A guide to container security

Containers are quickly becoming one of the most important tools for software development. As their popularity and adoption rises, so does the need for security that is built to protect this dream developer environment. In this ebook, we take a look at how to secure your containers from build to runtime and keep them compliant.

LACEWORK

Containers explained

What is a container?

Before we dive too deep, let's back up. What is a container? Simply put, it's a way of packaging up the code, the libraries, and configuration for all applications in one read-only image. This approach abstracts away most of the operating system, providing just enough access so you can focus on solving your business problem. By packaging applications this way they can run anywhere: on-premises, in a hybrid environment, or in the cloud.

Container growth is sky high

Container adoption has grown 70% over the last two years

"THE MATURATION OF CLOUD-NATIVE SECURITY: SECURING MODERN APPS AND INFRASTRUCTURE," ESG SECURITY RESEARCH, 2021

63% of North American enterprise infrastructure decision-makers have implemented or are in the process of implementing containers or microservices architecture

"ADOPTION PROFILE, CONTAINERS IN NORTH AMERICA," FORRESTER REPORT, 2021

The container application market is projected to reach $14.4 B in 2028, and is growing at an annual compound rate of 23%

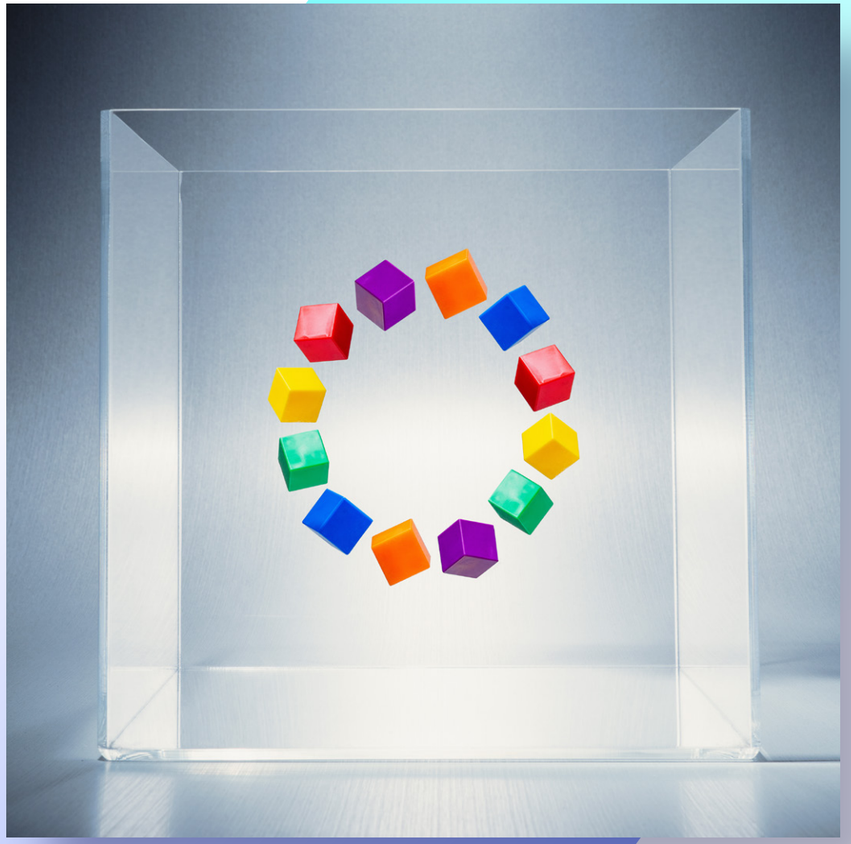
"APPLICATION CONTAINER MARKET," REPORTS AND DATA, 2019

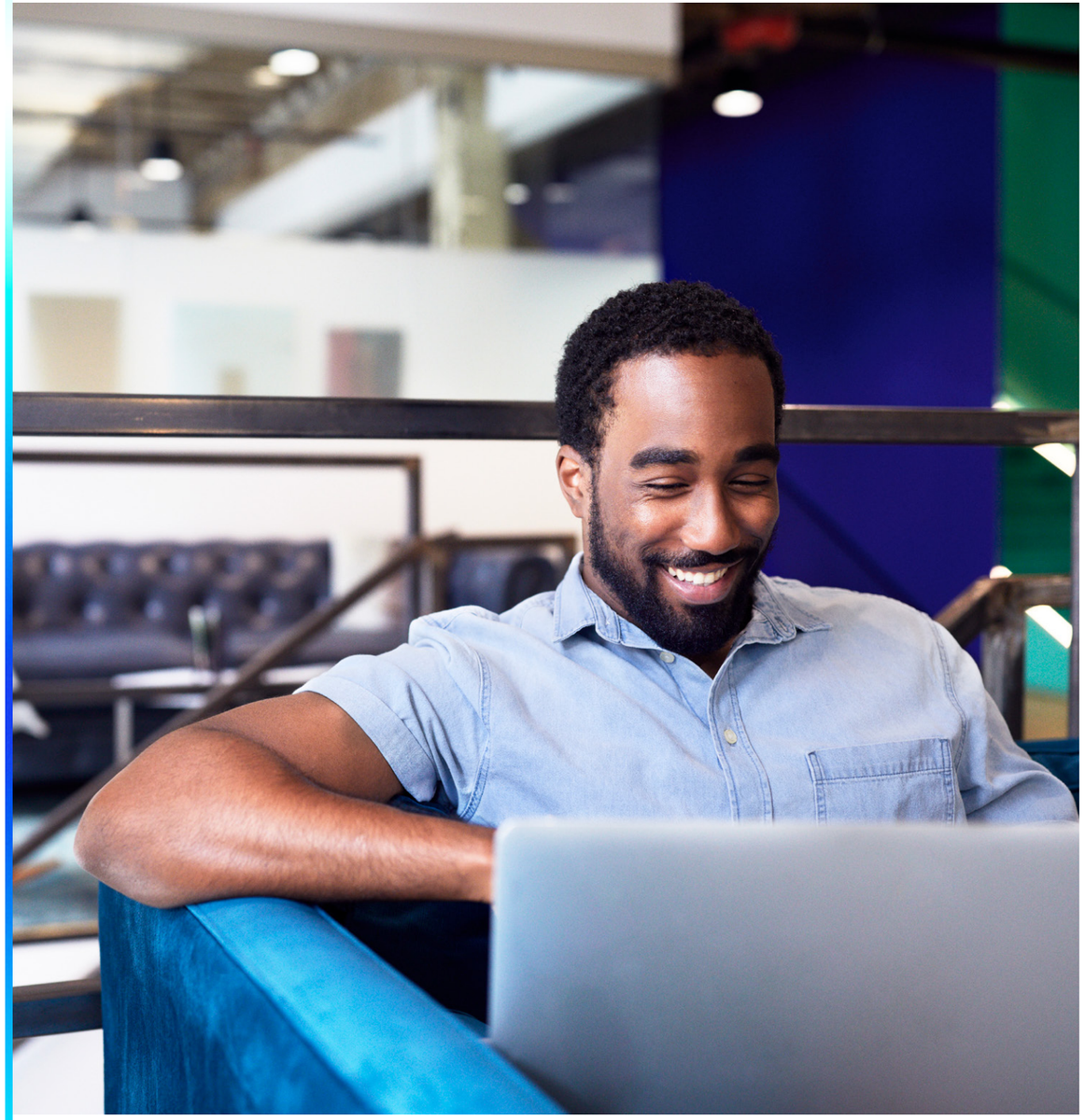
LACEWORK

New security challenges

Containers give builders the tools to rapidly develop, package, and apply code to create applications anywhere, anytime. This freedom has enabled a shift away from development practices previously built for on-premises environments. Container usage creates a ripple effect that is felt by everyone who engages with these applications, both inside and outside of an organization. Security and operation teams suddenly are faced with faster release cycles and more entities to secure, but less control over their environments. While containers speed innovation, they can add complexity and create new security challenges. Containers can increase the attack surface, making it harder for security teams to identify vulnerabilities, threats, misconfigurations, and compliance violations.

