anchore

Anchore 2021 **Software Supply Chain Security Report**

Enterprise Practices for Securing the Cloud-Native Software Supply Chain



64% *of organizations have been impacted by a software supply chain attack in the last year*

anchore

CONTENTS

Introduction **4**

Executive Summary **4**

Attribution Requirements for Sharing Charts **4**

Methodology **5**

Highlights **6**
- Growing Container Use Creates New Security Challenges 6
- Increasing Focus on Software Supply Chain Security 6
- Room for Improvement in Supply Chain Security 6
- Organizations Face Scanning Challenges 7
- Diverse DevOps Toolchains Create Risks That Require Security Attention 7
- Organizations Use Multiple Container Platforms 7

Respondent Demographics **8-10**

Growing Container Adoption Creates New Security Challenges **11**
- High Levels of Container Maturity 11
- Container Maturity Not Limited to Tech-Focused Industries 11
- Container Adoption Will Continue Strong Growth 12
- Containers are Used for All App Types 12
- Perceived Risk of Containers is Similar to Traditional Apps 13
- Advanced Container Users Perceive Higher Risks 13

Enterprises Are Focused on Securing the Software Supply Chain **14**
- Software Supply Chain Attacks Have Broad Impact 14
- Enterprises Focus Strongly on Software Supply Chain 15
- Mature Container Users Give Supply Chain More Focus 15
- Software Supply Chain Security is a Top Initiative 16

Container Security Gaps Threaten the Software Supply Chain **17**
- Open Source is the Top Container Security Challenge 17
- Respondents Underestimate Amount of Open Source Used 17
- Limited Use of Supply Chain Best Practices for Containers 18
- Development Toolchain is a Blind Spot for Many 18

Organizations Face Container Scanning Challenges **19**
- Organization Must Comply with Multiple Standards 19
- Moderate Use of Container Scanning Best Practices 19
- Organizations Face Container Scanning Challenges 20
- False Positives are a Significant Problem 20
- Container Security Requires Significant Collaboration 21
- Development Teams are Designating Security Champions 21

DevOps Toolchains Require Security Attention **22**
- DevOps Processes are Broadly Adopted 22
- DevSecOps is on the Rise 22
- Diverse Set of DevOps Tools 23
- DevOps Tools Used 23

Multiple Container Platforms are Used **24**
- Multiple Container Platforms are Used 24
- Number of Containers Running in Container Platforms 24

Recommendations **25**

About Anchore **26**

Introduction

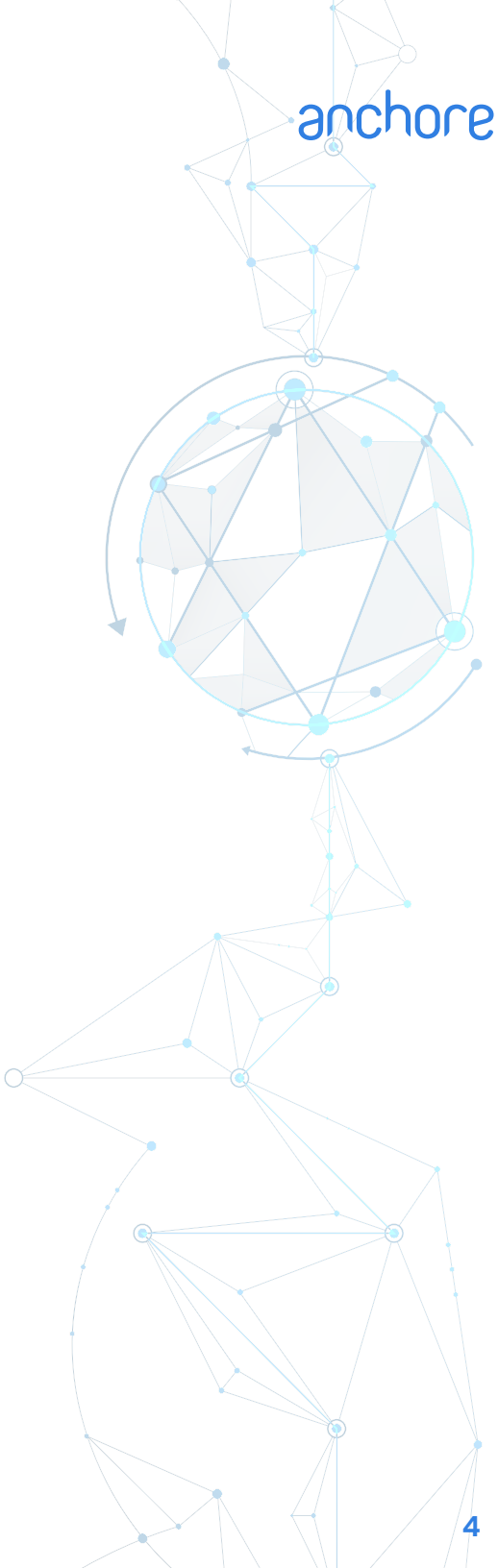
This report compiles the responses of 425 IT, Security, and DevOps leaders to identify the latest trends on how organizations are adapting to these new security challenges of the software supply chain. As enterprises increasingly move to cloud-native software, this report includes a special focus on the platforms, tools and processes used to secure the growing volume of software containers.

Executive Summary

The widespread use of DevOps processes to speed development has led to a concurrent rise in the use of software containers, with 65 percent of respondents reporting a significant number of their applications running in containers. While technology-focused industries, such as cloud service providers and software companies, lead the way in container adoption, traditional industries such as healthcare and financial services are also reporting significant container use.

Containers make it easy to package software during development, but commonly bring in multiple open source (OSS) or third-party dependencies as applications move through the DevOps pipeline, creating new security requirements. As a result, technical leaders ranked open source security and gaining a full understanding of the software bill of materials as top challenges.

Recent attacks such as SolarWinds have highlighted the risk in the software supply chain, and the Codecov attack specifically targeted containerized applications. With almost two-thirds of respondents reporting impacts from attacks in the last 12 months, organizations must now protect their software supply chain by adapting and extending existing processes to secure containerized software.



Methodology

This is the first report to provide an enterprise-focused view of practices for securing the software supply chain as provided by 425 IT executives and leaders.

Unlike many surveys that focus on developers and smaller organizations, this report is based on a survey of 425 vetted executives, directors and managers in IT, Security, Development and DevOps functions between May 1 and May 18, 2021. The respondents are exclusively from large enterprises that span a wide variety of industries. They range in size from a minimum of 1,000 employees to the largest organizations.

The respondents are located in North America and Europe and come from a vetted independent panel that validates their organizations and roles. Their responses provide a manager's unique perspective into current enterprise security practices and challenges.

Attribution Requirements for Sharing Charts

We encourage the reuse of data, charts and text published in this report under the terms of the **Creative Commons Attribution 4.0 International License**.

You are free to copy and redistribute the material per the terms of the license, but you must provide attribution to the **Anchore 2021 Software Supply Chain Security Report**.

Highlights

anchore

The Anchore 2021 Software Supply Chain Security Report identifies a number of trends in securing the software supply chain with a special focus on the impact of increased use of software containers.

Growing container use creates new security challenges

- Overall, 65% are at intermediate or advanced levels of container maturity, with cloud service providers and software organizations reporting the highest levels of maturity
- 55% of respondents in healthcare and 49% in financial services reported significant use of containers
- 84% plan to increase container use and 29% will increase container use significantly
- Respondents use containers for both internal applications and software products they sell
- 38% of advanced container users see containerized apps as higher supply chain risk vs 16% of beginner container users

Increasing focus on software supply chain security

- On average, organizations must comply with 2.7 standards for containerized apps
- 60% have made securing the software supply chain a top or significant area of focus
- Experienced container users are focusing more heavily on supply chain security
- Top initiatives are increasing container use (63%) and improving supply chain security (60%)

Room for improvement in supply chain security

- 23% rank OSS as top container security challenge, while 19% rank understanding the full software bill of materials (SBOM) as their top challenge
- Container users underestimate OSS as 26% of components/code (vs actual benchmarks of 70% per Synopsys 2020 Open Source Security and Risk Analysis Report)
- Less than half use container security best practices of scanning OSS containers and using private repos for dependencies
- Only half are using infrastructure-as-code to secure the DevOps toolchain

Highlights

anchore

Organizations face scanning challenges

- 64% have been affected by software supply chain attack in the last year
- While many orgs are scanning containers, most report challenges in identifying vulnerabilities (86%), too many false positives (77%), and getting developers to spend time remediating issues (77%)
- On average, respondents estimate that 44% of vulnerabilities found are false positives
- Security, Development, and DevOps have significant involvement in container security activities, which means collaboration is required
- 77% of orgs are designating security champions within Dev teams to facilitate tighter collaboration

