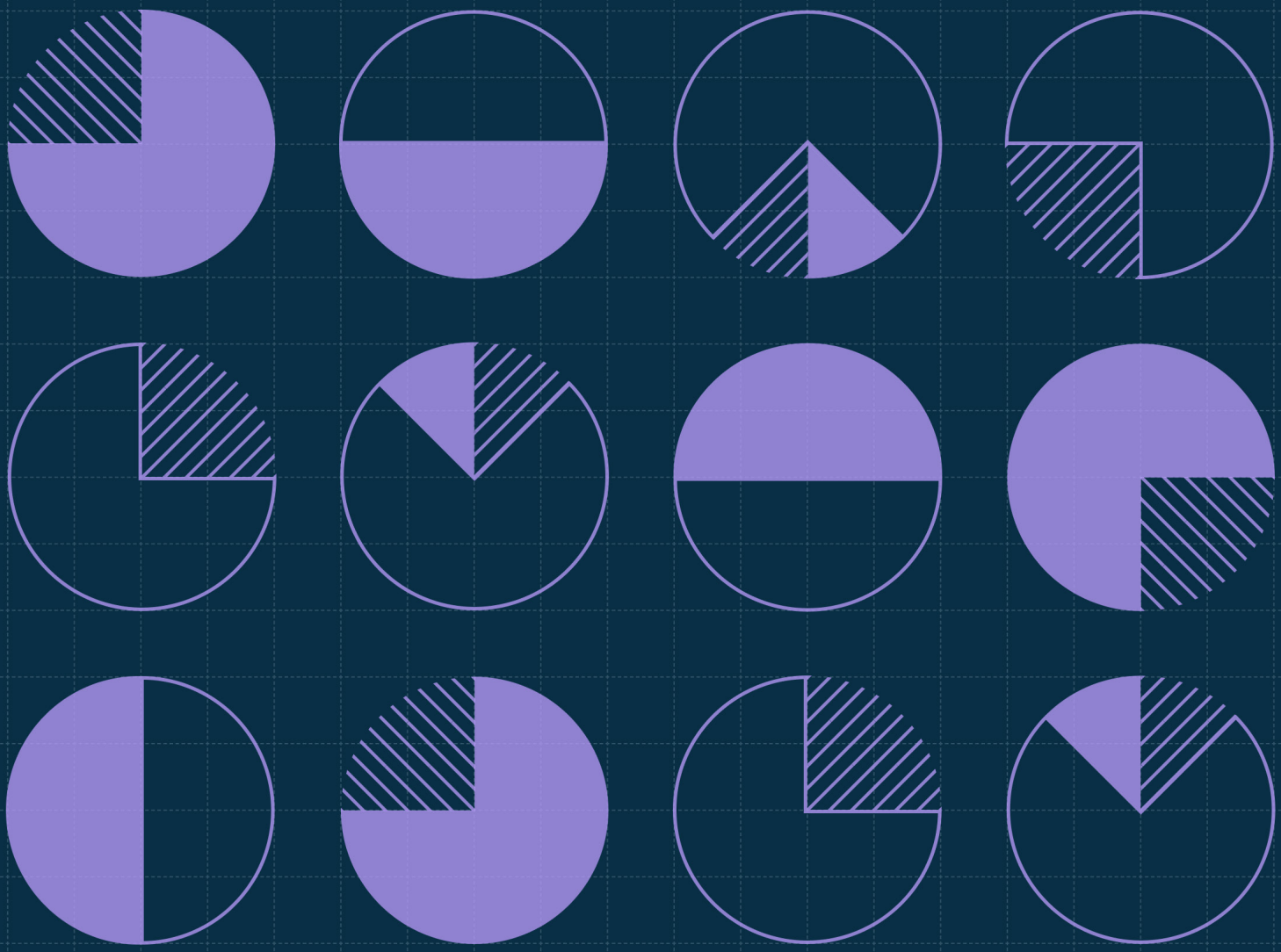
cloudsmith

Artifact Management Report 2025



Contents

03 Key Trends

04 Executive Summary by Glenn Weinstein

06 Security is a leading priority for 2025

10 Deciding on an artifact management tool is a team effort

12 Performance and latency is the biggest cause of frustration

13 Secure Delivery and Developer Habits

15 AI is now writing code at scale – but who's checking it?

17 That's a wrap

18 Methodology

Key trends

01

Security and supply chain integrity take center stage

With increasing threats to software supply chains, **56% of respondents cited improved security** as the leading benefit of artifact management tools.

02

AI and automation: a double-edged innovation

Respondents foresee **GenAI-powered automation will both streamline pipelines and challenge existing infrastructure** due to unpredictable behaviors and dependency issues.

03

Scalability and multi-cloud readiness are now mandatory

As development teams grow and adopt multi-cloud environments, **49% of respondents identified scalability as a critical benefit of artifact management tools.**

04

Compliance and regulatory pressures intensify

With tightening global standards, **48% of respondents rank regulatory compliance concerns among their top selection factors.**

05

Cost, complexity, and migration challenges drive frustration

Cost-effectiveness (60%) and integration with DevOps pipelines (55%) are paramount in selecting artifact tools.

06

Half of codebases are now AI-generated

42% of developers who use AI say at least half of their codebase is now AI-generated. Crucially, only 67% review AI-generated code before every deployment.

