Democratizing Security Data with Amazon Security Lake and Industry Leaders for Improved Protection

Table of contents

Challenges in analyzing enterprise security data

It is estimated that in the past four years, the amount of security data generated by organizations has tripled.[1] Some of these data sources include logs from on-premises infrastructure, firewalls, and endpoint security solutions—as well as multiple cloud services and accounts. And they are in different formats, which is complicating the process of using the data to prevent security incidents and threats.

As organizations strive to safeguard their digital assets, the challenges of collecting, organizing, and utilizing security data have become apparent. Security teams grapple with the daunting task of identifying and consolidating relevant security data from a multitude of sources. Proprietary formats can render security log data inaccessible without time-consuming conversions. Even when transformed, the resulting data may still be incompatible with security and analytics tools, due to the absence of a standardized schema. This lack of cohesion impedes seamless data ingestion and poses a significant obstacle to comprehensive security analysis. The ongoing effort required to meet stringent security and compliance standards adds yet another layer of complexity, driving up operational costs.

[1]ESG Master Survey Results: Cloud-scale Security Analytics Survey.

Navigating security data analytics

The following challenges hamper the process and accuracy of critical data security analytics:

- **Inconsistent and incomplete data:** Logs and alerts in varying formats are in data silos that are difficult to locate.
- **Complex data preparation:** Security teams spend more time reformatting, enriching, and normalizing data than analyzing it.
- **Inefficient use of data across use cases:** Specialized security tools can result in data duplication and reprocessing for each use case.
- **Lack of direct control over processed data:** Certain tools store processed data in their own system and proprietary schema, which affects your ability to use it.
- **Log storage constraints:** Cost limitations and security policies affect which logs you keep.

Centralizing data for analytics and detection and response

To identify potential security threats and vulnerabilities, you could centralize all your logs in a data lake. But even then, defining and implementing security domain-specific aspects can be a struggle. For example, data normalization requires analyzing each log source's structure and fields, defining schemas and mappings, and pulling in threat intelligence. However, with a security lake, you can tackle normalization and other challenges.

Let's explore how Amazon Security Lake and AWS Partners help you address these enterprise security data challenges for more accurate analysis and effective protection.

41%

of IT and security managers perceive security data analytics technologies as very important to protecting enterprise data.

Source: **BARC, Big Data and Information Security Analytics**

52%

of organizations keep security data online for longer periods of time than in the past.

28%

want to retain security data online but can't for cost or operational reasons.

Source: **CSO, Bracing for the security data explosion**

Diving into Amazon Security Lake

Amazon Security Lake automatically centralizes security data from AWS environments, SaaS providers, on premises, and cloud sources into a purpose-built data lake stored in your account. Built on top of Amazon Simple Storage Service (Amazon S3), it can:

- **Normalize AWS security logs and event data** in a common structure so that compatible security solutions can use it.
- **Collect, retain, and optimize data** to limit its duplication and multistep data movement and translation.
- **Centralize data visibility** with automatic aggregation that delivers enterprise-wide insights in minutes.
- **Analyze security data** using your preferred analytics tools while retaining complete control and ownership of that data.

Amazon Security Lake has features that specifically address the most common security challenges.

Variety of supported log and event sources

Amazon Security Lake automatically collects logs and security findings from more than 100 sources including AWS services and third-party security findings. AWS Partners can send data directly to Amazon Security Lake in the Open Cybersecurity Schema Framework (OCSF) format.

Data transformation

With OCSF support, Amazon Security Lake partitions and converts incoming log data to a storage and query-efficient format. As a result, you can use the data broadly and immediately for security analytics without post-processing. Amazon Security Lake supports integrations with AWS Partners to address a variety of security use cases such as threat detection, investigation, and incident response.

Customizable access management and availability

Amazon Security Lake enables you to customize the configuration of access to your data lake for your security and analytics tools. This includes granting access to datasets from specified sources, such as AWS CloudTrail. This customization and the other Amazon Security Lake capabilities described in this section deliver numerous advantages. Let's explore them in more detail.

What is OCSF?

- Developed jointly by Splunk and AWS, which built on the ICD Schema developed at Symantec—now part of Broadcom Software—OCSF is an open standard anyone can adopt to simplify security data normalization.
- OCSF delivers a simplified and vendor-agnostic taxonomy for security data that can be adopted in any environment, application, or solution provider.
- Over 145 participating organizations including AWS, Splunk, Broadcom, Cloudflare, CrowdStrike, DTEX, IBM Security, Palo Alto Networks, Rapid7, Salesforce, Securonix, Sumo Logic, Tanium, Trellix, Trend Micro, and Zscaler.

Why OCSF?

- Speed up data ingestion and analysis without the time-consuming, upfront normalization tasks.
- Combine data from OCSF-compliant sources to break down data silos that slow security teams.

