anchore

Anchore 2024 Software Supply Chain Security Report

76% of respondents prioritize software supply chain security as the effects of software supply chain attacks intensify

Contents

Introduction

This report compiles the responses of more than one hundred leaders and practitioners in security, development, DevOps, and IT to identify the latest trends in how organizations are responding to the ever-increasing security challenges of the software supply chain. It also identifies best practices and action items that organizations can use to improve their security stance and reduce the risk of attacks.

Executive Summary

Since our last report in 2022, security risks of the software supply chain have continued to grow apace with no slowdown in sight. Gartner predicts that by 2025, **45% of organizations worldwide will have experienced attacks on their software supply chains**, a three-fold increase from 2021.

The global annual cost of software supply chain attacks to businesses will grow to $60 billion in 2025.

— Cybersecurity Ventures.

This year's report found that the impact of a successful supply chain attack is increasing. As attackers grow more sophisticated, **the remediation expense, risk of financial losses, and reputational damage are further heightened**. Organizations see security as integral to business success.

"Securing our supply chain is one of our top priorities since we depend on it for the smooth operation of our company. With the increased cases of security breaches in supply chains, this has increased importance to us."

— Survey respondent

As software supply chain risks grow, governments and industry groups are responding with new guidelines and regulations. The US Executive Order 14028 led to new requirements this year for Secure Software Development Attestation, and there are also emerging sector-specific requirements, such as those from the FDA for medical devices. The EU NIS2 directive for improved software supply chain security and the Cyber Resilience Act will also come into play this year.

"Government regulations now require supply chain security. We were affected by the SolarWinds issues as well and had to quickly find other solutions."

— Survey respondent

As a result of growing risks and increasing compliance requirements, software supply chain security is top of mind for CISOs, the C-suite, and the board of directors.

"Because of rising software supply chain attacks, it is becoming clear that this is a necessity, not a nicety."

-Survey respondent

Organizations are looking to secure all elements of their software supply chain, including open source software and 3rd party libraries. Compliance with new industry and governmental standards is also a significant driver for many organizations.

"Our organization provides trusted applications to US Government entities and the private industry. As a result, we must ensure that we have a solid understanding of securing the supply chain for our customers and in order to ensure the data we store is secure."

-Survey respondent

The software bill-of-materials (SBOM) is now 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 just under 50% of respondents currently leverage SBOMs, a large majority plan to increase SBOM use over the next 18 months.

"Federal agencies are requiring things like SBOMs and CMMC compliance and we believe the "Sec" in DevSecOps should be given equal weight to development and operations in the SDLC"

-Survey respondent

Attribution requirements for sharing charts

Methodology

This report provides a view of practices for securing the software supply chain as provided by 106 leaders and practitioners involved in software supply chain security. Their responses provide a unique perspective on current security practices and challenges. The survey was conducted during August and September 2024.

Highlights

The Anchore 2024 Software Supply Chain Security Report identifies important trends in securing the software supply chain.

Effects of software supply chain attacks intensified

40% of organizations reported software supply chain attacks in the past 12 months, down from the 62% reporting attacks in 2022 in the wake of SolarWinds.

24% of organizations reported **multiple attacks**, while 15% reported a single attack.

For organizations that experienced an attack, **the effect was intensified**, with 21% reporting a significant impact vs. 10 % in 2022.

59% of those experiencing an attack reported **a significant or moderate impact** vs. 50% in 2022.

200% increase in organizations making software supply chain security a top priority

The proportion of respondents indicating that software supply chain security is a top priority **tripled in 2024** (24%) vs. 2022 (8%).

A supermajority (76%) indicates that software supply chain security is **a significant or top priority**.

Organizations with **high container maturity** are even more likely to make software supply chain security a top priority (47% of advanced container users vs. 25% overall).

Organizations struggle to verify the security of open-source and third-party software

Verifying the ***security of 3rd party software*** (46%) joins ***security of open source*** (42%) as the **top two significant challenges**. ***Security of the development toolchain*** is the third most cited challenge (34%).

These challenges tie directly to companies' **top-ranked priorities**, with ***reduce open-source risk*** (31%), ***automate scans across the SDLC*** (26%), and ***improve security of the DevOps toolchain*** (17%) cited most frequently.

Combining organizations' top three rankings, ***automating compliance checks*** (52%) is third in the top focus areas.

Organizations make significant investments in supply chain security to comply with an average of five different standards

Compliance with regulatory requirements and industry standards impacts almost every organization (92%).

Organizations **comply with an average of 4.9 standards**, up from 3 in the 2022 survey.

CIS Benchmarks are the most common standard (45%), followed by the CISA Directive on Known Exploited Vulnerabilities (36%).

35% of organizations invest **significant time and resources** in compliance for the software supply chain. The average effort is 3.9 on a scale of 1 to 5.

Only 1 in 5 respondents are very confident in their visibility into dependencies

Only 1 in 5 respondents are confident that they **fully understand all the components and dependencies** in their software.

As a result, 78% of organizations plan to **increase their use of SBOMs** in the next 18 months, with 32% planning a significant increase.

Under half of respondents follow **best practices** like creating SBOMs for software they develop (49%) or open source they use (45%) or requesting SBOMs from vendors (41%).

However, this is a **significant improvement from 2022**, when less than a third followed these best practices.

Software supply chain security is a shared responsibility requiring collaboration

59% of organizations have a **cross-functional or dedicated team** focused on software supply chain security to facilitate collaboration.

Security teams generally shoulder the responsibility of vetting the security of components and prioritizing security issues.

DevOps and Platform Engineering take the lead in generating and managing SBOMs, securing the toolchain, and addressing issues in staging and production.

Development teams take the most responsibility for security during the development phases.

Compliance teams are tasked with ensuring compliance, with the support of other functions.

Only 1 in 10 use VEX today, but 4 in 10 plan to adopt it in the next 18 months

Only 10% of respondents currently have a **strategy for using VEX** (Vulnerability Exploitability Exchange) docs, while 12% consume VEX docs and 8% produce them.

However, **interest in VEX is high**. One-quarter of respondents expect to adopt VEX in the next six months, and another 15-20% plan to adopt it within 18 months.

AI raises opportunities and concerns for software supply chain security

A large majority of respondents are **concerned about AI's impact on software supply chain security**, and as many as a third are very concerned.

The **highest concerns** are with code tested with AI (35%) and code generated with AI (32%) or with Copilots (27%).

Respondents are less worried about AI models built by the company (22%) or libraries embedded in their products (22%).

The effect of software supply chain attacks has intensified

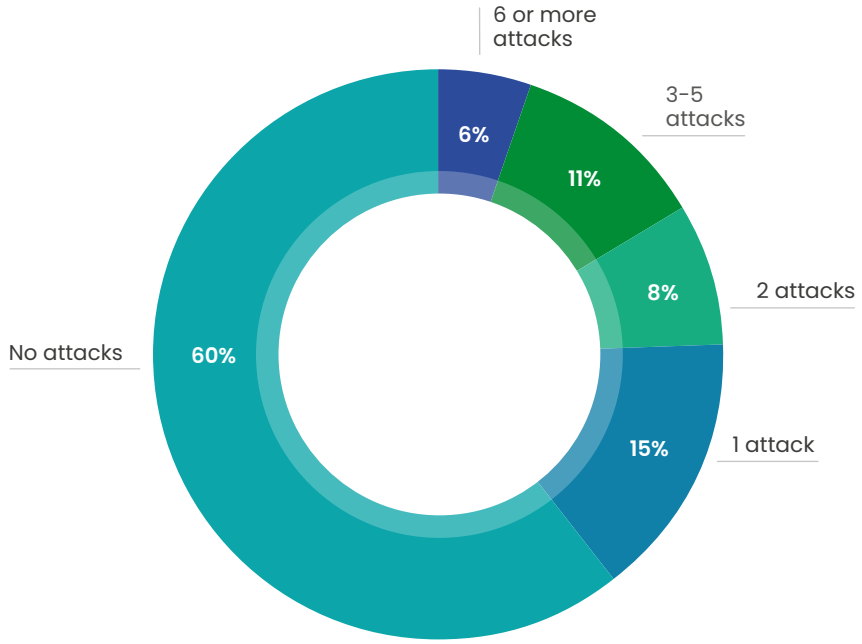
In our last report in early 2022, 62% of organizations had experienced software supply chain attacks in the prior year, with SolarWinds as the most extensive attack impacting 32% of respondents. This year's report shows that fewer organizations experienced supply chain attacks, but the effect was more significant for those who experienced an attack.