Executive summary by Glenn Weinstein

The Cloudsmith 2025 Artifact Management Report arrives at a pivotal moment for software development and DevOps teams worldwide. With escalating software supply chain threats and the meteoric adoption of GenAI-powered coding practices, organizations are being forced to rethink how they manage, secure, and scale their software artifact infrastructure.

Our survey results highlight a fast-evolving security landscape, where the majority of respondents cite improved security as the primary benefit of artifact management tools. Cloud-native development has accelerated innovation, as well as, the complexity and vulnerability of software supply chains. DevOps teams are tasked with delivering software faster, and doing so safely in the face of growing regulatory pressures.

Regulatory compliance is now a front-line concern. Frameworks like SLSA and new laws such as the EU Cyber Resilience Act (CRA), DORA, and NIS2 have highlighted the need to prioritize auditability and traceability, with just under half of respondents ranking compliance as a top selection factor for their artifact management tooling.

AI automation tools like Github's Copilot and Anysphere's Cursor coding assistant promise to improve software development with streamlined efficiency. This creates new challenges for security leaders by potentially introducing unforeseen behaviors and dependency risks, reshaping the very foundation of what we can trust in our software pipelines.

The report also surfaces operational pain points. Scalability and performance issues, flagged by nearly a quarter of respondents, are compounded by the increase of multi-cloud and globally distributed teams. Half of the respondents recognize scalability as a core benefit of modern artifact management solutions.

This year's findings reveal a software development ecosystem under pressure, where teams are balancing security, compliance, performance, and cost amid relentless change. The pace of innovation is outstripping the capabilities of legacy artifact management tools. The dynamic nature of modern developer environments demands solutions that are secure and scalable, but also agile enough to adapt to what's next.

With escalating software supply chain threats and the meteoric adoption of GenAI-powered coding practices, organizations are being forced to rethink how they manage, secure and scale their software artifact infrastructure.

Glenn Weinstein
CEO, Cloudsmith

01

Security is a leading priority for 2025

56%

of respondents cited improved security as the leading benefit of artifact management tools

In 2025, enterprise-grade artifact management solutions must go beyond traditional storage and retrieval capabilities. Whether you're building for cloud-native environments, on-premise servers, edge devices, or bare metal, modern software delivery pipelines face growing complexities – and with it, a rising wave of sophisticated supply chain attacks targeting development pipelines. To mitigate these threats, artifact management platforms need to provide advanced policy-as-code capabilities that automate security checks, enforce compliance, and ensure consistent governance across environments. These automated policies allow for real-time vulnerability scanning and mitigation, enabling teams to detect and respond to threats with greater speed and precision without disrupting developer productivity.

The urgency for such advanced security features is underscored by recent industry trends. In our 2025 user survey, over half of respondents (171 out of 307) cited improved security (particularly centralized vulnerability scanning, access control, and supply chain protection) as the leading benefit of their existing artifact management solution.

Most commonly cited benefits of current artifact management solutions

% RESPONDENTS

Centralized storage
Efficiently store and manage all artifacts in a single, organized repository.
53%

Improved security
Centralized vunerability scanning, access control, and protection against software supply chain attacks.
56%

Enhanced observability
Full visibility into artifact usage, dependencies, and software supply chain components.
36%

Scalability
Reliable management of artifacts as teams and projects grow.
49%

Cost efficiency
Reduction in storage, infrastructure, and operational overhead
52%

