Gigamon Deep Observability Pipeline and Sumo Logic

Overview

Modernizing applications and migrating to public cloud platforms enhance agility and flexibility. But, there are also trade-offs to consider, including new and borderless attack surfaces, lack of consistent visibility, and growing tool sprawl and tool expenses.

Here's where the Gigamon Deep Observability Pipeline — integrated with Sumo Logic Continuous Intelligence Platform — comes in to help you deliver secure, compliant, and reliable cloud applications. At the same time, NetOps and infrastructure teams benefit from streamlined hybrid cloud deployments and simplified management.

Gigamon accesses traffic from any cloud, extracts valuable L2–L7 network and application metadata attributes, and sends this network-derived intelligence to Sumo Logic. Gigamon augments traditional metrics, events, logs, and traces (MELT) data with more than 5,000 application- and security-related attributes.

Sumo Logic then analyzes, visualizes, and alerts on this intelligence, enabling you to discover vulnerabilities and detect rogue activities such as use of unsanctioned applications, weak SSL ciphers, expiring TLS certificates, and hidden crypto-mining activities.

Key Solution Features

- Access to more than 5,000 L2–L7 attributes that can be forwarded to Sumo Logic to solve new security and performance use cases
- Out-of-the box integration between Gigamon expands Sumo Logic's visibility into not just managed hosts, but also all hosts on the infrastructure, including BYO, IoT, and even container-to-container communications
- Visibility into East-West and North-South traffic across multi-cloud and on-premises environments
- Visualization of all applications running on your network

- Notifications on HTTP response code changes and anomalous traffic patterns to get ahead of potential performance or security issues
- Traffic optimization capabilities, including application filtering, packet de-duplication, and flow/packet slicing to fine-tune traffic going to tools — without sacrificing security data fidelity

The Problem and Solution

Enterprises with hybrid or multi-cloud environments are becoming the norm. However, moving applications to public clouds or developing cloud-native applications bring new challenges, such as:

- Decreased visibility and control, raising security and compliance risks
- Multi-Cloud silos that make a consistent security posture and quickly pinpointing the root of performance issues nearly impossible
- New tools and processes — which could vary by cloud — for teams to invest in and learn

All of the above can slow your cloud initiatives and make life harder for your teams. What if we told you Gigamon and Sumo Logic could address these critical hybrid cloud challenges? The Gigamon Deep Observability Pipeline gives you complete infrastructure visibility and, together with Sumo Logic, the power to see deeply into what's happening in your cloud deployments.

Here are just a few examples of security and compliance use cases enabled by the joint Gigamon and Sumo Logic solution:

- Identify expired or expiring TLS certificates and weak ciphers
- Detect unauthorized remote connections or high volumes of DNS requests that can be signs of data exfiltration

