SOLUTION BRIEF

LACEWORK

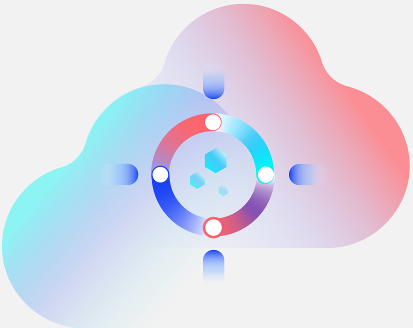
Comprehensive and automated Kubernetes security and compliance

Detect threats, demonstrate compliance, and identify vulnerabilities and misconfigurations with Lacework

OVERVIEW

Securing your cloud environments

More and more organizations are moving to the cloud and using containers to deploy revenue-generating applications faster, at a lower cost, and with near-unlimited, elastic scale. Kubernetes, or K8s, is a critical infrastructure layer in most cloud deployments, as it is the leading container orchestration and management technology. While Kubernetes offers substantial operational benefits, it also needs to be properly monitored and secured to prevent an external threat or malicious insider from compromising containers and the workloads within them. This compromise could lead to nefarious activities such as cryptomining, or finding and exfiltrating sensitive data. K8s security and event logging is also essential for ensuring compliance with regulations and frameworks such as the NSA and CISA Kubernetes Hardening Guide lists, NIST 800-53, CIS Benchmark for Kubernetes, PCI DSS, SOC 2, and ISO 27001.



Key Lacework benefits for Kubernetes security

- Comprehensive K8s monitoring leads to strong security and compliance posture
- Accurate, machine learning-based threat detection and contextual alerts minimize alert fatigue
- “Shifting left” automated security to DevOps speeds time to revenue and maximizes employee efficiency

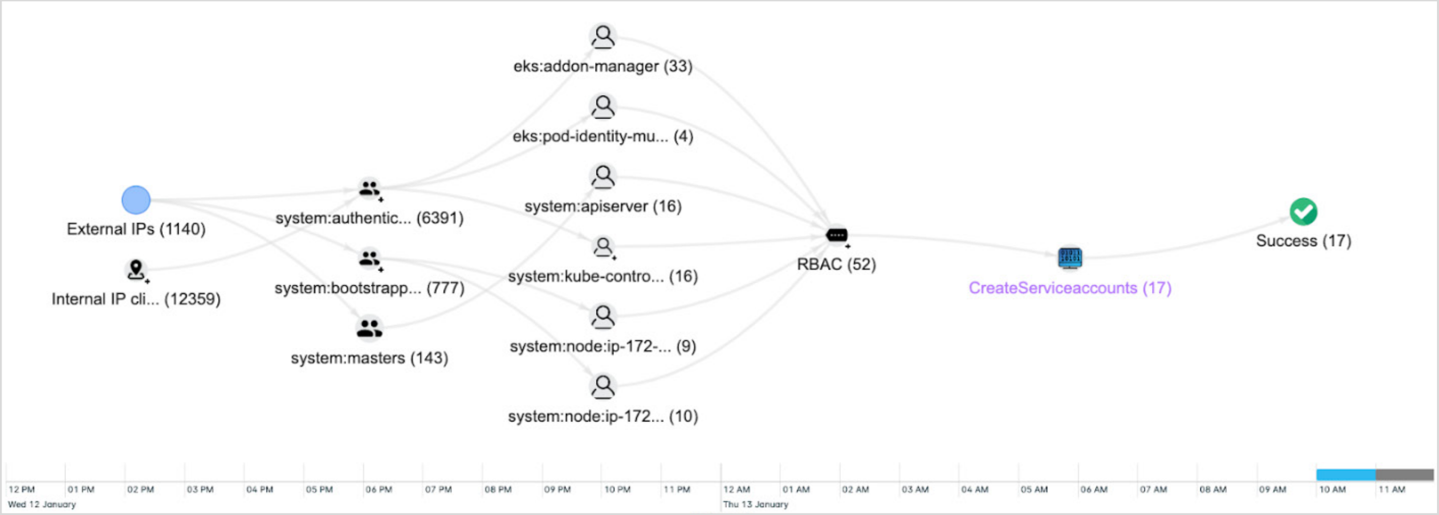


FIGURE 1 – Lacework uses our patented Polygraph® unsupervised machine learning against user, system, application, and network activity across the Kubernetes environment to automatically detect abnormalities that represent threats.