Improved collaboration
Easier sharing and reuse of artifacts across teams.
43%

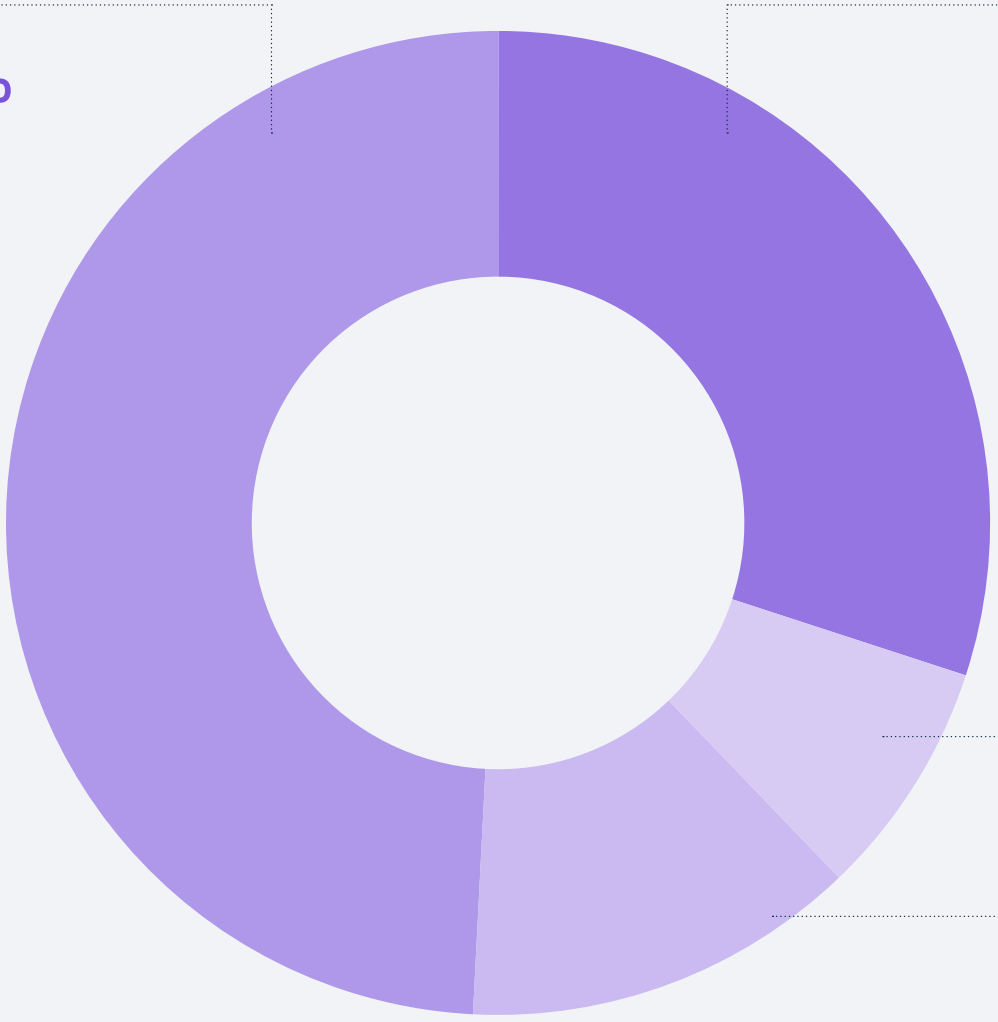
Version control
Reliable tracking and rollback of artifact versions.
44%

The rise of LLM-based AI technologies has amplified these concerns. While LLMs boost productivity by generating code quickly, they can inadvertently introduce risks by recommending non-existent or malicious packages. When asked if AI will exacerbate open-source malware threats (e.g. typosquatting, dependency confusion), **79.2% believe AI would increase the amount of malware in environments, with 30% saying it will significantly increase malware exposure.**

These new development behaviours increase the already significant software supply chain attack surface and puts developers at risk if artifact integrity is not strictly verified.

To address these emerging threats, modern artifact management solutions must embed intelligent access controls and offer end-to-end visibility into artifact provenance. With dynamic access control policies, organizations can ensure only authorized users and processes can interact with sensitive assets, reducing the likelihood of unauthorized changes or malware insertion. Coupled with robust policy-as-code frameworks, enterprises can establish and enforce security protocols that adapt as threats evolve, especially in environments where AI-generated code is becoming commonplace.

DO YOU BELIEVE AI WILL EXACERBATE OPEN-SOURCE MALWARE THREATS?



PagerDuty

"[Cloudsmith worked] directly with our security folks, not only saying, 'Yes, we have this' or 'No, we don't have this', but saying 'We will build this for you in order to make this work for PagerDuty'. It was a big deal because one of the big things we were looking for was engagement with our vendor – like a partner more than just someone that you pay money to and they give you a service – because with our previous vendor, that was a big struggle."

Dave Bresci
Senior Manager of Site Reliability Engineering
PagerDuty

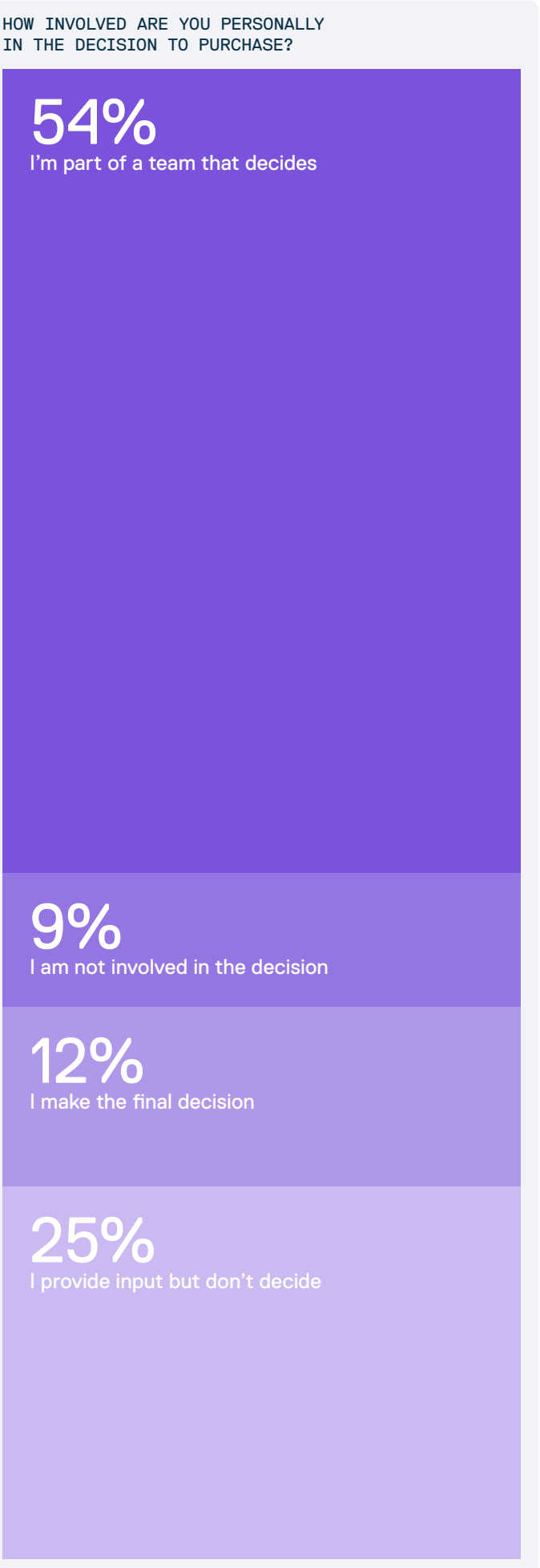
Deciding on an artifact management tool is a team effort

