SOLUTION BRIEF

Gain more value and visibility from cloud audit logs

Use automation to reduce costs, manual lift, and burnout

SUMMARY

Lower costs with Lacework for audit log ingestion

How do you know what's happening in your cloud? Cloud audit logs provide crucial insight into your increasingly complex cloud environments — including information like who did what, where they came from, and what region they did it in.

Each major cloud service provider has its own proprietary audit log: Amazon Web Services (AWS) CloudTrail, Azure Audit Logs, and Google Cloud Audit Logs. Even Kubernetes has a version of audit logs. This information needs to be ingested and processed efficiently — with domain expertise across all providers — to gain the right insights and value.

Many companies turn to a SIEM (security information and event management) solution to ingest this data and detect malicious events. However, audit log volume can quickly grow overwhelming, taking the majority of your total SIEM space. Additionally, a SIEM solution often requires lots of manual rule-writing and tuning to catch malicious activity and yields many false positive alerts.

Lacework offers a better alternative. Our platform features patented behavior analytics, which can ingest data from across your cloud — including audit log data — to build a baseline for normal behavior. We then surface any anomalous activity and correlate data points from a number of sources across your cloud to determine criticality. This means higher quality alerts, whether or not you choose to write custom rules.

Benefits of Lacework + SIEM

- 80% reduction in SIEM ingestion by pre-filtering cloud audit logs through Lacework
- Gain new insights into your cloud, without major time investment or security expertise
- Decrease time spent on investigations and compliance
- Alleviate alert fatigue and burnout

CHALLENGES
From data to burnout

Organizations of all sizes can benefit from the insight that audit logs provide. However, the volume of audit logs quickly grows overwhelming. Whether you're monitoring one account or hundreds, the log volume can account for half or more of your total SIEM volume — a problem that can become very costly very fast.

Additionally, the manual nature of SIEM rule maintenance can lead to burnout. Most SIEMs only have very basic rules for each cloud, so security teams find themselves having to author rules to handle new detections. These rules are general enough to apply to all of their cloud accounts, yet specific enough to catch bad activity. This leads to loads of false alerts. So security teams find themselves writing new rules or tuning old ones, while dealing with an endless alert queue.

And all of this only applies to "known bads." Most often, security teams don't have the expertise to write anomaly-based rules, so the typical SIEM isn't equipped to find unknown risks and threats. So, in spite of the incessant manual heavy-lifting, bad actors still seem to find their way into cloud environments.

There is a better way.

ENTER LACEWORK
The better way to manage your cloud audit logs

The real problem with relying on a SIEM for cloud audit log ingestion is that it isn't scalable. The costs are too high. The work is too manual. For the effort, the results simply aren't good enough. Security personnel can write rules against already known problems and can work on tuning the noise. But how do they keep up with hundreds of accounts across multiple clouds? And how do they defend those threats they don't yet know about?

Lacework was founded to solve these issues. Our platform is the more effective, cost efficient alternative to a SIEM for analyzing cloud audit logs. Lacework uses patented behavioral analytics to automatically build a baseline for your normal cloud behavior, then detects any anomalous activities in your cloud environment. This makes for dependable and scalable cloud security, whether or not your team chooses to write any custom rules.

Lacework specifically manages the challenge of cloud audit logs by converting every log entry into an activity and understanding which entity performed the activity, where the activity came from, and what resulted from the activity. We then compare this behavior to what we have historically observed about that user, the shared role, the region, and the service involved. If any parts of the chain look unusual, we alert you, along with the context you'd need to understand if this was evidence of cloud compromise.

BENEFITS AND DIFFERENTIATORS
Sifting through data to speed analysis

Lacework uncovers anomalies without human intervention. Are there changes to your S3 buckets? Are services in new regions being turned on? Is a new user modifying a security group? Lacework will alert you to all unusual activity in your audit logs, whether or not you choose to write rules. Lacework also tells you just how unusual the behavior is, letting you determine if there's a legitimate security issue or if it's a false alarm.

Every day, our platform helps security teams reduce manual lift and cut through the noise faster. Our behavioral analytics engine, Polygraph®, provides deep insights that can help security professionals, analysts, and investigators analyze cloud audit logs in less time. With facts and related activities at their fingertips, Lacework users can quickly see:

- What the entities involved in the incident did and what they did differently compared to their peers
- How far an attacker got and what else they did (i.e., blast radius)
- Detailed visualizations for alerts and incidents
- Any alerts or events related to the specific incidents

Lacework helps security teams reduce manual lift and cut through the noise faster.

THE LACEWORK APPROACH

Cloud security built from your own data

Lacework was built from the ground up to manage cloud and container security. Best of all, it grows with your needs and changes in the cloud. Here's how:

1. Automatically correlate data from across your environment. Our platform ingests massive amounts of your cloud data, then maps what you've deployed in each of your clouds. We then automatically connect the dots, tying together any of the most critical risks from across your cloud and telling you how to fix them.

2. Pinpoint any threat, whether known or unknown. With Lacework, rules are optional. Using your data, our platform creates a baseline of your normal cloud behavior, then continuously monitors for abnormalities. We continuously learn from your environment and deliver high quality alerts, with little to no manual lift required.

3. A platform to grow with you. Every cloud journey is different. With our layered agentless and agent-based approach, you can choose which data sources to tap into as it makes sense for your business and roll out the entire platform over time.

Summary

With the power of anomaly-based threat detection from Lacework, writing endless rules to cut through mountains of cloud audit data is a thing of the past. Now, you can reduce risk in your cloud environment while automating the security process. To free up time for what matters most, get started with Lacework today.

Examples of anomalies Lacework can identify

There's no need to write endless rules — Lacework automatically checks for these activities (and more):

- New regions or services turned on
- New identity and access management (IAM) users or keys
- Someone modifying route tables or new VPNs
- Changes to AWS S3 buckets
- Lambda IAM role acting in an unexpected way
- New user changing security group rules

Want to see more?

Schedule a demo

Learn more about anomaly detection