Akamai

WHITE PAPER

Delivering on the Promise of Containers

Simplifying and accelerating segmentation for critical assets and applications

Introduction

Containerization has rapidly emerged as the solution of choice for the deployment of applications in cloud and hybrid environments — and the proliferation of containers continues to accelerate. According to Gartner, 90% of global organizations will be running containerized applications in production by 2026 — up from 40% in 2021.[1] And according to a Forrester study for Capital One, **86% of IT leaders surveyed have prioritized the expanded use of containers for more applications**.[2]

> According to Gartner, **90% of global organizations** will be running containerized applications in production by 2026 — up from 40% in 2021

All of which, of course, puts added pressure on those responsible for securing IT environments to keep up with container deployment, particularly in a DevOps model that prioritizes rapid adoption and expansion. While a number of specialized container security solutions have sprung up, these platform-specific, container-only entities end up adding complexity and management overhead without addressing the enterprise data center as a whole — making life more complicated for security teams. What's needed is a single, comprehensive security solution that works consistently across all applications and technologies running in on-premises, cloud, and hybrid environments, including containers.

Before we dive into solutions, though, let's take a quick look at the container phenomenon, the forces driving it, and the implications from a security perspective.

The pressure's on: Business demands driving adoption

The movement toward containers and their projected growth in adoption can be traced back to the business demands being levied upon enterprise IT departments. Modern enterprises expect to be able to move with speed and agility in response to competitive threats and market opportunities. They need solutions that support innovation and accelerate time to market. And they're always looking for continual efficiency improvement. In an increasingly interconnected world, they want to make it easier to do business digitally, with suppliers and vendors, business partners, and especially their customers.

These are among the chief reasons enterprise IT is moving to the cloud, or more precisely to on-premises/cloud hybrid models. They are also the major drivers behind the DevOps trend, which seeks to speed deployment of critical applications by eliminating friction points from ideas to implementation, leveraging automation, and autoscaling to put applications into production more quickly.

> **"Organizations often underestimate the effort required to operate containers in production."**
>
> **— Gartner**

All this helps explain why IT departments have embraced containerization. Compared to virtual machines, containers are much easier and faster to launch, enabling just-in-time delivery with virtually no latency, and allowing teams to focus on "spinning up services, not servers." A key advantage of containers is portability for today's dynamic data center environments; they make it easier to migrate applications back and forth among on-premises facilities to multicloud instances. This is further enhanced through container orchestration via Kubernetes, or "K8s," which enables teams to deploy and manage higher volumes of containerized applications at scale across multiple environments. Orchestration is increasingly considered best practice in container implementation and management.

In short, containers enable IT to better respond to business demands for speed, automation, resiliency, and availability, and to do so at a lower total cost of ownership compared to other technologies. Implementation efforts, however, are not without drawbacks. "Organizations often underestimate the effort required to operate containers in production," says a 2019 Gartner report on containerization best practices.[3] Notwithstanding the popular appeal of containerization, the technology is still somewhat nascent, and best practices for secure deployment have not fully coalesced. According to the 2022 State of Kubernetes Security report from Red Hat, "security is [still] one of the biggest concerns with container adoption, and security issues continue to cause delays in deploying applications to production."[4] Clearly, enterprises cannot reap all the potential advantages of containers without an implementation strategy that necessarily includes cybersecurity.

According to the 2022 State of Kubernetes Security report from Red Hat, "**security is [still] one of the biggest concerns with container adoption**, and security issues continue to cause delays in deploying applications to production"

What does that mean for the security team?

"Security can't be an afterthought," Gartner asserts in its best practices report. "It needs to be embedded into the DevOps process." Too often, however, that's not the case. In the rush to implement containerization, security teams may sometimes feel like they're at the top of an "impossible triangle," an optical illusion also known as the Penrose Impossible Triangle (also known at Akamai as the Klein & Howard Impossible Triangle).

> Legacy security solutions aren't adaptable to the modern enterprise. Security solutions must be fast, adaptable, dynamic, and fit seamlessly into a "DevSecOps" approach.

In the same way the top point of the triangle appears illusively farther away than the other two corners, security appears to be lagging behind the business demands and the IT initiatives to meet them. But just as the triangle is an optical illusion, security solutions are actually closer than they appear. Teams simply have to think beyond the cumbersome, legacy solutions they've relied on in the past and look at solutions that map to the way enterprise IT delivers today and that fit seamlessly into a "DevSecOps" approach. That means a solution that is fast, adaptable, and dynamic, and that in itself employs the DevOps playbook approach. Most important is a solution that is decoupled from the underlying operating systems and platform to simplify implementation and management.