Developing applications with containers operationalizes speed, but it must be done without jeopardizing security





Why traditional security approaches fail

Public cloud platforms offer some security tools for containers and orchestration, but not enough. Most point container solutions only secure pieces of the application development process. They may be good at securing accounts, or workloads, but they lack other capabilities like encryption, intrusion detection, or governance. These approaches can't help customers quickly understand their environment and get visibility into what issues need to be fixed first.

Traditional security tools often rely on rules to watch for problems. Rules, however, take considerable time and effort to configure and implement. Plus rules protect against known threats, but can't protect against breaches that don't fit the rules. And rules require constant tuning, checking, and adjustment as threats evolve. Bottom line: this approach is not great for the ephemeral nature of containers.

Security professionals are left looking for tools that help them make sense of their environment. They need to easily find, monitor, and inventory all assets across their container environment without a lot of manual effort. Since security teams are overextended, many are opting for container security platforms that consolidate tools and automate management of security operations. A platform approach can help security teams understand their environment and keep pace with developers.

A successful approach to securing containers

The walls between IT operations have come down. Control is shifting into the hands of developers with the creation of DevOps. Look for a solution that offers these features in order to successfully secure your containers and cloud infrastructure.

Behavioral threat detection

Collect high-fidelity process, network, file, and user data to form a base model of normal infrastructure behavior. Leverage analytics and machine learning to detect anomalies that indicate threats in real time so you can minimize alerts and focus on the issues that matter.

Security that scales from build to runtime

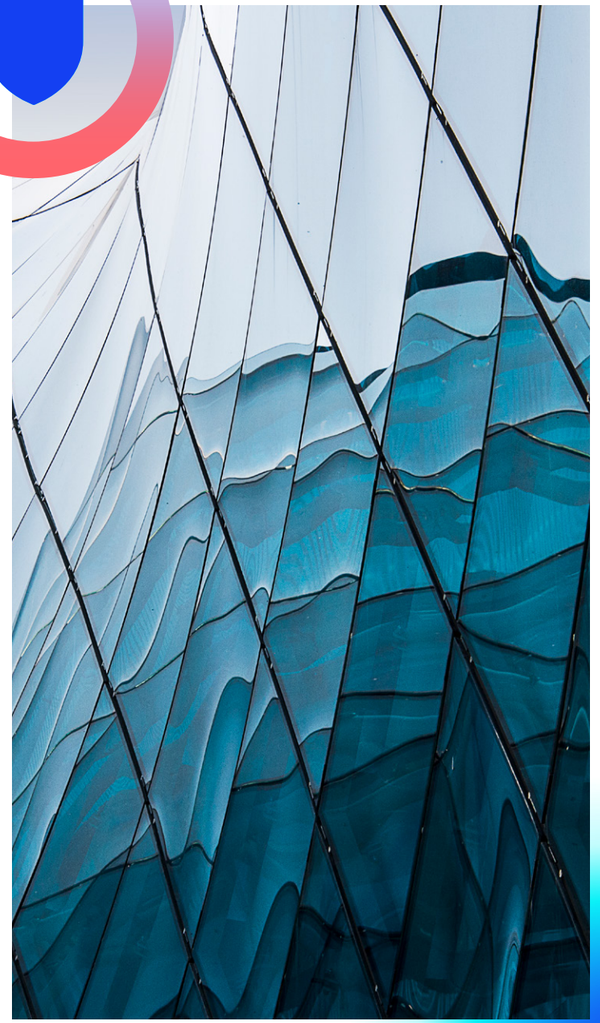
Secure container applications at build time to reduce the risk of threats at runtime. Ensure your security processes include identifying vulnerabilities and security issues with resources, applications, networks, files systems, APIs, and processes before they spread. Verify that alerts include security context to help DevOps and security teams investigate and assess the risk of pushing the container before it goes to production.

Continuous visibility across all layers

Gain visibility into container-related events, communication, new connections, and images across the application/process, container runtime, and orchestration layers to expose all threats. Ensure security for clusters and communication among the clusters at the namespace and pod level. This can help prevent misconfigurations and overprivileged access.

