sysdig | aws

Innovate at Scale with Runtime Insights and a Security Data Lake

Sysdig Secure and Amazon Security Lake provide a modern foundation for securing your cloud estate

Table of Contents

Modern Cloud Environments Require Streamlined Security at Scale

As the scale of your cloud-native applications and infrastructure grows, your security teams need effective ways to manage and accelerate security across multi-cloud and hybrid environments. Containers, Kubernetes, and cloud services are driving digital transformation, but it can be challenging to ensure robust security that keeps pace with the speed of building on Amazon Web Services (AWS).

Security teams need solutions that can provide situational clarity, detect threats in real time, and take action so they can better manage risk and prevent unauthorized access.

Together, Sysdig Secure and Amazon Security Lake provide a modern foundation for securing your cloud estate.

Sysdig Secure integrates with Amazon Security Lake, creating an efficient and streamlined approach to security and compliance at scale.

Read on to learn how these two solutions help you gain control of your security data for more accurate analysis and effective protection.

Top Security Challenges When Building in the Cloud

Security data is critical to protecting enterprise data, applications, workloads, and environments. But the following challenges hamper process and accuracy.

Visibility gaps in dynamic environments Developers are configuring infrastructure at will and deploying containerized microservices with the click of a button, leading to large volumes of cloud assets to track and IAM permissions to manage.

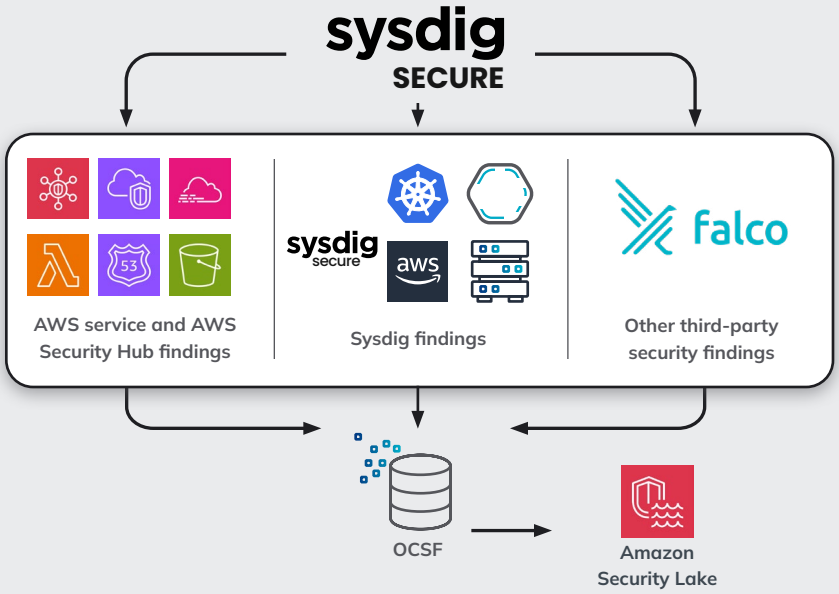
Growing volumes of security data As cloud estates continue to expand, security teams are spending more time managing data than analyzing it. It can be challenging to take action on high-priority threats in a sea of alerts.

Siloed solutions and inconsistent data Often times disparate security tools don't communicate with each other and share context. Logs and alerts may come in varying formats and reside in data silos that are difficult to locate.

Combine Real-Time Detection with a Purpose-Built Data Lake

When you bring together Sysdig's powerful runtime security capabilities with a scalable and cost-effective data lake solution, you gain a more complete view of security data across your entire organization. Sysdig integrates with Amazon Security Lake, enabling you to store enriched multi-platform cloud security events on AWS where you can use your preferred analytics tools to analyze your security data.

Amazon Security Lake automatically collects logs and security findings and aligns them in the same format using Open Cybersecurity Schema Framework (OCSF). 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.



Sysdig's CNAPP delivers runtime protection
Sysdig Secure is a Cloud-Native Application Protection Platform (CNAPP) powered by runtime insights that allows cloud and security teams to detect and respond to threats in real time.

Amazon Security Lake centralizes security data
Amazon Security Lake is a purpose-built service that centralizes security data from AWS environments, SaaS providers, and on-premises sources in a data lake stored in your AWS account.

Built On an Open Source Foundation

Sysdig is the creator of Falco, the open-source solution for cloud threat detection. Because it's open source, it helps drive standardization and accelerate innovation with community contributions.

OCSF is also an open-source project, providing a simplified and vendor-agnostic taxonomy for security data so it can be adopted in any environment, application, or solution provider.

Secure Your Cloud End to End

Sysdig Secure leverages real-time behavioral insights and threat intelligence to continuously monitor your infrastructure and applications for a unified and proactive defense against evolving threats. With the power of runtime intelligence, you can identify threats across your cloud environments, including Amazon Elastic Kubernetes Service (Amazon EKS), Amazon Elastic Container Service (Amazon ECS), and AWS Fargate, and gain the insights you need to immediately respond.

