Application Metadata Intelligence

Application Metadata Intelligence, Powered by Deep Packet Inspection, Provides Summarized and Context-Aware Information About Raw Packets Based on Layers 4–7

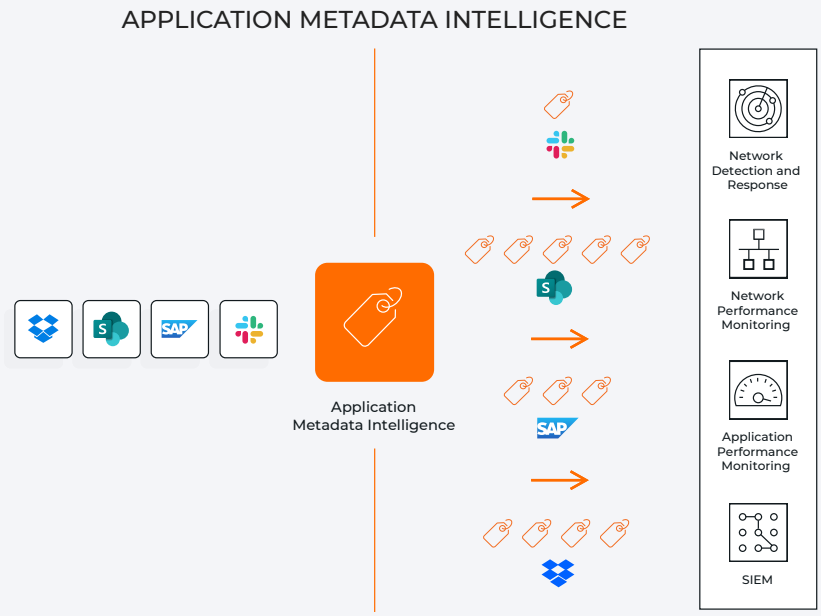

Figure 1. Application Metadata Intelligence extracts metadata elements for use by ecosystem solutions such as SIEM and performance monitoring tools.

Key Features

- Close to 6,000 protocols, applications, and user behaviors L4-7 attributes spanning over 4,000 standard and custom apps
- Identify specific users and link actions such as client login and subsequent file usage by application
- Metadata for 3G/4G LTE and 5G mobile core network traffic with optional subscriber-awareness, including protocols such as HTTP/2 and GTP-U
- Integration with Gigamon Application Visualization, Application Filtering, and GigaVUE-FM fabric manager solutions
- Use case based application and attribute templates for metadata extraction
- Export metadata in IPFIX, CEF and JSON over HTTP/S and Kafka

Key Benefits

- Increase network performance and uptime by identifying bottleneck and outage details
- Support investigators hunting threats and breaches from shadow IT and file-sharing sites
- Secure communication links by observing broad Layer 7 metadata to prevent malicious commands
- Simplify tool deployment for both on-prem or cloud-hosted scenarios, including SIEM, network, and performance monitoring
- Assist tools to ensure resource security by viewing and blocking actions such as social media users and requested file/video names
- Easily deploy specific metadata use cases by using pre-defined use case templates

