anchore

Anchore 2022 Software Supply Chain Security Report

Enterprise Practices for Managing the Software Supply Chain

62% of respondents have been impacted by a software supply chain attack in the last year

Table of Contents

Introduction 3

Executive Summary 4

Methodology 5

Attribution Requirements for Sharing Charts 5

Highlights 6
- The Shift to Containers Continues Unabated 6
- Supply Chain Attacks Impacted 62% of Organizations Overall 6
- Organizations Focus on Securing the Software Supply Chain 6
- SBOM Practices Must Mature to Improve Supply Chain Security 6
- Securing Containers Focuses on Supply Chain and Open Source 7
- Organizations Face Challenges in Scanning Containers 7
- Organizations Must Secure Across Diverse Environments 7

Respondent Demographics 8

The Shift to Containers Continues Unabated 11
- Respondents Show Container Maturity 11
- Tech and Retail Industries Are Most Mature 12
- Container Adoption Will Continue to Grow 13
- Container Use Across Application Type 14

Software Supply Chain Attacks Continue to Grow 15
- Supply Chain Attacks Impact 62% of Organizations 15
- Respondents Report More Attacks After Log4j is Published 16
- Supply Chain Attacks With the Biggest Impact 17
- Tech Industry Impacted Most by Attacks 18

Enterprises Focus on Securing the Software Supply Chain 19
- Supply Chain Focus Increases With Use of Containers 20
- Top Areas of Software Supply Chain Focus 21
- Organizations Comply with an Average of Three Standards 22

SBOM Practices Must Mature to Improve Software Supply Chain Security 23
- Few Follow SBOM Best Practices 23
- Mature Container Users Leverage SBOMs More 24
- SBOM Adoption Will Continue to Grow 25
- Mature Organizations Emphasize SBOM Use 26

Securing Containers Focuses on Supply Chain and Open Source 27
- More Mature Container Users See Higher Risks 28
- Open Source is the Top Container Security Challenge 29
- Supply Chain Security Is the Top Container Initiative 30
- Organizations Face Container Scanning Challenges 31
- False Positives are a Significant Problem 32
- Container Security Requires Significant Collaboration 33

Organizations Must Secure Diverse DevOps Toolchains 34
- Organizations Use Many DevOps Tools 34
- DevOps Tools Used 35

Organizations Must Secure Multiple Container Platforms 36
- Container Platforms are Used by Development and Production 36
- Number of Containers Running in Container Platforms 37

Recommendations 38

About Anchore 40

Introduction

This report compiles the responses of 428 leaders and executives in IT, Security, and Development to identify the latest trends on how larger organizations are adapting to the new security challenges of the software supply chain. As enterprises increasingly move to cloud-native software and DevOps methodologies, this report includes a special focus on the platforms, tools, and processes used to secure the growing volume of software containers.

Executive Summary

Last year started with the fallout of the SolarWinds SUNBURST attack and ended with multiple exploits against the Log4j zero-day vulnerability, highlighting the critical importance of securing the software supply chain. While this survey was largely conducted prior to the publishing of the Log4j vulnerability, almost two-thirds of respondents reported impacts from attacks in the prior 12 months. As a result, organizations are prioritizing software supply chain security with over half of respondents citing it as a significant or top area of focus. The level of focus is correlated with the maturity of container use, with 70 percent of advanced container users citing supply chain as a significant or top focus as compared to only 45 percent of beginners.

Organizations are looking to secure all elements of their software supply chain. While open source software risk is the top priority, it is closely followed by concerns about 3rd party libraries and commercial software as well as internally-developed software.

Compliance with emerging industry and governmental standards is also a significant driver for many organizations. This year almost a third of organizations are planning to comply with the May 2021 U.S. Executive Order on Cybersecurity and the CISA Directive on Known Exploited Vulnerabilities.

The software bill-of-materials (SBOM), which is included in the U.S. Executive Order, is rapidly gaining attention as a critical component of software supply chain security. An SBOM provides visibility into software ingredients and is a foundation for understanding software vulnerabilities and risks. While only a minority of respondents currently follow SBOM best practices, a large majority plan to increase SBOM use in 2022. This is especially true among advanced container users with 81 percent in this group planning to increase their use of SBOMs.

Methodology

This is the first report to provide an enterprise-focused view of practices for securing the software supply chain as provided by 428 IT executives and leaders. They come from a vetted independent panel that validates their organizations and roles, and their responses provide a unique perspective of managers into current enterprise security practices and challenges.

Unlike many surveys that focus solely on open source, developers, or smaller organizations, this report is based on a survey of 428 executives, directors, and managers in IT, Security, Development, and DevOps functions. The respondents are exclusively from larger enterprises in North America and Europe that span a wide variety of industries. They range in size from a minimum of 1,000 employees to the largest organizations.

The survey was conducted between December 3 and December 22, 2021, with 71 percent of the responses on or after the Log4j zero-day vulnerability was published to the NIST National Vulnerability Database on December 10, 2021.

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 2022 Software Supply Chain Security Report**.

Highlights

The Anchore 2022 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.

The shift to containers continues unabated

- 63% are at intermediate or advanced levels of container maturity
- Internet and retail organizations are the most mature container users with 90% and 84% at intermediate or advanced levels of maturity
- 88% plan to increase container use and 31% plan to increase it significantly
- More than half of organizations are running employee and customer-facing applications in containers

Supply chain attacks impacted 62% of organizations overall

- 65% of those responding after the Log4j zero-day reported being impacted by *any* supply chain attack vs. 55% of those responding *before* Log4j
- Excluding Log4j, the most widespread supply chain attack was SUNBURST (SolarWinds) affecting 32% of respondents
- MIMECAST and HAFNIUM which targeted Microsoft Exchange Server impacted 20% and 15% respectively
- 50% of Software/SaaS/Internet companies experienced significant or moderate impacts from a software supply chain attack in the prior 12 months

Organizations focus on securing the software supply chain

- 70% of advanced container users and 54% overall have prioritized software supply chain security as a top or significant area of focus
- Security of open source is the top supply chain focus with 46% ranking it in their top 3 priorities, followed by 3rd party libraries (45%) and commercial software (38%)
- Compliance with industry standards is also a driver with organizations complying with an average of 3 standards
- 30% are impacted by new federal standards in the U.S Executive Order on Cybersecurity

SBOM practices must mature to improve supply chain security

- Less than a third follow SBOM best practices such as maintaining an SBOM repository and requesting SBOMs from commercial vendors
- Only 18% have complete SBOMs for all of their applications, making it difficult to respond quickly to zero-day vulnerabilities
- Less mature container users are even less likely to leverage SBOMs, increasing the risk from supply chain attacks and zero-day vulnerabilities
- Recognizing the importance of an SBOM, 76% expect to increase their use of SBOMs in the next 12 months

Highlights

Securing containers focuses on supply chain and open source

- While respondents overall see containers as having a similar risk to traditional applications, advanced users see a higher risk for containers
- Top container challenges are open source (45%), internally developed code (44%), and other 3rd party code (41%)
- As a result, 61% rank supply chain security as their top container security initiative for 2022
- Organizations share responsibility for container security across security, DevOps, and development teams

Organizations face challenges in scanning containers

- Top overall challenges include finding vulnerabilities, remediation time, and identifying secrets
- 26% report identifying malware as a significant challenge
- Container users also report accuracy as a critical scanning issue, estimating that 38% of vulnerabilities identified are false positives

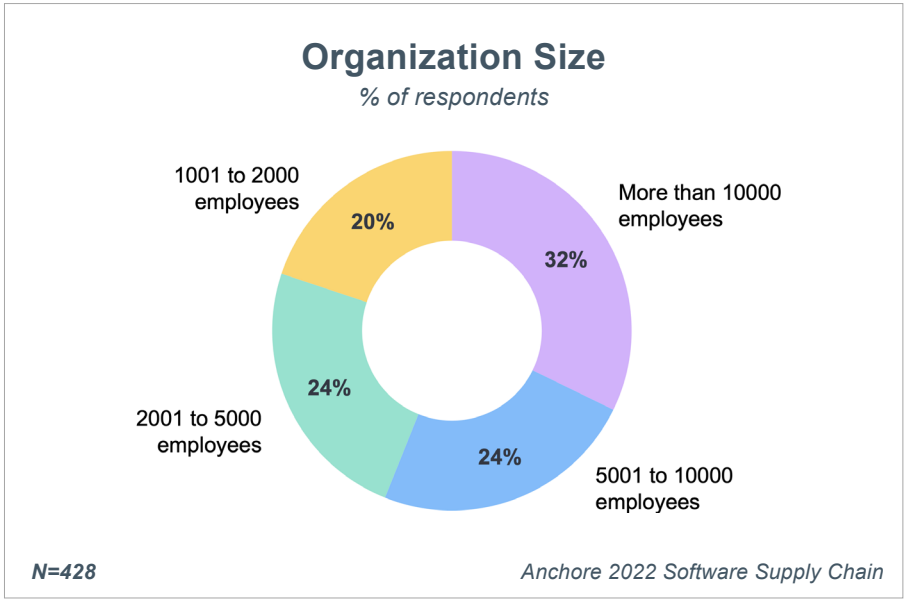
Organizations must secure across diverse environments

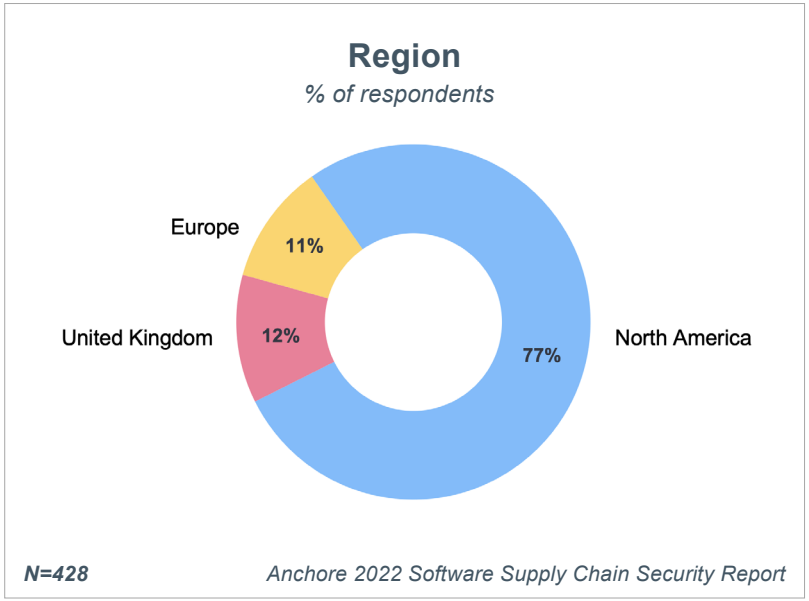
- 72% of organizations have more than one CI/CD system and respondents identify a median of 6 different tools in their DevOps toolchain
- The most used tools for DevOps include GitHub (69%), Azure DevOps tools (52%), and GitLab (46%)
- Organizations also use a median of 5 different container platforms
- The most widely used container platforms are "standalone" Kubernetes (75%), Azure Kubernetes Service (53%), and Red Hat OpenShift (50%)

Respondent Demographics

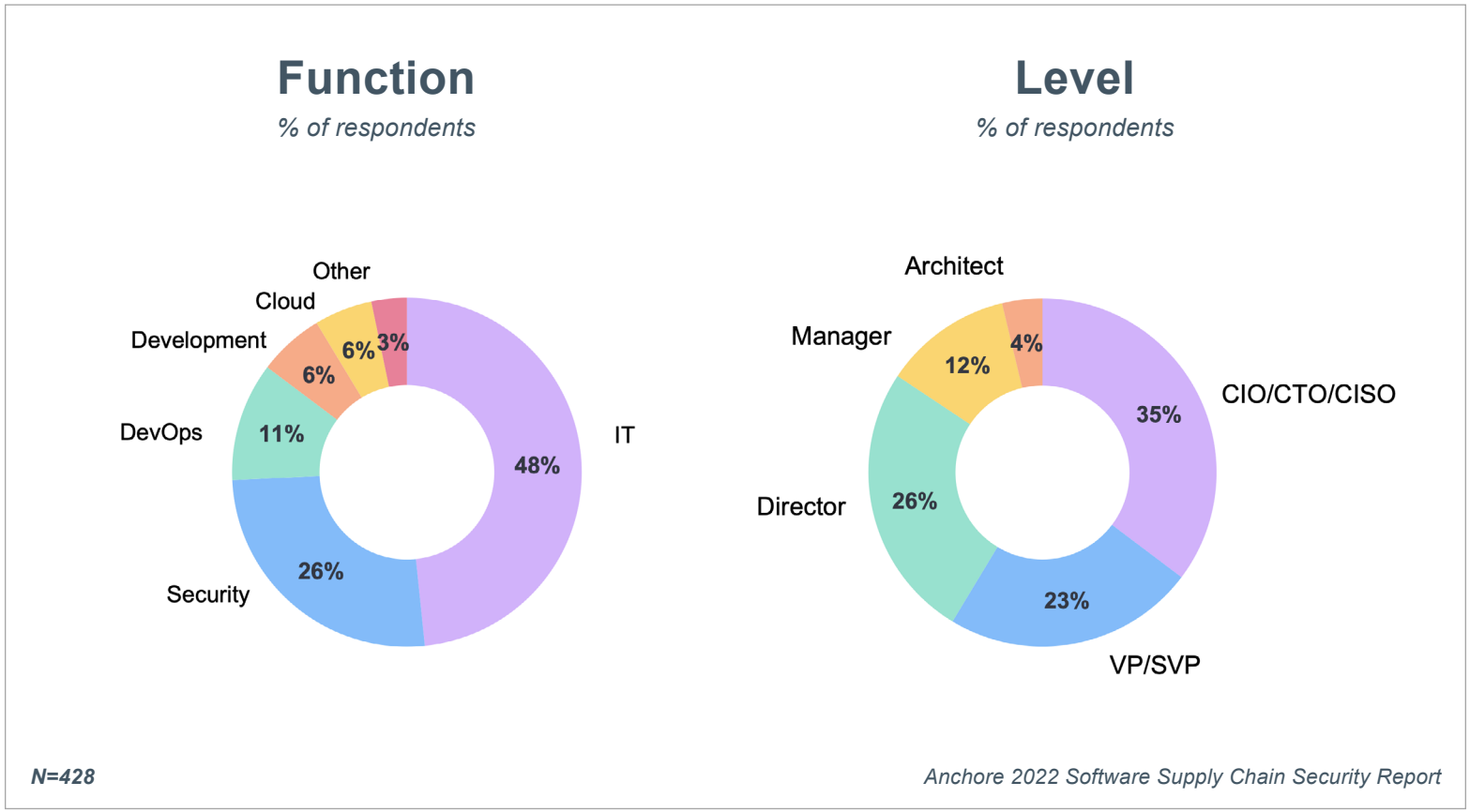
The survey was limited to organizations with at least one thousand employees. Over half of the respondents were at organizations with more than five thousand employees.