Klein & Howard Impossible Triangle

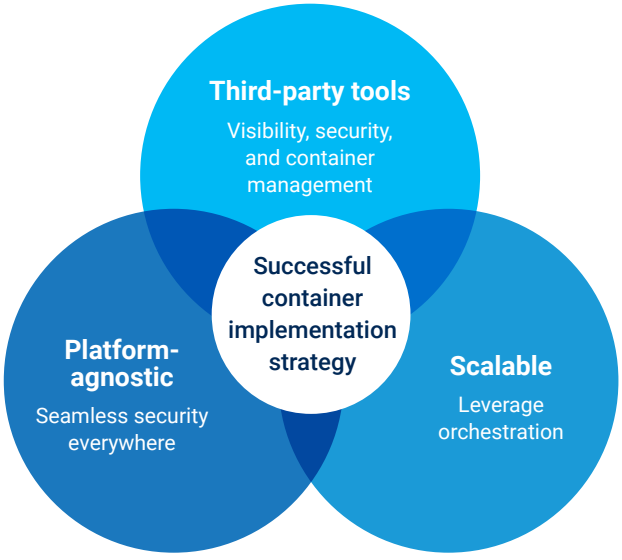
Why “native” is not enough

In the early days of virtualization and cloud migration, enterprises were often lulled into believing that cloud-native controls were sufficient for visualizing, managing, and protecting their workloads. Only after much trial and error did IT managers realize they needed an overlay management model incorporating third-party solutions that deliver security above and beyond native controls.

As Gartner and Forrester Research have said, a successful container implementation strategy is based on the “container trifecta”:

- Run containers in a portable, platform-agnostic manner that can be implemented anywhere across multiple cloud and on-premises architectures seamlessly
- Leverage orchestration to run and manage containers at scale
- Use third-party tools for container management, visibility, and security

Unlike past virtualization and cloud endeavors, the container industry has recognized from its inception that cloud-native management systems, and security controls specifically, are inadequate for an effective container strategy. In Gartner’s study of container management solutions, **65% of respondents said they intended to leverage third-party management tools to visualize, manage, and secure containerized workloads**.[5] However, these third-party tools need to work seamlessly across both on-premises and cloud instances and take a granular approach to avoid the pitfalls of cumbersome, mixed methods used in the past — such as security groups, VLANs, and firewalls, which offer zero visibility and negligible granularity.



Enable container adoption with Akamai Guardicore Segmentation

Akamai Guardicore Segmentation was designed to meet the challenges of today's dynamic, hybrid data center infrastructures. We provide comprehensive visibility into all applications and workloads running across multiple environments, and enable easily implemented, granular software-defined segmentation through the rapid creation, deployment, and enforcement of security policies around individual or logically grouped applications.

Let's be clear: Akamai Guardicore Segmentation is not a container-only point product. Rather, container security is a key capability of the platform, which works consistently across mixed environments that may also include bare-metal servers, virtual machines, serverless workloads, and remote devices. Accordingly, we provide organizations with a single, comprehensive solution for securing all data center and cloud assets regardless of where they reside or how they are deployed, eliminating the need to manage multiple point solutions. And because our solution is decoupled from the underlying platforms and operating systems, security policies follow applications and workloads as they move among on-premises and cloud environments — enhancing the portability factor that makes containers attractive for application deployment in hybrid-cloud infrastructures.

> Container security is a key capability of the Akamai Guardicore Segmentation platform, which works consistently across dynamic, heterogeneous data center environments

With respect to containers, Akamai Guardicore Segmentation works by placing agents on container host nodes, enabling visibility into the entire container cluster, including pod-to-pod and pod-to-virtual machine communication flows. This allows for very granular security policy implementation and enforcement by process, user, and fully qualified domain name (FQDN). In an orchestration scenario, we support K8s orchestration and allow visibility into Kubernetes and OpenShift metadata for superior context. A flexible labeling model enables operators to express policies using native K8s terminology. For K8s enforcement, we leverage the native Container Network Interface (CNI), a nonintrusive method for enforcing policies in K8s with no scale limitations. Dedicated templates enable users to ringfence Kubernetes business-critical applications — whether it's a namespace, application, or any other object. We also scale to K8s workload amounts and change rates. Since our solution also works across all of the other enterprise workloads in a similar manner, it serves as a single solution to visualize, manage, and secure assets across your entire enterprise.

Of particular importance in a DevOps environment, security policies you create will integrate effectively into continuous integration/continuous deployment (CI/CD) processes, helping ensure that security is not an afterthought, but fully integrated into the delivery model.

Conclusion

Containers are an increasingly integral part of many business environments. They can increase efficiency of resource usage, streamline processes, and enable increased portability and scalability. At the same time, the built-in security they provide is not enough, especially for businesses that utilize a hybrid environment.

As you look for a security solution that will grow with your company, be sure to choose a platform-agnostic tool that provides granular insights into your end-to-end processes, no matter where they occur. Akamai Guardicore Segmentation does that and more, offering the range of features and capabilities that modern enterprises require to be prepared for today and the future.

Using Akamai Guardicore Segmentation, your security team can achieve consistent security across dynamic, heterogeneous data center environments. In doing so, you can help IT teams deliver on the promise of containerization, realizing the rapid, cost-effective, and secure development and deployment of critical applications essential to your enterprise's business demands.

Simplify security across your entire environment. Learn more about our powerful unified security solution for containers and more: akamai.com/guardicore.

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

2 "Cloud Container Adoption In The Enterprise," Forrester, June 2020.

3 "Best Practices for Running Containers and Kubernetes in Production," Gartner, February 25, 2019.

4 "State of Kubernetes Security Report," Red Hat, May 2022.

5 "Gartner Forecasts Strong Revenue Growth for Global Container Management Software and Services Through 2024," June 25, 2020.