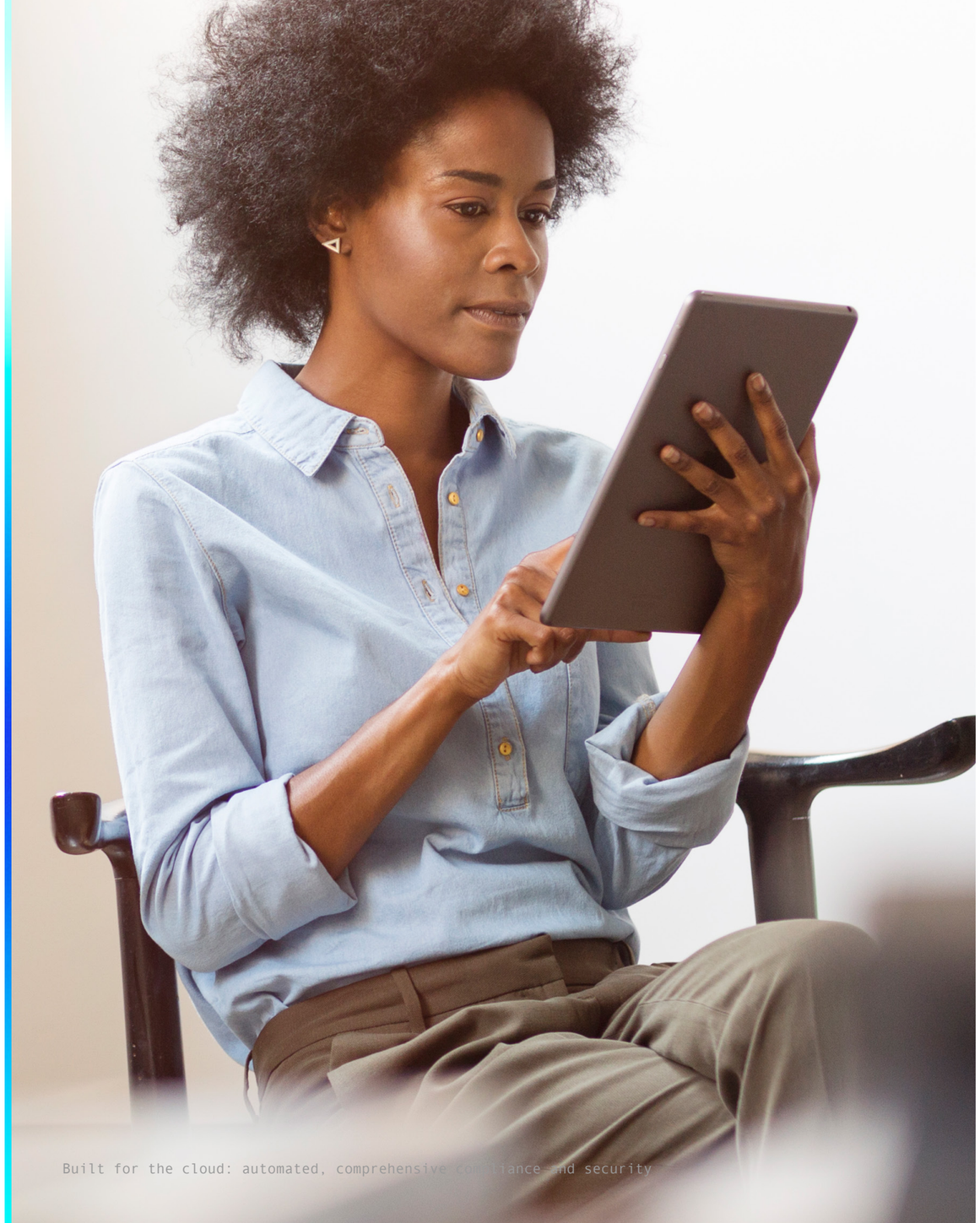
Built for the cloud: automated, comprehensive compliance and security

LACEWORK®

Introduction

First-generation cloud security solutions are designed like checklists. They use rules that map specifically to known compliance controls and measure the organization's performance against them. While this approach meets the objectives of compliance workflows, it requires continuous manual effort, and can't keep pace with the velocity of modern cloud environments.