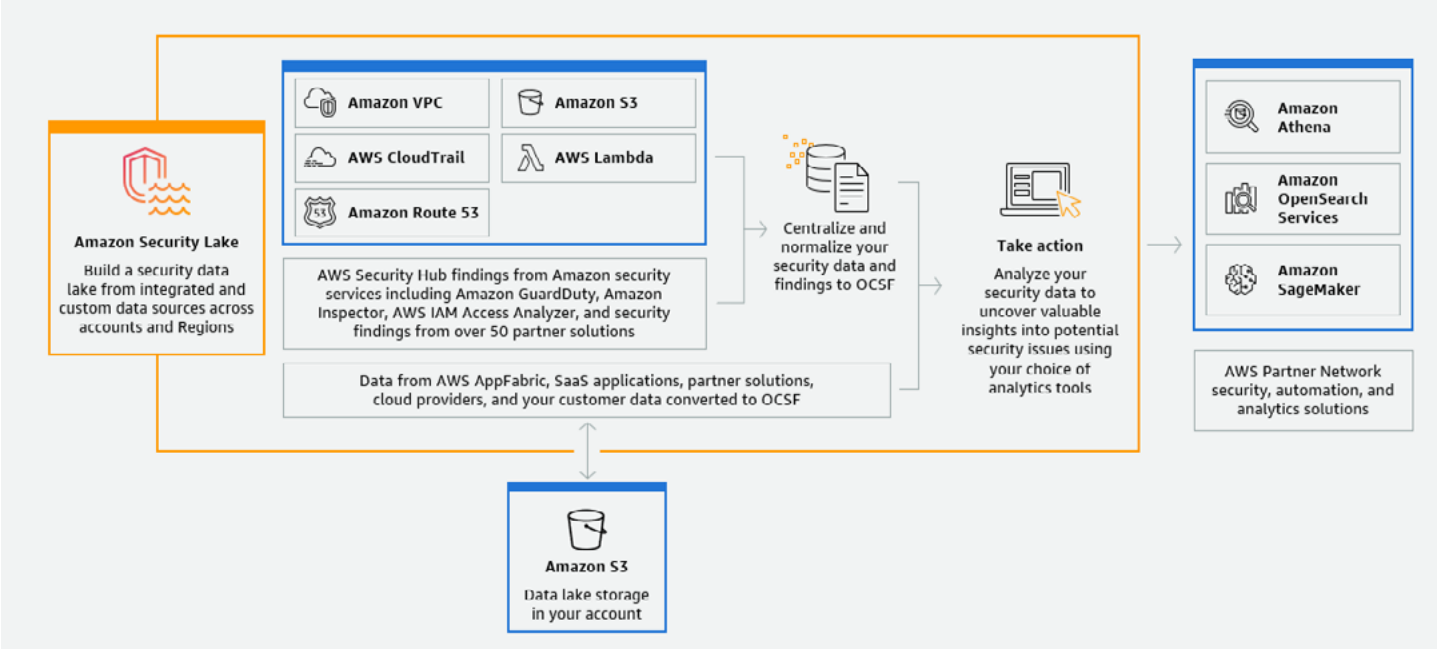
Learn more from Splunk, which co-founded OCSF with AWS

The benefits of setting up a security lake

With its open-source schema and the fact that you own the data, Amazon Security Lake offers numerous advantages.

Orchestration is the key

Amazon Security Lake integrates with AWS Organization, so you can gather logs across hundreds of accounts in a few clicks. It acts as an orchestrator based on your preferences, including the Amazon S3 tiering you use.



When Amazon Security Lake receives a notification of a new Amazon S3 object, it sets up a cross-account role for direct access to Amazon S3 and manages infrastructure and permissions. You then query it in place using Amazon Athena and get support with AWS Lake Formation.

You control your data

Amazon Security Lake runs in an Amazon VPC on top of Amazon S3, so that means you control with whom you share it. You can also do analytics without moving data around, or you can send the logs to the analytics tool of your choice. You govern the log data, and you don't have to send the same data to multiple vendors. AWS subscription partners simply query them without ingesting everything. You own the data, so you know where it is and who has access to it.

Gather all the logs you need

Can you analyze all the logs you generate, or have you been having to make some hard choices? The output of some logging tools can fall in the terabyte range. For example, VPC Flow Logs can produce hundreds of gigabytes of logs—if not more—so some organizations choose the logs they think are most useful. With Amazon Security Lake, all the logs reside in an Amazon S3 bucket, so you can analyze data without wondering what you might be missing.

Govern your security data

Owning your security data preserves privacy, prevents data duplication, and reduces cost because you don't have to provide multiple vendors with the same data. Customizable retention settings help you store data for a specific period, which may help you address regulatory mandates. You can also turn Amazon Security Lake off and still retain ownership of the underlying Amazon S3 buckets.

Another major advantage of Amazon Security Lake is the number of use cases it addresses—and the AWS Partners that support it.

