SOLUTION BRIEF

Find known and unknown threats faster

React quickly to real cloud security threats

OVERVIEW

As more organizations embraced the cloud, cybercriminals saw it as a lucrative target. To curb the spike in threats, organizations initially deployed their traditional on-premises detection and response solutions to help protect against threats inside cloud software. However, these "solutions" also introduced a whole new set of problems for security teams.

The security rules that historically powered detection solutions in traditional infrastructures, for example, were no match for dynamic cloud environments. Make the rules too broad, and you're receiving hundreds — possibly thousands — of alerts per day. Make the rules too narrow, and these solutions can't properly function. Security alerts were also of limited use. A lack of alert context made threat investigation a pain. And a lack of prioritization left teams guessing which alerts were most important.

The cloud demands more than what traditional security approaches can offer. The Lacework platform uses automation to analyze data from all across your environment and, ultimately, take the pain out of threat detection.

THE LACEWORK SOLUTION

The Lacework platform offers both agentless cloud control plane protection and agent-based workload protection across Amazon Web Services (AWS), Google Cloud, and Microsoft Azure. Lacework also monitors cloud activity in virtual machine (VM) workloads and containerized workloads, including Kubernetes (K8s), Google Kubernetes Engine (GKE), etc. At Lacework, we can help you reduce threats and gain a comprehensive view across multiple clouds in a single platform.

Lacework uses a combined agentless and agent-based approach to gather the right level of information from cloud provider APIs, as well as telemetry directly from your workloads with our lightweight, proven agent. Our agentless solution detects attacks, misuse, and misconfigurations in cloud accounts, while our agent-based approach monitors for workload vulnerabilities and for known and potential threats related to users, applications, network connections, and files. This method provides greater visibility to your assets, their connections, and their compliance with industry, governmental, and institutional standards from build time through runtime.

Challenges

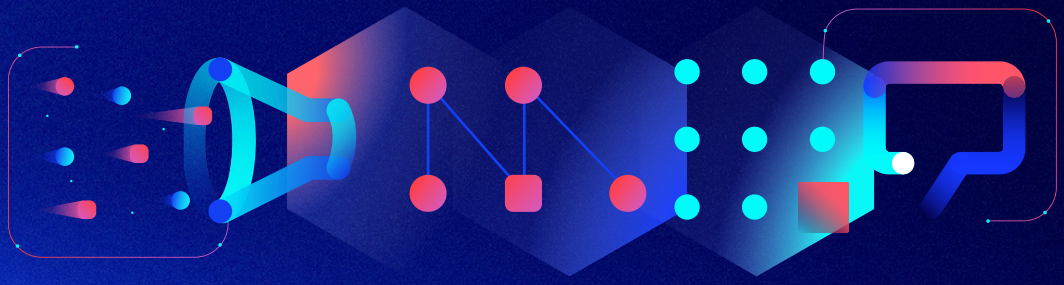
- Unable to detect unknown, ever-evolving threats
- Drowning in alert fatigue: Full alert queues hide critical issues
- Limited resources and security expertise to hunt for threats and maintain security rules
- Fragmented data across cloud providers, services, and technologies make investigations a pain

Lacework benefits

- Secure by design: Your data never leaves your environment
- Uncover threats earlier without excessive querying and significant expertise
- Protect your brand and revenue by reducing severity and scope of a major breach
- Reduce time spent managing alerts, freeing up time for more strategic work

The power of the Lacework platform

The Lacework platform ingests data, analyzes behavior, and detects anomalies across an organization's Amazon Web Services (AWS), Google Cloud, Microsoft Azure, and Kubernetes environments without relying on rules. This patented approach significantly reduces noise and turns millions of data points into prioritized, actionable events.



Ingest

The platform collects data via agentless and agent-based approach on activity related to:

- API calls
- User behavior
- Application launches
- Running processes
- Network behavior

Analyze

The platform's anomaly detection engine uses data to:

- Create groups for analysis
- Create baseline from activity

Detect

The platform's anomaly detection engine detects changes and risks to:

- Identify unusual behavior
- Identify malware from threat feed

Inform

Platform visualizations and alerts provide context to:

- Investigate more quickly
- Integrate with response tools

Anomaly detection

The Lacework platform delivers automated anomaly detection to detect threats in multicloud environments, whether or not they're known. The patented anomaly detection technology is fed by multiple distinct data sets, including activity data from an extremely lightweight agent and agentless cloud activity log data from your cloud providers. The platform continuously analyzes hundreds of terabytes of data around processes, applications, APIs, files, users, and networks. Machine learning is combined with behavioral analytics to correlate and analyze these disparate datasets, building a baseline for your normal cloud activity. Then any abnormal activities that fall outside of that baseline are surfaced and labeled, based on criticality.

