GUIDEPOINT SECURITY

LACEWORK

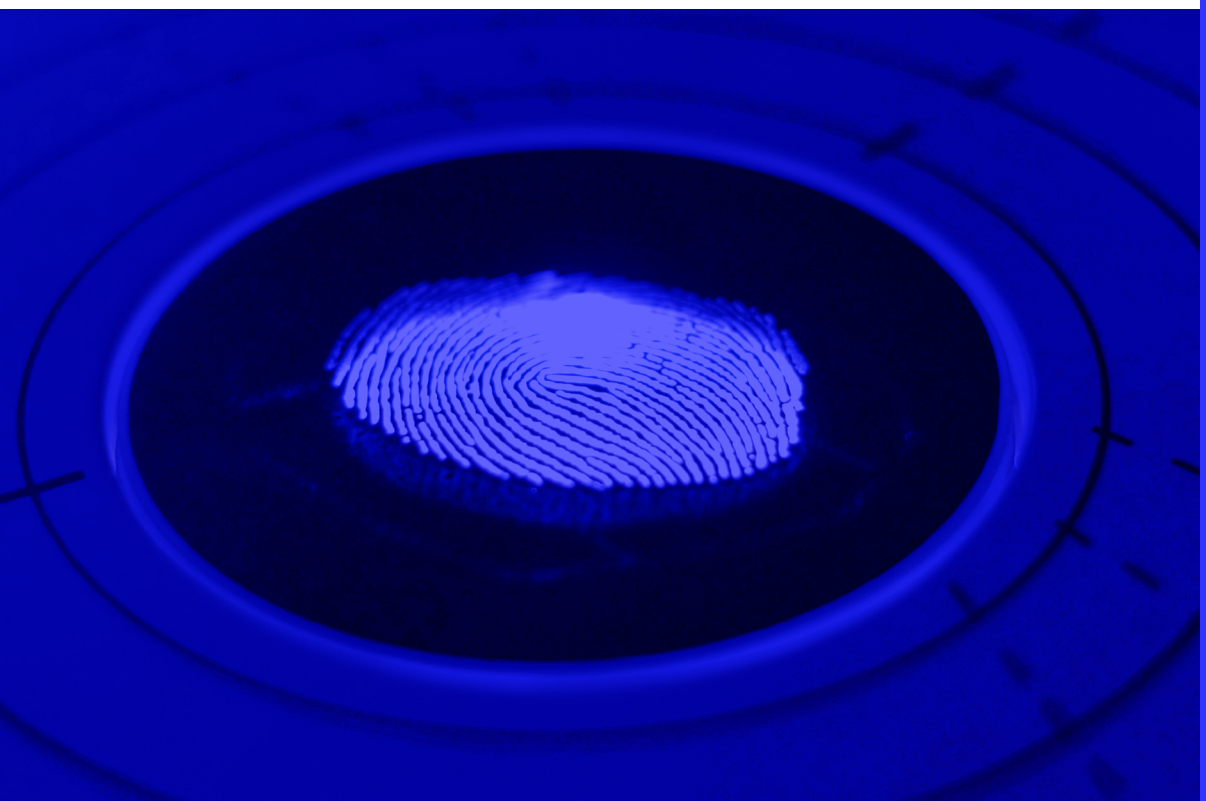
EBOOK

SECURE YOUR MODERN APPLICATIONS WITH AWS, GUIDEPOINT SECURITY, AND LACEWORK

Move Your Containers to the Cloud — And Get There Securely

aws marketplace

Table of Contents



The Rise of Containers Doesn't Mean Sacrificing Security

Whether your organization is migrating to the cloud or building cloud-native applications, chances are, you've begun your cloud adoption journey. Over the past few years, cloud adoption has grown immensely, to the point where 96% of organizations are using at least one public cloud, such as Amazon Web Services (AWS).[1]

In many cases, cloud adoption is spurred by the need to modernize legacy applications and take advantage of cloud scale and reliability. This is where containers come in. Containers, which are small packages that contain your application's code, configurations, and dependencies, ensure quick, reliable, and consistent deployments, regardless of environments. A containerized architecture, in lieu of a monolithic architecture, enables organizations to accelerate their application development, improve efficiency, and cut costs. Adoption of containers is in an upswing, so much so that Gartner estimates 90% of global organizations will be running containerized applications in production by 2026.[2]

While the mass exodus to the cloud and the uptick in containers have delivered major business value, for security leaders, the changes have also posed new questions about how to ensure workloads stay protected in dynamic cloud environments.