Diverse DevOps toolchains create risks that require security attention

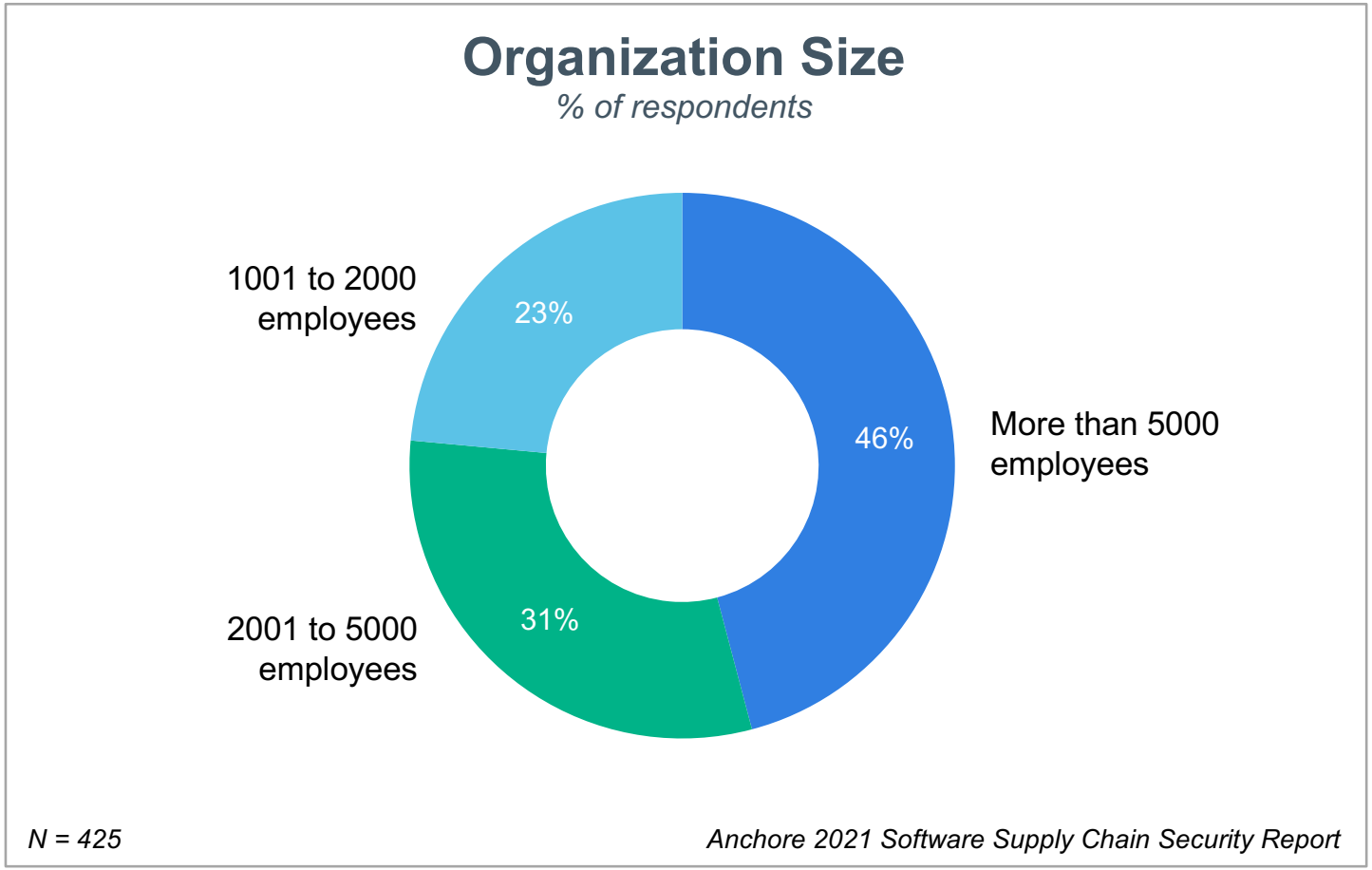
- Virtually every org is adopting DevOps, with 47% using it on at least half of their software projects
- 42% have implemented a DevSecOps Center of Excellence with 37% planning to create one
- Only 20% of orgs have a single CI/CD tool used by all teams, while 28% enable each team to choose their own tools
- Respondents identify a median of 6 different DevOps tools used
- The most used tools for DevOps include GitHub (78%), Azure DevOps (56%), Docker Hub (50%), GitLab (48%), and Jenkins (47%)

Organizations use multiple container platforms

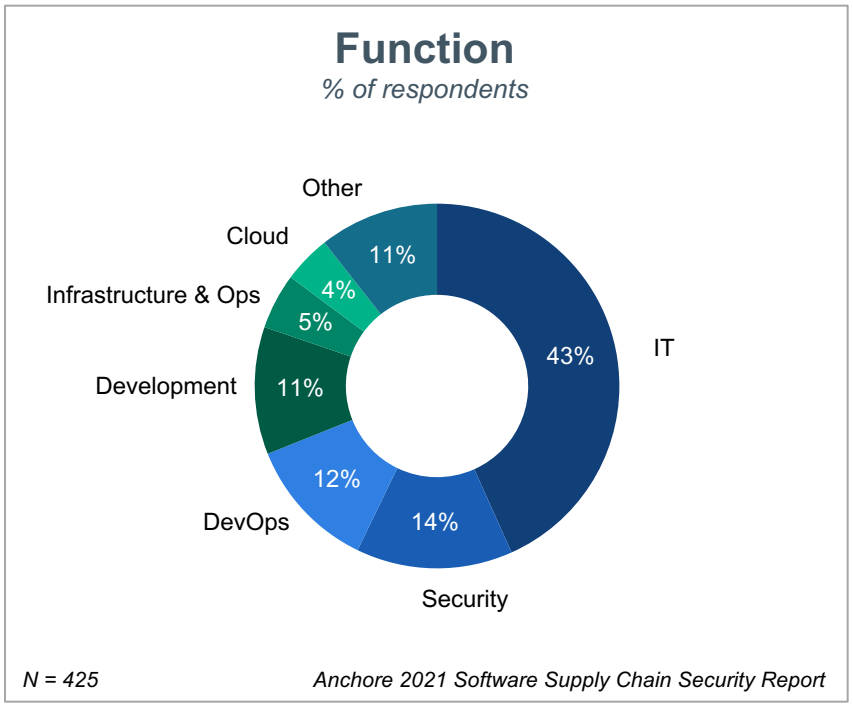
- Organizations use a median of 5 container platforms across production and development
- "Standalone" Kubernetes that is not part of a PaaS service—but may be run on-premise, hosted or even on cloud IaaS—is used most often by 71% of respondents
- The second most used container platform is Amazon ECS (56%)
- Tied for third place (53%) are Amazon EKS, Azure Kubernetes Services, and Red Hat OpenShift
- The container platforms most cited as running large workloads (1000+ containers) are "Standalone" Kubernetes (7%), Amazon ECS (7%), Amazon EKS (7%), Azure Kubernetes Service (7%), and SUSE-Rancher Labs (6%)

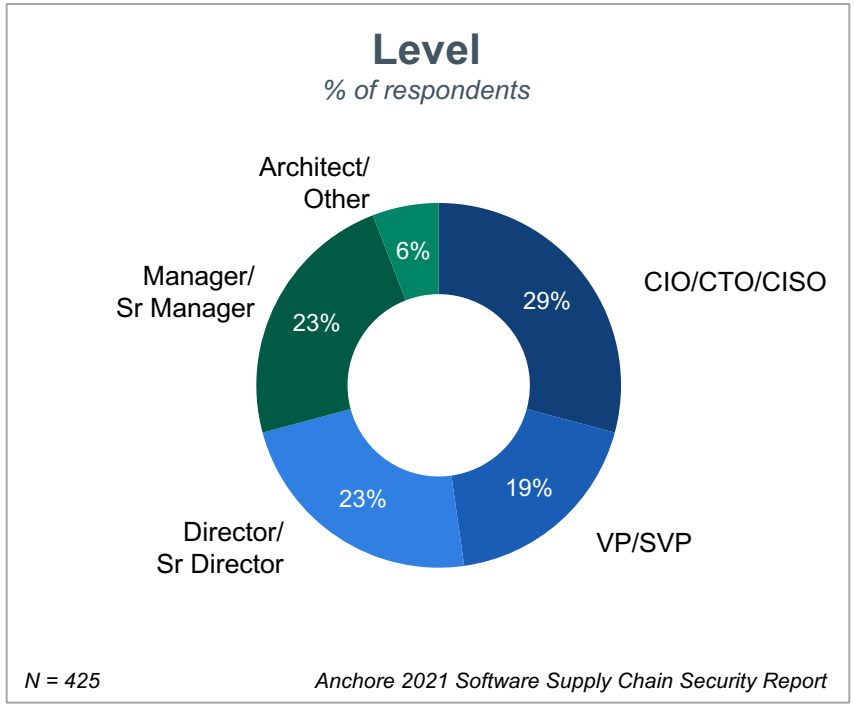
Respondent Demographics

The survey was limited to organizations with at least 1000 employees. Nearly half of the respondents were at organizations with more than 5000 employees, while the remainder were at organizations between 1000 and 5000 employees.



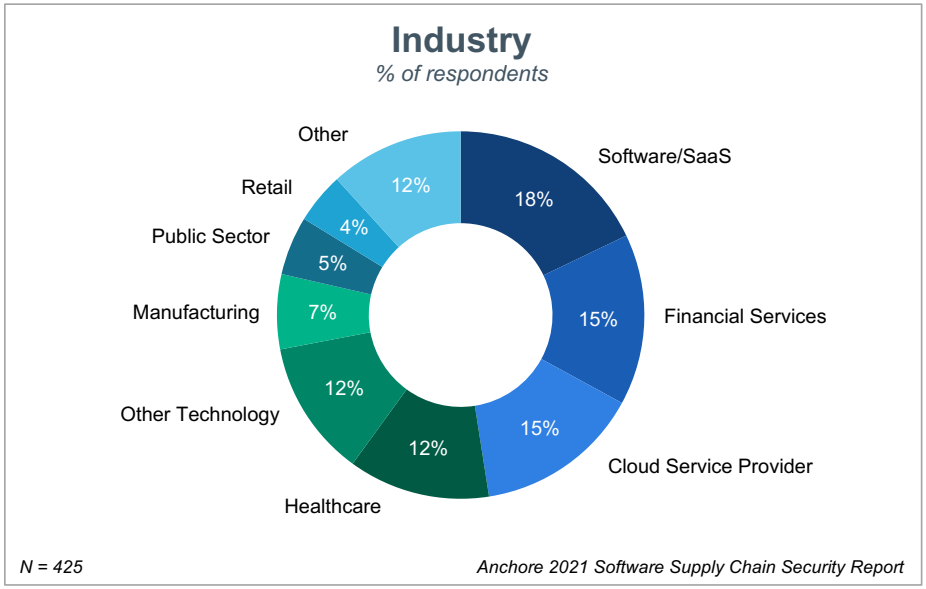
Respondents spanned a variety of technology functions, including IT, Security, Development and DevOps. In order to gain a broad perspective on enterprise practices, just under half of the respondents were C-level or VP-level, with the remainder made up of directors, managers, and architects.

