Gigamon®

Gigamon Application Metadata Intelligence for Superior Hybrid Cloud Security and Performance

Extend network intelligence capabilities of existing observability, SIEM, and network performance monitoring tools to proactively detect vulnerabilities and accelerate troubleshooting

KEY BENEFITS

- Enhance observability tools, SIEMs, and custom tools with up to 6,000 application attributes to identify vulnerabilities and unsanctioned activities
- Improve application performance and uptime with the information needed to pinpoint the causes of bottlenecks and outages
- Add more context to logs through incorruptible network telemetry from AMI
- Identify GenAI apps for enhanced security with AI traffic visibility and governance

Introduction

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 is 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 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 with the following benefits:

- Gain full stack visibility without the need for aggregation and correlation across multiple events and logs.
- Reduce noise by combining with other Gigamon traffic optimization techniques.
- Streamline data ingestion with structured data in standard export formats.
- Gather concise metadata information for troubleshooting issues.

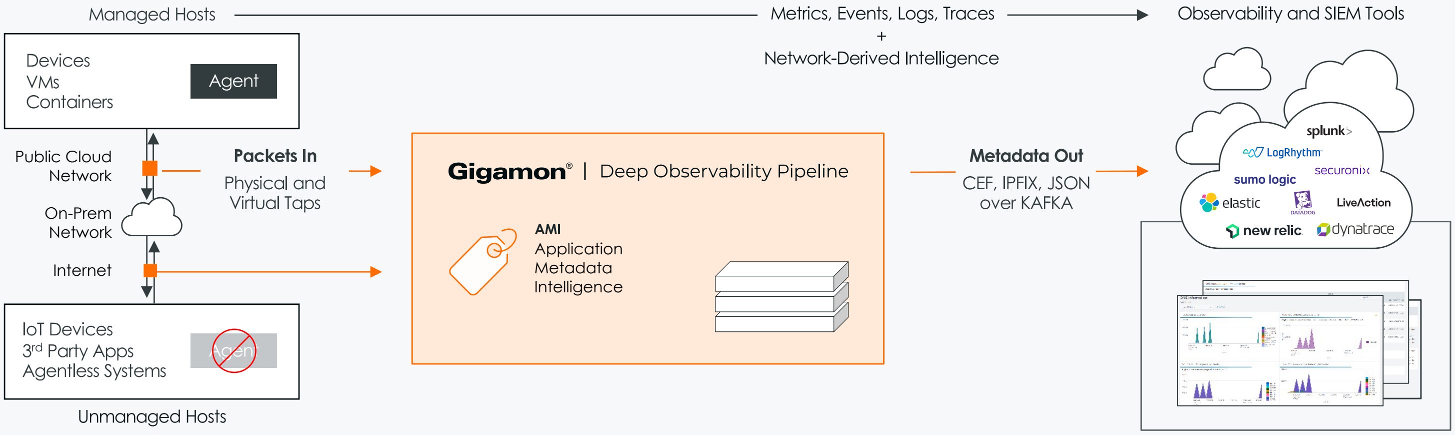


Figure 1. AMI augments MELT with network-derived intelligence. AMI data is ingested, analyzed, and visualized through our partner ecosystem tools.

Gigamon AMI Starter Packs comprises of pre-defined tool templates and plugins. The pre-defined tool templates help to export the relevant metadata attributes from the Gigamon device, and the plugins help to visualize the use cases in our partner ecosystem tools. Customers can download the plugins from the partner's marketplace as applicable. The starter packs allow you to pre-select the application and attributes required for the specific use case.

With AMI, you get this additional visibility through your existing tools. There is no need to buy additional tools or change the monitoring processes that your teams know so well. Gigamon has pre-built integrations with the most common security and observability tools, including, but not limited to: Dynatrace, Datadog, New Relic, Splunk, QRadar, Elastic. Now one of the top things on an operations team's wish list – to have a single-pane-of-glass for unified visibility across all environments – is a reality.

AMI Starter Pack	Security Posture	Anomalous Traffic	Troubleshooting	Suspicious Activities	Rogue Activities	M-21-31 Logging
Use Case	Detect and remediate flaws in securing applications in the network.	Detect and remediate challenges with HTTP, HTTPS, and DNS traffic.	Detect and remediate latency, connectivity, and protocol errors in the network.	Detect and remediate issues related to unmanaged devices, suspicious connections, and traffic outside norms.	Detect and remediate issues related to unsanctioned applications that can pose challenges to network and security.	Support a Zero Trust journey with U.S. Office of Management and Budget M-21-31 logging requirements.
Identify	• Untrusted Certificates • TLS Versions • Weak Cipher • Key Exchange Protocols • Signature Algorithms • Cryptographic Hashes • Compression Algorithm	• Unusual DNS Traffic • Shadow IT • Suspicious DNS Traffic • Abnormal activities in HTTPS/Web traffic • HTTP Traffic Policy Violations • Suspicious HTTP Traffic	• Server vs Network Latency • TCP/IP Connectivity Issues • DNS Server Failures • SIP Protocol Errors	• IoT Unmanaged Devices • Unwanted Services and Port Misuse • Traffic Outside Norms	• Unsanctioned P2P Apps • Crypto Jacking	• HTTPS and PKI Traffic Details • DNS Information • Shadow IT • IoMT Protocol Activity • OT Monitoring • Web Traffic Details

Figure 2. Application Metadata Intelligence Starter Packs.

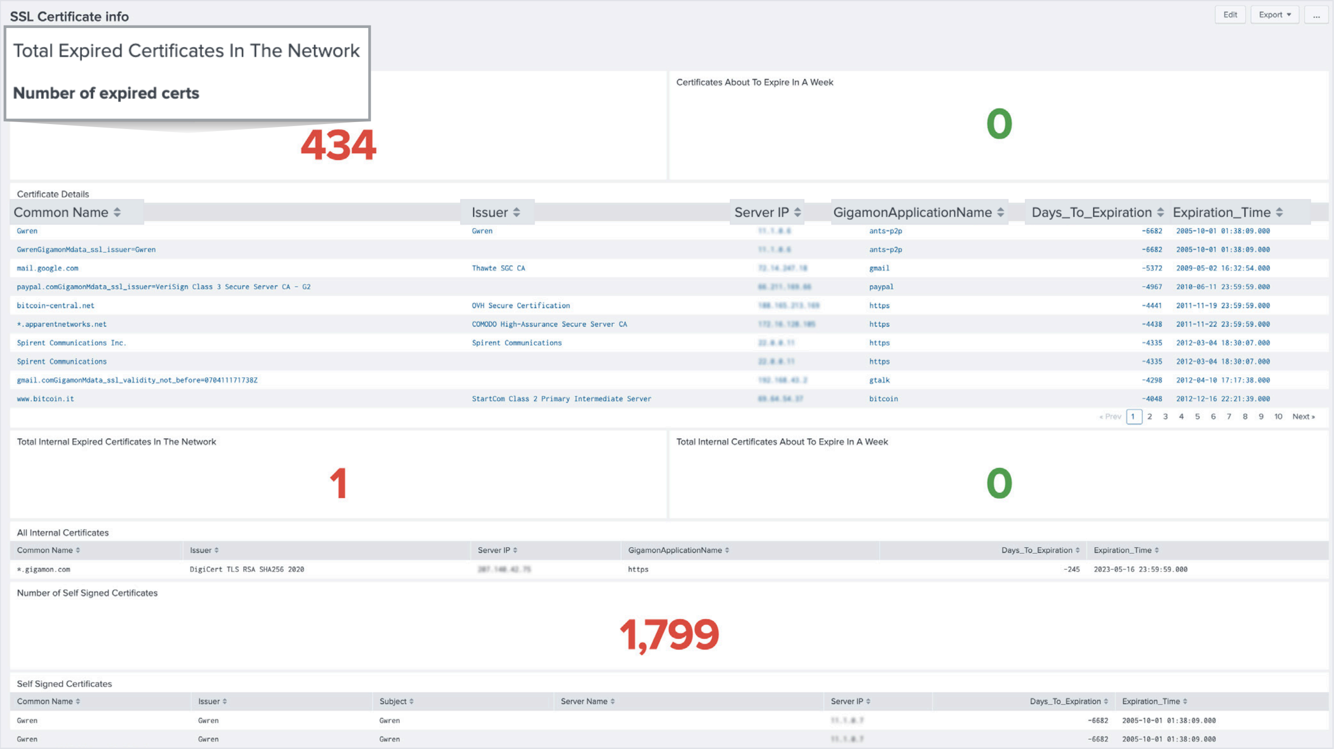
Security Posture and Anomalous Traffic Use Cases for SecOps, CloudOps, DevSecOps

Detect and remediate flaws in securing the applications and challenges with HTTP, HTTPS, and DNS traffic

Gigamon AMI ensures that your tools can correlate application behavior from AMI along with MELT to get a full picture of a specific security incident. Cryptographic failures are ranked second among Open Web Application Security Project (OWASP) Top 10 2021 failures. A lack of cryptographic security can make applications vulnerable. The SecOps, CloudOps, and DevSecOps teams have a need to verify whether TLS/SSL applications comply with their security policy and quickly identify and remediate any inconsistencies. With AMI, they can automate detection of anomalies such as unusual activities and vulnerable applications to stop cyber risks that overcome perimeter or endpoint protection.

