aws partner network | sumo logic

Cloud SIEM powered by AWS

Multi-Cloud and Hybrid Cloud Threat Protection

Challenges

Modernizing security to build trust and mitigate risks

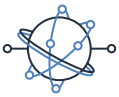
- Inability to monitor, secure multi-cloud and on-premises assets and applications.
- Constrained by siloed legacy security tools that create too many false positives, and alerts that lack meaningful insights.
- Poor visibility into risky users and malicious activities that negatively impact business and brand.
- Need to quickly detect and respond to the higher-priority issues.

The Sumo Logic Cloud SIEM Solution

Provides Multi-Cloud and Hybrid Cloud Threat Protection

The Sumo Logic Cloud SIEM is a Hybrid and Multi-Cloud Threat Protection solution that reduces security blind spots with comprehensive visibility in AWS, across multi-cloud and on-premises to identify issues before they become incidents, enhance security posture, and improve customer's risk profile. The solution provides:

- Unified security visibility for hybrid and multi-cloud architectures
- Deep security visibility into AWS services - tightly integrated with Amazon GuardDuty, AWS Security Hub and more
- Integrated Threat Intelligence that helps accelerate threat detection
- Reduced time and effort to meet audits for regulations, such as PCI, HIPAA, etc.
- Multi-dimensional context and security analytics on user activities
- Out of the box integration with key Amazon Web Services services and other cloud services



Multi-cloud and Hybrid Cloud Coverage

Complete cloud coverage that unifies security analytics and investigations within AWS with deep integrations, across AWS, other cloud data, and on-premises data

Deep security insights

Machine learning-driven detection, threat intelligence driven correlation, and deep search-based investigation

Rapid compliance

Pre-built reports that provide granular visibility to reduce the time and effort to meet audits for regulations, such as PCI, HIPAA

Easy to use and low TCO

Cloud-native, elastic scaling and flexible cloud licensing model provide unparalleled ease of use and low TCO

Sumo Logic on AWS

The Sumo Logic Cloud SIEM solution natively integrates with AWS services to automatically enable organization's need for modern cloud security across hybrid and multi-cloud environments. The solution is built on Sumo Logic's cloud Security Intelligence platform and leverages AWS security services such as GuardDuty, Security Hub, VPC FLow.
It provides deep insights to eliminate security blind spots across multi-cloud and hybrid environments and identify issues before they become incidents, enhance the security posture, and reduce an organization's risk profile.

Features

Real-time threat detection

It identifies threats in real time helping with quick response by leveraging advanced machine learning algorithms at cloud scale. You can enforce security configurations and monitor for any drifts across your cloud environments.

Built with security-first principle

The platform's third-party compliance attestations and certifications, including PCI DSS 3.2.1 Service Provider Level 1 attestation of compliance, SOC 2 Type 2 Audit Report, HIPAA Security Rule Attestation of Compliance, ISO 27001 Certification, and CSA STAR Level 2 Certification enables use in regulated environments and to meet business outcomes.

Automated prioritization and alert triage

Insights are generated by the Adaptive Signal Clustering (ASC) engine using principles modeled on the actions of world-class SOC analysts to group related Signals worthy of human review. This provides analysts with the identification and context of a significant issue and its movements, including multiple low-severity Signals that often go undetected.

Case study

medidata

Challenges

Medidata CISO needed insight into the security posture of its systems and be able to spot potential indicators of significant events from within its on-premises systems and cloud services, so that it could stop attacks as quickly as possible and be able to substantiate its high level of security to its clients.

Solution

Medidata simplified cloud and on-premises audits and strengthened its security posture with a composite view across the network, server, and application stack using Sumo Logic. Medidata security engineers uncover unknown security issues without relying on rules or predefined schemas to ward off impending threats.

Results

Medidata logs more than 2 terabytes of system event data each month. With Sumo Logic, Medidata has the same level of security visibility into cloud systems as on-premises systems. Now Medidata can proactively resolve security incidents that would have otherwise gone undetected.

Learn more about Cloud SIEM powered by AWS

Or start a Free Trial on AWS Marketplace today