Supply chain attacks impact 40% of organizations

A combined 40% of respondents were affected by at least one software supply chain attack during the prior 12 months. One-quarter of respondents experienced multiple supply chain attacks, while 15% reported a single attack.

Number of Software Supply Chain Attacks Experienced in Last 12 Months

% of respondents



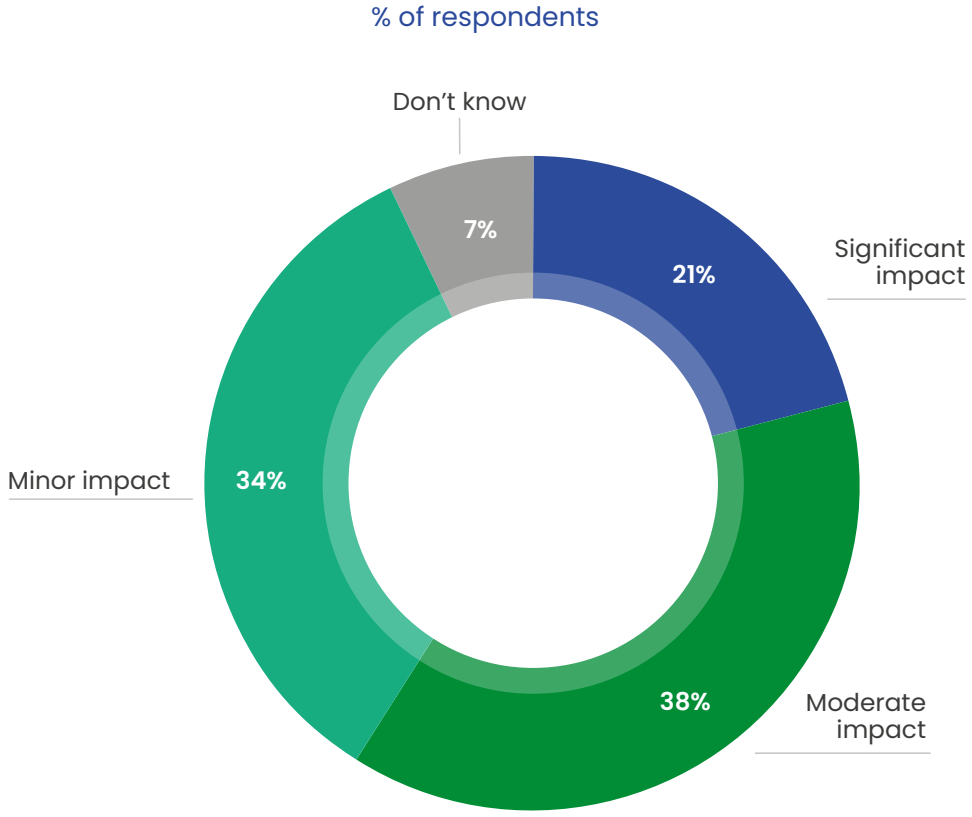
Anchore 2024 Software Supply Chain Security Report

N = 73

Effects of software supply chain attacks intensified

Of those experiencing a software supply chain attack, the effects were greater, with 21% reporting that it had a significant impact compared to 10% in 2022. More than half (59%) reported a significant or moderate impact compared to 2022 (50%).

Impact of Software Supply Chain Attack in Last 12 Months



Anchore 2024 Software Supply Chain Security Report

N = 29

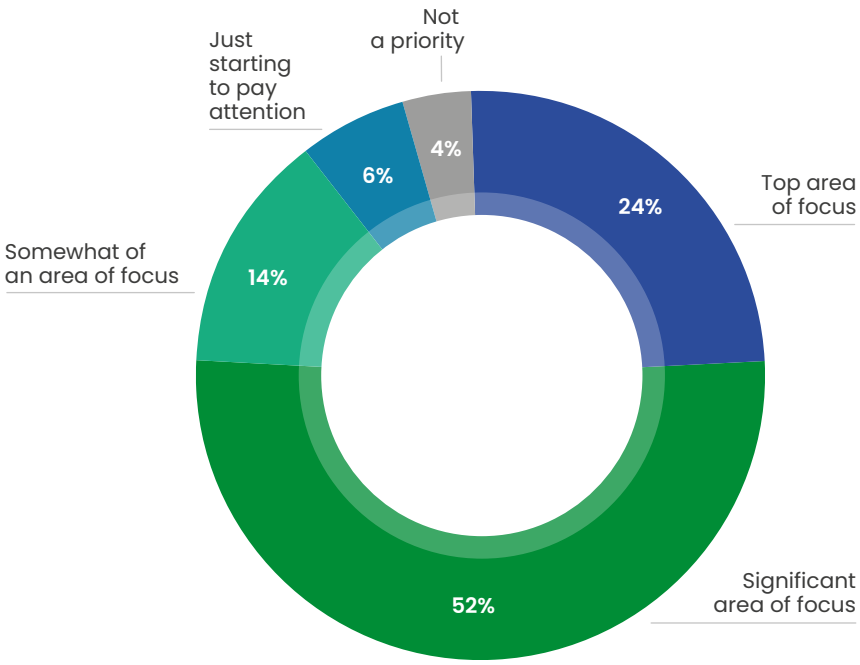
Software supply chain attacks drive higher priority on supply chain security

Organizations are placing significantly more focus on software supply chain security. Nearly one-quarter of respondents (24%) indicated that securing the software supply chain is a top area of focus, tripling from the 2022 report (8%).

In total, 76% of respondents say their organizations place a significant or top focus in this arena, while 14% indicate it is somewhat of a focus. Very few (4%) indicate that it is not a priority.

