Guardicore

DELIVERING ON THE PROMISE OF CONTAINERS

A COMPREHENSIVE SECURITY SOLUTION

WHITE PAPER

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 is only likely to accelerate. Gartner predicts that by 2022, more than 75% of global organizations will be running containerized applications in production.[1] According to a 2020 Forrester study for Capital One, **86% of IT leaders surveyed have prioritized the expanded use of containers for more applications**.[2]

Gartner predicts that by 2022, more than **75%** of global organizations will be running containerized applications in production, up from less than 30% today.

All of which, of course, puts added pressure on those responsible for securing cloud environments to keep up with container deployment, particularly in a DevOps model that allows for rapid adoption and expansion. While a number of specialized container security solutions have sprung up, these platform-specific, container-only entities add complexity and management overhead while not addressing the enterprise data center as a whole — the last thing a security team needs What's needed is a single, comprehensive security solution that works consistently across all applications and technologies running in on-premise, cloud and hybrid environments.

First, though, let's take a quick look at the container phenomenon, what is driving it, and the implications from a security perspective.

THE PRESSURE'S ON: BUSINESS DEMANDS DRIVING IT

The movement towards containers and projected growth in adoption can be traced back to the business demands being levied upon enterprise IT departments. Enterprises today 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 look for continual efficiency improvement. In an increasingly interconnected world, they also want to make it easier to do business digitally, whether 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-premise/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.

[1] "Gartner Forecasts Strong Revenue Growth for Global Container Management Software and Services Through 2024," June 25, 2020, https://www.gartner.com/en/newsroom/press-releases/2020-06-25-gartner-forecasts-strong-revenue-growth-for-global-co

[2] "Cloud Container Adoption In The Enterprise," Forrester, June 2020, https://ecm.capitalone.com/WCM/tech/cloud-container-adoption-in-the-enterprise-report-capital-one.pdf

“Organizations often underestimate the effort required to operate containers in production.”

- Gartner

All of 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-premise facilities to multi-cloud 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 in deployment have not fully coalesced. In particular, according to a 2018 Forrester study on container security, 43% of respondents said that “security was a challenge hindering container adoption” — more than any other type of challenge.[4] Clearly, enterprises cannot reap all the potential advantages of containers without an implementation strategy that necessarily includes cybersecurity.

According to a 2018 Forrester study on container security, **43%** of respondents said that

“security was a challenge hindering container adoption”

— more than any other type of challenge.

[3] “Best Practices for Running Containers and Kubernetes in Production,” Gartner, February 25, 2019, https://www.gartner.com/en/documents/3902966/best-practices-for-running-containers-and-kubernetes-in-

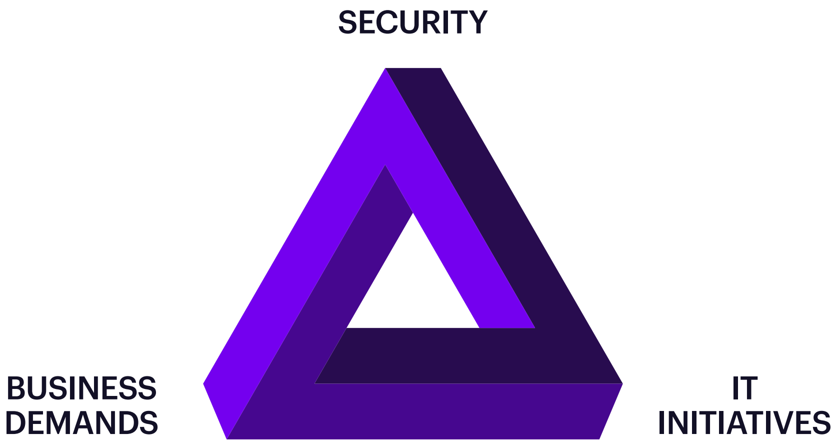
[4] “Now Tech: Container Security, Q4 2018,” Forrester, October 3, 2018, https://www.forrester.com/report/Now+Tech+Container+Security+Q4+2018/-/E-RES142078

