility into the increased attack surface that arises from the shift from LAN to WAN
+ Offers insight into the end-user experience for video chat and other traffic-heavy applications to help improve work-from-home capabilities

RELATED GIGAMON PRODUCTS

+ GigaSMART® applications
+ GigaVUE-FM Fabric Manager
+ Gigamon Adaptive Response Application for Splunk

Much of the world is now working from home and that's transforming how you and your team support employees. You need insight into network and application behavior in order to maintain network availability, performance and user experiences as network traffic shifts from LANs to WANs and users, to stay productive, turn to secure communications with VPNs and high-bandwidth apps, including videoconferencing. Last but not least, you also need to secure the increased attack surface and vulnerabilities this shift has created.

To achieve this, your NetOps and SecOps tools need quick insight into the network traffic generated by various applications and protocols. NetFlow typically offers only 5-tuple information — the set of five values that comprise a TCP/IP connection. That provides minimal data from Layers 2-4 of the OSI model, which gives you details on devices and the data they use, but not much beyond basic network management.

But with Gigamon Application Metadata Intelligence (AMI), you can use deep packet inspection (DPI) to get abridged and context-aware information about raw packets based on Layers 3–7 of the OSI model, which provides insights into application behavior.

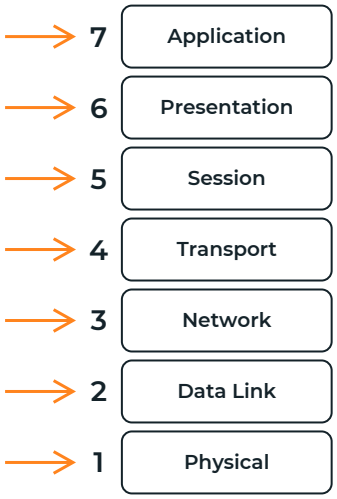

Figure 1. Gigamon AMI provides visibility into the upper layers of the OSI model so crucial for understanding application behavior.

AMI can feed your tools over 5,000 attributes that shed light on security and network status and help prevent breaches and poor performance — that's three orders of magnitude beyond what NetFlow offers.

With AMI, you can:

+ Gain insight into critical details pertaining to flows
+ Reduce false positives by separating signals from noise
+ Identify nefarious data extraction
+ Accelerate threat detection and remediation through proactive, real-time traffic monitoring, as well as troubleshooting forensics

AMI provides a rich set of metadata to your tools, such as:

+ **Identification:** Social media user, file and video names, SQL requests
+ **HTTP:** URL identification, command response codes
+ **DNS parameters:** Request/response, queries and device identifiers
+ **IMAP and SMTP** email-based communications with sender and receiver addresses
+ **Service identification:** Audio, video, chat and file transfers for VoIP and messaging

AMI also makes available dozens of elements on mainstream apps such as Facebook, YouTube, Gmail and Yahoo. Protocols such as FTS and SIP are also available. (Refer to the Application Aware Metadata data sheet for more details.)

Security Use Cases: Stay Secure in Changing Times

You're probably using security information and event management (SIEM) tools to lock down your infrastructure — a task that's getting much harder as work-from-home employees expand your organization's attack surface.

AMI makes sure your tools don't miss anything by sending application metadata to your SIEM solutions for security analysis, so they can correlate application behavior and analyze log data from servers and security appliances. Network security tools leverage metadata attributes to deliver the insight and analytics needed to manage the opportunities and risks associated with the digital transformation that's been accelerated by the coronavirus pandemic. SecOps administrators can automate detection of anomalies in the network and stop cyber risks that overcome perimeter or endpoint protection.

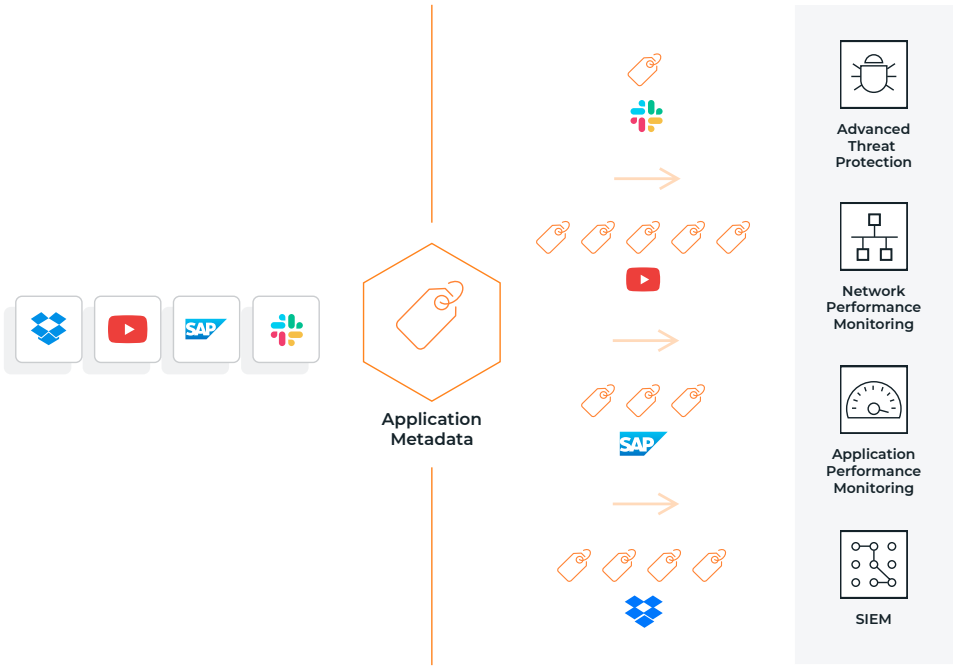

Figure 2. AMI extracts metadata elements for use by SIEM tools and other ecosystem solutions.