The survey was focused on respondents in North America, the United Kingdom, and other European countries.

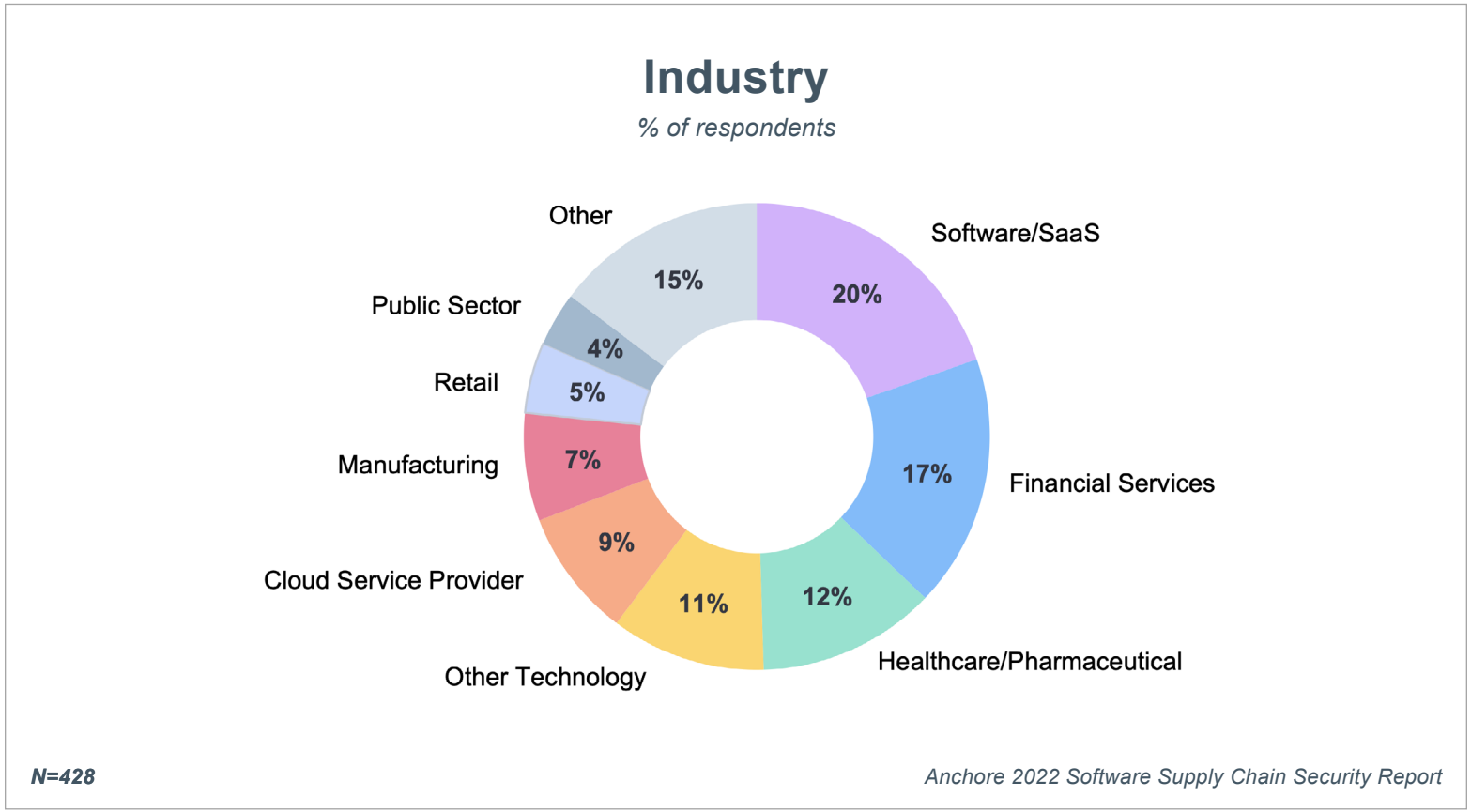




Respondents spanned a variety of technology functions with 74 percent coming from IT and Security. The survey reveals the perspective of technical leaders, with 58 percent of the respondents at the C-level or VP-level and the remainder made up of directors, managers, and architects.



A diverse set of industries was represented, led by Software/SaaS. The Other category includes industries that each represented 4 percent or less of the respondents and included Transportation, Wholesale, Media/Publishing, Consumer Goods, and more.

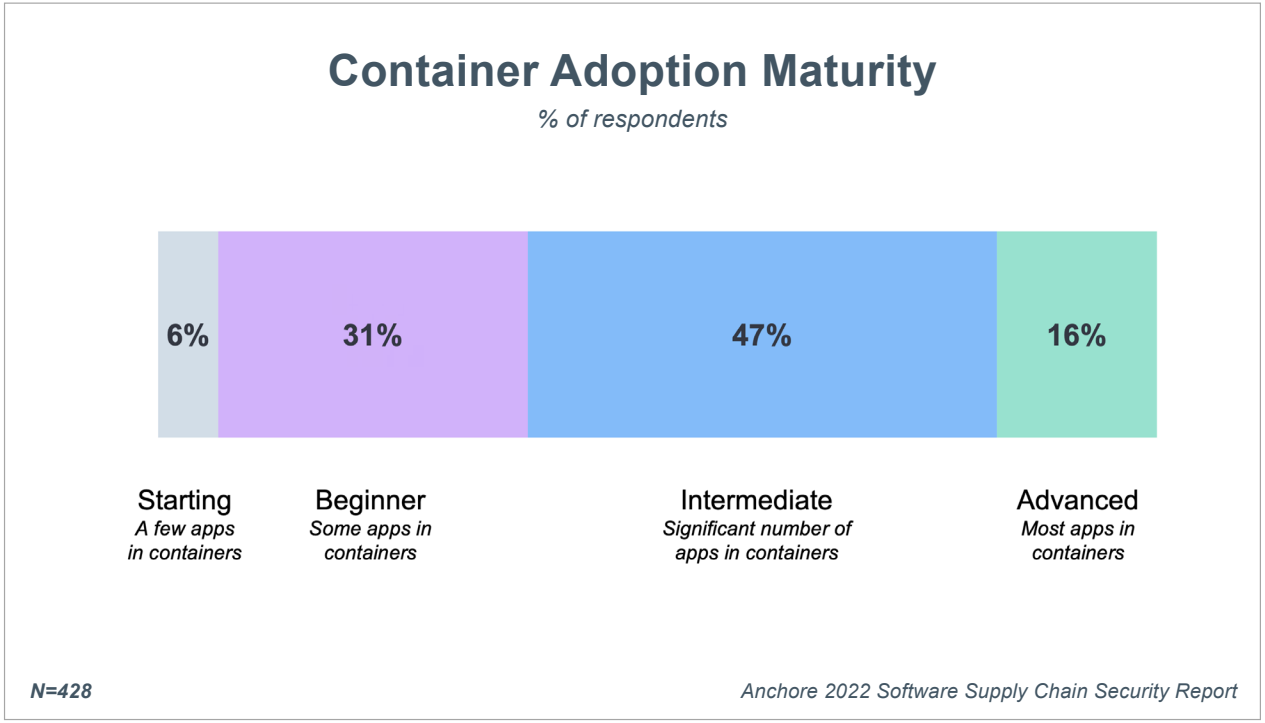


The Shift to Containers Continues Unabated

The shift to cloud-native development coupled with DevOps continues to drive the use of containers. While initially adopted by technology and internet startups, the use of software containers continues to flourish in large enterprises across a wide range of industries.

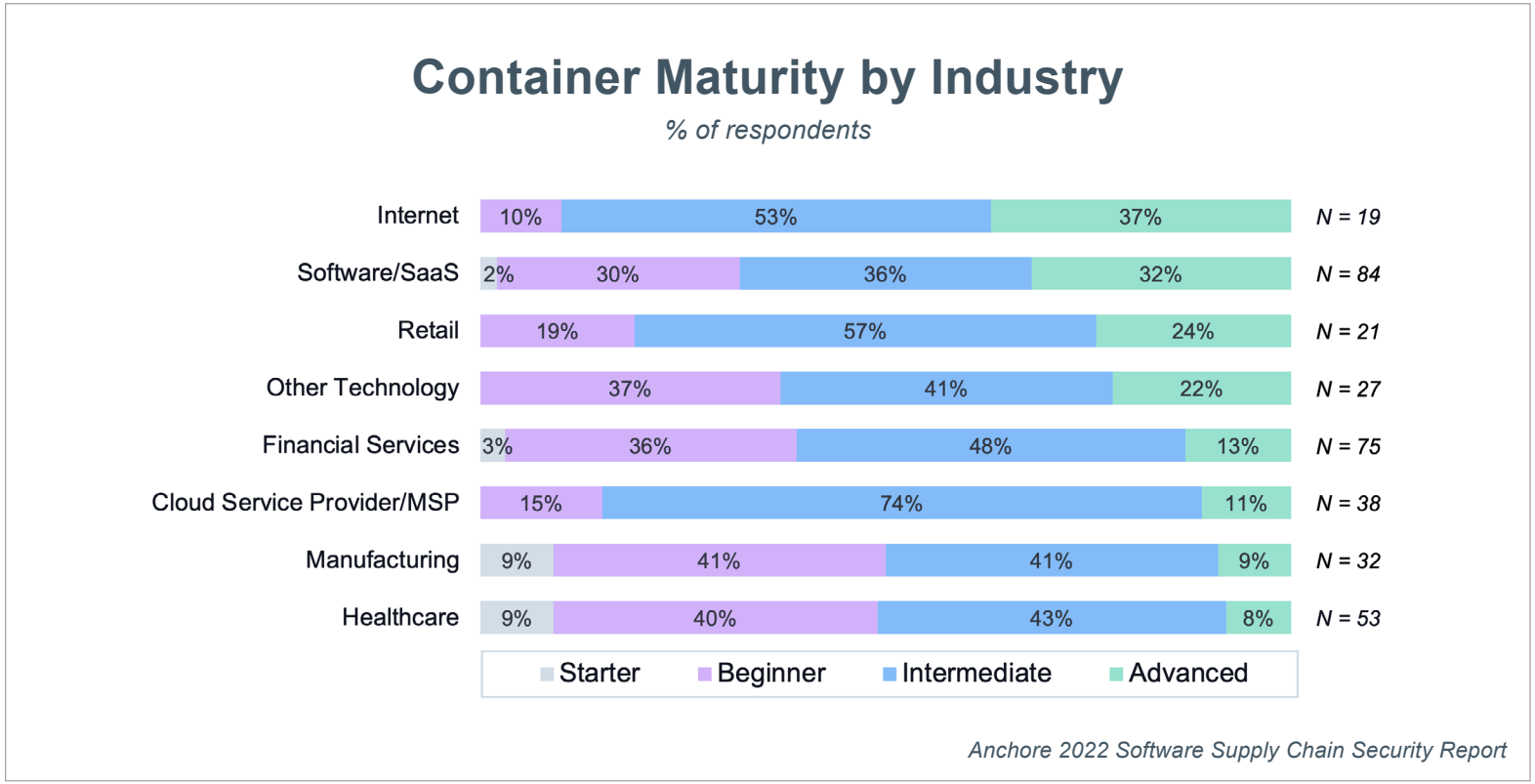
Respondents Show Container Maturity

Nearly two-thirds of respondents were at the advanced or intermediate maturity level, with a significant number of their applications running containers. Another 31 percent were at a beginner level, with just some applications running in containers.



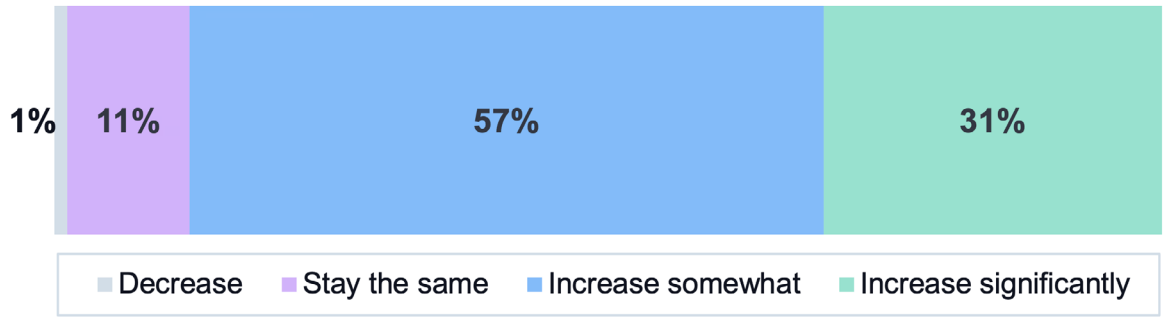
Tech and Retail Industries Are Most Mature

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



Container Adoption Will Continue to Grow

Enterprises plan to continue expanding container adoption over the next 24 months with 88 percent planning to increase container use and 31 percent planning to increase use significantly.

