EBOOK

Secure Your Containerized Applications

On AWS with Rapid7

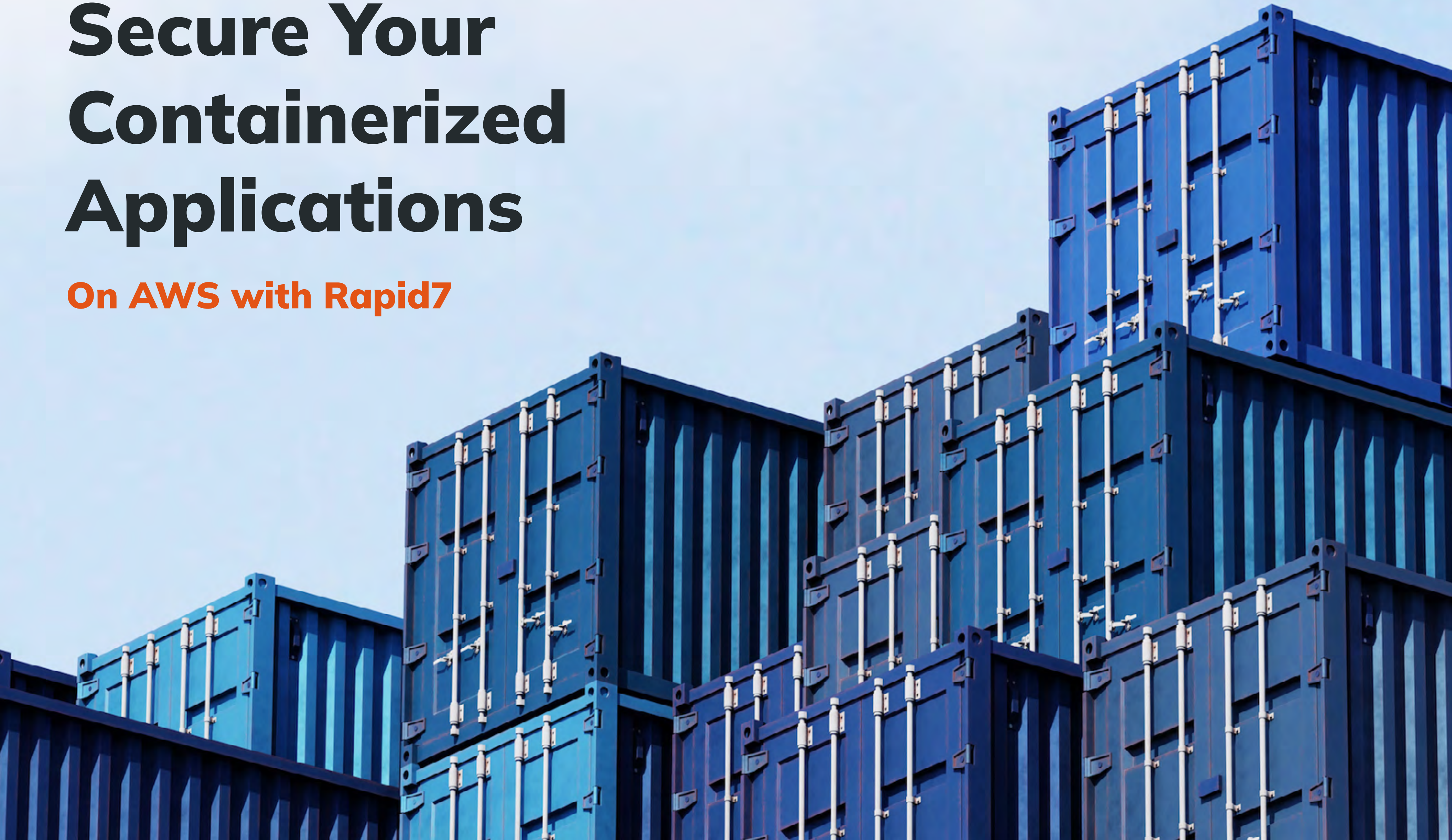

Table of contents

Cloud containers: A new way of shipping applications

Organizations have extensive experience in managing on-premises security for their monolithic applications. Yet many are now moving their applications to containers in the cloud to speed up innovation and be more agile. Cloud adoption, however, broadens an organization's attack surface and can introduce new security risks, leaving your applications vulnerable. As you enter the world of containerized applications, where security needs are vastly different, you'll quickly realize this new dynamic environment requires a new approach.

