

## Seamless Multi-Account Cloud Security with AWS Control Tower

### Why Lacework?

- Automatic onboarding of enrolled accounts into Lacework's unified cloud security platform with AWS Control Tower
- Get deep observability into your cloud accounts, workloads, and microservices to give you tighter security control
- Identify common threats that specifically target your cloud servers, containers, and IaaS accounts so you can action on them before your company is at risk
- Detect and resolve anomalous changes in behavior across your workloads, containers, and IaaS accounts that represent a security risk or an IOC
- Achieve compliance for SOC 2, PCI DSS, HIPAA, and other compliance measures that require host intrusion detection (HIDS)

### Lacework Cloud Security Platform overview

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

### Product features

#### Continuous AWS security monitoring of user activity

- See all activity on Amazon Web Services (AWS) resources, such as new activity in a region, activation of new services, or changes to access control lists.
- Quickly visualize all changes to users, roles, or access policies.
- Receive notification of access tampering or customer master key tampering.
- Reduce alert fatigue with customizable alerts and reports that eliminate repetitive or irrelevant results.

### The Power of the Polygraph

Our foundation is based on a patent-pending Polygraph technology, a deep, temporal baseline built from collecting high-fidelity machine, process, and user interactions over time. The Polygraph detects anomalies, generates appropriate alerts, and provides a tool for users to investigate and triage issues.