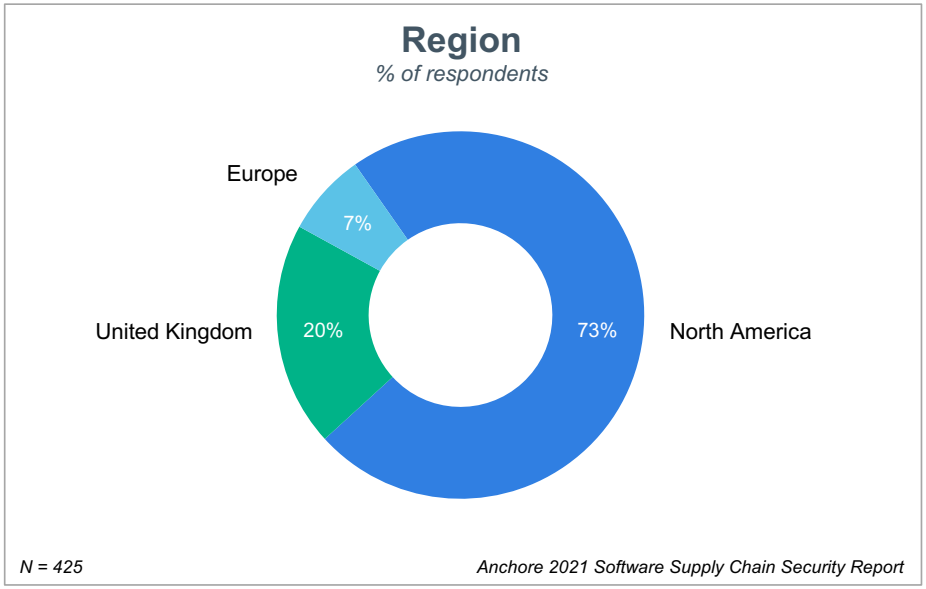




A diverse set of industries was represented. The Other category includes industries that each represented two percent or less of the respondents and included travel & hospitality, consumer goods, business services, media & publishing, energy, and more.

The survey was focused on respondents in North America, United Kingdom, and Europe.



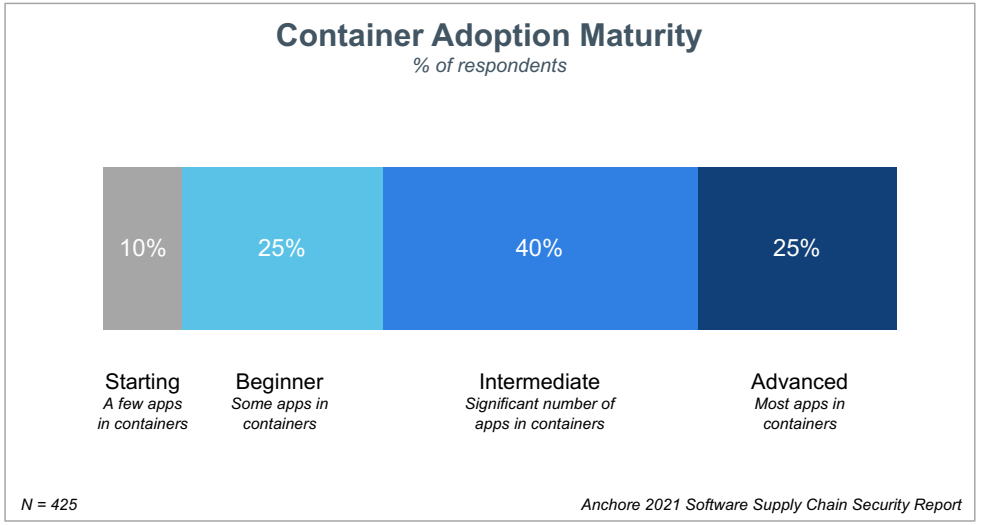


Growing Container Adoption Creates New Security Challenges

The shift to cloud-native development coupled with DevOps processes has driven an explosion in the use of containers since the emergence of Docker in 2013. While initially adopted by technology and internet startups, software containers are now well-entrenched in large enterprises across a wide range of industries.

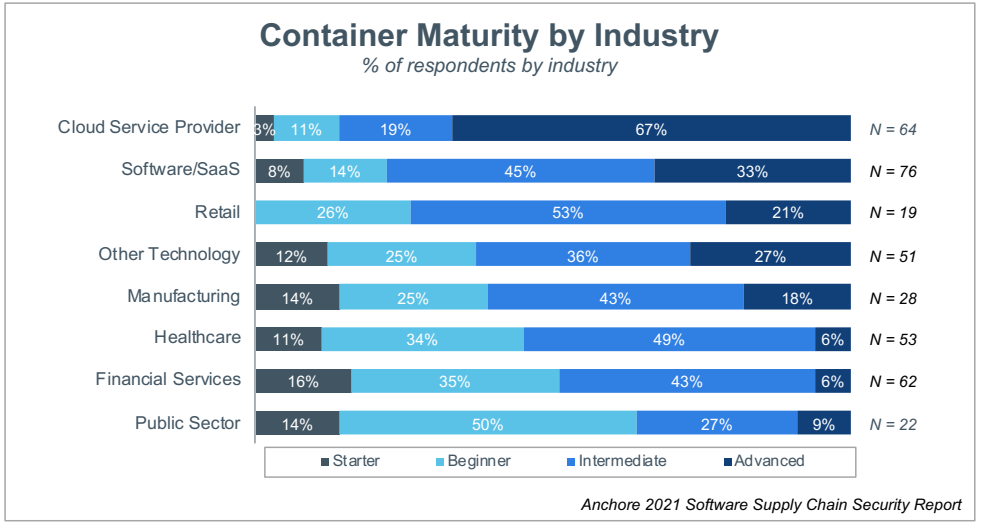
High Levels of Container Maturity

One-quarter of respondents were at Advanced maturity levels, with most of their applications running in containers. Another 40 percent are designated as Intermediate maturity with significant numbers of applications running in containers. In total, almost two-thirds of respondents are already at these later stages of container maturity.



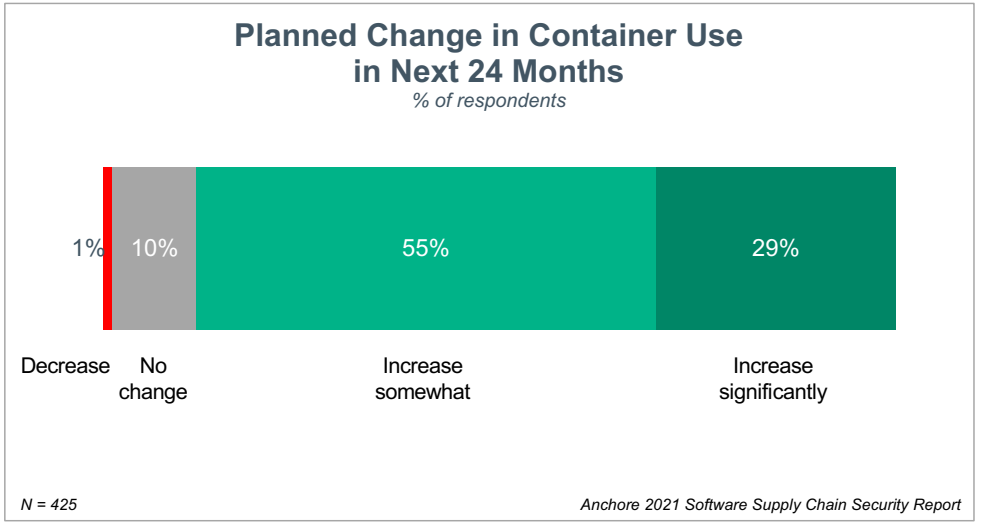
Container Maturity Not Limited to Tech-Focused Industries

Unsurprisingly, technology-focused industries such as cloud service providers and software companies had the highest levels of container maturity. However, even traditional industries such as retail, manufacturing, healthcare, and financial services had significant percentages of respondents at intermediate or advanced levels of container adoption.



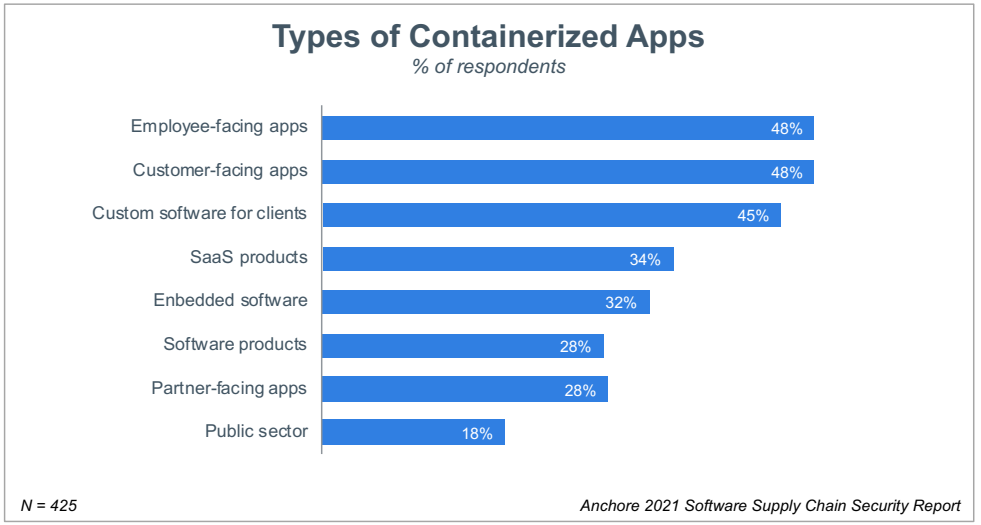
Container Adoption Will Continue Strong Growth

Enterprises also plan to continue expanding container adoption over the next 24 months with 84 percent planning to increase container use and 29 percent planning to increase use significantly.