Continuous compliance

Perform continuous configuration audits and identify compliance gaps with a unified management interface. Ensure the right level of coverage is provided for all resources and applications that containers are touching.



LACEWORK

Tools and tips for container security

Tools of the trade

As more applications rely on third-party and open-source software outside of their control, the stakes get higher. Your security must have the ability to associate vulnerability risks with runtime context to alert on anomalous activities associated with host OS, container images, and the containers themselves using real-time data.

- **Inline scanner** with continuous integration/continuous delivery (CI/CD) pipelines will shift security practices earlier and report for vulnerability risk as part of the build process
- **Platform scanner** will provide complete coverage of private registries
- **Container registry scanner** will continuously scan images for vulnerable packages and libraries
- **Proxy scanner** will provide better control on where container images are scanned
- **Admission controller** will offer a policy-driven allow/fail mechanism for deployment in K8s environments

Steps to build security into your container pipeline

1. Establish a way to identify where misconfigurations could lead to risks to the environment. The CIS Benchmark is a good guide for applications that use Docker and Kubernetes.
2. Use trusted images to prevent a single image from impacting your entire environment.
3. Control access to containers and limit permissions to those for whom it is absolutely necessary.
4. Understand cloud activity — know what's happening across your tools and resources
5. Follow log management best practices and maintain a timeline of activity correlated between containers, users, and applications, even after the container is gone.

LACEWORK

- Understand what is normal for your environment
- Reduce alert volume 100:1
- Get the who, what, why, when, and where of each alert

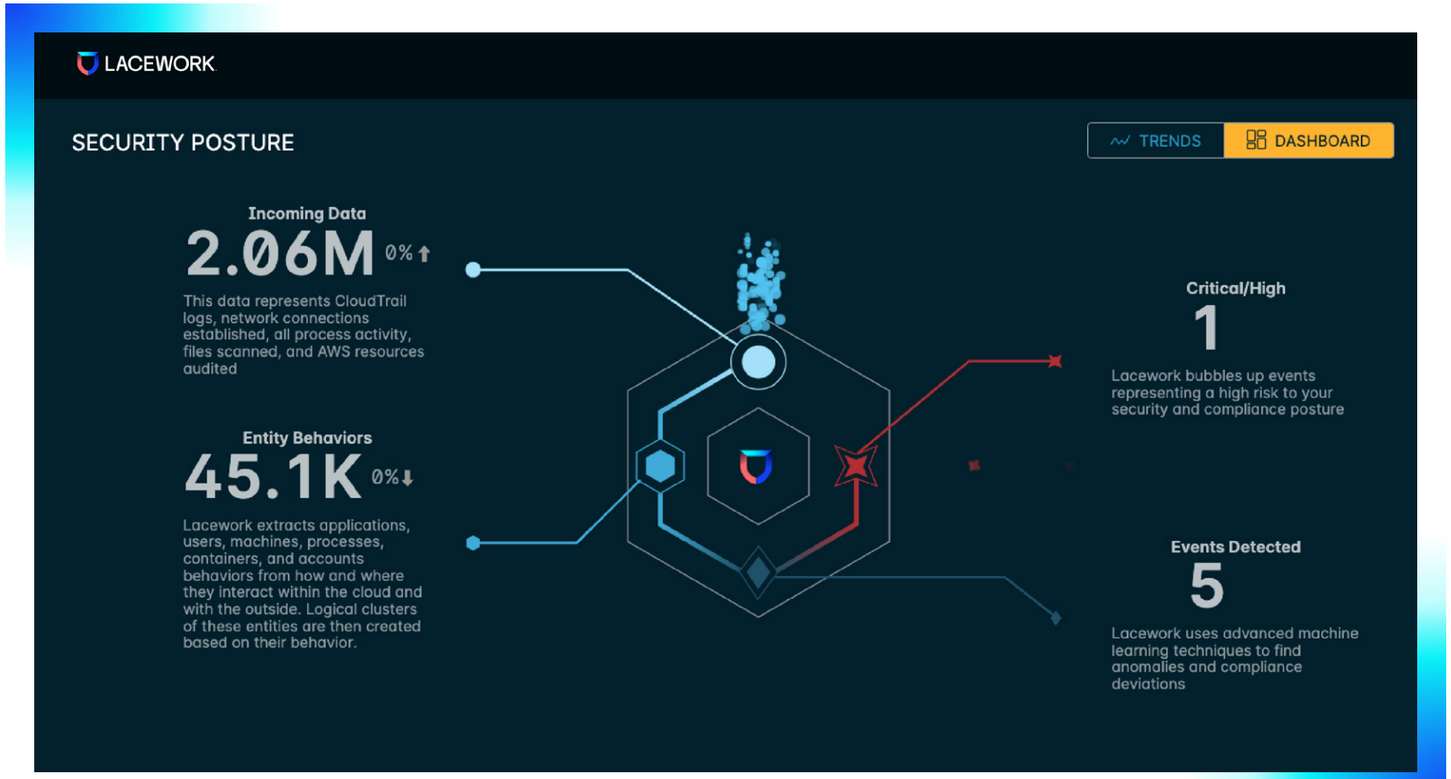
“If anything critical shows up, Lacework will alert us. I no longer worry about rogue systems in production. It allows me to manage so many systems with just two people.”