A significant **54% of respondents indicated that they are part of a broader team involved in the decision-making process for adopting an artifact management solution.** This suggests that the choice of such tooling is rarely made in isolation. Rather than relying on a single decision-maker, most organizations are opting for a more collaborative approach, where input is gathered from various stakeholders to ensure that the selected solution aligns with organizational needs and technical requirements.

In contrast, only **12% of respondents reported having sole authority to make the final decision regarding artifact management tooling.** While this suggests that sole ownership of such decisions is relatively rare among respondents, it does not necessarily reflect how decisions are structured across organizations as a whole. In large enterprises, it's possible that decision-making is centralized but falls to someone outside the surveyed group. Nevertheless, the data hints at a broader pattern: many organizations appear to involve multiple stakeholders when selecting foundational tools for their software delivery pipelines — reflecting the growing concerns around security, scalability, compliance, and developer experience.

These findings gesture toward a broader trend in enterprise software delivery: the centralization of core tooling decisions, particularly for systems as foundational as artifact management. While our data doesn't directly measure how decisions are consolidated across teams, the relatively low number of respondents with sole authority suggests that these choices are increasingly being made at the platform level — reflecting the influence of platform engineering efforts.

In this model, cross-functional collaboration among developers, DevOps, security, operations, and leadership ensures that selected tools meet organizational standards for scale, security, and reliability.



When polling survey responders about artifact management, we found there was significant variation in the job titles of those involved in the process. Ordered by most to least common response.

Software Engineer
Development Manager
Other
Engineering Manager
DevOps Lead
DevOps Engineer
Head of DevOps
CTO
Software Architect
Director of Engineering
Release Manager
Cloud Architect
Security Engineer
Platform Engineer
Automation Engineer
Build Engineer
Infrastructure Engineer
VP of Engineering
Developer Productivity Engineer
Site Reliability Engineer (SRE)

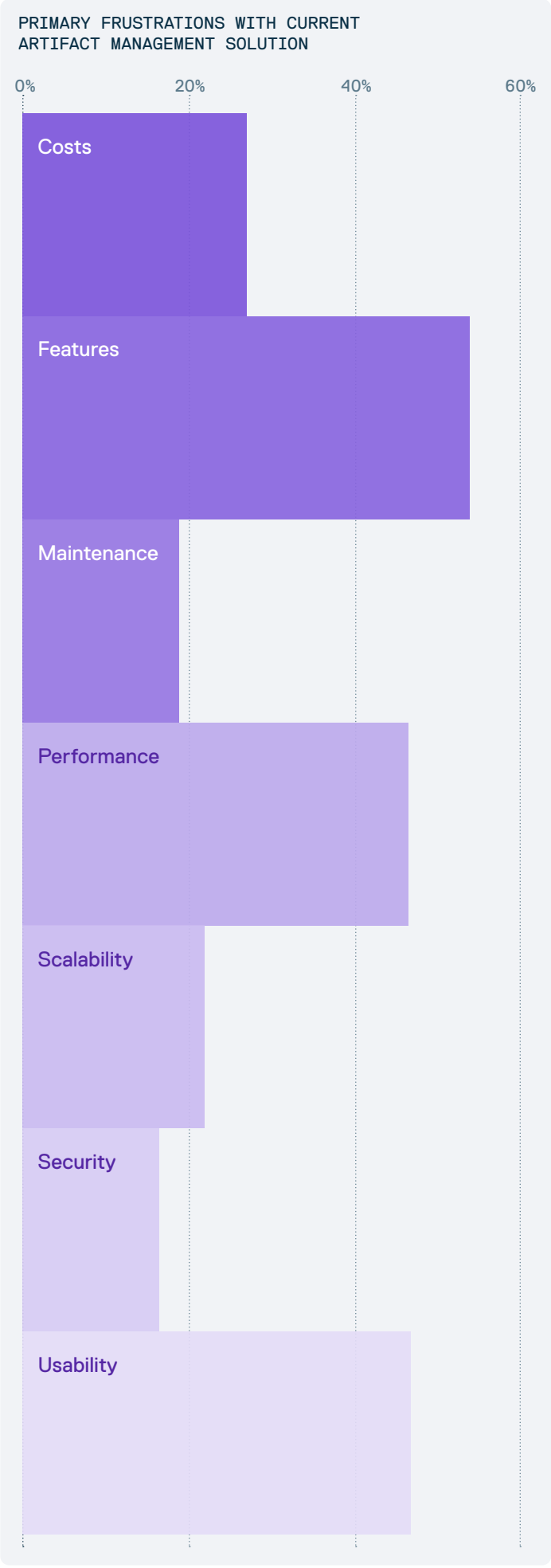
Performance and latency are leading causes of frustration

Performance and latency are the leading sources of frustration for DevOps professionals when it comes to artifact management. In our latest survey, 142 respondents identified **Performance**-related issues, such as slow artifact retrieval and sluggish CI/CD pipeline integration, as their primary bottleneck. Similarly, 143 participants raised concerns about **Usability,** signaling that user experience and intuitive interfaces are just as critical in the evolving toolchain landscape. Taken together, these insights highlight a broader dissatisfaction with the current generation of artifact management solutions.