Focus on Securing Software Supply Chain

% of respondents

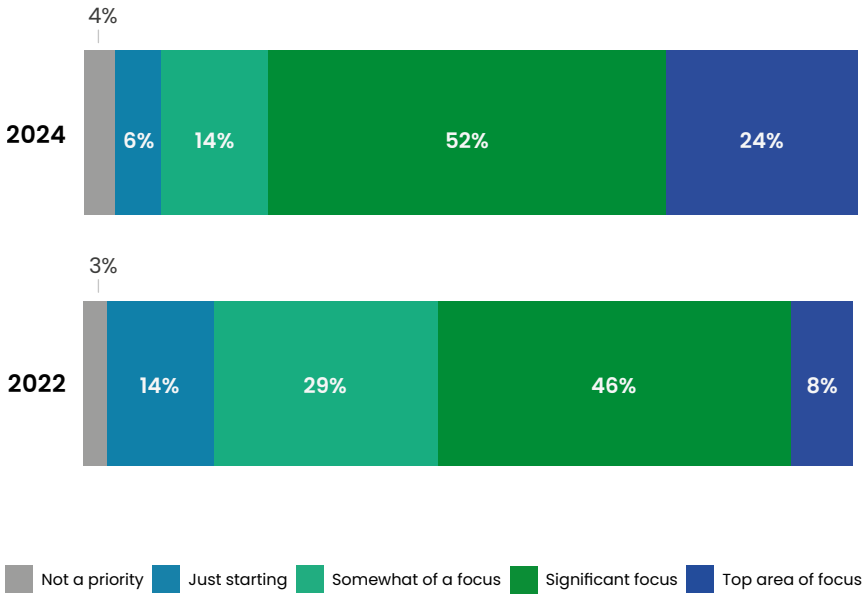


Anchore 2024 Software Supply Chain Security Report

N = 106

Focus on Supply Chain in 2024 vs. 2022

% of respondents



Anchore 2024 Software Supply Chain Security Report

N = 106

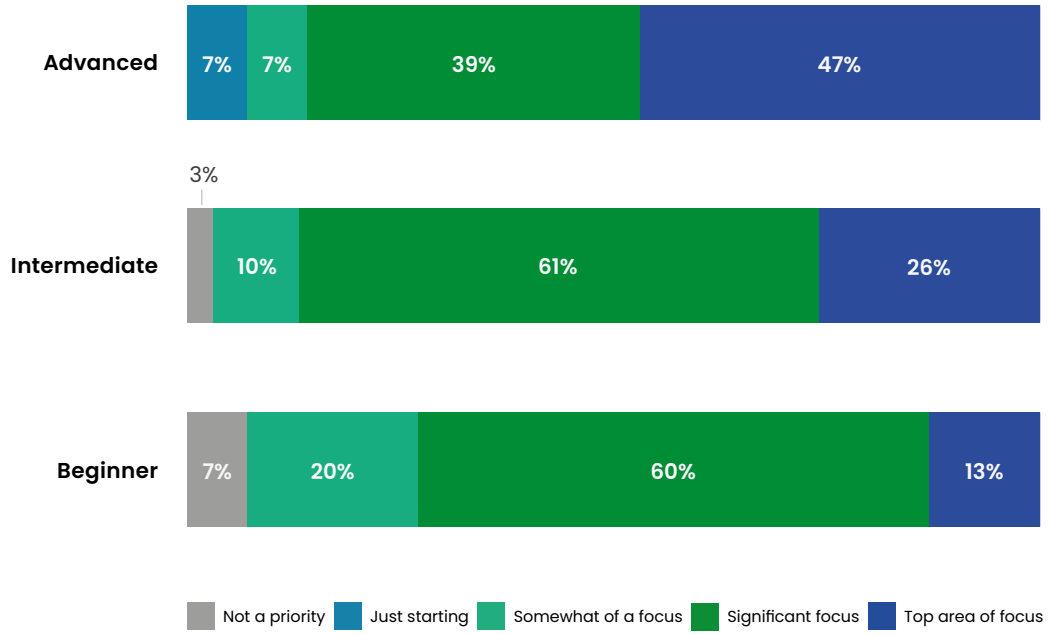
anchore

Supply chain focus increases with the use of containers

More mature container users are dedicating even more attention to software supply chain security. 47% of advanced container users identify this as a top focus, compared to 13% of beginner-level container users.

Focus on Securing Software Supply Chain by Container Maturity

% of respondents



Anchore 2024 Software Supply Chain Security Report

N = 106

Supply chain priorities align with top challenges

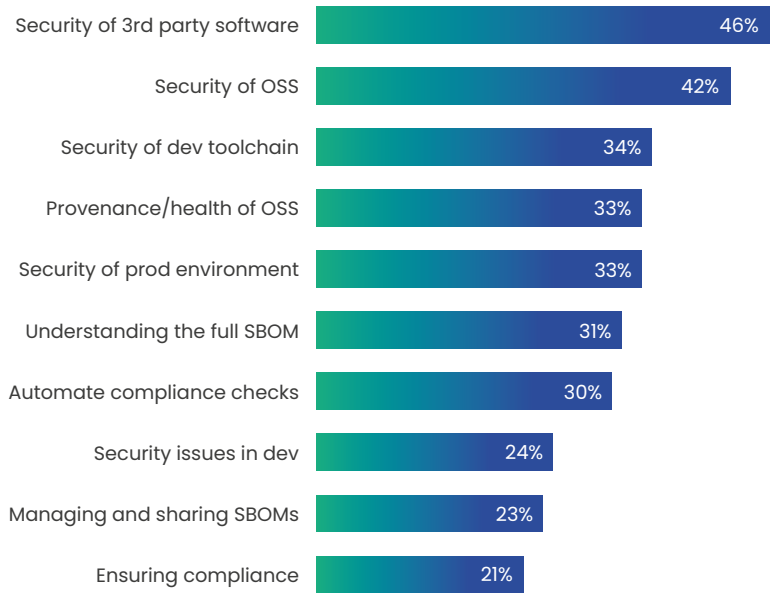
With increased prioritization of software supply chain security, organizations are aligning to their key areas of challenge and prioritizing best practices.

Third-party software joins open source as a top security challenge

While the ***security of open source software*** continues to be identified as a significant challenge (42%), in this year's report, even more respondents chose the ***security of 3rd party software*** as a significant challenge (46%). ***Security of the development toolchain*** rounds out the top three, with 34% citing it as a challenge.

Top Supply Chain Security Challenges

% of respondents rating as a significant challenge



Anchore 2024 Software Supply Chain Security Report

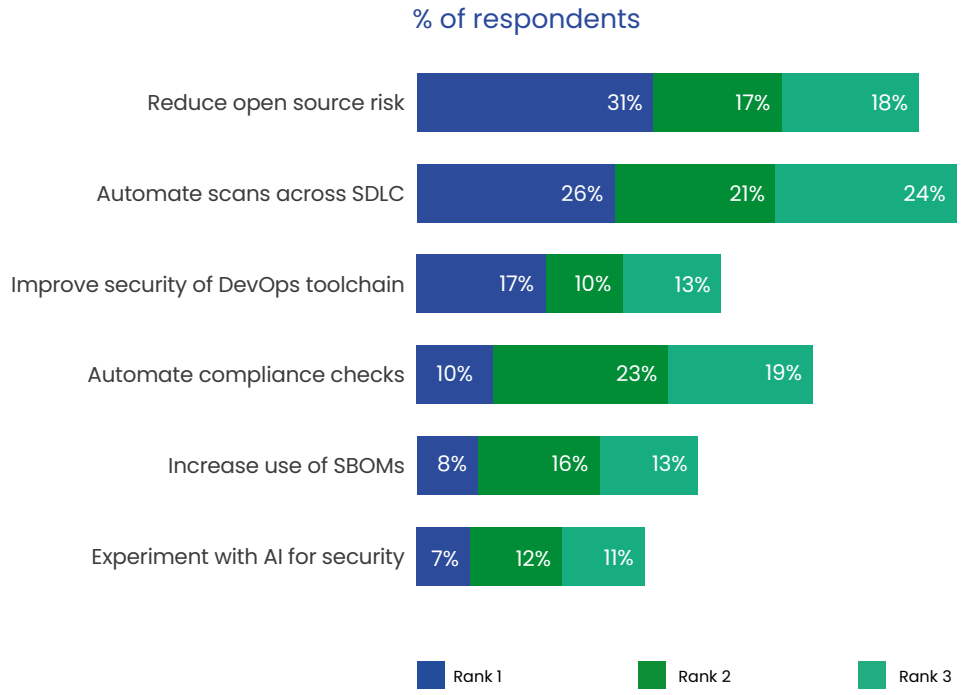
N = 101

Open source risk and scanning are top priorities

We asked respondents to rank their focus areas in software supply chain security. ***Reduce open source risk*** was ranked as the first priority by 31% of respondents, followed by ***automate scans across the SDLC*** (26%) and ***improve security of the DevOps toolchain*** (17%).

When combining the top three priorities, ***automate scans across the SDLC*** (71%) and ***reduce open source risk*** (66%) were joined by ***automate compliance checks*** (52%) as a primary area of focus.

Top Areas of Software Supply Chain Focus



Anchore 2024 Software Supply Chain Security Report

N = 106

Compliance is a significant driver in supply chain security

Industry, government, and organizational compliance requirements are a significant driver of supply chain security initiatives. When asked about the motivation behind their software supply chain focus, many respondents named compliance as an important factor.

[Software supply chain security is important because of the] overall security landscape but also to meet NIST SSDF/CISA mandated requirements.

[Software supply chain security is important because of] compliance like PCI, HIPAA, etc., and most importantly to reduce security incidents.