CHALLENGES

Difficulty monitoring the complexity and sheer size of the K8s environment

Traditional, on-premise security solutions struggle with Kubernetes visibility as they were not built to handle its complexity, the temporal nature of containers and their rapid scaling up and down, or the sheer volume of events they generate. A typical K8s environment could be hundreds of clusters running thousands of pods and containers with components constantly being created, shut down, or moved, and generating millions of events daily across data and control planes. The Kubernetes surface area to monitor becomes even larger if the deployment spans public clouds or includes K8s Admission Controllers and K8s Helm Charts to deploy applications on K8s. Even cloud security products come up short as they tend to protect only a portion of the overall K8s environment. As a result, some organizations resort to buying a patchwork of point cloud solutions, which leads to multiple, siloed tools, visibility blind spots, and no way to aggregate all relevant K8s event data into one place for better threat detection and compliance.

The struggle to accurately detect threats

Even if all K8s events and activities could be captured in one place, it is a challenge to find a way to accurately detect threats and compliance issues in this sea of never-ending event data generated by K8s. Most cloud security solutions use manual, human-written rules to detect threats, which results in far too much time spent writing and maintaining rules and an inability to detect anomalous, or unknown, threats. Manual rules can also lead to hundreds of false positive alerts on a daily basis, which quickly overwhelms security response teams and distracts them from hunting for legitimate threats and remediating compliance or vulnerability issues.

Manual security review in the K8s build process slows down revenue

As part of the pre-production K8s build process, DevOps often takes the lead on configuring Kubernetes and the containers that will run on it. This also includes writing Infrastructure as Code (IaC) to provision K8s infrastructure on the public cloud. However, DevOps are not security experts, often prioritize development over security, and do not want to leave their normal workflows and applications to work on security alerts. As a result, there is a risk that DevOps may build out the K8s environment that has security and compliance gaps. On the other hand, security teams do prioritize security over development, but since they are not K8s experts and do not want to slow down development, it might be necessary to bring in specialized K8s security experts to manually review the entire build process. However, this slows down getting revenue-generating applications and initiatives onto K8s in production, which both hurts the bottom line and is not scalable.

55% Of companies have delayed deployment due to a K8s security concern.

THE LACEWORK SOLUTION

Lacework can solve the challenges of securing your Kubernetes environment from build to runtime with comprehensive visibility, threat detection and alerts, configuration and compliance checks, and vulnerability scans.

Single platform to monitor and protect the entire K8s environment

Lacework is a single platform with end-to-end comprehensive and integrated monitoring and protection of the K8s environment. Capabilities include monitoring and threat detection across the K8s control and data planes, which spans K8s audit logs and user activity, application processes, and network connections. This includes visibility into running K8s clusters, namespaces, nodes, pods, and containers. This coverage is enabled by layered monitoring from both agentless and agent-based technologies. Lacework protects all versions of K8s, whether managed, unmanaged (or fully open-source), and serverless, and on the major cloud providers of AWS, Azure, and Google Cloud. In addition to threat detection, Lacework also performs vulnerability scans on host OSes and containers, and runs configuration and compliance checks on IaC, containers, hosts, and both Kubernetes and public cloud provider accounts. These checks power compliance reports that help accelerate and automate audits. Lastly, Lacework leverages the near-unlimited scale of cloud storage and compute to easily capture and analyze all events for threat detection, compliance logging requirements, and more.

Accurate detection of unknown and known threats with no alert fatigue

Lacework offers unique, patented Polygraph® detection based on unsupervised machine learning. It 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.

Automated security in the K8s build process to empower DevOps and accelerate revenue

Lacework empowers organizations to “shift left” security from security teams to the DevOps build process by seamlessly integrating automated K8s security into developer workflows including CI/CD pipelines and Git repositories. It removes any security skills gap DevOps might have by automatically finding issues like IaC or container misconfigurations, as well as giving guidance on fixes or auto-fixing issues. This allows DevOps teams and individual developers to quickly resolve possible security issues and deliver with confidence, enabling revenue-generating applications to enter production as quickly as possible.