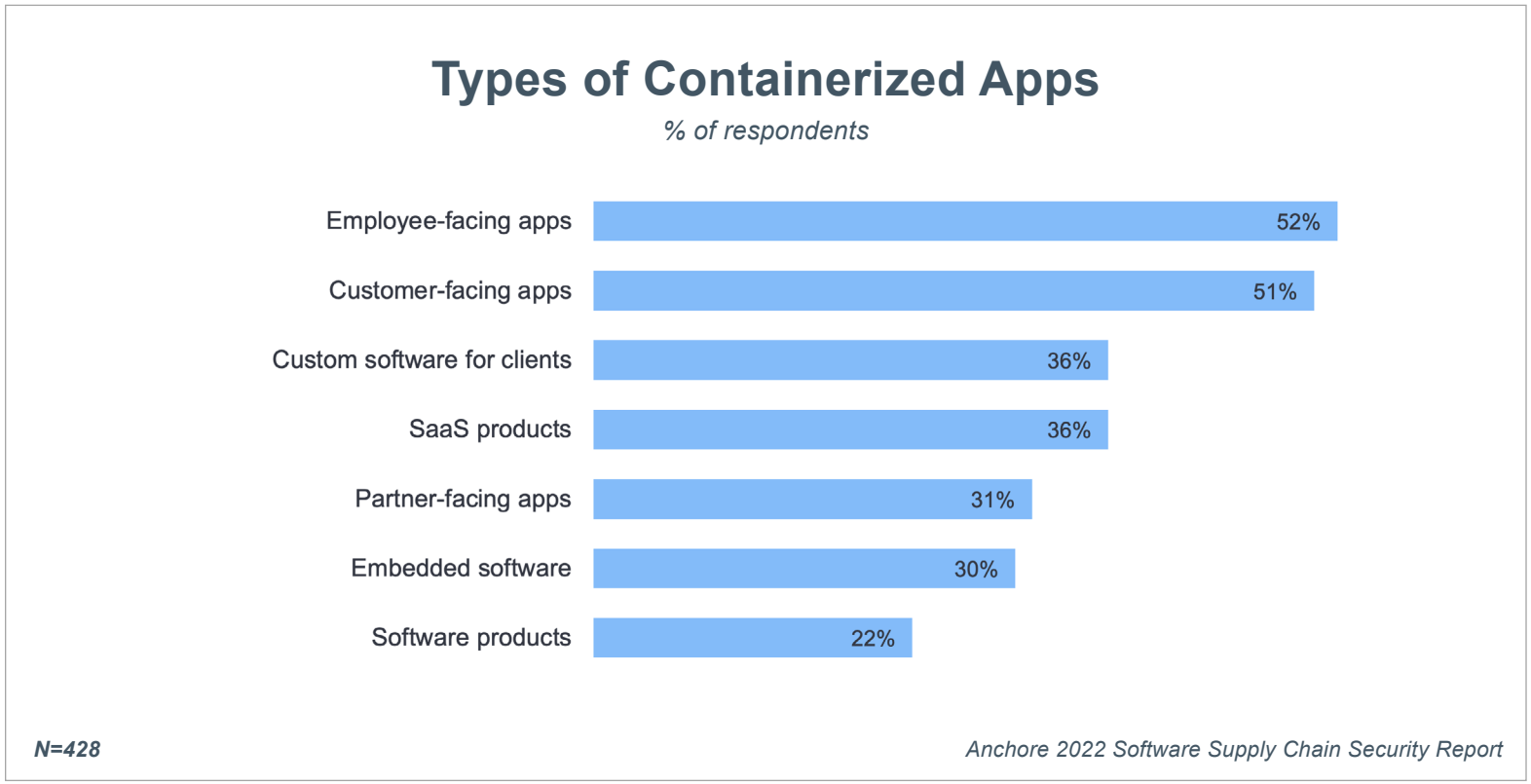


N=428

Anchore 2022 Software Supply Chain Security Report

Container Use Across Application Type

Respondents were using containers for all types of applications, with the majority used in employee and customer-facing apps.

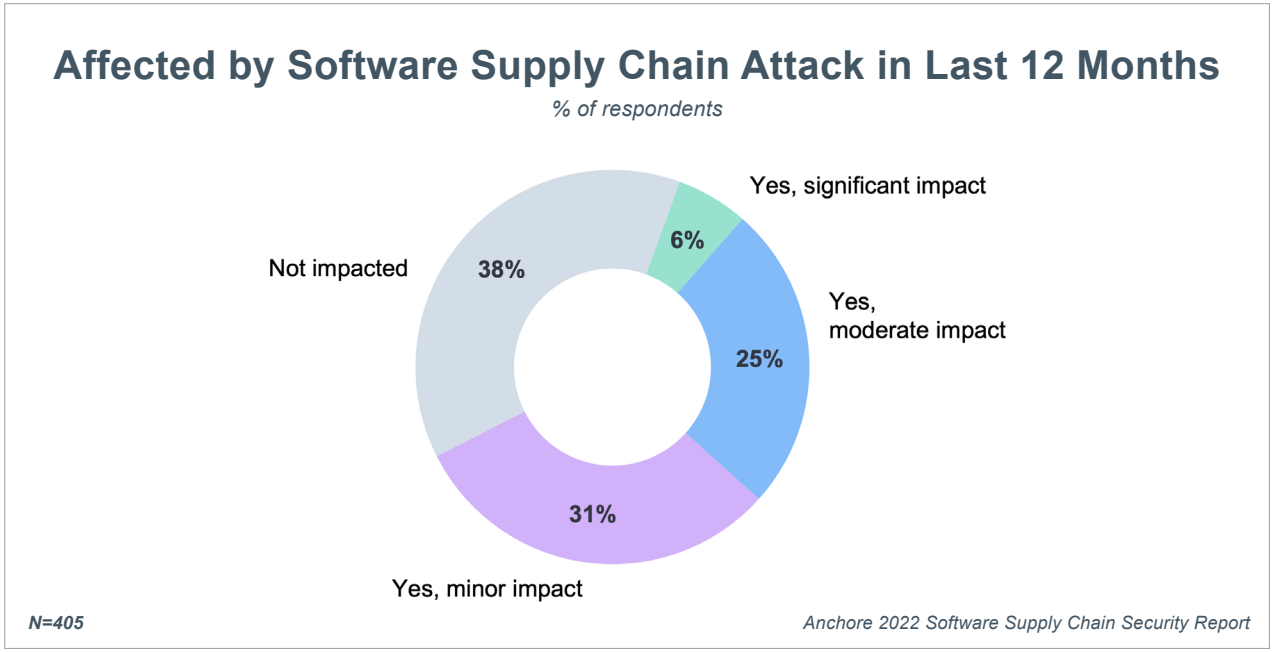


Software Supply Chain Attacks Continue to Grow

Widespread attacks such as SolarWinds, MIMECAST, HAFNIUM, as well as exploits of the recent Log4Shell vulnerability have brought the realities of the risk associated with software supply chains to the forefront. As a result, organizations are quickly mobilizing to understand and reduce software supply chain security risk.

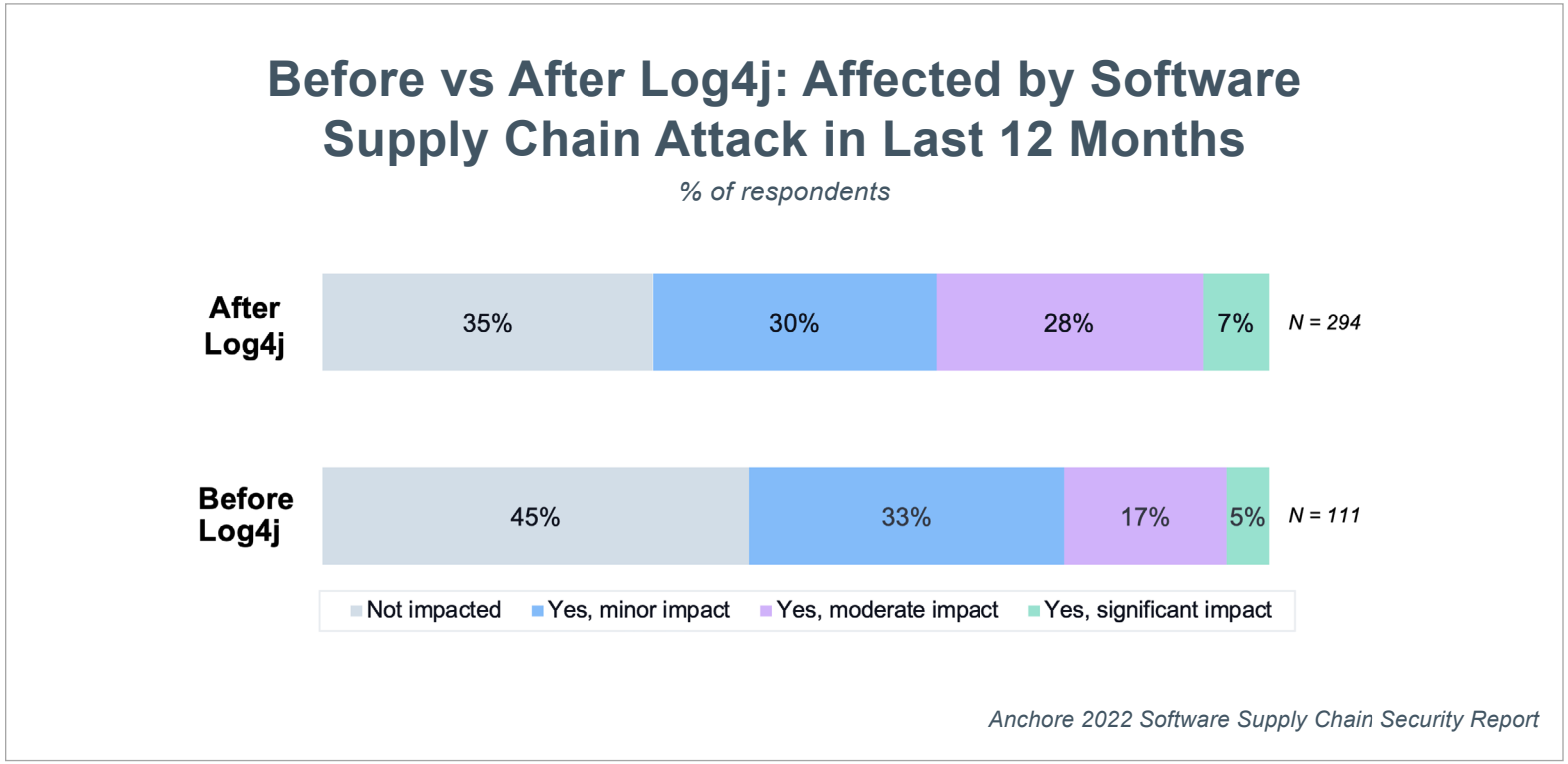
Supply Chain Attacks Impact 62% of Organizations

A combined 62 percent of respondents were impacted by at least one software supply chain attack during 2021, with 6 percent reporting the attacks as having a significant impact and 25 percent indicating a moderate impact.



Respondents Report More Attacks After Log4j is Published

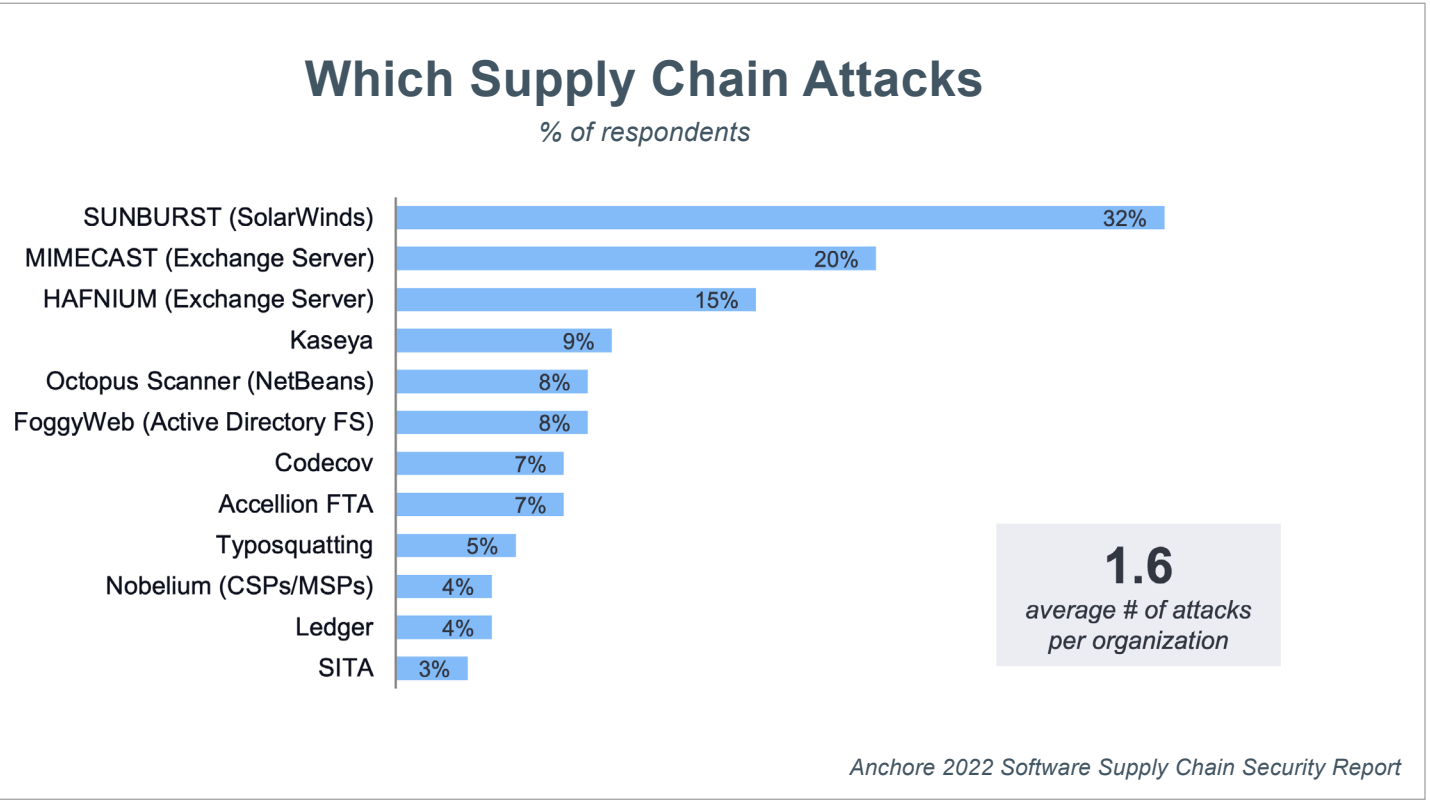
Because the survey was conducted over three weeks from December 3 to December 22, 2021, we were able to compare survey responses from before and after the Log4j vulnerability was published on December 10, 2021. The results showed that those who completed the survey after December 10 were more likely to report significant or moderate impacts from supply chain attacks (35 percent after Log4j vs. 22 percent before Log4j). This indicates that Log4j significantly widened the number of companies that experienced major supply chain attacks in 2021.