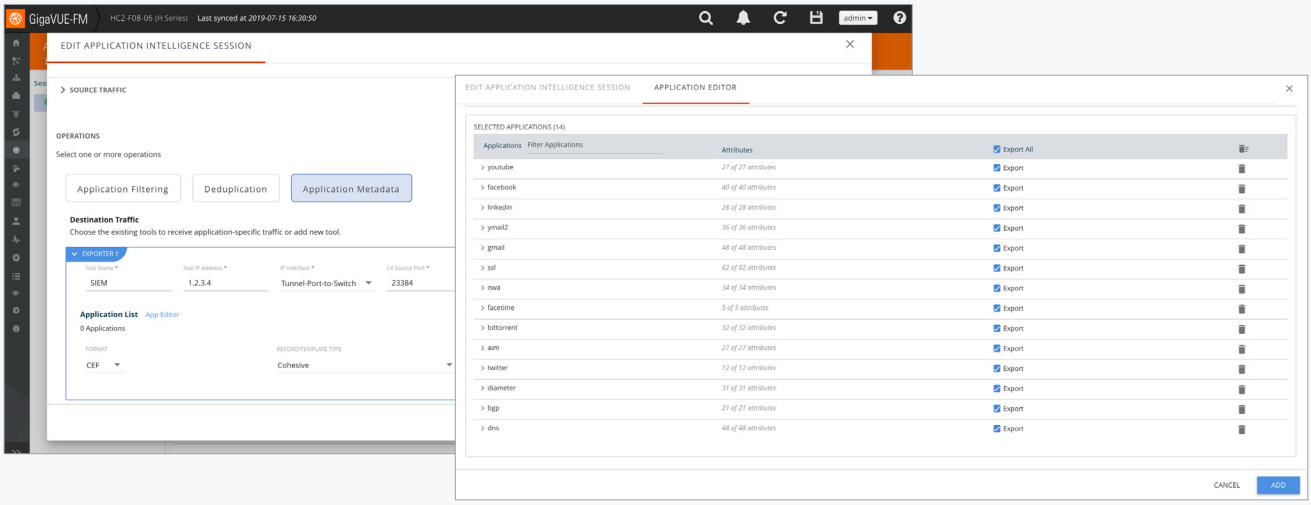

Figure 2. Dashboard allows granular selection of numerous metadata elements on a per app and protocol basis.

Application Metadata Intelligence (AMI) expands upon app layer visibility derived from Gigamon Application Visualization and Filtering and supports a comprehensive approach to obtain application behavior. Whether organizations deploy their workloads on-prem or in the cloud, they can acquire critical details pertaining to flows, reduce false positives by separating signals from noise, identify nefarious data extraction, and accelerate threat detection through proactive, real-time traffic monitoring as well as troubleshooting forensics.

SIEM solutions use this information to correlate and analyze log data from servers and security appliances. Network security and monitoring tools leverage AMI to deliver the insight and analytics needed to manage the opportunities and risks associated with a digital transformation. Administrators can automate detection of anomalies in the network, stop cyber risks that overcome perimeter or end-point protection, and identify bottlenecks and understand latency issues. AMI provides direct integration with observability tools such as Datadog, Dynatrace, Elastic, New Relic, and Sumo Logic via JSON and Kafka, allowing these observability tools to perform new security functions, such as identifying services, rogue activities, and weak crypto practices.

AMI uses deep packet inspection to provide summarized and context-aware information about raw network packets based on Layers 4–7. It enables tools to measure performance, troubleshoot issues, spot security events, and improve effectiveness. Available on HC Series hardware and GigaVUE Cloud Suite™ with GigaVUE V Series, AMI supplies network and security tools close to 6,000 metadata attributes that shed light on the application's performance, customer experience, and security. Gigamon extracts and appends elements to IPFIX, CEF, and JSON records over HTTP/S and Kafka that includes the following:

- Identification: Social media user, file and video names, and SQL requests
- HTTP: URL identification, command response codes levels
- DNS parameters: Multiple elements including 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
- Customer/network awareness: VoIP (SIP, RTP) and mobile user/data plane sessions

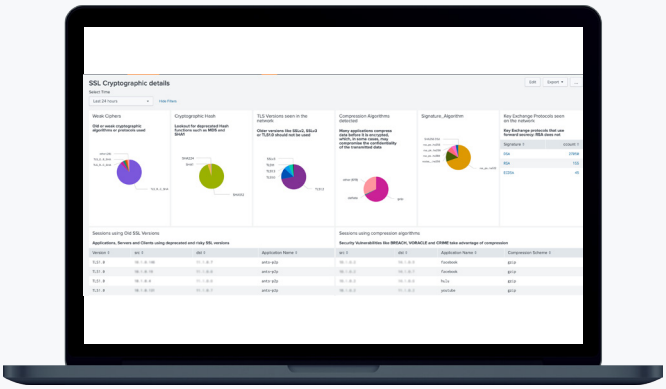

Figure 3. AMI metadata visualized in Splunk. The dashboard provides insights into weak ciphers, cryptographic hash, TLS versions, compression algorithms, signature algorithms and key exchange protocols.

