SOLUTION BRIEF

Cloud security posture management (CSPM)

OVERVIEW

Proactively manage risk and compliance

To tackle the increasing complexity of securing cloud environments, many security professionals look to cloud security posture management (CSPM). The Lacework Polygraph® Data Platform provides CSPM capabilities that deliver much-needed automation to help organizations find and remediate risks, while simplifying compliance. Through a combination of automated compliance monitoring and security assessments, Lacework helps ward off dangerous breaches by continuously checking for misconfigurations.

For many organizations, CSPM is also a key tool for achieving business goals. Continuous compliance assessments enable businesses to provide assurance on the state of their security posture to auditors and customers, which can result in new business and revenue streams. Across numerous industries, organizations trust Lacework to help meet critical compliance standards while increasing their visibility, efficiency, and security.

THE LACEWORK SOLUTION

A solid foundation for cloud security posture at scale

Whether you're using Amazon Web Services (AWS), Microsoft Azure, Google Cloud, or a combination, Lacework can help. Lacework uses a single platform to ingest cloud activity logs from all three major cloud service providers, as well as Kubernetes configurations. We assess and continuously monitor the current state of your configurations to help you uncover risk and prove compliance.

As a first step, catalog your cloud resources and gain an inventory of what is deployed by your builders across multiple clouds. You can capture inventory daily to understand how your resources are changing over time by using the resource management functionality in the Lacework platform.

Challenges

- Constant changes in the cloud make it difficult to check for and address configuration modifications and drift
- Proving compliance to auditors and customers is time-consuming, resource-intensive, and costly
- Posture management and best practices built for on-premises architectures don't adapt well in the cloud — a different approach is needed

Lacework benefits for CSPM

- Gain holistic visibility into cloud assets, security configurations, and cloud activity
- Continuously monitor and validate posture against industry best practices
- Surface misconfigurations and gaps in security controls at scale
- Automate and prove compliance faster, reduce risk, and ensure security audits keep up with cloud changes

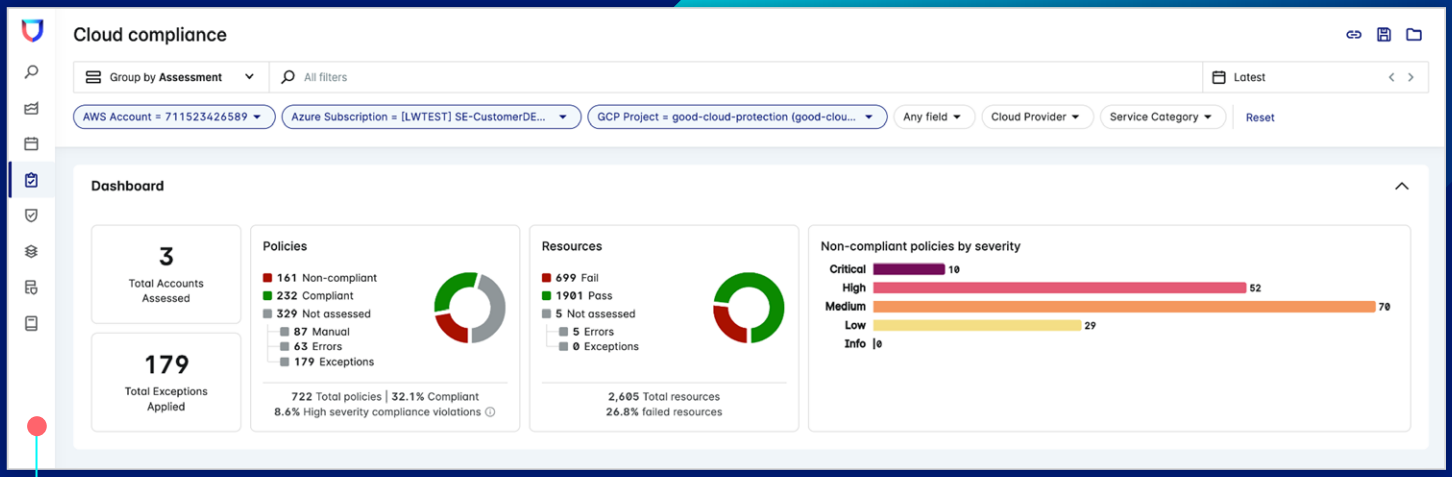
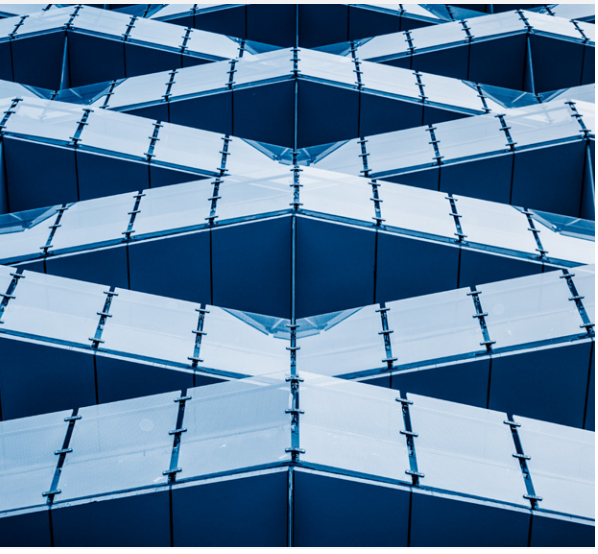


Figure 1: Understand your risk posture and gain a consolidated view of your compliance across all three major cloud service providers.