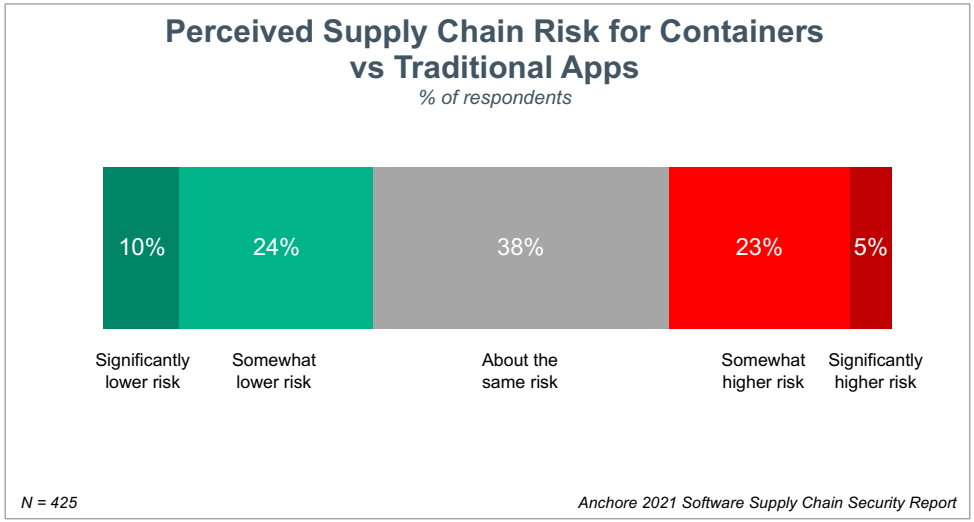
Containers Are Used for All App Types

Respondents are using containers for all types of applications. This includes applications accessed by employees and partners, as well as applications that are shipped or sold to customers.



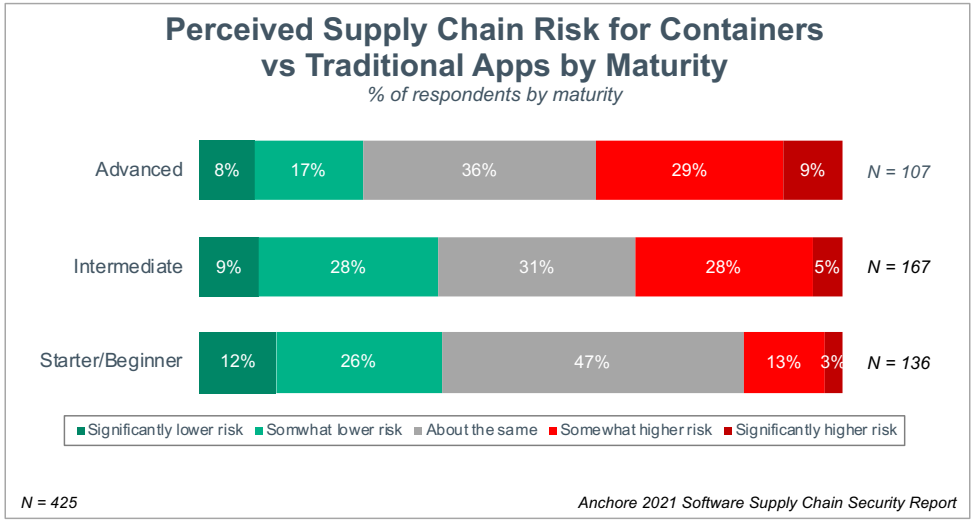
Perceived Risk of Containers is Similar to Traditional Apps

Across all respondents, containerized applications were perceived as no more risky than traditional applications. Only 28 percent of respondents see containers as having higher risk, while 34 percent see containers as being less risky.



Advanced Container Users Perceive Higher Risks

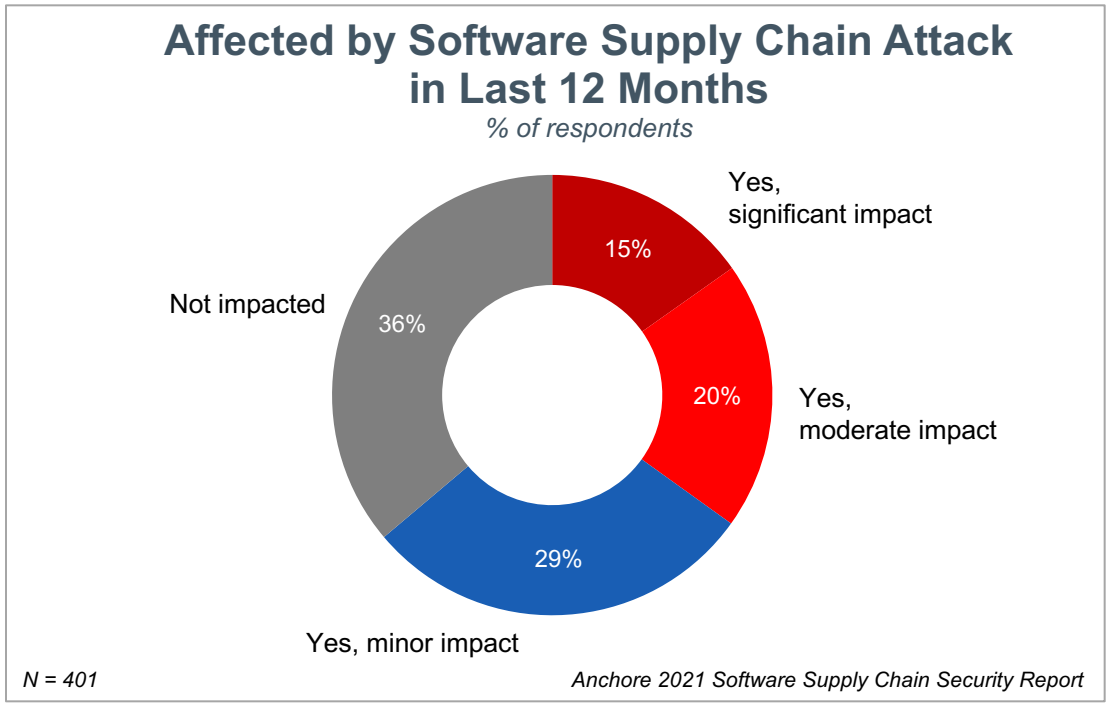
However, the perceived risk of containers varies by the container maturity of respondents. Importantly, 38 percent of advanced users see higher risks from containers vs only 16 percent of the least mature users. This likely arises from the fact that advanced users have a deeper understanding of the complex dependency chains that are common with containerized applications. They also better understand the need to adapt security processes and tools to adapt to unique container challenges.



Enterprises Are Focused on Securing the Software Supply Chain

Recent attacks such as SolarWinds, HAFNIUM, and Codecov have highlighted the risk in the software supply chain, and the Codecov attack specifically targeted a containerized application. As a result, organizations are quickly mobilizing to understand and reduce software supply chain security risk.

The May 2021 Executive Order by United States President Biden highlighted that "*the private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace.*" Similarly, the UK is also pursuing a National Cyber Security Strategy. Survey respondents indicate that they will focus on these software supply chain security issues.

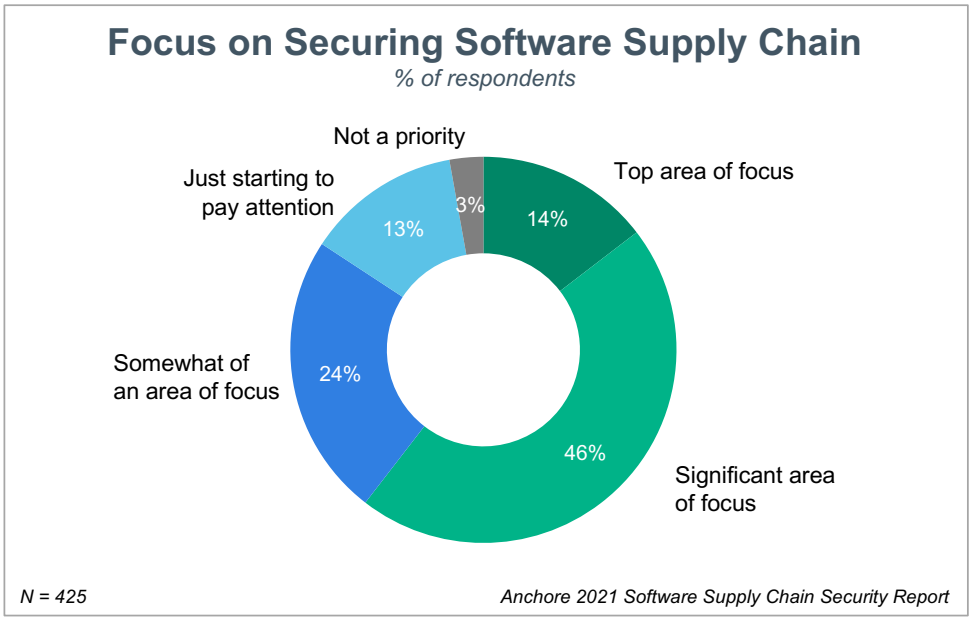


Software Supply Chain Attacks Have Broad Impact

With more than 18,000 organizations affected just by the SolarWinds attack, a significant majority (64%) of respondents have been impacted by a software supply chain attack within the last 12 months. More than a third report that the impact on their organizations was moderate or significant.

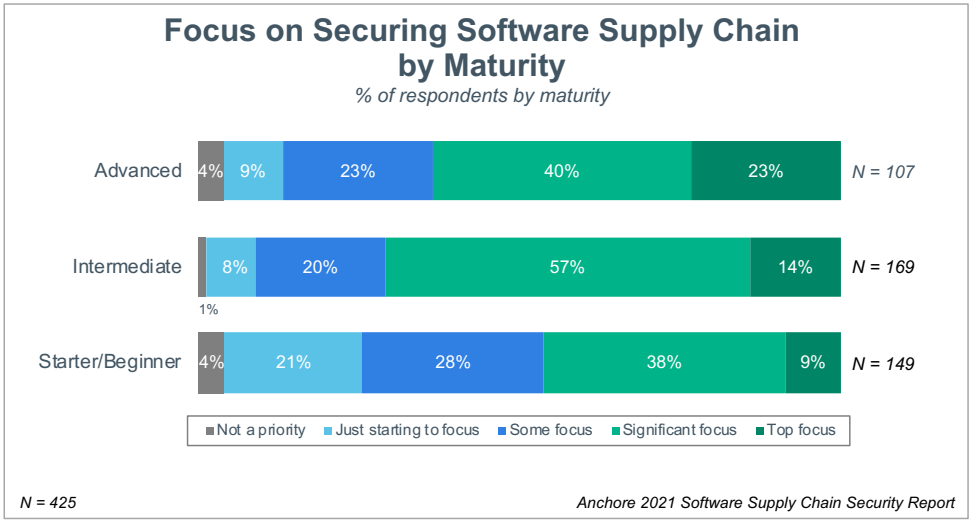
Enterprises Focus Strongly on Software Supply Chain

Against a backdrop of recent high-profile software supply chain attacks, 46 percent of respondents indicated that they have a significant focus on securing the software supply chain while an additional 14 percent have prioritized it as a top focus. Very few (3%) indicate that it is not a priority at all.



