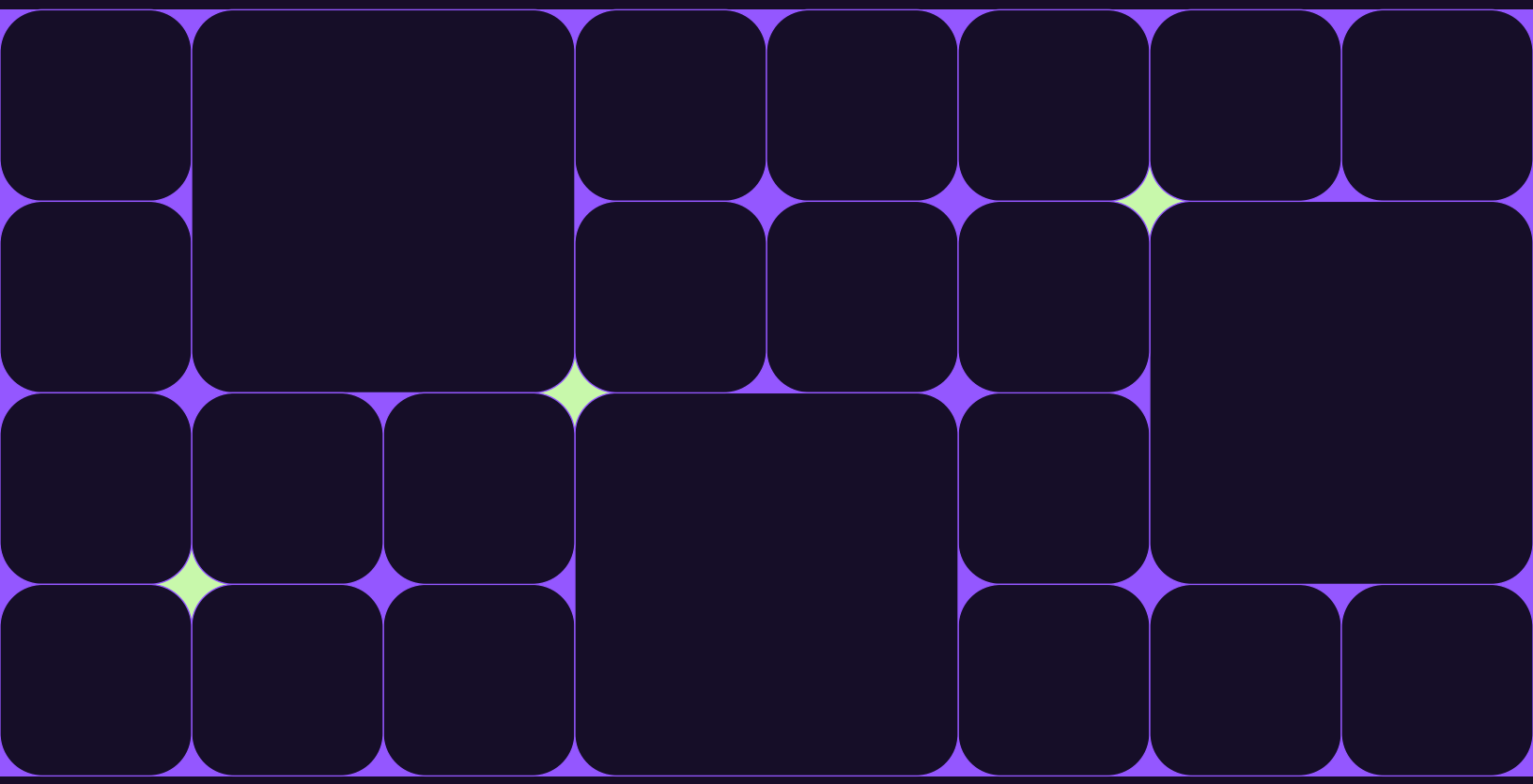
Survey Report

Use and Security of GenAI in Software Development



LEGIT

Introduction

Generative AI (GenAI) has quickly established itself as a transformative force in software development. From automating repetitive tasks to accelerating complex algorithm design, its impact is significant. However, as GenAI becomes more pervasive in development pipelines, security concerns are growing. Both developers and security teams are grappling with how to balance GenAI's innovations with the risks it introduces — risks that could expose the software supply chain to new vulnerabilities.

Legit Security conducted a comprehensive survey of security and development teams to assess the extent of AI use in software development, exactly how it's being used, and how security and development teams are thinking about GenAI security.

Survey Demographics

The survey, conducted by Regina Corso Consulting on behalf of Legit Security, gathered insights from over 400 security professionals and software developers across various industries in North America. Respondents were drawn from companies of all sizes, from small tech startups to large multinational organizations, all dealing with the integration of AI into their software development processes.

This survey aimed to capture the perspectives of both security and development teams to highlight differences in concern, visibility, and approaches to managing GenAI.

Executive Summary

This 2024 Legit Security survey reveals that generative AI has become a critical tool in software development.

According to the survey, 96% of security and software development professionals report that their companies use GenAI-based solutions for building or delivering applications. Among these respondents, 79% say that all or most of their development teams regularly use GenAI, signifying that AI is deeply embedded in the software development process.

