

Consolidated view of your AWS posture with AWS Security Hub

Cloud security posture is an important part of any organization's security practice. By understanding your assets and attack surface, you have a better opportunity to identify, detect, and respond. The problem is that security teams typically struggle with applying security policies consistently across the organization. This puts organizations at risk of security incidents due to gaps in security configuration from inconsistencies in policies. It simply takes a combination of tools to get the job done, but switching between multiple solutions in order to assess, investigate, and remediate cloud security events is no longer a tolerable option.

Amazon Web Services (AWS) Security Hub is a service that performs security best practice checks, aggregates alerts, and enables automated remediation. However, there's still the risk of missed configuration events. Together with Lacework, organizations can receive their Cloud Security Posture Management (CSPM), pipeline security scanning (Infrastructure as Code and image vulnerabilities), and workload protection alerts in one platform.

The Lacework Polygraph® Data Platform

The Polygraph Data Platform delivers comprehensive and continuous end-to-end AWS security and configuration support for both workloads and accounts running on AWS. As more organizations move their critical workloads to the cloud, there is an increasing need for a single, unified solution like our Platform to identify, analyze, and report on misconfigurations, vulnerabilities, and behavioral anomalies in user and account behavior.

Product features

This integration allows customers to view all of their AWS security events, whether from AWS native services, the Lacework Polygraph Data Platform, or any of the other AWS partners. You can:

- Consolidate multiple tools and reduce the time spent managing alerts
- Use existing response and remediation workflows for a much quicker time to value when implementing Lacework
- Receive events for posture management, shift-left security, and workload protection in a single interface

Why Lacework?



Avoid the challenge of managing security across multiple tools by consolidating Lacework-identified cloud security events into AWS Security Hub



Maintain best practices and governance across many security tools without difficulty



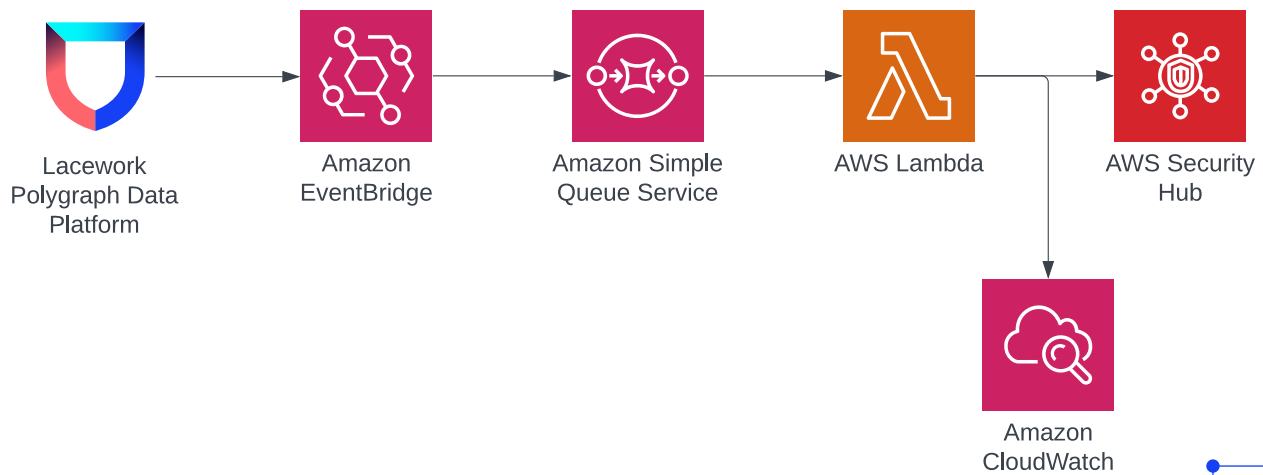
Avoid catastrophic impact to company and customers due to missed configuration, vulnerability, or unknown threats



Easily respond to and remediate cloud security events



Speed up the time to value when implementing Lacework by not requiring a new security event workflow



The power of the Polygraph

The Lacework Polygraph Data Platform learns and understands behaviors that introduce risk across your entire cloud environment, so you can innovate with speed and safety. With visibility from build time through runtime and automated insights into unusual activity, threats, vulnerabilities, and misconfigurations, you gain the context to prioritize and act faster.

Using patented cloud behavioral analytics, the Platform automatically learns how your environment is supposed to run and tells you when it deviates — providing the right alert, with the right context.

Whether you operate in one cloud or multiple, have a hybrid environment, or use Kubernetes and containers, Lacework has you covered with one platform to protect it all.

How it works

The Lacework integration pushes cloud security events from the Lacework Polygraph Data Platform to AWS Security Hub via the Amazon EventBridge alert channel, allowing your organization to manage all AWS posture and compliance events. The Lacework and AWS Security Hub integration uses multiple self-hosted AWS components that will transform a Lacework CloudWatch/EventBridge alert into a Security Hub finding.



Differentiators

Lacework helps you achieve the following outcomes:

- **Understand your AWS cloud** by seeing what's deployed by builders, automatically make sense of how and why the cloud changes, and uncover and prioritize risk.
- **Gain expert-level security** by empowering existing staff to find early signs of trouble without extensive querying.
- **Fix what matters earlier** by eliminating noise, removing reliance on static and complex rulesets, and spotting and fixing issues before production.
- **Prove cloud compliance in a fraction of the time** by automating the most tedious part of meeting compliance.
- **Lower overall total cost of ownership** by concentrating efforts on maintaining one (vs multiple) cloud security solutions and decrease the operational risk from employee turnover.

Get started now.

Solution available in [AWS Marketplace](#).

Contact alliances@lacework.net.

Visit [Lacework.com/aws](https://lacework.com/aws) for more details, demo videos, whitepapers, case studies, and customer testimonials.

Additional resources

- [Blog](#)
- [Demo](#)
- [eBooks](#)
- [Webinars](#)
- [Whitepapers](#)

Lacework is the data-driven cloud security company. The Lacework Polygraph® Data Platform delivers end-to-end visibility and automated insight on risks across multicloud environments, collecting, analyzing, and correlating data. Customers depend on Lacework to drive revenue, bring products to market faster and safer, and consolidate security solutions into a single platform. Get started at www.lacework.com