SOLUTION BRIEF

Kubernetes security

Gain control of K8s environments through an innovative end-to-end security platform

Overview

Kubernetes (K8s) environments present unique security challenges. They are complex and ephemeral and can generate a high volume of events. Traditional on-premises solutions and early cloud security tools fall short in providing adequate visibility and threat detection in Kubernetes, often leading to a disjointed security approach with multiple, uncoordinated point products. This results in security gaps, overwhelming false positives, and insufficient data correlation for effective threat protection.

The situation is further complicated by the involvement of DevOps in configuring K8s and writing infrastructure as code (IaC). Without specialized security expertise, these teams can increase the risk of security and compliance gaps. However, alternatively, involving K8s security experts can delay production, impacting the bottom line. This landscape requires a modern approach to Kubernetes defense that balances development speed with security strength.

The Lacework solution

Lacework provides a single platform that spans the entire cloud-native application cycle, delivering comprehensive visibility and actionable security insights into Kubernetes environments. Lacework protects all versions of Kubernetes, whether managed, unmanaged (or fully open-source), or serverless. The platform covers Amazon Web Services (AWS), Microsoft Azure, Google Cloud, and Oracle Cloud Infrastructure (OCI) environments.

The platform offers innovative ways to accomplish monitoring and threat detection across the Kubernetes control and data planes, which spans Kubernetes audit logs and user activity, application processes, and network connections. The platform can also perform vulnerability scans on hosts and containers and runs configuration and compliance checks on IaC, containers, hosts, and both Kubernetes and public cloud provider accounts. Any risks are then surfaced and prioritized within the context of your cloud environment.

CHALLENGES

- Teams struggle to monitor complex and ephemeral containerized environments
- True threats hide within crowded alert queues filled with false positives
- DevOps teams building K8s infrastructure lack security expertise

LACEWORK BENEFITS

- Reduce risk and minimize impact due to security incidents
- Continuously monitor for threats and anomalous behavior
- Minimize alert fatigue through prioritized, context-rich notifications
- Maximize efficiency by enabling developers to secure their own code

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.

The platform automatically combines events across many data sources, including K8s audit logs. This analysis can then produce K8s-based composite alerts, such as flagging a potentially compromised K8s user.

Custom risk scoring

The Lacework platform automatically assigns a custom risk score to any vulnerabilities identified within your environment. To create this score, Lacework takes NVD critical vulnerabilities, then layers on unique customer attributes, including which vulnerabilities may be exposed to the internet, what critical data assets are in the vulnerability's path, and whether active exploits exist in the wild. This novel combination of first-party and third-party data can deprioritize up to 90% of vulnerabilities in your environment.

Through our code aware agent (CAA), our platform can identify which vulnerabilities are currently running in production. Users can, then, filter to only see these vulnerabilities through our dedicated Vulnerabilities dashboard.