Our organization provides trusted applications to US Government entities and the private industry. As a result, we must ensure that we have a solid understanding of securing the supply chain for our customers and in order to ensure the data we store is secure.

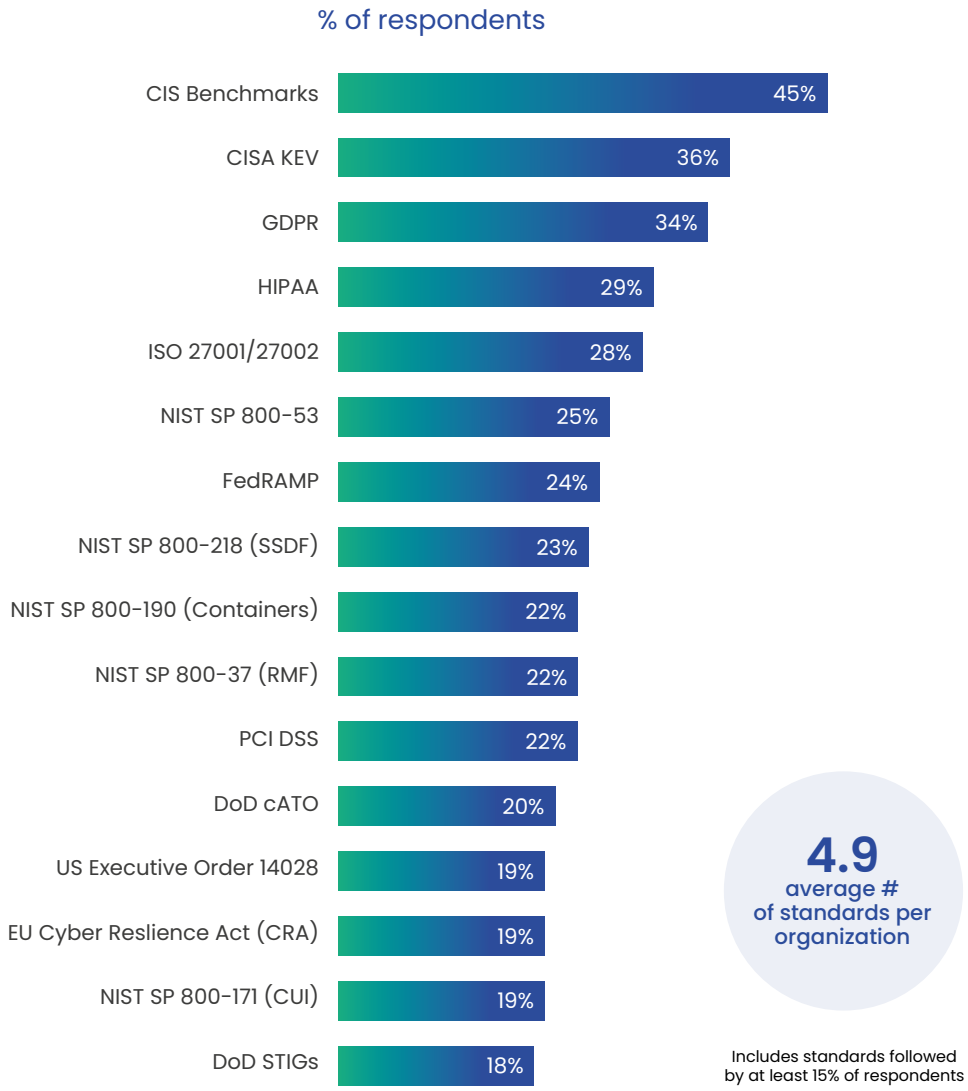
Federal agencies are requiring things like SBOMs and CMMC compliance and we believe the "Sec" in DevSecOps should be given equal weight to development and operations in the SDLC.

We are required to secure our software supply chain for customer compliance, but also best practice.

Organizations comply with multiple standards

Respondents reported the need to comply with an average of almost five separate standards per organization. New requirements from the US government are impacting many organizations, with 36% focusing on compliance with the CISA Directive of Known Exploited Vulnerabilities and 23% following the Secure Software Development Framework (SSDF), which organizations supplying software must now attest to via the Secure Software Development Attestation Form. While there were fewer respondents from the EU, the EU Cyber Resilience Act was cited by 19% since it also impacts non-EU companies selling into EU countries.

Compliance Standards Followed for Software Apps



4.9
average # of standards per organization

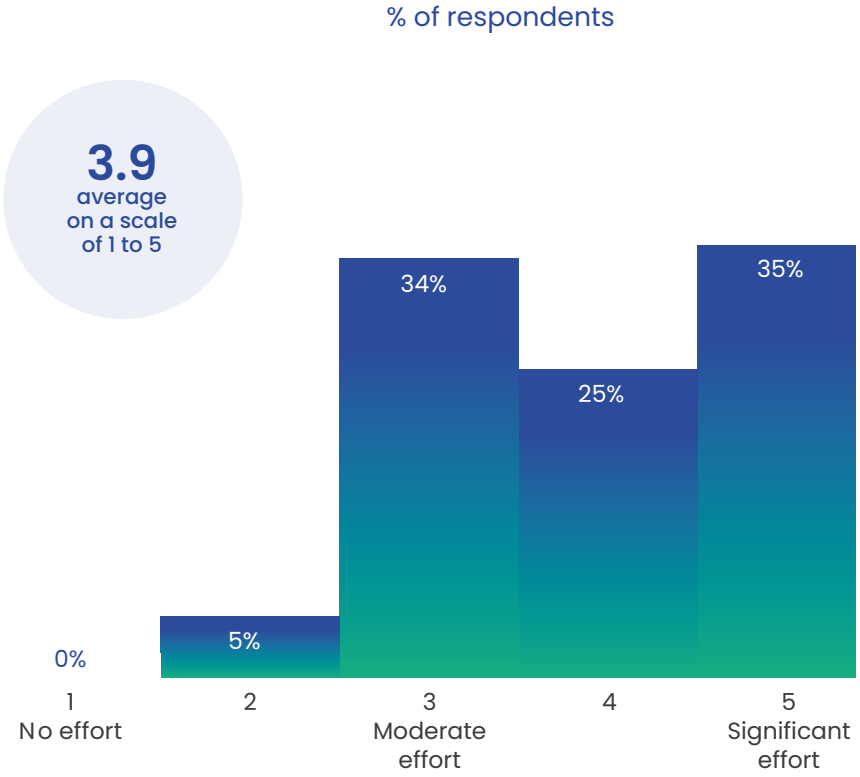
Includes standards followed by at least 15% of respondents

N = 96

Compliance requires significant investment and effort

When asked to rate the level of resources and effort invested in meeting compliance requirements on a scale of one to five (from no effort to significant effort), 35% of respondents rated the effort as a five, while 60% rated it as a four or higher. The average ranking was 3.9.

Effort on Software Supply Chain Compliance



Anchore 2024 Software Supply Chain Security Report

N = 100

Lack of visibility into dependencies drives growth in SBOM adoption

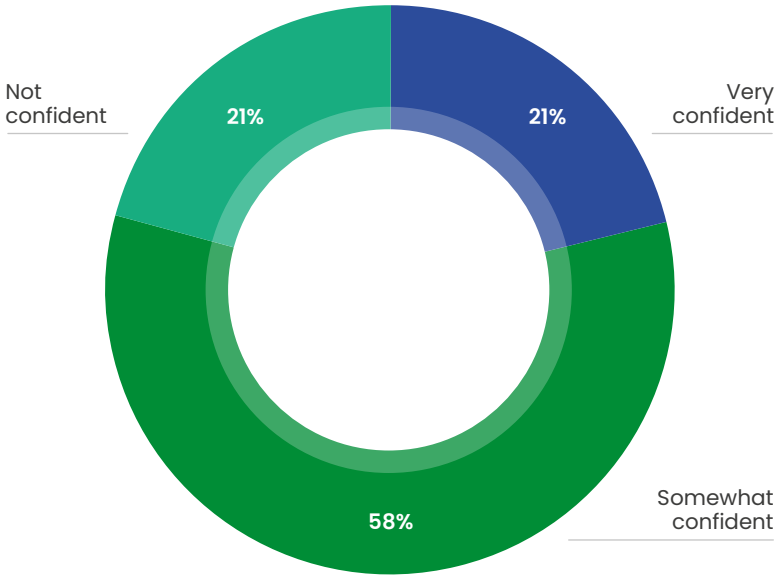
SBOMs are an important foundation for identifying vulnerabilities and securing the software supply chain. As a result, organizations are increasingly adopting SBOMs, but many have not yet fully adopted SBOM best practices.

