sumo logic

SOLUTIONS BRIEF

Modern cloud security

Critical visibility, scalability, insights, and assurances

Organizations around the world are adopting, building or shifting resources, applications and workloads to the cloud to take advantage of the inherent competitive, economic and agility gains that can be achieved in this environment.

Many organizations are finding that their legacy network and security tools are not able to provide them with the scalability and insights they need, to continue tightly managing their security and compliance requirements in the cloud.

Sumo Logic was designed in the cloud, for the specific needs of the cloud (public, private, hybrid and beyond) and is delivered via a true SaaS model. Sumo Logic uses machine data analytics, and built-in threat intelligence, to centralize and democratize visibility across the organization. Through the automated and actionable intelligence delivered by Sumo Logic these organizations are able to more quickly identify and remediate security and compliance threats in the cloud, and beyond. These newly gained capabilities and insights delivered by Sumo Logic are also enabling an accelerated transition to a more efficient, less complex, DevSecOps approach to managing security and compliance in the cloud.

Gain deep customer insights in real-time with Sumo Logic's cloud-scale machine data analytics platform

Business challenges

- **Lack of visibility -** Traditional security tools were built to manage and monitor logs from predominantly physical elements. As these physical elements rapidly become "virtualized" and "containerized" in the cloud, these tools are quickly losing the ability to provide the insights that are needed to effectively manage security and compliance in these new environments

- **Lack of scalability -** Traditional security tools cannot scale fast enough, or require the pre-purchase of capacity to support worse case scenarios, to properly monitor and analyze the transient, unpredictable and elastic volumes of data that are common in cloud workloads. Many of these tools were also built before the advent of "containers" and "microservices" which are common architectural elements in the architecture and components in the creation of today's modern applications. These elements pose unique challenges to legacy tools as, by their nature, they spin up quickly, typically last for a very short window of time commonly is outside standard data collection rates. These blinds spots create a potential window for attackers to compromise and exfiltrate critical and sensitive data.

- **Silos of security & compliance information** - While compliance is a top concern of IT leaders, information security can be seen as an inhibitor to agility. Many organizations rely on a number of tools to manage security and compliance in the cloud. Some are deployed and managed by DevOps teams, to support their specific needs, while others are deployed by SecOps in support of their own specific needs. This scenario creates a siloed and uncorrelated set of data, that can actually impede visibility and only serves to adds additional complexity to an already complex environment. And, in addition to the security and compliance risks, inherent with this approach, it can also negatively impact the agility and scalability benefits that were expected to be gained from the cloud.

Sumo Logic solutions

- **Security at the core** - Sumo Logic was designed to provide organizations with the visibility, confidence and assurances they need to manage security Gain deep customer insights in real-time with Sumo Logic's cloud-scale machine data analytics platform and compliance as they move to the cloud. This includes the level

of information security, confidentiality, integrity and availability required to meet rigorous standards.

This is achieved through regular independent third party audits of the Sumo Logic cloud platform to provide organizations and regulators with an independent verification of the security, privacy and compliance controls that are strictly managed across the entire platform. Independent auditors examine our security and compliance controls in our infrastructure, policies, procedures and operations.

PCI/DSS 3.2 Service Provider Level 1 Certified
SOC 2 Type II attestation
ISO 27001 certified
CSA Star certified
HIPAA-HITECH compliance
U.S. – EU Privacy Shield
AES 256-bit encryption at rest
TLS encryption in transit
FIPS 140-2 compliant
GDPR
FedRamp (Pending)

- **Scalable SaaS delivery model** - Legacy networking and security tools were not built to handle the massive increases in the amount of information that must be processed and analyzed in the cloud. With finite resources in these devices, and storage solutions, the elastic, unpredictable and highly dynamic nature of cloud environments quickly breaks the efficacy of these devices. Sumo Logic was built in the cloud to provide organizations with the same benefits they expect to achieve as they move to the cloud - flexibility, scalability, and agility as the types, quantities and sources of data continue to increase. Sumo Logic is delivered as a true SaaS model, following the "5 Essential Characteristics" as defined by the NIST (National Institute of Standards and Technology).
- On demand/self-service - (software and cloud storage as needed)
- Broad network access - (ubiquitous availability)
- Resource pooling - (multi-tenant)
- Rapid elasticity or expansion - (common code base for rapid updates)
- Measured service - (pay as you go)

- **Enabling DevSecOps with centralized visibility -** Sumo Logic provides DevSecOps teams, and other key stakeholders with a common, centralized platform for real-time visibility, with adaptive situational awareness into the organization's critical infrastructures, and full stack of business critical applications. In addition, external threat intelligence is built-in to provide additional context and awareness of threats outside of the organization. Armed with these holistic insights, organizations are able to more rapidly identify, remediate and manage threats to their security and compliance standards and minimize the risks to their strategic initiatives.

- **Cloud agility and scalability** - Sumo Logic is a cloud-native software as a service (SaaS) platform, to provide users with all the capabilities that they themselves expect from the cloud. Including agility, scalability, and elasticity and the delivery of continuous integration and continuous delivery (CI/CD) of increasingly optimized security and compliance applications at scale. A model that is just not possible with legacy premises based security tools, such and the majority of SIEMs on the market today.

- **Democratization of security & compliance information** - Sumo Logic enables organizations to collect, consolidate, and analyze log and event data, including insights into user activity. Sources include common cloud environments (including AWS, Microsoft Azure and Google Cloud Platforms), hybrid cloud environments and traditional, legacy, stand-alone premises based sources. Additional context and visibility can also be derived from integrations into 3rd party security solutions (such as Okta, Akamai, and Docker), and from common cloud application platforms (such as Salesforce.com, Box and Office 365). and derived from custom built critical business applications developed internally by the organization. With pre-built dashboards that provide insightful graphical context and centralized visibility.

About Sumo Logic

Sumo Logic is the leading cloud-native machine data analytics platform, that delivers real-time, continuous intelligence across the application lifecycle and stack. www.sumologic.com.

Toll-Free: 1.855.LOG.SUMO | **Int'l:** 1.650.810.8700
305 Main Street, Redwood City, CA 94603

www.sumologic.com