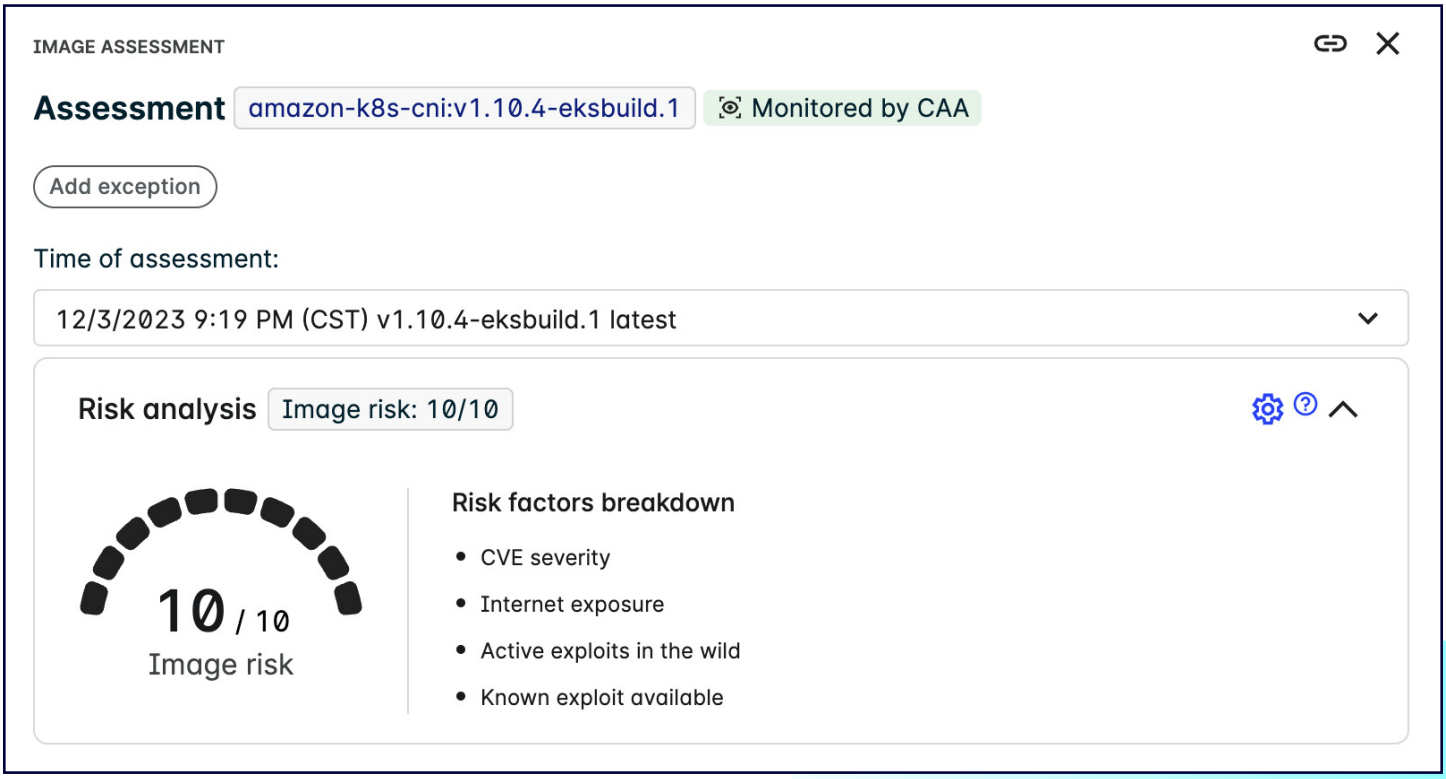

Figure 1: Lacework custom vulnerability scoring prioritizes vulnerabilities based on factors unique to your specific cloud environment.

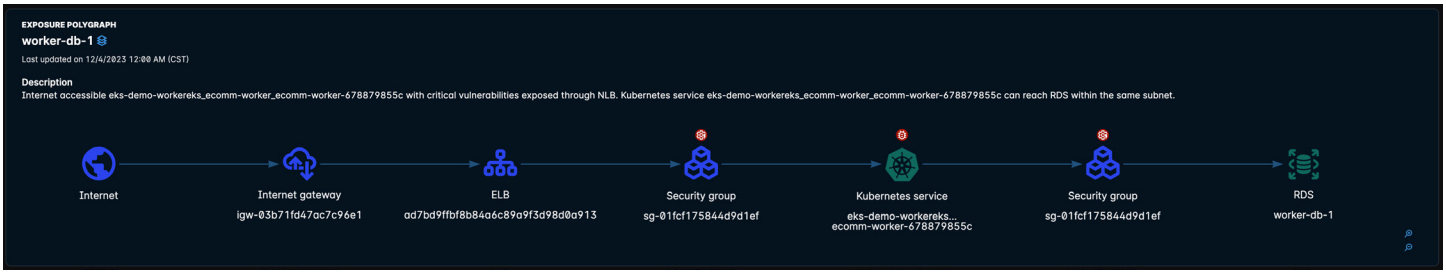

Figure 2: Exposure Polygraph visualizations map different ways attackers can enter a cloud environment and access data assets.

Patented anomaly detection

Lacework offers patented anomaly detection based on unsupervised machine learning. The capability baselines normal activity across your entire K8s environment and all its components, which then allows it to accurately detect anomalies that represent unknown or advanced threats. This results in a manageable number of high-fidelity alerts that include rich context on the who, what, where, when, and why for fast remediation. Lacework also offers policy-based rules for known misconfigurations and compliance reporting and signature-based detection for known bad files, processes, IPs, domains, and more. Together, these layered detection technologies ensure accurate threat detection, fast remediation, and reduced alert noise.

Attack path analysis

Lacework attack path analysis combines insights from cloud audit and configuration data, workload context from our lightweight agent, and agentless vulnerability and security scanning to provide context for any anomaly or policy-related event. Agentless scanning capabilities can also point out exposed data assets (e.g., RDS databases and S3 buckets), compliance violations, and hard-coded secrets like SSH private keys exposed on a host.