Before Log4j includes those that responded 12/10/2021.

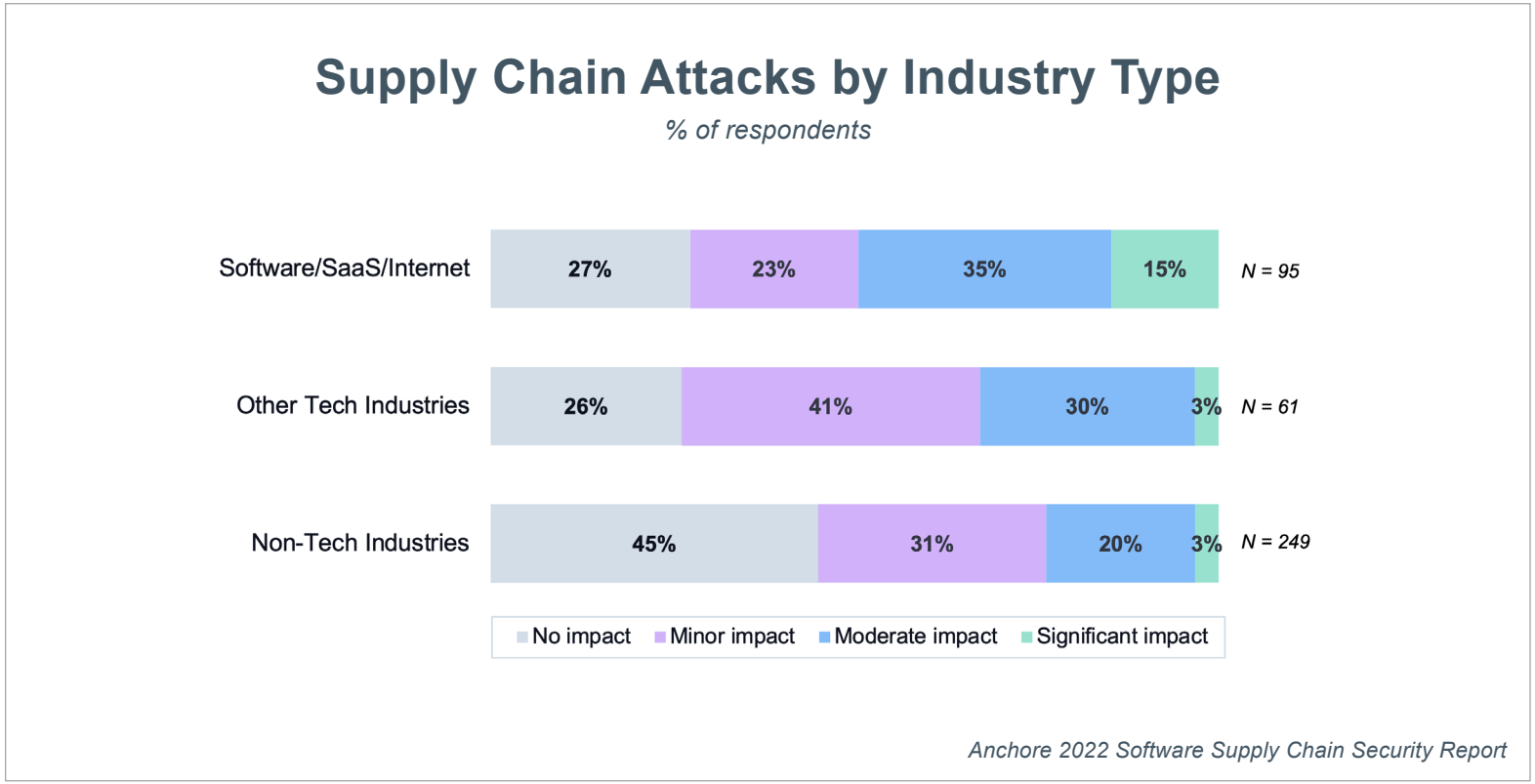
Supply Chain Attacks With the Biggest Impact

Because the Log4j vulnerability was published after the survey started, we were not able to include it in the list of vulnerabilities below, so this question covers other supply chain attacks. Excluding Log4j, respondents were impacted by an average of 1.6 supply chain attacks. The lingering effects of SUNBURST (SolarWinds) remains at the top of the attack list with the largest impact on respondents at 32 percent. Attacks such as the HAFNIUM exploit and MIMECAST also made the top of the list.



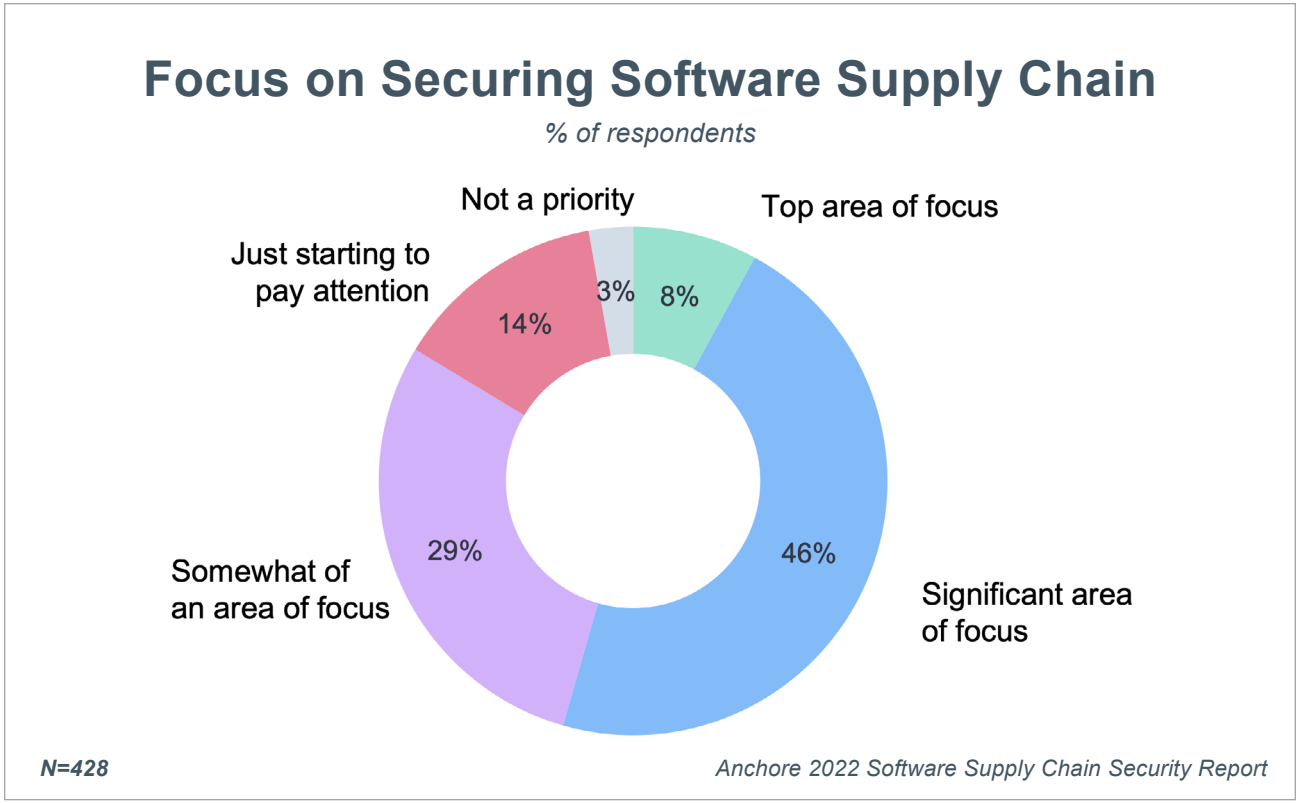
Tech Industry Impacted Most by Attacks

Organizations within the tech sector remain the most affected by supply chain attacks, with 15 percent in Software/SaaS/Internet reporting a significant impact as compared to 3 percent in other industries. This isn't surprising as supply chain attacks on software and internet companies can also impact the organization's customers, damaging brand reputation and revenue.



Enterprises Focus on Securing the Software Supply Chain

More than half of respondents (54 percent) indicated that securing the software supply chain is a top or significant focus, while an additional 29 percent report that it is somewhat of a focus. This indicates that recent, high-profile attacks have put software supply chain security on the radar for the vast majority of organizations, while very few (3 percent) indicate that it is not a priority at all.

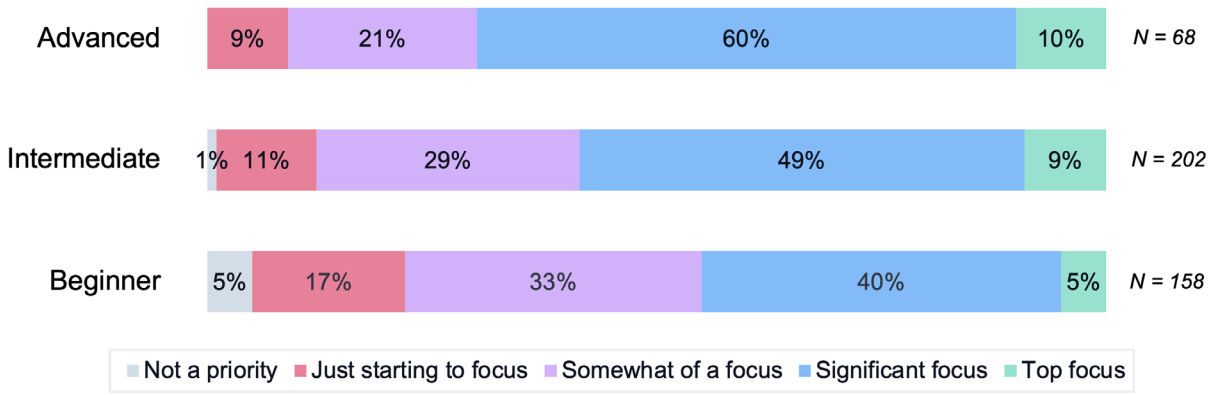


Supply Chain Focus Increases with Use of Containers

More mature container users are dedicating more attention to software supply chain security. 70 percent of advanced container users identify this as a top or significant focus as compared to 45 percent of beginner-level container users.