Key CSPM capabilities include:

- Automatically inventory cloud resources and understand when configurations change
- Continuously assess and validate your posture and compliance against security controls and key frameworks
- Assess risk, check for policy violations, and monitor for misconfigurations, including in infrastructure as code (IaC)
- Automate compliance reporting and generate necessary artifacts
- Monitor and evaluate cloud activity for abnormal behaviors



Continuous, automated compliance checks

Lacework validates your security posture against industry best practices and uncovers discrepancies between your current state and regulations, giving you confidence that you're meeting the correct security controls. Lacework helps organizations achieve a strong security posture and industry compliance by validating posture against the best practices from the Center for Internet Security (CIS). We map the CIS controls to a broad number of industry security benchmarks, with hundreds of pre-built policies. We support multiple security standards, including ones developed internally by Lacework. Use the cloud compliance dashboard for a unified view of your compliance across a multicloud environment.

To ensure your cloud follows the most recent security recommendations, Lacework policies and reports are quickly updated with the latest benchmarks after they are released. In addition, the Lacework AWS Security Addendum report contains 100 value-added policy checks that lend stricter controls for S3, IAM, and VPC policies, including resources on AWS GovCloud. You can view assessments per account or environment in an easy-to-understand user interface and identify resources that are not following best practices. We offer extensive push-button reports — including SOC 2, ISO 27001, PCI DSS, HIPAA, NIST 800, CIS Benchmark and more — in multiple formats to generate artifacts and help you rapidly prove compliance to customers, partners, auditors, and other stakeholders.

According to the Forrester Total Economic Impact Study, Lacework customers were able to avoid hiring an additional full-time employee specifically for compliance, resulting in $291K in savings over three years.[1]

Customized security posture

One size does not fit all. Lacework gives you customization to meet requirements specific to your organization that may not be covered in standard benchmarks. We offer custom policies for you to create fine-grained and accurate security assessments with ease across AWS, Google Cloud, and Azure. Using Lacework Query Language (LQL), you can define how configurations and access controls in your environment should behave and design a cloud operating model tailored to your business objectives and risk appetite. You can also generate custom CSPM reports across multiple accounts in a cloud service provider for the policies that are most relevant to your organization's security posture.

Misconfiguration checks

Lacework automatically monitors and and suspicious cloud activity in the cloud control plane. We offer rapid feedback when a misconfiguration or compliance violation arises, with context-rich recommendations on steps to take. You can accelerate your remediation efforts by integrating Lacework with tools such as Jira and Slack. In addition, our IaC scanning capabilities can help you to check for misconfigurations in IaC and resolve security and compliance issues at the earliest development stage.

Lacework IaC security automatically reviews and secures IaC as it is written, empowering developers to quickly identify and fix issues. Our IaC scanning capabilities work across Terraform, AWS CloudFormation, or Kubernetes/ Helm and require no special skills to use. Our platform automatically finds misconfigurations as developers submit IaC to a source code repository. We then alert developers of those risks within both the Lacework platform and the repository where the code was checked in and offer actions to remediate the issue.

> **"Lacework is a one-stop shop for security and compliance."**
>
> GOPI KRISHNAMURTHY, VICE PRESIDENT OF PRODUCT AND ENGINEERING, CLARINESS

Go beyond traditional CSPM

As you evolve and mature your cloud security practice, you'll need to move beyond prevention to detect and address suspicious cloud activity and potential threats across cloud accounts, services, and workloads. This requires deeper insights and the right context to understand what your users, entities, and resources are doing, and how they behave.

For example, by ingesting your audit logs into Lacework, you can continuously monitor activity and automatically detect abnormal user and resource activity, such as failed logins, IAM escalations, and more. Forget having to send all cloud audit logs to expensive SIEMs or write endless detection rules. Lacework pulls in AWS CloudTrail, Google Cloud Audit, and Azure Activity logs and uses patented Polygraph technology, which combines behavioral analytics and machine learning to detect abnormal activity from administrators or cloud resources.

You can also combine Lacework CSPM capabilities with our lightweight security agents for deeper telemetry and analysis of workload processes and anomaly detection. Lacework offers the full spectrum of build time and runtime capabilities to secure your build, cloud infrastructure, workloads, and data with ease.

> We have Lacework on our pipelines to make sure that how we deploy software, both for ourselves and for our customers, is compliant."
>
> STEVE COPPIN-SMITH, VICE PRESIDENT OF ENGINEERING, SNOWPLOW

Why Lacework?

- Gain full visibility into risks and threats with a single integrated platform that spans code to cloud and covers both control and data planes
- Have coverage across all hyperscale cloud providers, Kubernetes, hosts, containers, and more
- Leverage a range of capabilities including threat detection, vulnerability and configuration checks, compliance reporting, IaC security, and more
- Speed investigations with Polygraph visualizations to better understand what happened before, during, and after a specific event
- Leverage remediation guidance to quickly act on issues uncovered

Customer outcomes

- 86 percent of Lacework customers indicated that they'd gained a complete understanding of their cloud environment and the actions needed to include their security posture.
- John Turner, Senior Security Architect at LendingTree, was able to reduce alerts for his organization by 90 percent. Per Turner: "Lacework helped us deal with this firehose of information we were getting out of our cloud environment."
- Bren Biggs, Vice President of DevOps and Cybersecurity at Hypergiant, was able to bring his cloud environment up to NIST 800-171 standards by using Lacework to map the controls to his AWS environment. Hypergiant won $10M in new business as a result of achieving the needed compliance.
- Lacework customers reported 20 hours saved per week by eliminating manual security or compliance tasks.

Endnotes
1 Forrester Consulting, The Total Economic Impact of Lacework, 2022

Ready to chat?

Request a demo