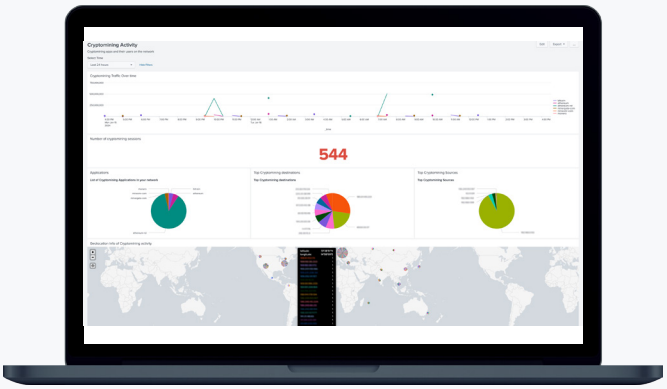

Figure 4. AMI metadata visualized in Splunk. The dashboard provides insights into Cryptomining activity.

Advanced L7 metadata can be used in a variety of use cases. The principal deployment for AMI is in providing metadata to SIEM tools for security analysis. Data exfiltration can be identified by the volume and type of DNS requests implying DNS tunneling and evaluating the legitimacy of the domains. Suspicious network activity can be investigated by detection of unauthorized remote connections, their bandwidth usage, and longevity of the connections as well as an unusual volume of SSH, RDP, or Telnet sessions. Time window analysis can be made by leveraging metadata to look at Kerberos, SMB, and HTTP use; by isolating their prior and post protocol activities that lead up to an incident, security breach origins can be found.

AMI can assist in identifying suspicious behavior. High-privilege user activity, particularly with logins from unauthorized systems or from multiple hosts, can suggest these user credentials have been compromised or a hacker is trying a brute force attack using the login ID of a privileged user. Analyzing HTTP client errors by looking at their occurrence relative to total response codes can reveal a brute force attack in progress.

Metadata can be used to evaluate network and application health using application broadcast and multicast control packets. Applications send these packets at regular intervals, and by analyzing them over time, IT can determine the average interval between control packets and their timing during this period. A differential in interval time between control packets could be due to device malfunction, network congestion, or network traffic storms. AMI attributes involving SNMP, STP, UPNP, and any broadcast packets can be useful in pinpointing the root cause.

For mobile core network use cases (such as marketing, security, troubleshooting), the power of AMI can be harnessed in combination with subscriber intelligence control plane metadata, where application metadata can be correlated and arranged in records based on key mobile network identifiers, such as user, user equipment, radio access network, network slice, and quality of service. This allows targeted analysis to be performed on user sessions that are more difficult to process due to the complexity of 3G/4G LTE and 5G core networks that use GTPv2 or HTTP/2 for the control plane and GTPv1 for tunneling the user traffic. AMI C-Tag distribution for GigaVUE HC Series platforms delivers a significant performance boost on GTP traffic, while TEID export and IPFIX multi-collect for GigaVUE HC Series platforms provide users more flexibility and visibility.

AMI Pre-defined Use Case Templates

Security Posture Template helps to detect and remediate flaws in securing applications in the network.	**This includes:** • Certificates • Versions • Weak Cipher • Key Exchange Protocols • Signature Algorithms • Cryptographic Hashes • Compression Algorithms
Anomalous Traffic Template helps to detect and remediate challenges with HTTP, HTTPs, and DNS traffic for organizations.	**This includes:** • DNS • Shadow IT • HTTPS/Web Traffic
Troubleshooting Template helps detect and remediate network delay, connectivity, and protocol errors in the network.	**This includes:** • Server vs Network Latency Issues • TCP/IP Connectivity Issues • DNS Server Failures • SIP Protocol Errors
Suspicious Activities Template helps detect and remediate issues related to unmanaged devices, suspicious connections, and traffic outside norms in the network.	**This includes:** • IoT Unmanaged Devices • Suspicious Connections • Traffic Outside Norms
Rogue Activities Template helps detect and remediate unsanctioned applications that can pose challenges to your network and security.	**This includes:** • P2P • Crypto Jacking
M-21-31 Logging Template helps certain federal use cases with U.S. Office of Management and Budget M-21-31 logging requirements.	**This includes:** • HTTPS and PKI Traffic Details • DNS Information • Shadow IT • IoMT Protocol Activity • OT Monitoring • Web Traffic Details

