SOLUTION BRIEF

Monitor your data, wherever it lives

A single platform for visibility into hybrid environments

Overview

Cloud migration is speeding up. According to McKinsey, large enterprises aspire to have roughly 60% of their environment in the cloud by 2025[1]. Yet tomorrow is not today. Today, greater than 55% of workloads still run in on-premises data centers[2]. Some estimates claim over 70% of organizations are operating in some sort of hybrid environment made of some mix of public clouds, private clouds, and/or on-premises infrastructure[3].

Even though companies' most sensitive data often resides on-premises, an overemphasis on cloud computing has left traditional infrastructures neglected. The innovation of modern security solutions has mostly been reserved for the cloud, often leaving on-premises teams with aging and outdated legacy capabilities, ill-equipped to handle modern threats. Also, the actual task of cloud migration often leaves data at risk, as siloed security tools leave visibility gaps when data is migrated from place to place.

The Lacework solution

The Lacework platform offers unified visibility and security for hybrid environments, bridging the gap between on-premises and cloud workloads. The platform maintains this visibility even as data moves from on-premises environments to cloud environments. Both cloud and on-premises workloads benefit from modern security features within the platform, including its advanced threat detection, which uses ML-based anomaly detection to pinpoint known and unknown threats. Since Lacework was built for the cloud, its security agent is extremely lightweight, scalable, and manageable, especially when compared to traditional on-premises security agents. By unifying protection across diverse environments, Lacework ensures simple consistent risk management and workload monitoring, unifies security teams, and offers seamless visibility wherever the data resides.

CHALLENGES

- On-premises workloads are often secured by outdated legacy technologies that are incapable of detecting modern threats
- Siloed processes and technologies cause rifts within security organizations
- Security teams lose visibility of sensitive data when moved to the cloud
- Traditional on-premises security solutions often lack visibility into Kubernetes

LACEWORK BENEFITS

- Consistent visibility into risks and threats across both cloud and on-premises environments, even as data migrates from place to place
- Lightweight, scalable, auto-updating agent that can be deployed across both cloud and on-premises environments
- Full visibility into Kubernetes workloads, whether cloud or on-premises

