LACEWORK

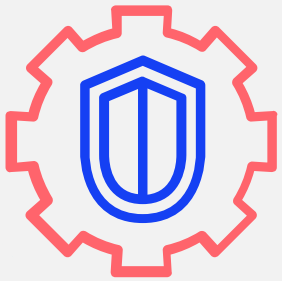
PARTNER INTEGRATION BRIEF

Up-level your cloud investigations with Amazon GuardDuty and Lacework composite alerts

Overview

Detecting and responding to possible threats in the cloud can be a daunting task for many reasons: the abundance of auditable activity, the complexity of cloud resource relationships, the ephemeral nature of cloud computing, and more. Cloud environments are complex, often spanning multiple clouds and generating billions of events per month. These events encompass cloud account access, workload changes, and the network-level relationships between your workloads and the public internet. Enterprises receive an overwhelming number of alerts, which can result in delayed responses and a limited understanding of the details surrounding potential risks or attack ranges. The result: security teams are required to spend considerable amounts of time manually connecting seemingly independent signals that, when combined with other events, can reveal a serious and legitimate threat.

Thankfully, the Lacework Polygraph® Data Platform on Amazon Web Services (AWS) simplifies overall cloud security management while quickly and automatically delivering visibility and actionable insights that truly matter to you and take your business to the next level.



This integration truly helps Lacework and AWS customers go further, faster in addressing cloud detection and response. You can:

- Gain greater visibility into your AWS cloud environment by enriching Lacework composite alerts with Amazon GuardDuty findings.
- Make use of lower severity alerts that you don't have time or resources to investigate. Lacework reports on the important event details that may be hidden within them.
- Improve your time to value with the ingestion of third-party data into Lacework, and time saved by eliminating the need to switch between user interfaces.

> Amazon GuardDuty and Lacework together give us greater insight and efficiency. The technologies working together have been a huge benefit for our organization."

RUSSELL K. | INFORMATION SECURITY ENGINEER, RAPIDSOS

The Lacework Polygraph Data Platform

Lacework offers a data-driven security platform for the cloud and is a leading cloud-native application protection platform (CNAPP). Lacework can collect, analyze, and correlate data across an organization's cloud and Kubernetes environments to focus on the handful of security events that matter — all without requiring manually written rules.

The high-fidelity composite alerts feature of the Lacework Polygraph Data Platform helps you detect compromised credentials, cloud ransomware, cryptomining, and other known and unknown cloud threats that would otherwise go unnoticed. Composite alerts combine human intelligence from Lacework Labs about prevalent attack sequences and tactics with automatic correlation of numerous events, including low criticality data from disparate sources. This gives you a single comprehensive, evidence-backed alert that includes complete context and practical information. This alert streamlines the investigation process for SOC teams by automating the evidence collection phase, allowing analysts to promptly address cloud threats without pivoting between various data sources.

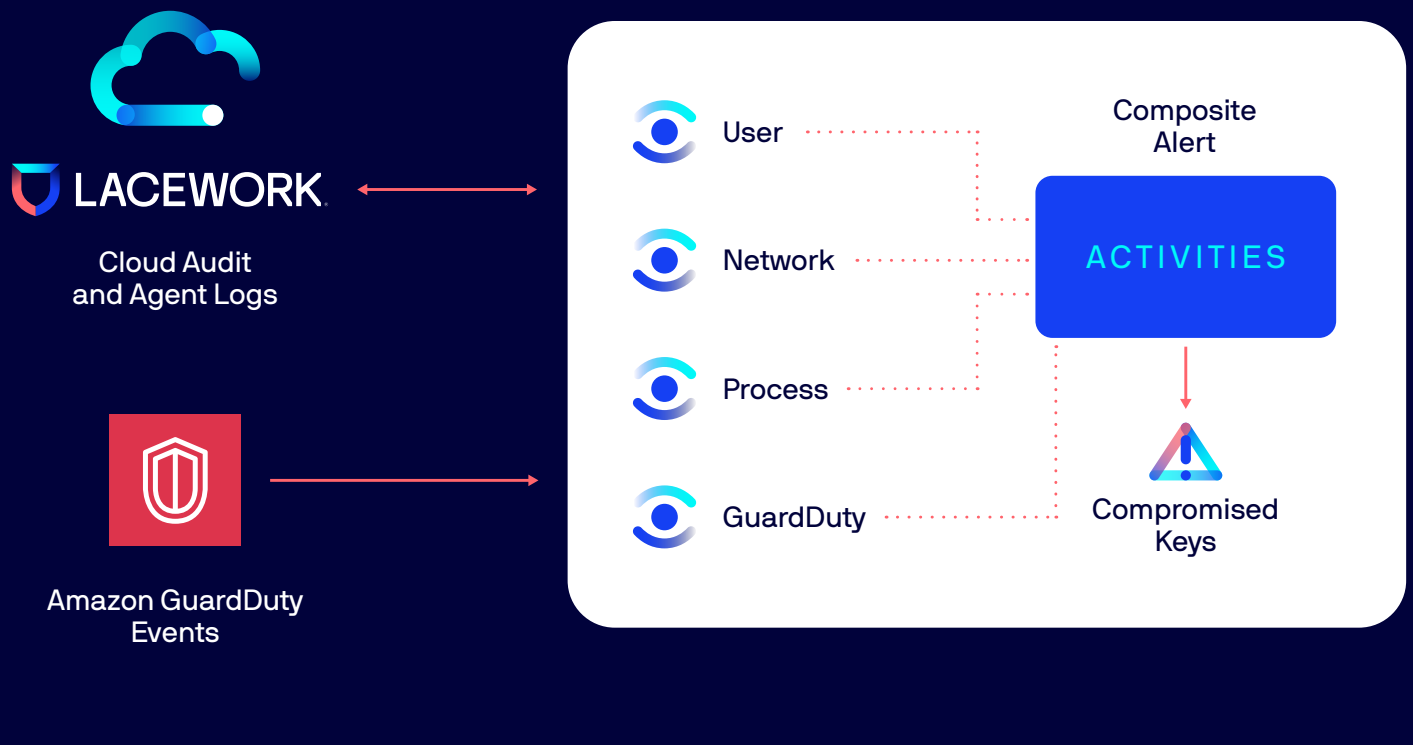
Composite alerts are an essential component of cloud detection and response (CDR), which is defined as a security tool primarily focused on detecting, confirming, and investigating suspicious activities and other security problems in various public cloud environments. CDR is a critical component of a CNAPP solution.