This ebook looks at how AWS employs a shared responsibility model for cloud security, how GuidePoint Security utilizes a five-phase approach to implement cloud security on AWS, and how Lacework Polygraph® Data Platform works in concert with AWS services to secure containerized applications.

[1] Flexera 2022 State of the Cloud Report, 2022, Flexera.

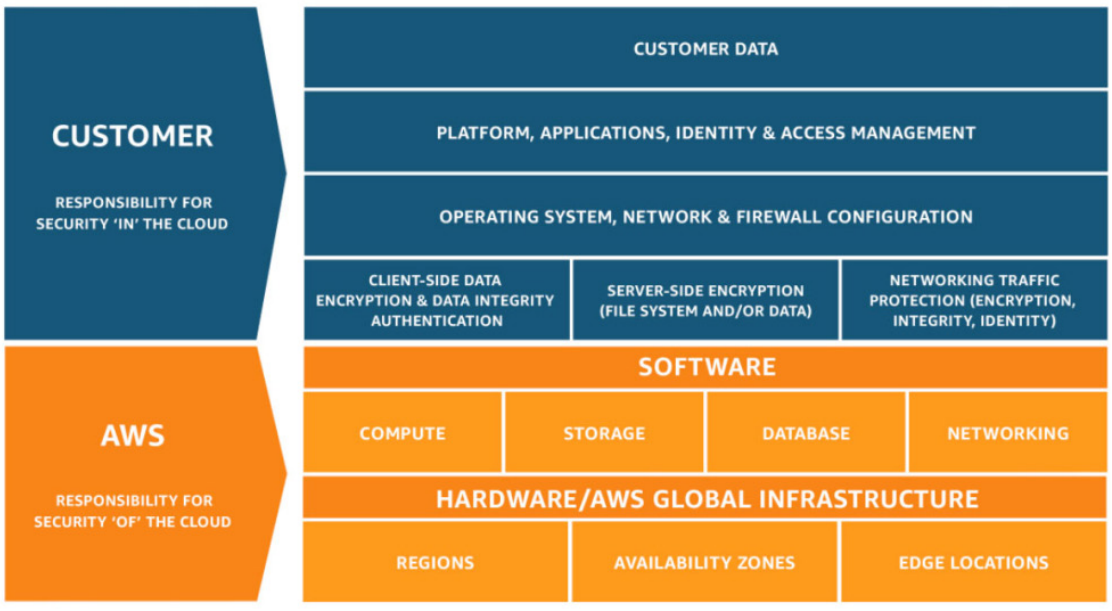
[2] Gartner, The Innovation Leader's Guide to Navigating the Cloud-Native Container Ecosystem, Arun Chandrasekaran, Wataru Katsurashima, August 18, 2021.

Sharing the Responsibility of Cloud Security

Security in the cloud is different than security on premises. On AWS, some of the security is taken care of for you, but other components are your responsibility. AWS outlines this ownership in its Shared Responsibility Model. Essentially, AWS is responsible for the underlying security of the cloud, and you're responsible for the security in the cloud. AWS structured the model this way, in part, to provide its customers a level of flexibility and control over their deployments.

On the infrastructure side of things, AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates.

As the AWS customer, your organization assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software, as well as the configuration of the AWS-provided security group firewall. In practice, protecting your workloads in the cloud aligns with the five basic units of the cybersecurity framework, which include identify, protect, detect, respond, and recover. Organizations often use a security service provider to augment these areas and deliver everything from governance and threat intelligence to endpoint security and incident response.



Building a Secure Cloud Architecture

Keeping the basics of the Shared Responsibility Model in mind, the first step is to define your AWS cloud strategy to maximize security. GuidePoint Security, an Authorized AWS Consulting Partner, has devised a five-phase approach that ensures your cloud security is built on a solid foundation that protects both operations and customers, while supporting current and future business needs.

1. FOUNDATION

The most important aspect to the five phases is making sure to build a strong foundation. You must initially determine your current posture, establish your baseline, and identify any major gaps that need to be remediated sooner versus later.

2. PERIMETER

In the cloud, you need to define a new boundary and determine your perimeter strategy. You may have a false sense of security about your network. Authorization and authentication could be weak. In addition, any compromise of a privileged AWS account will supersede anything you're doing on the network. As you build out your perimeter strategy, one of the early items you should address is identity access management along with a strong authorization process.

3. DATA PROTECTION

Encryption, key management, and secrets management services are major considerations for your data protection. In fact, many organizations choose to bring in a third-party solution to support these aspects.

4. VISIBILITY

When done right, you should be able to build a story around activity in your AWS environments. To efficiently collect, organize, and gain the right performance with your data, you need a logging platform that enables you to ingest logs and easily build search queries, or simply have an efficient way to identify particular events or anomalies.

