

Gain 360-degree visibility of your security

Dig into the modern threat landscape and right-size your security investment



What's inside?



Modern security analytics
for small business teams

3

Sumo Logic - AWS built-in

14

Security analytics challenges

6

Streamline and accelerate
your cloud transition

16

Why choose AWS?

8

Cloud Infrastructure Security
news across Europe

17

Why choose Sumo Logic?

10

Case studies

18

Sumo Logic and AWS together
deliver enhanced security

13

Future-proof your AWS
security with Sumo Logic

20

Modern security analytics for small business teams

Amazon Web Services (AWS) and Sumo Logic collaboration overview

Safeguard your applications with deep security insights

The cybersecurity landscape is rapidly changing. To modernize your applications and compete better, you must introduce changes to your software stack that expand your attack surface. This increases the amount of data generated, making the task of analyzing security data to uncover cybersecurity threats overwhelming—especially if you don't have a dedicated security team or have small IT teams lacking security expertise.

Sumo Logic on AWS provides powerful, automated data analytics tools, enabling real-time analysis and alerting across your services and infrastructure to start protecting your business instantly.

Whether you already operate in the cloud, or your organisation is migrating from a legacy on-premises infrastructure to a cloud-based solution, Sumo Logic on AWS offers out-of-the-box integrations for single-pane-of-glass security visibility that helps you reduce the time to detect and remediate security issues.

This ebook explores how you can benefit from an all-in-one cloud log analytics platform to stop advanced attacks, identify and manage emerging risks and enhance your security posture. Discover how to reduce the security risk of your cloud-native applications with Sumo Logic—enjoy continuous, scalable, centralized Cloud Infrastructure Security with pre-built dashboards to help minimize blind spots across your entire tech stack.



87%

of organizations say ensuring secure and available applications is a top three cybersecurity priority



At a glance—our complementary capabilities



Assess security alerts
across AWS accounts

Provides services to build
cloud applications

Protects AWS accounts and
workloads from malicious activity.



sumo logic

Security analytics
across AWS accounts

Tool consolidation to increase
efficiencies and reduce cost

Cloud Infrastructure Security to reduce
time to detect and investigate threats

AWS shared responsibility model

In the AWS shared responsibility model, you are responsible for securing the software, tools and data that use AWS Services, and Sumo Logic can help you identify gaps in those components. When you use Sumo Logic to analyze logs from AWS services, software tools and applications, you get unified security visibility across the shared responsibility model, eliminating gaps in security detection.

AWS responsibility

Responsible for security 'OF' the cloud.

AWS is responsible for the maintenance of all hardware, software, networking and physical facilities running AWS services.

AWS offers resources (e.g., frameworks, audits, reviews) to help you determine the distribution of responsibilities based on your unique use case.

SOFTWARE:

Compute, storage, database, networking

HARDWARE/AWS GLOBAL INFRASTRUCTURE:

Regions, availability zones, edge locations

Customer responsibility

Responsible for security 'IN' the cloud.

You are responsible for all necessary security configurations as determined by your selected AWS services (varying responsibilities—unique to each customer— also extend to IT controls).

You can take advantage of shifting certain controls in your use case to AWS in a distributed control environment.

Customer data, platform, applications, identity & access management, operating system, network and firewall configuration, client-side data encryption, server-side encryption, networking traffic protection.

The combined benefits of Sumo Logic on AWS are clear

Sumo Logic accelerates AWS cloud security insights into actions. Ingesting AWS logging data into Sumo Logic's analytics platform enables continuous threat detection with centralised security visibility without needing a team of expensive security experts.

More than 2,000 customers worldwide rely on Sumo Logic to run and secure their modern applications and cloud infrastructures. AWS and other cloud apps and services, you can ensure a secure and holistic view of your AWS accounts and applications.

Continue reading to discover how Sumo Logic on AWS can help you overcome specific security analytics challenges unique to your business and industry—uncover how Sumo Logic Cloud Infrastructure Security helps deliver the data-driven holistic protection you need.