Despite these high levels of adoption, there are still security concerns. 98% believe that security teams need a better handle on how GenAI-based solutions are being used in development. Furthermore, 94% feel that they need more effective ways to manage GenAI use in their company's research and development efforts.

Those in security and developers are actually of very similar minds when it comes to security and the use of GenAI for developing software. Overall, 80% say there are security concerns over relying too much on Gen AI solutions to develop software. However, there is a slight gap as developers are more likely than those in security to feel this way (85% vs. 75%).

Looking ahead, the consensus is clear: GenAI is the future of software development. In five years, 95% of respondents predict that software developers will be more reliant on GenAI, while only 5% expect reliance to remain the same, and none foresee reduced reliance.

96%

Of security and software development professionals report that their companies use GenAI-based solutions for building or delivering applications.

94%

Feel that they need more effective ways to manage GenAI use in their company's research and development efforts.

In the following sections, we will explore the findings in more detail.

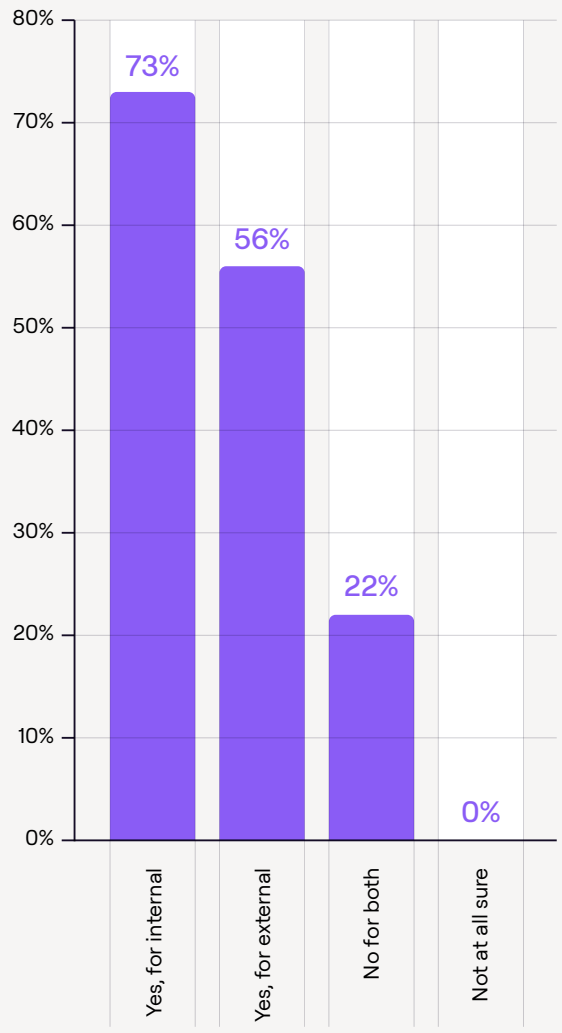
How Pervasive Is GenAI Use in Software Development?

Generative AI is now playing a pivotal role in automating tasks that once took developers hours, if not days, to complete manually. According to the survey, 96% of respondents report that their organizations are using GenAI tools regularly, particularly in areas such as code generation and optimization. AI-powered code assistants, such as GitHub Copilot and Tabnine, are the most widely adopted tools, with 88% of developers saying they use them within their development organization. This reflects a broad shift in how development teams are augmenting their capabilities with AI to meet tighter deadlines and more complex project demands.

Almost three-quarters of respondents (73%) say GenAI-based solutions are being used for building internal applications and over half (56%) say they are being used for building external applications. The research also finds that developers are slightly more likely to say they use GenAI-based solutions when building external applications.

The use of AI is making a significant difference for software development as almost all respondents say GenAI solutions are changing the way their developers build software. Over two-thirds strongly agreed with the statement "GenAI solutions are changing the way our developers build software," and 68% strongly agreed.

Do you use GenAI-based solutions when building internal or external applications?



