Protect your government agency's data and workloads in the cloud

With observability and real-time discovery and response from Sumo Logic, Gigamon, and AWS

sumo logic | Gigamon® | aws

What's inside

The current state of government cloud security

Government agencies are attractive targets for ransomware and state-sponsored bad actors. As a result, agencies must meet multiple U.S. federal government mandates, such as FedRAMP, NIST 800-53, OMB 21-31, and the Zero Trust Executive Order. In addition, many states and municipalities have additional compliance requirements. When agencies comply with these federal and state mandates and requirements, they are less vulnerable.

Safeguarding infrastructure and addressing compliance isn't easy. Agencies at all levels often have hybrid and multi-cloud environments, creating silos that are difficult to protect. State and local agencies, in particular, often lack cybersecurity resources and personnel. Incident response can be slow and difficult.

These agencies need visibility, which is key to protecting cloud and hybrid deployments. Agencies have likely adopted solutions and services to provide visibility, but consistency can be challenging. Multiple security tools for visibility require separate management, which increases costs and can delay resolution. In addition, it is often difficult to get a comprehensive picture of a threat landscape when the data sources are fragmented.

The good news is that there is a solution. Observability and real-time discovery and response can help your government agency or organization make the most of security budgets and grants. Sumo Logic, Gigamon, and Amazon Web Services (AWS) provide a joint solution that enables federal government and state, local and education (SLED) organizations to meet and track compliance with these requirements easily. This ebook covers how this solution could benefit you.

Observability drives cost-effective security in the cloud

Observability is the process of clearly assessing a system's internal state based on its external outputs. It takes metrics, events, logs, and traces (MELT)— four critical components of a complex system—and creates a view of data across applications, infrastructure, and security tools. This helps organizations troubleshoot reliability issues more effectively. It can also enable security-related observability and deep security observability.

Combine telemetry for security-related observability

Your government organization can use observability telemetry—typically environment, network, infrastructure and workload outputs such as logs and events—for audit and compliance, data lake protection, threat detection and investigation, and application security. With security-related observability, you can determine when an incident or attack occurred and gain insight into what attackers did while inside. You can also use the information provided through observability to improve your security posture further in the future.

This marriage of output data provides a comprehensive view of your agency's IT real estate and threat landscape. Understanding where you are protected and where you are vulnerable reduces risk and mean time to recovery (MTTR). However, it is possible to add one more output to deepen security-related observability.

Add network intelligence and integrate services on AWS for deep security observability

Deep observability provides network intelligence that augments logs, metrics, events, and traces so you can view all network traffic from metadata to packet level. It decreases complexity by integrating security and compliance vendors and products on AWS for end-to-end protection of infrastructure, apps, and workloads.

Because everything is on AWS, you can use deep observability to detect critical security and compliance issues across all environments. These include rogue or unauthorized applications, DNA, and expired SSL certificates. You can get to the root of performance issues before users are affected.

Look deep into your cloud in real-time

Gaining deep observability into all data in motion is the key to reaping the benefits of a secure, resilient digital infrastructure. This is where Sumo Logic and Gigamon—as well as their integration with AWS—come in.

Cloud-native SaaS analytics

Sumo Logic's cloud-native SaaS analytics platform helps agencies build, run, and secure modern applications and cloud infrastructures. Sumo Logic uses machine learning and AI to provide real-time insights into cloud infrastructures that allow your government organization to extend the value of your existing AWS investments. Its solutions are fully certified at the FedRAMP-Moderate level, and they have achieved SOC2, HIPAA, ISO, and Cloud Security Alliance (CSA) STAR certification.

Amplified observability

Gigamon continuously harnesses actionable network-level intelligence to amplify the power of observability tools. This powerful amplification helps government IT organizations assure security and compliance governance. It can also speed root-cause analysis of performance bottlenecks and lower the operational overhead of managing hybrid and multi-cloud IT infrastructures.

A powerful combination

Sumo Logic and Gigamon provide real-time security threat discovery and response on AWS, the world's most reliable cloud platform. Gigamon completes the deep observability picture for network telemetry. Sumo Logic combines that data with cloud, infrastructure, and business app data to help deliver:

- → **Compliance and data management**
- → **Monitoring and analysis across security tools**
- → **Automated incident response**

The combination detects security and compliance issues through log and network traffic analytics. It turns relevant, rich network contextual data into visualizations for faster triage and simplifies investigation efforts. Your agency benefits from a sound foundation for fortifying security across AWS environments.

How Sumo Logic, Gigamon, and AWS work together

The processes of the Sumo Logic, Gigamon, and AWS solution are smooth and virtually seamless. Gigamon augments MELT data with more than 5,000 application and security-related (L2 to L7) attributes to enable identification, detection, and observations of network activity. Data exchange is easy because Gigamon Application Metadata Intelligence sends metadata directly to Sumo Logic.

The Gigamon Deep Observability Pipeline enables Sumo Logic to address a wide range of security use cases that can enhance an agency's overall security posture. The most common of these use cases are available as pre-configured templates that enable your agency to achieve a rapid return on its Gigamon and Sumo Logic investment.