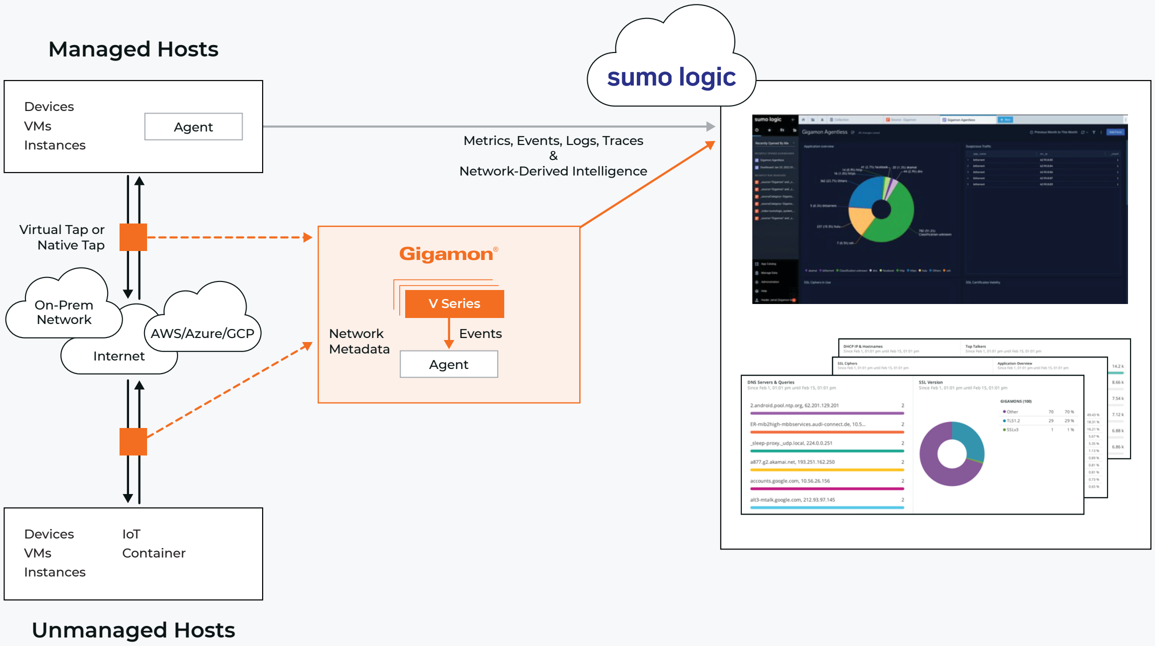


Figure 1. Gigamon accesses traffic from all sources, extracts network-derived attributes, and then sends this traffic to Sumo Logic.

- Monitor and control file access and obtain insights into which clients are obtaining specific files
- Detect suspicious WAN activities that could be emerging command-and-control attacks
- Guide troubleshooting of poor application performance by looking at user-reported issues together with TCP, HTTP, and DNS response types
- Spot rogue and unauthorized activities, such as the use of unsanctioned applications, cryptocurrency mining, and BitTorrent downloads

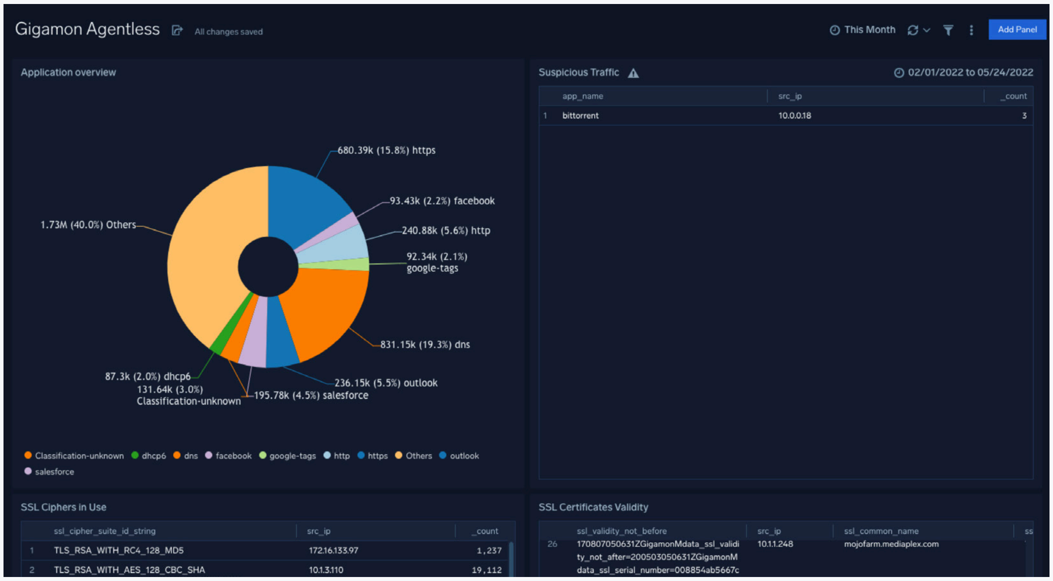
How the Joint Solution Works

The integration of the Gigamon Deep Observability Pipeline with Sumo Logic is straightforward: Once you have Gigamon in place, you only need custom HTTPS source URLs from Sumo Logic. In many cases, the joint solution can be fully operational in less than 10 minutes.

> Given that the cloud is the top target for workload migration projects, limited visibility into performance and security shortcomings restrict the use and impact of cloud delivery for critical workloads. Deep observability into these workloads — and associated infrastructure —enables ready and resilient migration and management.

MARK LEARY
Research Director with IDC

Source: Network Intelligence: Required Information and Insights in This Digital Era, April 6, 2022