5. CLOUD SOLUTIONS

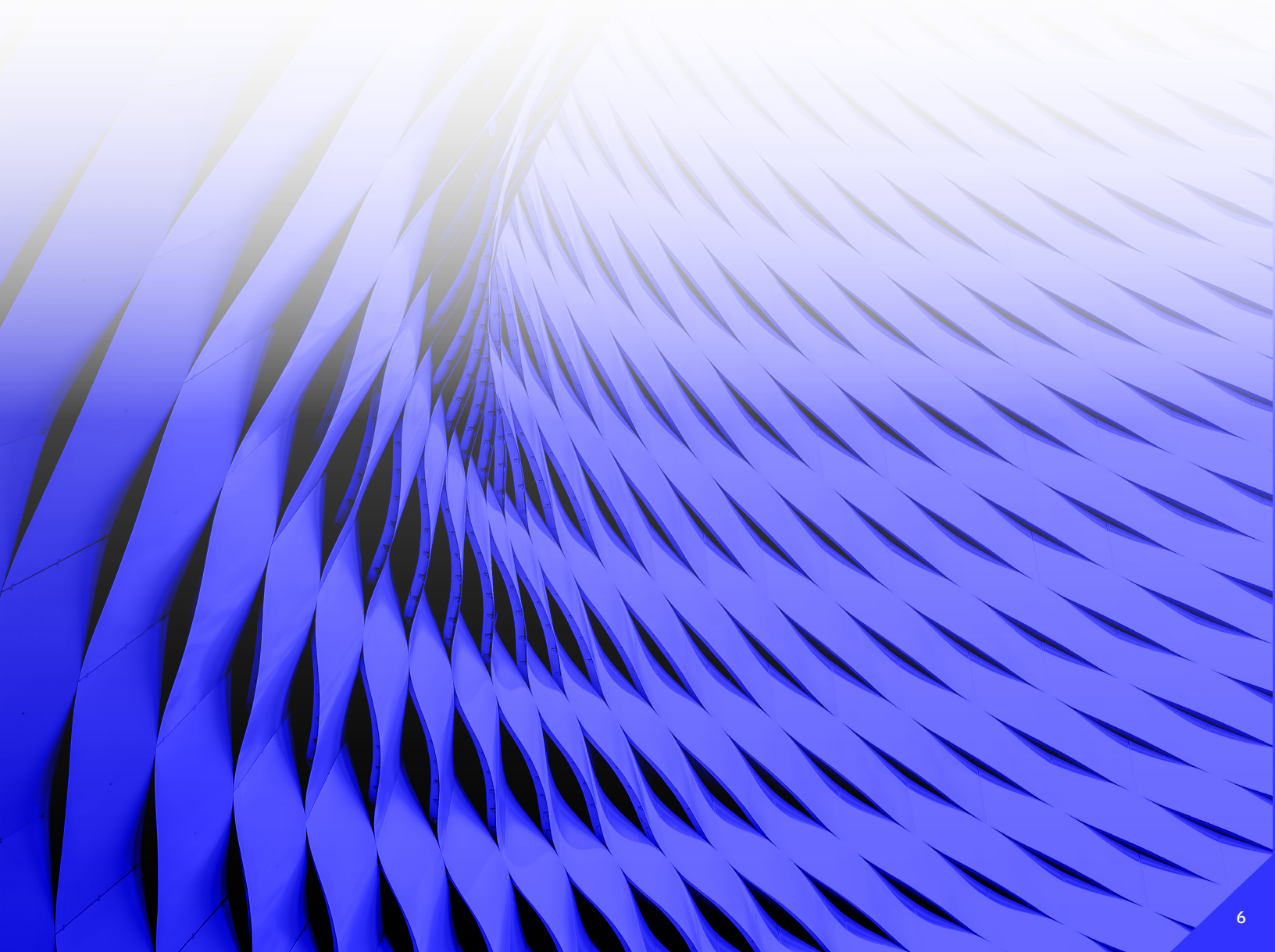
And finally, with a firm foundation and the other four phases implemented, you can address your cloud solutions. This phase includes your strategy for adopting new frameworks such as containers and cloud services like compute. Once this is in place, developers and engineers have the tools they need to safely build in the cloud.