These factors are all combined into a single visualization, referred to as an Exposure Polygraph, that maps out real ways attackers can exploit your environment and reach your critical data assets. This way, security professionals can quickly know if a host is affected, which entities are exposed to the internet, if there are any vulnerable Kubernetes services, if compliance violations exist, and more.

All attack paths within a cloud environment are listed within a dedicated attack path dashboard and are prioritized based on a number of factors, including the value of the data assets at risk. Users can also see, from a single dashboard, their most at-risk hosts, container images, data assets, and attack paths with exposed secrets. This way, teams can focus on fixing the items within their cloud environment that will have the most impact.

IaC security

The Lacework platform extends automated security and compliance checks of IaC early in the development process to prevent misconfigured cloud services from being deployed. Within minutes, Lacework can be connected to code repositories or CI/CD pipelines. The platform supports templates such as Terraform, AWS CloudFormation, and Kubernetes/Helm and can scan Dockerfiles. Teams can use Lacework to automatically discover IaC templates and code repos used across the organization.

Lacework adds security guardrails that automatically and continuously scan IaC for policy violations and immediately alert developers as they are writing code. When IaC is submitted (pull request or commit) to a code repository, Lacework will automatically test it against any assigned security and compliance policies. Organizations can also use Lacework to test IaC once it has been packaged for delivery to ensure production parameters, like us-west-1, are within policy.

All identified misconfigurations are recorded within the code repository, as well as the Lacework UI, to ensure both development and security teams have shared visibility into the security of the code. Developers receive immediate and automated remediation guidance for fixing the code, as well as the ability to auto-remediate with just one click.

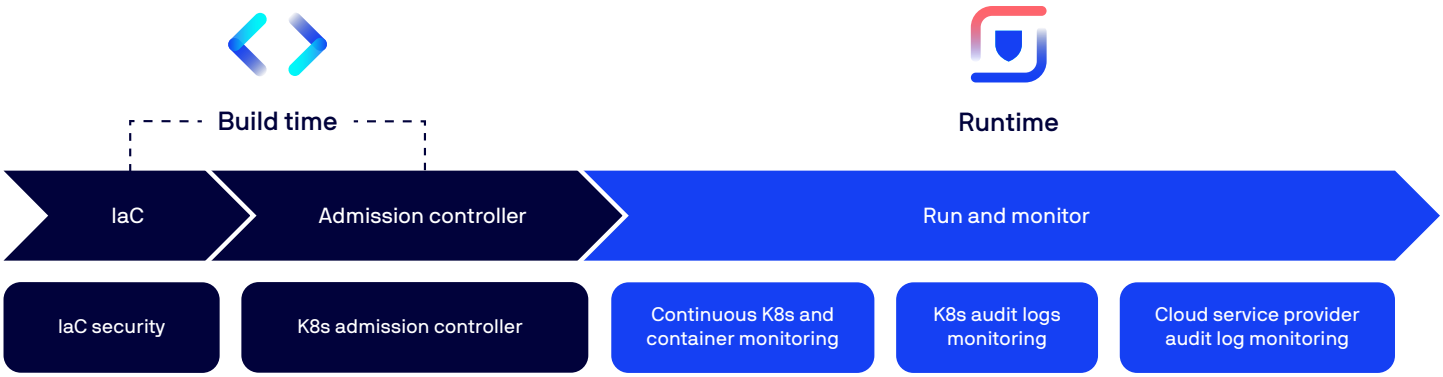

Figure 3: Lacework protects against all stages of Kubernetes usage.

K8s admission controller

As an additional safeguard during the build phase, Lacework offers a Kubernetes Admission Controller. This capability can scan K8s containers for misconfigurations or vulnerabilities prior to deployment and can optionally block insecure containers. This feature results in a greatly reduced chance that a misconfiguration or vulnerability will end up in production where it can lead to a breach and saves time and money needed to fix downstream issues in production.

Why Lacework?

- Comprehensive, integrated, end-to-end K8s coverage from a single vendor that spans both build time and runtime, from the control plane through the data plane
- Broad cloud security platform that protects all major cloud providers, K8s, hosts, containers, and more
- Features including threat detection, vulnerability, configuration checks, compliance reporting, and IaC security
- Accurate, ML-based anomaly detection alongside policy-based and signature-based threat detection

See it in action.

Request a live demo

Click through the platform >>