Lacework

Threat detection, compliance, and automated security monitoring for AWS

Why Lacework?

- **Security visibility** – Get deep observability into your cloud accounts, workloads, and microservices to give you tighter security control.
- **Threat detection** – Identify common security events that specifically target your cloud servers, containers, and infrastructure-as-a-service (IaaS) accounts so you can action on them quickly.
- **Anomaly detection** – Detect and resolve anomalous changes in behavior across your workloads, containers, and IaaS accounts.
- **Host compliance** – Help achieve compliance goals for SOC 2, PCI DSS, HIPAA, and other compliance measures that require host intrusion detection (HIDS).
- **Configuration compliance** – Spot IaaS account configurations that are non-compliant and identify opportunities to apply security best practices.

Product overview

Effective enterprise security demands more than just operating off of signatures and custom rules. Security teams must have a solution that not only identifies changes but understands their meaning and context.

To address the agile nature of the cloud, Lacework helps provide comprehensive, continuous end-to-end security and configuration support for workloads and accounts running in AWS environments. As more organizations move their critical workloads to the cloud, there is an increasing need for a single, unified solution like Lacework that can identify, analyze, and report on misconfigurations, potential risks, and behavioral anomalies in user and account behavior.

Product features

Actionable auditing of Amazon S3 bucket configurations

- Identify misconfigured Amazon Simple Storage Service (Amazon S3) buckets that may result in broad access or noncompliance with the CIS Benchmark
- Ensure use of encryption at rest and in transit
- Allow only users with multi-factor authentication to delete Amazon S3 buckets
- Protect against deletion or overwrite using version control
- Get specific recommendations on how to fix misconfigurations

Audit your AWS configuration

- Identify potential risks in identify and access management (IAM), including the use of “root” account, lack of multi-factor authentication, and inadequate password requirements
- Check for logging best practices, such as ensuring AWS CloudTrail is enabled across regions, and that log files are validated and encrypted
- Confirm secure network configurations, including limiting access to restricted ports, enforcing “least access” privileges and using flow logging

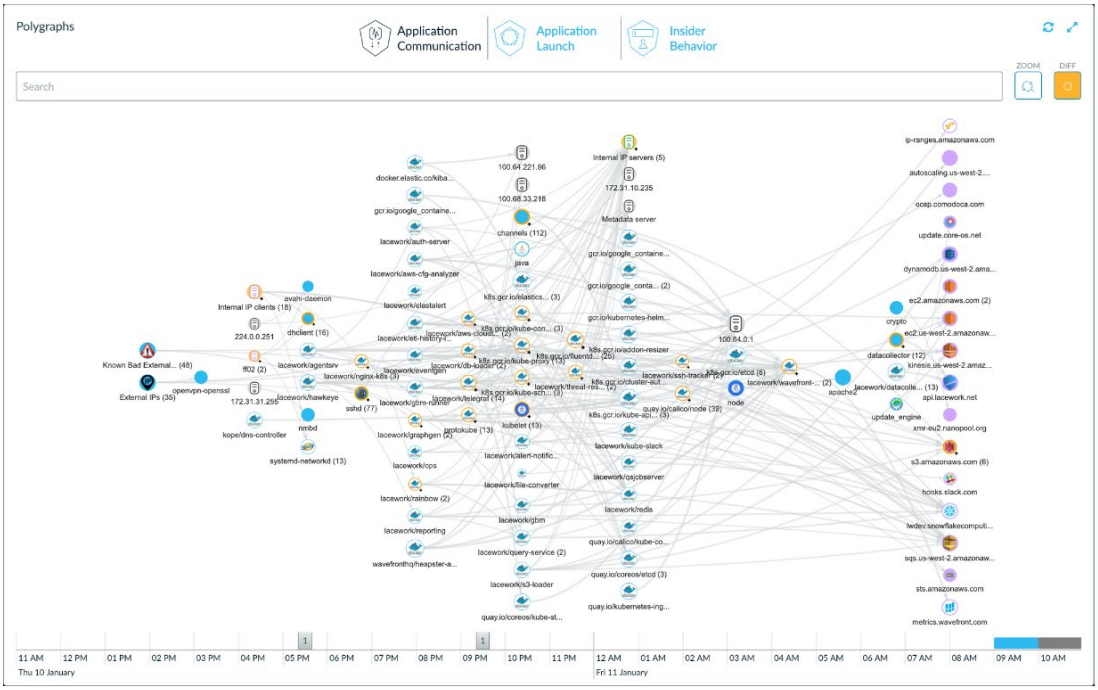
Product features (cont.)

Ongoing monitoring of activity

- Activity on AWS resources, such as new activity in a region, activation of new AWS services or changes to access control lists
- Monitor critical account activity, such as unauthorized API calls, and use of the AWS Management Console, and use of the “root” account
- Changes to users, roles, or access policies
- Access or customer master key tampering
- Reduce alert fatigue with customizable alerts and reports that eliminate repetitive or irrelevant results

The power of Polygraph

Lacework’s foundation is Polygraph, a deep temporal baseline built from collecting high fidelity machine, process, and user interactions over a period of time. The Polygraph is used to detect anomalies, generate appropriate alerts, and provide a tool for users to investigate and triage issues.



Differentiators

- **Integrated and comprehensive** – Pinpoint precisely how a file changed: content, metadata, and whether the file was modified or appended. Comprehensive information on executables, such as files created without a package installation, command lines used at launch, currently running processes (with users and network activity), and suspect versions. Cloud-wide capabilities for search, file type summaries, and detection of new files.
- **Cloud scale and speed** – Automated configuration, file discovery, and operations. Scalable architecture with no added complexity or performance penalties is included with all Lacework Cloud Security agents.
- **Meet compliance mandates** – Protect log and configuration files against tampering. Daily re-checks of all monitored files. Pre-defined directory maps monitor critical files and directories.

Solution available in AWS Marketplace