Automatically capture and store security events and indicators of suspicious activity in Amazon Security Lake. Sysdig findings are also made available, along with data from other native AWS services such as AWS CloudTrail, AWS Security Hub, and Amazon Inspector. These services integrate with Amazon Security Lake, so you can easily consolidate security findings from multiple sources.

Tap into Amazon Security Lake and real-time intelligence from Sysdig Secure to secure your AWS environments—from code to response.

CODE	BUILD	RUN		RESPOND
Infrastructure as code validation	Vulnerability management	Configuration and permission management	Threat detection	Incident response
Block risky configs Auto-remediate at the source	Scan in CI/CD and registries Block risky images Prioritize vulns using runtime context	Detect cloud misconfigurations Enforce least privilege access Use OPA to apply consistent policies	Use ML and Falco for multi-layered detection (ex. threats, drift, cryptojacking, etc.) Implement K8s native microsegmentation	Capture detailed record for forensics Remediate config issues Block malicious activity

A Reservoir of Valuable Use Cases

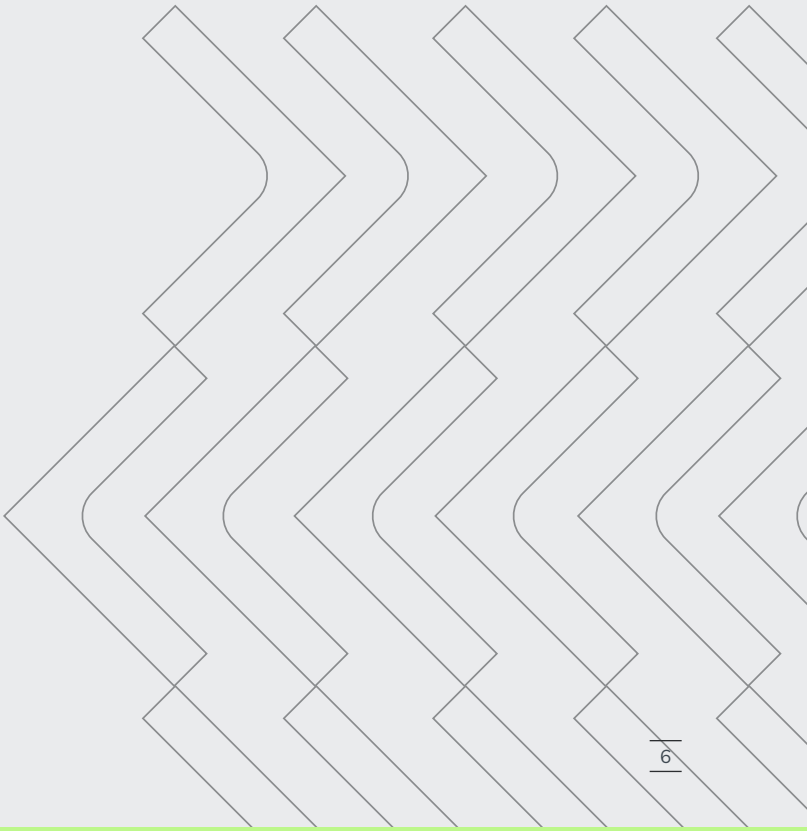
Amazon Security Lake supports numerous use cases for using security insights from Sysdig. Here are the top three.

Streamline security investigations: Investigate threats with Sysdig or use Amazon Security Lake with other preferred analytics tools to analyze your security data and uncover insights into potential security issues. By having security-related logs and findings in a centralized location and in the same format, your security teams have broader visibility to initiate thorough investigations and rapid responses.

Maximize security oversight: Runtime insights from Sysdig and data management at scale with Amazon Security Lake provide you with a more comprehensive understanding of risk across your business. Amazon Security Lake centralizes petabytes of data from Sysdig, AWS, third-party tools, and on-premises solutions. It also integrates

with security information and event management (SIEM) and extended detection and response (XDR) tools, as well as popular data analytics services like Amazon Athena and Amazon OpenSearch Service, to quickly query and analyze large volumes of data.