Amazon Security Lake Partners

Third-party Amazon Security Lake integrations include solutions from source and subscriber partners.

- Source partners can send logs and security events to your security data lake in the OCSF format.
- Subscriber partners help you analyze logs in the OCSF format and address a variety of security use cases such as threat detection, investigation, and incident response.
- Service partners can help you help you build and use Amazon Security Lake.

Get more details about Amazon Security

A reservoir of valuable use cases

Your organization can use Amazon Security Lake a number of ways. Let's explore some examples that showcase its value.

Analyze multiple years of security data quickly

Centralize petabytes of data from cloud, on-premises, and AWS source partners in your Amazon S3 buckets, and use your preferred AWS and AWS subscriber partner tools for security analytics. Amazon Security Lake integrates with security information and event management (SIEM) solutions, extended detection and response (XDR) tools, Amazon Athena, and Amazon OpenSearch Service to quickly query and analyze petabytes of data. AWS subscriber partners can help you analyze logs in the OCSF format.

Simplify your compliance monitoring and reporting

Make it easier to monitor and report on compliance across multiple log sources, AWS Regions, and accounts. With Amazon Security Lake, you can centralize security data from AWS and AWS source partners into one or more rollup Regions to simplify your compliance and reporting obligations.

Facilitate your security investigations with elevated visibility

Give your security teams the broader visibility needed to initiate thorough security investigations and rapid response to security incidents. Because the security-related logs and findings generated by AWS services and AWS source partners are centralized and in the same format, your security operations teams can more easily investigate issues.

Democratize security data management across hybrid environments

Optimize data accessibility across your organization and facilitate a more comprehensive approach to security operations. Amazon Security Lake can store security-related logs and data from various sources, including cloud, multi-cloud, and on-premises systems, making it simpler to collect and analyze security data in the OCSF format. Your security teams can query that data with AWS and AWS subscriber partner analytics tools to understand and respond to threats.

Amazon Security Lake not only makes these use cases a reality, but it has also helped AWS customers take a different approach to gathering security data while removing the heavy lifting of data retention and ETL. Some are already sharing their successes with gathering and controlling the data.

Crystal-clear data visibility delivers improved security

Salesforce and Interpublic Group (IPG) are two AWS customers who have adopted Amazon Security Lake and are enjoying its benefits.

Solving Salesforce log collection and inspection at scale

The Salesforce Detection and Response (DnR) team collects and inspects petabytes of security logs across dozens of organizations, some with thousands of accounts. Salesforce is a long-time AWS customer and partner, so the team decided to explore Amazon Security Lake to see if it could help solve the challenges associated with log collection and inspection.

Today, Amazon Security Lake is helping Salesforce address the heavy lifting involved with large-scale log collection, transformation, aggregation, search, and management. Moreover, Amazon Security Lake log aggregation and regional rollup fully align with DnR's own global, decentralized, and hybrid data lake infrastructure.

> "We anticipate that Amazon Security Lake will help offload 30%-50% of the traffic of our own data pipeline, significantly reduce our log onboarding time, and increase log coverage."
>
> **Lei Ye**, Software Engineering Architect, DnR, Salesforce
> **Ajith Jayamohan**, Vice President of DnR Engineering, Salesforce

Read the full Salesforce story

Providing IPG with a holistic view of its security posture

Global marketing solutions provider IPG was on the lookout for bigger and better approaches to using security data to handle threat detection and response. IPG chose Amazon Security Lake because it did all the heavy lifting for them, and is vendor agnostic. As a result, its logs and data aren't locked into another vendor's solution—and it can integrate with tools from AWS source and subscriber partners.

After adopting Amazon Security Lake, IPG was impressed with the common normalization format provided by OCSF. Previously, its team of data scientists had to look at all the different log data, translate and transform it, and reconcile aspects such as IP addresses. It was easy to miss things. As a result of using Amazon Security Data Lake, IPG brought in logs it had not been able to use previously. And this allowed it to achieve a vastly improved and holistic understanding of its security posture across hybrid environments.

Learn more about IPG and Amazon Security Lake in this Re:Inforce session

Read other customer success stories to see how Amazon Security Lake has improved their security

Take swift action to secure data

Your organization must be able to quickly detect and respond to security risks. Greater visibility into security activity across your entire organization can:

- Proactively identify potential threats and vulnerabilities.
- Assess security alerts so that you can respond accordingly.
- Help prevent future security events.

But the data you need for analysis is often spread across multiple sources and stored in a variety of formats, which impacts visibility and access.

In just a few steps with Amazon Security Lake, you can centralize, aggregate, normalize, and store data so you can respond to security events faster. And you can use your preferred tools from AWS or from Amazon Security Lake source and subscriber partners. All while retaining complete control of your data at all times.

Ready to learn more or get started?

Check out the Amazon Security Lake web page ›

Start a free 15-day trial today ›

Get more information about Amazon Security Lake Partners ›