Organizations are not confident in their visibility of dependencies

Only a minority (20%) of respondents are very confident that they have complete visibility into all the dependencies of the applications their organization builds. A similar proportion (21%) is not confident. Most respondents (58%) lie in the gray area, only somewhat satisfied that they understand their entire bill of materials.

Confidence in Visibility into All Dependencies

% of respondents



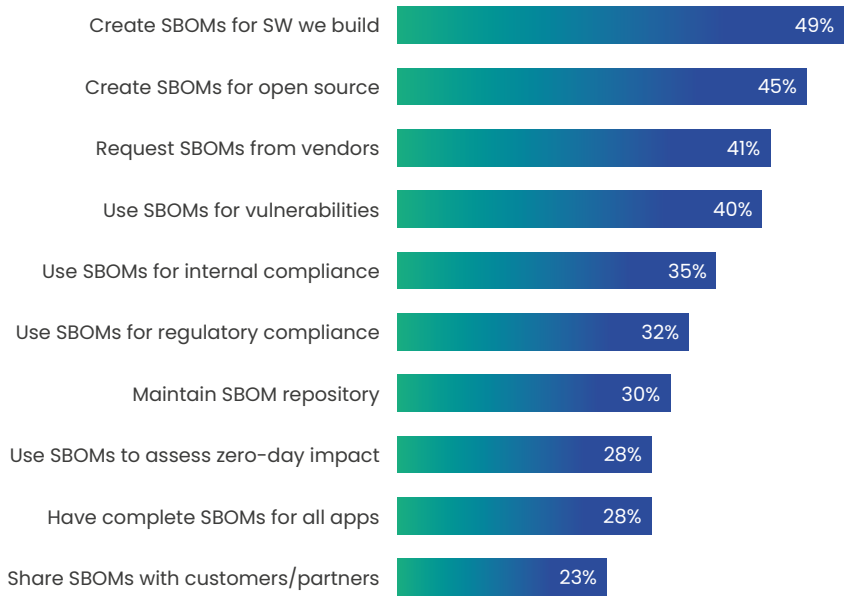
Anchore 2024 Software Supply Chain Security Report

N = 101

Less than half follow SBOM best practices

Despite the foundational role of SBOMs in providing visibility into the software supply chain, less than half of organizations follow SBOM best practices. Respondents are most likely to ***create SBOMs for the software we build*** (49%), ***create SBOMs for open source*** (45%), and ***request SBOMs from vendors*** (41%). However, only 28% of respondents ***have a complete SBOM for all apps***.

Current SBOM Practices



Anchore 2024 Software Supply Chain Security Report

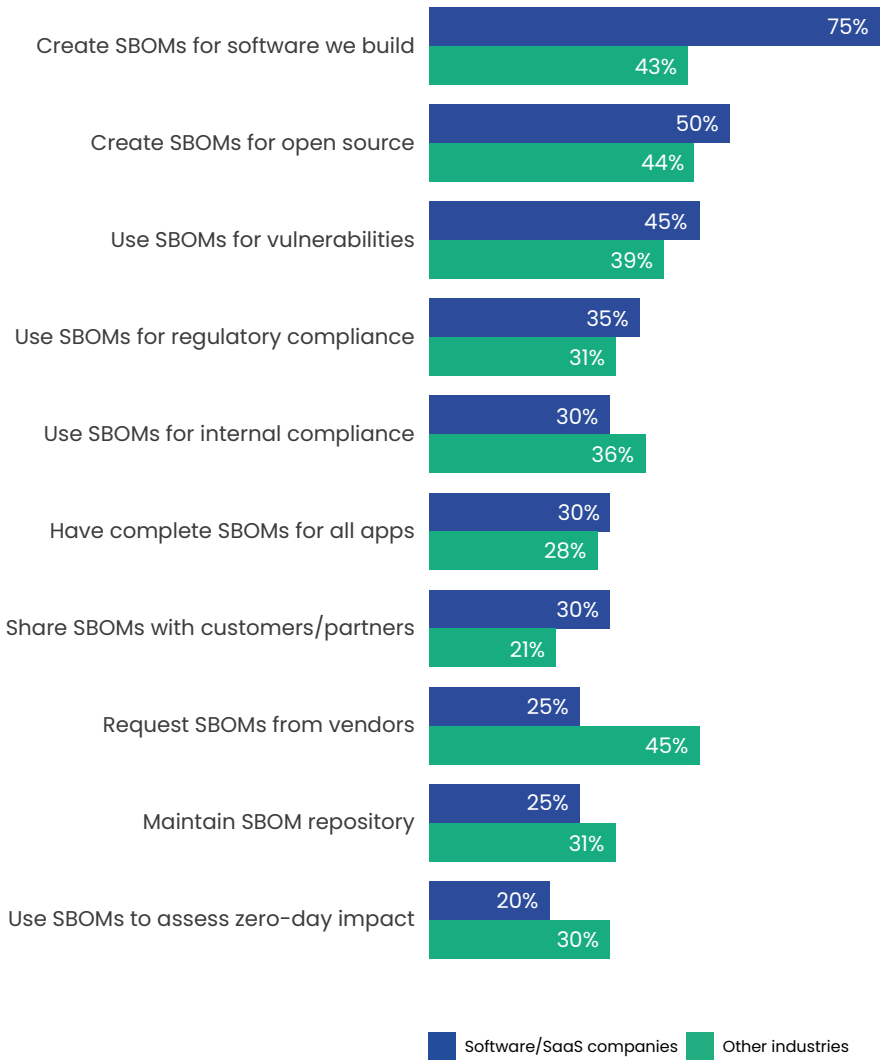
N = 100

SBOM best practices vary by industry

An organization's SBOM practices are closely aligned to whether or not they are a software vendor. Among software and SaaS companies, 75% create software for the software they produce, compared to 43% of companies in other sectors. Conversely, only 25% of software vendors request SBOMs from their vendors compared to 45% in other industries.

