PRIMUS PARTNERS®

Quote by Devroop Dhar, Co-Founder and India CEO, Primus Partners

Published in CSO
Mar 11, 2026, | 09:01 PM IST

AWS expands Security Hub for multicloud security operations

Authored by Nidhi Singh

Read on: https://www.csoonline.com/article/4143683/aws-expands-security-hub-for-multicloud-security-operations.html

Article Content:

The update introduces a unified operations layer designed to aggregate risk signals across cloud environments and help CISOs manage threats through a single security platform.

Amazon Web Services is expanding AWS Security Hub to function as a centralized security operations platform capable of aggregating risk signals across multicloud environments.

With the updated Security Hub, the company said it will introduce a unified operations layer that provides security teams with near real-time risk analytics, automated analysis, and prioritized insights.

As enterprise workloads have spread across multiple cloud providers, the expansion of Security Hub aims to address the growing complexity faced by CISOs and help them focus on managing risks rather than tools, the company said in a blog post.

AWS Security Hub reimagined

As security teams struggle to manage multiple tools, the expanded Security Hub introduces a common data layer designed to unify security signals from across enterprise workloads. It will then offer a single view of risk to security teams instead of a fragmented collection of consoles.

Security teams will also be able to manage their cloud security posture using Security Hub CSPM checks, which provide posture visibility and extend vulnerability management through expanded

Amazon Inspector capabilities, including virtual machine scanning, container image scanning, and serverless workload scanning, the company said.

Security Hub originally played a narrower role. But in December last year, AWS pulled together signals from its security services into a single interface to automatically analyze threats, vulnerabilities, misconfigurations, and sensitive data exposures. This list of services includes Amazon GuardDuty, Inspector, Security Hub Cloud Security Posture Management, and Amazon Macie.

The latest multicloud expansion will be built on that foundation, as well as AWS's earlier launch of AWS Security Hub Extended, which allows enterprises to deploy and manage third-party security tools directly through Security Hub at pre-negotiated pay-as-you-go pricing without long-term commitments.

The curated portfolio includes vendors such as CrowdStrike, Okta, Proofpoint, SailPoint, Splunk, and Zscaler, enabling organizations to extend security visibility beyond AWS environments.

Cross-cloud security monitoring

While AWS has not provided technical details on how it will identify vulnerabilities outside its native environment, Sanchit Vir Gogia, chief analyst at Greyhound Research, said multicloud visibility typically works by collecting signals from multiple security systems and translating them into a consistent format so they can be analysed together.

A key enabler of this approach is the Open Cybersecurity Schema Framework, which defines a common structure for representing security events and vulnerabilities.

"When it comes to monitoring external environments beyond AWS, Security Hub is likely to rely on integrations and standardized telemetry. Most multicloud security solutions retrieve data through APIs from other cloud vendors, security platforms, and enterprise monitoring tools," explained Devroop Dhar, co-founder and CEO at Primus Partners.

"For example, Security Hub would ingest data from vulnerability management platforms, endpoint security tools, identity systems, and configuration management solutions. AWS has a robust partner ecosystem, so integration with existing security technologies will likely be an important factor," Dhar added.

Gogia noted that Security Hub can also analyse assets that are reachable from the internet and add context about exposure pathways. This technique works across infrastructure boundaries because internet exposure can be observed externally, regardless of where the infrastructure is hosted.

"If a workload is visible externally, the risk exists regardless of which cloud hosts it," he said.

Operational security impact

For CSOs and security leaders, the expansion of AWS Security Hub reflects a broader shift in enterprise security operations. Aggregating security signals into a unified solution could help security teams correlate threats, prioritize risks, and streamline incident response across distributed environments.

"As enterprises use multiple clouds and hybrid environments for their workloads, there is a constant toggle between various dashboards and logs. Having a central view of all risks across all clouds is highly desirable because it helps reduce operational costs. The idea is not only to have visibility but

also to understand what vulnerabilities represent the highest level of risk for the organization," added Dhar.

Gogia noted that managing multiple cloud environments also contributes to alert fatigue, which has become one of the defining characteristics of modern security operations centres. Teams frequently process enormous volumes of alerts while having limited resources to investigate them thoroughly. Solutions that combine telemetry from multiple sources into a single operational view can help reduce that friction.

However, while the idea of centralization is attractive, there are practical considerations as well.

Visibility is only as strong as the integrations behind it. If some workloads or tools are not integrated properly, it can create a false sense of completeness.

When security teams rely on a single interface to interpret telemetry and coordinate response, the availability of that interface also becomes critical.

"Organizations need to ensure they can still access telemetry and respond to incidents even if their primary console becomes unavailable. Maintaining alternate access paths and independent telemetry pipelines becomes an essential part of sound security architecture," Gogia added.

Dhar noted that integrating dozens of tools into a single solution is not always straightforward. CISOs will also weigh the risk of vendor lock-in, since security workflows that become tightly tied to one vendor's platform can be difficult to move away from later.

The move also reflects a broader industry trend toward consolidated security solutions that bring multiple capabilities under a single operational layer. As enterprise environments grow more complex, vendors are increasingly combining threat detection, posture management, and vulnerability analysis into unified security architectures.

"The industry has seen multicloud capabilities from pure-play security vendors for years. Microsoft Defender for Cloud and Google Cloud Security Command Center have also extended their reach beyond their native cloud environments," said Amit Jaju, global partner/senior managing director – India at Ankura Consulting.