Vulnerability management for cloud computing

LACEWORK

Overview

Cloud computing provides limitless potential for organizations to develop faster, more cost-effectively, and at scale. It creates an environment that empowers employees to innovate, but unfortunately the current security measures leave gaps that place data at risk. Customers are inundated with software vulnerabilities that affect their applications. In many cases, customers incur risk from 3rd party software they don't touch, yet still needs to be remediated. The delicate dance of DevOps taking advantage of the productivity benefits of Infrastructure as Code (IaC) must be balanced with the ability to provide security teams visibility and context in order to project risk.

Customers are seeking security solutions that help them manage the scale and complexity of their cloud environments and guard against threats such as ransomware and zero day vulnerabilities. Continual end-to-end monitoring of cloud runtimes using a data-driven approach is the best way to help organizations of any size assess, prioritize, and manage vulnerabilities to reduce risk.

LACEWORK

Challenges

Companies often sacrifice security for expediency. As the pace of innovation increases, cloud security has fallen short. Security professionals are left overwhelmed, uncertain, and without the visibility they need to protect their organization's security posture and every stage of the development cycle and supply chain.

Part of the problem is the sheer amount of vulnerabilities— both known and unknown—that can exist. According to the Clearpath survey commissioned by Lacework, the greatest security risk organizations face is "vulnerabilities we aren't aware of." **37% cite unknown vulnerabilities as the greatest risk to an organization.**[1]

Security teams are left in the dark and often don't know where infrastructure is deployed, what operating system is being used, package versions, and more. A steep rise in vulnerabilities and sophisticated attacks pose risks to diverse cloud entities like cloud VMs, hosts, containers, and functions. Traditional security tools and workflows cannot keep up with the sheer volume and fail to provide an accurate measure of "true" risk.

Improving cloud security is the top priority for organizations over the next six months, according to the Clearpath survey. A shortage of skilled professionals has impacted the ability to keep abreast of a dynamic threat landscape, and teams are facing burnout. One widespread problem is IT and security practitioners are constantly chasing alerts of intrusions that turn out to be nothing. **80% say at least 1-in-5 critical alerts is a false positive.**[2] If organizations could eliminate false positives they would have more time to focus on real threats, core work, and innovation.

37% cite unknown vulnerabilities as the greatest risk to an organization.

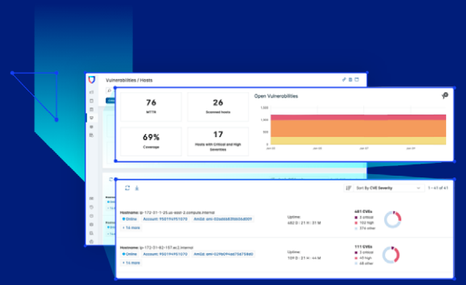
80% say at least 1-in-5 critical alerts is a false positive.

Lacework simplifies vulnerability management

Lacework offers a fast and scalable vulnerability management platform that integrates insights from build time to runtime to enable customers to separate “real” vulnerability risks from the noise. By using machine learning and artificial intelligence to automate tasks, it helps teams to deal with the shortage of IT and security staff, and frees employees to devote time to more valuable work. This end-to-end vulnerability management enables you to proactively manage risk across your hosts, containers, and cloud infrastructure. Lacework delivers insights that can be used for policy-based alerting and admission control in the continuous integration and continuous delivery pipeline, securing innovation while staying ahead of vulnerabilities.

LACEWORK

Lacework: collect, detect and inform



Collect

Broad data collection significantly increases visibility into the attack surface.

- Get data on containers and hosts with our combined agentless and agent approach.
- Monitor continuously for vulnerabilities from build time to runtime.
- Support AWS, Azure, Google Cloud, and Kubernetes environments.
- Support OS packages, Java, Python, Node, and PHP language libraries, plus distroless images.

Detect

Strong performance in synchronous CI/CD and asynchronous registry-based scanning modes to support sensitive response times.

- Check container images in build time with an inline scanner that integrates with continuous integration (CI) tooling.
- Block or notify when container images do not meet security standards prior to production with our admission control for Kubernetes.
- Continuously monitor all images in your registries for vulnerabilities.

Inform

Deep in-product workflows and provide filtering, grouping by host and CVE, and MTTR for resolved vulnerabilities.

- Provide detailed info to create remediation tickets for developers.
- Capture record of all open and previously fixed vulnerabilities.
- Provide a risk score with actionable risk-related insights unique to your environment.
- Ensure SecOps remediates highest risk items based on active/running status of hosts, images, packages, and containers (future).