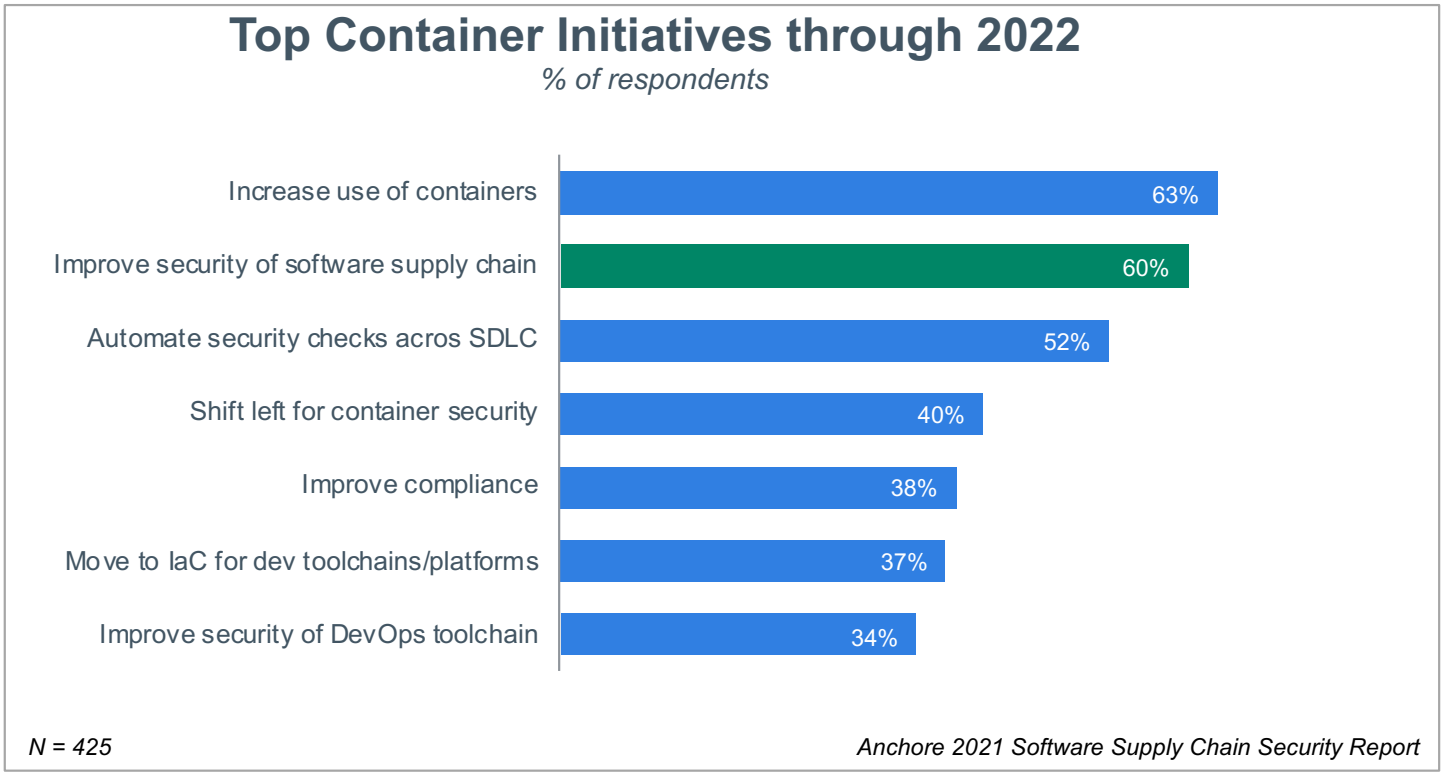
Mature Container Users Give Supply Chain More Focus

Aligned with their perception of higher risks from containers, more mature container users are giving more attention to software supply chain security. Twenty-three percent of advanced container users identify this as a top focus as compared to nine percent of less mature container users.



Software Supply Chain Security is a Top Initiative

The intersection of increased software container adoption and increased supply chain security concerns is impacting technology leaders' container initiatives. Through 2022, the top container initiative is to increase use of containers (63%) while close behind in second place is to improve the security of software supply chain (60%).

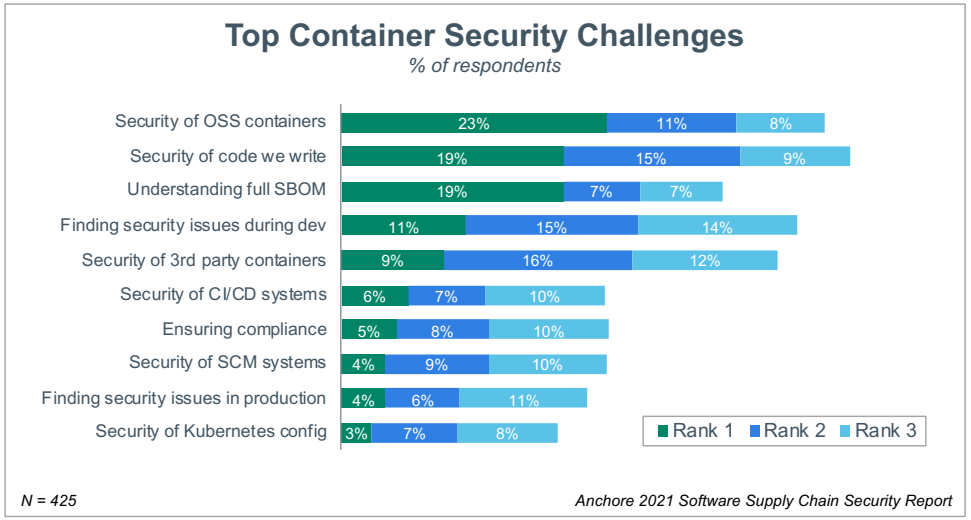


Container Security Gaps Threaten the Software Supply Chain

Despite the rapid adoption of containers and the high level of focus placed on the software supply chain challenge, there are significant gaps in the security practices for containerized applications.

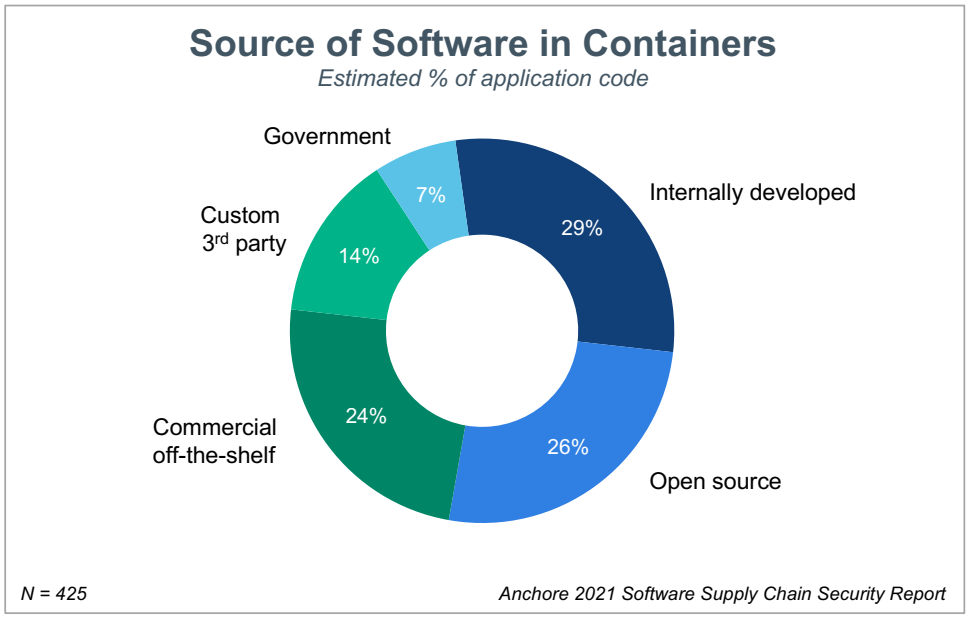
Open Source is the Top Container Security Challenge

Developers incorporate a significant amount of open source software (OSS) in the containerized applications they build. As a result, the security of OSS containers is ranked as the number one challenge by 23 percent of respondents. Tied for second place (19%) is understanding security of code that an organization writes themselves and understanding the full SBOM. SBOMs are a critical part of President Biden's Executive Order because they are the foundation for many security and compliance practices.



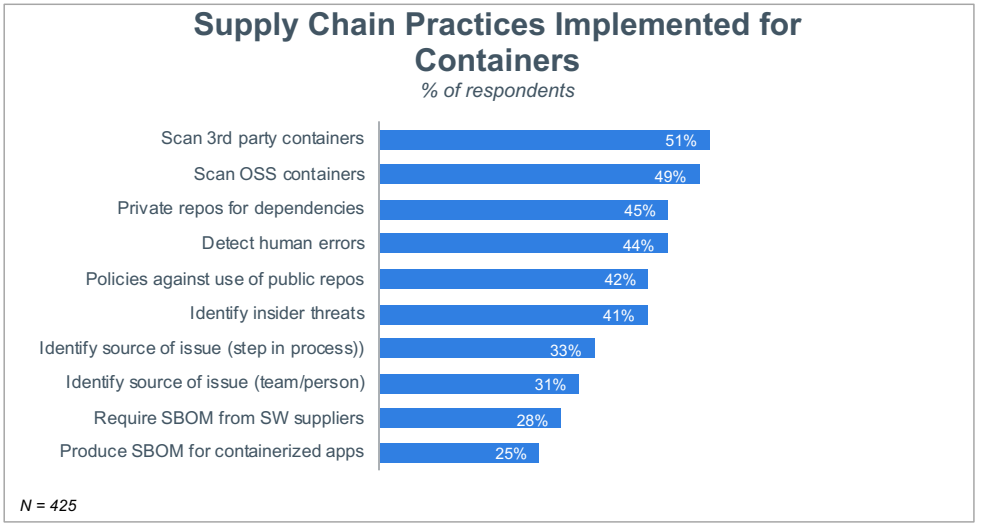
Respondents Underestimate Amount of Open Source Used

Despite the concern about open source software security, respondents estimated an average of only 26% of their application code or components were from open source. These numbers are almost certainly underestimated. In comparison, scans by Synopsys across code bases across industries identified that 70% of code was from open source (Source: Synopsys 2020 Open Source Security and Risk Analysis Report).