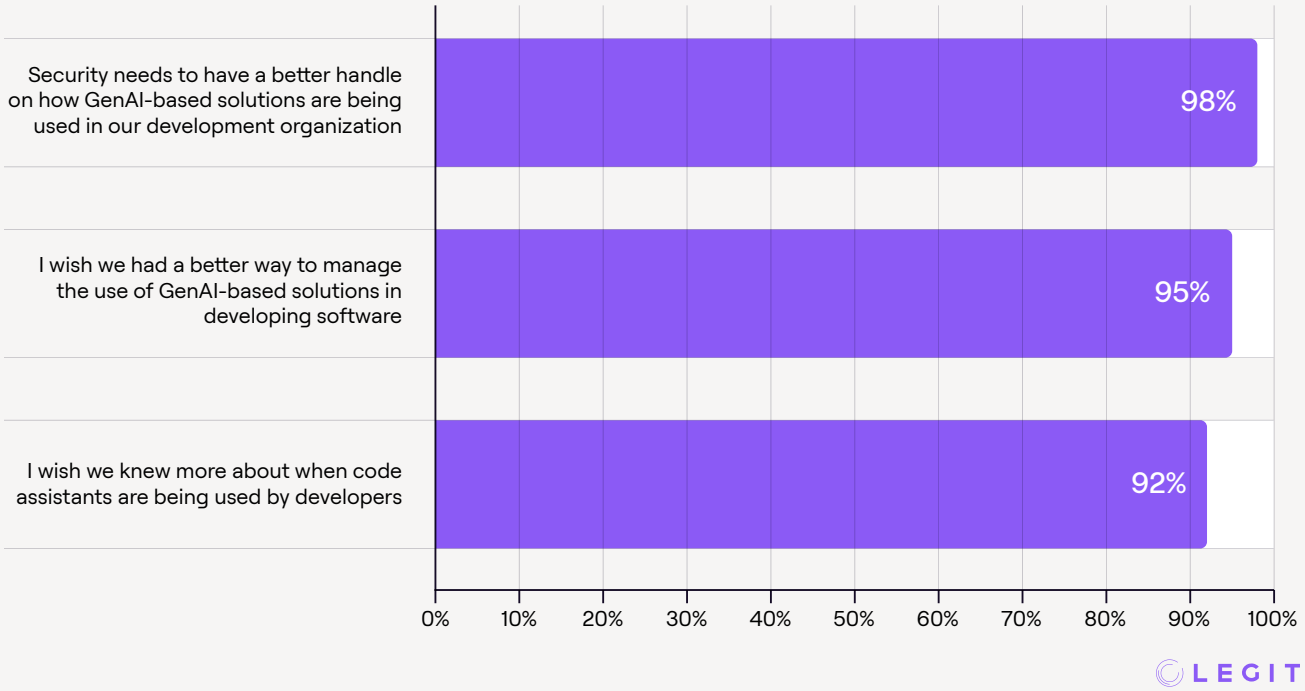
Do Security Teams Have the GenAI Insights They Need?

While the majority of respondents say they have full visibility into the use of GenAI in their development organizations, over nine in 10 (94%) also say they need a better way to manage GenAI usage in their company's R&D. "Our biggest concern is that our development team will become so reliant on the data, they may not check for its validity," said one respondent when asked about concerns.

A lack of validity can lead to security gaps, particularly when AI-generated code is integrated into mission-critical systems without proper vetting.

In addition, almost all security respondents (98%) report that security needs to have a better handle on how GenAI-based solutions are being used in their development organizations.

How strongly do you agree or disagree with the following statements?



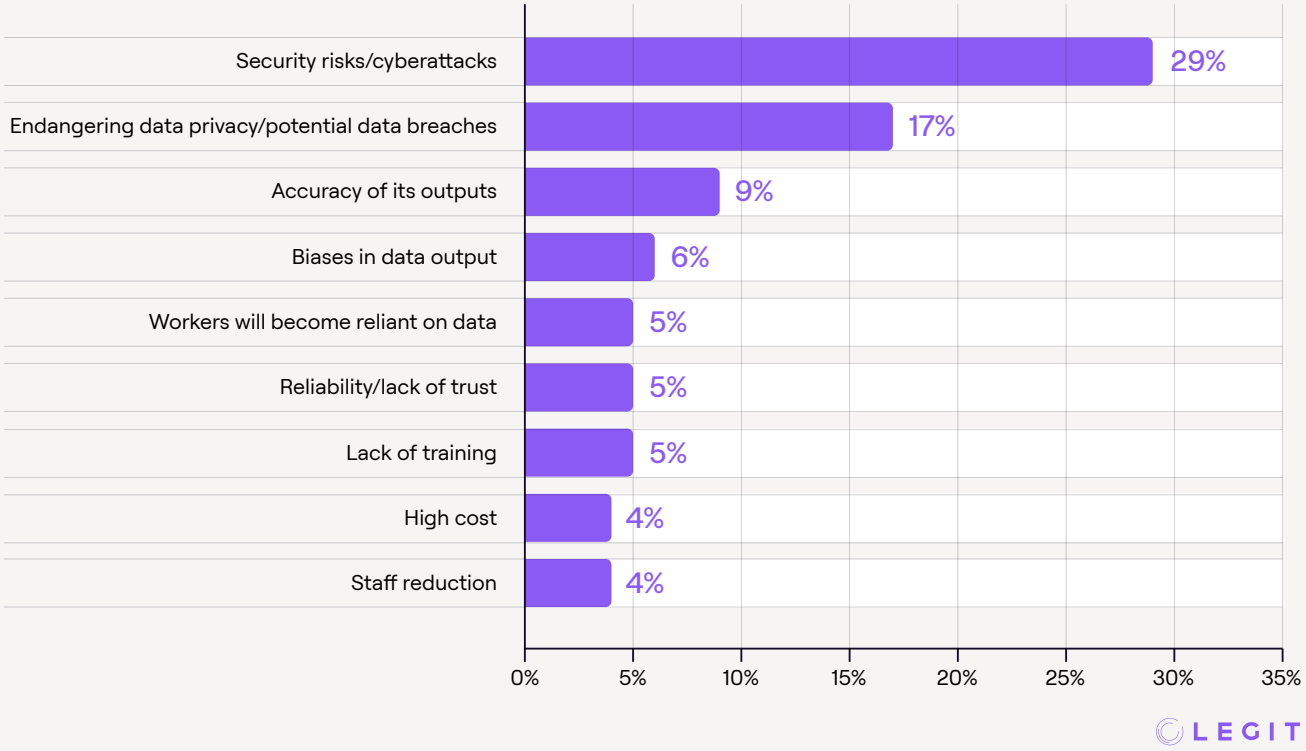
Are There Security Concerns About GenAI Use?