When we examined the data more closely, a striking pattern emerged: **over 25% of all responses cited performance and latency** specifically as the key challenges they hope to address in 2025. These aren't abstract complaints. These concerns translate directly into slower delivery cycles, increased engineering toil, and ultimately, a drag on innovation. As software teams scale and shift towards more distributed, hybrid, and edge environments, the expectation for near-instant artifact availability is becoming non-negotiable. Legacy platforms, originally built for static and centralized workflows, are struggling to keep up.

It's also worth noting that **52% of respondents identified "scalability and reliable artifact management as teams and projects grow"** as a key benefit of Artifact Management — highlighting its critical importance in 2025.

This signals a critical inflection point for artifact management platforms. The next generation must be built with performance, usability, and global scale at their core, rather than an afterthought. Platforms that embrace a cloud-native, globally distributed architecture, are more uniquely positioned to lead this transition. Artifact management platforms in 2025 are providing capabilities far beyond simple storage. Businesses need to accelerate software velocity, while reducing friction in the developer experience, and simultaneously enable secure, seamless delivery pipelines at scale.

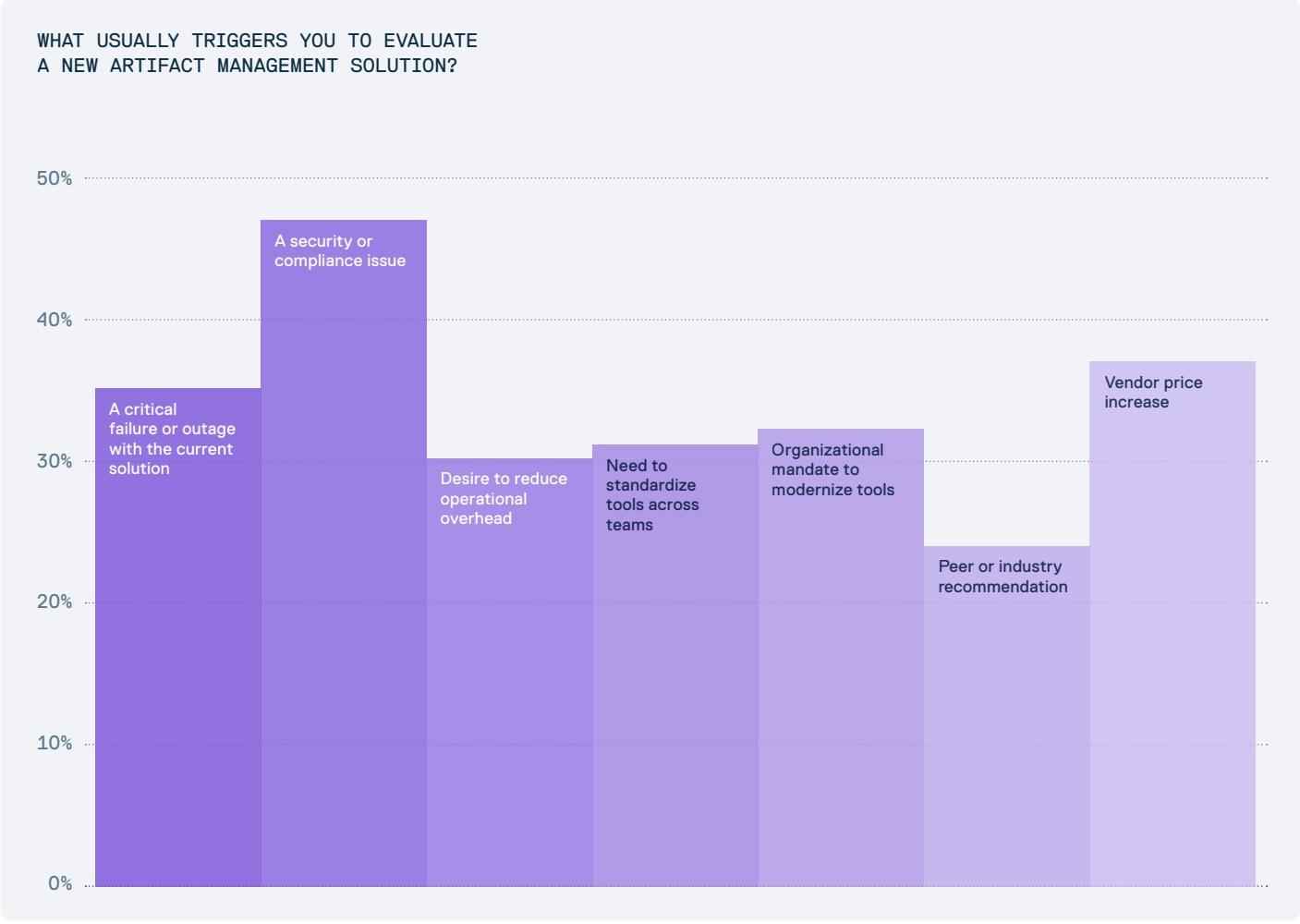


Secure delivery and developer habits

When asked what usually triggers you to evaluate a new artifact management solution, we received a wide-variety of interesting insights. Not surprisingly, security and compliance is the leading driver in this report. However, more surprisingly, **35% of feedback suggested that a critical failure or outage with the current solution has led to teams revising whether or not to stick with their current artifact management solution.**