Monitoring TLS/SSL certificates
Applications should use trusted certificates to ensure their legitimacy. Organizations have a need to check whether applications are using certificates issued by trusted and approved Certificate Authorities (CAs). AMI enables you to export metadata to SIEMs to identify the following for further investigation and remediation:

- Application Name and its host address
- Certificates that are expired or about to expire
- Self-signed certificates
- Certificates issued by untrusted CAs



Total Expired Certificates In The Network

Number of expired certs

434

Certificates About To Expire In A Week

0

Certificate Details

Common Name	Issuer	Server IP	GigamonApplicationName	Days_To_Expiration	Expiration_Time
Gwren	Gwren	[redacted]	ants-p2p	-6682	2005-10-01 01:38:09.000
GwrenGigamonMdata_ssl_issuer=Gwren		[redacted]	ants-p2p	-6682	2005-10-01 01:38:09.000
mail.google.com	Thawte SGC CA	[redacted]	gmail	-5372	2009-05-02 16:32:54.000
paypal.comGigamonMdata_ssl_issuer=VeriSign Class 3 Secure Server CA - G2		[redacted]	paypal	-4967	2010-06-11 23:59:59.000
bitcoin-central.net	OVH Secure Certification	[redacted]	https	-4441	2011-11-19 23:59:59.000
*.apparentnetworks.net	COMODO High-Assurance Secure Server CA	[redacted]	https	-4438	2011-11-22 23:59:59.000
Spirent Communications Inc.	Spirent Communications	[redacted]	https	-4335	2012-03-04 18:30:07.000
Spirent Communications		[redacted]	https	-4335	2012-03-04 18:30:07.000
gmail.comGigamonMdata_ssl_validity_not_before=070411171738Z		[redacted]	gtalk	-4298	2012-04-10 17:17:38.000
www.bitcoin.it	StartCom Class 2 Primary Intermediate Server	[redacted]	bitcoin	-4048	2012-12-16 22:21:39.000

Total Internal Expired Certificates In The Network

1

Total Internal Certificates About To Expire In A Week

0

All Internal Certificates

Common Name	Issuer	Server IP	GigamonApplicationName	Days_To_Expiration	Expiration_Time
*.gigamon.com	DigiCert TLS RSA SHA256 2020	[redacted]	https	-245	2023-05-16 23:59:59.000

Number of Self Signed Certificates

1,799

Self Signed Certificates

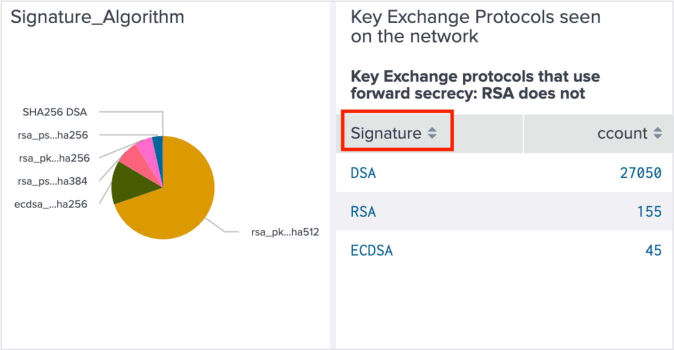
Common Name	Issuer	Subject	Server Name	Server IP	Days_To_Expiration	Expiration_Time
Gwren	Gwren	Gwren		[redacted]	-6682	2005-10-01 01:38:09.000
Gwren	Gwren	Gwren		[redacted]	-6682	2005-10-01 01:38:09.000

Figure 3. AMI metadata visualized in Splunk.

Monitoring Perfect Forward Secrecy (PFS)

Applications should use PFS to protect past sessions against future compromises of private keys. Security teams need to be able to check whether applications use Key Exchange protocols that support PFS and then identify and remediate noncompliant encryption protocols and algorithms. With AMI, teams can export metadata to SIEMs to identify the following for further investigation and remediation:

- Key exchange protocols
- Signature algorithms


Signature_Algorithm

Key Exchange Protocols seen on the network

Key Exchange protocols that use forward secrecy: RSA does not

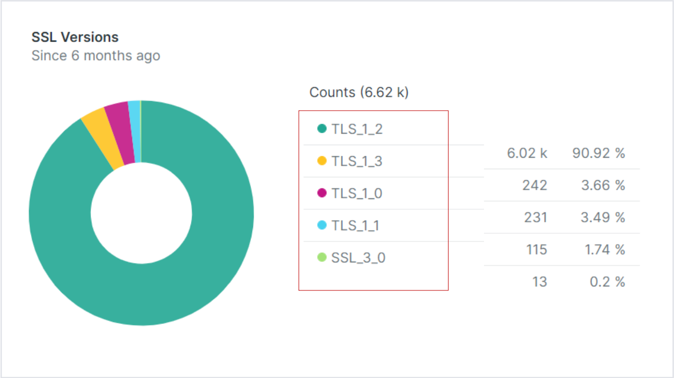
Signature ⇕	ccount ⇕
DSA	27050
RSA	155
ECDSA	45

Figure 4. AMI metadata visualized in Splunk.

Monitoring TLS/SSL versions

Applications should use the latest TLS/SSL version to protect against known vulnerabilities. This helps the security teams to identify the applications to be updated or retired. With AMI, you can export metadata to SIEMs to identify the following for further investigation and remediation:

- Older SSL/TLS versions
- Application and the endpoints


SSL Versions
Since 6 months ago

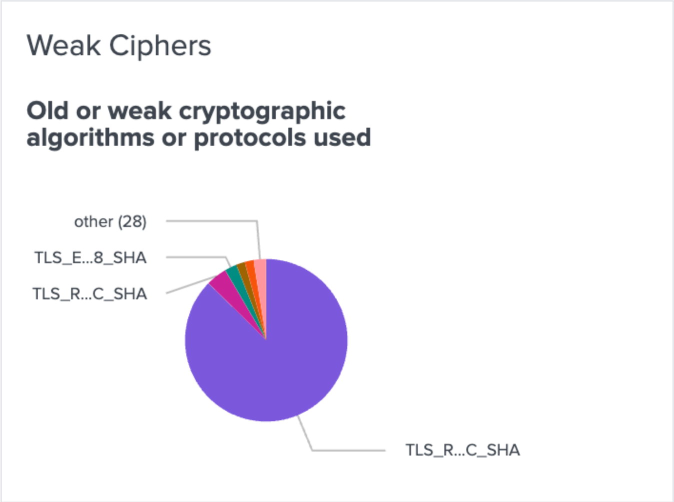
Counts (6.62 k)

● TLS_1_2	6.02 k	90.92 %
● TLS_1_3	242	3.66 %
● TLS_1_0	231	3.49 %
● TLS_1_1	115	1.74 %
● SSL_3_0	13	0.2 %

Figure 5. AMI metadata visualized in Splunk.

Monitoring weak ciphers

Applications should use strong algorithms for authentication, encryption and integrity of data in motion. There is a need to check whether ciphers that govern TLS/SSL session comply with the security policy. AMI can help export metadata to SIEMs to review and harden server and client-side configurations to use more secure ciphers. For example, use keys that support PFS (DSA, ECDSA) and minimum 128-bit encryption (AES128 or above) and avoid hashing algorithms that are prone to collision (SHA1, MD5).


Weak Ciphers

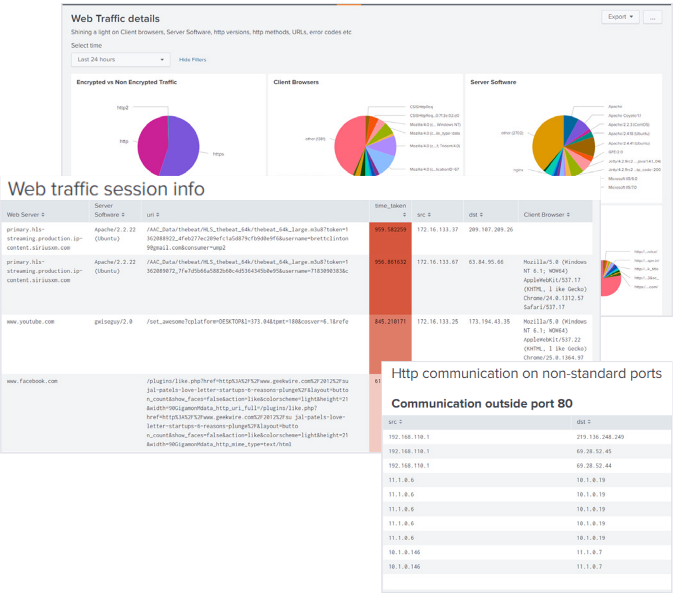
Old or weak cryptographic algorithms or protocols used

Figure 6. AMI metadata visualized in Splunk.