LACEWORK



Built for the cloud: automated, comprehensive compliance and security

As cloud security evolves, so do the needs of customers as they start to adopt cloud-first strategies.

Cloud compliance typically addresses the immediate need for cloud operational hygiene, but it still leaves gaps when it comes to improving your cloud security posture.

The most difficult part of an audit is having to prove compliance with the framework. Often, it's necessary to gather a lot of evidence both before and during the audit. If your organization has never achieved compliance with a particular standard before, you also face the unknown cost and risk of preparing for that audit and potentially going through a pre-audit to make sure the final audit is successful. Pre-audits and audits, along with the accompanying need to gather evidence, are time-consuming and expensive.

Your cloud security strategy should include security operation workflows and cloud incident response readiness. This ensures that your cloud environment is operating at an appropriate risk level as you scale to meet your business needs. Because changes can lead to new vulnerabilities and potential threats, potentially impacting your security posture and compliance goals,

Lacework was built specifically to deliver contextual data about cloud events.

Lacework identifies and analyzes every update, configuration change, and access point, along with a million other activities that might represent potential threats.

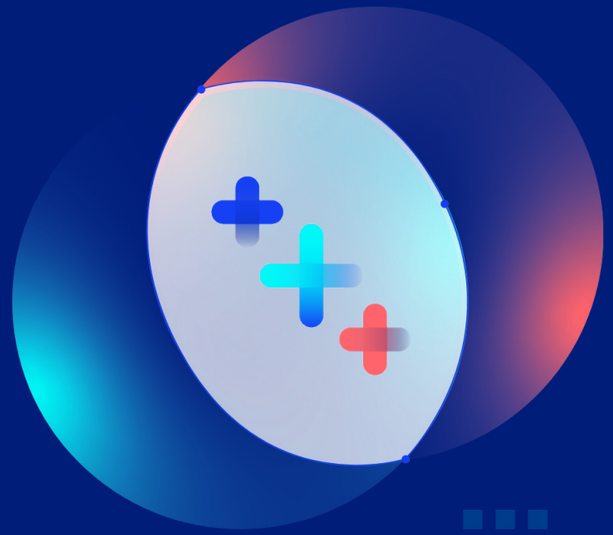
Compliance and security built to scale

Actionable

Lacework gives you the visibility and context to meet industry and customer security requirements (including for M&As), ultimately improving your bottom line. Get the right amount of data and context at the right time to take the action you need.

Scalable

Grow with the Lacework platform as your security needs evolve. We support all AWS, Google Cloud, Azure, and Kubernetes configurations, and we help you operate at scale across hundreds of accounts and thousands of containers and hosts.



Valuable

Unlock opportunities to sell to customers in new regions, industries, and segments by demonstrating compliance. Lacework also helps you avoid fines with continuous monitoring and historical reports.

Streamlining compliance: continuous protection and security automation

The cloud is increasingly popular for all types of organizations, and that popularity makes it a great target for hackers. Companies that run workloads in the cloud are left exposed and vulnerable to data leaks, account hijacks, cloud server breaches, and other illicit activity.

Lacework supports organizations with an automated, comprehensive security solution for multicloud and container environments that helps you maintain control of your business. The Lacework Polygraph® Data Platform will scan for risks and also continuously monitor cloud account activity and workload behavior in runtime to identify attacks at the start. Plus, it will tie those insights together to help you effectively prioritize and fix critical issues. This new technology gives small security teams the same compliance management power as the largest enterprise security organizations.

Lacework features

Lacework is a complete compliance solution that eliminates the need to direct large numbers of IT staff to compliance readiness. We automate compliance monitoring, assessment, and reporting so that your development team can accomplish more in less time. Here are some of the many features that you can use to streamline your compliance journey.