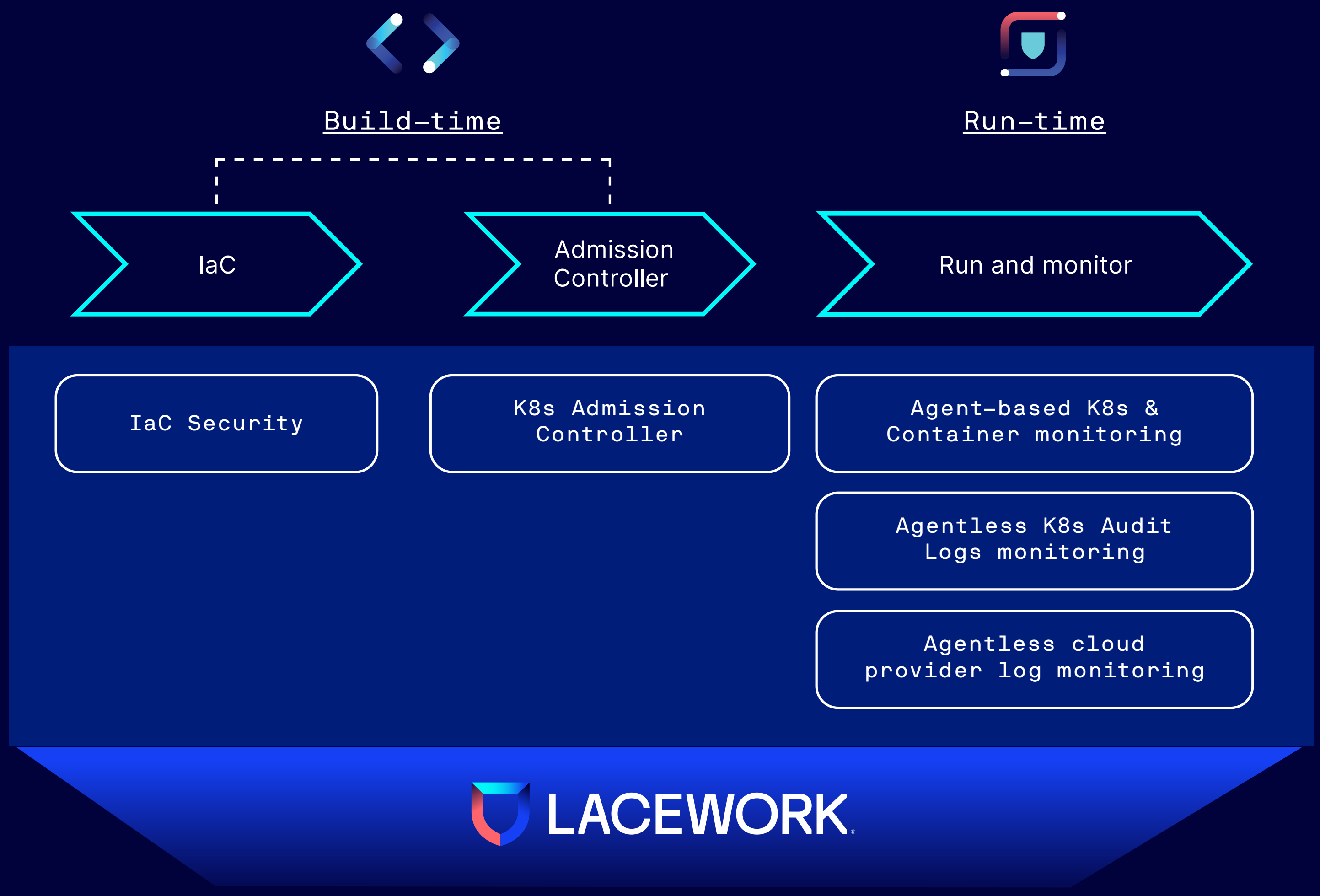

Build-time
Run-time
IaC
Admission Controller
Run and monitor
IaC Security
K8s Admission Controller
Agent-based K8s & Container monitoring
Agentless K8s Audit Logs monitoring
Agentless cloud provider log monitoring
LACEWORK

FIGURE 2: Lacework protects across all stages of Kubernetes usage.