The findings from this survey reflect the complex security landscape surrounding the use of GenAI-based solutions. Security concerns are at the forefront, with over four in five developers and three-quarters of those in security saying there are security concerns over relying too much on GenAI solutions to develop software. Three in 10 respondents identified security risks and/or cyberattacks as the biggest concern when using GenAI.

"When it comes to using GenAI-based solutions in our organization, my biggest concern is hackers," one respondent noted.

They are right to be concerned — research is revealing that LLMs and AI models contain bugs and vulnerabilities that have the potential to cause AI supply chain attacks, like the vulnerabilities Legit recently uncovered in LLM automation tools and vector databases or the AI Jacking vulnerability Legit discovered last year.

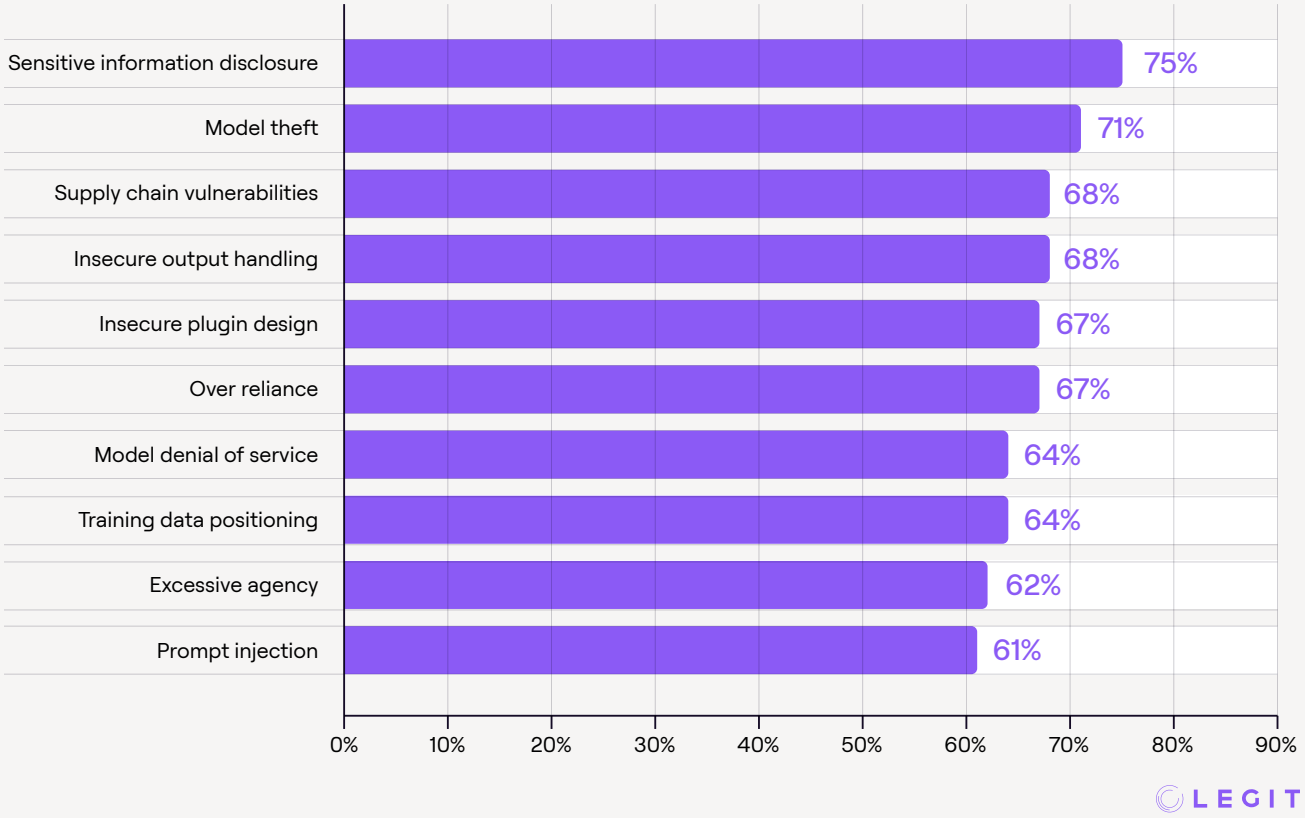
When it comes to using GenAI-based solutions in your development organizations, what are your biggest concerns?



Regarding specific risks, three-quarters (75%) of respondents view sensitive information disclosure as a critical risk for GenAI-based applications. Close behind, 71% are concerned about model theft, and over two-thirds (68%) point to supply chain vulnerabilities and insecure output handling.

Other risks include insecure plugin design and over-reliance on AI solutions, with 67% identifying these as potential threats. Additionally, over three in five respondents are wary of risks like model denial of service (64%), training data poisoning (64%), and excessive agency (62%), with prompt injection also a concern for 61%.

How much of a risk, if any, are each of these when it comes to GenAI-based apps?



Interestingly, developers are slightly more likely than those in security to say over reliance is a significant risk when it comes to GenAI-based apps, while those in security are a little more likely to say supply chain vulnerabilities are.