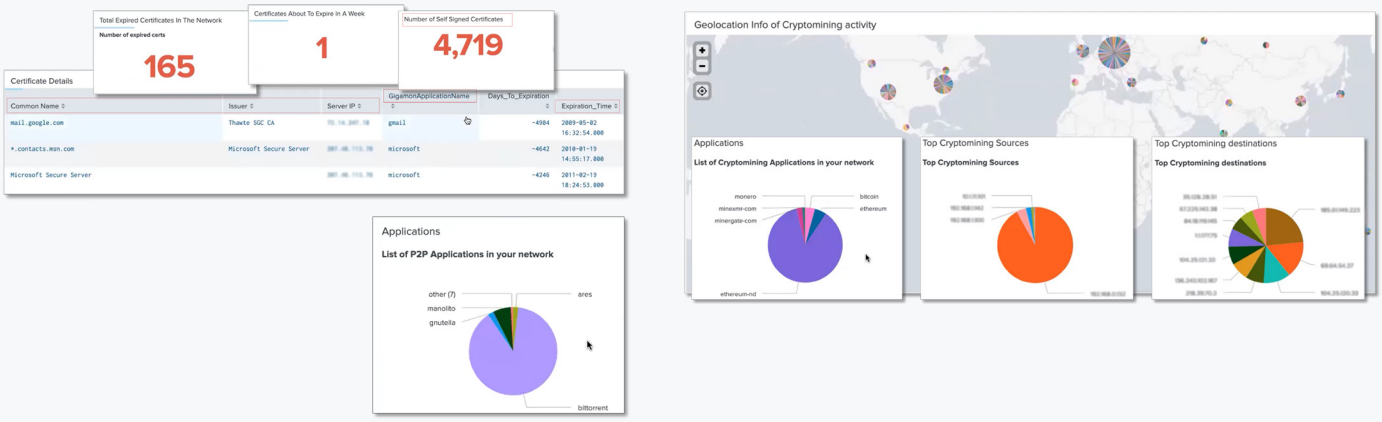

Figure 5. AMI metadata visualized in Splunk.

Key Metadata Attributes

Application identification	AMI works in concert with Gigamon Application Visualization to determine applications in use, in turn, **multiple attributes are generated, such as:** • User of social media sessions • SQL requests for database servers • User name, file upload/download for file sharing services • Industrial control system metrics, including function codes, control flags, and data records • Names of videos played in streaming media services
HTTP commands	**Detailed information on HTTP sessions including:** • URL identification • GET, POST, and DELETE • All five HTTP response code levels • HTTP certificates, including those that have expired
DNS	**DNS-related parameters, including:** • Response name • Response code • Query name • Device identifiers • Op Codes • Response TTL • ResponseIPv4Addr • ResponseIPv6Addr
Content identification	**Content with potential malware can be highlighted, such as:** • Attached file within an email
Service identification	• Audio, video • Chat, instant messaging • File transfers • VoIP sessions
Video file	**Obtain information to help measure customer experience:** • Codec • Bit rate in a Flash video • Video start/stop times • Resolution levels (such as standard, high-definition) and changes
URL	• HTTP GET • POST • PUT • DELETE • HEAD