Successfully mastering containerized application management

When adapting your security practices to protect containerized applications, keep in mind these three main objectives: gaining real-time visibility into your entire container environment, and the cloud infrastructure they run on, being able to see—in complete context—what is running in your containers, and having the ability to automate risk alerts and remediation.

Context delivers the full picture
One of the biggest challenges with containerized environments is that often security teams are overwhelmed by the large volume of alerts that arise from having hundreds and thousands of containers running, all with various issues. This makes it hard to identify true risks and act on them in a timely fashion. You need additional context to prioritize the threat level associated with a resource, which you can only derive by collecting insights from every layer of the stack.

Real-time visibility keeps pace with the cloud
Real-time visibility is crucial because container environments shift on a second-to-minute basis and security teams often do not have a full picture of everything running in them. A security solution that only provides one daily scan, which may have worked in an on-premises environment or monolithic architectures, is not enough for containerized applications, with their dynamic activity.

Automation helps minimize alert fatigue
Because developers are constantly spinning up new containers and their components, you might have tens of thousands of resources to watch over. And with thousands of resources come even more alerts. The ability to automate repeatable notification and remediation processes is key for your security teams to keep pace and manage alerts quickly. Automation also quickly routes alerts to the developer or resource owner who has the authority to make a required change.

In sum, you need full control over your container environments to ensure they stay secure.

90%

of organizations will run containerized applications in production by 2026.[1]

[1] Gartner. "Gartner Identifies the Top 10 Strategic Technology Trends for 2020." October 2019.

Boosting container security on AWS

As you migrate your applications to containers on AWS, it's important you are familiar with the AWS Shared Responsibility Model to protect your applications.

What is the Shared Responsibility Model?

AWS is responsible for the security of the cloud while customers are responsible for security in the cloud. While AWS works to keep its infrastructure safe, you are in charge of IT controls such as encryption and identity and access management, patching guest operating systems, configuring databases, and employee cybersecurity training. For more information, visit the Shared Responsibility Model page.

Enhance your container security with the NIST cybersecurity framework

One way to understand how to protect your containers in the cloud is to use a security framework. These frameworks provide guidelines and best practices for securing your cloud environments. A popular framework is the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), which US federal agencies use to align their cybersecurity risk management. But a framework is only one piece of your security posture. To enhance your container security, you need appropriate tools and solutions to assess, build, and manage your alignment with the CSF.

Five categories of the NIST cybersecurity framework

Identify

Asset management, Business environment, Governance, Risk Assessment, Risk Assessment Strategy, Supply Chain Risk Management

Protect

Access Control, Awareness and Training, Data Security, Information Protection, Processes and Procedures, Maintenance, Protective, Technology

Detect

Anomalies and Events, Security Continuous Monitoring, Detection Processes

Respond

Response Planning, Communications, Analysis, Mitigation, Improvements

Recover

Recovery Planning, Improvements, Communication

AWS offers a wealth of resources for running containers and containerized applications in the cloud in accordance with NIST. Establishing fundamental security controls during container deployment should be your first step. Begin with a multi-account strategy and guardrails for identity and access management (IAM). These will make it easier to implement privacy, separation of duties, and least-privilege access. Protections are implemented for the entire AWS organization or specific users, actions, resources, and conditions when permissions are granted to IAM entities.

Rapid7 safeguards AWS container applications with enhanced security

In addition to the security resources that AWS offers, you can secure your containerized applications with the help of AWS Partner Rapid7. Rapid7 are cybersecurity experts that provide practitioner-first solutions across cloud security, threat intelligence, vulnerability management, and detection and response. Not only is Rapid7 an AWS Partner, it has also achieved the AWS Security, AWS Containers, and AWS Cloud Operations competencies. From securing container images pre-deployment to scanning production applications using coding best practices, Rapid7 is uniquely positioned to help you build out a secure containerized application development program.

Meet the Rapid7 solutions that help you build securely on AWS

insightCloudSec

InsightCloudSec is a cloud risk and compliance management platform that enables organizations to securely accelerate cloud adoption with continuous security and compliance throughout the entire software development lifecycle. The platform detects risk signals in real-time and in complete context, allowing your teams to focus on the issues that present the most risk to your business based on potential impact and exploitability.

insightIDR

InsightIDR - Rapid7's cloud-native SIEM and XDR solution - delivers highly efficient, accelerated detection and response. With InsightIDR's frictionless SaaS deployment experience, hyper intuitive interface, expertly vetted out-of-the-box detections, and automation - teams can feel confident that they're protected across their AWS and broader environment.