The findings underscore the need for organizations to prioritize the security and privacy of GenAI tools, ensuring that robust safeguards are in place to mitigate these diverse and evolving risks.

While all may be a risk, which two would you say are the most significant when it comes to Gen AI based apps?

	Security	Developers
Sensitive information disclosure	45%	43%
Model theft	24%	24%
Over reliance	18%	23%
Supply chain vulnerabilities	23%	17%
Insecure output handling	16%	18%
Model denial of service	17%	14%
Insecure plugin design	14%	17%
Excessive agency	16%	14%
Training data positioning	14%	14%
Prompt injection	12%	15%
None of these	1%	1%

LEGIT

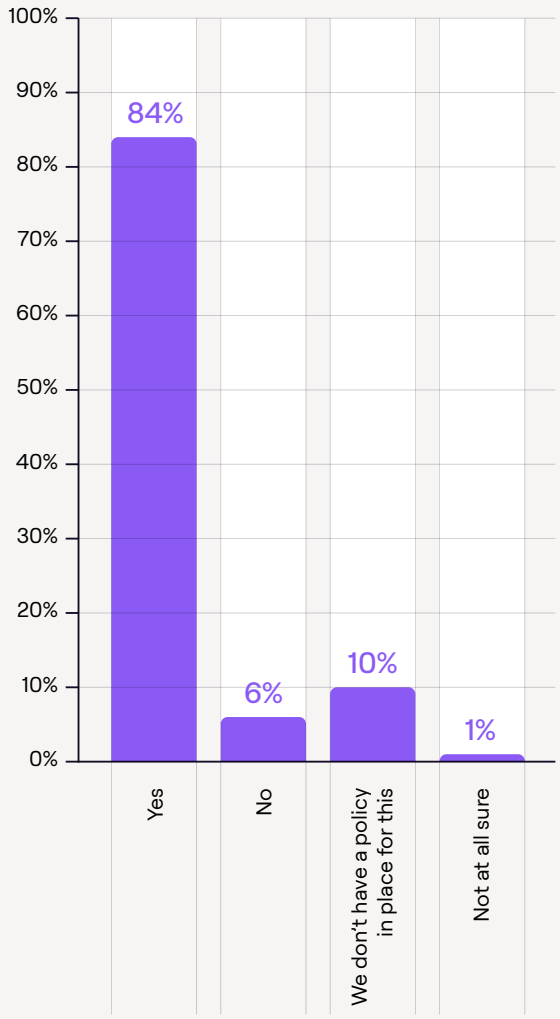
What GenAI Policies Are in Place Today?

The survey reveals that the majority of respondent organizations have policies in place governing the use of GenAI software. Nine in 10 (89%) report having a policy, with 76% stating that their policy is formal and written, while 13% indicate their policy is more informal or unofficial. However, 9% of respondents admit that their organization does not have any policy for using GenAI software at all.

Similarly, for GenAI code assistants, such as GitHub Copilot, 88% of respondents say they have a policy in place. Of these, 71% describe their policy as written and formal, while 17% follow more unofficial guidelines. Meanwhile, 11% of respondents report that no policy exists in their organization for the use of GenAI code assistants. These findings highlight that while most organizations have established some form of governance around GenAI, there is still a minority that lacks formal oversight, especially for code assistant usage.

Looking more specifically at code assistants, over four in five of those in IT (84%) say corporate policy allows for the use of code assistants within their development organization while less than one in ten (6%) say they do not and one in ten (10%) say they do not have a corporate policy in place for this.

Does corporate policy currently allow for the use of code assistants within your development organizations?



LEGIT

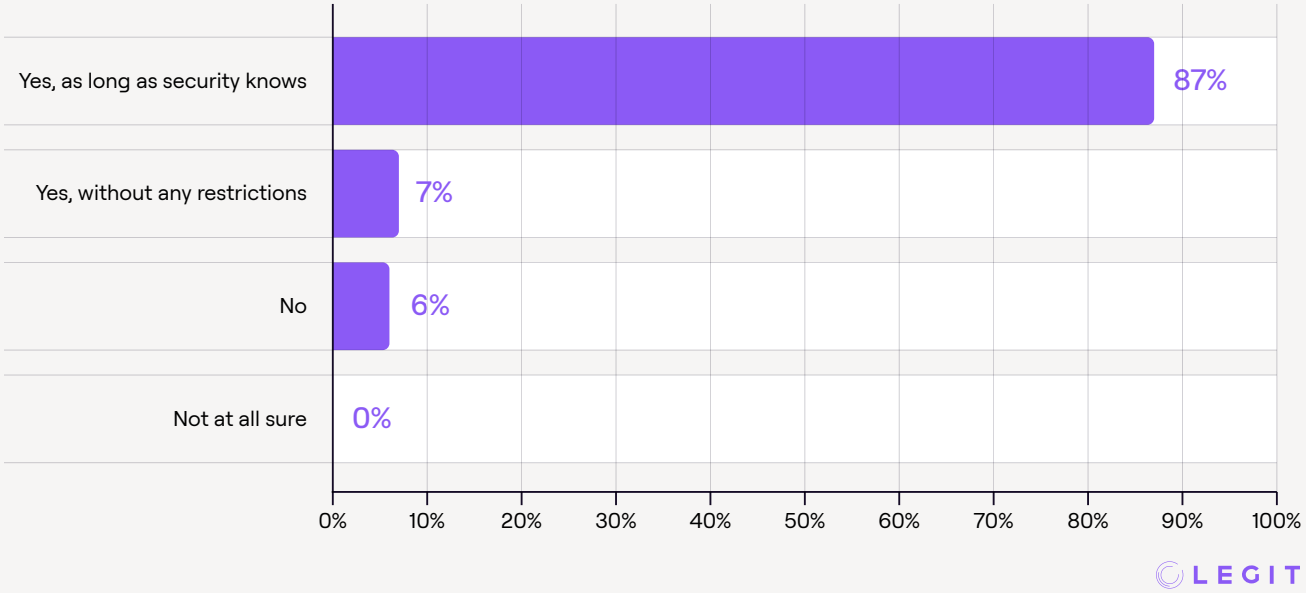
How Pervasive Are Code Assistants?