Monitoring HTTP traffic for policy violations

SecOps teams have a need to check whether the HTTP traffic and the endpoints involved comply with baseline security requirements. With AMI, you can export metadata to SIEMs to identify the following for further investigation and remediation:

- Types of servers and their version and port numbers
- HTTP versions
- Types of user agents



Web traffic session info

Web Server ⇕	Server Software ⇕	uri ⇕	time_taken ⇕	src ⇕	dst ⇕	Client Browser ⇕
primary.hls-streaming.production.ip-content.siriusxm.com	Apache/2.2.22 (Ubuntu)	/AAC_Data/thebeat/HLS_thebeat_64k/thebeat_64k_large.m3u8?token=1362088922_4feb277ec209efc1a5d879cfb9d0e9f6&username=brettclinton9@gmail.com&consumer=ump2	959.582259	172.16.133.37	209.107.209.26	
primary.hls-streaming.production.ip-content.siriusxm.com	Apache/2.2.22 (Ubuntu)	/AAC_Data/thebeat/HLS_thebeat_64k/thebeat_64k_large.m3u8?token=1362089072_7fe7d5b66a5882b60c4d5364345b0e95&username=7183090383&c	956.861632	172.16.133.67	63.84.95.66	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.17 (KHTML, l ike Gecko) Chrome/24.0.1312.57 Safari/537.17
www.youtube.com	gwiseguy/2.0	/set_awesome?cplatform=DESKTOP&l=373.04&tpmt=180&cosver=6.1&refe	845.210171	172.16.133.25	173.194.43.35	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.22 (KHTML, l ike Gecko) Chrome/25.0.1364.97
www.facebook.com		/plugins/like.php?href=http%3A%2F%2Fwww.geekwire.com%2F2012%2Fsu jal-patels-love-letter-startups-6-reasons-plunge%2F&layout=button_count&show_faces=false&action=like&colorscheme=light&height=21&width=90GigamonMdata_http_uri_full=/plugins/like.php?href=http%3A%2F%2Fwww.geekwire.com%2F2012%2Fsu jal-patels-love-letter-startups-6-reasons-plunge%2F&layout=button_count&show_faces=false&action=like&colorscheme=light&height=21&width=90GigamonMdata_http_mime_type=text/html	61			

Http communication on non-standard ports

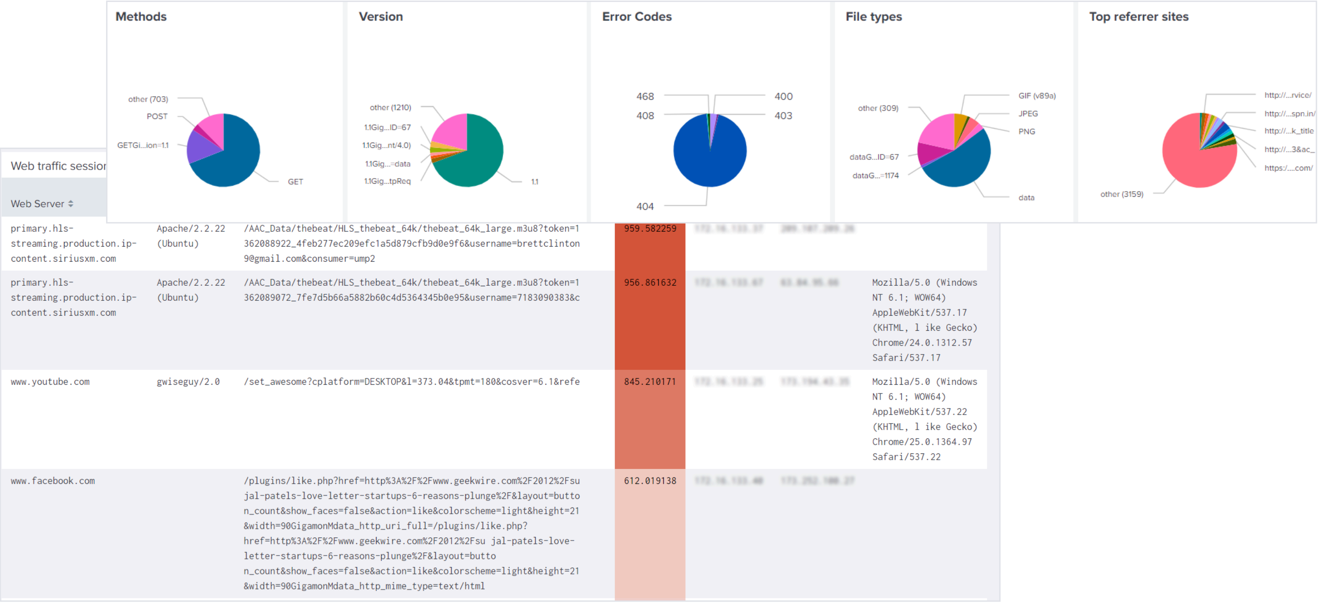
Communication outside port 80

src ⇕	dst ⇕
192.168.110.1	219.136.248.249
192.168.110.1	69.28.52.45
192.168.110.1	69.28.52.44
11.1.0.6	10.1.0.19
11.1.0.6	10.1.0.19
11.1.0.6	10.1.0.19
11.1.0.6	10.1.0.19
11.1.0.6	10.1.0.19
10.1.0.146	11.1.0.7
10.1.0.146	11.1.0.7

Figure 7. AMI metadata visualized in Splunk.

Monitoring suspicious HTTP traffic

SecOps teams have the responsibility to dissect the HTTP connections to uncover malicious intent such as uncommon redirections, unwarranted file transfers, bad/unauthorized/forbidden client requests, etc. AMI helps them to export metadata to SIEMs to monitor end-to-end connection details for further investigation and remediation.



Web traffic session info

Web Server ⇕						
primary.hls-streaming.production.ip-content.siriusxm.com	Apache/2.2.22 (Ubuntu)	/AAC_Data/thebeat/HLS_thebeat_64k/thebeat_64k_large.m3u8?token=1362088922_4feb277ec209efc1a5d879cfb9d0e9f6&username=brettclinton9@gmail.com&consumer=ump2	959.582259	[redacted]	[redacted]	
primary.hls-streaming.production.ip-content.siriusxm.com	Apache/2.2.22 (Ubuntu)	/AAC_Data/thebeat/HLS_thebeat_64k/thebeat_64k_large.m3u8?token=1362089072_7fe7d5b66a5882b60c4d5364345b0e95&username=7183090383&c	956.861632	[redacted]	[redacted]	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.17 (KHTML, l ike Gecko) Chrome/24.0.1312.57 Safari/537.17
www.youtube.com	gwiseguy/2.0	/set_awesome?cplatform=DESKTOP&l=373.04&tpmt=180&cosver=6.1&refe	845.210171	[redacted]	[redacted]	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.22 (KHTML, l ike Gecko) Chrome/25.0.1364.97 Safari/537.22
www.facebook.com		/plugins/like.php?href=http%3A%2F%2Fwww.geekwire.com%2F2012%2Fsu jal-patels-love-letter-startups-6-reasons-plunge%2F&layout=button_count&show_faces=false&action=like&colorscheme=light&height=21&width=90GigamonMdata_http_uri_full=/plugins/like.php?href=http%3A%2F%2Fwww.geekwire.com%2F2012%2Fsu jal-patels-love-letter-startups-6-reasons-plunge%2F&layout=button_count&show_faces=false&action=like&colorscheme=light&height=21&width=90GigamonMdata_http_mime_type=text/html	612.019138	[redacted]	[redacted]	

Figure 8. AMI metadata visualized in Splunk.

Monitoring unusual DNS traffic to detect and remediate DNS attacks

NetOps and SecOps teams are required to check whether DNS infrastructure is subject to any DNS attacks such as Amplification/Reflection/Combined DDOS attacks. Their need is to identify and remediate the endpoints involved. With AMI, they can export metadata to SIEMs to identify the following for further investigation and remediation (as visualized in Spunk using AMI metadata):

- Trends in the DNS traffic e.g., DNS traffic trend per domain and per endpoints.
- Clients and servers involved in DNS look ups along with the types of queries, records, and responses.

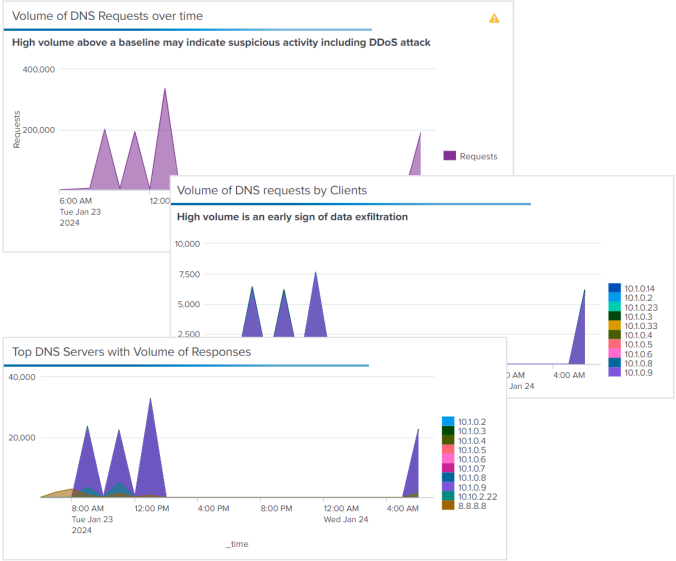
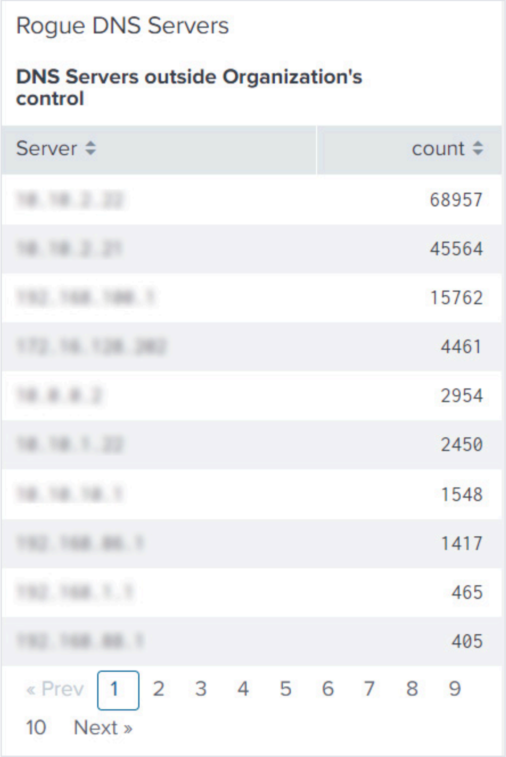


Figure 9. AMI metadata visualized in Splunk.

