Best Practices For Container Security

Protecting Containerized Applications Requires Technical And Organizational Steps

by Sandy Carielli and Andras Cser

July 24, 2020

Why Read This Report

Container adoption is increasing, and security must come along for the ride. Organizations value the scalability and agility that containers offer, but containers introduce new security challenges that can't be addressed with traditional tooling. To be successful, security pros must change their mindset about containers: They're not VMs or hosts. Security leaders should read this report to discover technical and non-technical best practices that they can adopt to protect their containerized application environments.

Key Takeaways

Traditional Security Tools Don't Apply In The Container World . . .

Commonly accepted security tools like vulnerability scanners, network forensics, and endpoint detection and response (EDR) are too heavyweight for a container environment. Security pros need tooling that is purpose-built for high scale, lightweight, ephemeral container environments.

. . . And Neither Does Traditional Thinking

It's time for a mindset shift. Security pros will struggle if they don't adapt existing requirements to the realities of containers. If your auditor simply hands you the same checklist for containers that they have used for VMs, your job is to educate them and work together to address new underlying risks.

Influence Vendor Roadmaps To Get The Right Features

A new crop of vendors has emerged to address container security challenges, forcing customers to adopt new tooling and build new relationships. While the market has matured, feature and coverage gaps are common, so expect to push your vendor in the direction you need to go.

Best Practices For Container Security

Protecting Containerized Applications Requires Technical And Organizational Steps

by Sandy Carielli and Andras Cser
with Amy DeMartine, Dave Bartoletti, Melissa Bongarzone, and Peggy Dostie

July 24, 2020

Table Of Contents

Recommendations

Related Research Documents

The Forrester Wave™: Cloud Workload Security, Q4 2019

Now Tech: Container Security, Q4 2018

Ten Basic Steps To Secure Software Containers

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Containers Accelerate Development But Challenge Security Teams

Technology leaders are jumping at the chance to implement containers in their organizations, citing scalability, agility, and cost reduction as top benefits. Container implementations range from fully on-prem to fully in the cloud; many firms use some combination of both. Firms have ramped up their investment in containers, with 33% of global developers telling us that their development organization currently uses containers and another 25% indicating that they would like to do so in the next 12 months (see Figure 1). Security teams, however, often find themselves figuring out security for containers after the development team has adopted them. As security teams scramble to figure out what it means to protect a containerized environment, they find that:

- **Traditional tools flounder in container environments.** Traditional security tools such as vulnerability scanners, network forensics, host-based firewalls, EDR, and security analytics are too heavyweight for monitoring containers and container orchestration platforms like Kubernetes. Security, development, and infrastructure and operations (I&O) professionals told Forrester that to effectively scan, deploy, and monitor container images and instances they need dedicated, lightweight tools whose agents are built for container clusters and distributed, containerized apps. Reporting and dashboarding must be specific to containers, which are often widely distributed and transient.

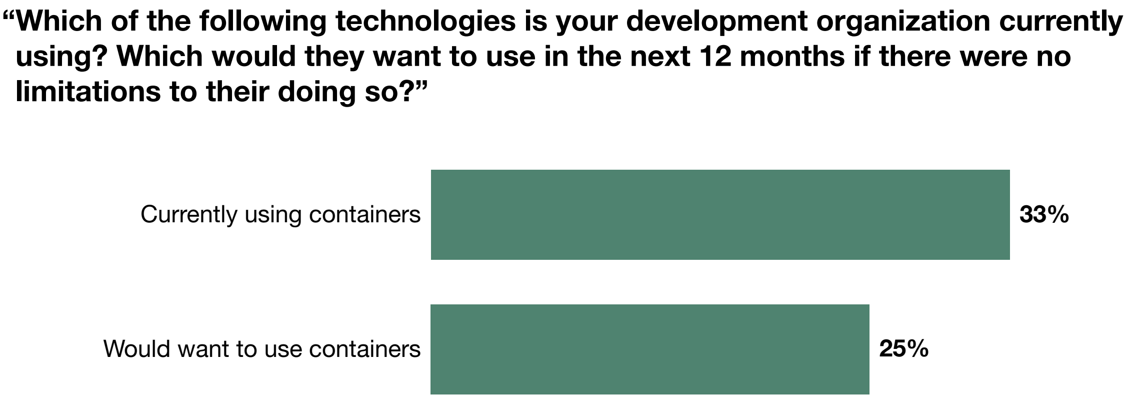
- **Overstuffed container images are difficult to secure.** Container image repositories contain images (especially Windows) that are too big and as a result insecure. Simply put, because of time pressures and pure convenience, developers tend to cram too many tools, libraries, and agents into container images. These images not only take a long time to deploy and consume high levels of CPU, RAM, disk, and network resources, but are also hard to perform vulnerability scanning and configuration management on. A North American software vendor said that in their container environment they “need to perform the frustrating but necessary refactoring and find where dead bodies are buried.”