Nearly nine in 10 developers (88%) say they currently use code assistants in their development work, reflecting the high level of integration of these tools. Among security professionals, 87% say they allow the use of code assistants within the organization, provided that security teams are informed. A small portion, 7%, allow unrestricted use, and 6% prohibit their use altogether. However, despite allowing the use of code assistants, over nine in 10 (92%) security professionals express a desire to have more visibility into when developers are utilizing these tools.

On average, respondents estimate that 43% of their developers regularly use code assistants, with 40% of their overall software capabilities relying on GenAI technologies. Security professionals tend to estimate a higher rate of code assistant usage, with 47% believing that more of their developers regularly use these tools, compared to the 40% cited by developers themselves.

These findings reveal both the growing dependence on GenAI-powered code assistants within development organizations and the need for improved oversight, particularly from a security standpoint.

Do you currently allow the use of code assistants within the development organization?

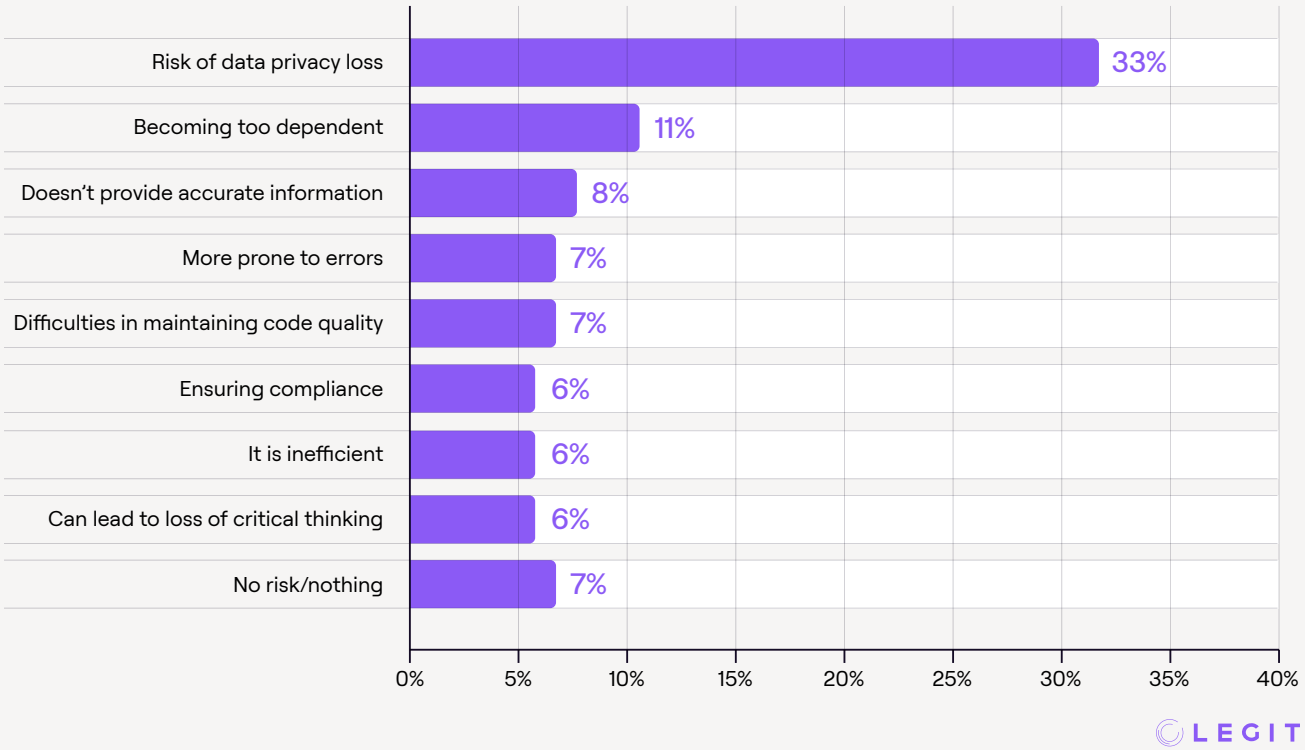


Are Teams Concerned About the Use of Code Assistants?

