sumo logic

WHITEPAPER

Accelerate Government IT Modernization

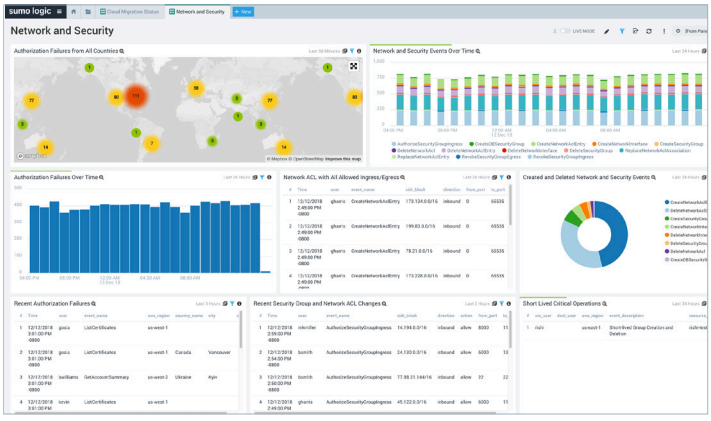
Improve mission outcomes with unified operations and security analytics.
Empower teams to quickly resolve cybersecurity and performance incidents.

Modernizing today's Government IT systems is critical for protecting mission success. According to the 2017 Federal Office of Management and Budget (OMB) report, 74% of Federal agencies need crucial and immediate improvements. The vast majority of IT teams are flying blind with little to no ability to detect and investigate for signs of data breaches or performance issues.

Today's government IT teams are ill-equipped to differentiate poor system performance from code issues, misconfiguration, or malicious attacks. Many attack vectors remain exposed for years, giving threats unrestricted access to siphon large amounts of private and personal data from critical systems without notice. Organizations must modernize applications, infrastructure, and processes to reduce attack surfaces on mission critical systems while also improving user experiences.

Understanding Risk

Today's modern DevSecOps platforms empower teams to quickly identify, triage, and investigate issues across diverse operating environments much faster than legacy point solutions. Unified data analytics platforms give cross functional teams an easy way to develop insights from largely fragmented systems. Today's teams need to collaborate with data that's traditionally siloed between Developers, IT Operators, and Security experts.



Most agencies today agree that reducing mean time to resolution (MTTR) is a crucial first step to managing execution risk. When incidents happen, teams with poor visibility spend unreasonable amounts of time gathering, cross referencing, and attempting to build insights while critical days, weeks, and months roll by. Meanwhile, stakeholders lack context and correlation across disparate information to take action. With Sumo Logic, teams are able to collaborate effectively because they have the right context and correlation to build insights without context switching across point solutions.

Modern Architectures

To deliver secure always-on digital services, leading government organizations are now using COTS such as containers, microservices, and kubernetes on cloud platforms like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). It's the only way to meet required performance and scalability demands while also achieving necessary cost economics. Chosen solutions must accommodate today's highly variable machine data volumes and bursty nature.

Legacy single-tenant and point solutions just don't meet the mark. Platforms like Sumo Logic make it easy for organizations to support both modern and legacy environments by providing teams multiple ways to ingest diverse data types. Teams with 3-tier applications can install local host data collectors while modern teams are able to use hosted API endpoints or direct integrations. Organizations benefit from the flexibility and extensibility to unify typically segregated analytics solutions in a single user interface.

Tool Consolidation

We continually see rapid advances in the tools and processes customers use to build, run and secure today's modern and hybrid applications. Agencies and organizations often rely on hundreds of bespoke tools for their mission critical systems, driving up costs and creating unnecessary complexity with little value. Point solutions force practitioners to frustratingly context switch between tools when they attempt to correlate across different time periods, data sources and classifications of data. This leads to extremely stressful incidents when mean time to resolution (MTTR) is crucial.

Unified solutions, like Sumo Logic, are designed with hundreds of out of the box integrations. You can consolidate tools and create merged views of logs, metrics, and event streams as panels within real-time dashboards. Power users can drill down to underlying queries showing unaggregated events where Sumo Logics, Patented & Out of the Box Machine Learning Analytics, like LogReduce and Log Compare uncover outliers that plague availability. DevSecOps teams are now able to iterate faster using shared insights across functions because they have the data they need for leaders to make informed decisions.

Common Needs

- **Full-stack visibility** - Capture real-time event streams for both modern cloud-native and traditional environments.
- **Powerful analytics** - Improve mean time to resolution so teams get to root causes faster and take immediate action.
- **Machine learning** - Advanced pattern recognition to reduce millions of logged events from multiple sources down to a few meaningful signatures uncovering outliers.
- **Silo elimination** - Democratize data by allowing DevOps and Security teams to collaborate in the same solution without being restricted by user seats.
- **Threat intelligence** - Be informed, not overwhelmed by real-time alerts so teams can effectively prevent breaches, uncover threat vectors, and identify adversaries.
- **Security & compliance** - Cloud solution with mature security processes meeting PCI, HIPAA, SOC 2 type 2, CSA Star, and ISO 27001.
- **Enterprise controls** - Role-based access controls, two factor authentication, audit logs, and identity provider integration to ensure the accountability of users.