2000+

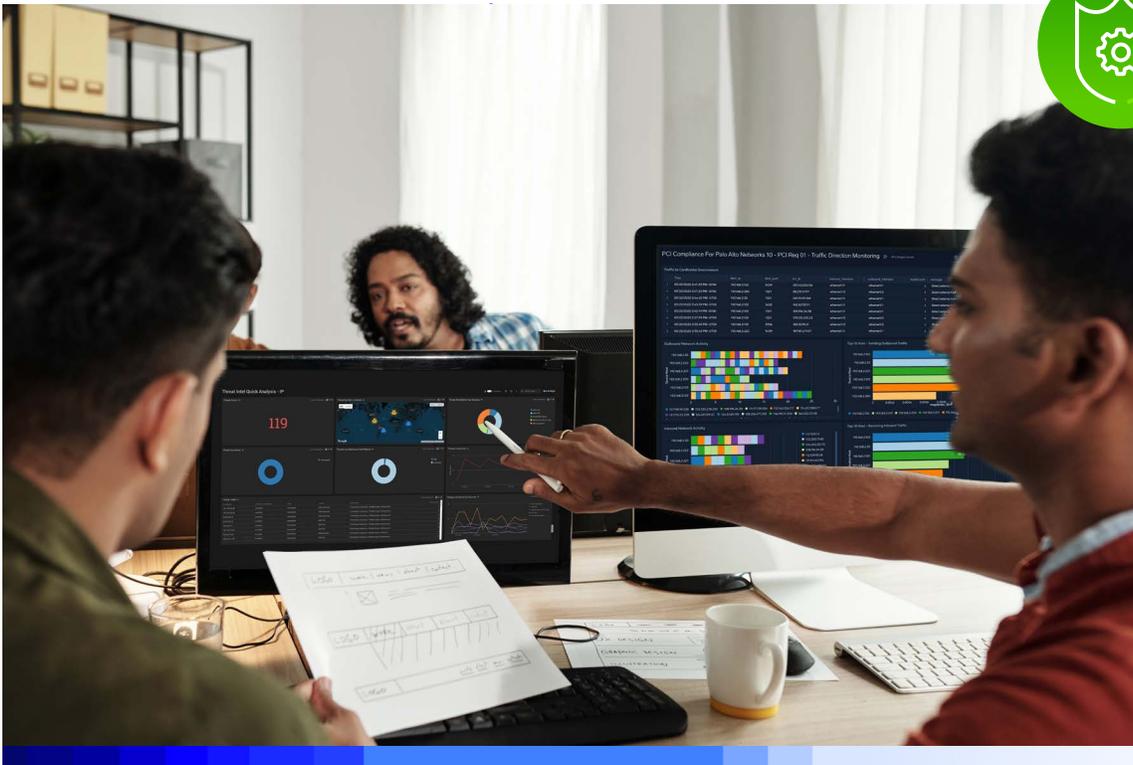
customers rely on Sumo Logic

99.99%

service uptime

200+

AWS services integrations



Security analytics challenges

Gain unified visibility across your AWS accounts

Prevent, detect, respond and remediate

Establishing strong in-house security practices raises multiple challenges. For example, you may encounter IT resource constraints, costly hardware and software maintenance, not enough time or resources to make sense of the large volume of security events, and a lack of access to on-demand, reliable digital security expertise. You need an all-in-one, AWS-native cloud infrastructure security solution that lets you take control of what's hard to control.

Sumo Logic on AWS enables you to automate manual security analytics across your environments by continually monitoring your software stack to surface the most relevant security threats in real time, improving visibility across your AWS cloud infrastructure and applications.

Your teams can instantly visualize and assign specific queries to custom or out-of-the-box dashboards for faster threat detection and resolution times.

Access the tools you need to quickly identify, analyze, and investigate the root cause of potential security events or unauthorised activities, all in one place.

Top security challenges facing business decision makers and technical practitioners

These are the most common infrastructure security challenges, highlighting how Sumo Logic can help address them:



Complexity

Multiple tools collecting and generating security data force operations teams to 'swivel chair' between tools and management consoles to detect cyber threats in their apps and infrastructure. Sumo Logic provides unified visibility across security tools that eliminates the swivel chair and reduces the time to detect and resolve security issues.



Lack of visibility and context

With the data explosion from modern apps and services, security professionals find they lack holistic visibility into their security posture and potential cyber threats. Sumo Logic centralizes security logs and leverages ML to correlate them and enhance them with threat intelligence, providing companies with the context they require to accelerate security threat resolution.