Current SBOM Practices

% of respondents



Anchore 2024 Software Supply Chain Security Report

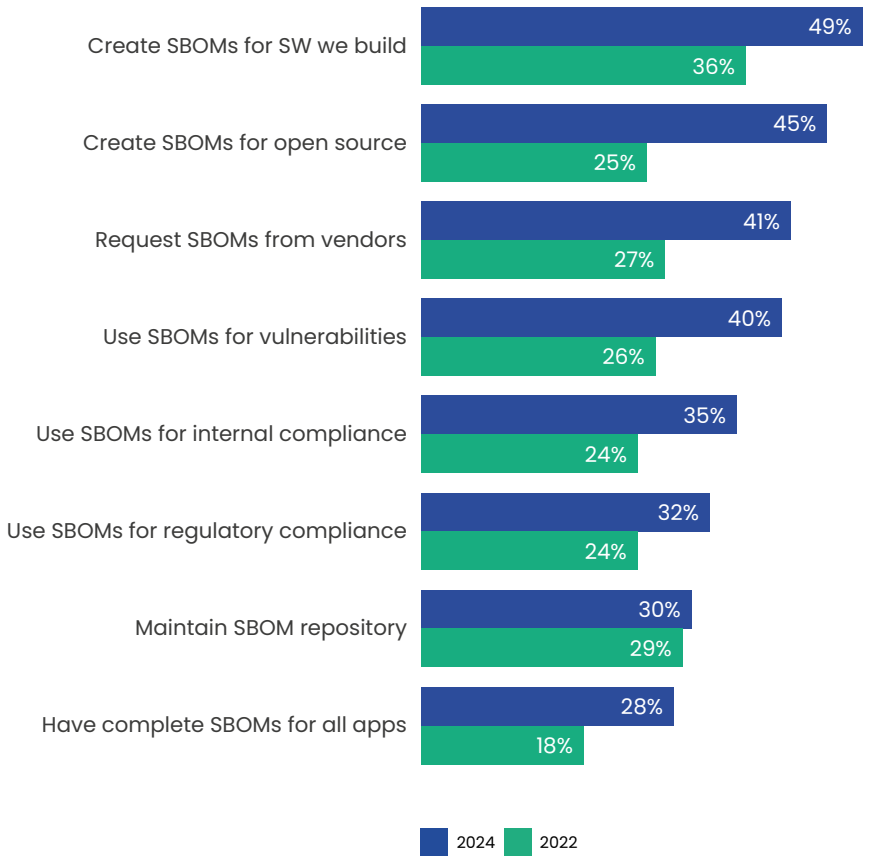
N = 100

Adoption of SBOM best practices is growing

While there is room for improvement, the adoption of SBOM best practices has increased significantly since our 2022 report, when fewer than a third were following best practices. The most significant gains were respondents who ***create SBOMs for open source*** (45% vs. 25% in 2022), ***request SBOMs from vendors*** (41% vs. 27% in 2022), and ***use SBOMs for vulnerabilities*** (40% vs. 26% in 2022)

SBOM Practices 2024 vs. 2022

% of respondents



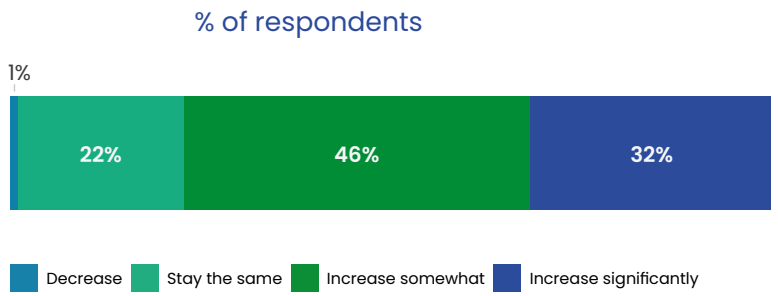
Anchore 2024 Software Supply Chain Security Report

N = 100

SBOM adoption will accelerate

While SBOM adoption has grown significantly over the past two years, respondents indicate that SBOM use will continue to expand over the coming 18 months. More than three-quarters (78%) of respondents indicate they plan to increase their SBOM usage in the next 18 months, with 32% planning a significant increase.

Planned Change in SBOM Use in Next 18 Months



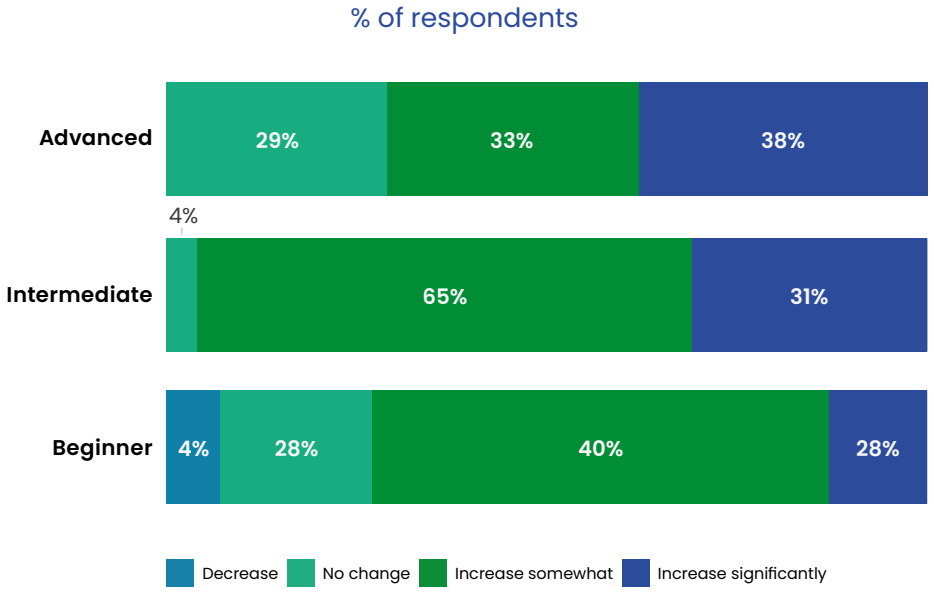
Anchore 2024 Software Supply Chain Security Report

N = 90

Organizations of all maturity levels plan to increase SBOM use

Regardless of their container maturity level, most organizations plan to increase their use of SBOMs. Advanced organizations already have a higher level of SBOM adoption, so there is less room for growth. The highest growth is in those with intermediate container maturity, with 96% planning to increase SBOM use.

Planned Change in SBOM Use by Container Maturity



Anchore 2024 Software Supply Chain Security Report

N = 90

Software supply chain security is a shared responsibility requiring collaboration

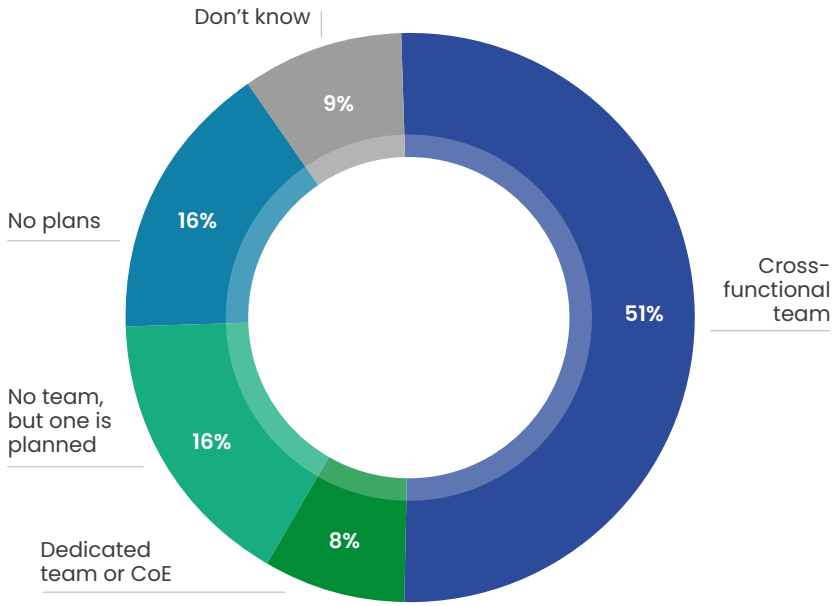
Many teams across the organization contribute to effective software supply chain security. As a result, organizations must increase collaboration and define roles and responsibilities.

Organizations facilitate collaboration for software supply chain security

Security, Development, DevOps, IT, and Compliance teams all have a role to play in software supply chain security. Organizations are taking different approaches to facilitate cross-team collaboration. The most common approach is a cross-functional team (51%), while a few respondents have a dedicated team or Center of Excellence (8%). An additional 16% plan to create a team, while 25% have no plans or don't know.

Collaboration Approach for Software Supply Chain Security

% of respondents



Anchore 2024 Software Supply Chain Security Report

N = 94

Supply chain roles and responsibilities are emerging

While the role of each team in software supply chain security varies by company, divisions of responsibility are starting to emerge.

DevOps and Security teams are the most active in supply chain security efforts.

DevOps and Platform Engineering are involved in almost every aspect of software supply chain security. They take the lead in securing the toolchain (47%) and addressing vulnerabilities in staging and production (40%). They are also heavily involved in SBOMs, including generating SBOMs (42%), managing SBOMs (33%), and sharing SBOMs with customers (30%).