Asset management

Track your cloud resources with the Lacework resource management function. You can edit the resources summary to show different information, including Resource Name, Account ID, Account Alias, Service, Type, Status, etc. You can also export the resource summary to a CSV file, which you can use as evidence of your organization's cloud asset inventory.

Vulnerability scanning

By managing vulnerabilities and compliance continuously, you can mitigate risk as it is introduced into your cloud infrastructure. Lacework automatically and continuously scans your organization's cloud environment for vulnerabilities, which we communicate via alert channels configured by the admin user. The Lacework Vulnerability Assessment summary shows a list of all identified vulnerabilities and rates them based on criticality. You can then export the report to a CSV file to share with auditors.

Logging and monitoring

Automated monitoring and reporting throughout the development lifecycle helps ensure that you're compliant from day one. Lacework monitors all events, configurations, and behavioral activities on the cloud, offering you a complete view of your entire cloud ecosystem. The events dashboard gives an overview of all events that have been logged in their environment. Event records include a description of why the event was triggered, which account was responsible, what API was affected, and the source IP address. Lacework also enables you to send high fidelity contextual alerts to your SIEM solution.

Host intrusion detection

Lacework acts as a host-based intrusion detection system (HIDS), where an agent is loaded into various types of Linux workloads to gain visibility into changes in baseline behaviors. Lacework can also monitor Kubernetes-based workloads as well as files within containers and VMs.

Kubernetes security

Gain deep visibility into your Kubernetes deployment with dashboards of your clusters, pods, nodes, and namespaces combined with application-level communication between all of these at the application, process, and network layer.

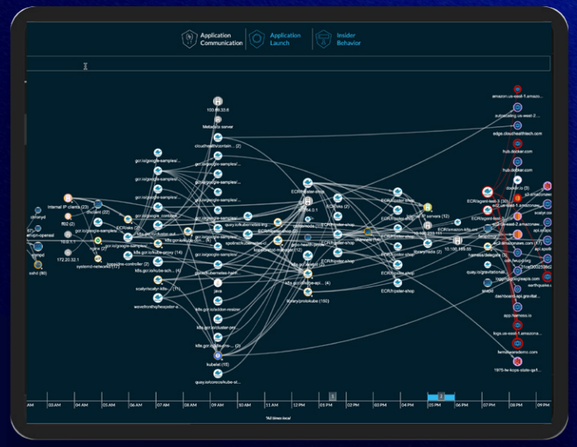
File integrity monitoring

Automate setup and eliminate labor-intensive rule development, ACL specification, and configuration that results in the reduction of false positives so security teams can focus on the FIM events that really matter.

Anomaly detection

Get real-time anomaly detection for all cloud and container environments. Machine learning identifies and analyzes behavioral deviations from normalized behaviors that result from vulnerabilities.

LACEWORK



Ready to chat?

Request a demo

Lacework is the data-driven security company for the cloud that delivers end-to-end visibility and automated insight into risk across cloud environments, so you can innovate with speed and safety. The Lacework Polygraph® Data Platform ingests data, analyzes behavior, and detects anomalies across an organization's Amazon Web Services (AWS), Google Cloud, Microsoft Azure, and Kubernetes environments. This patented approach significantly reduces noise and turns millions of data points into prioritized, actionable events. Customers all over the globe depend on Lacework to take software services to market faster and more securely, while consolidating overlapping security solutions into a single platform for better visibility and coverage across a multicloud environment. Founded in 2015 and headquartered in San Jose, Calif., Lacework is backed by leading investors like Sutter Hill Ventures, Altimeter Capital, D1 Capital Partners, Tiger Global Management, Counterpoint Global (Morgan Stanley), Franklin Templeton, Durable Capital, GV, General Catalyst, XN, Coatue, Dragoneer, Liberty Global Ventures, and Snowflake Ventures, among others.

Get started at www.lacework.com