When given the opportunity to explain what the issue or challenge was specifically, recurring challenges included:

- **System crashes and downtime leading to disrupted delivery cycles**
- **Rigid integrations and poor scalability during periods of high demand**
- **Complex permission models and unintuitive interfaces slowing teams down**
- **Ballooning storage costs from unmanaged artifacts and outdated binaries**
- **Inefficient collaboration caused by inconsistent version control across teams**
- **Vendor lock-in and migration barriers creating long-term risk and inertia**



Reasons for wanting to migrate away from current artifact management solution

Lack of consistency of use across multiple teams.

The product can be slow in particular with large repositories.

Version control between different teams, making it hard to merge.

Not being available to handle extreme loads during busy seasons.

Integration with our current structures and maintainability of the packages.

We've had different systems with different lifecycles and we had to retire some.

Price increases, vendor locking, and migrational complexities remain a challenge.

The biggest issues and challenges always arise from unplanned downtimes or crashes.

Overly complex implementation tends to slow us down which is frustrating in an agile environment.

Learning curve and complex permission management when dealing with large teams (Azure Artifacts).

Vendor solution was compromised and thus it created significant downtime and operational loss of business.

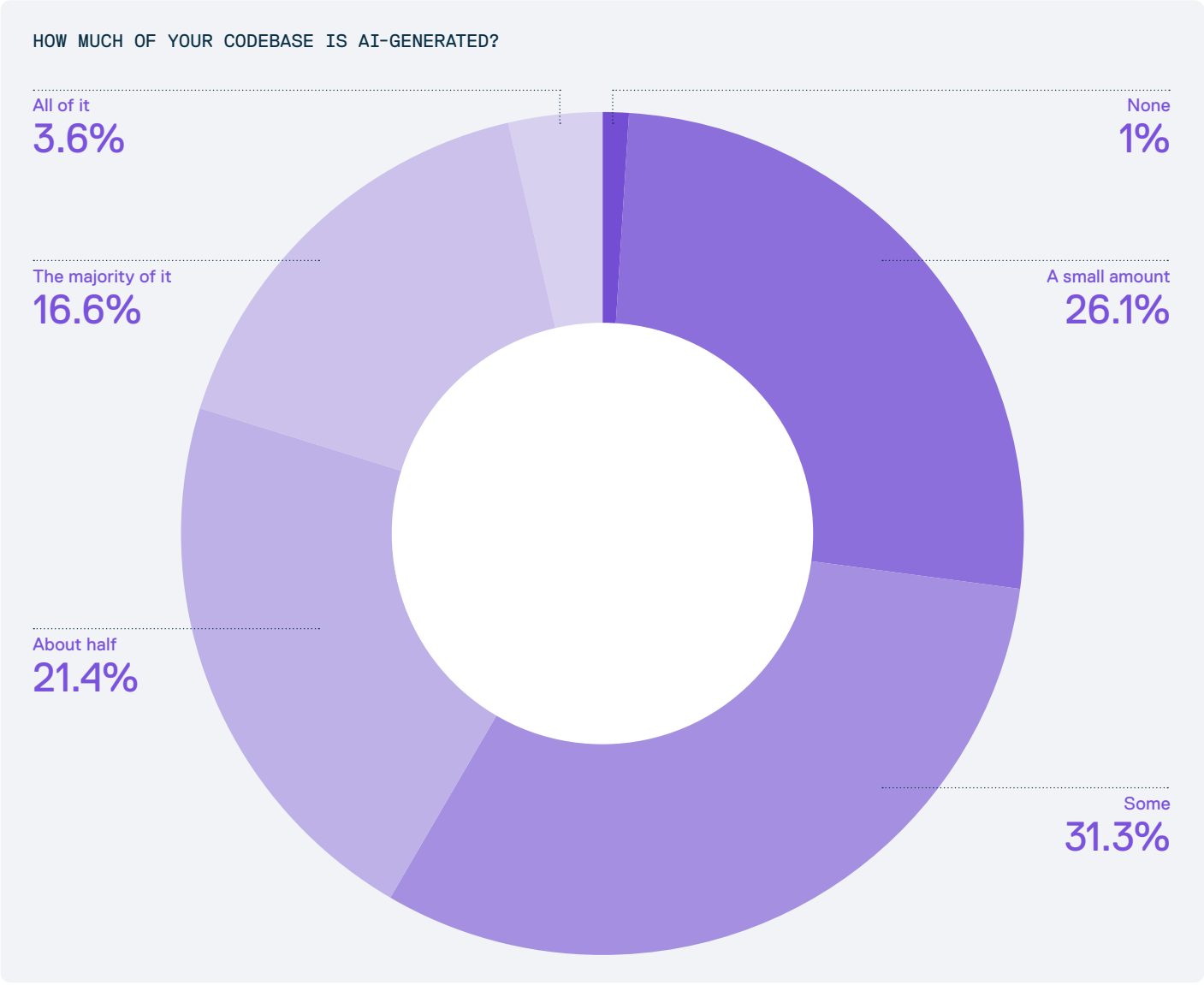
Complex UI makes it difficult to use it for inexperienced users. Some rules have to be imposed and controlled manually, a more flexible artifact management policy would help.