Detect and remediate rogue DNS servers by monitoring shadow IT

Attackers can host shadow IT within your network for diverting traffic and launching man-in-the-middle attacks. The NetOps and SecOps teams need to be able to identify and remediate the server(s) involved. AMI provides details that help you list the total number of DNS servers in your network, distinguishing rogue servers from those that are trusted or publicly known servers.



Rogue DNS Servers

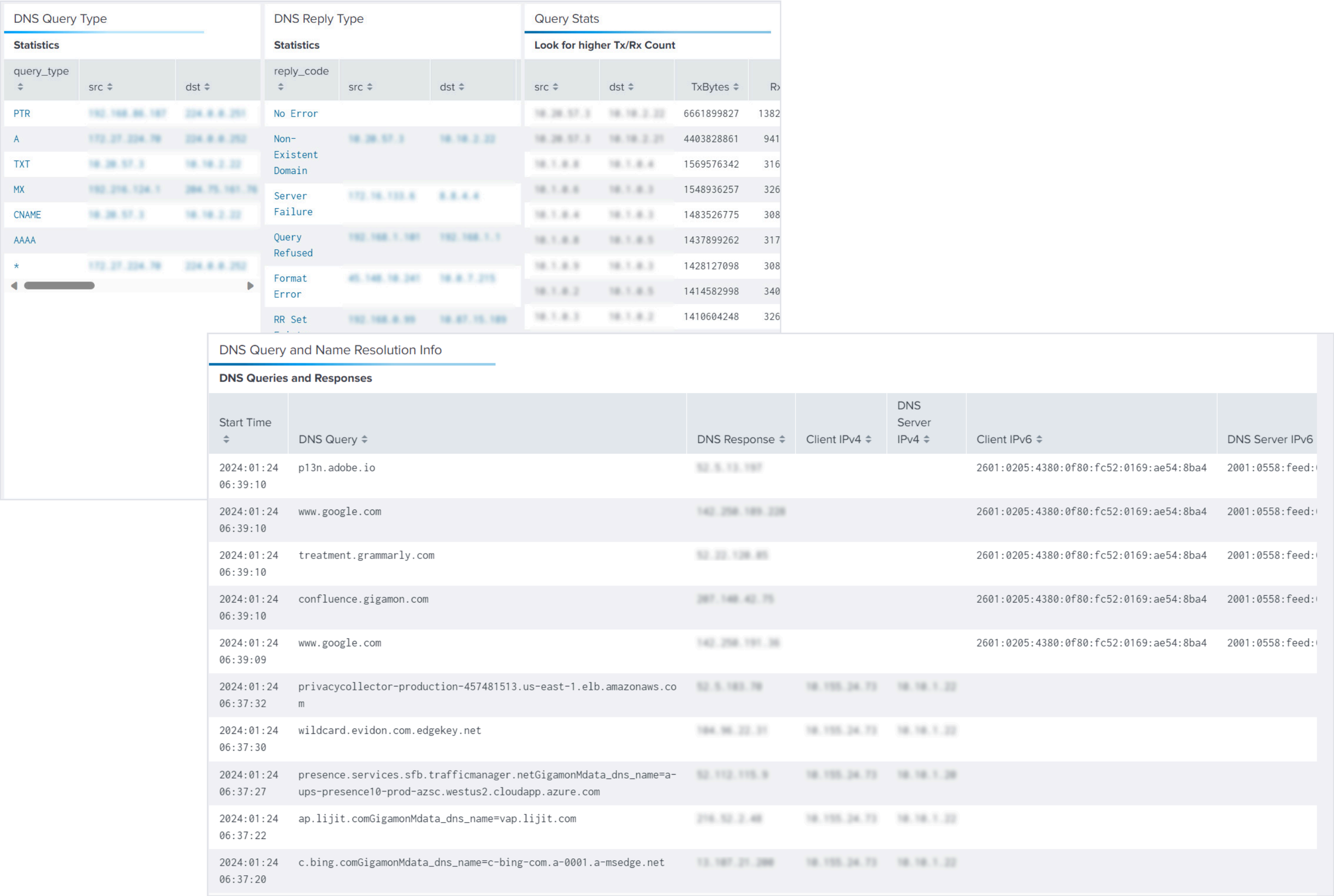
DNS Servers outside Organization's control

Server ⬍	count ⬍
[redacted]	68957
[redacted]	45564
[redacted]	15762
[redacted]	4461
[redacted]	2954
[redacted]	2450
[redacted]	1548
[redacted]	1417
[redacted]	465
[redacted]	405

Figure 10. AMI metadata visualized in Splunk.

Detect uncommon DNS queries, records and response types.
NetOps and SecOps teams should be able to check for any uncommon domains, DNS Tunneling and policy violations and identify and remediate the endpoints involved. AMI helps these teams to monitor suspicious DNS traffic by exporting metadata to SIEMs to identify the following for further investigation and remediation:

- Domains and records' types, counts, and sizes.
- Unusual count of DNS queries indicating potential nefarious activity.



DNS Query Type

Statistics

query_type	src	dst
PTR	[redacted]	[redacted]
A	[redacted]	[redacted]
TXT	[redacted]	[redacted]
MX	[redacted]	[redacted]
CNAME	[redacted]	[redacted]
AAAA		
*	[redacted]	[redacted]

DNS Reply Type

Statistics

reply_code	src	dst
No Error		
Non-Existent Domain	[redacted]	[redacted]
Server Failure	[redacted]	[redacted]
Query Refused	[redacted]	[redacted]
Format Error	[redacted]	[redacted]
RR Set	[redacted]	[redacted]

Query Stats

Look for higher Tx/Rx Count

src	dst	TxBytes	Rx
[redacted]	[redacted]	6661899827	1382
[redacted]	[redacted]	4403828861	941
[redacted]	[redacted]	1569576342	316
[redacted]	[redacted]	1548936257	326
[redacted]	[redacted]	1483526775	308
[redacted]	[redacted]	1437899262	317
[redacted]	[redacted]	1428127098	308
[redacted]	[redacted]	1414582998	340
[redacted]	[redacted]	1410604248	326

DNS Query and Name Resolution Info

DNS Queries and Responses

Start Time	DNS Query	DNS Response	Client IPv4	DNS Server IPv4	Client IPv6	DNS Server IPv6
2024:01:24 06:39:10	p13n.adobe.io	[redacted]			2601:0205:4380:0f80:fc52:0169:ae54:8ba4	2001:0558:feed:
2024:01:24 06:39:10	www.google.com	[redacted]			2601:0205:4380:0f80:fc52:0169:ae54:8ba4	2001:0558:feed:
2024:01:24 06:39:10	treatment.grammarly.com	[redacted]			2601:0205:4380:0f80:fc52:0169:ae54:8ba4	2001:0558:feed:
2024:01:24 06:39:10	confluence.gigamon.com	[redacted]			2601:0205:4380:0f80:fc52:0169:ae54:8ba4	2001:0558:feed:
2024:01:24 06:39:09	www.google.com	[redacted]			2601:0205:4380:0f80:fc52:0169:ae54:8ba4	2001:0558:feed:
2024:01:24 06:37:32	privacycollector-production-457481513.us-east-1.elb.amazonaws.com	[redacted]	[redacted]	[redacted]		
2024:01:24 06:37:30	wildcard.evidon.com.edgekey.net	[redacted]	[redacted]	[redacted]		
2024:01:24 06:37:27	presence.services.sfb.trafficmanager.netGigamonMdata_dns_name=a-ups-presence10-prod-azsc.westus2.cloudapp.azure.com	[redacted]	[redacted]	[redacted]		
2024:01:24 06:37:22	ap.lijit.comGigamonMdata_dns_name=vap.lijit.com	[redacted]	[redacted]	[redacted]		
2024:01:24 06:37:20	c.bing.comGigamonMdata_dns_name=c-bing-com.a-0001.a-msedge.net	[redacted]	[redacted]	[redacted]		

Figure 11. AMI metadata visualized in Splunk.

Troubleshooting Use Cases

Detect and Remediate Network Delay, Connectivity, and Protocol Errors in the Network

Whether your applications and workloads are in cloud and/or on-prem, AMI can help you with application performance analysis viz-a-viz server delay vs network delay. The following AMI starter packs empower you to detect and remediate latency issues in your network.

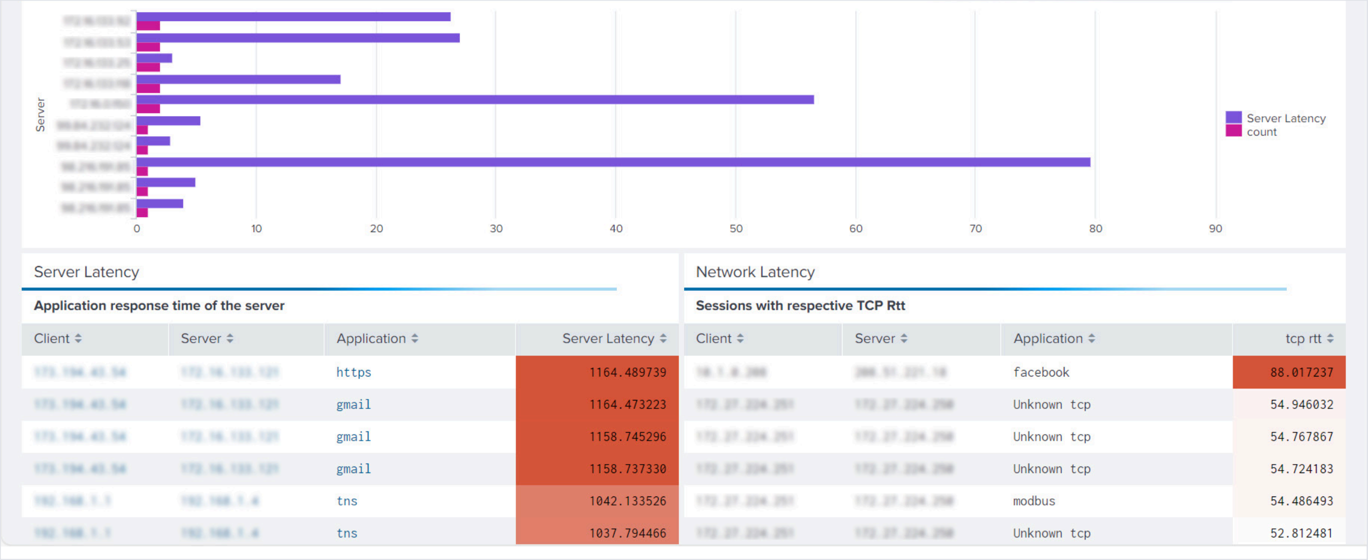
Isolate between network delay and server delay in the network.
The NetOps, CloudOps, DevOps, and DevSecOps have the need for visibility into latency issues and to know whether it is happening on the network or on the server side that is providing connectivity to the applications browsed by the end user.