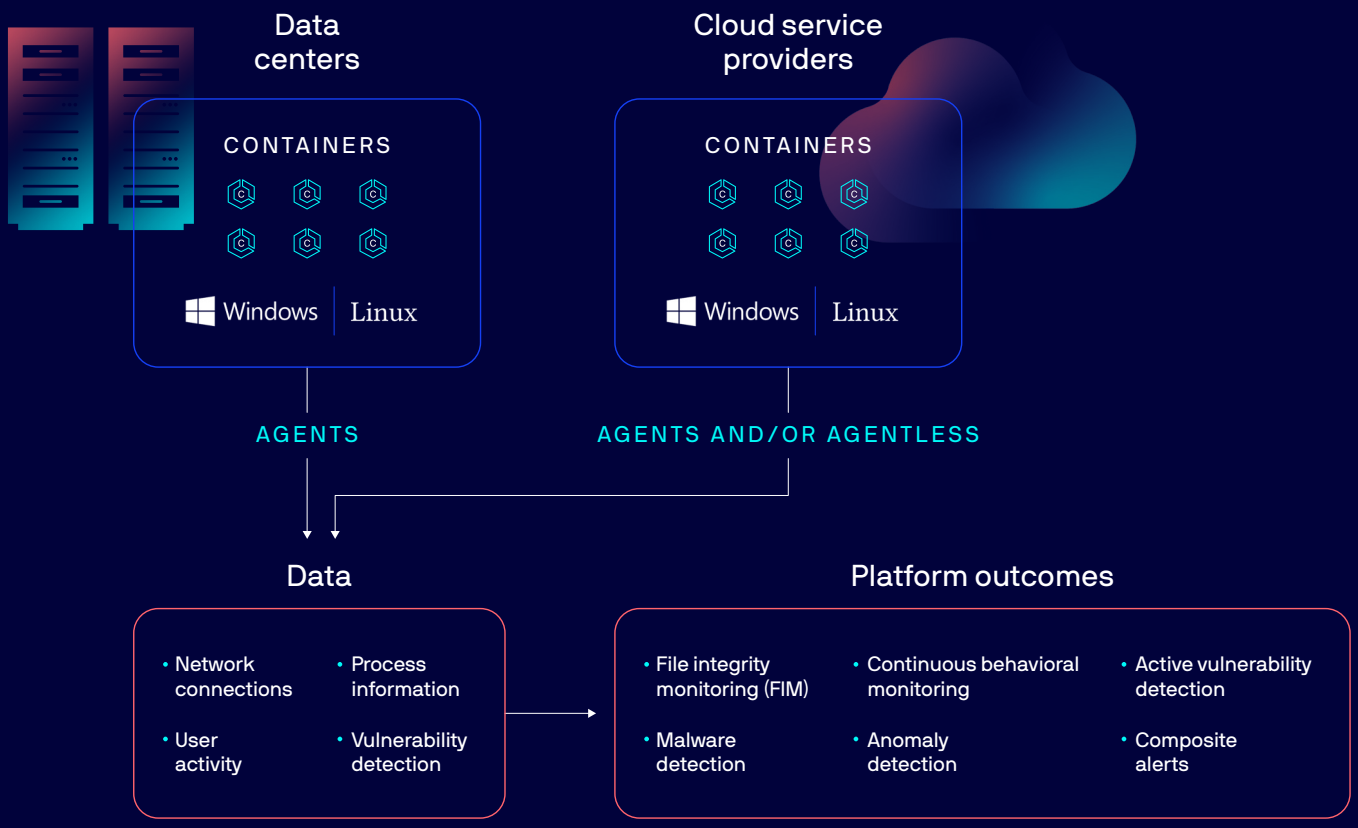


Figure 1: Lacework analyzes data from both cloud and on-premises environments in a single platform and produces security outcomes to safeguard against modern risks and threats.

A lightweight, stable agent

The Lacework platform boasts one of the most lightweight security agents in the industry, stable in both cloud and on-premises environments. The agent supports every major Linux distribution, Windows servers, every major container runtime, every major container orchestrator, and serverless runtimes like Amazon Fargate and Google Cloud Run. With the Lacework agent, fleet management is simple; the agent is extremely scalable and auto-updates, which means minimal maintenance for teams as environments grow or shrink.

Our agent was designed to consume the least amount of CPU while analyzing as much data as possible. It collects essential data without causing system disruptions, providing a clear view of what's happening in real-time. The Lacework agent intelligently observes, filters, aggregates, deduplicates, and compresses data that feeds into the unified knowledge graph, which in turn powers runtime alerting and enriches context across various findings and alerts, including vulnerability management.

Active vulnerability detection

Without the right tools, when a security team notices an application vulnerability, it's difficult to determine whether that issue in the package is actually tied to running software. Flagging inactive vulnerabilities to developers can ultimately waste time for development teams, which can naturally lead to friction with security teams.

Using active vulnerability detection from our agent, you can automatically identify vulnerable software packages that are active. This capability, which is compatible with Linux workloads, significantly reduces noise from inactive vulnerable packages and refocuses developer time on work that creates value for the business. This capability gives teams the context to determine the most important items to fix that will reduce their overall risk, instead of spending time fixing vulnerabilities that don't really matter.

Known and unknown threat detection

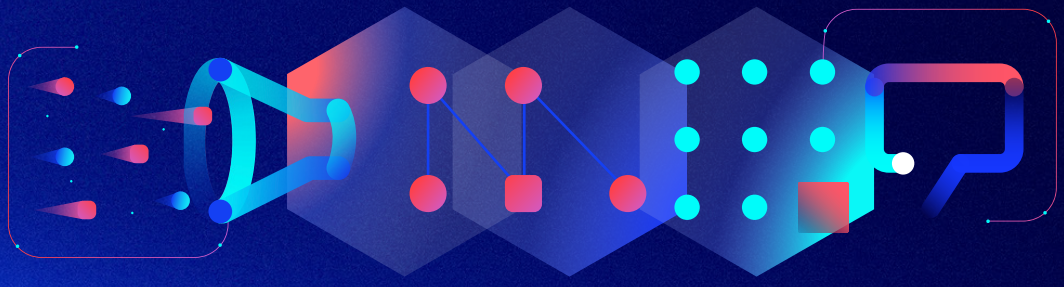
The Lacework platform delivers automated anomaly detection to detect threats in hybrid environments, whether or not the threats are tied to known rules or signatures. Through agent-based and agentless data ingestion methods, the platform continuously analyzes hundreds of terabytes of data around processes, applications, APIs, files, users, and networks. Then our patented ML-based anomaly detection technology correlates and analyzes different datasets, building a baseline for normal activity. After that, any abnormalities 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.

> **"By adopting a single platform, we fully eliminated five tools, which has saved us valuable time and reduced our costs."**
>
> HANS-MICHAEL ODENTHAL, SYSTEMS EXPERT, AOK SYSTEMS GMBH

The power of the Lacework platform

The Lacework platform ingests data, analyzes behavior, and detects anomalies across an organization's hybrid environment 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 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 baselline 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