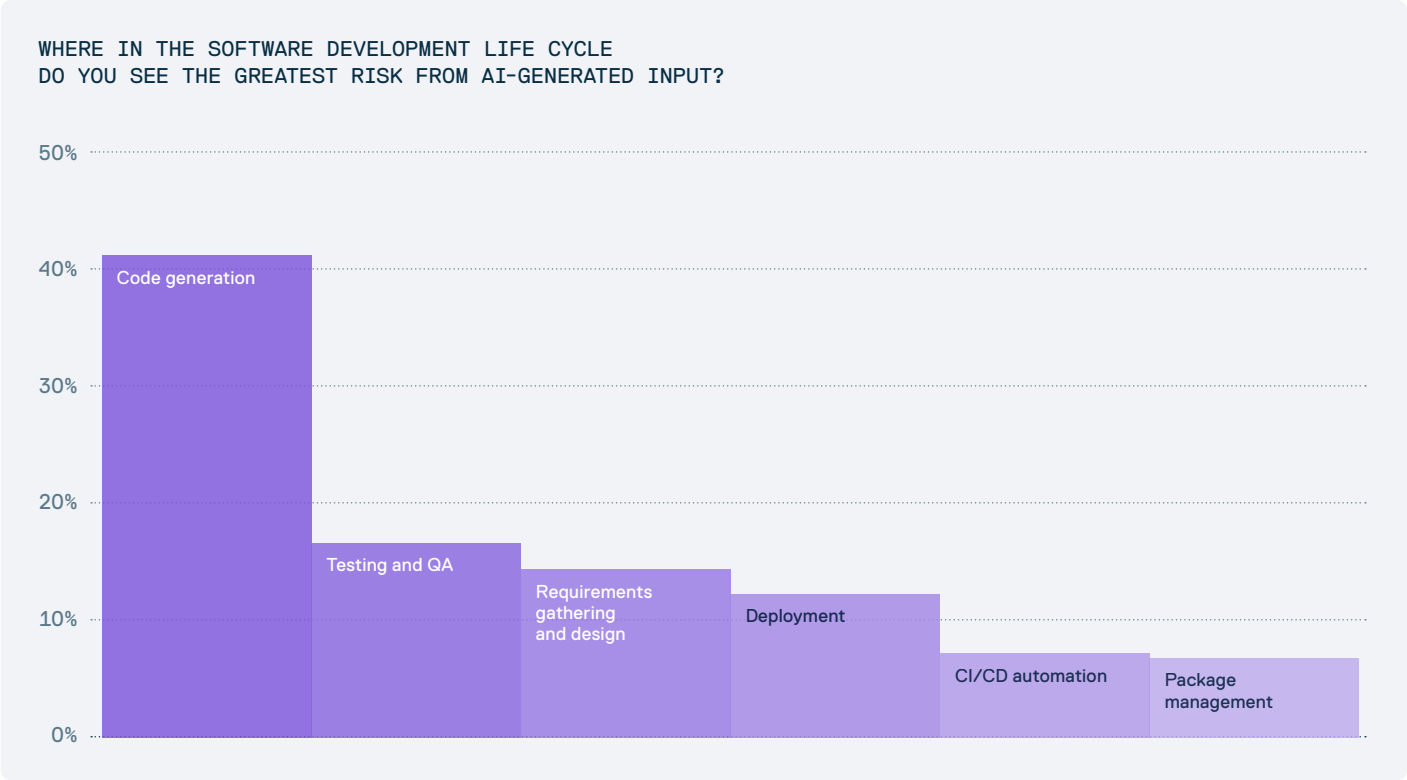
AI is now writing code at scale – but who's checking it?

The adoption of AI in software development is accelerating rapidly (not just in concept, but also in code). In our survey, **42% of developers using AI said that at least half of their codebase is now AI-generated.** This is no longer theoretical. We are a long way past that point. AI is now clearly shaping the heart of modern applications and the developers workflow.

While many view the rise of Generative AI (GenAI) as a positive shift, the reality is more complex.

Increasingly, adversaries are exploiting this trend – not by attacking traditional infrastructure, but by infiltrating the software ecosystem itself. Malicious actors are engaging in slopsquatting – creating deceptive, malicious software packages that are easily mistaken for legitimate ones. Developers, often under pressure and relying heavily on AI-assisted tooling, are inadvertently incorporating these packages into production code without proper vetting.