Users want to be able to determine:

- How much is the network delay and the delta between the network and server delay
- What are the worst-performing servers
- Which application use is experiencing server or network latency

AMI can be used to:

- Report on TCP round-trip-time pointing to latency between the user and the network
- Report on the application round-trip-time to identify the latency added by the servers providing that application connectivity
- Identify the worst-performing servers
- Metadata can be exported to performance tools and is useful for troubleshooting network latency issues



Server Latency

Application response time of the server

Client ⬍	Server ⬍	Application ⬍	Server Latency ⬍
[redacted]	[redacted]	https	1164.489739
[redacted]	[redacted]	gmail	1164.473223
[redacted]	[redacted]	gmail	1158.745296
[redacted]	[redacted]	gmail	1158.737330
[redacted]	[redacted]	tns	1042.133526
[redacted]	[redacted]	tns	1037.794466

Network Latency

Sessions with respective TCP Rtt

Client ⬍	Server ⬍	Application ⬍	tcp rtt ⬍
[redacted]	[redacted]	facebook	88.017237
[redacted]	[redacted]	Unknown tcp	54.946032
[redacted]	[redacted]	Unknown tcp	54.767867
[redacted]	[redacted]	Unknown tcp	54.724183
[redacted]	[redacted]	modbus	54.486493
[redacted]	[redacted]	Unknown tcp	52.812481

Figure 12. AMI metadata visualized in Splunk.

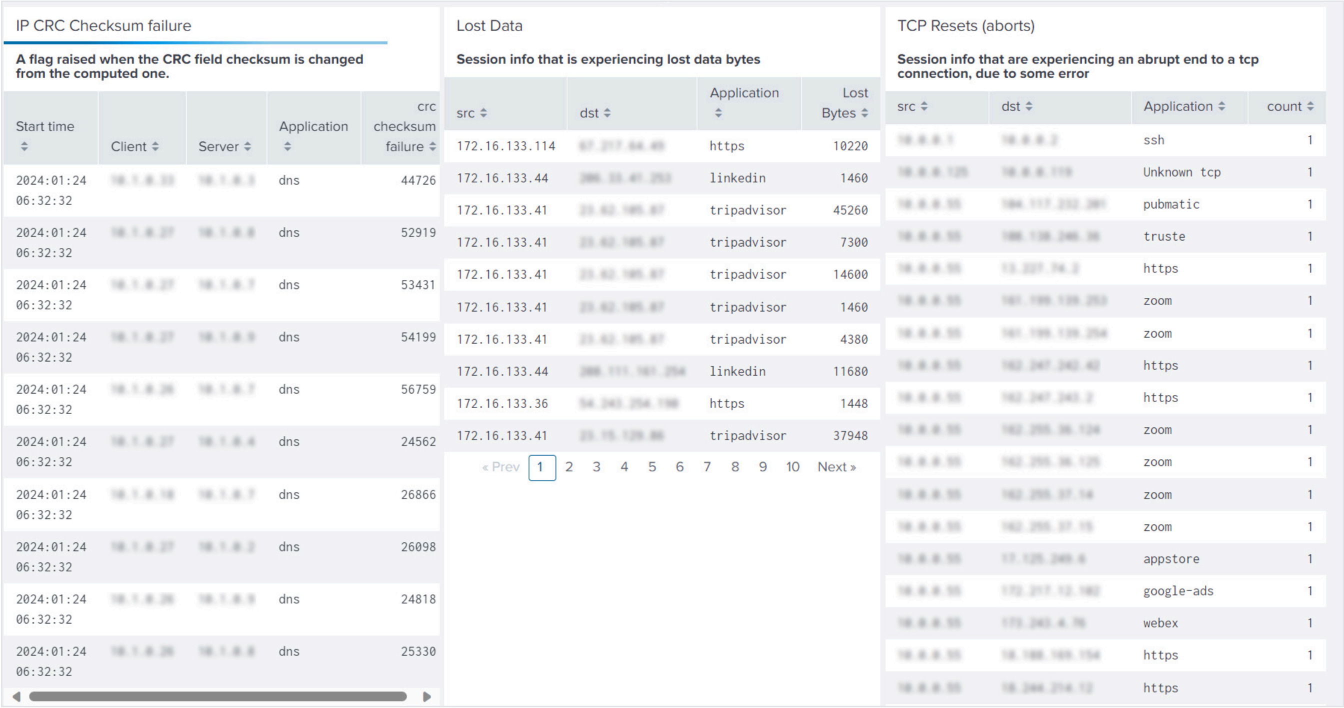
Detect and remediate TCP connectivity issues in your network.

NetOps, CloudOps, DevOps, and DevSecOps teams need visibility into connectivity issues experienced by the users due to any of these network reasons:

- Where in the network TCP resets are happening
- Where in the network retransmission and packet loss is happening
- Whether resets are not due to retransmission or incorrect parameters to narrow it down to application-level reset

AMI helps these teams to:

- Identify sessions with TCP reset along with the source, destination, and application information
- Identify sessions with packet loss with details on lost bytes, source, destination, and application information
- Identify sessions with CRC checksum failures
- The metadata can be exported to performance tools and is useful for troubleshooting TCP connection issues



IP CRC Checksum failure

A flag raised when the CRC field checksum is changed from the computed one.

Start time ⇕	Client ⇕	Server ⇕	Application ⇕	crc checksum failure ⇕
2024:01:24 06:32:32	[redacted]	[redacted]	dns	44726
2024:01:24 06:32:32	[redacted]	[redacted]	dns	52919
2024:01:24 06:32:32	[redacted]	[redacted]	dns	53431
2024:01:24 06:32:32	[redacted]	[redacted]	dns	54199
2024:01:24 06:32:32	[redacted]	[redacted]	dns	56759
2024:01:24 06:32:32	[redacted]	[redacted]	dns	24562
2024:01:24 06:32:32	[redacted]	[redacted]	dns	26866
2024:01:24 06:32:32	[redacted]	[redacted]	dns	26098
2024:01:24 06:32:32	[redacted]	[redacted]	dns	24818
2024:01:24 06:32:32	[redacted]	[redacted]	dns	25330

Lost Data

Session info that is experiencing lost data bytes

src ⇕	dst ⇕	Application ⇕	Lost Bytes ⇕
172.16.133.114	[redacted]	https	10220
172.16.133.44	[redacted]	linkedin	1460
172.16.133.41	[redacted]	tripadvisor	45260
172.16.133.41	[redacted]	tripadvisor	7300
172.16.133.41	[redacted]	tripadvisor	14600
172.16.133.41	[redacted]	tripadvisor	1460
172.16.133.41	[redacted]	tripadvisor	4380
172.16.133.44	[redacted]	linkedin	11680
172.16.133.36	[redacted]	https	1448
172.16.133.41	[redacted]	tripadvisor	37948

TCP Resets (aborts)

Session info that are experiencing an abrupt end to a tcp connection, due to some error

src ⇕	dst ⇕	Application ⇕	count ⇕
[redacted]	[redacted]	ssh	1
[redacted]	[redacted]	Unknown tcp	1
[redacted]	[redacted]	pubmatic	1
[redacted]	[redacted]	truste	1
[redacted]	[redacted]	https	1
[redacted]	[redacted]	zoom	1
[redacted]	[redacted]	zoom	1
[redacted]	[redacted]	https	1
[redacted]	[redacted]	https	1
[redacted]	[redacted]	zoom	1
[redacted]	[redacted]	zoom	1
[redacted]	[redacted]	zoom	1
[redacted]	[redacted]	zoom	1
[redacted]	[redacted]	appstore	1
[redacted]	[redacted]	google-ads	1
[redacted]	[redacted]	webex	1
[redacted]	[redacted]	https	1
[redacted]	[redacted]	https	1

Figure 13. AMI metadata visualized in Splunk.