Instant Analytics

Most organizations can't allocate the necessary resources to build and maintain a big data analytics platform that meets both short and long term requirements across the lifecycle of a project. SaaS platforms help to reduce complexity for organizations so they never have to worry about resource management and service scaling when they need data driven answers fast. Teams never waste time tuning databases, building out hadoop clusters, or scaling infrastructure to support fast queries, it just happens instantly behind the scenes for managed SaaS analytics products.

Sumo Logic combines powerful machine learning and at-scale analytics so teams can instantly get to insights from petabytes of unstructured, semi-structured and structured data without worrying about the underlying architecture. Teams immediately improve visibility across their entire stack so they can shift from reactive team postures to proactive problem solving. Analysts not only build insights from real-time streams, but are also able to rapidly filter and facet historical data to determine trends and find anomalous behaviors.

Improve Security Postures

Sumo Logic simplifies analytics so that anyone in the organization can build insights without having to be a big data expert. Teams get ahead of issues by sharing dashboards integrating metrics, logs, and events across the organization. Practitioners stop wasting time compiling logs from servers and can focus their energy finding answers from their data using an intuitive web interface.

Government cloud migration teams benefit from visualizations of the relationship between on-premise and cloud deployments side by side on shared dashboards. Out of the box integrations with cloud platforms and services makes it easy for government teams to shift to cloud native offerings without having to add additional monitoring tools. Sumo Logic integrates with local on-prem network and firewall equipment like Cisco, F5, and Palo Alto Networks in addition to cloud security solutions such as CloudStrike, AWS Guard Duty, and Azure Audit. Teams are covered for what they have today, and what they need in the future.

Zero Management

It takes a huge amount of industry expertise to build and maintain infrastructure for high-performance log analytics platforms. We see teams new to log analytics experiment with basic tools, open-source projects, and packaged software. As requirements evolve in terms of data volume, performance, and security these solutions usually fall short because of the upkeep. Initial experimenters end up burning precious time while driving up project costs.

Cloud based analytics solutions solve ongoing maintenance challenges by empowering a single administrator to easily manage the platform for an entire organization and delegate management to team leaders. Zero internal resources are required for deploying hardware, installing/upgrading software, and dealing with security patches to the thousands hosts required to operate the analytics platform. Teams instantly benefit from 24/7 availability of the latest version of the software and scale to match current consumption. Governments no longer need to dedicate hundreds of engineers to build and manage analytics platforms, releasing resources to focus on core mission needs.