Focus on Securing Software Supply Chain by Container Maturity

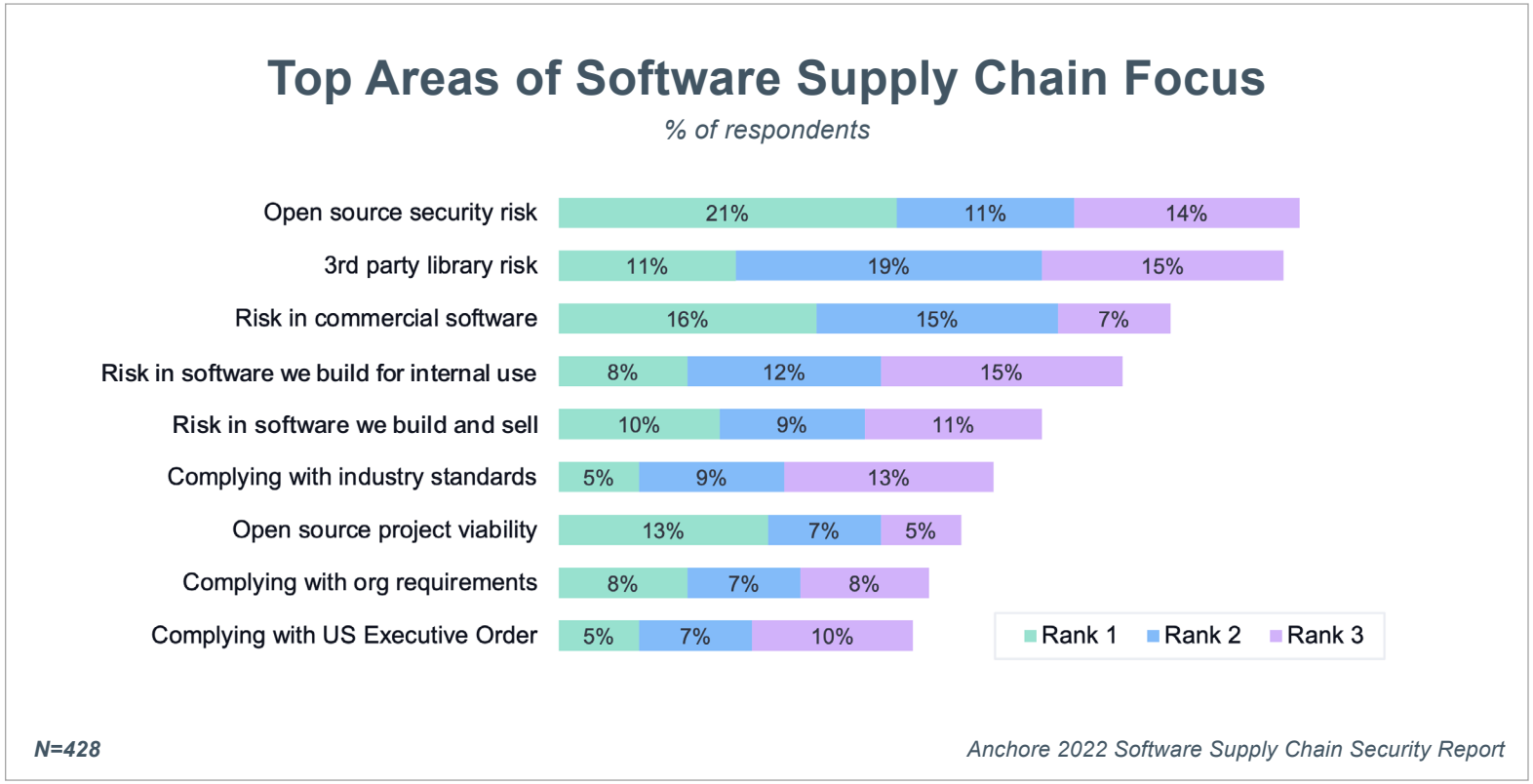
% of respondents



Anchore 2022 Software Supply Chain Security Report

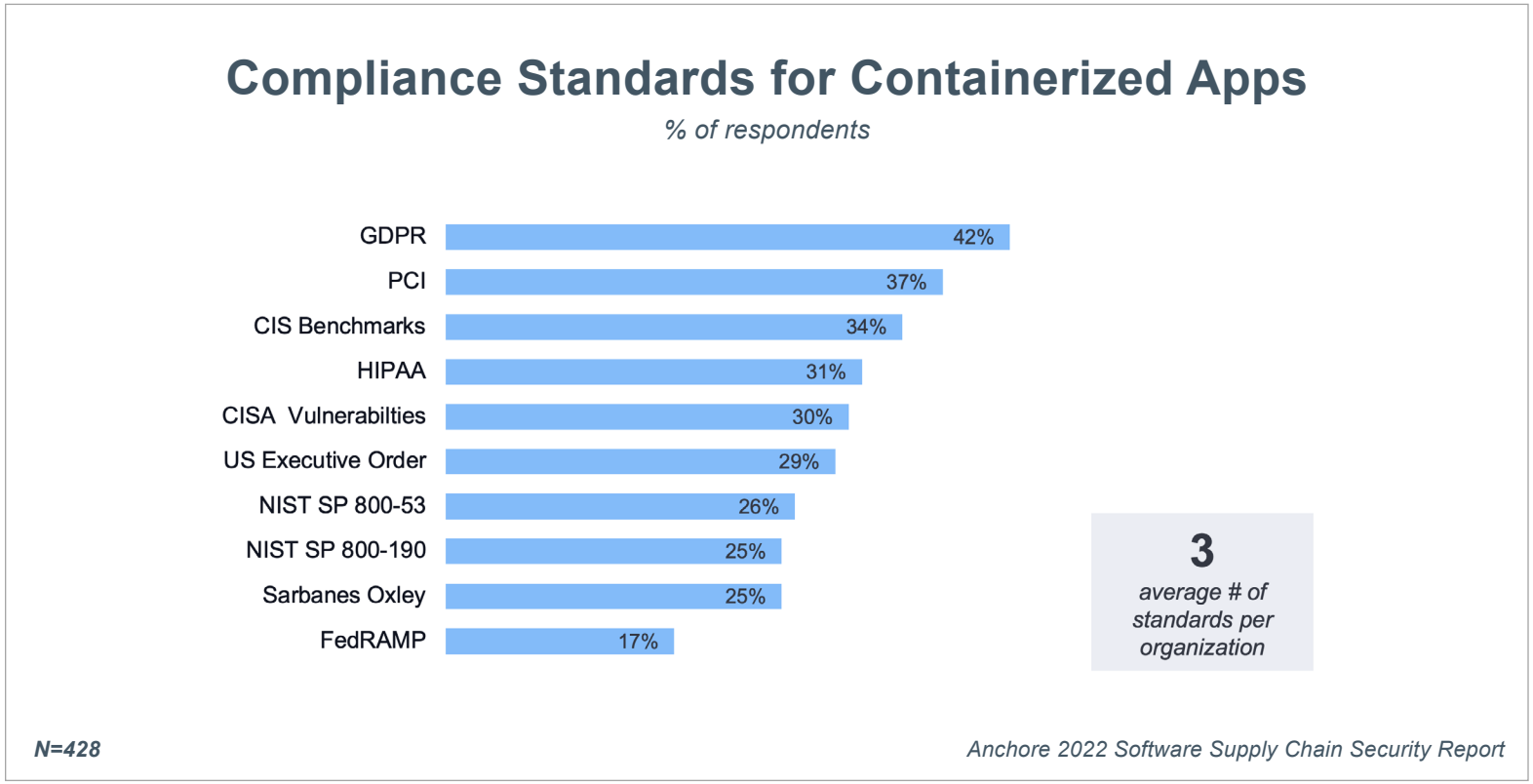
Top Areas of Software Supply Chain Focus

The security of open source is the top supply chain focus with nearly half (46 percent) ranking it in their top 3 priorities. This was closely followed by 3rd party libraries (45 percent) and commercial software (38 percent).



Organizations Comply with an Average of Three Standards

Industry, government, and organizational compliance requirements are also driving supply chain security initiatives. Respondents reported the need to comply with an average of three separate standards per organization. New requirements from the U.S. government are impacting many organizations, with 30 percent focusing on compliance with the CISA Directive of Known Exploited Vulnerabilities and 29 percent the U.S. Executive Order on Improving the Nation's Cybersecurity which was first introduced in May of 2021.

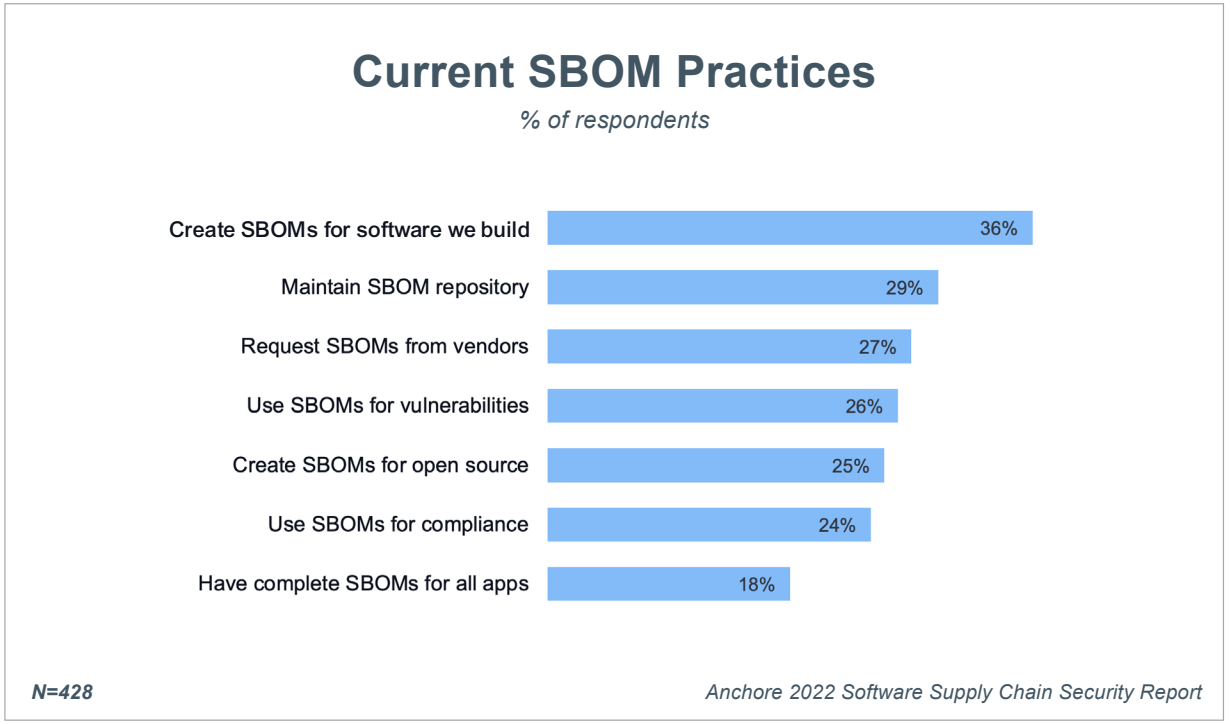


SBOM Practices Must Mature to Improve Software Supply Chain Security

Securing the software supply chain is top of mind for many of the survey respondents, yet the data shows few are incorporating SBOMs into their security posture or following SBOM best practices to achieve this goal. Despite these low numbers, respondents did report however that they plan to increase their SBOM usage in 2022, so these trends may change as adoption continues to grow.

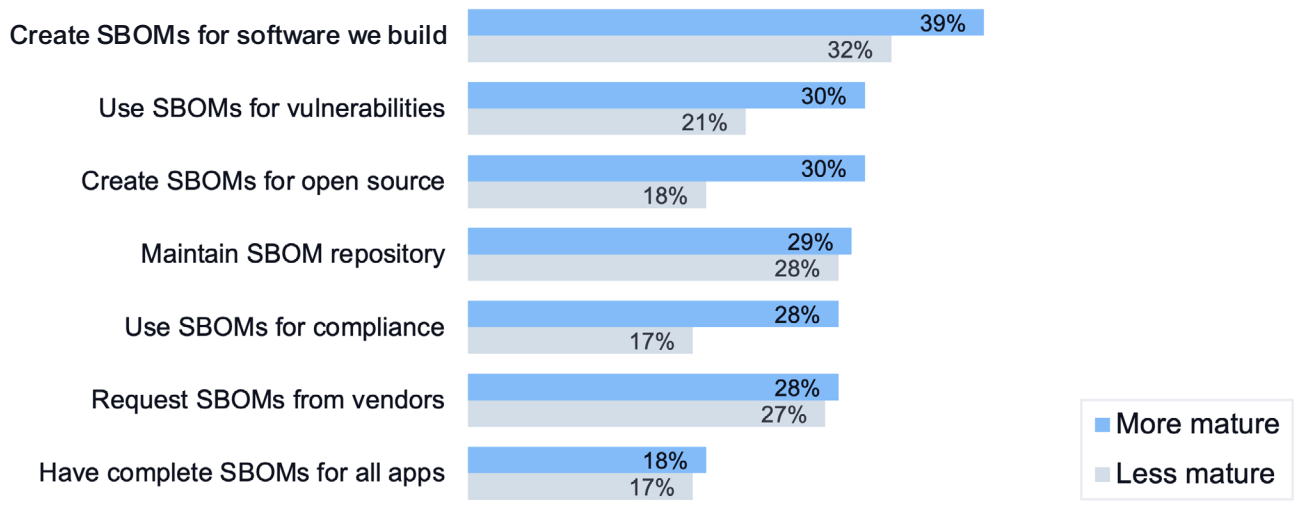
Few Follow SBOM Best Practices

Despite SBOMs foundational role in providing visibility into the software supply chain, less than a third of organizations are following SBOM best practices. In fact, only 18 percent of respondents have a complete SBOM for all applications.



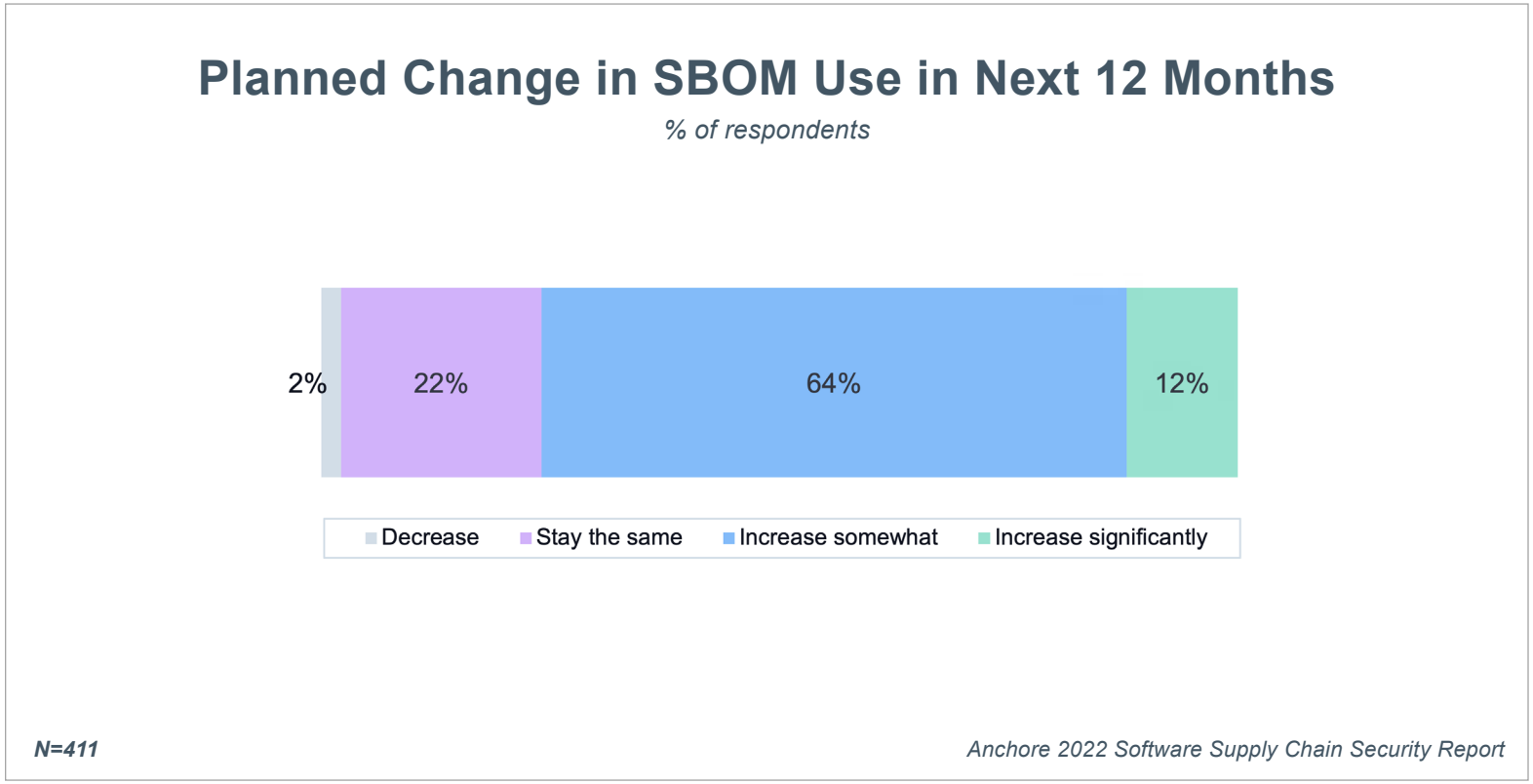
Mature Container Users Leverage SBOMs More

Not surprisingly, organizations that are more advanced in their container maturity leverage the use of SBOMs more, particularly in the creation of SBOMs for the software they build, maintaining SBOM repositories, and requesting SBOMs from vendors.