Sumo Logic analyzes and visualizes this intelligence and sends alerts, enabling you to discover vulnerabilities and detect rogue activities. Pre-built dashboards aggregate and visualize deep insights on the performance, reliability, and security of agencies' critical applications and infrastructure, used to quickly identify and remediate risk. Visibility expands to all hosts on the infrastructure, including managed hosts, BYO, IoT, and even container-to-container communications.

The value of the joint solution to government agencies

Time savings and cost containment

Your agency can take advantage of deep observability, discovery, and response while containing the escalating costs of data exchange and storage. Reducing irrelevant or duplicate data sent to Sumo Logic enables more efficient operations, consolidated spending, and decreased costs. Built-in functionality reduces mean time to identify (MTTI) and mean time to recovery (MTTR).

In addition, Gigamon can feed metadata attributes from a single agent to multiple observability and security tools, thereby reducing the number of agents or mirroring processes that need to be deployed. This reduction in turn decreases compute cycles and data duplication on the network. Additionally, using this Gigamon metadata capability reduces the size of network aggregations to only 2–5 percent of the size of full network events, keeping storage and data movement costs low.

Improved infrastructure defense

With this joint Gigamon, Sumo Logic, and AWS solution, your agency and your IT and security teams can:

- Strengthen and fortify your infrastructure protection.
- Gain visibility into East-West and North-South traffic across your government organization's multi-cloud and on-premises environments.
- Detect anomalous WAN activities, unauthorized remote connections or high volumes of DNS requests. These are all signs of data exfiltration.
- Identify expired or expiring TLS certificates and weak ciphers.
- Visualize activities such as crypto-mining and P2P traffic that impair both security and performance.

MORE SECURITY FOR YOUR AGENCY

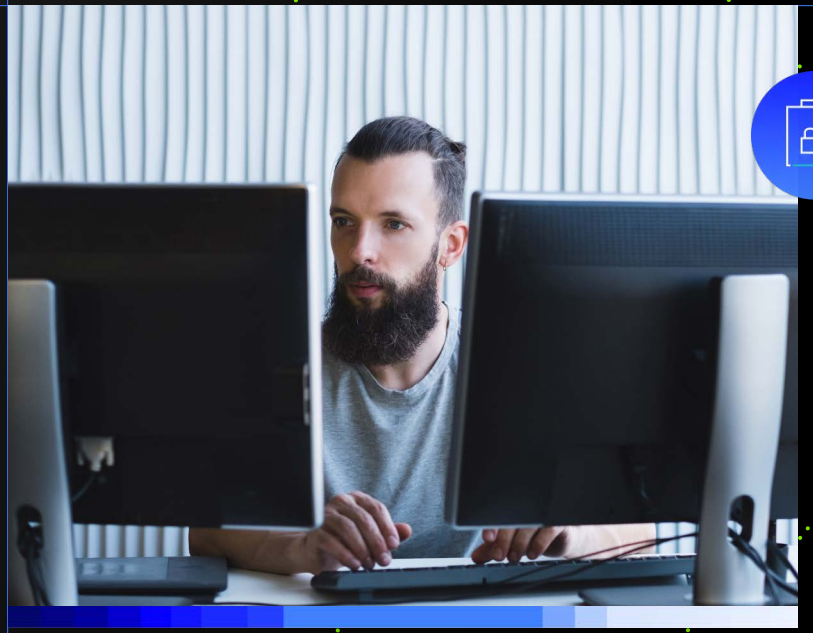
In addition to the cost and time savings, the combination of Gigamon, Sumo Logic, and AWS improves your security posture.

Improved application protection

Defending your assets includes your business applications. The joint solution enables your agency to troubleshoot application performance by looking at user-reported issues and TCP, HTTP, and DNS response types. With its complete picture of your IT and cloud landscape, you can spot unauthorized activities, such as using unsanctioned applications.

Zero Trust at all levels

Because Executive Order 14028 explicitly recommends using Zero Trust architecture to secure your infrastructure, workload, and applications, it is top of mind for most agencies. The Gigamon, Sumo Logic, and AWS solution address Zero Trust by enabling you to monitor and control file access and obtain insights into which clients are obtaining specific files. Sumo Logic tools for analyzing, monitoring, and governing access to data and other IT resources support Zero Trust. In addition, Gigamon's Deep Observability Pipeline and other visibility tools are the backbone of Zero Trust at the U.S. Department of Defense.[1]



1 SOURCE

Conclusion

Security blind spots are common in many hybrid cloud deployments today, and government agencies are especially susceptible. Addressing compliance with regulations and mandates designed to protect government infrastructure and data is critical. Gigamon, Sumo Logic, and AWS have created an integrated solution to help your agency IT organization assure security and compliance governance while lowering the operational overhead of managing hybrid and multi-cloud infrastructure.

→ Sumo Logic is available in AWS Marketplace

sumo logic | Gigamon® | aws