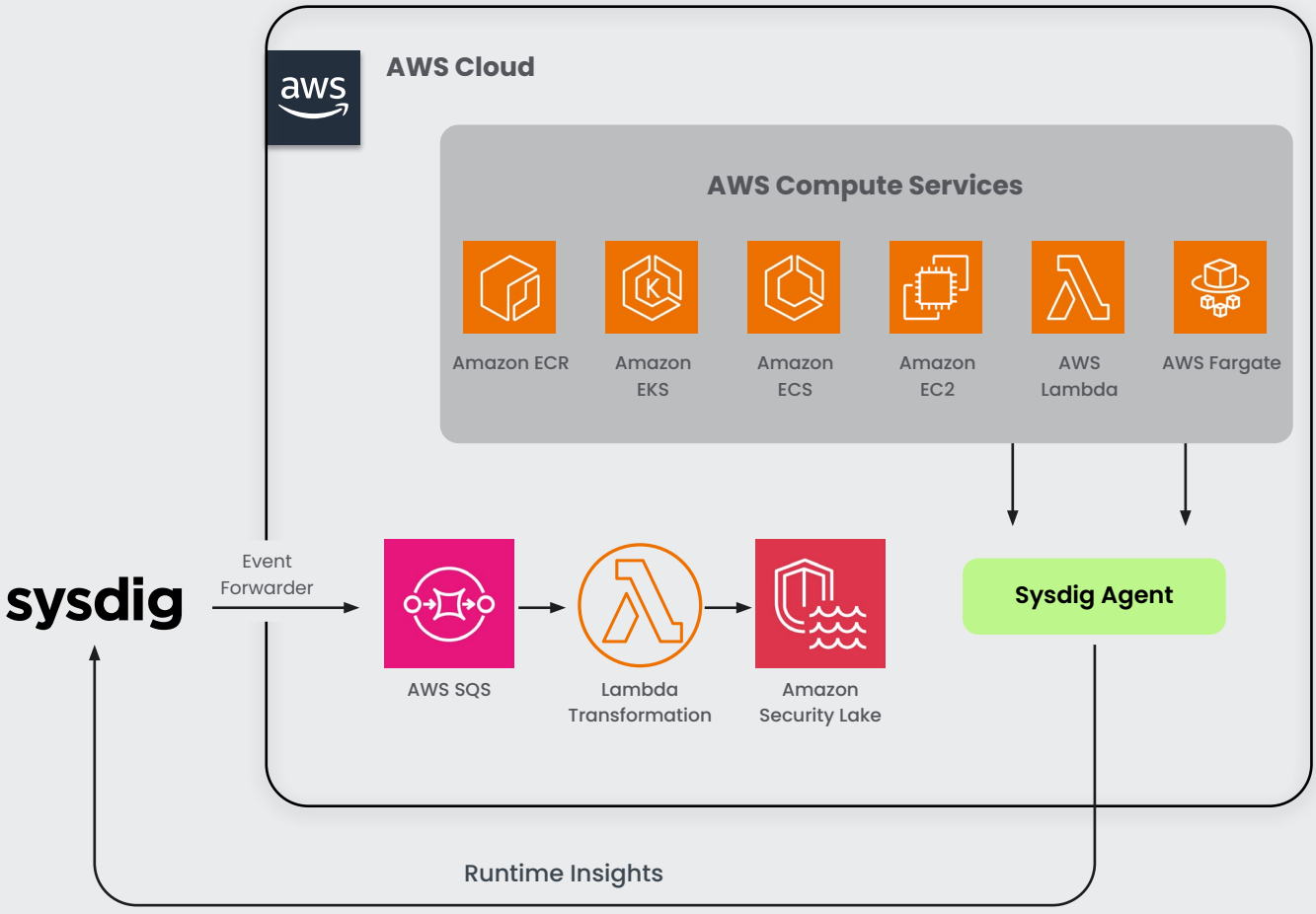
Simplify cloud compliance: Sysdig and Amazon Security Lake help you measure, monitor, and report on compliance across regions and accounts, reducing the time spent on gathering information and proof points. With Amazon Security Lake, you can centralize security data from multiple log sources, AWS Regions, and accounts into one or more rollup Regions to simplify your compliance and reporting obligations. Customizable retention settings help you address regulatory mandates to store data for a specific period.

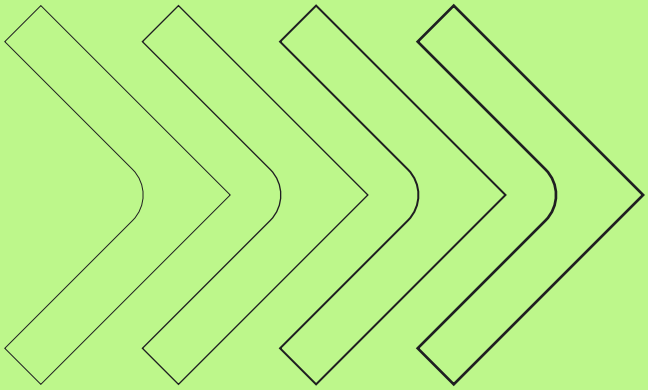


Send events automatically to Amazon Security Lake

Sysdig Secure captures runtime events in real time across your applications and infrastructure using detection rules based on open source Falco. If an activity looks suspicious or is an indicator of compromise, it triggers an alert. Details about the event are captured, along with context such as region, user, namespace, and more to aid investigation.

From there, Sysdig Secure uses a built-in event forwarding capability to automatically send security events to Amazon Simple Queue Service (Amazon SQS). Using the Sysdig Secure interface, you can deploy the AWS CloudFormation template or Terraform template to create Amazon SQS and Lambda function. The AWS Lambda function is triggered that starts an extract, transform, and load (ETL) transformation, and the runtime findings are batch uploaded to Amazon Security Lake in OCSF format.





sysdig | aws

See for yourself

Learn more about how Sysdig secures innovation on the AWS Cloud, find Sysdig solutions in AWS Marketplace, or get started with Sysdig Secure.