**Key benefits**

- **Enhanced visibility**
  Delivers context across users, networks, devices, alerts, cloud services and applications while prioritizing the information needed to speed response times.

- **Improved productivity**
  Automates the manual, repetitive validation tasks that limit efficiency, freeing analysts to make advancements in identifying new threats.

- **Unlimited scalability**
  Supports growth with a cloud native, open source, and big data architecture.

- **Focused workflows**
  Enables analysts to perform high value risk-reduction activities like threat hunting, response, and remediation.

- **Advanced insights**
  Automatically groups related threat signals into Insights, alleviating manual triage efforts.

**Product overview**

The Sumo Logic cloud-native analytics platform helps you manage the operation and security of modern applications. Collect, correlate, and analyze all types of machine data (logs, metrics, events) to reduce the time to identify, troubleshoot, and resolve performance, security, and compliance issues.

**Product features**

**Alert analytics generating signals from logs**

Sumo Logic provides a convergence of data sources, collecting millions of logs and security-relevant data from cloud, on-premises, and hybrid architectures. It uses pattern and threat intelligence matching with correlation logic, statistical evaluation, and anomaly detection to filter the raw records down to thousands of signals in near real-time.

**Correlation-based detection**

Insights represent the intelligent, correlated, and prioritized clustering of signals and other data enrichments for analysts to immediately investigate. Insights dramatically decrease validation and investigation times by presenting an automatically generated storyline of potential security incidents containing all of the relevant context analysts require to make rapid response decisions.

**Automated prioritization and alert triage**

Insights are generated by the Adaptive Signal Clustering (ASC) engine using principles modeled on the actions of world-class security operations center (SOC) analysts to group related signals worthy of human review. This provides analysts with the identification and context of an attack and its movements, including multiple low-severity signals that often fly below the radar. ASC engine algorithms are continuously improved as customers identify patterns, validate signals and Insights, or add new searches.
How it works

Sumo Logic leverages powerful machine learning driven analytics capabilities such as pattern identification, outlier detection and predictive trending to quickly alert and troubleshoot applications and infrastructure performance and security issues. Sumo Logic provides out-of-the-box pre-built analytics and dashboard for AWS services including Amazon Elastic Compute Cloud (EC2), Amazon Simple Storage Service (S3), AWS CloudTrail, Amazon CloudFront, Elastic Load Balancing (ELB), Amazon VPC Flow Logs, AWS Config, and AWS Lambda.

Differentiators

- Benefit from a cloud native, multi-tenant architecture that processes more than 100 petabytes of data and handles 20+ million queries daily. Use an elastic solution that scales irrespective of data volume or number of users.
- Protect your users' data with first-rate security technologies, rigorous security process, and daily rotated, per-customer encryption keys.
- Identify and predict anomalies in real-time with outlier detection and uncover root-causes using patented pattern analyses. Enable power users via a rich library and empower others with easy-to-use search templates.
What our customers are saying

Pokémon Strengthens Its Security and Saves Time with Sumo Logic

Challenge
Following the immense success of Pokémon Go app, The Pokémon Company International needed to migrate much of the company’s technology stack to Amazon Web Services (AWS), and then establish it as a core platform to support many other usages.

Solution
Pokémon adopted Sumo Logic’s born-in-the-cloud technologies to ingest and organize machine data from across its entire AWS portfolio. This also encompassed adopting a comprehensive set of dashboards, alerts, and other automated tools to continually monitor the threat landscape.

Benefits
- Substantially enhanced reactive capabilities
- Centralized machine data
- Applied automated responses across its security environment
- Slashed the amount of time necessary to conduct critical business operations

“With hundreds of millions of customers, any security breach would be devastating. There’s simply no way that we could hire enough analysts to manually carry out the hard work of protecting sensitive user information that Sumo Logic does for us automatically.”

John Visneski, Director of Information Security and Data Protection Officer, Pokémon

Solution available in AWS Marketplace