aws marketplace

Security ebook Series

The value of next-generation SIEM in AWS environments

Improving cloud-specific detection and response strategies through security incident and event management (SIEM)

Complex IT environments and emerging threats demand advanced tools

Enterprises worldwide are struggling to keep pace with fighting emerging threats and managing complex IT environments that handle massive volumes of data. They also face the ongoing difficulty of acquiring and retaining the advanced operational skills these challenges require. A 2022 SANS Institute survey identified this skills gap as the number one concern of today's security operations centers (SOCs).

Many enterprises are responding by moving their SOCs to the cloud. But cloud-based SOCs require cloud-based tools with advanced capabilities that extend far beyond what traditional solutions can offer. Enterprises are looking to next-generation security incident and event management (SIEM) to deliver enhanced visibility, greater automation and orchestration of security functions, and improved operational efficiency.

In this ebook from SANS and AWS, you'll learn how next-generation SIEM tools can heighten your SOC's operational efficiency and dramatically improve protection for complex computing environments.

The challenges facing today’s SOC

Enterprise security teams must keep pace with an increasing volume of cyberattacks. They often find that many of the traditional security tools they’ve relied on now require more modern technologies to aggregate, process, protect, and share data. Compounding this is a lack of critical training in security operations, meaning that busy, short-staffed teams must do more with less.

What is next-generation SIEM?

Where the traditional SIEM model addresses on-premises applications and systems—with less emphasis on cloud-specific events and unauthorized scenarios—next-generation SIEM tools address the demands of complex, highly distributed IT environments. They include capabilities such as automation, deep integration with cloud-native services, and powerful visualization and data-analysis tools.

Core capabilities SOCs should look for in a next-generation SIEM solution

To help SOC teams quickly identify and investigate events in AWS and better manage AWS deployments, their AWS-focused SIEM platforms should feature new, cloud-centric capabilities including automation, deep integration with AWS-native services, and powerful visualization and data-analysis tools.

Here are core capabilities that SOCs should have in next-generation SIEM solutions:

Advanced expertise in dealing with cloud-specific events

The cloud is changing both the nature and the scale of security threats, and SIEM needs to be able to adapt in response.

Threat intelligence and anomalous signal detection

Next-generation tools can help to address the need for advanced skills—skills that enterprises often don’t have in-house.

Deep integration with third-party providers’ application programming interfaces (APIs)

A cloud-native SIEM platform enables the simple, rapid implementation of a broad range of highly specialized tools.

Analytics and processing at massive scale

To detect needle-in-a-haystack threats, SOCs must be able to handle massive amounts of data across a broad array of applications, services, and huge workloads.

FINRA protects American investors with Splunk Cloud and AWS

As many as 100 billion securities market financial transactions take place every day in the US, involving billions of investors' dollars. **The Financial Industry Regulatory Authority (FINRA)** is a Congressionally authorized not-for-profit organization that regulates one critical part of the securities industry—brokerage firms doing business with the public in the US.

The Challenge

Market integrity is a key factor in fostering vibrant capital markets. FINRA needed a centralized solution to process and analyze massive volumes of data while protecting it from unexpected threats. The organization had a SIEM solution in place, but despite high costs, it provided limited functionality.

The Solution

Splunk Cloud gives FINRA a way to capture, index, and correlate big data from all of its desired sources in real time, and to customize queries through flexible dashboards. Leveraging mature data-collection agents within Splunk enabled FINFA to start consuming data within days instead of months. AWS integrations help FINRA reliably, securely, quickly, and cost-efficiently move AWS logs into the Splunk solution for analysis, which breaks down the silos between developers, network staff, and security specialists silos.

The Results

Today, FINRA relies on Splunk to ingest data—on almost every US stock and options market—from 170 applications and AWS services. The pay-per-use cloud model enables FINRA to run code without provisioning or managing servers, paying only for the compute time consumed. FINRA gained cost and operational efficiencies, as well as an unparalleled ability to protect investors from fraud.