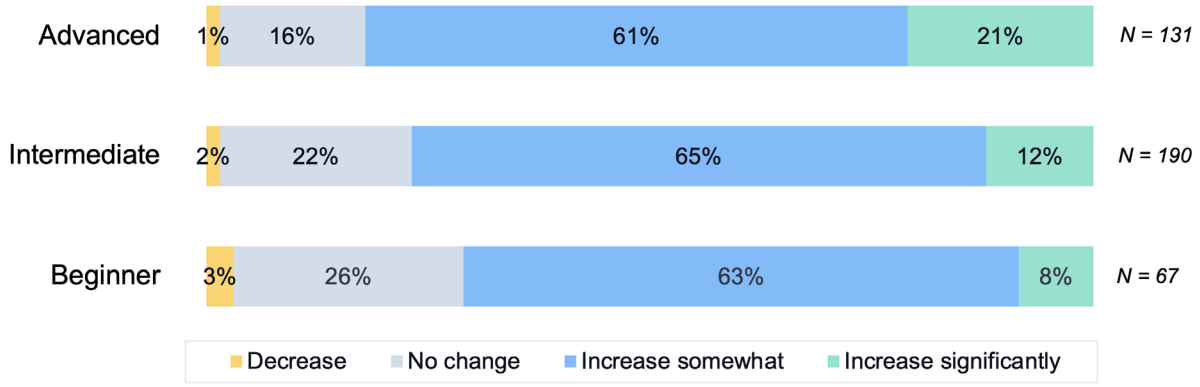
SBOM Adoption Will Continue to Grow

While SBOM adoption is still in its early stages, it will continue to grow and become more commonplace with 76 percent of respondents reporting that they plan to increase their SBOM usage in the next 12 months.



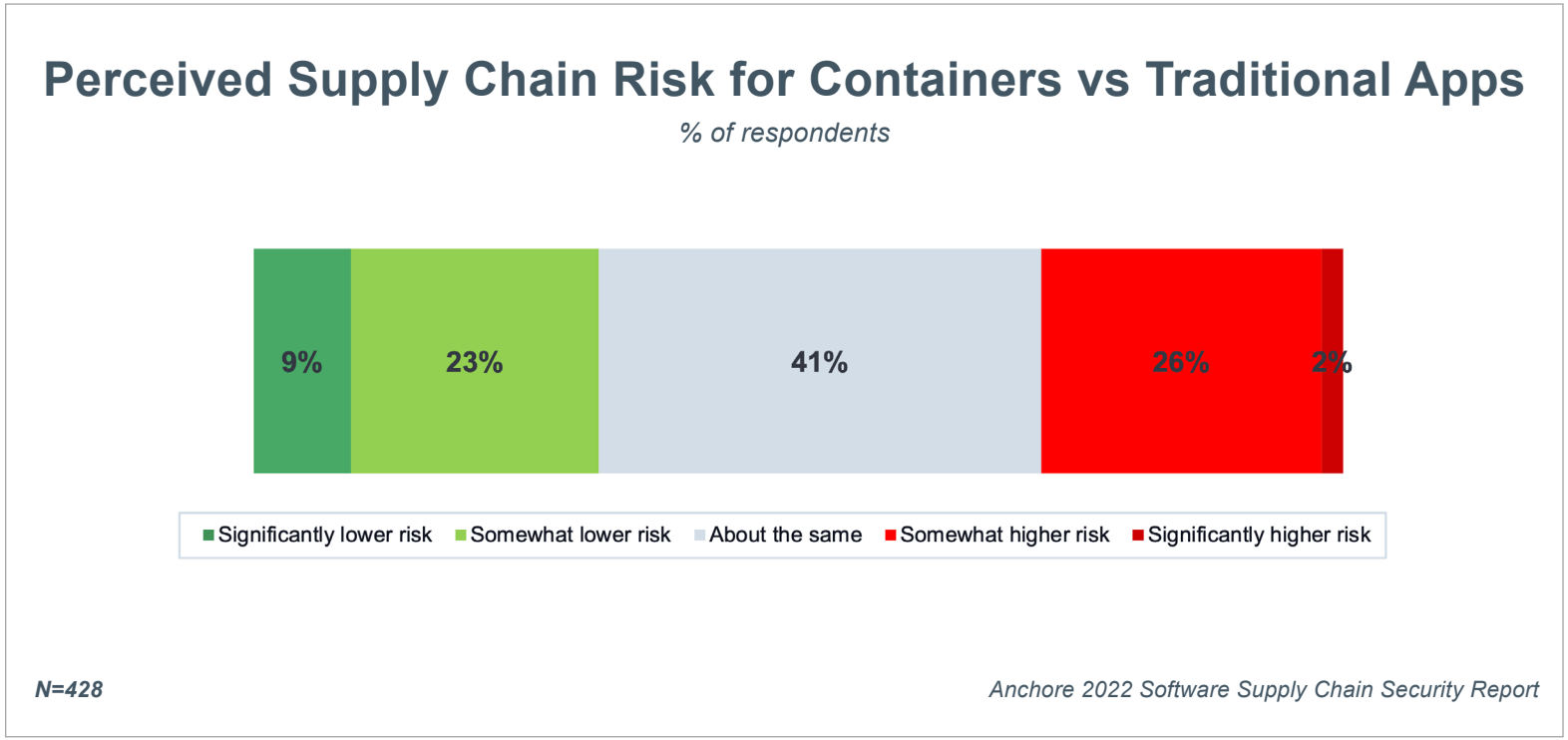
Mature Organizations Emphasize SBOM Use

As with software supply chain security, there is alignment between the container maturity of an organization and their plans to adopt SBOMs. Organizations across all levels of container maturity plan to increase their use of SBOMs, with 82 percent of advanced users citing plans to increase their use of SBOMs.



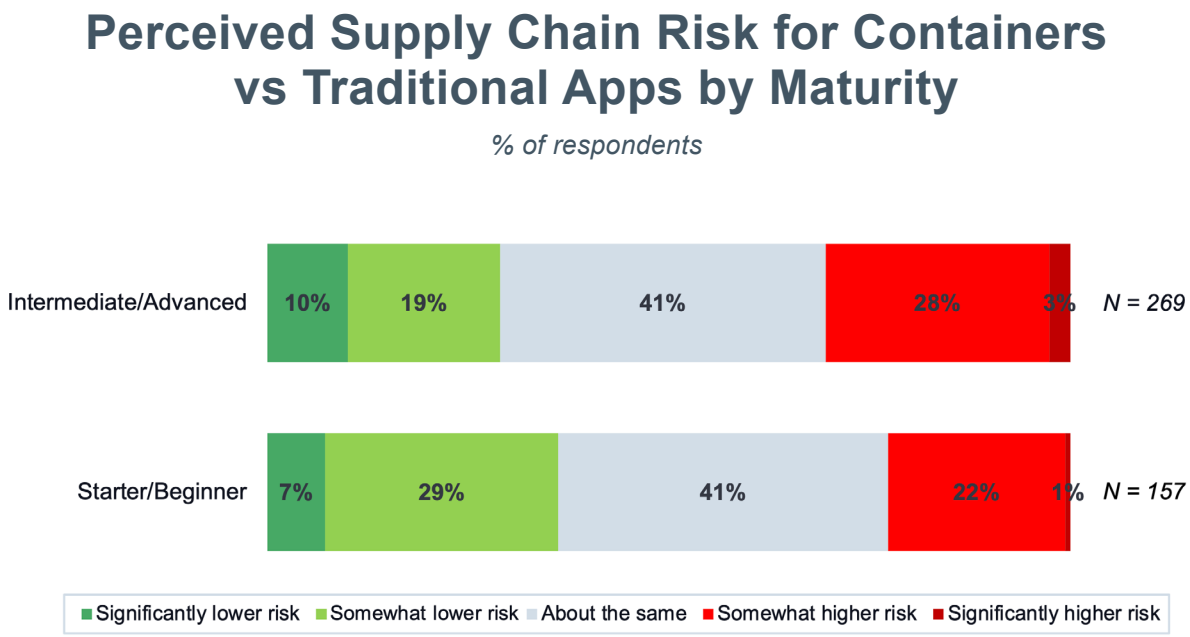
Securing Containers Focuses on Supply Chain and Open Source

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 32 percent see containers as being less risky.



More Mature Container Users See Higher Risks

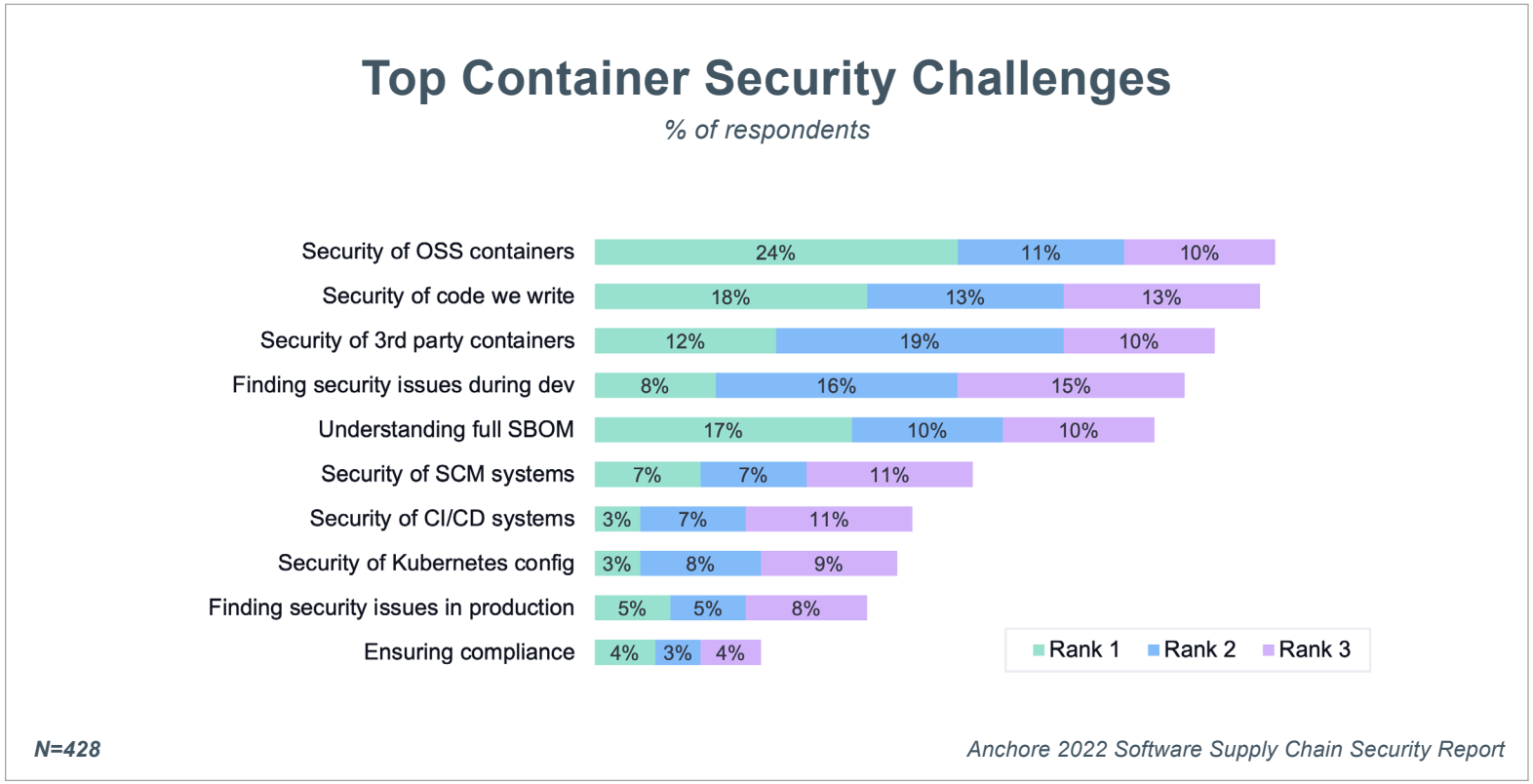
However, the perception of risk does vary with container maturity. Intermediate and advanced containers users see containers as having higher risk than beginner containers users (31 percent vs 23 percent). As users leverage containers more, they may be more likely to understand risks such as typosquatting and dependency hijacking that can impact containers.