- **Gaps in awareness lead to mindset clash.** The security leader of a healthcare company relayed the challenges of mapping existing processes and tools to containers and noted that standards like PCI sometimes contain requirements that don’t make sense for containers. A related challenge was dealing with auditors requesting an inventory of all containers or expecting to see a scanning agent deployed on each container. If security, compliance, and legal stakeholders attempt to treat containers like VMs or focus only on scanning during runtime, they will face a series of muddled conversations and incur high costs on their way to insufficiently meeting security requirements.

- **Container sprawl introduces runtime complexity.** Security pros are challenged by the logistics of managing different orchestration platforms, different container types, and different runtime environments, often with tooling that only supports limited types of containers and runtime environments. Implementation details vary between these environments, adding another layer of complexity as security teams attempt to monitor container behavior and implement appropriate access controls.

- **Gaps in controls make it hard to ensure image integrity and authenticity.** Just as organizations face container sprawl, they also face container image sprawl. Images originate from various repositories, and developers may use them as is or modify them to meet their needs. Without a clear set of baseline images, container registries to help manage them, and controls to ensure image authenticity, firms risk deploying containers built on unmanaged or malicious images.

FIGURE 1 Organizations Are Eagerly Adopting Containers



Base: 2,073 global developers

Source: Forrester Analytics Business Technographics® Developer Survey, 2020

Container Security Spans Development And Deployment

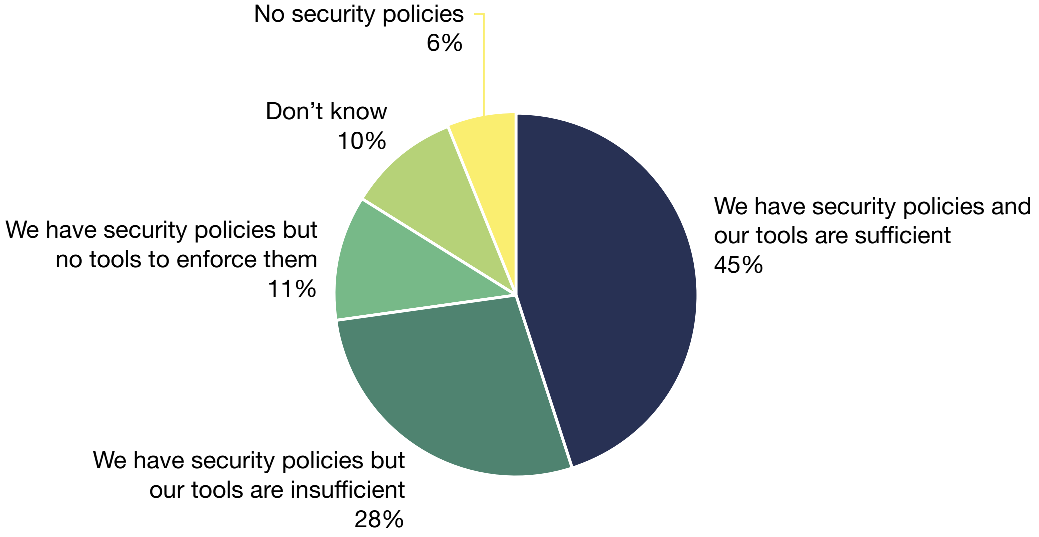
As container security has taken off, customers have adopted container security policies and invested in tooling throughout the lifecycle. Some 84% of global security decision makers report that they have security policies in place for the use of containers: While only 45% report that they have enough tooling in place to support those policies, there are signs of progress (see Figure 2). In the next 12 months, 36% of security pros who are implementing/expanding container security plan to implement it during testing, 37% plan to implement it in development, and 20% plan to implement it during design (see Figure 3). When implementing container security policy and tools, keep in mind that:

- **Security and development team collaboration is common.** While decision making around container security varies between organizations, joint ownership between security and development teams is common. A few firms described a structure where the development team owns the day-to-day decision making and the security team lays out broad requirements, sets policy, or has veto power over certain decisions. One security leader shared their aspirations to move container security decisioning from a dev ownership model to one where the security team defines policy and provides tools to enable the dev team to implement that policy.