Suspicious Traffic ⚠ 02/01/2022 to 05/24/2022

	app_name	src_ip	_count
1	bittorrent	10.0.0.18	3

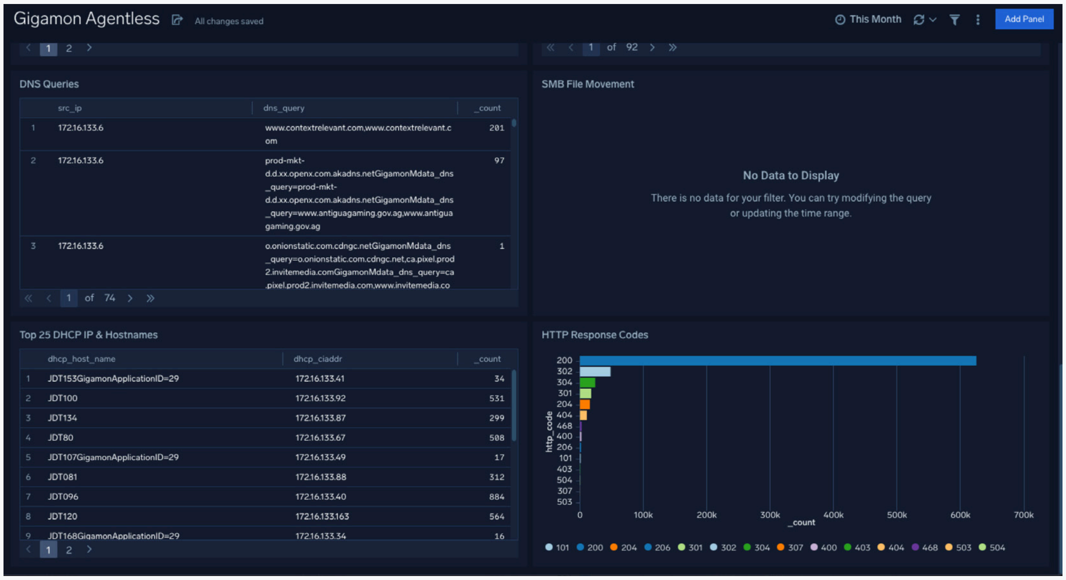
SSL Ciphers in Use

	ssl_cipher_suite_id_string	src_ip	_count
1	TLS_RSA_WITH_RC4_128_MD5	172.16.133.97	1,237
2	TLS_RSA_WITH_AES_128_CBC_SHA	10.1.3.110	19,112

SSL Certificates Validity

	ssl_validity_not_before	src_ip	ssl_common_name	ss
26	170807050631ZGigamonMdata_ssl_validity_not_after=200503050631ZGigamonMdata_ssl_serial_number=008854ab5667c	10.1.1.248	mojofarm.mediaplex.com	

Figure 2. Gigamon Application Metadata Intelligence exposed through the Sumo Logic dashboard shows all applications running on a network, suspicious traffic, as well as the state of SSL ciphers and SSL certificate validity.



DNS Queries

	src_ip	dns_query	_count
1	172.16.133.6	www.contextrelevant.com,www.contextrelevant.com	201
2	172.16.133.6	prod-mkt-d.d.xx.openx.com.akadns.netGigamonMdata_dns_query=prod-mkt-d.d.xx.openx.com.akadns.netGigamonMdata_dns_query=www.antiguagaming.gov.ag,www.antiguagaming.gov.ag	97
3	172.16.133.6	o.onionstatic.com.cdngc.netGigamonMdata_dns_query=o.onionstatic.com.cdngc.net,ca.pixel.prod2.invitemedia.comGigamonMdata_dns_query=ca.pixel.prod2.invitemedia.com,www.invitemedia.co	1

1 of 74

SMB File Movement

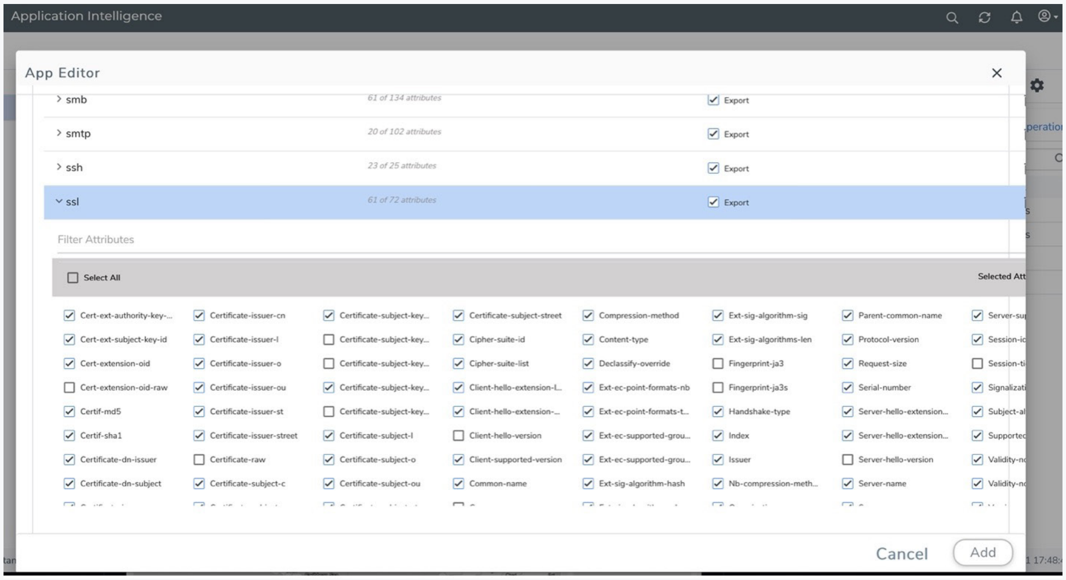
No Data to Display

There is no data for your filter. You can try modifying the query or updating the time range.