Lack of staff, or lack of security experience

As the threat landscape continues to evolve, security operations continue to be an area requiring more human resources from a limited pool of candidates. Companies are forced to dedicate their small security engineers or analyst teams to focus on detecting, investigating and responding to cyber threats using legacy tools that are too expensive or can't scale for the job. Sumo Logic monitors and analyzes security logs in real time across all of the security tools (e.g., SASE, Endpoint, IAM, Email, Threat Intel, Vulnerability Management), cloud infrastructures (e.g., AWS), and SaaS applications (e.g., Office 365, Salesforce, Zoom, Slack), providing the most relevant information teams need to address security issues.



High cost

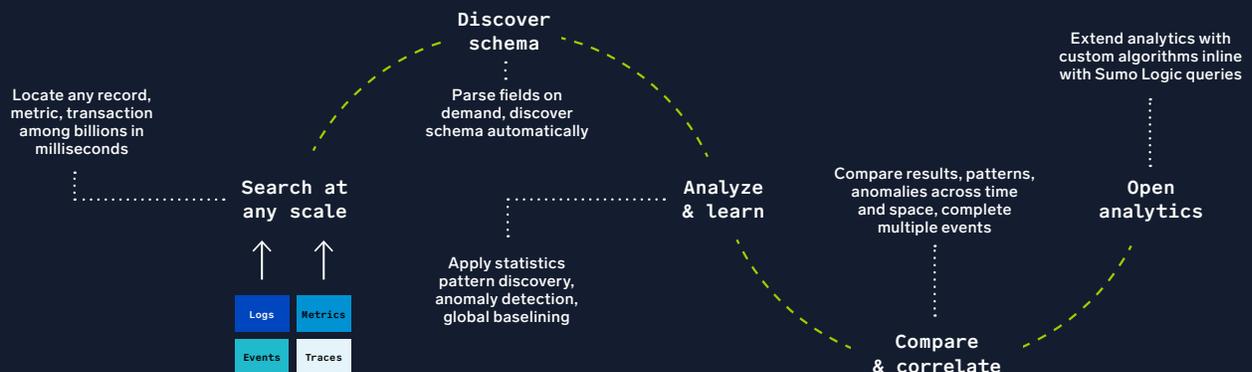
Security teams often face tough decisions about which data sources they can afford to collect and store for use in threat detection. This can leave out crucial indicators of threats and malicious activities that can have disastrous consequences. Sumo Logic data tiering allows you to store and analyze as much data as needed with optimized cost and flexible licensing that eliminates overages charges during spikes.



Disparate tools for security monitoring

Sumo Logic allows you to ingest a diverse array of firewall, identity/access and CDN data, providing a single pane of glass to help your team reduce the time needed to identify security issues.

Analytics that enable multiple sophisticated platform use cases



Why choose AWS?

Kickstart innovation and expand into new markets faster

Elevate customer experiences with the cloud

Continuous innovation and speed to market have become driving factors in how businesses your size conceive, develop and implement security practices. That's why security log analytics for your new cloud-based applications remain a high priority for small and medium-sized businesses. No SMB can afford the risk to run their cloud-based application without knowing their security posture and how to detect security threats.

AWS provides baseline security measures to help you migrate and monitor mission-critical workloads with confidence. Armed with easy-to-use, cloud-native security tools and capabilities, your teams can enhance visibility across your environments to minimize blind spots and protect every layer of your architecture.

69%¹

Reduction in unplanned downtime

43%²

Fewer monthly security incidents

31%³

Average cost savings

“The cloud abstracts the complexity of the physical security from you and gives you the control through tools and features so that you can secure your application.”

AWS security best practices

¹ Source: The Hackett Group - The Business Value of Migration to Amazon Web Services

² Source: Business Value on AWS - Realizing Business Value with the AWS Cloud Value Framework

³ Source: IDC White Paper - Fostering Business and Organizational Transformation to Generate Business Value with Amazon Web Services

How you can benefit from working with AWS

AWS lets you safeguard your customer data, corporate data, and operating environments. What's more, AWS experts and partners are on hand to help train your teams on how to quickly detect and correctly respond to developing threats. You can also automate manual security tasks so your teams can focus on scaling and developing business objectives.



The highest level of cloud security

AWS security infrastructure is built to satisfy the highest requirements of the world's leading financial, educational and governmental institutions.