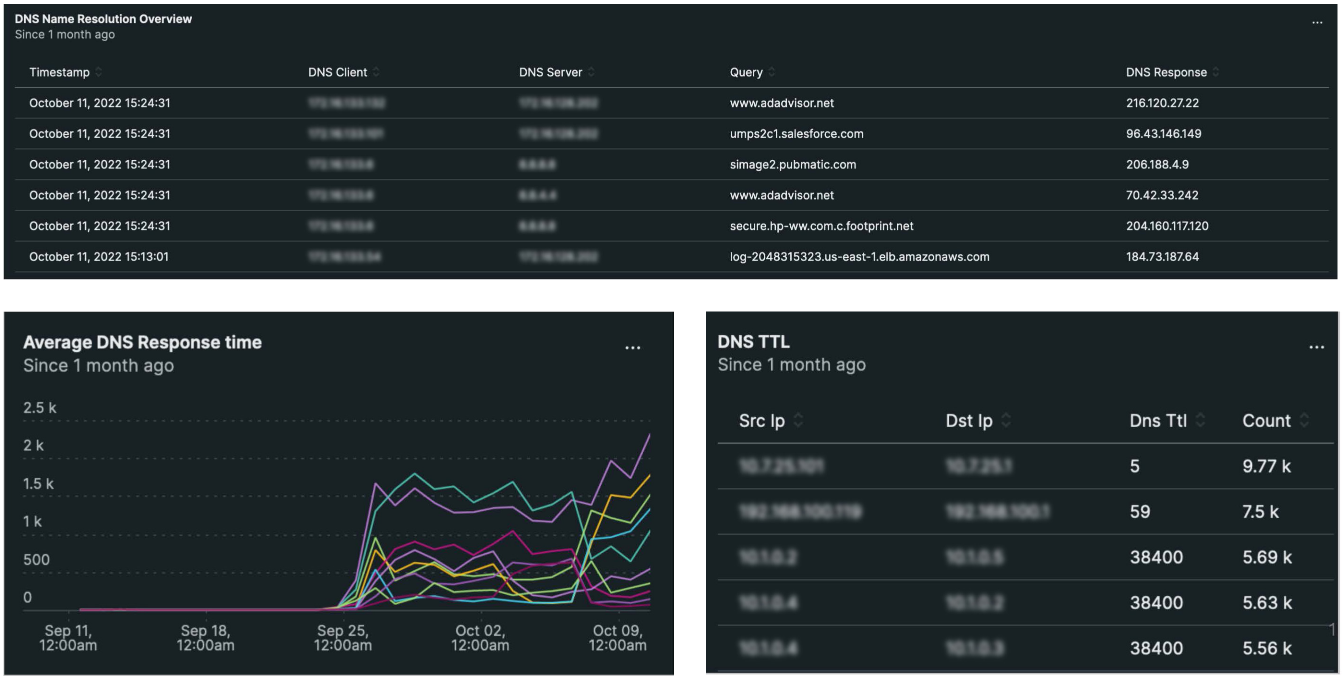
Analyze poor application response times by detecting and remediating DNS issues in your network.

NetOps teams require visibility into DNS transactions in their network for a wide range of applications:

- Visibility into DNS performance determined by DNS server response times
- Determine DNS configuration issues that make some sites unreachable
- Visibility into volume of traffic monitoring for key DNS servers

AMI can help them to:

- Identify DNS transactions with details on DNS server IP, source and destination IP and application information
- Identify the top DNS servers being queried over a period
- Identify DNS response times of the top DNS servers being used
- Monitor DNS time-to-live to see how long it takes f or DNS record updates to reach the end user helping identify possible misconfigurations



DNS Name Resolution Overview
Since 1 month ago

Timestamp	DNS Client	DNS Server	Query	DNS Response
October 11, 2022 15:24:31	[redacted]	[redacted]	www.adadvisor.net	216.120.27.22
October 11, 2022 15:24:31	[redacted]	[redacted]	umps2c1.salesforce.com	96.43.146.149
October 11, 2022 15:24:31	[redacted]	[redacted]	simage2.pubmatic.com	206.188.4.9
October 11, 2022 15:24:31	[redacted]	[redacted]	www.adadvisor.net	70.42.33.242
October 11, 2022 15:24:31	[redacted]	[redacted]	secure.hp-ww.com.c.footprint.net	204.160.117.120
October 11, 2022 15:13:01	[redacted]	[redacted]	log-2048315323.us-east-1.elb.amazonaws.com	184.73.187.64

DNS TTL
Since 1 month ago

Src Ip	Dst Ip	Dns Ttl	Count
[redacted]	[redacted]	5	9.77 k
[redacted]	[redacted]	59	7.5 k
[redacted]	[redacted]	38400	5.69 k
[redacted]	[redacted]	38400	5.63 k
[redacted]	[redacted]	38400	5.56 k

Figure 14. AMI metadata visualized in New Relic.

Availability of applications to end users by defining SLOs.
It has become a critical requirement for the applications to be available without any glitches. For any business to run with zero downtime, the applications need to be both secure and available to their end users for a rich customer experience. The availability of applications is defined by SLIs (service-level indicators) and SLOs (service-level objects). SLOs are high-level goals that are defined as percentages over time. For example, 99.5 percent of requests shall be successfully processed per minute or 99.7 percent of the requests serviced per minute shall have sub 10m latency, etc. SLIs are the quantitative measures or metrics that help to track the SLOs. AMI can help to measure SLIs such as latency (e.g., network, app, and server response time), errors (e.g., lost bytes, malformed packets, http errors) and user traffic (e.g., http requests/sec, concurrent users). You can then create SLOs to measure the performance and uptime of your applications. Based on those SLOs, you can compute metrics such as app uptime, round-trip time, resets, and drops that indicate the health of the applications. Using AMI, you can also set up notifications and alarms in your tools if the availability SLO goes down a certain threshold and the overall security score takes a dip.

Suspicious Activities Use Cases

Detect and remediate issues related to unmanaged devices, suspicious connections, traffic outside norms in the network

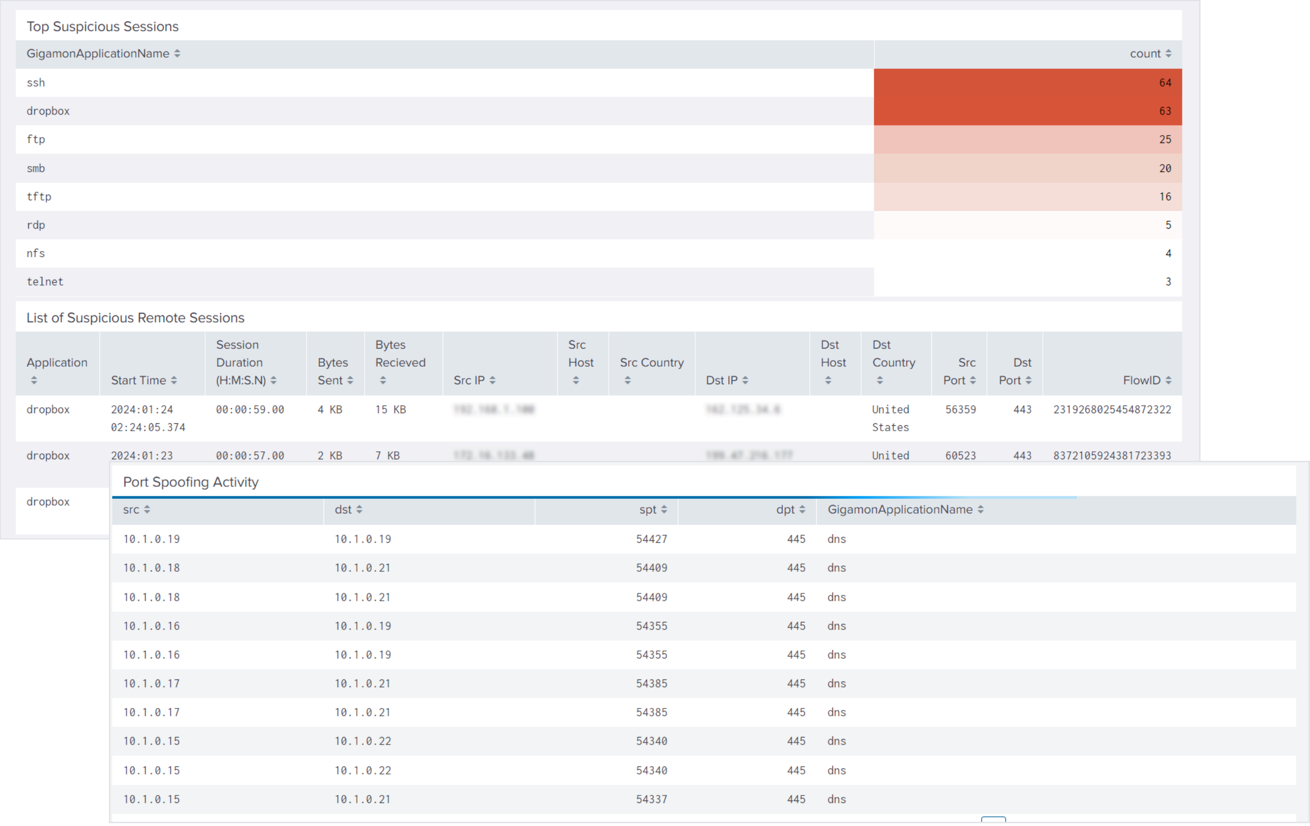
Pervasive visibility is essential to ensure that unwanted activities cannot evade identification in SIEMs. AMI can provide the necessary metadata to SIEMs, enabling SecOps teams to identify suspicious activities for investigation and remediation. The following AMI starter packs empower you to detect and remediate gaps in your network security that may be overlooked.

Detect unwanted services and port misuse through monitoring suspicious connections.

Attackers can attempt to evade firewall rules by configuring services on compromised hosts to run on non-standard ports. Users could set up or access services in violation of the Acceptable Use Policy (AUP). NetOps, CloudOps, DevOps, and DevSecOps teams need pervasive visibility about such services and usage patterns.