Top 25 DHCP IP & Hostnames

	dhcp_host_name	dhcp_ciaddr	_count
1	JDT153GigamonApplicationID=29	172.16.133.41	34
2	JDT100	172.16.133.92	531
3	JDT134	172.16.133.87	299
4	JDT80	172.16.133.67	508
5	JDT107GigamonApplicationID=29	172.16.133.49	17
6	JDT081	172.16.133.88	312
7	JDT096	172.16.133.40	884
8	JDT120	172.16.133.163	564
9	JDT168GigamonApplicationID=29	172.16.133.34	16

Figure 3. Gigamon and Sumo Logic enables you to instantly see and get alerted on suspicious or anomalous traffic. For example, you can spot unusual DNS queries and hosts talking to DNS servers outside the enterprise, which could be signs of a command-and-control attack.



› smb	61 of 134 attributes	☑ Export
› smtp	20 of 102 attributes	☑ Export
› ssh	23 of 25 attributes	☑ Export
⌄ ssl	61 of 72 attributes	☑ Export

Filter Attributes

☐ Select All — Selected Att

☑ Cert-ext-authority-key-...	☑ Certificate-issuer-cn	☑ Certificate-subject-key...	☑ Certificate-subject-street	☑ Compression-method	☑ Ext-sig-algorithm-sig	☑ Parent-common-name	☑ Server-su
☑ Cert-ext-subject-key-id	☑ Certificate-issuer-l	☐ Certificate-subject-key...	☑ Cipher-suite-id	☑ Content-type	☑ Ext-sig-algorithms-len	☑ Protocol-version	☑ Session-ic
☑ Cert-extension-oid	☑ Certificate-issuer-o	☐ Certificate-subject-key...	☑ Cipher-suite-list	☑ Declassify-override	☐ Fingerprint-ja3	☑ Request-size	☐ Session-ti
☐ Cert-extension-oid-raw	☑ Certificate-issuer-ou	☑ Certificate-subject-key...	☑ Client-hello-extension-l...	☑ Ext-ec-point-formats-nb	☐ Fingerprint-ja3s	☑ Serial-number	☑ Signalizati
☑ Certif-md5	☑ Certificate-issuer-st	☐ Certificate-subject-key...	☑ Client-hello-extension-...	☑ Ext-ec-point-formats-t...	☑ Handshake-type	☑ Server-hello-extension...	☑ Subject-al
☑ Certif-sha1	☑ Certificate-issuer-street	☑ Certificate-subject-l	☐ Client-hello-version	☑ Ext-ec-supported-grou...	☑ Index	☑ Server-hello-extension...	☑ Supportec
☑ Certificate-dn-issuer	☐ Certificate-raw	☑ Certificate-subject-o	☑ Client-supported-version	☑ Ext-ec-supported-grou...	☑ Issuer	☐ Server-hello-version	☑ Validity-nc
☑ Certificate-dn-subject	☑ Certificate-subject-c	☑ Certificate-subject-ou	☑ Common-name	☑ Ext-sig-algorithm-hash	☑ Nb-compression-meth...	☑ Server-name	☑ Validity-nc

Figure 4. Gigamon Application Metadata Intelligence generates thousands of attributes for discovering security and performance issues. In GigaVUE-FM fabric manager, you can see the list of available SSL attributes you can send to Sumo Logic for analysis. For any application or protocol, you can also manually select specific attributes to address the precise security and visibility gaps in your environment.

Conclusion

Whether you're tasked with securing applications, ensuring good user experiences, or managing hybrid cloud infrastructure, you'll want deep observability enabled by Gigamon and Sumo Logic.

Gigamon, integrated with Sumo Logic, lets you detect critical security and compliance issues across all environments, identify threats before they do damage, and get to the root of performance issues before users are affected. Gigamon and Sumo Logic puts you back in control even as applications and environments continue to evolve.

About Sumo Logic

Sumo Logic empowers the people who power modern, digital business through its Continuous Intelligence Platform™. Practitioners and developers around the world rely on Sumo Logic to gain real-time analytics and insights from their cloud-native applications, helping them ensure application reliability, secure and protect against modern security threats, and gain insights into their cloud infrastructures.

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.

For more information on the Gigamon Deep Observability Pipeline and Sumo Logic please visit gigamon.com | sumologic.com

Gigamon®

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