Real savings businesses can see and measure

AWS offers free tools and calculators to assess costs and measure your migration ROI, taking the guesswork out of operational costs and identifying new opportunities to save money.



Built-in reliability and resiliency

AWS's investment in global availability zones and redundant networks, storage, and computers helps ensure you always have access to critical data and applications.



Support through best-in-class partners, programs and training

AWS and its partners can help you plan, scope and size data migration, as well as reduce risk and complexity by automating shifting workloads to the cloud.



A broad, deep, and constantly growing set of capabilities

AWS has 200+ fully featured services for compute, storage, databases, networking, analytics, machine learning and artificial intelligence, Internet of Things, mobile, security, hybrid, virtual and augmented reality, media, and application development, deployment, and management.

Why choose Sumo Logic?

Extract meaningful security insights in real time, regardless of data volume

Conceived and launched on AWS

Sumo Logic is a highly scalable security log analytics platform that complements AWS security services, helping you streamline and accelerate migrations to AWS by monitoring and securing software stack and cloud apps.

Combine AWS and non-AWS services under Sumo Logic to enable multiple security analytics use cases and take your security analytics to the next level by tapping into global threat benchmarking across AWS services.

Security capabilities enabled by combining Sumo Logic security analytics with AWS services

Independent response and compliance status



AWS Security Hub



AWS CloudTrail

Zero Trust



Amazon GuardDuty



AWS Config



AWS CloudTrail

Vulnerability Management



Amazon GuardDuty



Amazon Inspector



Amazon VPC

Inside Threat Detection



Amazon GuardDuty



AWS CloudTrail

- Reduce security blind spots and reduce your risk profile
- Automatically turn on and configure key AWS features
- Addresses your multi/hybrid cloud security capability needs
- Global threat benchmarking across AWS CloudTrail & GuardDuty

Security and compliance SaaS solutions close the gap

Sumo Logic is a leader in cloud infrastructure security. Organisations of your size can leverage cloud computing to address modern data challenges and identify new security opportunities. The Sumo Logic SaaS Log Analytics Platform automates the collection, ingestion and analysis of application, infrastructure, security, and IoT data to derive actionable recommendations within seconds.

Sumo Logic delivers a multi-tenant SaaS architecture that supports many AWS integrations, including:



AWS CloudTrail

Gain insight into who is accessing your AWS account and receive alerts when users make changes.



AWS Config

Get a 360 view across your AWS environments with instant access to changes happening in real time.



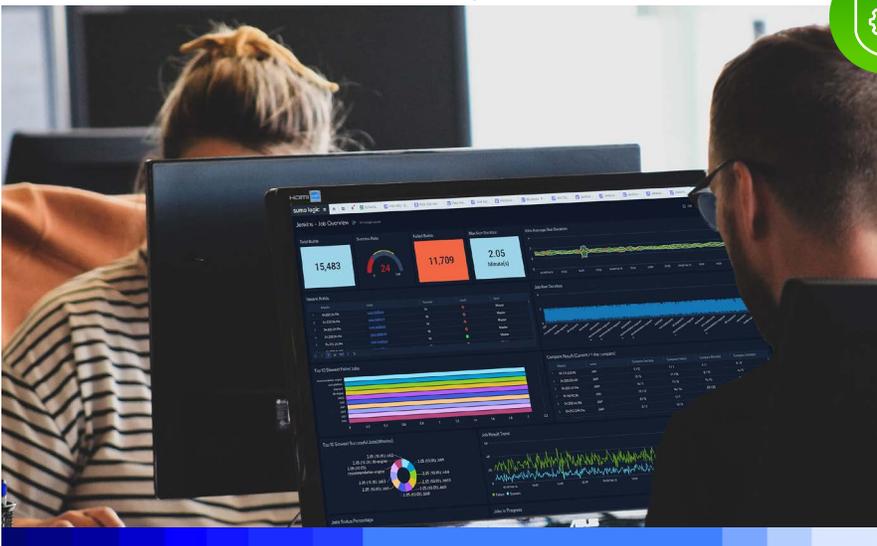
Amazon Virtual Private Cloud (Amazon VPC)

See where and how changes to your data are impacting your network traffic and latency.



Amazon Inspector

Understand how the changes to your systems and applications affect your security and compliance.