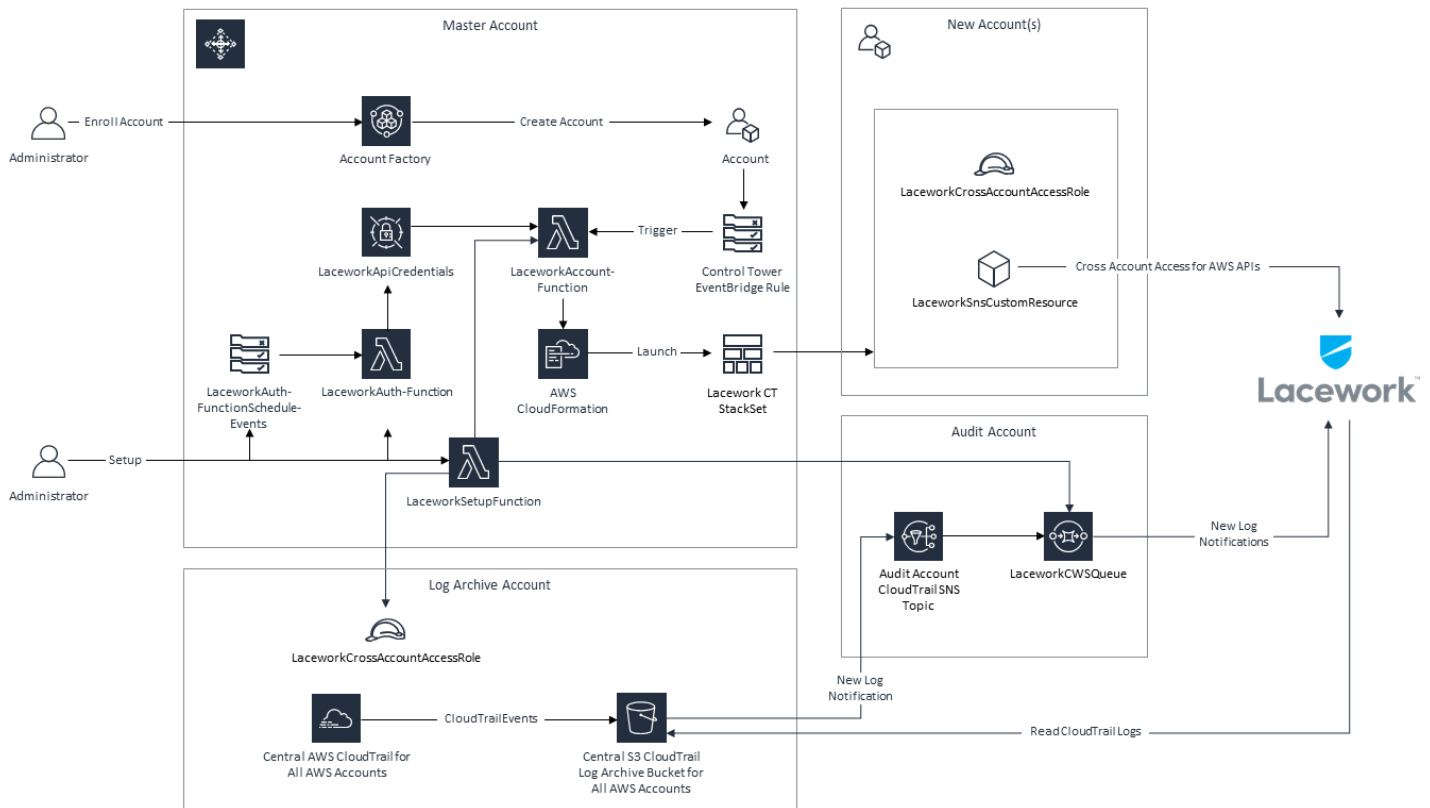
### Speed, scale, and integration

Pinpoint exactly how files change—from content and metadata to whether the file was modified or simply appended. Extended information on executables, such as files created without a package installation, command lines used at launch, or currently running processes.



## How it works

Lacework's AWS Control Tower integration enables a seamless AWS account onboarding experience with the Lacework Cloud Security Platform. Account administrators can automatically add Lacework's security auditing and monitoring to new AWS accounts during account creation. All the required Lacework and AWS account configurations that allow access to AWS configuration and CloudTrail logs are managed for you by Lacework's AWS Control Tower integration. The integration is launched with a CloudFormation template which creates all the necessary resources to connect your Lacework to your AWS accounts. This template includes stack set templates, roles & permissions, Lambda functions, SQS queues and EventBridge rules.



## Differentiators

- Delivers threat detection, compliance, and automated monitoring for AWS cloud environments.
- Provides actionable auditing of security configurations, ongoing monitoring of user activity with behavioral detection, and automated and scalable architecture.
- Eliminates unnecessary hardware or software maintenance, manual rule configuration, and excessive alerting.

## What our customers are saying

# Snowflake Accelerates Penetration Testing with Lacework on AWS

### Challenge

Snowflake required a faster way to enable third-party penetration testers to simulate threats against the Snowflake system in order to detect gaps and vulnerabilities.

### Solution

Lacework easily identified and traced the patterns of the penetration testing to expose vulnerabilities and gaps and prevent further threats. Lacework's forensic capabilities outperformed any previous tools that Snowflake had tried.

### Benefits

- Enabled full end-to-end visibility across Snowflake's environment
- Reduced configuration and analysis of events and alerts from 3 hours daily to 15 minutes.
- Detected security incidents within minutes



### About Snowflake

Snowflake offers a cloud-based data storage and analytics service, which allows corporate users to store and analyze data at a fraction of the cost of traditional solutions. Snowflake delivers the performance, concurrency, and simplicity needed to store and analyze an organization's entire data in one location.



### About Lacework

Lacework provides security and compliance for the cloud. The platform delivers build-time to run-time threat detection, behavioral anomaly detection, and cloud compliance across multi-cloud environments, workloads, accounts, containers, and Kubernetes.

“It's nothing short of revolutionary. It's making a change in how security teams are thinking about their environment and what they're doing on a daily basis.”

Mario Duarte, Director of Security, Snowflake

## Data points

80%

Faster threat investigation

95%

Reduction in false positives

1.4

Average security alerts generated daily per customer

2-5

Fewer security tools per customer

## Additional resources

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

## Get started now!

Visit [Lacework](#) or our [AWS Marketplace Listing](#) for more details, whitepapers, case studies, demo videos, and customer testimonials.

[Contact APN Partner](#) or [alliances-partnership@lacework.net](mailto:alliances-partnership@lacework.net)

Solution available in [AWS Marketplace](#)