eBook

Modernizing security operations with Cloud SIEM powered by AWS

Table of contents

The importance of modernizing security in the cloud

The staggering number of organizations transitioning to the cloud indicates a demonstrative shift in the future norms and challenges of IT security. The flexibility and scalability of the cloud has presented enterprise and small businesses with unprecedented opportunities for transformative growth, enhanced productivity, and augmented capacity for seemingly boundless innovation.

As organizations transition to the cloud at an increasingly rapid pace, their security needs also change. Many companies that migrate to the cloud focus on the potential for growth and deprioritize the evolution of their security needs. Others that recognize the importance of modifying security practices often lack the technical knowledge and resources to follow through.

A modernized security practice requires an active, multifaceted approach that helps an organization optimize its cloud experience. This is achieved by enhancing workflow, detecting novel and complex threats, and securing remote work environments. A SIEM is a central security tool that enhances an organization's visibility into their environment.

The right SIEM solution codifies an organization's incident response plan. It also incorporates security best practices and enhances productivity. With its potential to inspire customer confidence, a reliable SIEM solution can also enhance reputation and bolster revenue. Ultimately, the choice to modernize security operations has become a distinguishing factor in an organization's longevity and prosperity in the cloud.

Challenges with securing multi-cloud and hybrid environments

Challenges with securing multi-cloud and hybrid environments

In the pursuit of a fully functioning cloud environment, organizations often underestimate the complexities of maintaining security within a holistic digital transformation. This underestimation often leads to preventable challenges, especially when it comes to securing cloud hybrid and multi-cloud assets.

Cloud security gaps

Cloud security gaps refer to security oversights within an IT infrastructure. Gaps can be present on cloud servers, workloads and throughout the cloud environment. These gaps require targeted security attention that legacy security solutions are not calibrated to address.

Event fatigue

Without real-time insights into the incidents occurring within a cloud environment, multi-tasking IT professionals will lack the visibility they need to prioritize alerts, detect threats or internal malfunctions, and take appropriate actions within a timely manner.

Distributed operations

Outdated security protocols lack the dexterity to support security teams in managing, overseeing, and acting efficiently within an organization’s diverse environments. As remote work continues to become more commonplace, business operations can often be distributed across various countries and IT environments that include a mix of on-premises and multi-cloud assets. Without security to monitor and protect various activities from a single location, results will be inconsistent.

Too many tools

When it comes to reliable and effective security management, less is often more. IT managers who are saddled with a broad range of unintegrated, complex cybersecurity tools may operate inefficiently with a delayed response to pressing security challenges.

Streamline security modernization with Cloud SIEM and SIEM Advanced Powered by AWS

Through Cloud SIEM and Cloud SIEM Advanced, organizations are positioned to securely and responsibly accelerate their digital transformations. The cloud-native design and centralized control platform of both Cloud SIEM solutions are intuitive, collaborative, and user-friendly. As incidents emerge across an organization's cloud, hybrid or on-prem environments, the enhanced visibility of Cloud SIEM solutions facilitates swift and appropriate action. It triages threats by correlating and enriching data from multiple sources, such as AWS GuardDuty and Security Hub as well as 3rd party tools, and provides actionable and reliable insights to the SOC operator. By consolidating tools through its centralized platform Cloud SIEM solutions eradicate complexity and drive action forward, establishing a dependable and efficient security protocol.

Modernize your security with Sumo Logic Cloud SIEM powered by AWS

Modernizing security has become a best practice for every organization in the cloud and a fundamental step in a successful transition from on-premises operations. As a proponent of a shared responsibility security model, AWS partners with cybersecurity solutions that streamline its built-in security features.

Powered by AWS, the Sumo Logic Cloud SIEM solutions offer a range of capabilities that enable AWS cloud users to continually enhance and modify their security to adapt to their burgeoning cloud environments.

Unified security visibility and analytics across multi-cloud using native and 3rd party data sources

Integrated threat intel which accelerates threat detection and reduces time to detect and investigate

Quick time-to-value with out-of-box integration with all key cloud (AWS services, other cloud services), on-premises and many more SaaS services

Sumo Logic Cloud SIEM Solutions powered by AWS

Cloud SIEM security is available through two solutions to deliver flexibility and specificity to meet the needs of all organizations—those that operate with and without a Security Operations Center (SOC).

Cloud SIEM for organizations without a SOC
With limited visibility into the malicious activities occurring within their environments, security teams with a SOC consistently struggle to maintain their security posture. The Cloud SIEM solution supports organizations without SOCs by accelerating threat detection and response timelines. It helps customers make the best use of cloud-native capabilities like CloudTrail and GuardDuty on AWS, leading to improved decision making.

Cloud SIEM Advanced for organizations with a SOC
Members of a SOC team are often overrun by excessive alerts and lack the resources to effectively investigate and prioritize them. Security teams at these organizations also lack the visibility to get ahead of their expanding security needs in multi-cloud or hybrid IT environments.

The Cloud SIEM Advanced solution addresses these common security concerns for organizations with a SOC. Through its cloud-native design and calibration for multi-cloud, on-prem and hybrid challenges, Cloud SIEM Advanced automates instance responses for streamlined workflows. It provides context for instances and organizes them to indicate priority.

Both Cloud SIEM solutions also streamline regulation compliance on AWS and ensure that permissions are centrally monitored, controlled, and allocated by the appointed security team. As security challenges are addressed, workflows can continue securely without interruption.

Cloud SIEM solutions help enterprise and small business security teams easily monitor and troubleshoot logs and metrics. Through the multi-cloud and hybrid cloud coverage on Cloud SIEM Advanced, the process of moving data to the cloud is stable and secure. Both solutions uncover threat indicators in the earliest stages, enacting preventative solutions that streamline the digital transformation.

medidata

Experience (Summarized Case Study)

The Medidata Clinical Cloud is a web-based metadata solution that helps to streamline clinical trial and study reporting for nearly two million participating patients in about 9,000 studies.

The platform leveraged Cloud SIEM Advanced on AWS to secure its on-premises and cloud systems and improve its level of visibility into security events.

Challenge
The organization needed a reliable way to identify and mitigate potential attacks across its hybrid environment, which included on-premises systems and multiple AWS accounts.

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. By enriching AWS GuardDuty findings with on-premises data source information and additional third-party threat feeds, Medidata can now proactively resolve security incidents that would have otherwise gone undetected.

> "Sumo Logic has helped us effectively manage our hybrid infrastructure and accelerate innovation. Now we can collect logs from both our on-prem data center as well as our cloud applications, make sense of it and take action in real-time, and that's really the golden nugget."
>
> **—Glenn Watt, CISO, Medidata**

aws marketplace

Jumpstart Your Modernization Journey Today

Embark on your security modernization journey.

Learn more or get started with Sumo Logic Cloud SIEM powered by AWS today!