WILLIAM AU, SENIOR DIRECTOR OF DEVOPS, JITTERBIT

The Lacework Polygraph® Data Platform

The Polygraph Data Platform helps organizations of all sizes automatically uncover suspicious activity across containers so they can detect and address risks to their business from build time through runtime. Lacework is the only company to offer automated anomaly detection and provide consistent visibility, context, and security across Amazon Web Services (AWS), Google Cloud, Microsoft Azure, and Kubernetes EKS environments.

The Polygraph Data Platform uses anomaly detection to compare an organization’s data to its own data, not against a pre-set list of security rules. This enables customers to see and understand cloud container changes within their own environment, without requiring manual intervention. No other vendor can provide this type of automated analysis.



Lacework capabilities

Lacework provides cloud and container security from build time to runtime, which reduces the potential threat surface, while enabling DevOps and security teams to achieve their goal without sacrificing speed.

Uncover vulnerabilities at build time

Identify vulnerable container images and update them before they are ever deployed, all without involvement from the security team, using our inline vulnerability scanner. Developers can perform fast, low latency, on-demand scans directly within their CI pipeline through integrations with developer-focused tools like Jenkins.

Establish a behavioral baseline

Discover every container in the cloud and cluster the container based on behaviors. Security teams can continuously monitor communications, launches, and runtime behaviors using unsupervised machine learning to detect abnormal behaviors in real time.