Benefits of Sumo Logic

Quickly detect threats and security incidents with granular dashboards tuned to threat detection and investigation use cases, allowing your teams to quickly drive to resolutions when security incidents do occur. Generate actionable security recommendations via use-case-driven queries, dashboards and alerts.



Instant value

With Sumo Logic's cloud-native SaaS offering, you can get started in minutes. Access all the latest capabilities without the need for time-consuming, expensive upgrades. Start small and expand as your business grows.



Elastic scalability

Sumo Logic's multi-tenant architecture scales on demand to support cloud migration and rapid application growth. The service overcomes the limitations of traditional architectures by allowing you to burst as needed without manual intervention.



Proactive analytics

Sumo Logic is known for powerful machine learning and analytics. You can benefit from out-of-the-box integrations to help you quickly make sense of expected and unexpected behaviours across your environments.



Secure by design

Sumo Logic maintains the highest level of security certification to protect your data, including CSA STAR, GDPR, PCI DSS Service Provider Level 1, ISO 27001, SOC 2 Type II, FIPS 140 Level 2 and HIPAA.



Reliability

SLAs on availability and performance ensure Sumo Logic services are always on and performing per your expectations. Sumo Logic also publishes live service status updates for greater transparency.



Out-of-the-box competencies

Instantly begin to monitor your data, identify trends and stay on top of critical events. Easily build dashboards for your custom applications.

When you're ready to evolve your security practices with add-on modules, Sumo Logic still has you covered with SIEM.

Sumo Logic and AWS together deliver enhanced security

Security best practices that work

AWS provides the most reliable and scalable services to build your cloud applications and Sumo Logic provides log aggregation, pattern detection and machine learning capabilities across AWS and non-AWS services to give you the detailed visibility you need to help resolve security analytics challenges faster. Capture, visualize, and analyze your data from a unified platform—together, the advantage is clear.



Eliminate data silos in your organization

Through unified visibility across your AWS accounts, your teams can easily eliminate data silos, reduce tools sprawl and close the skills gap created by disparate solutions.



Accelerated remediation

Give your security teams the anomaly detection tools they need to identify deviation events in real time, analyze threats, and resolve issues before they become incidents.



Out-of-the-box AWS integrations

Pre-defined dashboards for many AWS services enable you to quickly visualize your data with contextualized alerting. Flow your AWS telemetry into Sumo Logic's platform in minutes.



Get insights in seconds

Attack surface benchmarking improves workload threshold efficiencies by comparing data with AWS peer groups to help detect misaligned behaviors in your cloud infrastructure.

Sumo Logic - AWS Built-in

The better together vision

AWS built-in (ABI) is a rigorous AWS designation that helps you accelerate your cloud adoption by making it easier to configure key AWS services with ISV solutions. AWS Built-in solutions go through an exhaustive AWS certification and validation process before they are approved for launch. Sumo Logic is proud to be one of the first partners with the AWS Built-in designation for cloud infrastructure security.

Sumo Logic AWS Built-in helps you:



Reduce your
employee workloads



Deploy and configure
the right AWS
services faster



Accelerate deployment
of a cloud scalable
analytics solution



Reduce business
risks originating from
misconfiguration

How does Sumo Logic - AWS Built-in work?

Legacy security tools cannot handle the massive increases in information processed and analysed in the cloud. Maintaining a strong security posture when handling thousands upon thousands of log messages—containing potentially sensitive data—across multi accounts environments is a monumental task. Sumo Logic AWS Built-in reduces the time to configure and enable a unified security analytics solution across multiple accounts.

- Single deployment to enable and configure key AWS services across an entire AWS organization
- Configures Sumo Logic to receive, visualize, and alert on GuardDuty and CloudTrail events
- Implements best practices in the AWS Security Reference Architecture (security tooling and log archive OUs)
- Enables Sumo Logic Global Intelligence Service—ML-driven global threat benchmarking across AWS CloudTrail and GuardDuty

Customer benefits of Sumo Logic ABI



Fast time to value

Single deployment to configure AWS security services across an entire AWS organization, and set up Sumo Logic using a Sumo Logic AWS Quick Start.



Full cloud coverage

Unify security visibility across AWS accounts and hybrid environments.