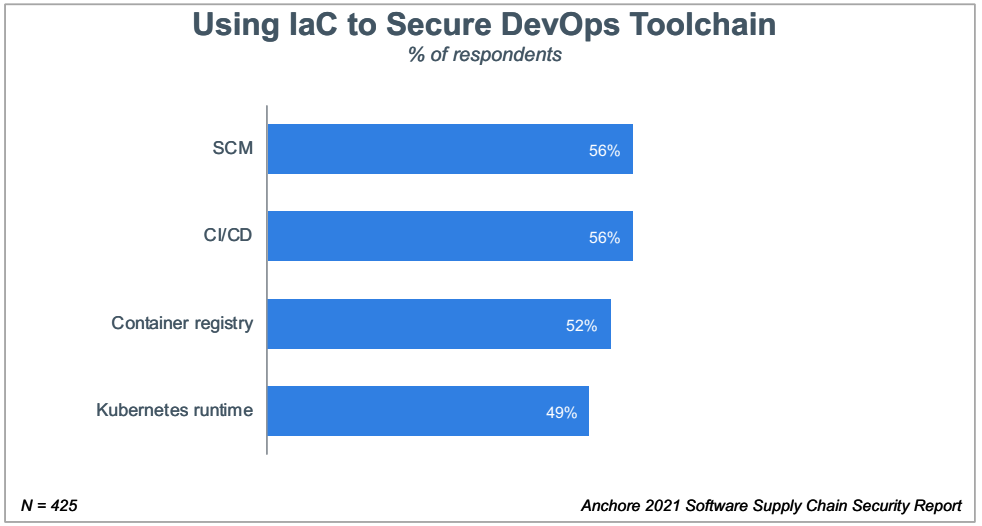
Limited Use of Supply Chain Best Practices for Containers

In addition, fewer than half of organizations have implemented most supply chain best practices. Fewer than half (49%) scan OSS containers and even fewer (45%) leverage private repos for dependencies which reduces the potential for insecure OSS containers to be pulled from public repositories. Despite the importance of an SBOM for container security practices, only 25 percent produce an SBOM for containerized apps they build and only 28 percent require an SBOM from their software suppliers.



Development Toolchain is a Blind Spot for Many

Experts have identified development platforms and toolchains as a significant risk point for software supply chain security. If these tools are compromised, attackers can gain access to many different software applications that move through the development pipeline. This opens the door for bad actors to insert malicious code or backdoors that can be exploited once the software is deployed in production or (even worse) shipped to customers. A critical best practice is to leverage infrastructure-as-code (IaC) to secure each platform or tool in the development process to ensure they are properly secured. Just over half of respondents are using IaC to secure these various platforms.

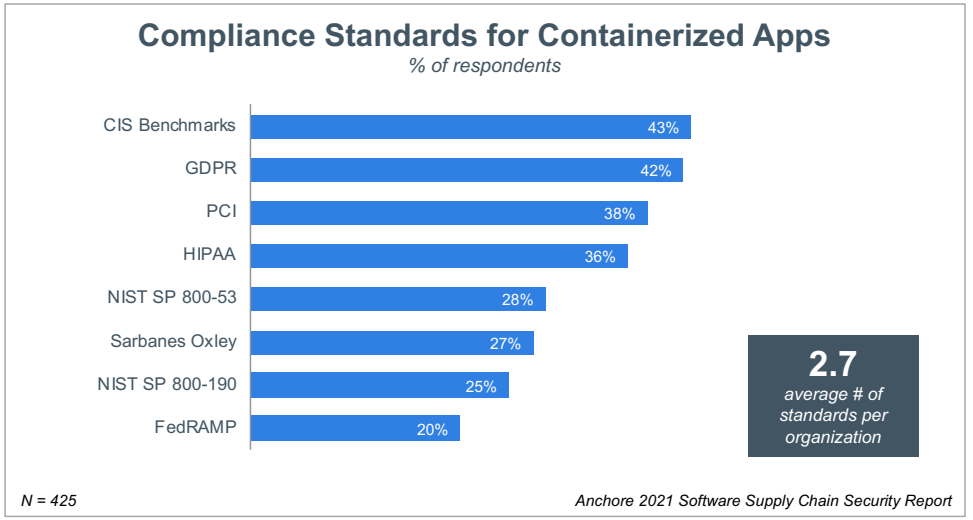


Organizations Face Container Scanning Challenges

As organizations seek to close the gaps in container security, they face a number of challenges. These challenges require them to adapt or extend their security processes and tools to shore up container security gaps.

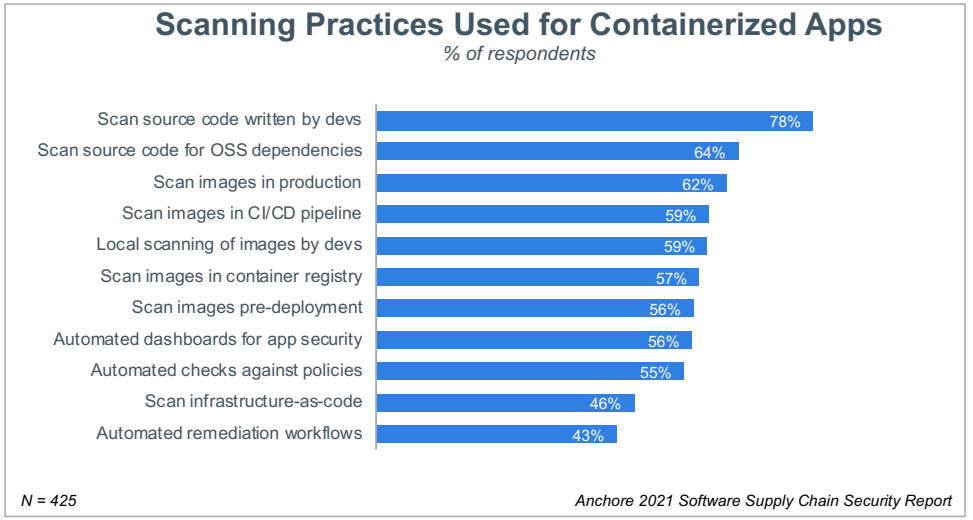
Organization Must Comply with Multiple Standards

With container adoption becoming common in even highly-regulated industries, organizations must ensure that they comply with relevant standards for their containerized applications. On average, respondents identified 2.7 standards they must meet for containers. Some standards such as CIS Benchmarks and NIST standards are foundations for other regulatory standards. By complying with these foundational standards, organizations can streamline their compliance efforts.



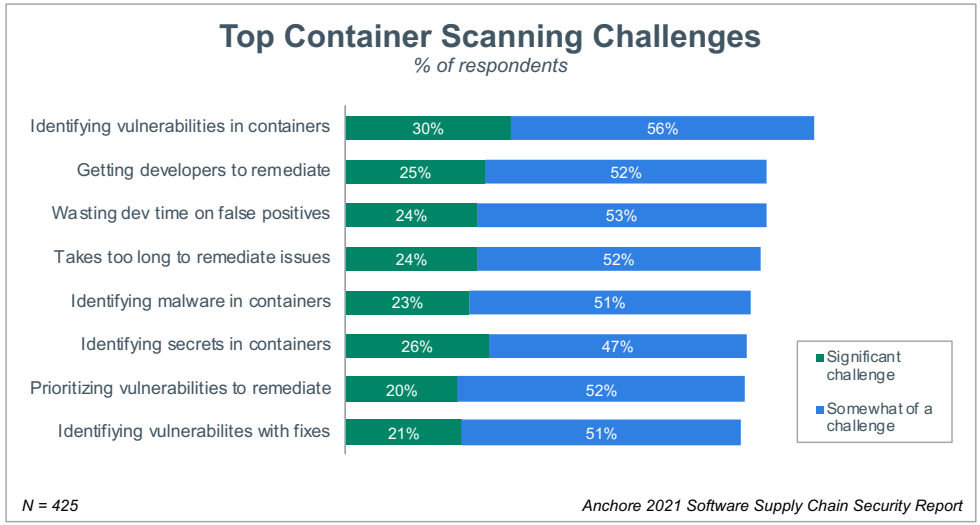
Moderate Use of Container Scanning Best Practices

The first step for securing containerized applications is to embed security scanning and checks at each phase of the development process. While most respondents *scan source code written by developers* (78%), scanning at other stages of the process is lower. Only 57 percent *scan images in the container registry* and 46 percent *scan infrastructure-as-code*. Even fewer (47%) have *automated remediation workflows* to help developers fix issues that are identified in scanning.