Security teams generally shoulder the responsibility of vetting the security of components (41%) and prioritizing security ssues (41%).

Development teams have the primary responsibility for addressing vulnerabilities during the development phase (32%).

Compliance teams are tasked with ensuring compliance with standards (40%), with the support of other functions.

Software Supply Chain Security Responsibilities

% of respondents

	Security	DevOps/ Platform Eng	Development	I&O	Compliance
Vet security of components	41%	28%	15%	9%	7%
Prioritize security issues	41%	19%	20%	12%	9%
Secure the DevOps toolchain	23%	47%	12%	11%	8%
Generate SBOMs	25%	42%	25%	4%	5%
Find security issues in staging/prod	21%	40%	22%	14%	3%
Manage SBOMs	28%	33%	17%	12%	9%
Share SBOMs with customers	20%	30%	13%	10%	27%
Finding security issues in dev	21%	29%	32%	13%	6%
Ensure compliance	24%	20%	11%	6%	40%

Anchore 2024 Software Supply Chain Security Report

N = 94

Vulnerability Exploitability eXchange is garnering interest

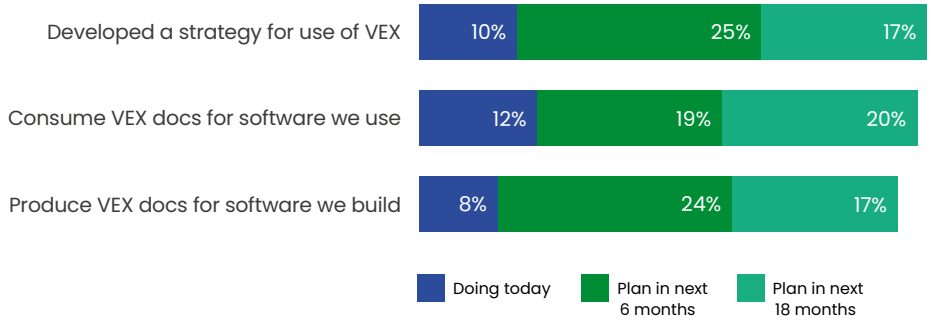
The Vulnerability Exploitability eXchange (VEX) is a standardized way to communicate whether specific vulnerabilities actually affect a particular product or software component. It adds context that helps users to understand which vulnerabilities pose a real threat.

VEX adoption is slated to grow significantly

Currently, VEX is in the early adopter stage. Only 10% of respondents currently have a strategy for using VEX docs, while 12% consume VEX docs and 8% produce them. However, interest in VEX is high. One-quarter of respondents expect to adopt VEX in the next six months, and another 15 to 20% plan to adopt it within 18 months.

Adoption of VEX

% of respondents



Anchore 2024 Software Supply Chain Security Report

N = 101

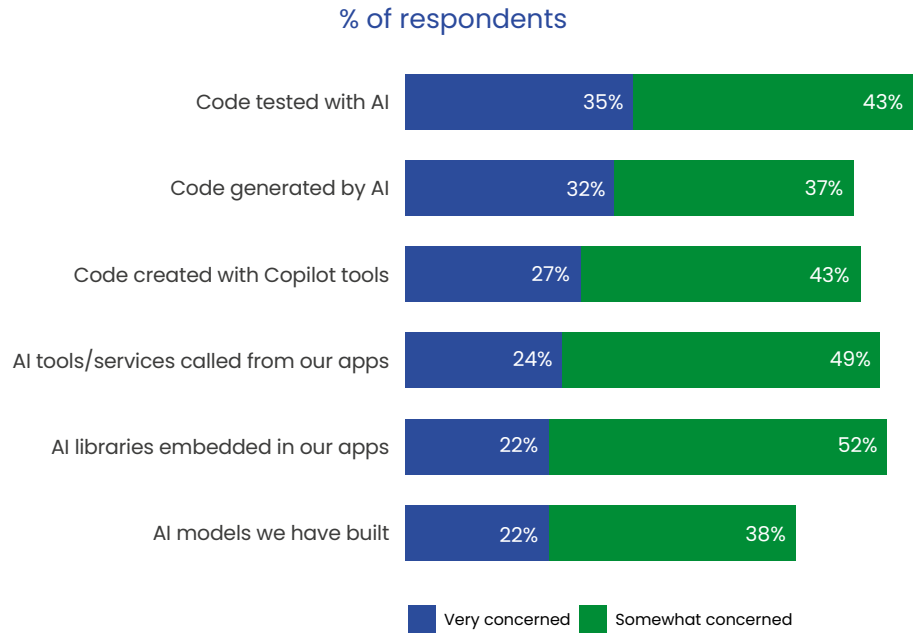
AI raises opportunities and concerns for software supply chain security

A large majority of respondents are concerned about AI's impact on software supply chain security, and as many as a third are very concerned.

A majority of respondents are concerned about AI

The highest concerns are with code tested with AI (35%) and code generated with AI (32%) or with Copilot tools (27%). Respondents are less worried about AI models built by the company (22%) or libraries embedded in their products (22%).

Level of Concern about AI Impact on Software Supply Chain Security



Anchore 2024 Software Supply Chain Security Report

N = 94

Action Plan

As the effect of software supply chain attacks intensify, organizations must implement supply chain security best practices to minimize risk, avoid reputational damage, and protect downstream users and customers.

Software supply chain security must become a new practice for every organization that uses or builds software. SBOMs are now a critical foundation of this new practice, providing visibility into the dependencies and risks of the software you use.

Here are seven steps to take your software supply chain security to the next level:

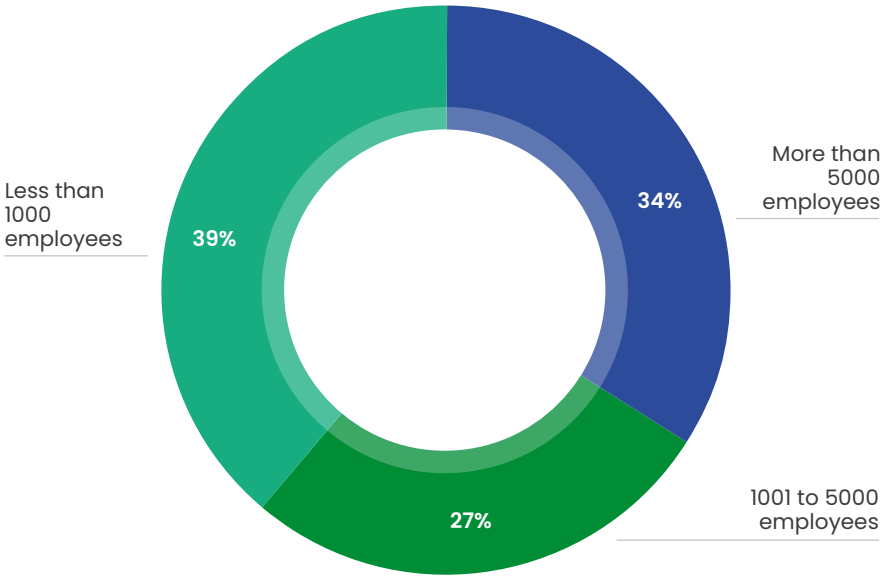
1. Assess your software supply chain maturity against best practices.
2. Identify key challenges and create a plan to make tangible improvements over the coming months.
3. Develop a methodology to document and assess the impact of supply chain attacks on your organization, along with improvements to be made.
4. Create a plan to generate, manage, and share SBOMs as a key pillar of your supply chain security initiative. Learn more with the Expert Guide on SBOMs in Cybersecuity and 6 Ways to Prevent SBOM sprawl.
5. Delve into existing and emerging compliance requirements and create a plan to automate compliance checks. Learn how to meet compliance standards like NIST, SSDF, and FedRAMP.
6. Identify gaps in tooling and create plans to address the gaps. Try open source tools like Syft for SBOM generation and Grype for vulnerability scanning as a good way to get started.
7. Create an organizational structure and define responsibilities to address software supply chain security and risk.

