SOLUTION BRIEF

Harnessing the power of data to automate cloud security

Lacework is a data-driven cloud security platform that delivers end-to-end visibility into what's happening across your cloud environment, including detecting threats, vulnerabilities, misconfigurations, and unusual activity. Lacework takes a different, rules-optional approach to cloud security across Amazon Web Services (AWS), Google Cloud, Microsoft Azure, workloads, containers, and Kubernetes to aid security and developer practitioners from both build to runtime.

Our foundational Polygraph® Data Platform ingests data, analyzes behavior, and detects anomalies across an organization's multicloud environment. This patented approach significantly reduces noise and turns millions of data points into prioritized, actionable events. Lacework can also be embedded into your continuous CI/CD pipelines for vulnerability scanning across hosts and container registries to identify vulnerable containers before they are promoted into production.

With Lacework you can:

- Automatically detect known and unknown threats across your cloud infrastructure, workloads, and application behavior
- Reduce costs associated with your legacy tools, like cutting your SIEM ingest spend by 20-40%
- Reduce toil and management time for cloud security, reallocating time to other high-value tasks
- Cut alert volume by 86% by automatically filtering out noise associated with informational and low critical alerts
- Improve the quality and speed of investigations by up to 80% with highly contextual alerting
- Drive streamlined workflows over cross-functional teams with an API-first platform and an extensible technology partner ecosystem
- Accelerate compliance audits with full visibility into your cloud infrastructure and workloads
- Consolidate multiple tools to simplify management tasks, accelerate workflows, and improve analytics efficacy by correlating across a single platform, and free up a limited budget

How the Lacework Polygraph Data Platform works

Collect

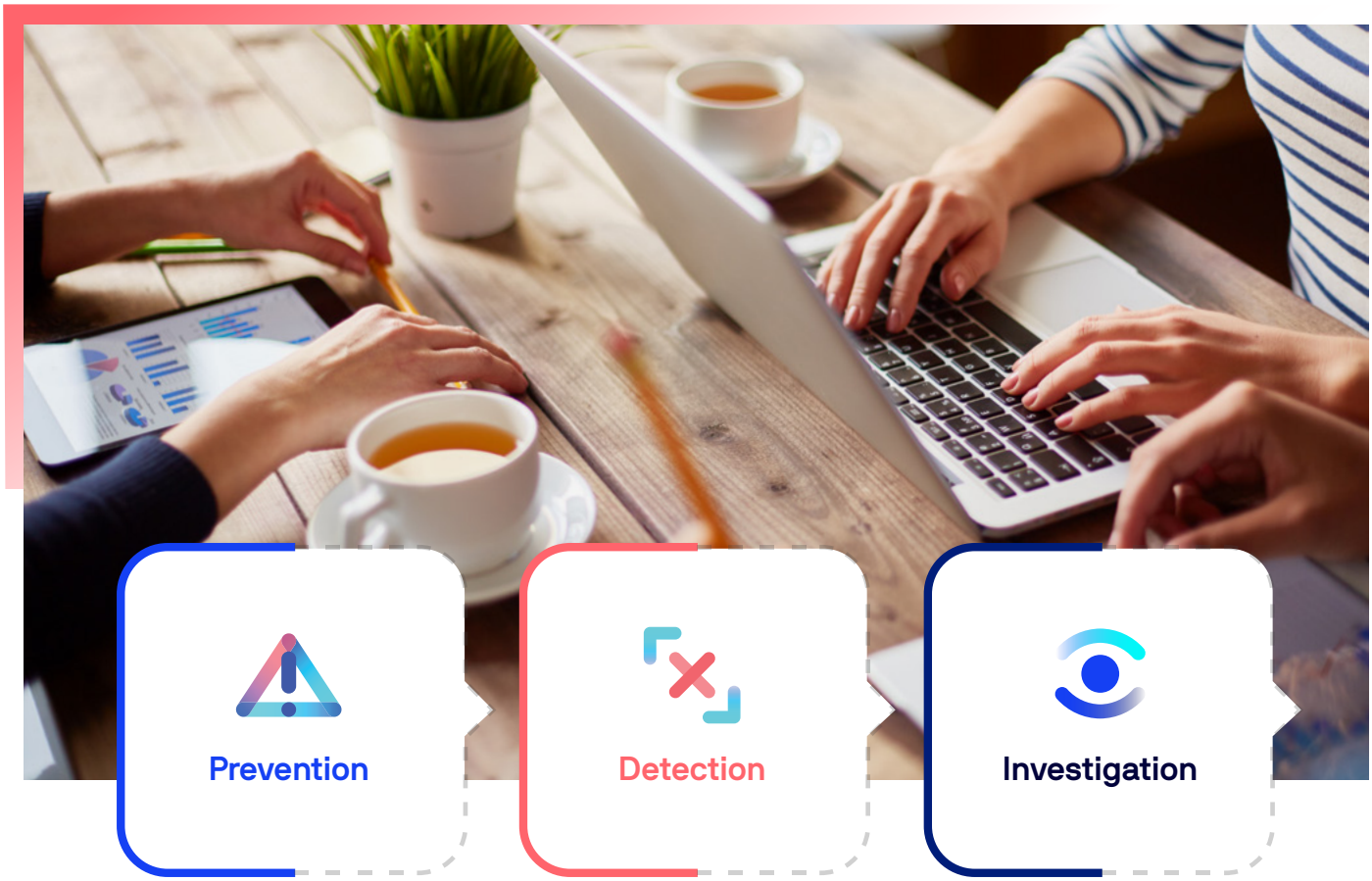
- Support AWS, Google Cloud, Azure, Kubernetes, and hybrid environments
- Get complete cloud account asset inventory via agentless approach
- Get data on cloud workloads via agent
- Continuously monitor user, app, process, and network behavior, plus vulnerabilities and cloud configurations