- **Container security market is starting to mature.** The emergence of new tools and vendors in container security has been confusing for customers; however, we are in the early stages of consolidation. Platform providers like Trend Micro have added container security functionality, while Palo Alto Networks went the acquisition route and picked up Twistlock. On the development side, SCA vendors like Snyk have extended into container security through image scanning. Meanwhile, leading container and orchestration platform providers, along with cloud workload and host OS providers, offer some security measures natively while also partnering with specialists.[1]

FIGURE 2 Security Respondents Have Adopted Container Security Policy But Need To Accelerate Tooling

"Does your firm have security policies and tools in place for the use of containers?"

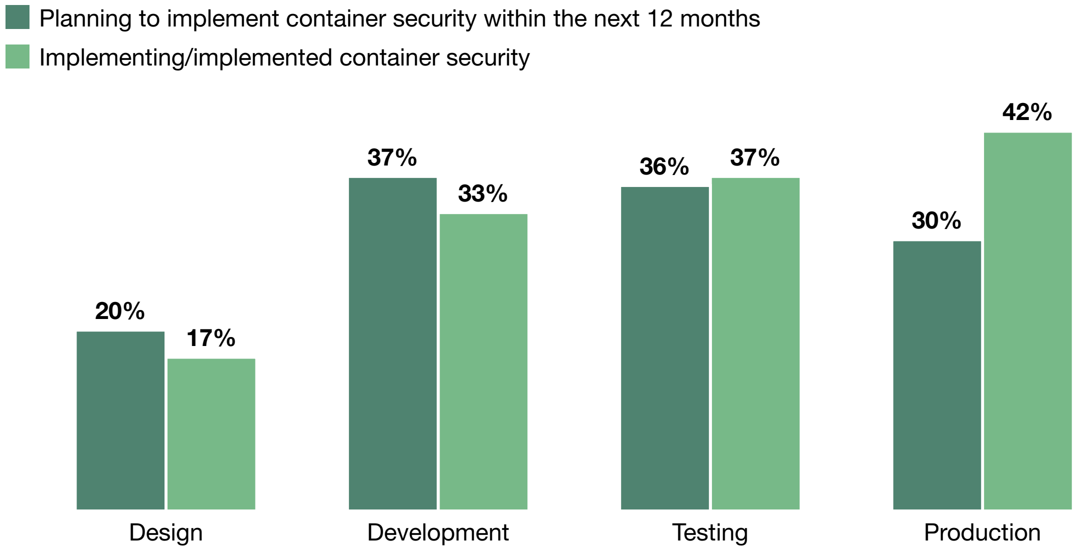


Base: 3,438 global security technology decision makers (20+ employees)

Source: Forrester Analytics Global Business Technographics® Security Survey, 2019

FIGURE 3 Container Security Pushes Left In The Software Development Lifecycle

"In what phase of the application development lifecycle do you plan to implement or are you implementing container security?"



Base: 291 (planning) and 794 (implementing) global security decision makers whose firms are adopting container security

Source: Forrester Analytics Global Business Technographics® Security Survey, 2019

Adopt These Container Security Best Practices

Container security is a complex and rapidly changing field. We looked at container security best practices from the: 1) technical and 2) non-technical perspectives. Protecting data stored in and moving between containers is the primary motivation.

Implement Technical Best Practices In Development And Deployment

Container security starts with having a solid technology foundation for containers. Your firm can only safely realize the benefits of containerization if it pays attention to appropriate technical container security measures. You must:

- **Adopt strict change control policies for images.** Scanned and verified "golden images" are the bedrock of your container security. Start with a single image registry with version control that is an integral part of your firm's software development lifecycle process. Begin with a known baseline: Always start from scratch, use private images, and after you've scanned, secured, and tagged them, check them into your internal registry. Publish this image as the "golden image" for internal consumption. An interviewee mentioned that if the most current image version is "N," their SDLC process only allows the firm to use the previous, "N-1" image, but nothing older.