> "When we looked at what other companies were providing, they were playing catch-up to the capabilities that were already in Splunk. We didn't want to play that game."
>
> — Gary Mikula, Senior Director, Cyber and Information Security, FINRA

Splunk provides the leading software platform for real-time Operational Intelligence. Splunk software and cloud services enable organizations to search, monitor, analyze, and visualize machine-generated big data coming from websites, applications, servers, networks, sensors, and mobile devices. Enterprises, government agencies, universities, and service providers in over 90 countries use Splunk software to deepen business and customer understanding, mitigate cybersecurity risk, prevent fraud, improve service performance, and reduce cost.
Learn more

Medidata finds the cure for security analytics with Sumo Logic

Medidata helps clinical trials and studies run better. Today, more than two million patients participate in about 9,000 studies that depend on Medidata's cloud platform, the Medidata Clinical Cloud. The Medidata Clinical Cloud improves productivity and quality in the clinical testing process of new medical treatments.

The Challenge

Medidata generates nearly two terabytes of log data every month. In addition to securing its on-premises and cloud systems, Medidata needed to improve its level of transparency into security events on its systems, help substantiate its high level of security diligence to clients, prevent data leakage, and be able to analyze attacks in near real time.

The Solution

Sumo Logic delivers real-time, continuous intelligence across Medidata's entire infrastructure and application stack and helps it to automatically generate audit-ready compliance reports from both its on-premises and AWS event logs. Sumo Logic also simplifies Medidata's cloud and on-premises audits and strengthens its security posture with a composite view across the network, server, and application stack. Additionally, predictive analytics powered by machine-learning algorithms uncover unknown security events without relying on rules or predefined schemas to ward off impending threats.

The Results

With Sumo Logic, Medidata got its SIEM up and running in minutes, and the company can now more easily substantiate its security efforts. It gained visibility into events on AWS as well as the ability to identify any potential suspicious traffic that may arise. Also, that same reporting helps Medidata comply with CFR Part 11 from the Food and Drug Administration.

> "Our move to Sumo Logic has been a great success in every aspect. We can see what we need to see in both our physical datacenter and within Amazon Web Services. Sumo Logic helps us to substantiate what our customers need to know about our security program; there are potentially a lot of attacks and activities that are unknown to us and Sumo Logic helps us to now see that activity."
>
> — Glenn Watt, CISO,
> Medidata

Sumo Logic is a secure, cloud-native, data analytics service, delivering real-time, continuous intelligence across an organization's entire infrastructure and application stack. More than 700 customers around the globe experience real-time operational, business, and customer insights using Sumo Logic for their DevOps, IT ops, and security and compliance use cases. With Sumo Logic, customers gain a service model advantage to accelerate their shift to continuous innovation, increasing competitive advantage, business value, and growth. Learn more

Has your SOC fully evolved to better handle modern cloud deployments and cyberthreats?

Monitoring and managing a SIEM takes thought, planning, and a lot of attention to detail—three resources a SOC doesn't always have in-house: In 2022, monitoring/managing SIEM platforms was the main IT security function outsourced to a managed security service provider (MSSP).[1]

As the need for more capable security event monitoring and triage solutions rises, so do the options available to SOC teams to improve their security operations efficiency.

As showcased with FINRA and Medidata, a next-generation SIEM model can help organizations improve their security operations efficiency for AWS assets and infrastructure. Find many more examples of how AWS Marketplace sellers can help you overcome your biggest security challenges.

[1] "Main IT Security Functions Outsourced to a MSSP Worldwide 2022," Statista, Aug. 3, 2022.

AWS Marketplace

Simplify the procurement, provisioning, and governance of third-party software, services, and data.

Why use AWS Marketplace?

AWS Marketplace is a curated digital catalog that simplifies software discovery, procurement, provisioning, and management. With AWS Marketplace, customers can also utilize features that speed up production evaluation, improve governance and cost transparency, and enhance control over software spend. AWS Marketplace offers third-party solutions across software, data, and machine-learning tools that enable builders to find, test, and deploy solutions to expedite innovation.

Explore and deploy solutions

IT decision-makers (ITDMs) cut their time in half using AWS Marketplace compared to other sources.

