Build and operate secure containerized environments at scale

Security best practices to help you thrive in the container era

This eBook is for technology and IT security professionals who are interested in exploring expert guidance for securing containerized applications and workloads at scale.

Table of contents

INTRODUCTION

Containers are reshaping the cloud

The growing adoption of containerized workloads is fundamentally transforming how applications are developed, deployed, and managed.

As Gartner projects that more than 95 percent of global organizations will be running containerized applications in production by 2028,[1] it is imperative that business and technology leaders evaluate their strategies in the context of an increasingly containerized world.

The advantages and challenges of containers

The appeal of containers is rooted in their portable, lightweight, and flexible nature. Unlike traditional application deployment, which requires developers to create separate versions of the application for each platform or operating system (OS) where it will run, containers encapsulate the application's code and its dependencies into one package that can run consistently in virtually any environment.

Containers can thus allow software engineers to be more efficient by developing applications faster and in a modular and more scalable manner. Within a cloud computing environment, containerized workloads can improve resource utilization, facilitate seamless deployment, and drive agility and innovation.

The dynamic, rapidly changing nature of a containerized cloud environment can lead to risks and challenges across visibility, manageability, and security, however. Further, securely operating a containerized environment requires unique capabilities and skills that differ greatly from traditional networks, which can cause further issues—especially for organizations that are just starting their container journey.

This eBook explores best practices for building and operating containers securely. It details the challenges of containerization, explores strategies for maximizing container advantages while minimizing risks, and demonstrates how Amazon Web Services (AWS) solutions can help organizations confidently and securely leverage the agility, speed, and dynamism of a containerized cloud environment.

[1] "A CTO's Guide to Navigating the Cloud-Native Container Ecosystem," Gartner, March 2023

CONTAINER CHALLENGES

Addressing container risks and challenges

There is little mystery as to why containers are growing more popular and prevalent across the cloud computing landscape. Improvements in development velocity and efficiency are driving the preference for containers among software engineers. And container benefits like increased agility, scalability, and resource optimization are high priorities among today's organizations, pushing adoption even further.

To achieve sustainable success in a containerized environment, organizations must have a security strategy that encompasses the security of the container image itself, the security of the environment into which the container is deployed, and the monitoring of container activities after deployment. This can help prevent enthusiasm and the immediate realization of benefits of container adoption from creating unchecked complexity or risk—and help the organization stay ahead of growing needs and changing requirements as its cloud ecosystem evolves.

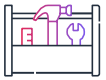
Challenges of containerized environments

Rapid scaling and dynamism: Containerized environments tend to grow more dynamic and complex as they scale. This is due to the ephemeral nature of containers, which can be quickly provisioned and destroyed, and the growing number of short-lived containers on the network. Containers used to facilitate upgrades and redeployments of new functionalities, for example, may exist only for brief moments before they dissolve. The rapidly changing nature of containerized environments can make it challenging to maintain visibility and track behavior.

New configurations: Containers have some unique configuration characteristics that are distinct from those found in traditional infrastructure or virtual machines (VMs). Choosing the ideal configuration for various scenarios—and understanding the security implications of a particular configuration—often requires a steep learning curve. Organizations need to get up to speed quickly to avoid compromising the environment outside of the container.

Insecure sources: Container images may be obtained from public or other insecure sources and may include outdated or unnecessary software packages. This can widen the attack surface in the container host and create additional security vulnerabilities.

Lack of expertise: As the containerized environment scales, the organization may need to bring on additional IT and security experts and provide training for new skills to help protect a dynamic and rapidly changing landscape. Skills shortages and resource restrictions may complicate or restrict this effort.



Limitations of existing tools: Existing network configurations and security tools may not be aware of all containers on the network and all code inside of them. Further, traditional security tools may not be able to operate at a container scale, manage the rate of change in a containerized environment, or have visibility into container activity.

BEST PRACTICES

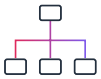
Approaching containerization with a focus on security

The rapidly scaling and dynamic nature of the containerized environment can make it difficult for teams to maintain visibility, control, and security throughout. This is especially true for organizations that are still relying on the tools and processes of traditional networks.