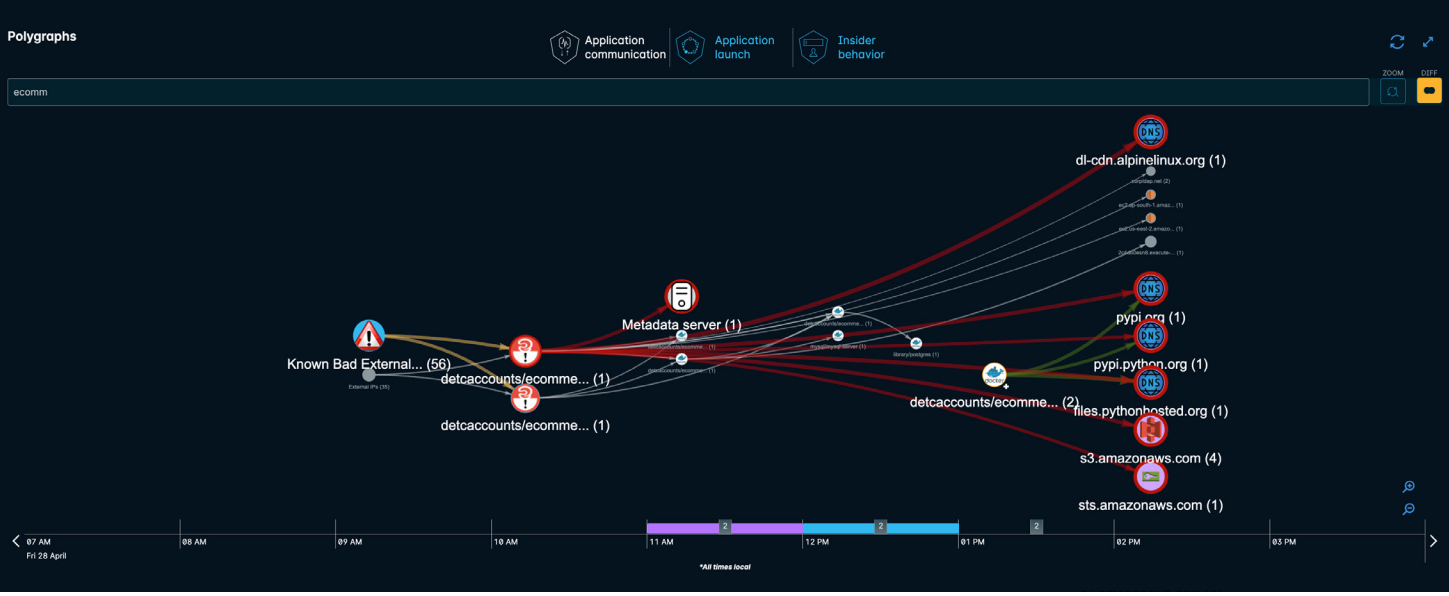


Figure 2: Lacework maps out all activities and communications throughout your hybrid environment. These visualizations automatically highlight any anomalous activities and can track cloud exploits from the malicious source through the vulnerability to any affected cloud entities.

Advanced host intrusion detection (HIDS)

Within the Lacework platform, security teams can monitor activity within hybrid environments in a number of different ways. Lacework offers continuous file integrity monitoring (FIM), where the platform monitors 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.

The Lacework platform also offers deep network and process monitoring. As our platform analyzes your cloud and on-premises data, it plots a detailed map of your network and process activity. Then, as abnormal activity occurs, the platform clearly marks these activities as anomalous and allows users to track how this activity has moved throughout your environment.

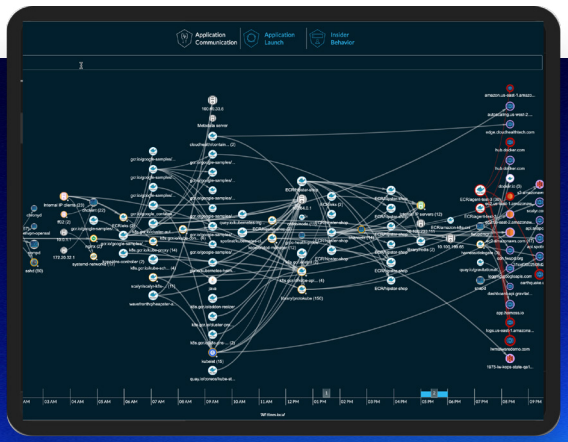
Low maintenance, high impact

Since Lacework is a software as a service (SaaS) platform, teams experience all the benefits that come with a cloud-hosted application, whether their data is in the cloud or on-premises. The platform is accessible from the internet, which means ubiquitous access from anywhere in the world, and its components (including its agent) can be auto-updated and are simple to maintain, which means a lighter lift for security admins.

An added benefit of using Lacework across hybrid environments is security team development. By having on-premises and cloud security teams working within the same platform, security personnel working on traditional infrastructures can begin to upskill for the cloud. Lacework can develop these teams into cloud security admins, as they'll be encountering cloud data and cloud concepts on a daily basis.

Ready to chat?

Request a demo



Footnotes:

1. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/projecting-the-global-value-of-cloud-3-trillion-is-up-for-grabs-for-companies-that-go-beyond-adoption
2. https://www.oreilly.com/radar/the-cloud-in-2021-adoption-continues/
3. https://info.flexera.com/CM-REPORT-State-of-the-Cloud-2023-Thanks