Lacework is upping our CDR capabilities by enriching threat investigations with detections from Amazon GuardDuty – marrying qualified findings from Amazon GuardDuty with Lacework-generated detections. By combining Amazon GuardDuty events with the Lacework insights from our composite alerts, our customers now have an enhanced layer of security insights and context. Together, Lacework composite alerts and Amazon GuardDuty help to surface both known and unknown threats faster, reducing false positives and investigation time.

How it works

The Integration with AWS Security Hub collects all the findings from Amazon GuardDuty, adds the entities and relationships to our patented model, and presents relevant Amazon GuardDuty findings as supporting facts in Lacework composite alerts. Composite alerts may then be pushed to Amazon Security Lake, giving you the ability to pull from multiple sources so you can manage security data for more efficient storage and query.

With this approach, you and your teams no longer need to struggle correlating data across multiple products. Instead of pivoting between the Lacework and Amazon GuardDuty UIs / CLIs to build an understanding of what was compromised, relevant Amazon GuardDuty detections are displayed directly within Lacework composite alerts.



Experience the Lacework difference

Understand your cloud and find unknown threats

A leading CNAPP company that automatically identifies net new cloud behaviors and detects unknown threats

Our patented technology automatically learns your cloud environment, visualizes all its complex relationships, baselines normal behavior and activity, and alerts on changes that warrant attention — all without manual configuration.

Focus on risks that matter most

Automatically correlates data from code to cloud to put risks into context

Lacework natively integrates into existing workflows and toolchains and provides highly-contextualized alerts that detail who, what, why, when, and where within a singular view so the right people on your team can take the right action.

Single platform delivering continuous security and an integrated experience

One user experience for multi-cloud, hybrid, and Kubernetes coverage on Linux and Windows

The Polygraph Data Platform has a flexible architecture that easily adapts to evolving cloud technologies for continuous security and a centralized view of auditable compliance evidence.

Fast and flexible to operationalize at scale

Natively integrates into your DevOps, IT, and security workflows

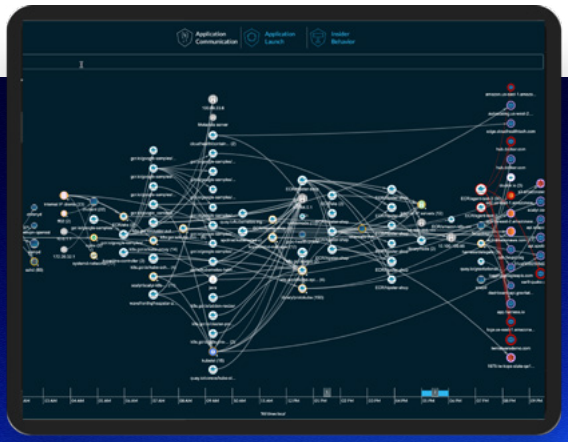
Our full SaaS platform is turn-key and has the ability to adapt with you as your cloud security needs evolve, whether you grow into multiple clouds, scale out the size of your environment, or need additional security capabilities.

Get started now

This solution is available in AWS Marketplace.

Contact alliances@lacework.com.

Visit lacework.com/AWS for more details, demo videos, whitepapers, case studies, and customer testimonials.



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.

LACEWORK

 | 888.292.5027 | lacework.com

aws Available in AWS Marketplace