This layered approach discovers new behaviors without the need for human intervention. The platform takes a data-driven approach to security; the more data the platform analyzes, the smarter the platform becomes. This automated intelligence drives better efficacy and a higher return on your investment.

> "[Lacework] has freed up my team from spending 2-3 hours a day configuring, tweaking, and looking at alerts to less than 15 minutes. It's freed up so much time to do other things that are security related."
>
> MARIO DUARTE,
> DIRECTOR OF SECURITY, SNOWFLAKE, INC.

Composite alerts

Lacework composite alerts automatically combine multiple detections to define more specific alert conditions without excessive querying or significant expertise and effort. The platform can accurately detect active cloud attacks by automatically combining multiple low severity alerts that often go unnoticed by security teams into a single, meaningful alert.

To date, Lacework composite alerts have detected attacks like cloud ransomware, cryptomining, and compromised credentials. When applicable, composite alerts also integrate Amazon GuardDuty findings to enrich evidence of an ongoing security issue. This allows users to gain greater insights from a single location without the need to correlate data from multiple products.

Alert context and visualizations

As threats are surfaced, security event details are provided in a comprehensive event card that displays the who, what, why, where, and when of each event. This information includes the user name associated with the event, machine details, process-related information, any related alerts, and more. This rich context is sourced and organized from cloud audit and configuration data, workload context from its agent, and agentless vulnerability and security scanning.

These alert cards also include visualizations to arm you with rich context so that you can quickly investigate and remediate issues. By analyzing audit log and workload data, the Lacework platform builds detailed visualizations that can track network, application, process, and user activities across hosts. Security analysts can then zero in on any suspicious activity, trace an intruder's steps, and remediate the situation.

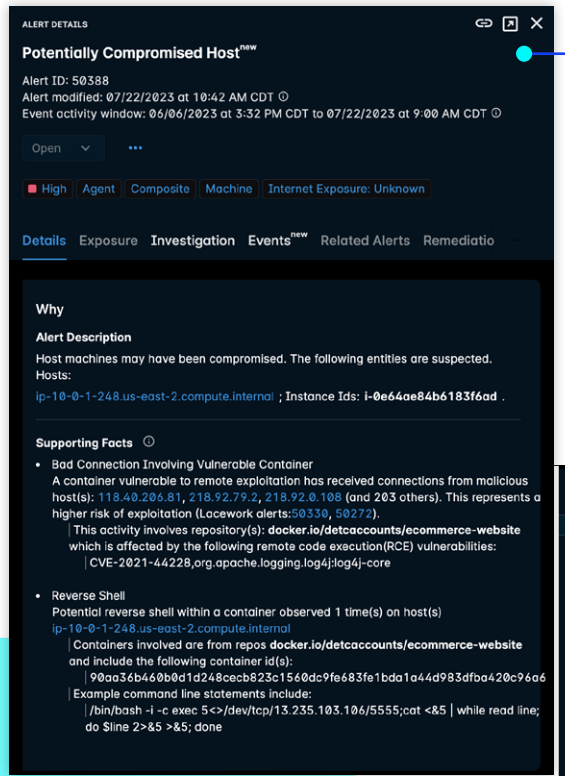


Figure 1: Lacework composite alerts compile multiple low severity alerts into a single high severity alert, pointing to potential malicious activity.