The findings on risks and concerns related to the use of code assistants reveal several areas of apprehension within development and security teams. "A major concern is the potential risk of biased or inaccurate decision-making due to flawed training data, lack of transparency, and insufficient human oversight," one respondent noted.

Among all respondents, 33% cite data privacy loss as their primary concern when using code assistants, while 11% are most worried about becoming too dependent on these tools. Other concerns include the potential for inaccurate information (8%), the propensity for errors (7%), and challenges in maintaining code quality (7%).

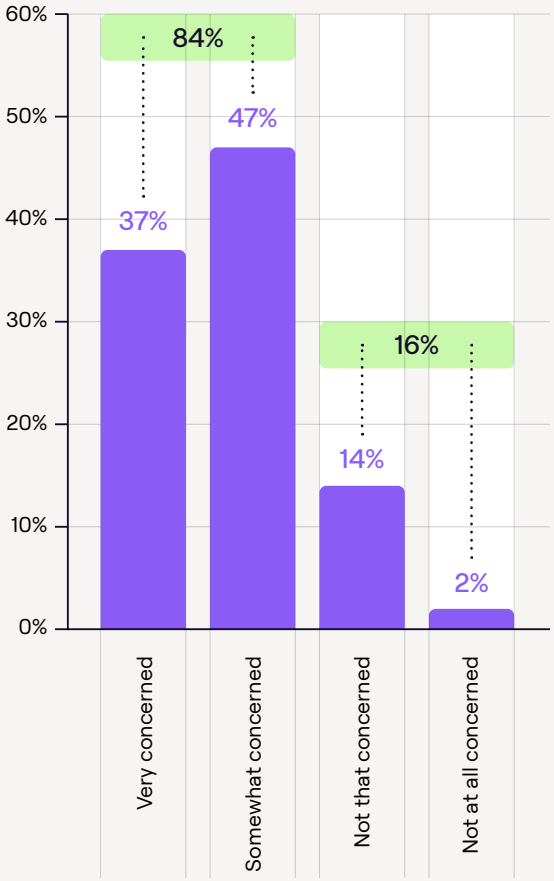
What are you most concerned about regarding the use of code assistants by your development team?



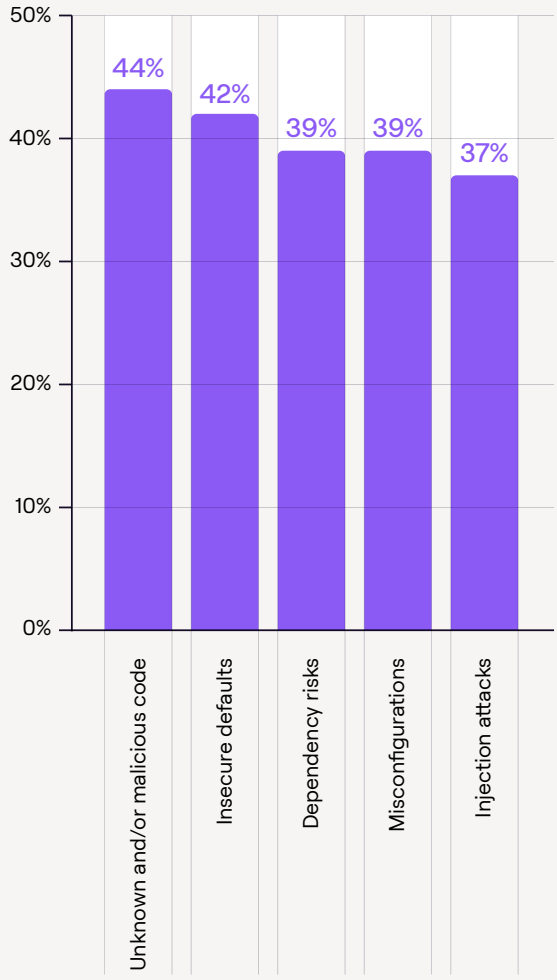
In the security realm, over four in five (84%) security professionals express concerns about the security risks posed by code assistants, with more than one-third (37%) being very concerned.

When asked to rank their top concerns, 44% of respondents point to unknown or malicious code as their biggest worry, followed closely by insecure defaults (42%). Concerns about dependency risks (39%) and misconfigurations (39%) also rank highly, as do fears of injection attacks (37%).

How concerned, if at all, are you about security when your developers are using code assistants?



Which of these risks would you say you are most concerned about when it comes to the usage of code assistants?



Legal risks are also a major consideration, with over nine in 10 (94%) respondents very or somewhat familiar with the legal risks tied to code assistants, and 93% indicating that their security team is prepared to manage the legal and security risks associated with these tools. Security professionals report a higher level of preparedness and familiarity, with 63% saying they are very familiar with the legal risks (compared to 47% of developers) and 56% feeling very prepared to manage these risks (compared to 43% of developers).

These findings highlight a range of concerns that span both technical and legal challenges, underscoring the need for careful management and oversight when integrating code assistants into development workflows.

When asked specifically about concerns for code assistant use, several respondents cited the potential for skills loss. "A major concern is the potential loss of coding skills and deep technical knowledge among developers who rely too heavily on AI-generated code, leading to decreased productivity and innovation," said one respondent. Another said "The convenience and efficiency of AI coding assistants could lead to a reliance that diminishes a developer's ability to code independently, eroding fundamental skills over time."

