GUIDEPOINT SECURITY

LACEWORK

JOINT SOLUTION BRIEF

From Cloud to Containers: Stay Secure at Every Step

While containers deliver business value and speed, they introduce new challenges for security leaders tasked with protecting workloads in dynamic cloud environments. The rise of containers doesn't mean sacrificing security. Containers enable organizations to accelerate application development, improve efficiency, and cut costs. To realize the benefits of containers, your cloud security must be built on a solid foundation.

By 2026, an estimated 90% of global organizations will be running containerized applications in production.[1]

Containerizing Applications on AWS

On Amazon Web Services (AWS), you'll find several container services that make it easier to manage your underlying infrastructure, whether on-premises or in the cloud, so you can focus on innovation and your business needs.

AMAZON ELASTIC CLOUD COMPUTE (AMAZON EC2) allows you to have full control over your compute environment. Use Amazon EC2 to build out your own host—whether that's based on Docker or Kubernetes—and run containers that comprise your distributed application.

AMAZON ELASTIC CONTAINER SERVICE (AMAZON ECS) enables you to deploy, manage, and scale containerized applications with a fully managed container orchestration service. When you build your own containers that run on Amazon EC2 instances, you can use Amazon ECS to manage them and spin them up as needed.

AMAZON ELASTIC KUBERNETES SERVICE (AMAZON EKS) lets you start, run, and scale Kubernetes applications on AWS or on-premises with the most trusted way to run Kubernetes. Running containers with Kubernetes makes it easier to efficiently run multiple containers, with options to automate tasks like spinning up and down containers.

[1] Gartner, The Innovation Leader's Guide to Navigating the Cloud-Native Container Ecosystem, Arun Chandrasekaran, Wataru Katsurashima, August 18, 2021.

5 Steps to a SECURE Cloud Architecture

GuidePoint Security's five-phased security approach protects both operations and customers, while supporting current and future business needs.

1. **Foundation:** Determine your current posture, highlight organizational security needs, recognize current and future cloud architecture plans.
2. **Perimeter:** Determine your perimeter strategy by defining the identity boundary.
3. **Data protection:** Focus on encryption, key management, and secrets management services to bolster data protection.
4. **Visibility:** Collect and organize logging data for enhanced visibility that allows you to identify events or anomalies.
5. **Cloud services:** Adopt new solutions like containers, functions, and cloud platforms that help move the business forward.

GUIDEPOINT SECURITY

LACEWORK

Keeping Containers Safe: The Lacework Polygraph® Data Platform

Containers can increase the attack surface, making it harder for security teams to identify vulnerabilities, threats, misconfigurations, and compliance violations. The Lacework Polygraph Data Platform helps organizations automatically uncover suspicious activity across containers so they can address risks to their business from build time through runtime.

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 an inline vulnerability scanner.

Establish a behavioral baseline: Discover every container in the cloud and cluster the container based on behaviors.

Achieve compliance with ease: Continuously monitor configuration changes and API activity.

Block vulnerable containers from deploying: Ensure container images meet security standards before deployment with the Lacework admission controller for Kubernetes.

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.

Take the next step to secure containers

With GuidePoint Security, Lacework, and AWS working together, you can keep your containerized applications secure and safely continue your cloud journey.

To learn more about GuidePoint Security services for AWS, visit AWS Marketplace.

Discover Lacework solutions designed for AWS, and check out Lacework in AWS Marketplace.

About Us

GuidePoint Security provides trusted cybersecurity expertise, solutions and services to help organizations make better decisions that minimize risk. GuidePoint's unmatched expertise has enabled a third of Fortune 500 companies and more than half of the U.S. government cabinet level agencies to improve their security posture and reduce risk.

GUIDEPOINT SECURITY

2201 Cooperative Way, Suite 225, Herndon, VA 20171
guidepointsecurity.com • info@guidepointsecurity.com • (877) 889-0132

aws marketplace