- **Apply Zero Trust principles to container deployments.** The admin access credentials to the container orchestration platform should be managed just like any other privileged account, and you will need a container-compatible secrets solution like CyberArk or HashiCorp. Employ role-based access control for the rights for container orchestration system admins and minimize privilege sprawl. Pay attention to who can push containers into the registry: Best practice is to only allow CI/CD tools and build pipelines to check-in containers into the registry. It's imperative that you not store secrets in images and that you harden images by removing all unnecessary software components, libraries, configuration files, etc. Define and enforce segmentation and microsegmentation between containers to limit processes in one container to communicate with authorized processes in other containers (solutions like Guardicore and Illumio help here).
- **Prioritize automation and forget runtime patching.** Manual processes in containerland won't cut it: Not only are they slow (and against the grain of DevOps mentality), but they're also painfully inaccurate and insecure. Be sure that everything is scripted: A North American media streaming company told us that it started container build, configuration, and deployments with scripting. They paid special attention to automate all processes, including vulnerability scanning. Automation also helps with easy and efficient handling and automated deployment of a large number of minimally sized, carefully assembled, and secure containers. Patching containers at runtime is a bad idea; all interviewees recommend against it because it's not a DevOps-friendly process and can counteract build pipeline configuration and image scanning.
- **Use templates to simplify policy and ensure consistency.** Create container templates that encapsulate basic security baselines, such as secure network and kernel configurations, or regulatory specific baselines that meet HIPAA, PCI, CIS, etc. requirements. Use template inheritance to safely create descendants of a template and minimize configuration change processes. The build process must carefully log and audit template changes and track which final container images inherit from which templates.

Augment Technical Best Practices With Education, Vendor Relationships, And Policy

Security pros must move beyond the technical tools to build a successful container security strategy. When considering container security, don't forget to also:

- **Train continuously to mitigate organizational challenges.** Many security pros find themselves jumping into containers and Kubernetes without understanding how it works and how it's different. Address the necessary mindset shift head-on with regular training, and reinforce the point that this is a significant change. One security leader recommended regularly running through scenarios. Another makes sure to cover container basics and best practices at their annual developer conference. Make the training relevant by tailoring it to issues that you and your team have seen.

- **Partner with your container security vendor on its product roadmap.** Thinking beyond features and platform support, security pros considered roadmap influence when they selected their container security vendor — they wanted a vendor that they could work with, that would accommodate feature requests, and that would ask for their inputs on priorities. With the container security market still maturing, now is the best time to push your vendor's roadmap. Don't engage with vendors that aren't willing to listen to your feature requests.
- **Establish and document container governance and policy.** Security leaders stressed that a global policy must be documented in order to be successful — the document will give you something to stand behind when presenting requirements to the development and I&O teams. Develop a policy with a defined SLA for remediations and clearly identified escalation paths. In addition, document your platform access control policies, specifically noting who has access to containers.

Recommendations

Tailor Your Container Security Roadmap

The security, development, and I&O teams must collaborate to identify the most pressing problems in their container deployment and compare current implementation and processes to best practices. Prioritize your container security roadmap according to your top challenges and the best practices that address them (see Figure 4).

FIGURE 4 How Best Practices Address Challenge Linkages

	Problems				
Recommendations	**Traditional tools flounder**	**Overstuffed images**	**Awareness gaps**	**Container sprawl**	**Control gaps**
Adopt strict change control policies for images		●			●
Apply Zero Trust principles to container deployments			●	●	
Prioritize automation and forget runtime patching	●			●	●
Use templates to simplify policy and ensure consistency		●		●	
Train continuously to mitigate organizational challenges			●		
Partner with your vendor on its product roadmap	●		●	●	
Establish and document container governance and policy		●	●	●	●

Supplemental Material

Survey Methodology

The Forrester Analytics Business Technographics® Developer Survey, 2020, was fielded in January and February 2020. This online survey included 2,073 respondents in Australia, Canada, France, Germany, the UK, and the US.

The Forrester Analytics Global Business Technographics Security Survey, 2019, was fielded between April and June 2019. This online survey included 3,890 respondents in Australia, Canada, China, France, Germany, India, the UK, and the US from companies with two or more employees.

Forrester Analytics' Business Technographics ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of business and technology products and services. Dynata fielded these surveys on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates.

Please note that the brand questions included in these surveys should not be used to measure market share. The purpose of Forrester Analytics' Business Technographics brand questions is to show usage of a brand by a specific target audience at one point in time.

Companies Interviewed For This Report

We would like to thank the individuals from the following companies who generously gave their time during the research for this report.

Aqua Security

Palo Alto Networks

Qualys

Sectigo

Snyk

StackRox

Sysdig

Endnotes

[1] See the Forrester report "Now Tech: Container Security, Q4 2018" and see the Forrester report "The Forrester Wave™: Cloud Workload Security, Q4 2019."

FORRESTER®

forrester.com

We work with business and technology leaders to drive customer-obsessed vision, strategy, and execution that accelerate growth.

PRODUCTS AND SERVICES

- Research and tools
- Analyst engagement
- Data and analytics
- Peer collaboration
- Consulting
- Events
- Certification programs

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO

B2B Marketing

B2C Marketing

Customer Experience

Customer Insights

eBusiness & Channel Strategy

Technology Management Professionals

CIO

Application Development & Delivery

Enterprise Architecture

Infrastructure & Operations

› Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.