Shedding light on your container environments

It's uncommon for any one configuration error, vulnerability, or overly permissive role to provide enough background information for you to confidently prioritize risks across container environments and take prompt action. This is largely due to the enormous volume of unique risk signals produced by all your cloud resources and services. Many enterprise customers are running thousands of resources across numerous platforms. Because of this, the time it takes to identify and assess the severity of risk, and then prioritize and address it is extended. This adds to your security team's workload, contributes to alert fatigue, and can increase your overall level of risk because it takes longer to remediate critical issues.

InsightCloudSec separates the signal from the noise. It analyzes risks and provides rich contextual insight into every layer of the cloud container stack. Within 60 seconds or less, it enables teams to identify and prioritize remediation efforts on the vulnerabilities and misconfigurations that pose the greatest risk. When many teams first deploy InsightCloudSec, seeing the full extent of their attack surface can be truly eye-opening.

Integrating with AWS for further protection

InsightCloudSec offers a cloud detection and response capability that integrates with AWS services such as Amazon GuardDuty. This is a continuous security monitoring service that analyzes AWS container-specific logs to detect potentially unauthorized, malicious activity. Further, you can configure Amazon GuardDuty to have its logs forwarded to InsightIDR for log search, reporting, and automatic matching against community and Rapid7 MDR threat intelligence, giving you full visibility.

Eliminate blind spots with container scanning in real time

In your brave new containerized world, security needs to keep pace to protect your applications. The goal is to see alerts in real time—on everything from CPU to network usage—so you can see critical events, before it's too late.

InsightCloudSec continuously scans infrastructure, orchestration platforms, and workloads to enable real-time assessment of your cloud risk posture. Because everything is in a single location, you can easily monitor your container environments, getting a comprehensive, up-to-the-minute inventory of every asset across AWS. Thanks to the solution's agentless approach, which eliminates the need to include an agent in each container, InsightCloudSec accelerates time to value, decreases overhead, and eliminates blind spots.

In fact, Rapid7 solutions can scan containers in sub-minutes. You can start seeing scans on an open or exposed port often in less than 60 seconds, eliminating the need to wait hours, and allowing you to begin remediation immediately.

Integrating with AWS for further protection

InsightCloudSec can integrate with AWS Security Hub to vet cloud risk posture, centralize high-priority alerts, and automate actions triggered by security alerts across AWS environments. This integration helps security teams increase visibility as they work with IT and DevOps to secure their environments.

Automate remediation of critical risks

Stay alert by automating notifications

Due to the rapid pace of cloud innovation, security teams now have to manage an exponentially greater volume and variety of data. However, these environments are challenging for humans to manage alone due to the sheer volume of alerts, wide attack surfaces, and rate of change. This is where automation comes in.

InsightCloudSec automates the protective and reactive controls necessary for an enterprise to innovate quickly. InsightCloudSec automates cloud risk communication, starting workflows by integrating with your enterprise security systems, and ultimately automating the remediation of critical risks in real time. In essence, InsightCloudSec enforces an organization's standards and takes care of remediation for it.

InsightCloudSec accomplishes this by updating a misconfigured resource once it has been seen. Public access is then closed, all within 60 seconds. This is in sharp contrast to waiting hours before a vulnerability is detected, and then receiving a programmed alert notification, forcing security staff to manually update the resource.

InsightCloudSec can also automatically react to alerts for the entire platform and Amazon GuardDuty findings.

Integrating with AWS for further protection

InsightCloudSec enables automated monitoring and corrective action around access management, role management, identity authentication, and compliance auditing. You can integrate InsightCloudSec with AWS Config to manage configurations and identify misconfigurations automatically.

Your entire container security toolbox in a single solution

With better insights into associated risks, InsightCloudSec from Rapid7 enables you to continuously monitor all of your container services on a single, user-friendly platform. By providing complete context across the infrastructure, orchestration, workload, and data tiers, it enables real-time container risk assessment so you can build confidently on AWS.

Find Rapid7 solutions in AWS Marketplace and join the AWS Cloud Risk Assessment program.

AWS Marketplace

It's time for a different approach