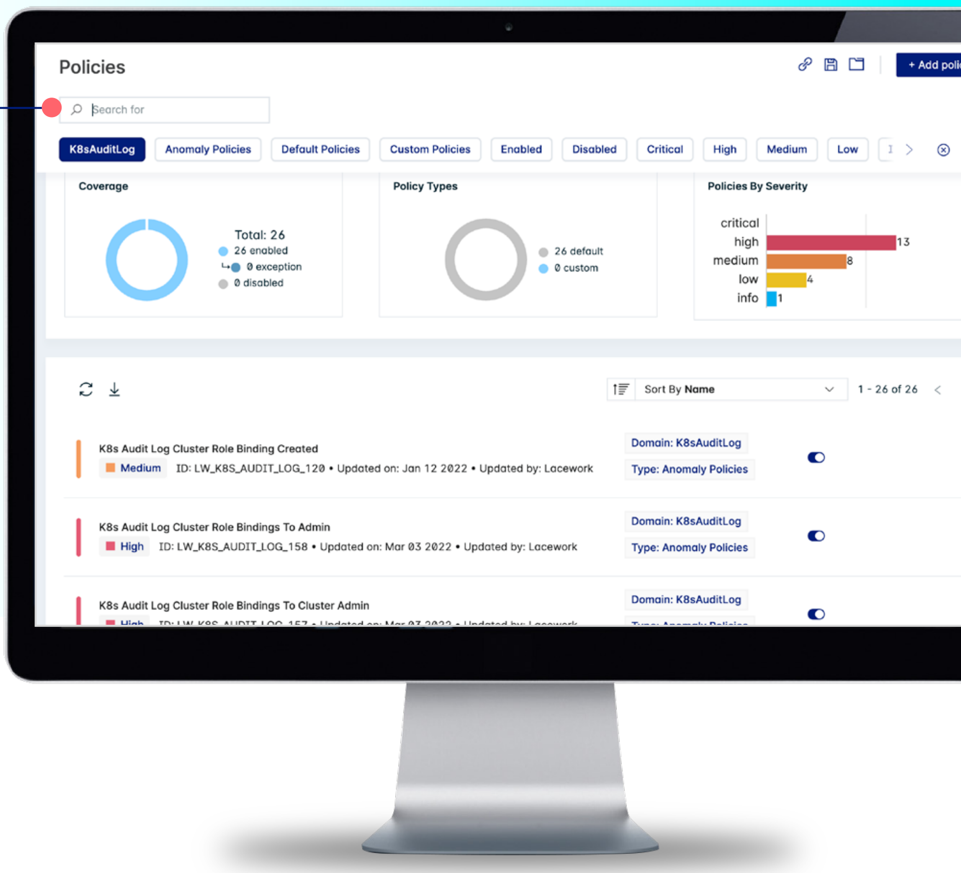
CAPABILITIES AND USE CASES

Advanced protection for Kubernetes

As shown in the diagram above, Lacework capabilities protect across all stages of Kubernetes from build time to runtime, and enable a range of use cases, including:

- **Monitoring and threat detection** to detect unknown and known cyberthreats across the runtime K8s environment
- **Compliance reporting** against frameworks and regulations such as CIS, HIPAA, ISO, NIST, PCI, and SOC 2
- **Vulnerability scanning,** including prioritizing vulnerabilities by severity and risk
- **Configuration assessments,** including prioritizing misconfigurations by severity
- **Asset inventory,** including clusters, namespaces, workloads, pods, containers, and nodes

Key Lacework capability	What it does / use cases	Threat detection	Compliance reporting	Vulnerability scanning	Configuration assessments	Asset inventory
Agent-based K8s and container monitoring	Provides runtime visibility into a wide range of K8s platforms, host OSes, clusters, nodes, pods, and containers to monitor and detect threats, and identify host vulnerabilities. Used for anomaly-, signature-, and policy-based detection. Captures activities on running K8s hosts and/or containers including network connections, processes, and user behavior. Can also perform File Integrity Monitoring, Host Intrusion Detection, and host vulnerability scanning.	✓	✓	✓		✓
Agentless K8s audit logs monitoring	Provides visibility into the K8s audit logs from the K8s API and all the valuable event information it captures on who did what in the K8s environment. Used for both anomaly-based and policy-based detection. Captures activities in the K8s environment including UI-based or manual user activities, deployment or updates of workloads or Kubernetes RBAC, authentication and authorization checks, and errors that might be the result of lateral movement or incorrect permissions.	✓	✓		✓	
Agentless cloud provider log monitoring	Provides visibility into public cloud account activities that can impact the K8s environment from public cloud logs such as Amazon CloudTrail. Used for both anomaly-based and policy-based detection. Captures cloud provider activity relevant to K8s environment including encryption strength, container registries, storage bucket settings, load balancers, and more.	✓	✓			✓
K8s Admission Controller	Lacework integrates with the Kubernetes Admission Controller to scan K8s containers for misconfigurations or vulnerabilities prior to deployment, and optionally block insecure containers. Is seamlessly integrated into DevOps workflows. Results in a greatly reduced chance 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.			✓	✓	
IaC Security	Lacework integrates with Git-based repositories to automatically scan IaC code, including K8s Helm charts, Terraform, and AWS CloudFormation, prior to deployment. Over 600 pre-built policies are applied to check for misconfigurations or insecure code, and violation detail appears in Git to empower DevOps to easily fix any issues within the workflows they are used to. Results in a greatly reduced chance 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.		✓		✓	