With AMI, they can export metadata to SIEMs to identify the following for further investigation and remediation:

- Services irrespective of whether they are running on the standard ports
- Source and destination endpoints
- Amount of data transferred between the endpoints



Top Suspicious Sessions

GigamonApplicationName ⇕	count ⇕
ssh	64
dropbox	63
ftp	25
smb	20
tftp	16
rdp	5
nfs	4
telnet	3

List of Suspicious Remote Sessions

Application ⇕	Start Time ⇕	Session Duration (H:M:S.N) ⇕	Bytes Sent ⇕	Bytes Recieved ⇕	Src IP ⇕	Src Host ⇕	Src Country ⇕	Dst IP ⇕	Dst Host ⇕	Dst Country ⇕	Src Port ⇕	Dst Port ⇕	FlowID ⇕
dropbox	2024:01:24 02:24:05.374	00:00:59.00	4 KB	15 KB	[redacted]			[redacted]		United States	56359	443	2319268025454872322
dropbox	2024:01:23	00:00:57.00	2 KB	7 KB	[redacted]			[redacted]		United	60523	443	8372105924381723393
dropbox													

Port Spoofing Activity

src ⇕	dst ⇕	spt ⇕	dpt ⇕	GigamonApplicationName ⇕
10.1.0.19	10.1.0.19	54427	445	dns
10.1.0.18	10.1.0.21	54409	445	dns
10.1.0.18	10.1.0.21	54409	445	dns
10.1.0.16	10.1.0.19	54355	445	dns
10.1.0.16	10.1.0.19	54355	445	dns
10.1.0.17	10.1.0.21	54385	445	dns
10.1.0.17	10.1.0.21	54385	445	dns
10.1.0.15	10.1.0.22	54340	445	dns
10.1.0.15	10.1.0.22	54340	445	dns
10.1.0.15	10.1.0.21	54337	445	dns

Figure 15. AMI metadata visualized in Splunk.

Detect and remediate issues related to unmanaged devices in your network.
IoT devices are not necessarily hardened for security thereby increasing the attack surface. Owing to the proliferation and diversity of the IoT devices, existing IoT device management can be inadequate. The NetOps teams require pervasive visibility into all the unmanaged hosts and their traffic patterns.

AMI can help the teams to:

- Identify IoT protocols
- IoT and other unmanaged device IP addresses
- Listing of session statistics by unmanaged device
- Enforce asset-based policy rules

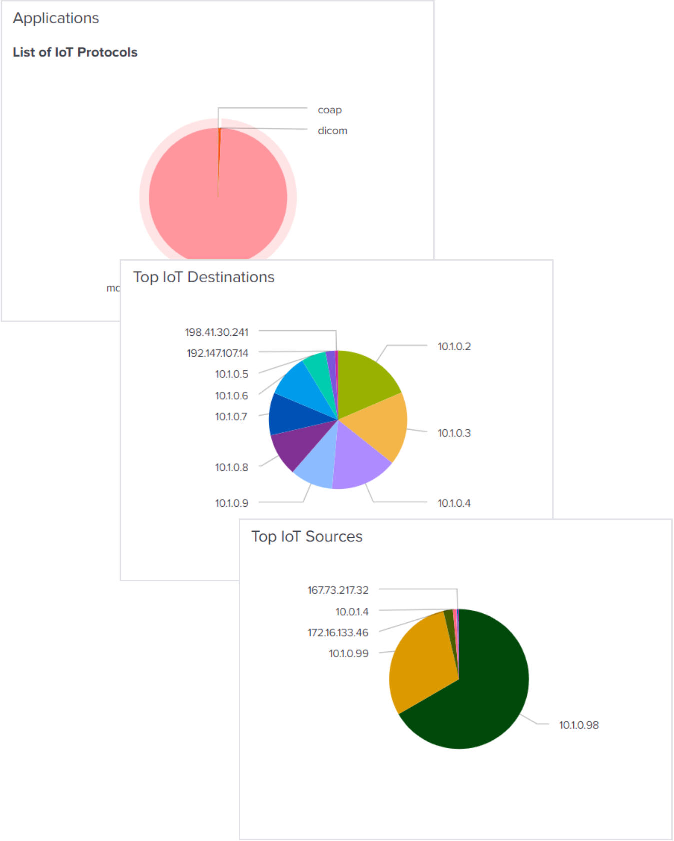
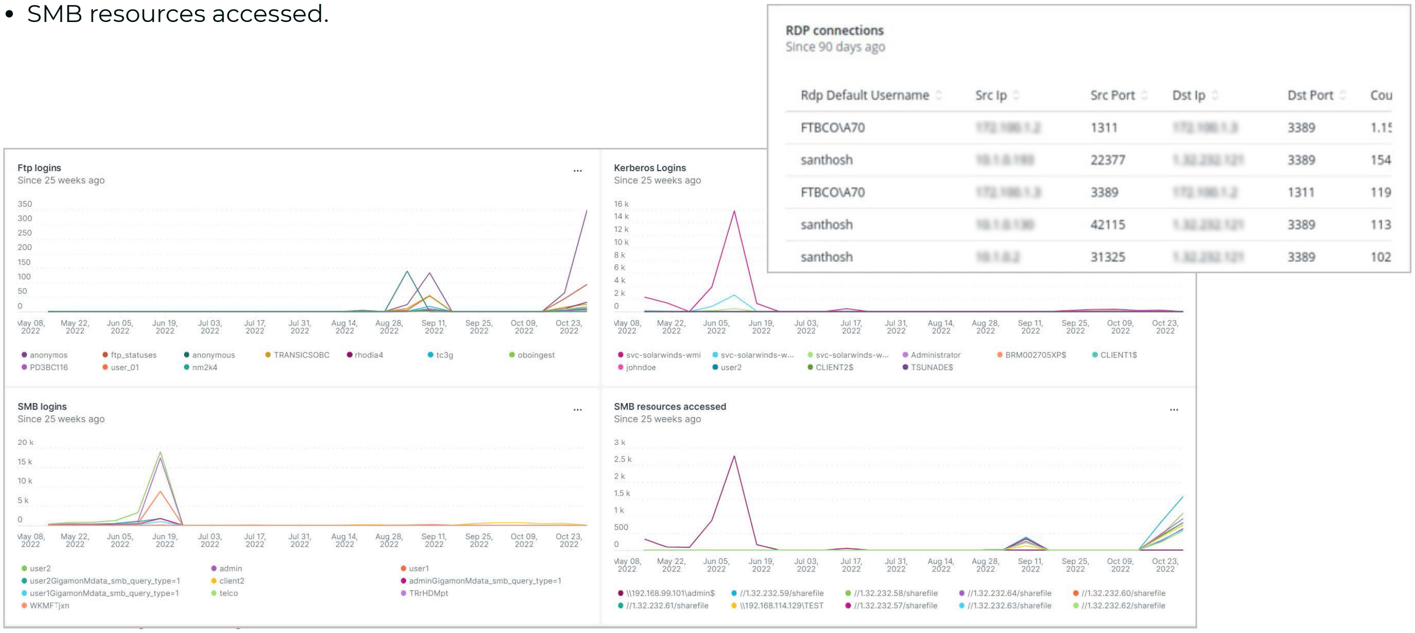


Figure 16. AMI metadata to detect and remediated issues related to unmanaged devices as visualized in Splunk.

Detect suspicious traffic outside norms.
NetOps teams want to know about any traffic patterns that are outside normal pattern, whether the traffic is restricted to few users, or it is widespread.

With AMI, they can export metadata to SIEMs to identify the following for further investigation and remediation:

- Trend graphs of logins for SMB (Server Message Block), FTP (File Transfer Protocol), RDP (Remote Desktop Protocol), Kerberos etc.
- SMB resources accessed.



RDP connections
Since 90 days ago

Rdp Default Username	Src Ip	Src Port	Dst Ip	Dst Port	Cou
FTBCO\A70	[redacted]	1311	[redacted]	3389	1.1:
santhosh	[redacted]	22377	[redacted]	3389	154
FTBCO\A70	[redacted]	3389	[redacted]	1311	119
santhosh	[redacted]	42115	[redacted]	3389	113
santhosh	[redacted]	31325	[redacted]	3389	102

Figure 17. AMI metadata to detect suspicions traffic outside norms as visualized in New Relic.

Rogue Activities Use Cases

Detect and Remediate Unsanctioned Applications that can Pose Challenges to your Network and Security

Gigamon AMI offers a powerful solution for detecting and remediating unsanctioned applications including GenAI, that pose challenges to network performance and security. By leveraging advanced analytics and real-time visibility into application metadata, you can proactively identify and address rogue activities, ensuring a secure and optimized network environment.