Detect

- Uncover unusual activity that could indicate compromise, like escalation of privileges, with patented Polygraph anomaly-based approach
- Discover vulnerabilities in build time and runtime
- Find cloud misconfigurations like exposed assets
- Identify when cloud best practices and compliance requirements are not met

Inform

- Eliminate alert fatigue and surface only the most critical risks
- Respond quickly with context-rich visualizations and notifications
- Create detailed reports for compliance
- Get precise information to integrate with ticketing, messaging, security information and event management (SIEM), and workflow applications to accelerate developer action



Lacework focuses on four primary cloud challenges from our Cloud Workload Protection Platform (CWPP) to Cloud Security Posture Management (CSPM) that assist customers in prevention, detection, and investigation with our automated security monitoring. Below are details of Lacework's integrated platform:

Configuration compliance (CSPM)

Prevent threat actors from exploiting misconfigurations throughout your multicloud infrastructure control plane. Maintain cloud configuration compliance with continuous monitoring and reporting against common cloud configuration security controls.

Cloud API and user activity

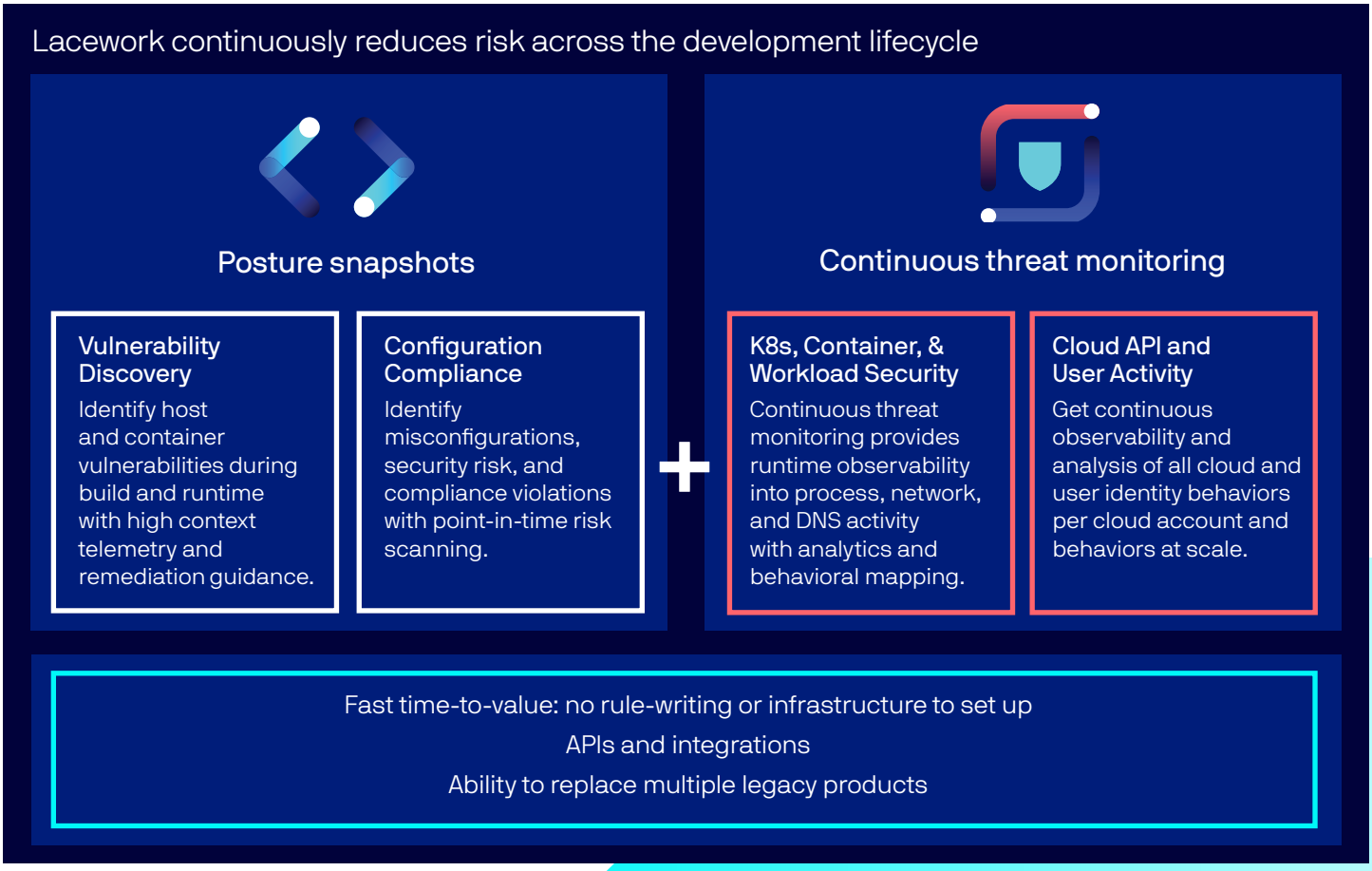
Detect and investigate unknown threats across your entire cloud infrastructure control plane by continuously monitoring customers' cloud user and entity activity, modeling normal behaviors, and automatically identifying threats at scale.