Policies

Coverage

Total: 26
26 enabled
0 exception
0 disabled

Policy Types

26 default
0 custom

Policies By Severity

Sort By **Name**

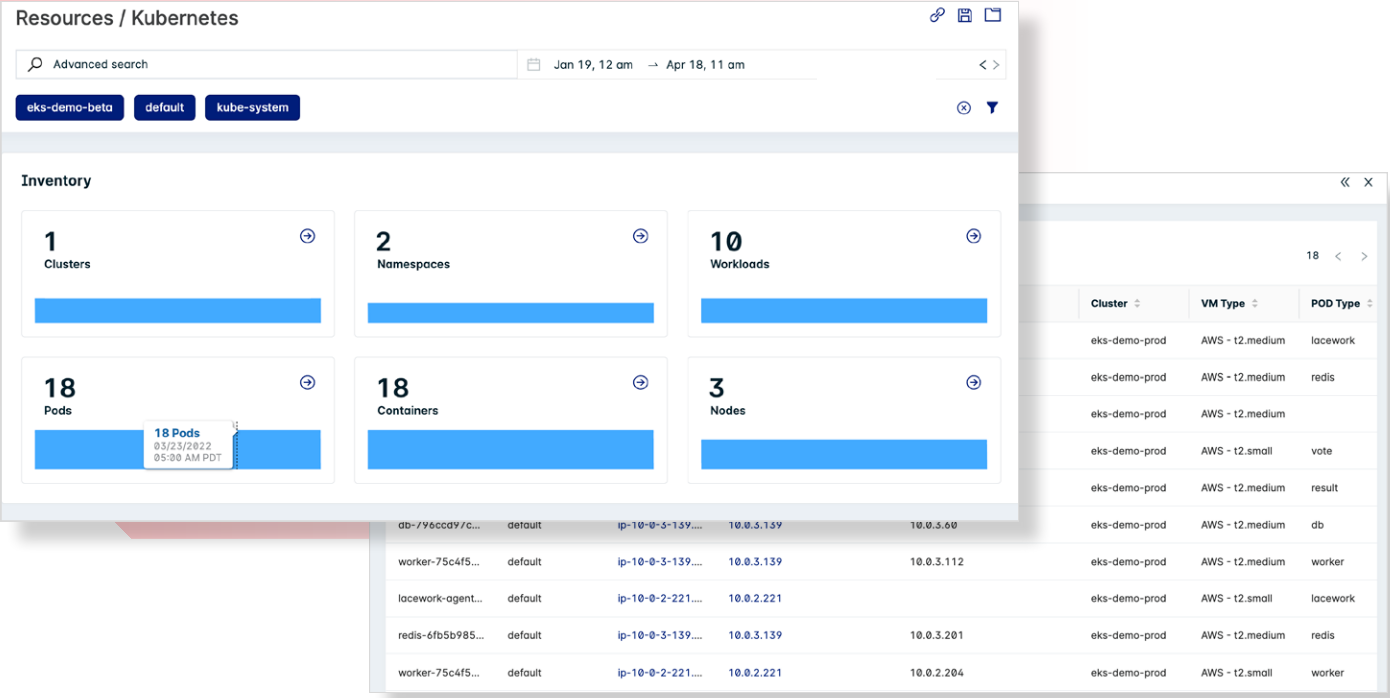
1 - 26 of 26

K8s Audit Log Cluster Role Binding Created
🟧 Medium ID: LW_K8S_AUDIT_LOG_120 • Updated on: Jan 12 2022 • Updated by: Lacework
Domain: K8sAuditLog
Type: Anomaly Policies