Respondent Demographics

Respondents were qualified based on ther involvement in some aspect of software supply chain security. Overall there were 106 respondents, however some respondents did not answer all questions.

Organization Size

% of respondents

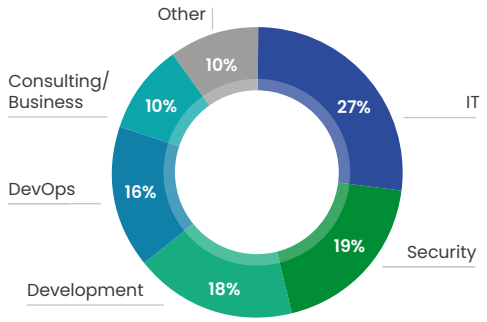


Anchore 2024 Software Supply Chain Security Report

N = 106

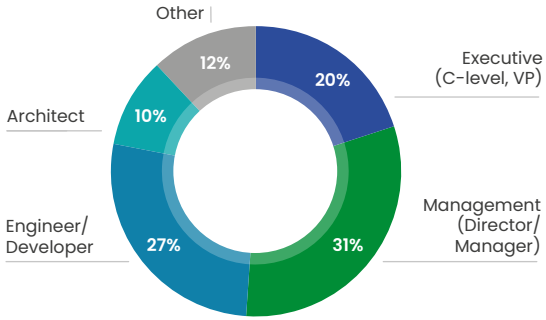
Function

% of respondents



Level

% of respondents

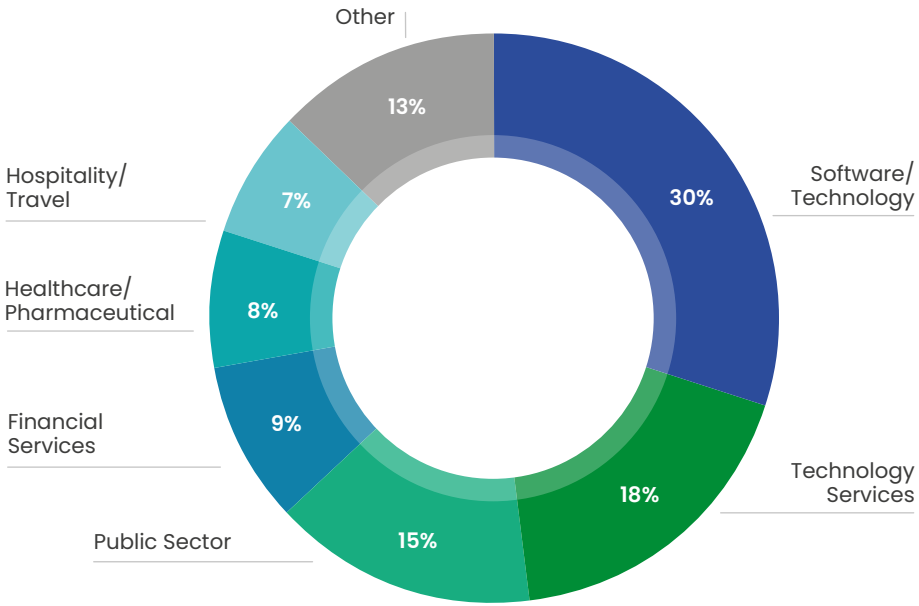


Anchore 2024 Software Supply Chain Security Report

N = 106

Industry

% of respondents

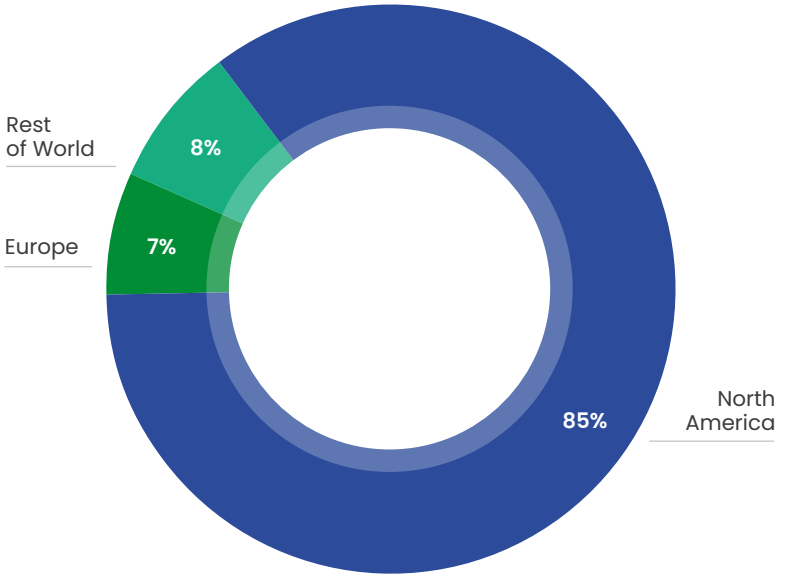


Anchore 2024 Software Supply Chain Security Report

N = 106

Region

% of respondents

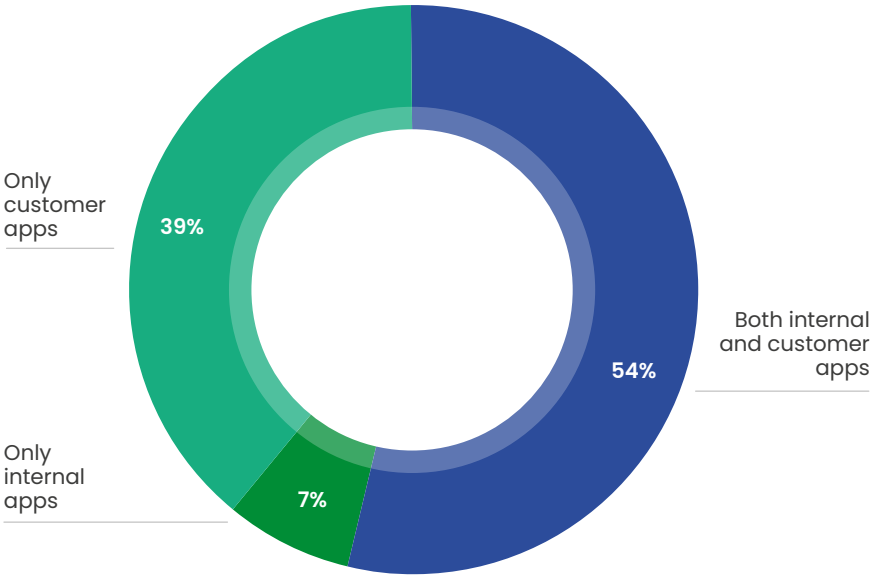


Anchore 2024 Software Supply Chain Security Report

N = 106

Types of Software Apps Developed

% of respondents

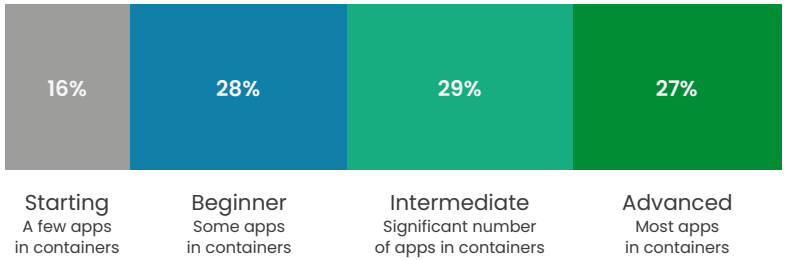


Anchore 2024 Software Supply Chain Security Report

N = 106

Container Adoption Maturity

% of respondents



Anchore 2024 Software Supply Chain Security Report

N = 106

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 to generate a comprehensive software bill of materials, continuously scan for vulnerabilities, secrets and malware and automate compliance enforcement. 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

sales@anchore.com

anchore.com