Reduce detection and investigation times

ML-driven detection, integrated threat intelligence correlation, deep search-based investigation.



Ease of use and low TCO

Unify overages during spikes and over-provisioning for bursts in workloads and data.



Rapid compliance readiness

Broad integration and pre-built reports accelerate your compliance readiness.



Security-first principle

PCI DSS Level 1 Service Provider, SOC 2 Type 2, HIPAA attestations and FedRAMP™ authorized.



Flexible and easy to extend

Extensibility of security investments and option to automate SecOps workflows with Sumo Logic.

Streamline and accelerate your cloud transition

Access full cloud migration support

Boost your cloud migration strategy

Sumo Logic provides powerful security analytics across your legacy environment and AWS that help you migrate your application to AWS confidently. With Sumo Logic, you can analyse side-by-side logs from your legacy application and the new software stack on AWS to have a full picture of the application security and remediate security threats quickly.

Out-of-the-box integrations with AWS also mean you can quickly and easily implement best practices for modern cloud infrastructure security challenges across hybrid and multi-cloud environments, with real savings businesses can see and measure.



Accelerate the time to make decisions

Out-of-the-box cloud migration services provide application architecture and environment health indicators in real time, which can help inform your decision-making process during migration.



Release applications with confidence

Create customizable application analytics. Leverage KPIs from both structured and unstructured logs and metrics. Compare side-by-side performance in on-premises, hybrid and public cloud environments, enabling application optimization prior to production.



Data-driven decisions

Sumo Logic empowers you to build high-quality, real-time, automated models of applications and dependencies, delivering the data-driven insights you need to lay the foundations of cloud migration.



Benchmark and optimise cloud systems

Measure and compare your security data with the community. Create baseline alerts for emerging modern threats and gain insights to help your teams continuously innovate and advance data security and remediation strategies.

Cloud Infrastructure Security news across Europe

Europe leads the US in using machine data analytics for security use cases

European businesses are considerably ahead of the USA when it comes to security analytics. Customer experience, compliance and security represent strong values for European businesses that want machine data tools to drive even more insight.

Stay ahead of the changing attack surface

Sumo Logic Cloud Infrastructure Security accelerates security engineering by providing granular visibility at cloud scale. Always on monitoring provides holistic visibility across perimeterless cloud infrastructures, empowering your teams to prioritize and investigate security threats that would have otherwise gone undetected.



Increased visibility across your tech stack

Gain increased visibility, from logging cloud data to monitoring and securing hybrid clouds.



Native cloud support

Ingest firewall, database, identity/access and CDN data. Prioritize and act on incidents as they occur.



Advanced security focus

Your security teams can explore user-level granularity via Sumo Logic's native query language, dashboards and alerts.



Detect threats in real time

Identify threats, monitor for drifts and enforce security configurations in real time across environments.

Sumo Logic makes it easy for your security teams to seamlessly identify relevant security insights across users, devices, IPs, networks and databases relevant to your desired requirements.

Whether digging into specific messages to identify security insights or summarizing a broad data set through Sumo Logic operators (e.g., LogReduce), the fast and efficient algorithms can help deliver advanced insights into your ongoing security needs.

Case studies

Showcasing the business benefits of enhanced data visibility

Sumo Logic on AWS provides you with modern security log analytics tools, enabling your security teams to break down data silos, improve monitoring, and enhance your troubleshooting capabilities. See how Medidata, HashiCorp, Standard Chartered, Pokémon and SoSafe leveraged Sumo Logic on AWS to increase visibility and gain key security insights.



The challenge

Medidata wanted to respond to threats quickly by leveraging a single-pane-of-glass displaying IP calls, network flows and any relevant information, protecting not just the company's data perimeter but its entire AWS environment.

The solution

Sumo Logic delivered security recommendations in real time across Medidata's entire infrastructure, providing compliance reports and a composite view across the network, server and application stack.



The challenge

HashiCorp recognised the need for fast security investigation capabilities, enabling security teams to sift through infrastructure telemetry data for tens of thousands of customers (including the massive volumes of various events HashiCorp generates).

The solution

Sumo Logic's cloud-native solution unlocked centralized security visibility and monitoring for HashiCorp across complex environments, comprising three infrastructure-as-a-service cloud environments and API integrations with each cloud vendor's full suite of products.