Organizations Face Container Scanning Challenges

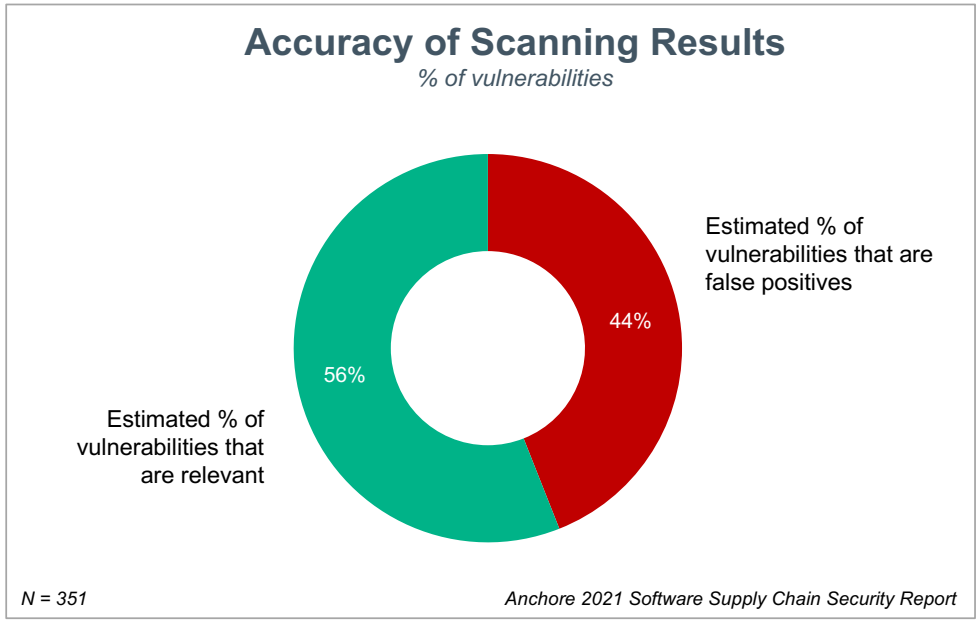
As organizations implement container scanning, a large majority face critical challenges. Top challenges include *identifying vulnerabilities in containers* (86%), *getting developers to remediate issues* (77%), *wasting developer time on false positives* (77%), and *takes too long to remediate issues* (76%). Organizations will need to adopt more accurate container scanning tools that can pinpoint vulnerabilities with fewer false positives and automated remediation capabilities to accelerate the time to remediate.



False Positives are a Significant Problem

Respondents estimated that 44 percent of vulnerabilities identified in scanning are false positives that are not relevant to the particular application being scanned. This often occurs when scanning tools don't accurately identify a package or don't leverage the most appropriate vulnerability source data.

When false positives occur, developers must spend time researching the issue and often provide justifications to the security team on why each particular vulnerability is not relevant. This wastes time for the developer and takes time away from fixing important security issues. Organizations should select scanning tools that reduce the level of false positives produced.



Container Security Requires Significant Collaboration

Respondents identified which teams in their organization are involved in particular container security activities. The table shows darker colors for the highest percentages. Security, Development, and DevOps teams are the most heavily involved in container security. Development teams are increasingly following best practices to find and fix security vulnerabilities earlier in the development process. On average, each container security activity involves two to three different functions. This identifies a need for processes and tools to share information and streamline collaboration across multiple teams.

Container Security Responsibilities

% of respondents

	Security	Development	DevOps	Product Security	Cloud Team	I&O	Platform Engineering
Security checks for OSS images	60%	43%	38%	36%	30%	24%	23%
Prioritizing security issues	58%	33%	28%	36%	22%	21%	21%
Ensuring compliance with standards	57%	30%	32%	29%	27%	30%	25%
Finding vulnerabilities during staging/production	50%	40%	40%	31%	26%	24%	28%
Finding vulnerabilities during development	49%	52%	34%	32%	21%	18%	19%
Fixing security issues in container images	42%	44%	38%	27%	24%	17%	22%
Fixing security issues in the container runtime	38%	36%	35%	24%	27%	25%	31%
Securing the DevOps toolchain	38%	27%	59%	22%	24%	20%	21%

N = 425

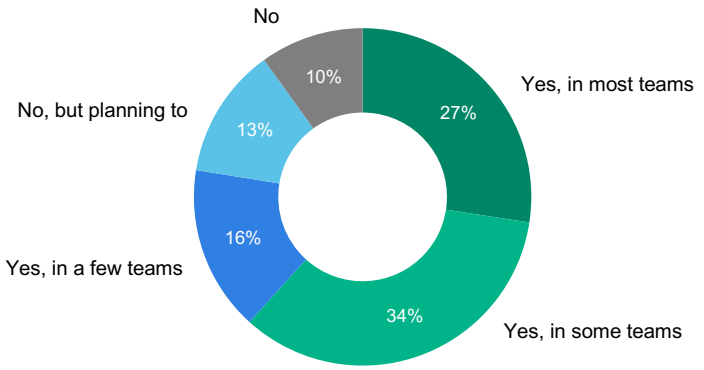
Anchore 2021 Software Supply Chain Security Report

Development Teams are Designating Security Champions

As organizations mature from DevOps to DevSecOps practices, they require development teams to take on more security responsibilities. To embed more security expertise into development teams, many organizations are designating particular developers as security champions. Their role is to mentor and advise other developers as they seek to improve security of the applications they create. Seventy-seven percent of respondents indicate they are designating security champions, with 27 percent indicating they implement the practice across most development teams.

Use of Designated Security Champions

% of respondents

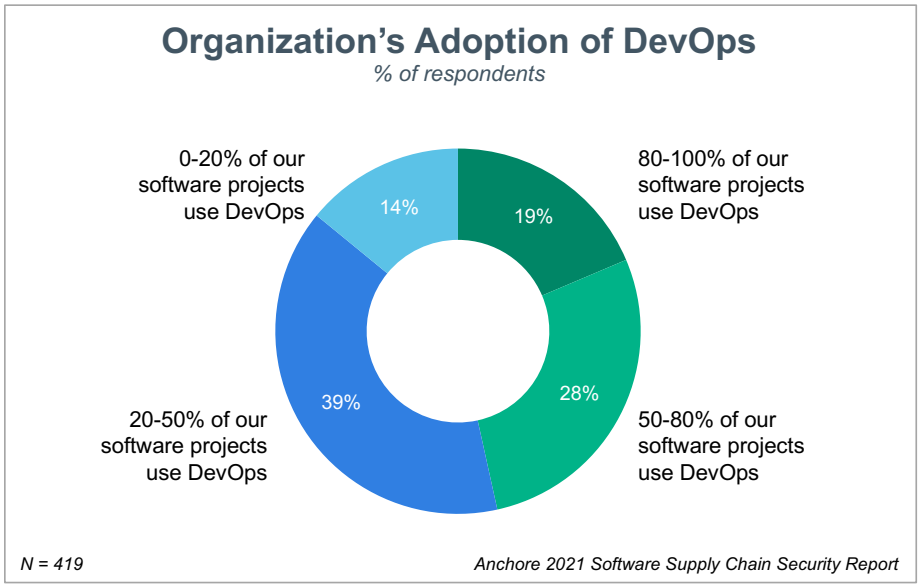


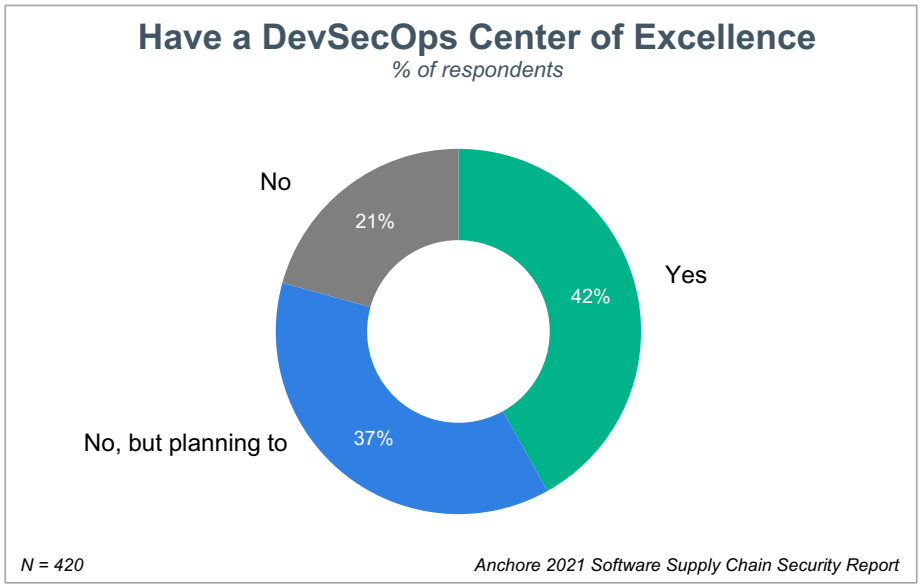
N = 423

Anchore 2021 Software Supply Chain Security Report

DevOps Toolchains Require Security Attention

As discussed earlier in this report, DevOps toolchains introduce risks that require security attention. DevOps and Security teams must work together to secure these critical platforms.