Anchore 2022 Software Supply Chain Security Report

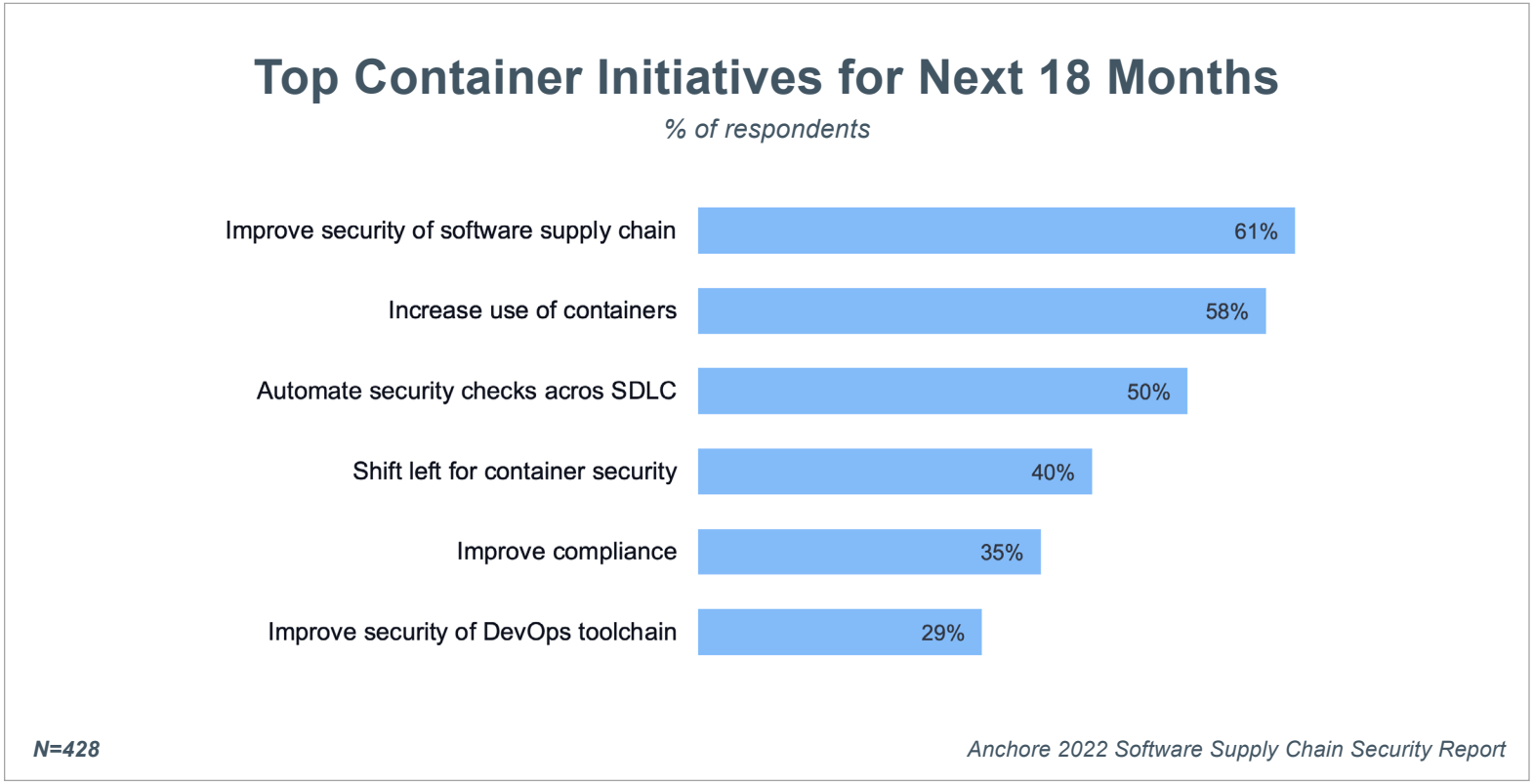
Open Source is the Top Container Security Challenge

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 24 percent of respondents with almost half (45 percent) ranking it among their top three challenges. Ranked next was *Security of the code we write* with 18 percent of respondents choosing that as their top container security challenge and *Understanding full SBOM* with 17 percent.



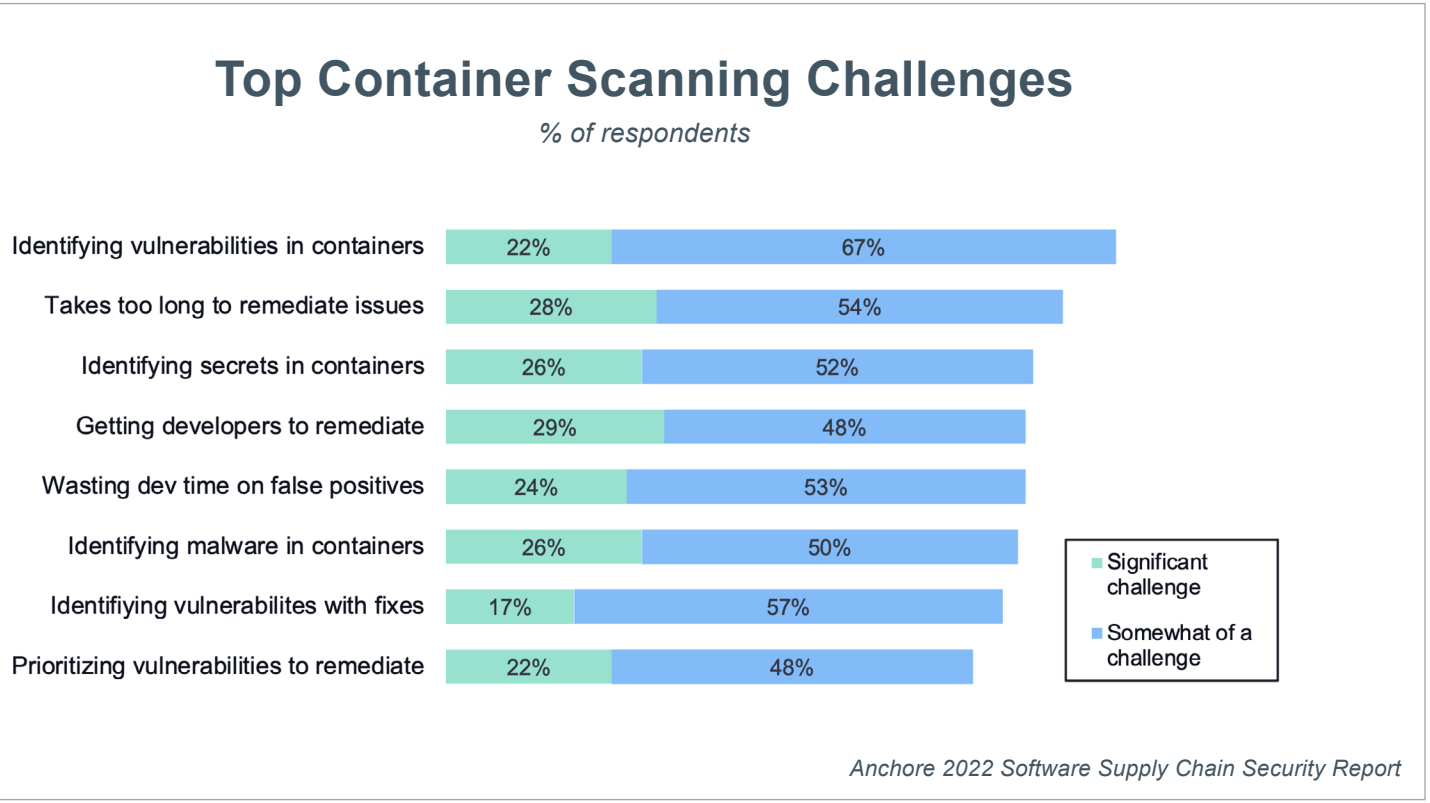
Supply Chain Security Is the Top Container Initiative

Survey respondents reported that their top container initiative for 2022 is to improve the security of the software supply chain (61 percent). This is not surprising given the prevalence of software supply chain attacks and the number of enterprise organizations impacted by them over the past year. The second most popular response was to increase the number of containers being used (58 percent).



Organizations Face Container Scanning Challenges

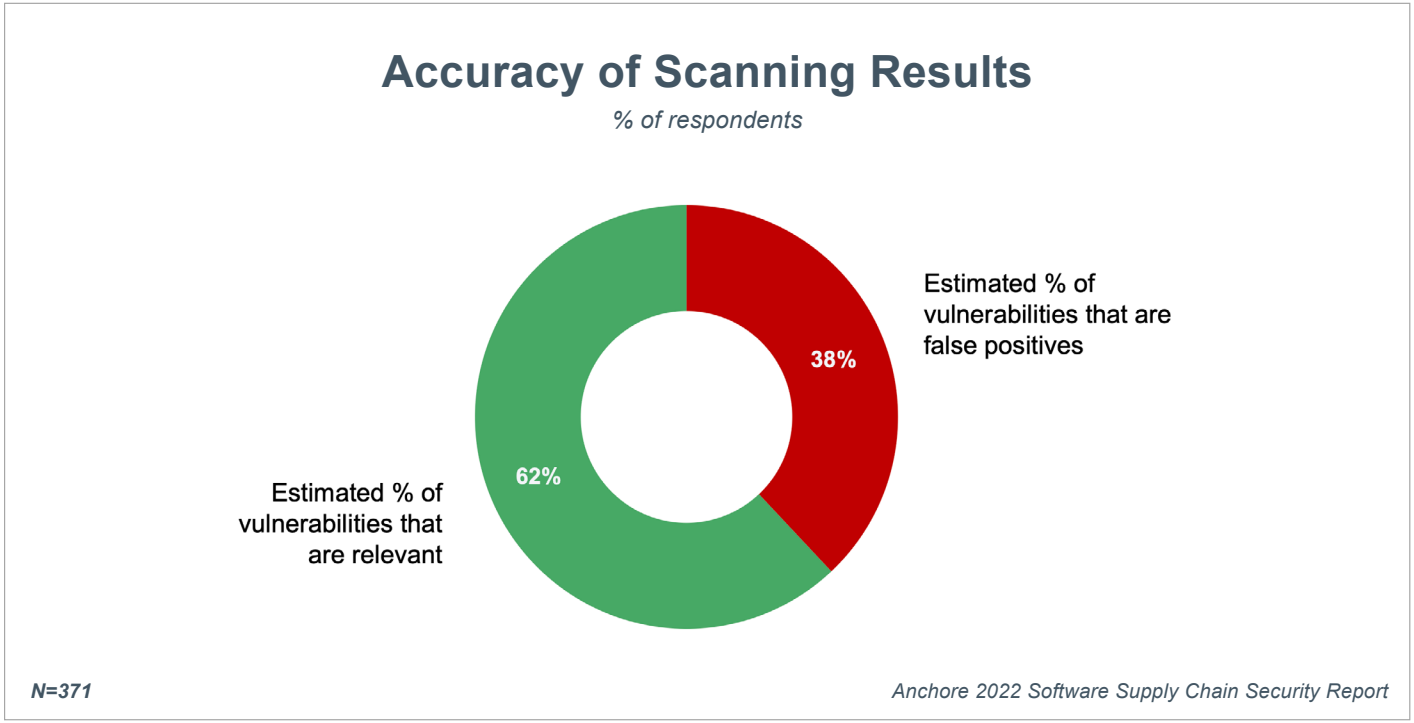
As organizations continue to expand their container use, a large majority face critical challenges related to identifying and remediating security issues within containers. Top challenges include identifying vulnerabilities in containers (89 percent), the time it takes to remediate issues (82 percent), and identifying secrets in containers (78 percent). Organizations will need to adopt more accurate container scanning tools that can accurately pinpoint vulnerabilities and provide recommendations for quick remediation.



False Positives are a Significant Problem

Respondents estimated that 38 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, security teams can build up large remediation backlogs and risk missing legitimate vulnerabilities. In addition, developers must spend time researching the issue and often provide justifications to the security team on why each particular vulnerability is not relevant. Over time, it can also degrade trust and collaboration between development and security teams. 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 heat map on this table shows darker colors for the highest percentages. Security, DevOps/Platform Engineering, and Development teams are the most heavily involved in container security.

Container Security Responsibilities

% of respondents

	Security	DevOps/ Platform Eng	Development	Product Security	I&O	Cloud Team
Ensuring compliance with standards	63%	39%	31%	32%	28%	24%
Prioritizing security issues	59%	35%	30%	29%	22%	16%
Security checks for OSS images	57%	41%	38%	33%	26%	21%
Finding vulnerabilities during staging/production	55%	44%	37%	28%	26%	23%
Finding vulnerabilities during development	51%	37%	50%	28%	14%	19%
Securing the DevOps toolchain	42%	59%	24%	20%	18%	20%
Fixing security issues in the container runtime	38%	47%	34%	22%	28%	22%
Fixing security issues in container images	37%	44%	45%	22%	20%	20%

N=428

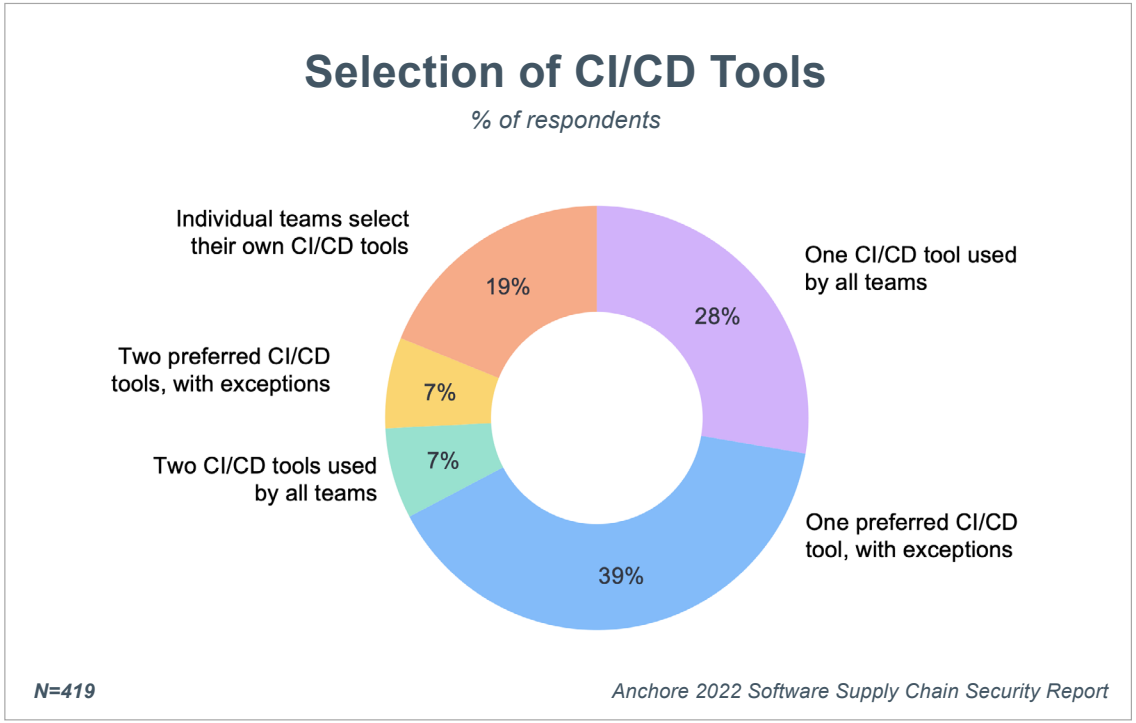
Anchore 2022 Software Supply Chain Security Report

Organizations Must Secure Diverse DevOps Toolchains

As organizations increasingly adopt DevOps processes, they are incorporating new toolchains that speed up software development. Additionally, they are embedding security checks into these processes in order to better protect the software supply chain. However, organizations rarely have just one toolchain, which means that they need ways to standardize and centralize their security processes and policies across these diverse environments.