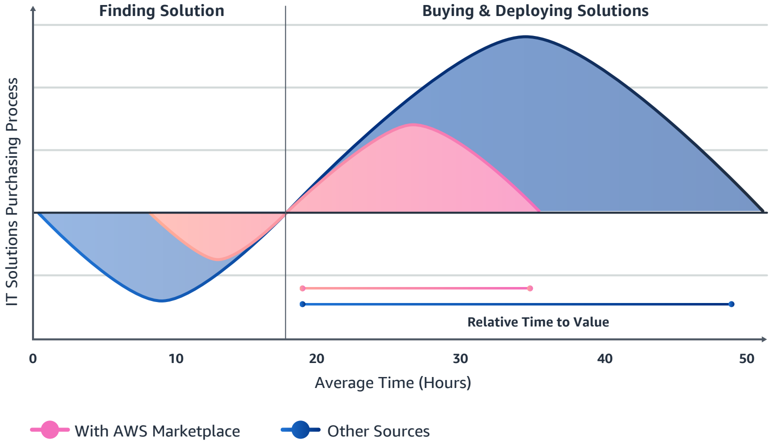
AWS Marketplace benefits

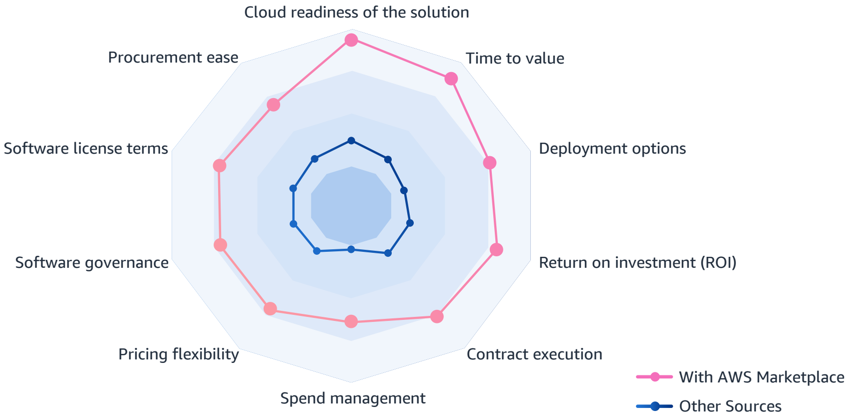
Customers can launch preconfigured solutions in just a few clicks in both Amazon Machine Image (AMI) formats and SaaS subscriptions, with entitlement options such as hourly, monthly, annual, and multi-year contracts.

AWS Marketplace is supported by a global team of solutions architects, product specialists, and other experts to help IT teams connect with the tools and resources they need to streamline migration journeys to AWS.

Make more-satisfying purchases

ITDMs feel 2.4 times better about purchasing using AWS Marketplace compared to other sources.





* Amazon Web Services (AWS) Marketplace surveyed 500 ITDMs and influencers across the US to understand software usage, purchasing, consumption models, and compared savings.

Getting Started

AWS Marketplace Security Solutions

Helping buyers, sellers, and consulting partners reach favorable agreements, cut down negation time, and reduce sales cycles by 49%

Innovative AWS Marketplace features enable you to reduce software purchasing inefficiencies with cloud-based procurement. One way is through AWS Marketplace seller private offers, which make you eligible to receive product pricing and terms that are not publicly available from sellers in a centralized portal.

To help govern purchasing, you can establish Private Marketplaces to control which products users in your AWS account can purchase from AWS Marketplace. This can help ensure that products purchased comply with your organization's internal policies.

You can also purchase software solutions in AWS Marketplace directly from Consulting Partners who have industry expertise and can offer specialized support. Many Consulting Partners offer both software and professional services on AWS Marketplace to provide you with comprehensive solutions via a fast and friction-free purchasing experience.

> "AWS Marketplace makes it easier to do business with our vendors in everything from simplifying our licensing to streamlining billing to accelerating procurements. This has alleviated a major operations burden and given us time back to focus on more innovative tasks."
>
> — Stephen Pearson,
> Head of IT Vendor
> Management,
> Agero

AWS Marketplace

Discover security products to meet your business needs

splunk>

Product overview | Product tour

sumo logic

Product overview | Data sheet

logz.io

Product overview | Video

DEVO

Product overview | Data sheet

HUNTERS

Product overview | Video

New SIEM, same SOC. Just happier.

Download whitepaper

Find, buy, deploy, and govern software solutions on AWS Marketplace.

Visit AWS Marketplace

Get connected with a solutions architect that can share best practices and help solve unique challenges.

Get in touch with an AWS Expert