sumo logic

Sumo Logic Cloud Security Analytics Security data lake promotional offer

Sumo Logic Cloud Security Analytics is a cloud-native solution that makes it easy and cost-effective to collect, store and search your security information and cloud data in one central, secure location with flexible licensing and data tiering. Sumo Logic maintains rigorous compliance certifications, including PCI, HIPAA, FISMA, SOC 2 Type II, GDPR and FedRAMP™.

Selling propositions

- Centralized storage for your structured and unstructured data
- Single security data lake and analytics tool that can visualize and provide a comprehensive view of all the data from an organization's information systems
- Scalable data management allows you to store high-value data used for detection and first level investigations alongside high volume data used for audit/ compliance and extensive threat investigations

Challenges/Opportunities

- **Data everywhere: Security logs and event data are spread across disparate systems/tools**
- **Lack of visibility: Organization is unable to derive insights from their heterogeneous data**
- **High costs: Storing the high volume of data necessary for audit/compliance and extensive threat investigation is too expensive**

Key data points

Strong Performer

2022 Forrester Wave recognition for Security Analytics Platforms

Secure & Compliant

HIPAA, FISMA, ISO 27001, SOC 2 Type II, GDPR and FedRAMP™, and a certified PCI-DSS Level 1 Service Provider

Vendor Agnostic

Data collection and storage of security logs, combined with domain-agnostic analytics

Products

Cloud Security Analytics - Security data lake

Offers: 10GB, 50GB, 100GB or 150GB

Audience

Security Engineer, IT Engineer, Security Analyst, DevSecOps Engineer, Information Security Compliance Analyst/Manager

Ecosystem

Amazon Security Lake

GCP

Azure

Competitors

Splunk

Datadog

Exabeam

Valid for Transactions through September 30, 2023

sumo logic

Available assets

- Cloud Security Analytics solution page
- Security data lake use case page
- Sumo Logic security platform video
- Medidata case study
- Sumo Logic Accelerates Data Insights to Modernize SecOps press release
- How to improve your microservices architecture security blog

Offer details

- **Cloud Security Analytics - Security Data Lake 10GB:** 10GB daily log ingest plus 365-day retention and 25K data points per minute (DPM) for additional investigative analytics.
- **Cloud Security Analytics - Security Data Lake 50GB:** 50GB daily log ingest plus 365-day retention and 150K DPM for additional investigative analytics.
- **Cloud Security Analytics - Security Data Lake 100GB:** 100GB daily log ingest plus 365-day retention and 150K DPM for additional investigative analytics.
- **Cloud Security Analytics - Security Data Lake 150GB:** 150GB daily log ingest plus 365-day retention and 150K DPM for additional investigative analytics.

Key Sumo Logic differentiators

- All data in one place for storage, search and API access
- Flexible and configurable Data Tiers for different types of security data
- Depth of search capability plus usage-based pricing when accessed
- Full-featured support for convergence of SecOps and DevOps on a single cloud-native SaaS platform (running natively in AWS for 12 years)
- Sumo Logic is a certified PCI-DSS Level 1 Service Provider
- Available via our FedRAMP™ Moderate authorized product offering

Competitive rebuttals

OBJECTION	RESPONSE
"We use **Exabeam's** Data Lake	Are you running it on-prem with their physical appliance or virtual machine? If so, then you know that it's just Elastic on the back-end, and that's why their search is very limited, and can buckle under load. Or, are you using Exabeam's "new-scale" Security Log Management? Sumo Logic **has been running natively in AWS for 12 years** (as of 2023) with a multi-tenant, microservices architecture. We've always understood the importance of scale and our platform analyzes 1.7 exabytes of data per day on average.
"We're happy with **Datadog.**"	Datadog is not a great solution for storing log data due to its high cost of long-term retention. Since they lack the concept of data-tiers, they pressure their users to store data in their own cloud storage, via their "logging without limits" feature, to save cost, but then charge their customers to rehydrate that data back into the platform when they want to run analysis on that data.