When looking at the difference between security and development concerns over code assistants, developers are more concerned about maintaining code quality and a loss of critical thinking.

What are you most concerned about regarding the use of code assistants by your development team?

	Security	Developers
Risk of data privacy loss	34%	33%
Becoming too dependent	10%	11%
Doesn't provide accurate information	8%	7%
More prone to errors	8%	7%
Difficulties in maintaining code quality	3%	10%
Ensuring compliance	7%	5%
It is inefficient	6%	5%
Can lead to loss of critical thinking	3%	8%
No risk/nothing	9%	5%

LEGIT

What Is the Future of GenAI in Software Development?

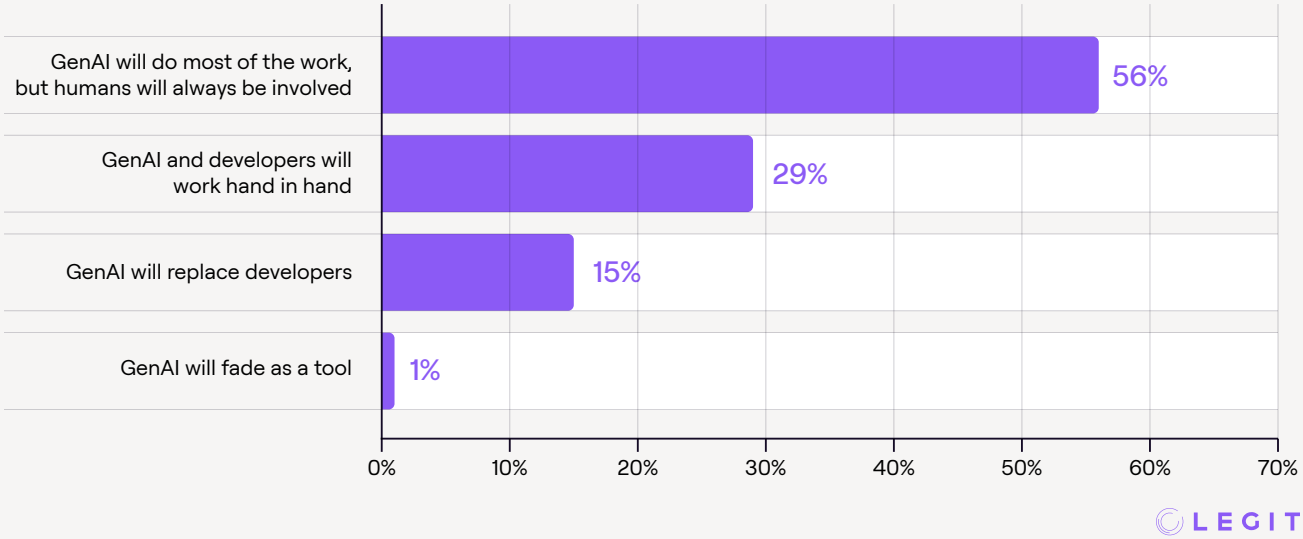
The survey results indicate a strong consensus about the increasing reliance on GenAI in software development over the next five years. 95% of respondents believe that developers will become more reliant on GenAI, with none predicting a decrease in its use. While both developers and security professionals agree on this trend, security professionals are more likely to predict that developers will be much more reliant on GenAI (52% vs. 45% of developers), while developers are more inclined to say developers will be somewhat more reliant (51% vs. 42% of security professionals).

In terms of how GenAI will work alongside developers, 56% of respondents foresee a future where GenAI will handle most of the work, but humans will always remain involved in the process. 29% believe that GenAI and developers will work collaboratively, hand in hand, and 15% predict that GenAI will eventually replace developers. Only 1% think that GenAI will fade as a tool.

There is a notable difference in perspectives between security professionals and developers. 61% of security professionals believe GenAI will do most of the work, with human oversight, compared to 51% of developers. On the other hand, 36% of developers believe that GenAI and developers will work in close collaboration, compared to 23% of security professionals.

Overall, the findings point to a future where GenAI will play a pivotal role in development, though humans will continue to be part of the equation, either as collaborators or overseers.

Which is closer to your vision of the relationship between GenAI and developers in a few years?



Conclusion

The survey makes clear the growing importance of Generative AI in software development, where it is increasingly seen as an essential tool for automating tasks and accelerating workflows. However, as GenAI becomes more pervasive, organizations must address the associated security risks and governance challenges. While most organizations have policies in place, there remains a need for greater oversight and collaboration between development and security teams.

Looking ahead, it's clear that AI will continue to play a pivotal role in development, though human involvement will remain crucial in ensuring both productivity and security.

Learn more about the security implications of GenAI use.

Visit our website

LEGIT

Legit is a new way to manage your application security posture for security, product and compliance teams. With Legit, enterprises get a cleaner, easier way to manage and scale application security, and address risks from code to cloud. Built for the modern SDLC, Legit tackles the toughest problems facing security teams, including GenAI usage, proliferation of secrets and an uncontrolled dev environment. Fast to implement and easy to use, Legit lets security teams protect their software factory from end to end, gives developers guardrails that let them do their best work safely, and delivers metrics that prove the success of the security program. This new approach means teams can control risk across the business — and prove it.

legitsecurity.com