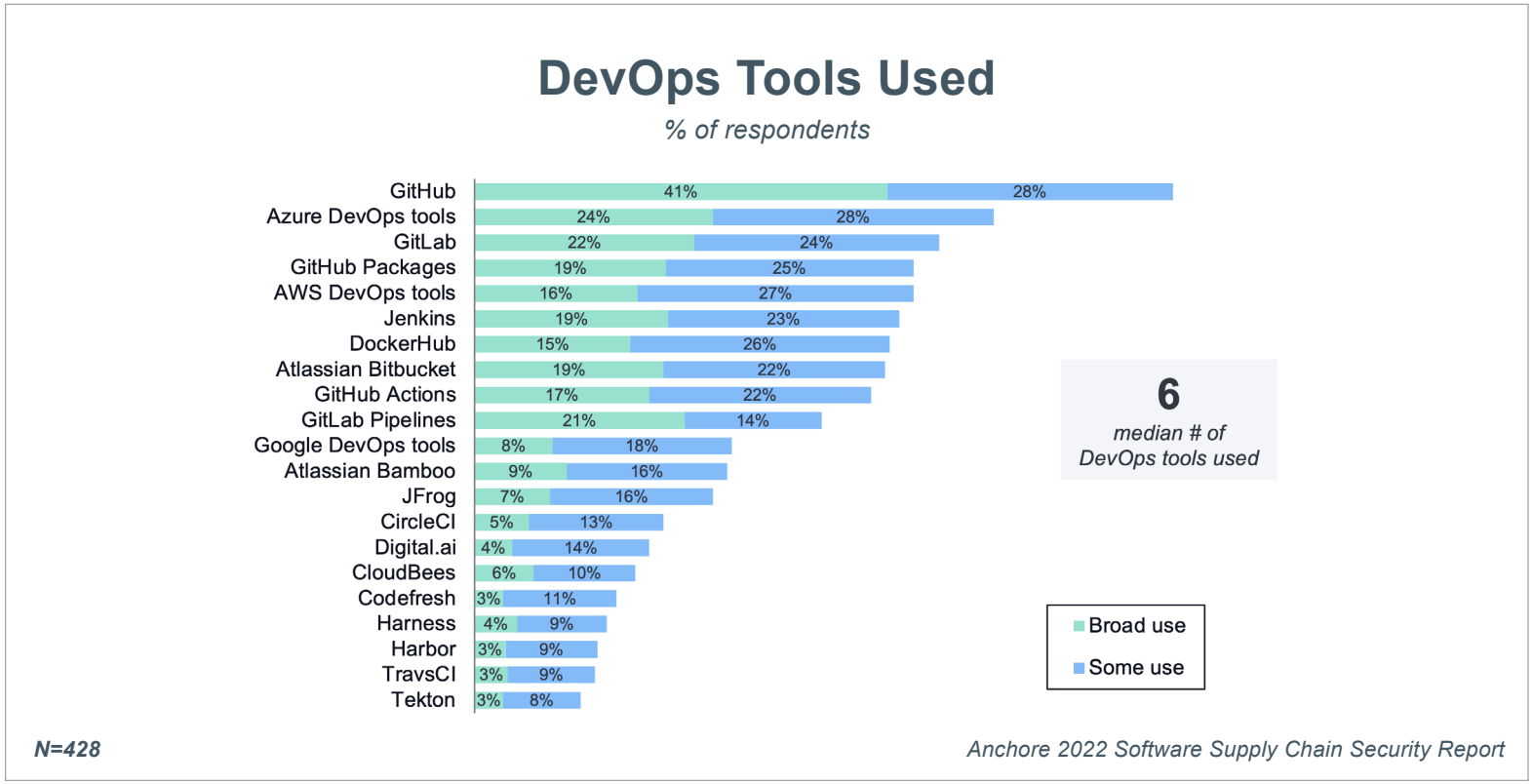
Organizations Use Many DevOps Tools

Continuous integration and delivery (CI/CD) tools are a critical foundation for DevOps processes. However, within an organization, different development teams and business units will select different tools. Only 28 percent of respondents reported only one CI/CD tool is being used by all teams, while 72 percent are using multiple different tools across teams.



DevOps Tools Used

As organizations assemble the complete set of DevOps tools needed, they are using a median of 6 different DevOps tools in their toolchain. The most used tools for DevOps include GitHub (69 percent), Azure DevOps (52 percent), GitLab (46 percent), GitHub Packages (44 percent), and AWS DevOps tools (43 percent). Organizations must look for ways to embed security into this diverse set of tools and platforms.

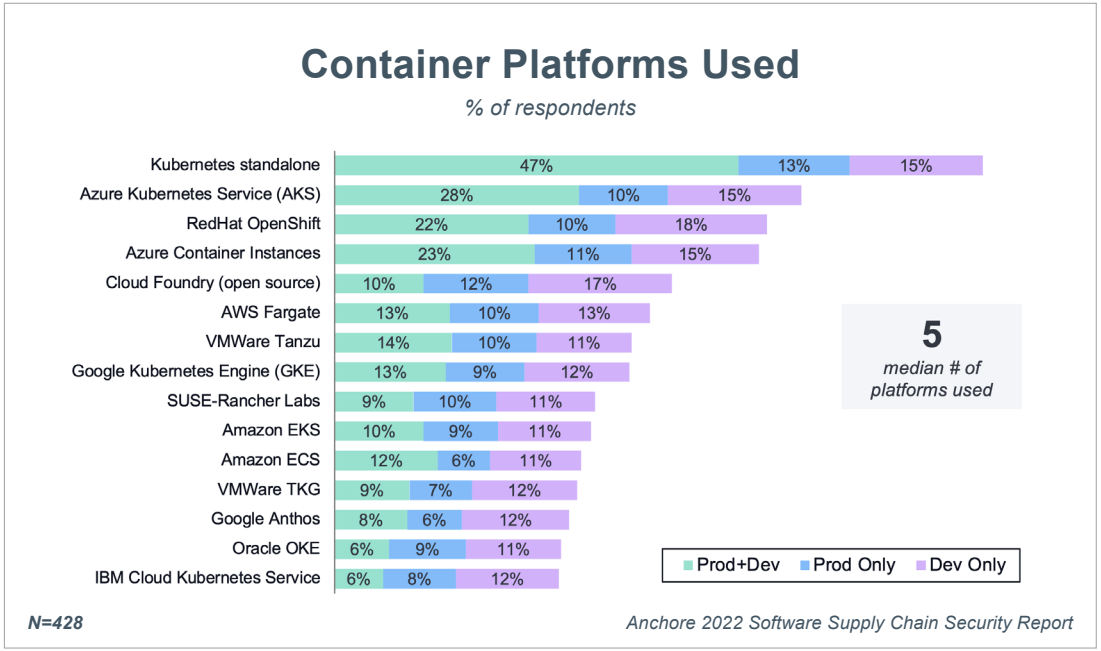


Organizations Must Secure Multiple Container Platforms

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. Security teams must provide processes and tools that work across this diverse set of container platforms.

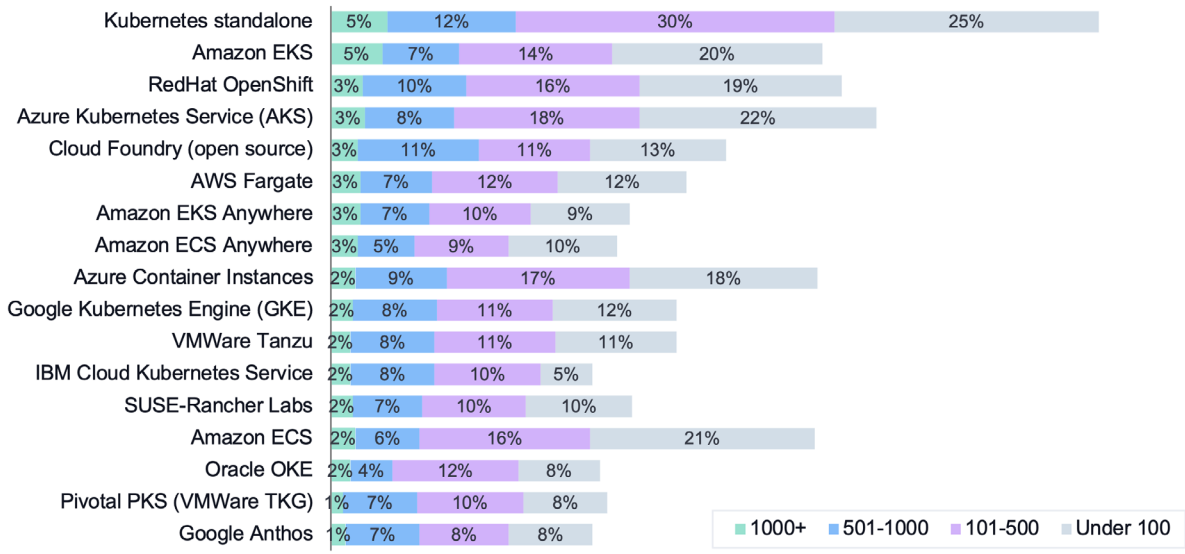
Container Platforms are Used by Development and Production

Respondents used a median of 5 container platforms. "Standalone" Kubernetes based on the open source package is used most often by 75 percent of respondents. These environments may be run on-premises, through a hosting provider, or on a cloud provider's infrastructure. The second most used container platform is Azure Kubernetes Service (AKS) (53 percent) and Red Hat OpenShift is third with 50 percent. The top container platforms are also heavily used in both production and development environments.



Number of Containers Running in Container Platforms

As container use continues to grow, the number of containers running is increasing. Five percent of respondents run at least 1000 containers in “Standalone” Kubernetes and Amazon EKS environments while Red Hat OpenShift, Azure Kubernetes Service (AKS), Cloud Foundry (open source), AWS Fargate, Amazon EKS Anywhere, and Amazon ECS Anywhere are all tied at 3 percent.



N=428

Anchore 2022 Software Supply Chain Security Report

Recommendations

Security and technical leaders had a wake-up call in 2021. The year was bookended by the SolarWinds SUNBURST attack and the Log4j zero-day vulnerability which showed how costly supply chain security risks can be to organizations across a wide set of industries. Now organizations are sitting up and paying attention. They are increasing their focus on securing their software supply chain.

Meanwhile the world is rapidly shifting to cloud-native software that runs in containers and is built using DevOps processes. This shift exacerbates supply chain risks as we leverage easily accessible open source components with complicated dependencies that are not always readily apparent. As a result, we must implement new supply chain security protocols and tools that address these new realities.

Software supply chain management must become a new practice for every organization that uses or builds software. SBOMs are rapidly becoming a critical foundation of this new practice, providing visibility into the ingredients of the software you use.

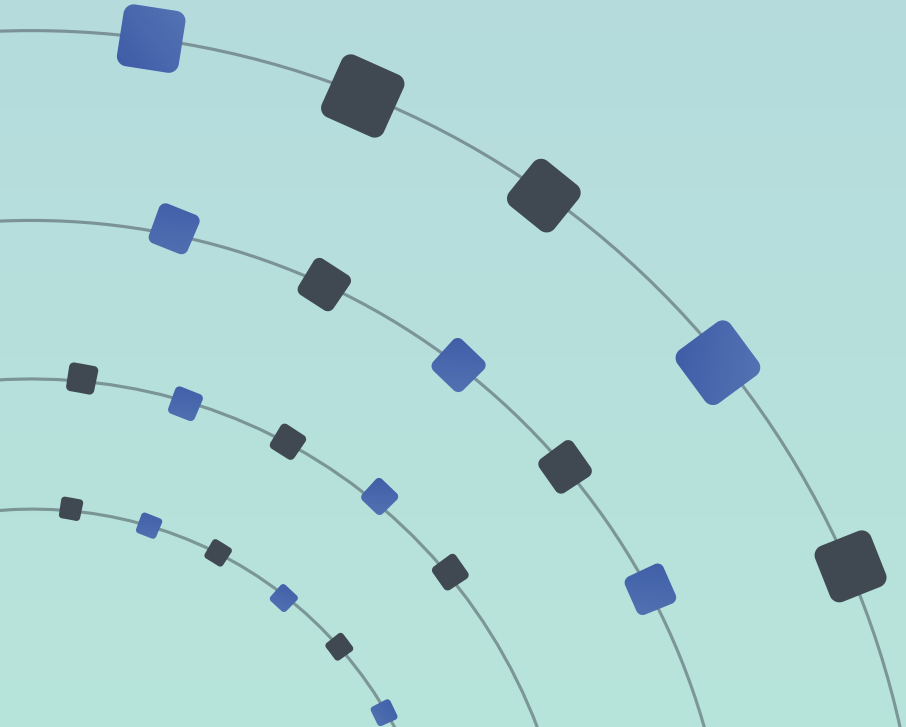
Recommendations

Here are seven steps for 2022 to begin your journey to better software supply chain management:

1. Educate your organization on software supply chain security. Identify where security threats can enter your processes and tools. Learn more.
2. Create a working group or Software Supply Chain Center of Excellence to develop best practices and a plan for your organization to improve cybersecurity.
3. Start with the software bill-of-materials as a prerequisite for software supply chain security best practices. Require SBOMs in standard formats from your software vendors, and produce SBOMs for the software you build. Learn more.
4. Identify tools to generate, store, and manage SBOMs. Use SBOMs to identify vulnerabilities, including those that arise post-deployment. Open source tools such as Syft are a great starting point to give you visibility into the software containers you use.
5. Shift security left by embedding security at each step in your DevOps process. Implement continuous scanning and security checks in code repositories, CI/CD pipelines, container registries, staging environments, pre-deployment, and post-deployment. Look for scanning tools (such as open source tool Grype) with powerful APIs that are easy to embed in your toolchains.
6. 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.
7. 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 is a leader in software supply chain security and enables organizations to protect cloud-native applications against software supply chain attacks. Anchore technology embeds continuous security and compliance checks at every stage of the software development process to prevent security risks from reaching production. Large enterprises and government agencies use Anchore solutions to generate a comprehensive software bill of materials, pinpoint vulnerabilities, identify malware and discover unprotected credentials that can lead to hacks and ransomware. With an API-centric approach, Anchore solutions integrate into the tools developers already use to detect issues earlier, saving time and lowering the cost to fix vulnerabilities. To learn more visit www.Anchore.com.



anchore

info@anchore.com
anchore.com