Vulnerability discovery

Prevent exploitation of known operating system (OS) and third-party package vulnerabilities across your fleet of hosts and containers in the cloud by identifying these vulnerabilities across build time and runtime with high-context telemetry and remediation guidance.

K8s, container, and workload security (CWPP)

Find and fix known and unknown threats across your cloud workloads by monitoring application runtime process execution and network traffic activity across your containers and hosts, modeling normal behaviors, and automatically identifying known threats with indicator blacklists and unknown threats specific to your organization's environment at scale.



Deployment and integrations

Lacework simplifies customer deployments and can be deployed to even the largest and most complex customer cloud environments **in minutes, not weeks.** We offer a simple, layered deployment approach that combines static risk posture with continuous threat detection by providing you both agentless and agent-based data monitoring. And by seamlessly integrating with tools you already use, we empower your security and DevOps teams to collaborate and maximize efficiency.

How to get started with Lacework

CSPM: Terraform for Lacework Overview

CWPP: Agent Installation Options

Extending Lacework:

CLI: Install and Configure the Lacework CLI

In-Line Scanner: Integrate Inline Scanner

Alert Channels: About Alert Channels

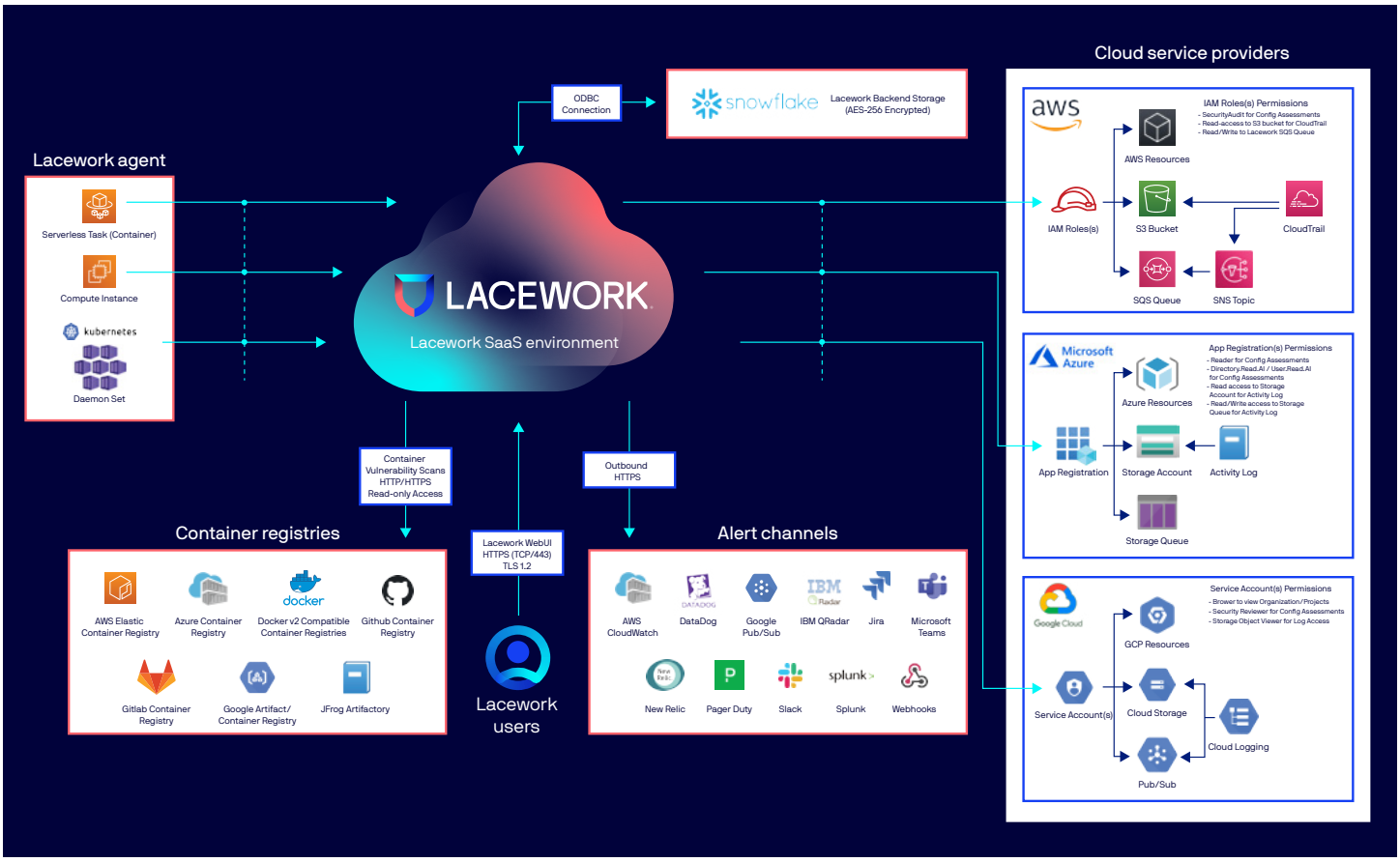


Diagram 2: Lacework solution diagram and non-exhaustive container registry + alert channel integration paths.

Example Lacework use cases by category

Quickly identify active and externally facing hosts and containers with known vulnerabilities.

Cloud API and user activity

- Identify new or anomalous activity correlated across an entire cloud account, including regions, users/ principals, CSP services, API calls, API responses, and more.
- Trace cloud account activity and resources across the control plane back to the originating calling resource or principal.