The challenge

Standard Chartered required a unified analytics platform, supporting security analytics, DevOps, customer experience and much more. Specifically, the solution had to be relatively easy for both technical and non-technical users to adopt quickly.

The solution

Sumo Logic provided a user-friendly, cloud-native architecture, enabling company-wide data visibility, hyper scalability and extensive API and data collection support for turnkey integration into Standard Charter's ecosystem.



The challenge

In light of the Pokémon Go app's unprecedented success, Pokémon decided to migrate the company's technology stack to AWS, bringing the game's development in-house. Pokémon highlighted the need for a top-tier security operations center (SOC).

The solution

Sumo Logic centralized Pokémon's machine data, providing dashboards, alerts and other automated tools to continually monitor the threat landscape. This substantially enhanced Pokémon's reactive capabilities and slashed the time to conduct critical business operations.

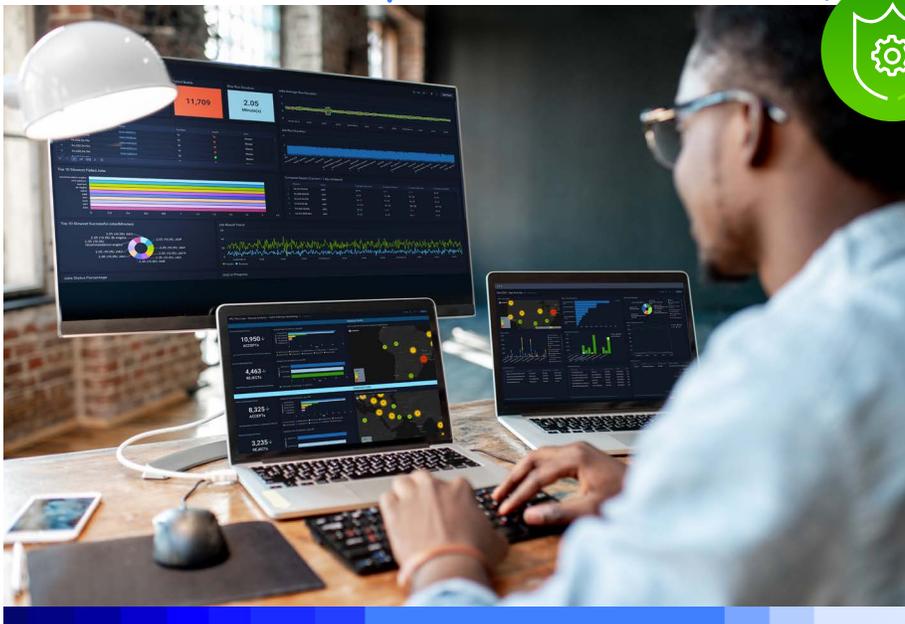


The challenge

A cloud-native, serverless-first company, Snoop has accrued over 1 million app downloads and 250,000 active users. Snoop's small team needed a way to maintain high levels of customer service in the face of such rapid growth.

The solution

Sumo Logic helped Snoop implement distributed tracing, meaning they can track and uncover issues before they become customer-facing problems. Sumo Logic's support frees up Snoop's team to focus on delivering great customer experiences.



Futureproof your security with Sumo Logic on AWS

Let's continue the conversation

This ebook has shown how Sumo Logic's out-of-the-box—and easy-to-implement—security integrations can help you achieve a 360-degree view of your security data across your AWS cloud environments.

The unique differentiators of Sumo Logic on AWS include:



Security integrations

Out-of-the box security integrations yield a shorter time to value.



Incident remediation

Use-case driven queries, dashboards and alerts can help speed your incident remediation.



Visibility

Increased visibility empowers you to act against threats to help you stay ahead of the evolving attack surface.

Leverage a highly elastic and scalable SaaS log analytics platform

Using Sumo Logic on AWS, you can rigorously identify suspicious behavior, and apply pattern clustering to log data to surface outliers and improve threat detection. Join businesses like yours in building a baseline of security measures to stay ready for the future of your data security.

Learn how to align AWS security strategies with your enterprise control objectives and discover how Sumo Logic can help your security teams achieve the holistic approach they need to protect your people, processes, data and technology.

To find out more about how Sumo Logic's all-in-one cloud log analytics platform can help you safeguard your business against advanced threats, **Speak to our helpful experts today.**