Lacework for AWS CloudTrail protects AWS deployments by automatically detecting any anomalous activity in the millions of events logged by CloudTrail. Lacework Polygraph baselines AWS account activity, detects deviations from the baseline, alerts on anomalies, and simplifies the investigation of incidents.

Lacework for CloudTrail enables you to make sense of the millions of events captured in CloudTrail and is the perfect antidote to cloud security complexity: no rules, no policies, and no time spent on tedious event analysis.

**Unauthorized Activity on AWS Resources**

- Changes to AWS S3 buckets
- Unusual activity in new regions or accounts
- Activation of new AWS services
- Changes to AWS access control lists (ACLs)

**Suspicious Changes to Users, Roles, or Access**

- Adding users or roles to AWS
- Activation of new services, new users, and new APIs
- New users changing security groups or IAM policies
- Bypass of two-factor authentication (2FA)

**Manipulation of AWS Infrastructure Services**

- Changes to network interfaces and services
- Modifications to route table or new VPNs
- CloudTrail service stopped or logs deleted
- Access or customer master key tampering
Unprecedented Insights Into AWS Accounts

By deploying Lacework’s Polygraph on AWS CloudTrail, you instantly gain a better understanding of what’s happening in your AWS deployment. Our approachable visualization highlights the who, when, what, and how for all AWS account activity. No more tedious log correlation or guesswork. With Polygraph, your cloud infrastructure and security staff can work faster and smarter.

**EFFICIENT**

Zero-touch implementation, configuration, and operations: no rules, no policies, no log analysis. Operate without tuning, tweaking, or whitelisting.

**SIMPLE**

Categorize, group, analyze, and correlate AWS CloudTrail events automatically. Reduce security staff grunt work.

**POWERFUL**

Lacework automatically evaluates every AWS account event for you. You are only presented with what matters: anomalies, with easy access to insights.