But while the speed and efficiency benefits are clear, the oversight is not. **Only 67% of those developers review AI-generated code before every deployment,** leaving large portions of production code potentially unvetted. This is quickly becoming a growing vulnerability in the software supply chain.

This behaviour, driven by a desire to move faster, is dramatically expanding the attack surface. AI isn't just introducing new code, it's also introducing new risks, often at scale. Traditional concerns like artifact integrity, dependency management, and SBOMs (Software Bill of Materials) are being compounded by AI's ability to rapidly consume and reuse unknown or untrusted code.

41% of respondents identified code generation as the riskiest point of AI influence, yet practices around review and trust remain inconsistent:

66% said they only trust AI-generated code after manual review.

Just 20% fully trust AI output without extra scrutiny.

59% apply additional reviews to AI-generated packages, but only 16% treat them like any other package, without further checks.

This uneven approach is happening against a backdrop of expanding AI usage: alarmingly, **86% of organizations have seen more AI-influenced dependencies in the last year,** with **40% seeing a significant increase.** Yet, only **29% of teams feel very confident in their ability to detect malicious code in open-source libraries,** which is the very ecosystem where AI tooling tends to source its suggestions. The threats, according to those surveyed, range from sensitive data leakage to the inclusion of compromised dependencies. These risks are amplified when developers blindly trust AI-generated code or package suggestions without security oversight.

These findings point to a critical inflection point. AI is becoming a core contributor to the software stack, but we haven't fully adapted our trust models, tooling, or policies to match this new reality. Relying on developers to manually spot every risk (especially under time pressure) is not sustainable.

What's needed is a secure checkpoint for AI-assisted development:

Automatically-enforced policies to catch unreviewed or untrusted AI-generated artifacts.

Artifact provenance tracking to distinguish between human-authored and AI-authored code.

Integration of trust signals directly into the development pipeline, so that reviews become automatic rather than optional.

That’s a wrap

The Cloudsmith 2025 Artifact Management and Usage Report emphasises a growing disconnect between the capabilities of legacy artifact management systems and the real-world needs of modern software teams. Feedback from users across engineering, operations, and leadership roles points to the common pain points: recurring downtime, sluggish performance under load, poor integration with existing toolchains, high operational costs and fragmented workflows.

These issues are not isolated. They reflect systemic limitations in how artifact management has been traditionally approached. And as organizations accelerate digital transformation and increasingly adopt AI-enabled development, the cost of these limitations grows.

The report makes it clear: artifact management is no longer solely an infrastructure problem. It is a cross-functional priority that spans software development, DevOps, security, architecture, and compliance. Teams are looking for platforms that are secure by design, natively integrate with cloud-first workflows, scale effortlessly, and offer visibility and control without friction.

This is a call to action for all artifact management vendors and stakeholders: it’s time to rethink the foundations. Solutions must evolve to meet the speed, scale, and security expectations of modern software delivery. They must support hybrid and remote teams, reduce operational complexity, and provide the observability needed to navigate emerging regulatory and AI-related risks.

In a cloud-native era defined by speed, scale, and automation, artifact management should no longer be the bottleneck — it should be driving resilience, trust, and improved pace of software delivery across the entire software supply chain.

Methodology

At Cloudsmith, we prioritize sharing accurate, data-driven insights. This report is based on real-world survey responses, reflecting genuine trends and challenges in software development and artifact management — rather than opinions or selectively filtered results. Our data spans a broad spectrum of industries and company sizes, from early-stage startups to large-scale enterprises. All findings are derived from anonymized responses collected through Cloudsmith-led research.

Participants

Total respondents: 307

For context, nearly 40% of respondents represent organizations with over 50 software engineers **(Fig. 01).** These larger teams are more likely to encounter complexities with artifact management systems — especially those involving multiple teams, diverse permission structures, and the need to scale both access controls and artifact distribution.

The participants in this usage report represented a diverse range of roles and responsibilities **(Fig. 02).** This cross-functional mix provided a well-rounded perspective on the requirements and pain points associated with current artifact management solutions.

When participants were asked which factors matter most in selecting an artifact management solution in 2025, responses often reflected an 'all of the above' mindset **(Fig. 03).** This reinforces the need for comprehensive, end-to-end platforms. However, the real insight lies in the specific pain points surfaced — particularly around securing packages, maintaining compliance, and ensuring high availability. These priorities highlight where current solutions are falling short and where future innovation must focus.

Notes

Percentages may not sum to exactly 100% due to rounding

All respondents who were selected for this survey use or interact with AI during their daily software development, DevOps, or CI/CD workflow. Those who do not use AI in any way were screened out. We have reflected this in the key findings section.

Fig. 01: Number of developers per company surveyed

NUMBER OF DEVELOPERS	TOTAL	PERCENTAGE
1–3	13	4%
4–9	37	12%
10–14	50	16%
15–24	41	13%
25–49	40	13%
50–99	44	14%
10–249	26	8%
250+	61	20%

Fig 02: Which of the following job titles most closely matches your role or area of responsibility

JOB TITLES OF RESPONDENTS	PERCENTAGE
Security	3%
Release	3%
Automation	2%
DevOps/Infrastructure	20%
Development	26%
Leadership	11%
Management	23%
Architecture	4%
Other	9%

Fig. 03: What factors are most important when selecting an artifact management tool?