Incorporating these best practices can help your organization overcome these obstacles—so you can harness the benefits of containers while optimizing security.

Best practices for container security

Build in security from the start and at every stage: Embed container security into every step of the DevOps lifecycle, including build, development, deployment, and runtime stages. Invest in security products with allowlisting, behavioral monitoring, the ability to assess container workloads for vulnerabilities, and anomaly detection.



Adopt a multi-account architecture: Deploy a **multi-account strategy** and identity and access management guardrails to help implement the principle of least privilege, separation of duties, and privacy. Using multiple AWS accounts to help isolate and manage your business applications and data can help you optimize across most of the **AWS Well-Architected Framework** pillars, including operational excellence, security, reliability, and cost optimization.

Automate tasks to save time and reduce risk: Automated, software-based security mechanisms improve your ability to scale quickly, cost-effectively, and securely. Create secure architectures and implement controls that are defined and managed as code in version-controlled templates.

Establish a centralized logging account: Storing all logs in a centralized account can help with root cause analysis and attribution, allowing you to quickly identify, investigate, and remediate security incidents.

Protect data in transit, at rest, and at all layers: Classify your data into sensitivity levels and use mechanisms such as tokenization and access control where appropriate. AWS also recommends encryption as an additional access control to complement identity, resource, and network-oriented access controls. To protect data in transit, AWS advises leveraging a multilevel approach to address the physical, network, application, and transport layers.

80%

of all containerized applications in the cloud run on AWS[2]

[2] "Guidebook: Containers and Kubernetes on AWS," Nucleus Research, October 2019

AWS SERVICES

Layer AWS security services for container protection

AWS offers a range of services that can help your organization adhere to security best practices for containerized environments. With AWS, you can gain the visibility, control, and scalability needed to maximize success and minimize security risks so you can continue to move fast and stay secure.

AWS services for container security

AWS Security Hub is a cloud security posture management service that automates best practice checks, aggregates alerts, and supports automated remediation. The service monitors accounts and workloads for container-related misconfigurations and relays remediation steps to address them.

Amazon Inspector is an automated vulnerability management service that continually scans AWS workloads for software vulnerabilities and unintended network exposure. It automatically discovers and scans container images in **Amazon Elastic Container Registry** (Amazon ECR) for package vulnerabilities. Amazon Inspector can also scan container images that are built in continuous integration and continuous delivery (CI/CD) pipelines, such as Jenkins or TeamCity. This allows you to scan the image before it is checked into a repository and supports the DevOps strategy of validating the security early in the build stage. The service provides details on findings, prioritizes impact, and offers remediation steps.

Amazon GuardDuty is a threat detection service that continuously monitors your AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation. For customers using **Amazon Elastic Kubernetes Service** (Amazon EKS), the service automatically collects Kubernetes audit logs to help detect malicious activity associated with the control plane of Kubernetes clusters. It also offers broad runtime visibility, providing insight into on-host and OS-level activities and container-level context for potential threats to Amazon EKS and **Amazon Elastic Container Service** (Amazon ECS) workloads—including serverless workloads on **AWS Fargate**.

Amazon Detective simplifies the investigative process and helps security teams conduct faster and more effective investigations. It is container-aware, continuously aggregating telemetry into its graph model and analytics. The service allows you to pivot from the GuardDuty console to investigate root cause analysis of a container security finding. Plus, Detective automatically collects log data from AWS resources—leveraging machine learning (ML), statistical analysis, and graph theory for more efficient security investigations.

CONCLUSION

Next steps

Containerized applications can start up faster, scale with greater ease, and use fewer resources than their monolithic ancestors. As the use of containers scales across an environment, these and other benefits can become increasingly advantageous. Left unchecked, however, the security risks can also grow more pronounced with each container added to the network.

To reap the rewards and minimize the risks of containers, organizations must take care to implement the right strategies and tools from the start—and continue evolving and optimizing their approach at every step in the container journey.

AWS services like the ones outlined in this eBook can help your organization achieve the visibility and control needed to securely manage and protect today's containerized environments. With AWS, your organization can maintain its security posture as your network and its requirements expand. This allows you to forge ahead with confidence—and thrive in an increasingly containerized future.

Learn more about AWS Cloud Security ›