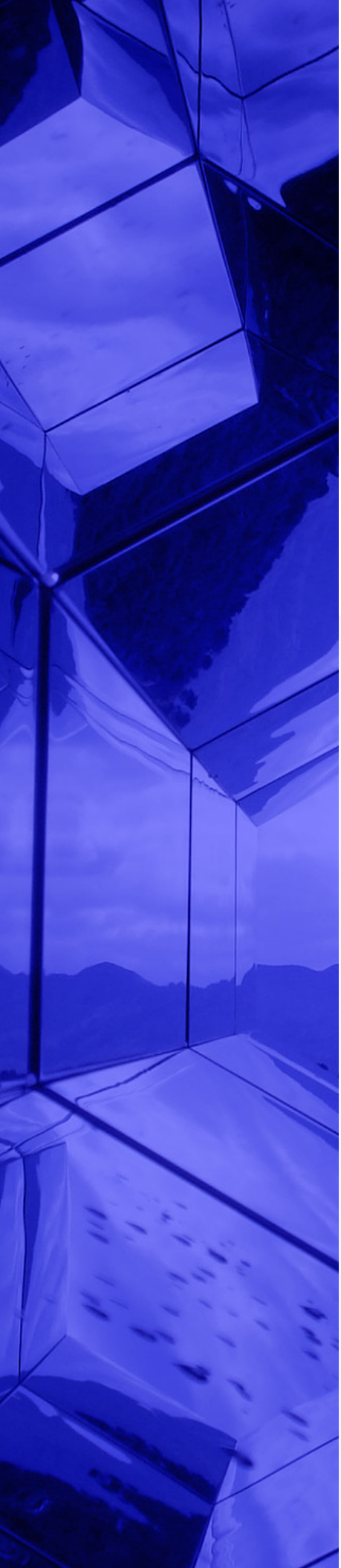
Deploying One Platform for All Phases

Regardless of which phase your organization is in, as you modernize applications and migrate workloads to AWS, it helps to have a security platform in place that can protect your dynamic cloud environments—no matter what.

Many organizations are turning to Lacework, an AWS Security Competency Partner, for a modern cloud security platform approach. The Lacework Polygraph Data Platform delivers end-to-end visibility into what's happening across your AWS environments, including detecting threats, vulnerabilities, misconfigurations, and unusual activity. The Platform automatically learns activities and behaviors that are unique to your environment, and surfaces unexpected changes, along with the full context to make investigations quick and easy.

The Platform ingests massive amounts of cloud and workload activity data and analyzes these interactions and behaviors. Using sophisticated algorithms, the Platform creates a detailed model of how your company's cloud systems operate, then it tailors its algorithm to your business, user base, and applications.





Containerizing Applications on AWS

When your organization is at the fifth phase—cloud solutions—containers will likely be a key component of the conversation. Containers give builders the tools to rapidly develop, package, and apply code to create applications anywhere, anytime.

On 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. The services you choose will depend on your needs for compute and container orchestration, as well as the level of management you'd like to take on.

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. The advantage is this combination abstracts away some of the tedious control-plane management.

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. The benefit to running containers with Kubernetes is it makes it easier to run multiple containers in an efficient way, with options to automate tasks like spinning up and down containers.

Keeping Containers Safe

Although containers speed innovation, from a security perspective, they also present new challenges around visibility and complexity. Security and operations teams must be prepared for faster release cycles and more entities to secure, while at the same time, less control over their environments. Because they increase the attack surface, containers can make it harder for security teams to identify vulnerabilities, threats, misconfigurations, and compliance violations.

The Lacework Polygraph Data Platform helps organizations of all sizes 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. 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:

Continuously monitor configuration changes and API activity. Center for Internet Security (CIS) Benchmark scans are performed during container image development and container deployment.

Additionally, the Platform 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.

Leveraging Native AWS Security

Because your containers will run on AWS, you can apply the AWS Shared Responsibility Model to better understand how security will be achieved together. Leverage native AWS features to bolster your security posture.

AWS INFRASTRUCTURE

AWS secures the underlying infrastructure of your application, including the Amazon EC2 compute resources, as well as the AWS global infrastructure, such as Availability Zones and Regions.

AWS IDENTITY AND ACCESS MANAGEMENT (IAM)

Control access to Amazon ECS by creating and applying IAM policies. With AWS IAM you can dictate who is authorized to spin up new pods and manage things like Amazon EKS clusters. This service provides full visibility into both the privileges that you're granting one service, as well as an AWS CloudTrail record of the use of those privileges.

AWS KEY MANAGEMENT SERVICE (AWS KMS)

For secrets management, you can securely store API keys, database credentials, and other secret materials in AWS KMS.

GUIDEPOINT SECURITY

LACEWORK

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 the **AWS Marketplace page**. You can also learn more about **Lacework solutions designed for AWS**, and check out the **Lacework page in AWS Marketplace**.

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

aws marketplace