LACEWORK®

Lacework differentiators

Traditional security solutions do not scale well for cloud-born companies that build and deploy at a high velocity. Lacework shift-left security strategies work better than traditional scanning solutions to find more vulnerabilities faster, with simpler management. Lacework provides board coverage on commonly used operating systems for cloud-based public sources including NVD, OS vendor advisory. Lacework supports multiple scanning capabilities to ensure DevOps and SecOps know exactly which risks to remediate to eliminate disruption to the business.

Host vulnerability scanning

Ensure that host weaknesses are made visible and patching is prioritized based on risk, using details around fixability, severity, and CVSS scores.

Container image registry cloud scanning

Access public registries and continuously scans container images for vulnerable packages and libraries, with a cloud scanner that uses cross account trust.

Private image registry cloud scanning

Scan private registries and ensure sensitive applications and images have minimal public access with a proxy-scanner that offers auto-poll and registry notification.

Container image CID/inline scanning

Integrate the inline scanner to detect and report for vulnerability risks as a part of their build process, shifting security practices left.

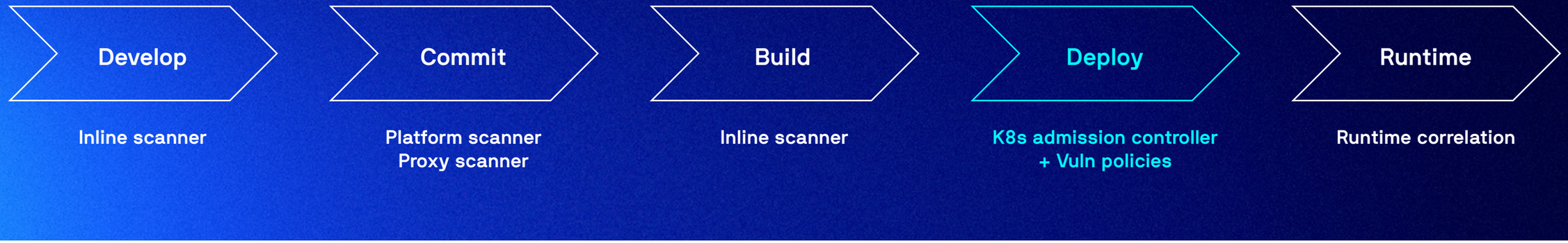
LACEWORK

Securing the supply chain

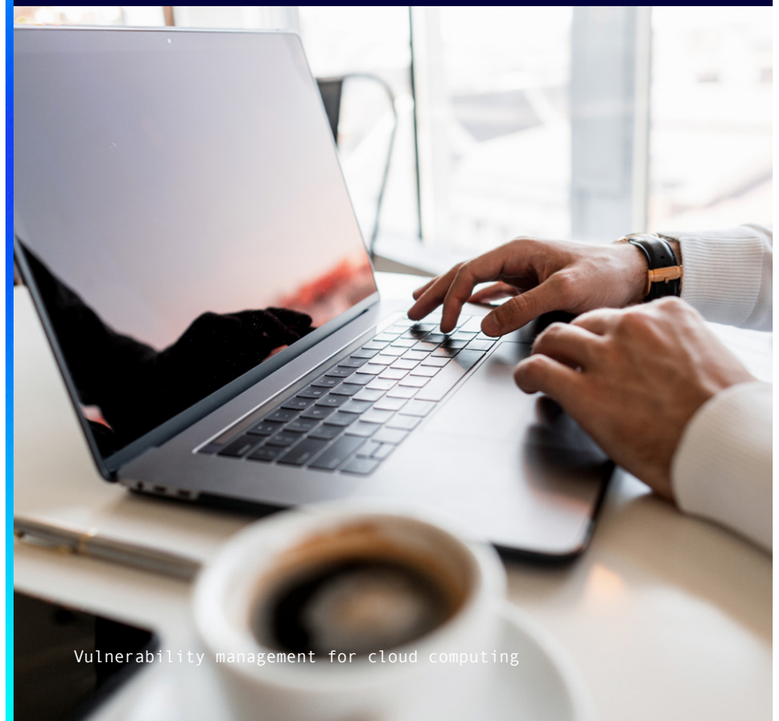
For container image scanning, Lacework offers a wide range of form factors that can be used for supporting every stage of the software supply chain. Integrations include:

- Inline scanner with CI/CD pipelines to support shift-left security strategy
- Proxy scanner for better control on where container image contents are scanned
- Platform scanner for absolute ease (auto-poll, registry notifications)
- Admission controller for a policy driven allow/fail mechanism of container deployment in K8s environments

Lacework associates vulnerability risks with runtime context. This enriches information to alert on anomalous activities associated with vulnerable hosts and containers. Lacework integrated vulnerability alerts work with other workflow management tools like ServiceNow and Jira.