Detect and remediate unsanctioned P2P applications.
Unsanctioned Peer-2-Peer (P2P) applications could enable malware distribution, and pirated content and enable C2 channel for botnets. Excessive usage of file-sharing services like Kazaa, BitTorrent and Gnutella may affect network throughput for regular users. SecOps and CloudOps teams need to know which P2P applications are active and the associated endpoints. AMI helps you detect P2P activities by exporting metadata to SIEMs to identify the following for further investigation and remediation:

- P2P applications running on the network
- Source and destination endpoints
- Amount of data transferred between the endpoints

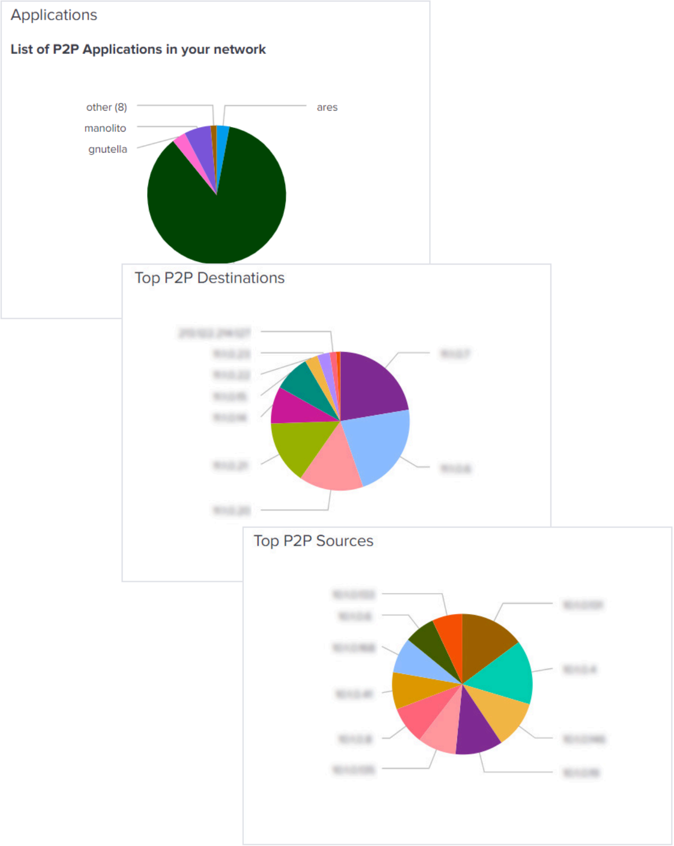


Figure 18. AMI metadata visualized in Splunk.

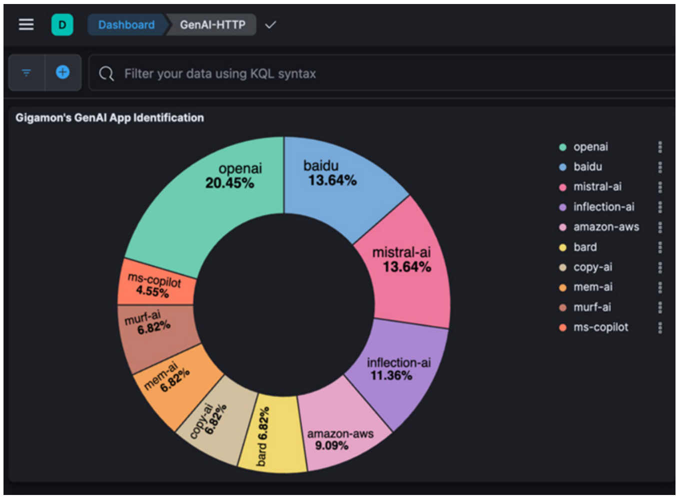


Figure 19. Gigamon's detection of GenAI applications.

Detect and remediate crypto jacking in your network.
Crypto jacking can have regulatory and compliance implications. In the cloud, the financial implications can be catastrophic. The Sec/Cloud/DevSec Ops teams need to know whether any of their compute resources are illegally compromised for crypto mining. AMI can help them identify crypto mining applications such as Bitcoin, Monero, Ripple, etc. Metadata about the crypto protocols including the source and destination IPs can be a starting point for further investigation and remediation by exporting to a SIEM tool.

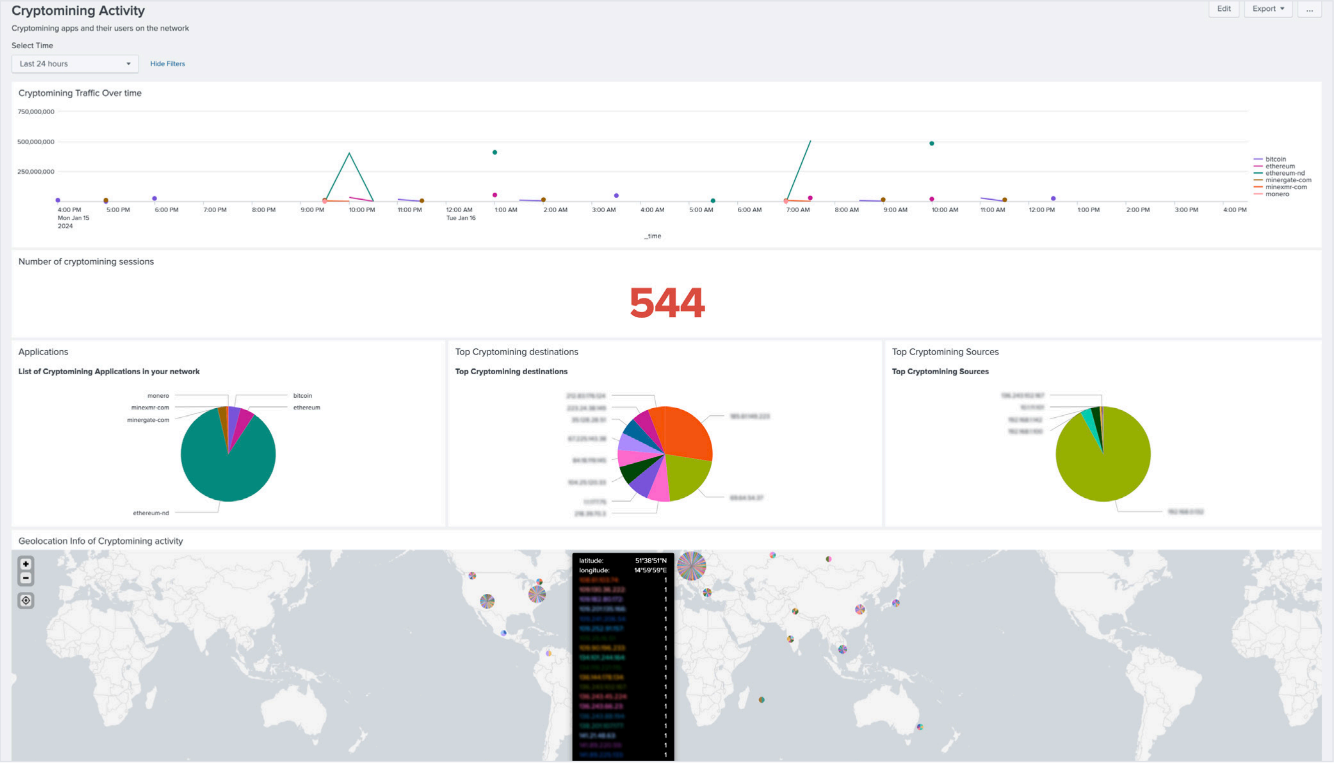


Figure 19. AMI metadata visualized in Splunk.

Compliance Use Cases

Ensure Compliance and Support a Zero Trust Journey

AMI can help organizations to comply with government and federal directives such as M-21-31 log management for monitoring HTTPS, Web, and DNS traffic. Please refer to the following relevant use cases under ‘Security Posture and Anomalous Traffic’ sections above:

- Monitoring HTTP Traffic for Policy Violations
- Monitoring Suspicious HTTP Traffic
- Monitoring DNS traffic

API Security Use Cases

Monitor and Remediate OWASP API Security Vulnerabilities

The Open Worldwide Application Security Project (OWASP) is an open community dedicated to enabling organizations to develop, purchase, and maintain applications and APIs that can be trusted. Gigamon AMI helps organizations monitor and remediate following OWASP API security vulnerabilities:

API6:2023 Unrestricted access to sensitive business flows.
Exploitation usually involves understanding the business model backed by the API, finding sensitive business flows, and automating access to these flows, causing harm to the business. An API Endpoint is vulnerable if it exposes a sensitive business flow, without appropriately restricting the access to it.

Common examples of sensitive business flows and risk of excessive access associated with them:

- Purchasing a product flow – an attacker can buy all the stock of a high-demand item at once and resell for a higher price (scalping)
- Creating a comment/post flow – an attacker can spam the system
- Making a reservation – an attacker can reserve all the available time slots and prevent other users from using the system

AMI can help in monitoring endpoints and traffic patterns per API. We could build trending timeline as in the DNS monitoring dashboards (under M-21-31 in the Splunk app) to illustrate traffic patterns based on server and client side. The trending could also include the methods exercised for accessing the APIs.

API9:2023 Improper inventory management.
Threat agents usually get unauthorized access through old API versions or endpoints left running unpatched and using weaker security requirements. In some cases, exploits are available. Alternatively, they may get access to sensitive data through a 3rd party with whom there's no reason to share data with. AMI can help to monitor the following:

- The API versions, which are active
- Server and client server user agents
- Files and images exchanged b/w the endpoints
- Original client behind the proxy that's initiating the calls

API10:2023 Unsafe consumption of APIs.
Exploiting this issue requires attackers to identify and potentially compromise other APIs/services the target API integrated with. Usually, this information is not publicly available, or the integrated API/service is not easily exploitable. AMI can help monitor HTTP redirections, strengthening the security posture of the API calls.

API10:2019 Insufficient logging and monitoring.
Attackers take advantage of lack of logging and monitoring to abuse systems without being noticed. AMI can export HTTP error codes from client or server side that can cover for any gaps in logging. It can also export HTTP RTT values that can help to detect whether an application is getting overwhelmed.

Empowering Your Current Set of Tools

The Gigamon Application Metadata Intelligence features 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, IPFIX, or JSON. Reports and accompanying dashboards are fully customizable.

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 are Here to Help Navigate What is 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.

Support and Services

Gigamon offers a range of support and maintenance services. For details regarding the 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 efficiently delivers network-derived telemetry to cloud, security, and observability tools. This helps eliminate security blind spots and reduce tool costs, enabling you to better secure and manage your hybrid cloud infrastructure. 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.

Gigamon®

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