How can AMI provide visibility into issues on your network that may indicate breaches or weak security defenses? Here are some example use cases:

+ **Uncover suspicious remote connections.** AMI can help identify suspicious SSH, RDP and Telnet remote connections, looking for leading indicators like bandwidth use, connection longevity, IP reputation and geolocation. This can help you detect unauthorized external remote connections used for data exfiltration.
+ **Detect suspicious WAN activity.** With the help of machine learning, AMI can identify command-and-control attacks. You can determine whether a domain is legitimate or was generated using a botnet-controlled domain generating algorithm (DGA), and your SecOps teams can verify authenticity by leveraging external sources such as VirusTotal. Dashboards of interest here include the total unique domains seen on the network and those predicted to be legitimate as opposed to DGA generated.
+ **Recognize dubious end-user activity.** Highly privileged users logging in from unauthorized systems demonstrating unusually high levels of login activity 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.
+ **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 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 is shrinking — some are only good for a few weeks, for example — so it is imperative to find those on your servers that are defunct. There are several attributes you can use 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 apps, 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 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 servers in your network, distinguishing rogue servers from those that are trusted or publicly known servers.

Network Use Cases: Maintain the User Experience as Usage Shifts

AMI can also help you face your networking challenges as work-from-home employees drive a shift from the LAN to the WAN. The surge of new north-south traffic carries a significant bandwidth overhead and can quickly overwhelm performance monitoring tools.

AMI gets the right data to those tools at the right time without flooding them with irrelevant packets. With AMI, you can still monitor application behavior and performance without degrading the user experience.

Example use cases include:

+ **Maintain network and application health.** You can leverage Layer 4–7 metadata to evaluate network health by looking at application broadcast and multicast control packets. 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, SMTP, UPNP and any broadcast packets to pinpoint root causes of network problems.
+ **Improve videoconferencing experience.** 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:
  - The frame-per-second rate at the beginning of the video, and how it changes over time
  - Bitrate changes over time
  - Any 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.** App-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.

Gigamon Partner Use Cases: Optimizing Your Current Toolset

Empowered partners can take advantage of AMI to add more value to their tools. The Gigamon AMI solution works out of the box with Splunk and QRadar, and their reports and accompanying dashboards are fully customizable.

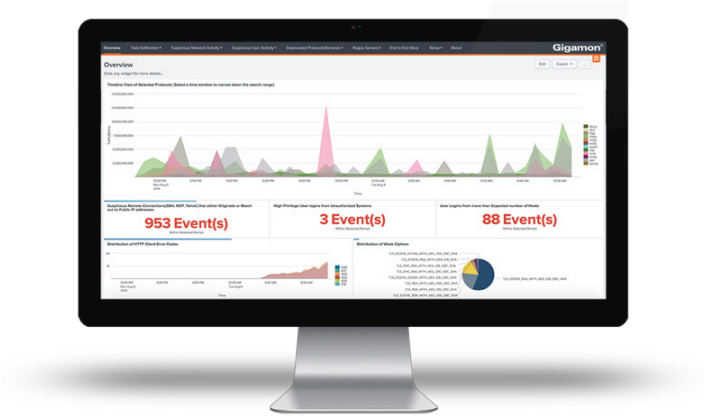

Figure 3. Gigamon AMI dashboard within Splunk, showing suspicious connections, unusual login activity, HTTP error codes and more.

But any security analytics tool can receive and use metadata from AMI, so long as the tool has an adapter to parse the incoming CEF or IPFIX so that it can identify and understand the metadata. Creating such an adapter is not a complex undertaking, and several vendors have done so. Ecosystem partners with adapters include:

+ **Active Countermeasures:** Combines penetration testing best practices, app metadata and AI to reduce the time and effort required in threat hunting.
+ **Spirent:** Uses app metadata to replicate application and user loads for mission-critical, high-volume lab-to-live application testing.
+ **Plixer:** Uses app metadata to reduce risk, lower operational cost and improve the efficiency of their Scrutinizer platform, which unifies SecOps and NetOps.
+ **FireEye:** Uses metadata to provide Helix, the company's cloud-hosted security operations platform, with the raw material it needs for a host of extremely valuable security investigation and operational use cases.

+ **NetFlow Auditor:** App metadata assists big data and machine learning for network forensics, helping you correlate threat intelligence and identify cyber threats and abnormal behavior.

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 app, 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
+ 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 visibility nodes via GigaVUE-FM and can redirect certain apps 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 app leverages Splunk's Adaptive Response framework and uses a RESTful API to integrate with GigaVUE-FM.

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

Gigamon Application Metadata Intelligence gives you unparalleled visibility into Layers 3–7 of the OSI model. Armed with that knowledge, you can more efficiently manage, monitor and secure your infrastructure even as more of your workforce logs on remotely — often using the tools you already have, without a need for costly network or tooling upgrades. If the use cases outlined here sound like they can meet your changing needs, then contact us for a demo and view our on-demand webinar for more insights.

In this time of uncertainty and change, solutions from Gigamon like AMI can help your organization run fast and stay secure while optimizing costs. With Gigamon, you can save time, save money and stay prepared for the new tomorrow, whatever it may bring.

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 VirusTotal
Suspicious Network Activity: Suspicious Remote Connections	Total No. of SSH Sessions Total No. of RDP Sessions Total No. of Telnet Sessions Total No. 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 | www.gigamon.com