> “Lacework was crucial to helping us quickly determine our exposure to Log4j, and as a result, we were able to maintain transparency and open communication with our customers in real-time.”
>
> DAVID TING, CHIEF INFORMATION SECURITY OFFICER, NYLAS



A rise in vulnerabilities, a closer look at Log4j

The Log4j vulnerability discovered in December 2021 began as a zero-day threat. News quickly spread through the cybersecurity community about a flaw in a popular piece of code that could allow bad actors to insert malicious code and seize control of servers. **Lacework was able to identify anomalous behavior in customer environments before the vulnerability was even disclosed.** Lacework combines agentless and agent-based approaches to eliminate reliance on snapshots of data that miss important activity and information. The Lacework anomaly detection leads to fast remediation for zero-day threats.

The latest Lacework agent includes application vulnerability discovery for containers, hosts, and virtual machines, tying together Log4j vulnerability data and anomaly detection. Not only can Lacework customers better prioritize remediation efforts, they can actively watch for exploits targeting those Log4j vulnerable systems - including those stemming from commercial, off-the-shelf tools they don’t control.

Automation paves the way to better cloud security

As companies migrate data to the cloud and adopt digital strategies that match this new reality over the next few years, they will find themselves vulnerable to criminals and malicious actors who seek to disrupt operations and steal data. As a result, businesses must find ways to protect data and secure systems without impeding innovation.

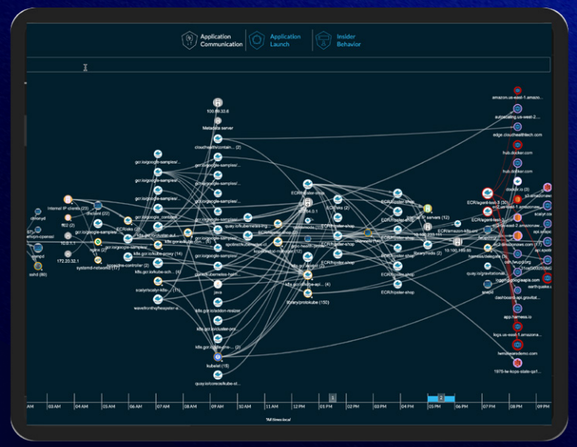
Companies that invest in data security and balance security with innovation from development to production will win more customers, more readily report compliance, and create a culture that minimizes risk to the business. Companies that trust machine learning and artificial intelligence to automate tasks will find relief from staffing shortages and burnout. Automation will free developers, security engineers, and DevOps practitioners to focus their time and energy on more than just chasing the next big vulnerability.

Take the next step

Lacework provides insights into vulnerabilities and misconfigurations for developers, as well as an inventory of cloud assets, compliance checks, monitoring of cloud configuration, and cloud account threat detection.

Let Lacework do the heavy lifting to stop vulnerabilities in their tracks so you can focus on more strategic projects. Eliminate the stress of worrying about exploits tied to vulnerabilities that have not yet been discovered. Lacework will help you to not only detect vulnerabilities, but will continuously watch for exploit activity at runtime.

LACEWORK



Ready to chat?

Request a demo

Lacework delivers security and compliance for the cloud generation. The Polygraph® Data Platform is cloud-native and offered as-a-Service, delivering build-time to run-time threat detection, behavioral anomaly detection, and cloud compliance across multi-cloud environments, workloads, containers, and Kubernetes. Trusted by enterprise customers worldwide, Lacework significantly drives down costs and risk, while removing the burden of unnecessary toil, rule writing, and inaccurate alerts. Lacework is based in San Jose, California, and backed by Sutter Hill Ventures, Liberty Global Ventures, Spike Ventures, the Webb Investment Network (WIN), and AME Cloud Ventures.

Get started at www.lacework.com

LACEWORK®

Sources

1-2 2022 Cloud Security Outlook https://info.lacework.com/cloud-security-outlook-report.html?utm_source=website&utm_medium=blog&utm_campaign=lightning-strike