Application Aware Metadata

Application Metadata Intelligence powered by deep packet inspection provides summarized and context-aware information about raw packets based on Layers 4-7

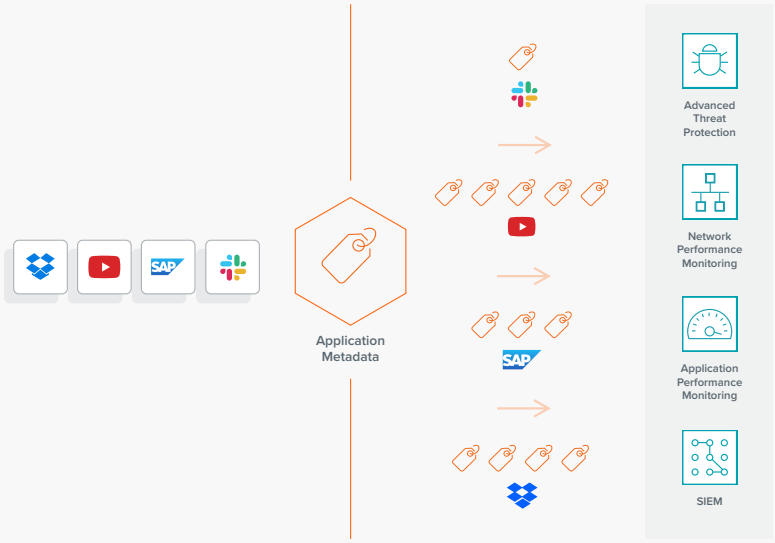

Figure 1. Application Metadata Intelligence extracts metadata elements for use by ecosystem solutions such as SIEM and performance monitoring tools

Key Features

- Over 7,000 protocol, application and user behavior L4-7 attributes spanning 3,000 apps
- Dozens of elements for apps such as Facebook and protocols including DNS, FTS, IMAP and SIP
- Identify specific users and link actions such as client login and subsequent file usage by application
- Provides metadata export capability for tunneling protocols such as GTP to address mobile carriers
- Integration with Gigamon App Visualization, App Filtering and Fabric Manager solutions
- Supported by connectors for SIEM tools-Splunk and QRadar and out-of-box by other Gigamon partners

Key Benefits

- Enable tools to measure performance, troubleshoot issues, spot security events and improve effectiveness
- 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 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

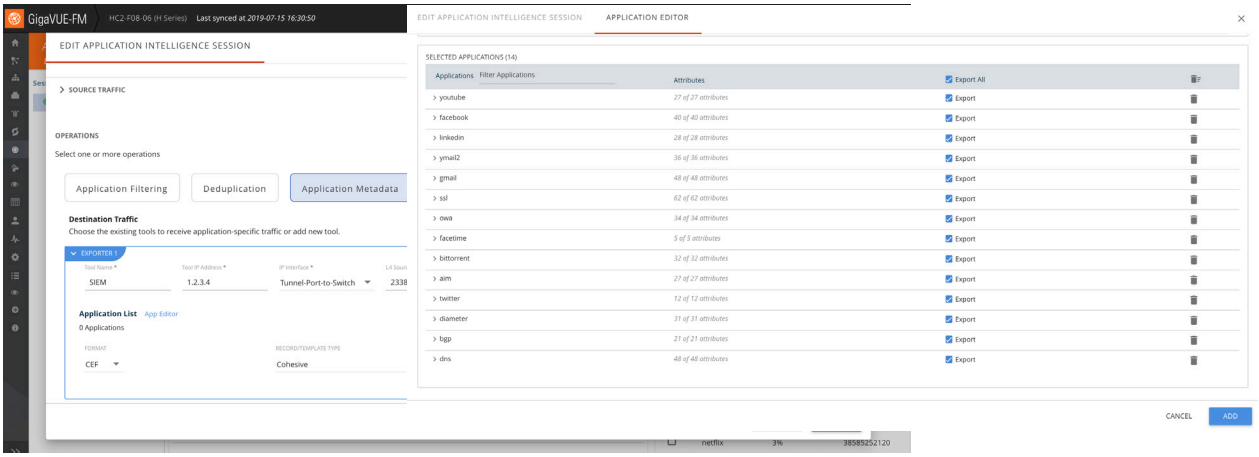

Figure 2. Dashboard allows granular selection of numerous metadata elements on a per app and protocol basis

Application Metadata Intelligence (AMI) expands upon app layer visibility derived from Gigamon's App Visualization and Filtering and supports a comprehensive approach to obtain application behavior. Organizations 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 utilizes deep packet inspection to provide summarized and context-aware information about raw network packets based on Layers 4–7. It supplies network and security tools more than 7,000 metadata attributes that shed light on the application's performance, customer experience and security. Gigamon extracts and appends elements to NetFlow and IPFIX records including:

- Identification: Social media user, file and video names, SQL requests
- HTTP: URL identification, commands response codes levels
- DNS parameters: 39 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

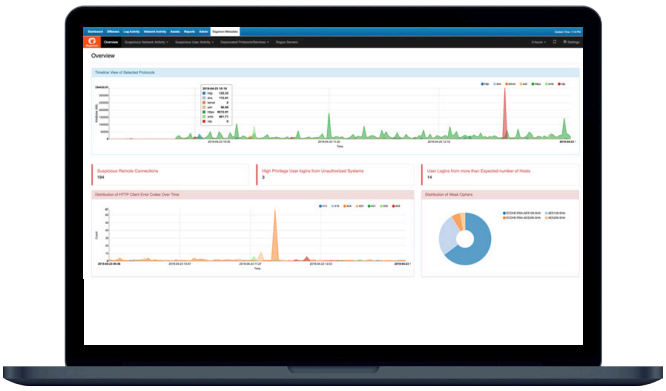

Figure 3. QRadar dashboard example displays potential malicious activity: suspicious remote logins, logins from unauthorized systems, unusual large number of user logins per host and use of weak ciphers

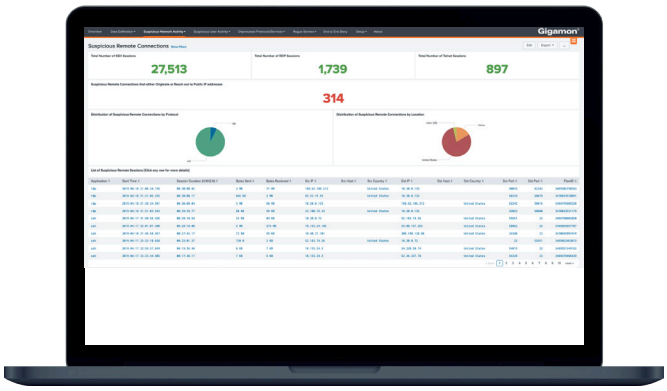

Figure 4. Spunk dashboard example displays of total number of sessions using SSH, RDP and Telnet, the number of suspicious remote connections that originate in or reach out to public IP address and their distribution by protocol and location

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, longevity of the connections as well as an unusual quantity of SSH, RDP or Telnet sessions. Time window analysis is supported 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 breache 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.

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 codes levels • HTTP certificates including those that have expired
DNS	39 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-top times • Resolution levels (i.e., standard, high-definition) and changes
URL	• HTTP GET • POST • PUT • DELETE • HEAD
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
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

Example Applications and Protocols with Number of Attributes Available

APPLICATION	PROTOCOL
• ActiveSync-57	• AMQP-13
• Adobe-11	• ARP-9
• Amazon-8	• BGP-21
• AOL Instant Messaging-41	• CDP-10 (Cisco Discovery Protocol)
• Apple-10	• CHAP-5
• Bit Torrent-35	• CIP-8
• Facebook-73	• DCE/RPC-30
• Gmail-117	• DHCP-44
• Google-91	• Diameter-33
• Hotmail-22	• DIMP-27
• Jabber-34	• DNP3-28
• Line-56	• DNS-48
• LinkedIn-28	• FTP-22
• Modbus-38	• Gnutella-15
• MongoDB-8	• GTP-133
• MySQL-13	• H225/248-74
• Outlook Web Access-35	• HTTP2/Proxy-168
• Postgres-16	• ICMP-23
• Pronto-45	• IMAP-112
• Twitter-12	• IP4/6-54
• WhatsApp-7	• POP-70
• Yahoo-43	• Radius-47
• Yahoo Mail-75	• SIP-85
• YouTube-28	• SMTP-80
• Zimbra-59	• SSL-29

Ordering Information

PRODUCT CATEGORY	PART NUMBER	DESCRIPTION
AMI License	SMT-HC1-AMI	Application Metadata Intelligence (1 Month) – GigaVUE-HC1
	SMT-HC2-AMI	Application Metadata Intelligence (1 Month) – GigaVUE-HC2
	SMT-HC3-AMI	Application Metadata Intelligence (1 Month) – GigaVUE-HC3

Note: Minimum purchase of 12 months

Learn More

For more information on Application Metadata Intelligence visit this website. As AMI is part of the overall Gigamon Application Intelligence suite; you can obtain a deeper perspective by visiting this website, reading the Solution Brief and requesting a demo.

Gigamon®

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

08.19_01