Lacework

Data-Driven Security Platform for the Cloud

As global demand for cloud computing continues to grow, more organizations are enjoying the associated opportunities for dynamic, scalable, and flexible workloads.

While the cloud has created enormous opportunities for companies to compete in new innovative ways, it comes at a cost and with distinct challenges. Challenges such as new attack surfaces, unknown vulnerabilities, lack of visibility across your environment and everything happening at the speed and scale of the cloud. The big question: Who knows what's going on in your cloud environment? We do.

A NEW APPROACH TO CLOUD SECURITY

Our foundation is based on the patented Polygraph™ technology, which uses unsupervised machine learning, behavioral analytics, and anomaly detection to uncover threats, misconfigurations, known bads and outliers across AWS, Microsoft Azure, Google Cloud, workloads, containers, and Kubernetes. Lacework automatically learns activities and behaviors that are unique to each customer's environment, creates a baseline, and surfaces unexpected changes so they can uncover potential issues and threats before they become a major problem.

With Lacework You Can:

Investigate threats 80% faster

Consolidate 2-5 tools

Reduce false positives by an average of 95%

Increase productivity for your security team

Accelerate security audits by 35%

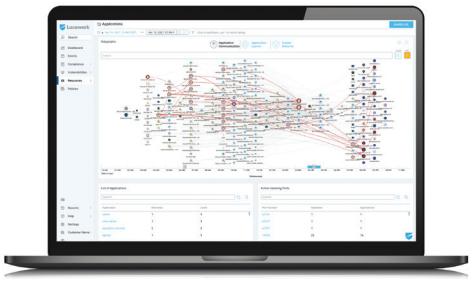
The Power of Polygraph

INGEST
Millions of data points per second

ANALYZE
Patented machine learning models, behavioral analytics

DETECT
Anomalies, misconfigurations, vulnerabilities and outliers

Lacework's data-driven Polygraph™ engine simplifies security by learning your business for you. It brings automation and machine learning to cloud security, allowing you to move beyond the traditional rules-based responses that lack contextual insight, require constant updating, and leave you vulnerable to compromise. Our technology allows organizations to detect malicious behaviors without creating a single rule.



This self-adapting technology uses behavioral and raw infrastructure metadata to develop behavioral models at scale, updating as workload behavior changes. Polygraph is the visual representation of interconnected application, user, machine and network behaviors that provide visibility to both security operations and DevOps staff. Lacework identifies anomalous behavior while achieving deep, contextual visibility into your unique workload and environment to provide comprehensive cloud security with speed, scale, and accuracy.

Lacework's data-driven, automated security platform delivers comprehensive cloud native application security, enhanced compliance and visibility allowing your organization to securely access all the benefits the cloud has to offer.

Our platform offers a number of advantages:

Advanced Threat Detection — Identify anomalous activity that deviates from behavioral models and may indicate a threat.

Tool Consolidation – Eliminate unnecessary tools to consolidate tooling and boost scalability.

Improved Efficiency – Reduce alert noise and false positives with data-driven analysis, saving time and resources.

Enhanced Visibility – Achieve deep visibility into and across processes and applications within cloud and container environments to improve threat detection, incident investigation, and triaging.

Continuous Configuration Compliance – Detect and report on misconfigurations that violate regulatory compliance requirements.

FIND OUT MORE

lacework.com
info@lacework.net
press@lacework.net

Platforms we support:

aws · Google Cloud · Azure · docker · kubernetes · ubuntu · Linux · CoreOS · rackspace

Lacework
6201 America Center Dr
Suite 200
San Jose, CA 95002

08/21

Lacework