Key Metadata Attributes, cont'd

HTTP response codes	• 100-199 (informational) • 200-299 (success related) • 300-399 (redirection)	• 400-499 (client requests) • 500-599 (server related)
SSL details	**SSL Certificate** • Valid Not Before • Valid Not After • Serial Number • Signature Algorithm	• Subject Pub Algorithm • Subject Pub Key Size • Subject Alt Name • Server Name Indication • Server Version
Device ID	**Identify source or destination machine type:** • Port ID • TTL • Platform • SW Version • Native VLAN ID Capabilities	• Network Prefix Address • Network Prefix Mask • Interface Address • Management Address
LLDP	**Identify source or destination machine type:** • Chassis IP • Port ID • TTL • Port Description • System Name • System Description • Management Address • Capabilities Available • Capabilities Enabled	• VLAN Name • Port VLAN ID • Management VLAN ID • Link Aggregation ID • Link Aggregation Status • MTU

Key Metadata Attributes, cont'd

SIP	**Sender and receiver information to get source and destination caller information in addition to IP addresses for a SIP call:** • INVITE • ACK • BYE • REGISTER • OPTIONS • CANCEL request types
Object-relational database	**Attributes available to correlate SQL queries with query parameter values include:** • Authentication type • User's login and password strings • Protocol version • Error codes • SQL queries • Bind variables, format (text/binary) with type, and value strings and query-id • Request and response op codes • Message length • Unique identifiers for request and response
SCADA applications and Industrial Control Systems	**Securing and modernizing IT and OT (operational technologies) in critical infrastructure industries:** • Modbus: Over 30 attributes such as Modbus request and function codes • Transport unique identifier • Data record • DNP3 (Distributed Network Protocol) function code, control flags
3G/4G LTE and 5G Core Networks	**Analyzing user sessions within mobile core networks:** • User plane • Application: ID, Name, UR, family • Flow: ID, Start and End, Last Packet, Src and Dest IP, Src and Dest Port, Protocol, Src and Dest Octets and Packets • GTP session: TEID, outer Src and Dest IP

Example Applications and Protocols

Application	Protocol
ActiveSync	AMQP
Adobe	ARP
Amazon	BGP
AOL Instant Messaging	CDP (Cisco Discovery Protocol)
Apple	CHAP
Bit Torrent	CIP
Facebook	DCE/RPC
Gmail	DHCP
Google	Diameter
Hotmail	DIMP
Jabber	DNP3
Line	DNS
LinkedIn	FTP
Modbus	Gnutella
MongoDB	GTP
MySQL	H225/248
Outlook Web Access	HTTP2/Proxy
Postgres	ICMP
Pronto	IMAP
Twitter	IP4/6
WhatsApp	POP
Yahoo	Radius
Yahoo Mail	SIP
YouTube	SMTP
Zimbra	SSL

Ordering Information

Requirement	Description
GigaVUE-FM fabric manager	Single-pane-of-glass management and monitoring of all the physical and virtual nodes across your on-premises, virtual, and public cloud deployments, with simplified workflows for traffic policy configuration, end-to-end topology visualization, hierarchical grouping based on location, and customizable dashboards. Available as a hardware or a software-only virtual appliance, each GigaVUE-FM instance can manage hundreds of visibility nodes across multiple locations, including multi-cloud deployments.
GigaVUE Intelligent Appliances: GigaVUE-HCT, GigaVUE-HC1, GigaVUE-HC1-Plus, or GigaVUE-HC3 and GigaVUE Cloud Suite for cloud and virtual environments	GigaVUE Intelligent Appliances deliver consistent insight into data that travels across your network, including data centers, cloud, and remote sites. With the Gigamon solution, you will have the coverage and control you need to safeguard critical network and business assets.

Support and Services

Gigamon offers a range of support and maintenance services. For details regarding Gigamon Limited Warranty and its Product Support and Software Maintenance Programs, visit gigamon.com/support-and-services/overview-and-benefits.

About Gigamon

Gigamon offers a deep observability pipeline that harnesses actionable network-derived intelligence to amplify the power of observability tools. This powerful combination helps IT organizations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures. The result: Modern enterprises realize the full transformational promise of the cloud. Gigamon serves more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, nine of the ten largest mobile network providers, and hundreds of governments and educational organizations worldwide. To learn more, please visit gigamon.com.

Gigamon®

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

03.24_09