- Get contextual, event-driven incident reviews with filtering capabilities that provide a deep and efficient understanding of events and cloud workflows.
- Report on failed API or resource access along with custom query capabilities to extend out-of-the-box reports.

Cloud compliance (CSPM)

- Enjoy complete visibility across cloud accounts and CSPs for resources that are out of compliance, along with inventory visibility.
- Demonstrate compliance with out-of-the-box reporting on common cybersecurity frameworks and compliance standards such as HIPAA, PCI DSS, NIST 800-171, NIST 800-53, ISO 27001, SOC 2, and CIS Benchmarks.
- View historical reporting for configurations and changes for up to 6 months.
- Run automatic daily checks across all accounts, or on-demand scans as required.
- Receive fully exportable compliance reports from both the UI and CI/CD tooling.

Visibility and security across containers and workloads (CWPP)

- Automate detection of running applications and correlation of relationships within the environment.
- Identify hosts and containers with unknown or suspicious processes and correlate across known IOCs and threat feeds.
- Get best-in-class HIDS capabilities, including FIM, anomalous process detection, signature-based attacks, and privilege escalation.

Build time and runtime vulnerability detection

- Identify both hosts and containers with known active vulnerabilities.
- Integrate with container registries for vulnerability scanning and reporting.
- Catch misconfigurations before containers are deployed into production with IaC scanning capabilities.

Supported environments

- CSPM: AWS, Google Cloud, and Azure
- CWPP: Any supported Linux operating system and Kubernetes runtime, cloud, or on-prem

Want to see what operating systems Lacework supports?

See our list of agent-supported operating systems.

Want to know more?

Reach out to your local sales team for more information or browse our FAQ.

Platforms we support

aws
Google Cloud
Azure
docker
kubernetes
ubuntu
Linux
CoreOS
rackspace

Ready to chat?

Request a demo

Are you an existing customer? You can now find Lacework in the Google Cloud Marketplace!