Cloud Native

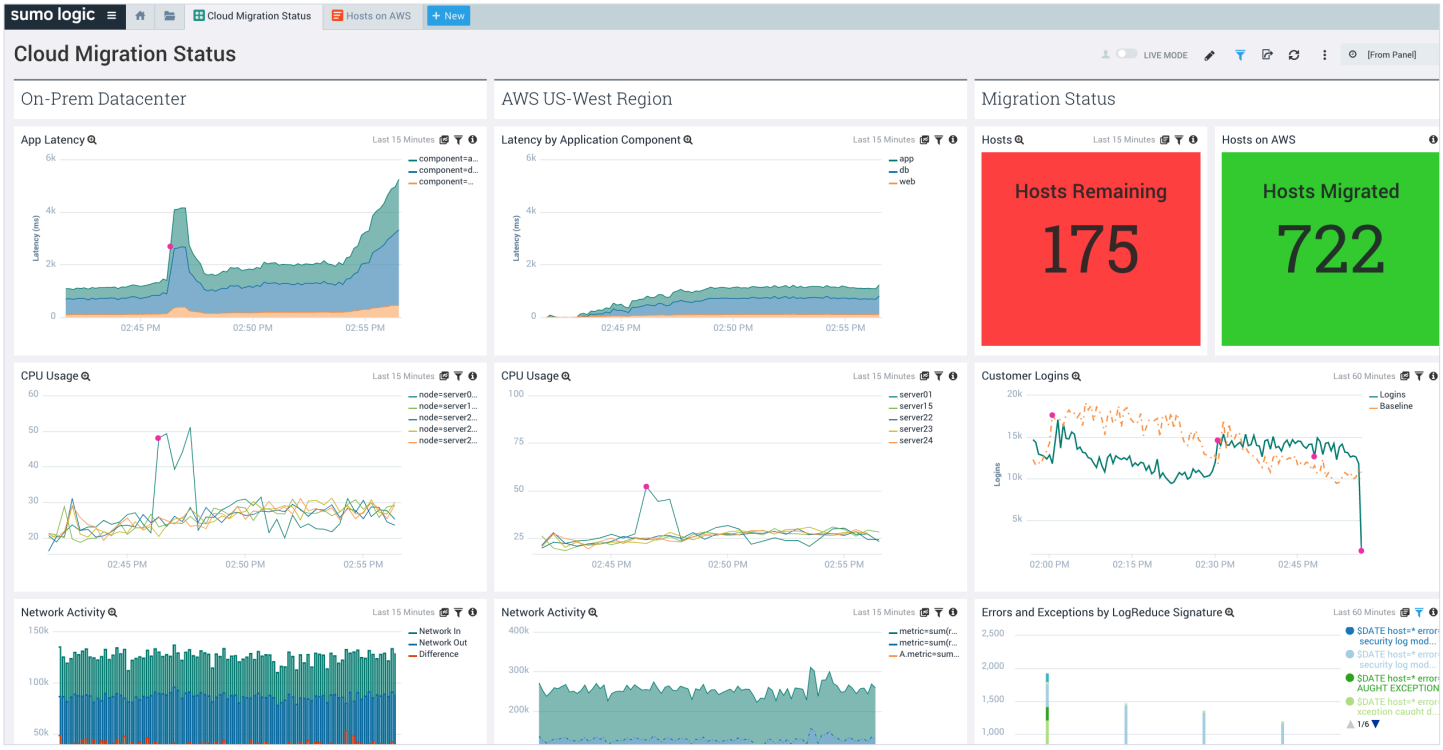
Not all solutions marketed as cloud are created equal. Legacy enterprise software vendors often attempt to pass single-tenant software hosted on their managed servers as a cloud offering. These products are actually a stopgap instead of a true multi-tenant SaaS solution and suffer performance, cost, and scaling issues. Cloud-native solutions are much more cost effective because they are comprised of decoupled and individually scalable components. In addition, they typically deploy new code and configurations multiple times per day allowing critical security patches to be pushed to applications, services, and hosts more frequently.

Sumo Logic is comprised of nearly a dozen clustered microservices for ingest, indexing, database, search, and frontend services. Instead of wasting resources replicating monolithic instances, resources are actively provisioned to individual bottleneck components in real-time to match demand. Gained operating efficiency is passed back to customers as improved performance. Organizations never worry about servers sitting idle or over provisioning for peak workloads. It is all handled by the managed service provider and remains consistent in performance.

At Scale Today

Sumo Logic operates thousands of backend hosts ingesting over 150TB per day across 7 operating regions from over 2 million data sources. During a typical month, over 15,000 unique users visit 50,000 unique dashboards. The elasticity of multi-tenant SaaS platforms allow for peak ingest to fluctuate 10-100x their normal load while only paying for what they use in the moment they use it.

Legacy on-prem software can't achieve this because it's provisioned and licensed to static hardware resources. Organizations typically over-provision for peak demand and pay for excess capacity the rest of the year. Others who under-provision suffer long processes to purchase licenses to deploy more instances during unexpected big days. Single-tenant software just can't match the kind of scale, performance, and cost efficiency of cloud native solutions like Sumo Logic.



Secure by Design

Modern solutions approach security with a zero-trust model versus a moat approach. Instead of protecting a perimeter around servers, a zero-trust approach assumes every communication independent of location is secure. Credentials always start minimally and when expanded is limited in scope to reduce impact when compromised. Sumo Logic also protects customer data by using key encryption accounts during ingest, storage, and presentation. Our mature security practices include regular audits, penetration tests, and compliance with difficult industry standards such as SOC2 Type 2, CSA Star, ISO 27001, PCI, and HIPAA.

The Sumo Logic Platform integrates a number of built-in capabilities for organizations to better manage the security of data they send into the platform. We start with integration to identity providers using SSO/SAML for authentication and let groups policies be built with role based access controls (RBAC) to limit access to data partitions and sources. In addition, built-in audit logs empower administrators to leverage the same dashboard, search, and log analysis tools they use to monitor their own environments with the user activity in our SaaS platform.

Conclusion

Government organizations need to quickly modernize their people, processes, and technology to improve their security and operations postures. Teams need a unified platform where they can quickly build insights from a wide number of data sources and types, troubleshoot new issues quickly, and build dashboards for cross functional practitioners to rally around. These platforms must not only have out of the box integrations to existing on-premises applications and infrastructure, but also for hybrid and new cloud native applications. Cloud native SaaS analytics platforms like Sumo Logic empower teams to accelerate their IT modernization projects in a cost effective and secure way.

sumo logic

Toll-Free: 1.855.LOG.SUMO | **Int'l:** 1.650.810.8700
305 Main Street, Redwood City, CA 94603
public-sector@sumologic.com
sumologic.com/solutions/industry-public-sector