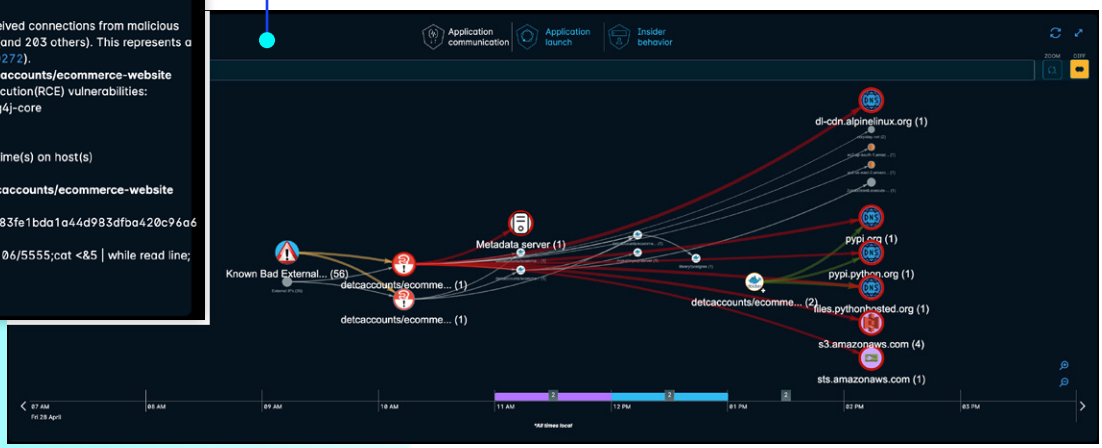


Figure 2: Lacework maps out all activities and communications throughout your cloud environment. These visualizations automatically highlight any anomalous activities hour-by-hour and can track cloud exploits from the malicious source through the vulnerability to any affected cloud entities.

Continuous file integrity monitoring (FIM)

The Lacework platform can monitor for changes in files and directories in near-real time. Lacework users can choose to watch for file/directory creation, deletion, modification, and move or attribute changes in specific folders or on specific files. This way, security analysts can monitor critical files or directories for change control, files for indications of tampering, and directories for evidence of malware activity.

A deep network of integrations

Lacework is easy to operationalize due to its large roster of integrations with other workflow tools. Our integration partners include (but are not limited to):

- **Monitoring / logging tools** (e.g., Splunk, Snowflake, and New Relic)
- **Incident response / ticketing tools** (e.g., Splunk, Jira, PagerDuty, and ServiceNow)
- **Messaging tools** (e.g., Slack)
- **Remediation / compliance tools** (e.g., Kaholo and Tines)
- **Developer tools** (e.g., Buildkite, Puppet, Chef, and Hashicorp)

Each alert within Lacework is actionable because of its detailed alert context. The platform integrations ensure that each of those actionable alerts are seamlessly routed to the right tools for next steps.

> “When we get an alert through Lacework, we have the ability to see who did it, why the signal fired, what all the API calls are, and where it happened. The evidence is easy for pretty much anyone to understand.”
>
> MICHAEL LYBORG, CISO, SWIMLANE, INC.

“It took maybe four clicks, and you wait five minutes, and boom, the accounts are recognized and Lacework is now ingesting all cloud trail data. It was mind-blowing.”

GARY TSAI, APPLICATION SECURITY ENGINEER, MARQETA

Why Lacework?

Prioritize cloud security risks with visibility and context

Quickly gain complete visibility into deployments, configurations, and workloads to pinpoint and prioritize the most critical vulnerabilities and misconfigurations for remediation.

Find known and unknown threats faster

Discover threats within your dynamic cloud environment with anomaly detection and threat intelligence. Gain rich context surrounding each alert to promptly investigate and remediate cloud security issues.

Increase operational efficiency

Accomplish more with less and know where to focus. Lower the total cost of ownership through a single platform and improve time to value with automated, DevOps-friendly cloud security.

Achieve continuous compliance

Prove and maintain continuous compliance across your entire cloud estate for requirements like SOC2, ISO 27001, HIPAA, and more. Automate audit requests and free up time for high-value security tasks.

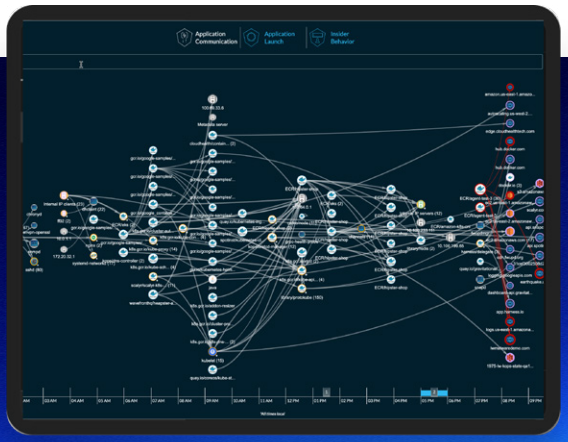
Customer outcomes

- 100:1 reduction in alerts
- 95% reduction in false positives
- 90% reduction in manual cloud security tasks
- 81% of customers see value in < 1 week

See it in action.

Request a demo

Read about our layered security approach



LACEWORK

 | 888.292.5027 | lacework.com

09/23