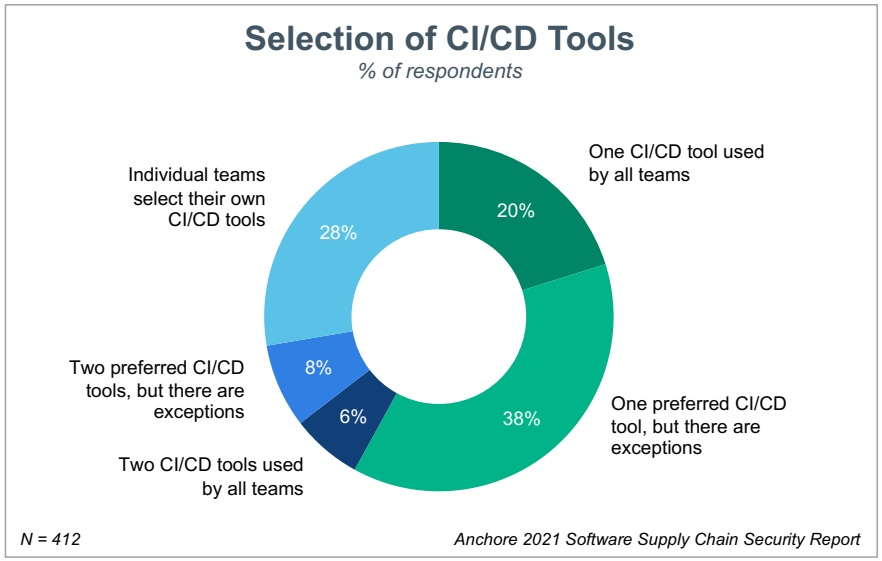


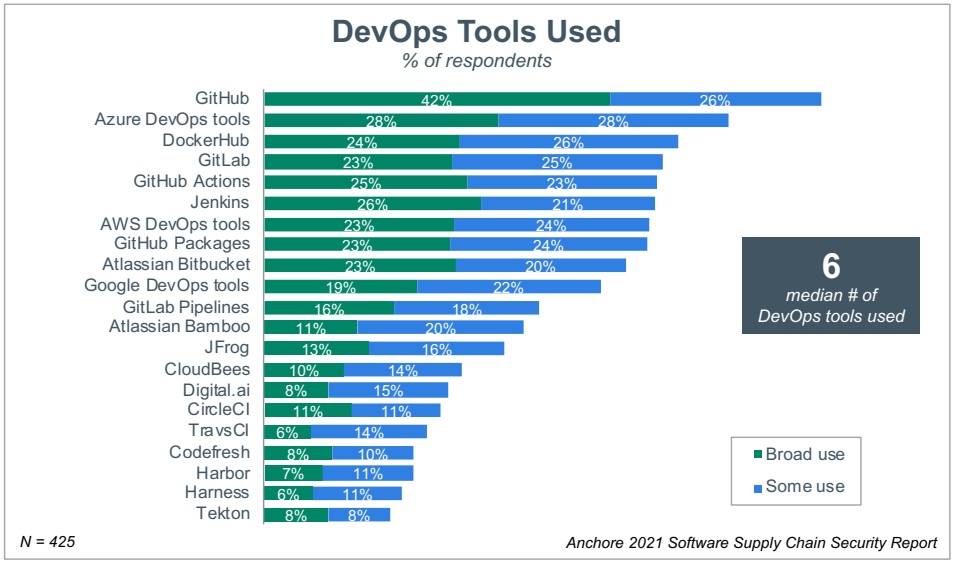
DevOps Processes are Broadly Adopted

In the last 10 years, DevOps has gained strong adoption in organizations across a variety of industries. Fourty-seven percent of respondents indicate that they leverage DevOps in more than half of their software projects, with an additional 39 percent leveraging DevOps in 20 to 50 percent of their projects.

DevSecOps is on the Rise

As DevOps has matured, more organizations are shifting to DevSecOps by embedding security into their DevOps processes. Many organizations will develop a "Center of Excellence (CoE)" as a focal point for implementing new practices or technologies. Fourty-two percent of respondents indicate they already have a DevSecOps CoE while 37 percent indicate they are planning one.





Diverse Set of DevOps Tools

As DevOps spreads to more teams within the enterprise, there are also an increasing number of DevOps platforms and tools being used. One of the most common tools is a CI/CD tool. Only 20 percent of respondents have standardized their organization on a single CI/CD tool, as compared to the 28 percent that allow individual teams to select their own CI/CD tools. Other organizations have one or two preferred tools, but those commonly have exceptions.

DevOps Tools Used

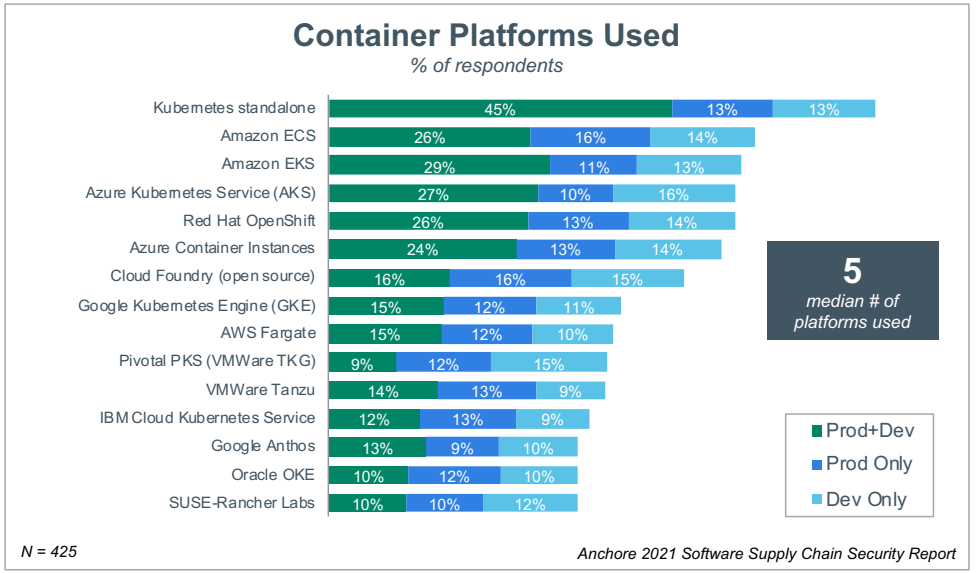
As organizations assemble the complete set of DevOps tools needed, they are using a median of six different DevOps tools in their toolchain. The most used tools for DevOps include GitHub (78%), Azure DevOps (56%), Docker Hub (50%), GitLab (48%), and Jenkins (47%). Organizations must look for ways to embed security into this diverse set of tools and platforms.

Multiple Container Platforms are Used

Container platforms based on Kubernetes are used to run containerized applications, whether during development/testing, staging, or production. These platforms can be run in-house, through a hosting provider, or obtained from a cloud provider or another vendor.

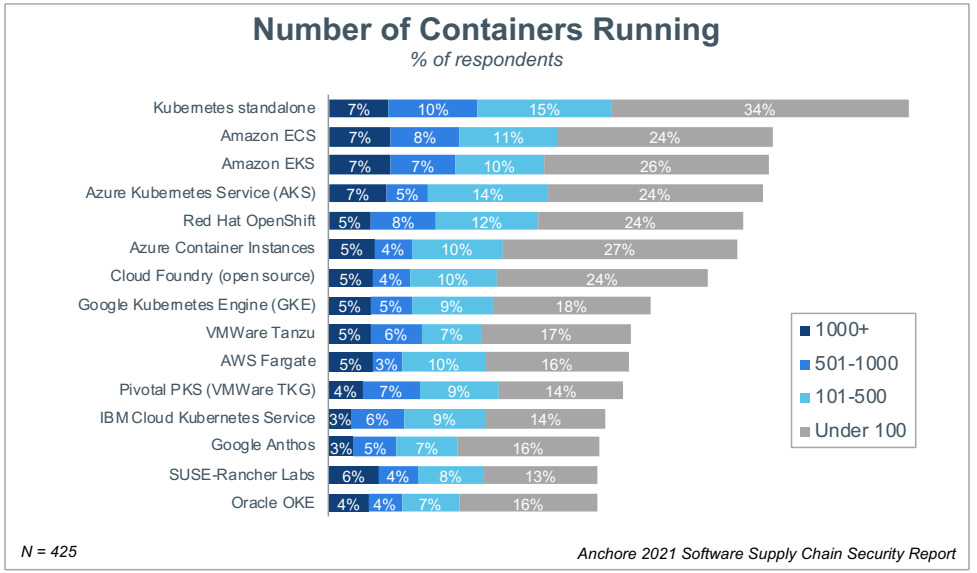
Multiple Container Platforms are Used

Respondents used a median of five container platforms. "Standalone" Kubernetes (that are not part of a PaaS service) is used most often by 71 percent of respondents. These instances may be run on-premises, through a hosting provider, or on a cloud provider's infrastructure. The second most used container platform is Amazon ECS (56%) which is a platform-as-a-service (PaaS) offering. Tied for third place (53%) are Amazon EKS, Azure Kubernetes Services, and Red Hat OpenShift.



Number of Containers Running in Container Platforms

The container platforms where respondents are running more than 1,000 containers are "Standalone" Kubernetes (7%), Amazon ECS (7%), Amazon EKS (7%), Azure Kubernetes Service (7%), and SUSE-Rancher Labs (6%).



Recommendations

The explosion in cloud-native software combined with growing attacks on the software supply chain are causing enterprise IT, Security, and DevOps leaders to sit up and take notice. The focus is rapidly shifting to protecting containerized applications built using DevOps processes.

These modern applications streamline development by leveraging easily accessible open source components delivered as software containers. However, this building-block approach introduces risks that are not always readily apparent as complicated dependency changes make it difficult to fully understand the ingredients of a containerized application.

Enterprise technology leaders must take steps to secure these cloud-native container supply chains by implementing new processes and tools that are tightly integrated into developer workflows and automated DevOps toolchains.

Here are six steps to secure the supply chain for your cloud-native and containerized applications:

1. Get a complete picture of your cloud-native software supply chain. identify where security threats can enter in your processes and tools. Learn more.
2. Start with the SBOM as a prerequisite for your container security practice. Open source tools such as Syft are a great starting point to give you visibility into the software containers you use.
3. Shift security left by embedding vulnerability scanning at each step in your DevOps process. Implement continuous scanning and security checks in CI/CD pipelines, container registry, staging environment, on deployment, and once in production. Look for scanning tools (such as open source tool Grype) with powerful APIs that are easy to embed in your toolchains.
4. Don't limit your security checks to vulnerabilities. Look for tools that have policies that can uncover secrets, malicious code, and other checks needed to meet your compliance requirements.
5. Collaboration is critical. Gain buy-in from Security, Developers, and DevOps teams on your container security processes. Consider designating security champions in your development teams to act as mentors.
6. Find out how Anchore Enterprise can help provide a continuous security and compliance solution that embeds checks across the development process and provides security teams visibility into the security stance of your containerized applications.



About Anchore

Anchore accelerates the development of secure and compliant cloud-native applications with solutions that enable software supply chain security, from vulnerability scans to generating a software bill of material. Anchore's container security solutions seamlessly embed into the DevOps toolchain with continuous security and compliance checks early in the software development process. From sourcing to CI/CD pipelines to production, Anchore's solutions protect the software supply chain and prevent container security risks from reaching production. Using Anchore as part of the DevSecOps toolchain creates a reliable way to detect issues earlier, save developers time and lower the cost to fix vulnerabilities. Built with an open source foundation, Anchore solutions provide transparency into source code and the benefit of peer reviews.

Anchore customers include large enterprises and government agencies that require secure and compliant cloud-native applications. To learn more about Anchore's solutions, visit **www.Anchore.com**.

anchore

info@anchore.com
anchore.com