Achieve compliance with ease

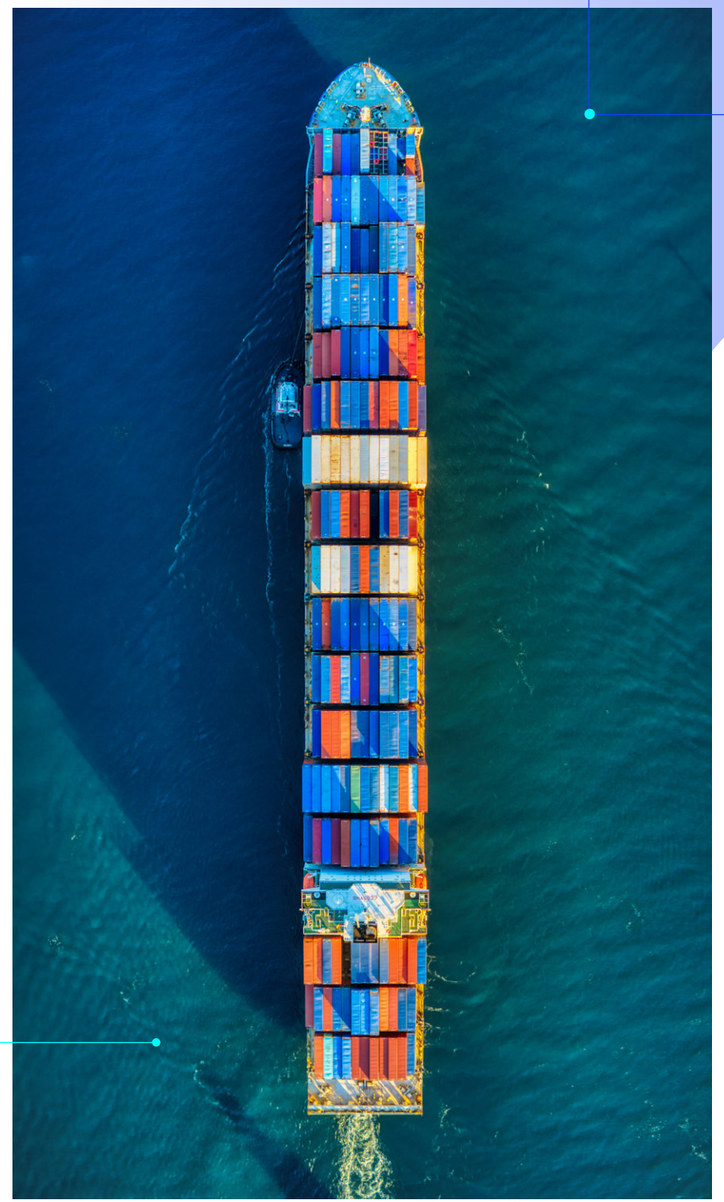
Monitor configuration changes and API activity for containers across AWS, Azure, and Google Cloud platforms continuously. CIS Benchmark scans are performed during container image development and container deployment. Additionally, Lacework includes supplemental checks based on industry best practices and common compliance frameworks like PCI DSS, SOC 2, HIPAA, and NIST.

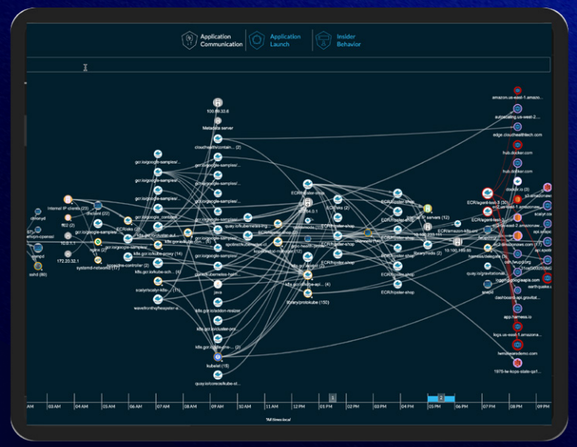
Block vulnerable containers from deploying

Ensure container images meet security standards before deployment with the Lacework admission controller for Kubernetes. Organizations can automatically block container images that fail to meet standards from deploying in production.

Prioritize fixes in runtime with actionable risk scoring

Prioritize remediation tasks with risk-based scoring that leverages a combination of insights across build time and runtime to measure the true risk within your unique environment. Lacework will rank alerts by severity and offer context-rich recommendations for effective remediation.





Ready to chat?

Request a demo

Lacework is the data-driven security company for the cloud that delivers end-to-end visibility and automated insight into risk across cloud environments, so you can innovate with speed and safety. The Lacework Polygraph® Data Platform ingests data, analyzes behavior, and detects anomalies across an organization's Amazon Web Services (AWS), Google Cloud, Microsoft Azure, and Kubernetes environments. This patented approach significantly reduces noise and turns millions of data points into prioritized, actionable events. Customers all over the globe depend on Lacework to take software services to market faster and more securely, while consolidating overlapping security solutions into a single platform for better visibility and coverage across a multicloud environment.

Founded in 2015 and headquartered in San Jose, Calif., Lacework is backed by leading investors like Sutter Hill Ventures, Altimeter Capital, D1 Capital Partners, Tiger Global Management, Counterpoint Global (Morgan Stanley), Franklin Templeton, Durable Capital, GV, General Catalyst, XN, Coatue, Dragoneer, Liberty Global Ventures, and Snowflake Ventures, among others.

Get started at www.lacework.com

LACEWORK®