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 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 seems 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 — 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

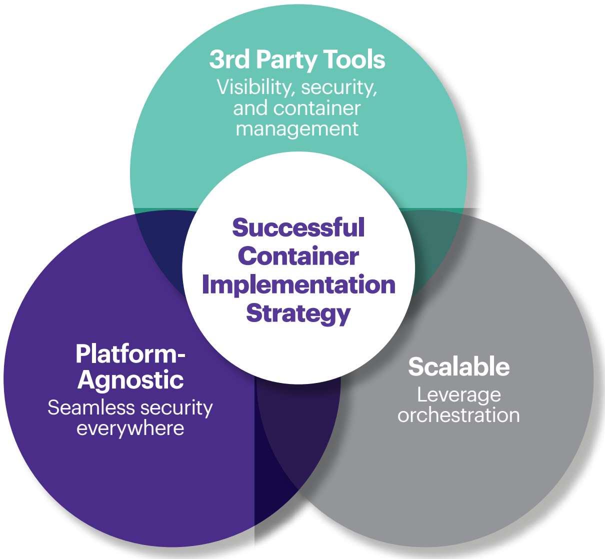
In the early days of virtualization and cloud migration, enterprises were often lulled into believing that cloud native controls were sufficient for visualizing, managing and protecting their workloads. Only after much trial and error did IT managers realize they needed an overlay management model that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

> *"Third-party tools are a must for container management, visibility and security."*
>
> - Gartner

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-premise 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 inception that native cloud management systems, and security controls specifically, are inadequate for an effective container strategy. In Gartner's 2020 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 on-premise and cloud instances and take a granular approach in order 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.


3rd Party Tools
Visibility, security, and container management
Successful Container Implementation Strategy
Platform-Agnostic
Seamless security everywhere
Scalable
Leverage orchestration

[5] "Gartner Forecasts Strong Revenue Growth for Global Container Management Software and Services Through 2024," June 25, 2020, https://www.gartner.com/en/newsroom/press-releases/2020-06-25-gartner-forecasts-strong-revenue-growth-for-global-co

THE GUARDICORE CENTRA PLATFORM: ENABLING CONTAINER EXPANSION

The Guardicore Centra Platform was designed to meet the challenges of today's dynamic, cloud-hybrid data center infrastructures. It provides comprehensive visibility into all applications and workloads running across multiple environments, and enables 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: Guardicore Centra 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 and serverless workloads. Accordingly, it provides 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 Guardicore is decoupled from the underlying platforms and operating systems, security policies follow applications and workloads as they move among on-premise 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 Guardicore Centra platform, which works consistently across dynamic, heterogeneous data center environments.

Simplified Container Security and More

Built for the modern enterprise, Guardicore Centra secures your entire environment.

	Guardicore Centra	Legacy Solutions
Granular, holistic visibility	✓	✗
Platform-agnostic; single pane of glass	✓	✗
No IP address or network changes	✓	✗
Segmentation in weeks (vs. months)	✓	✗

With respect to containers, Guardicore 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, Guardicore supports K8s orchestration and allows visibility into Kubernetes and Openshift metadata for superior context. A flexible labeling model enables operators to express policies using native K8s terminology. It also scales to K8s workload amounts and change rates. Since Guardicore Centra 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, Guardicore security policies 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 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 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. Guardicore Centra does that and more, offering the range of features and capabilities that modern enterprises require to be prepared for today and the future.

Using Guardicore Centra, 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. With Guardicore Centra, your company can realize 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 Guardicore's powerful unified security solution for containers and more:

www.guardicore.com

About Guardicore

Guardicore is the segmentation company disrupting the legacy firewall market. Our software-only approach is decoupled from the physical network, providing a faster alternative to firewalls. Built for the agile enterprise, Guardicore offers greater security and visibility in the cloud, data-center, and endpoint. For more information, visit www.guardicore.com or follow us on Twitter or LinkedIn.

Guardicore