K8s Audit Log Cluster Role Bindings To Admin
🟥 High ID: LW_K8S_AUDIT_LOG_158 • Updated on: Mar 03 2022 • Updated by: Lacework
Domain: K8sAuditLog
Type: Anomaly Policies

K8s Audit Log Cluster Role Bindings To Cluster Admin
Domain: K8sAuditLog

FIGURE 3: Lacework includes pre-built policies to detect misconfigurations or suspicious activity specific to Kubernetes audit log monitoring.



Resources / Kubernetes

Inventory

1 Clusters

2 Namespaces

10 Workloads

18 Pods

18 Pods
03/23/2022
05:00 AM PDT

18 Containers

3 Nodes

18

					Cluster	VM Type	POD Type
					eks-demo-prod	AWS - t2.medium	lacework
					eks-demo-prod	AWS - t2.medium	redis
					eks-demo-prod	AWS - t2.medium	
					eks-demo-prod	AWS - t2.small	vote
					eks-demo-prod	AWS - t2.medium	result
db-796ccd97c...	default	ip-10-0-3-139....	10.0.3.139	10.0.3.60	eks-demo-prod	AWS - t2.medium	db
worker-75c4f5...	default	ip-10-0-3-139....	10.0.3.139	10.0.3.112	eks-demo-prod	AWS - t2.medium	worker
lacework-agent...	default	ip-10-0-2-221....	10.0.2.221		eks-demo-prod	AWS - t2.small	lacework
redis-6fb5b985...	default	ip-10-0-3-139....	10.0.3.139	10.0.3.201	eks-demo-prod	AWS - t2.medium	redis
worker-75c4f5...	default	ip-10-0-2-221....	10.0.2.221	10.0.2.204	eks-demo-prod	AWS - t2.small	worker

FIGURE 4: Lacework displays full inventory and detail on all your Kubernetes components

> [Lacework] works not only with the virtual machines (VMs) that we have deployed, but also with the Kubernetes clusters. We're able to deploy Lacework across our entire environment and get a comprehensive view of our configuration. The unique anomaly detection from Lacework's Polygraph technology, paired with the CIS functionality, is just incredible. I haven't seen another tool that does it all like that."

AUSTIN GREGORY, INFORMATION SECURITY ENGINEERING MANAGER, NYLAS

Why Lacework?

- Comprehensive, integrated end-to-end K8s coverage from a single vendor that spans build to runtime, and 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 and configuration checks, compliance reporting, and IaC security
- Accurate, machine learning-based threat detection with Polygraph, and complementary policy-based and signature-based detection

Customer outcomes

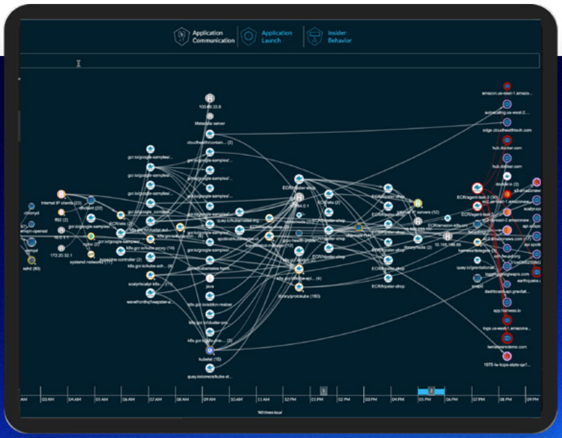
- Strong overall K8s security and compliance posture and deep visibility spanning all clouds
- Reduced costs and consolidated technology from several security vendors
- Ensures accurate threat detection, fast remediation, and no alert fatigue
- Speeds time to revenue by "shifting left" K8s security to the development process

Kubernetes efficiency + Lacework security

Across your entire Kubernetes environment, gain unmatched visibility and threat detection, improve your security posture, and ensure compliance at automated scale. Learn more about how Lacework helps with Kubernetes security, and contact Sales to learn more and see a live demo or discuss a trial.

Ready to chat?

Request a demo



| 888.292.5027 | lacework.com