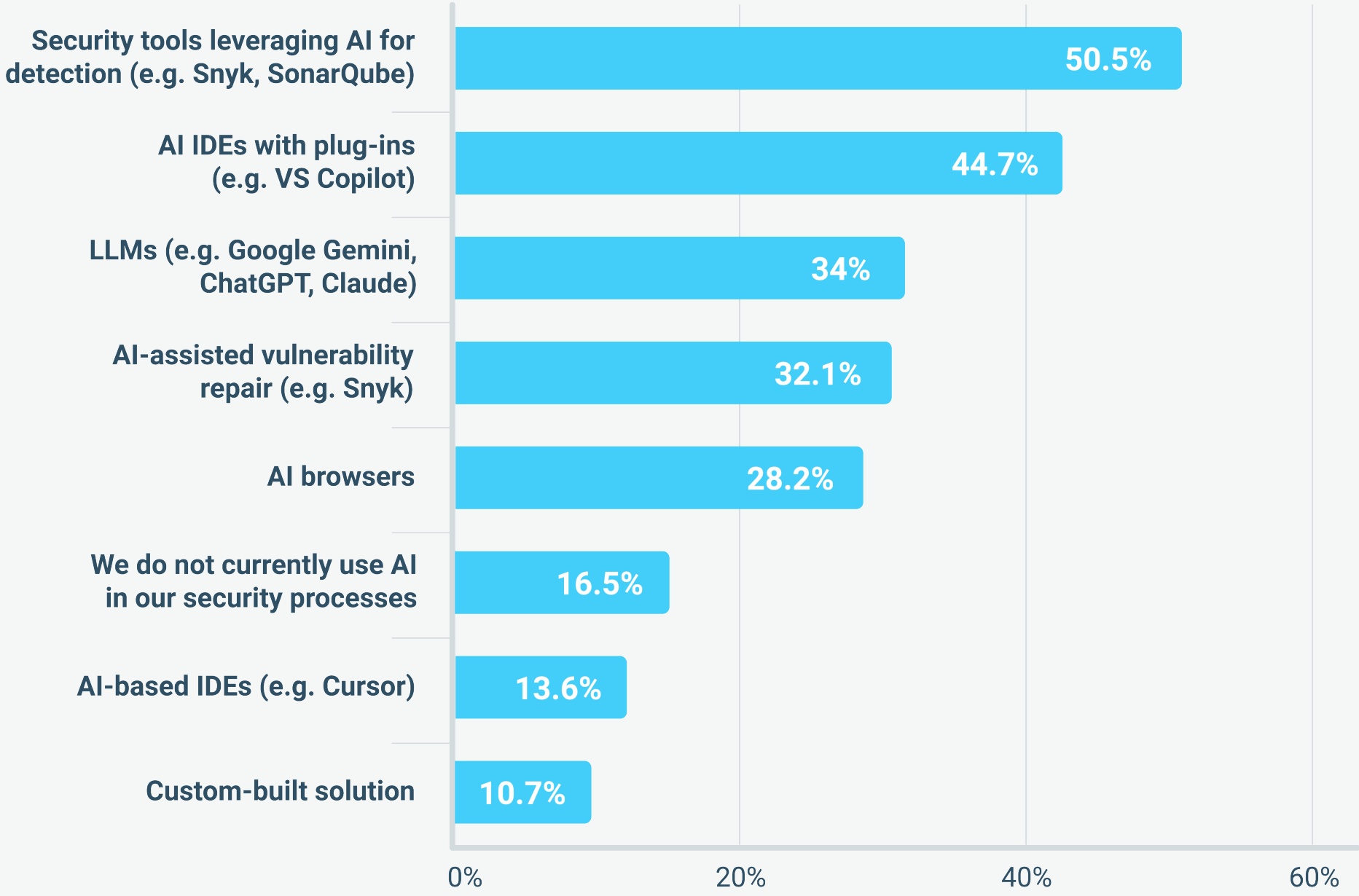
AI in Security

AI is reshaping how software is built, and teams are feeling the impact just as directly. What began as experimentation with AI-assisted coding has expanded into broader adoption across detection, analysis, and testing workflows. For many organizations, AI is no longer a future consideration; it is already embedded in day-to-day security operations.

At the same time, this shift introduces a new layer of complexity. AI is increasing both the volume of code and the range of potential vulnerabilities, while raising new concerns around trust, data privacy, and governance. Security teams are being asked to move faster, analyze more, and adapt to risks that did not exist just a few years ago. The result is a clear duality: AI is unlocking new efficiencies, but also raising the stakes. This section explores how teams are applying AI today, how it is reshaping security posture, and what is limiting broader, more effective adoption.

Do you currently leverage AI tools in your existing security processes? If yes, which?



Over half of teams use AI for threat detection, signaling mainstream adoption

AI is already embedded in security workflows. Over half of respondents (50.5%) report using AI for detection, alongside strong adoption of AI-assisted IDEs (44.7%) and large language models (34%). This shows that adoption spans both security operations and development environments, extending AI's role across the entire software lifecycle.

Rather than being confined to isolated use cases, AI is becoming a foundational layer in how teams identify and respond to threats. It enhances developer productivity, accelerates analysis, and expands detection capabilities. As adoption scales, organizations are operating under an AI-augmented security model that balances speed and efficiency with oversight, validation, and control.

AI is now embedded across both development and security workflows, fundamentally changing how teams build and protect software. As a result, security operations are shifting toward AI-augmented models that rely on automation and intelligent analysis. However, increased dependence on AI introduces new requirements for validation, oversight, and trust. While these workflows expand what teams are capable of, they also broaden the risk surface and make it critical to balance efficiency gains with stronger controls and visibility.

- **AI is now becoming mainstream in security workflows**
- **Adoption spans both development and security layers**
- **AI introduces new risks alongside efficiencies**

How has AI code generation impacted your security posture today?

	% share of selected responses
Enabled advanced testing approaches (predictive analytics, anomaly detection)	20.6%
Improved accuracy of testing outcomes	14.3%
Created concerns for overall application security	12.9%
Minimal impact on my role so far	12.8%
Increased efficiency and automation of security testing	12.5%
Allowed focus on more strategic and complex tasks	10.0%
Created concerns over job stability	8.4%
Required learning new skills or upskilling	7.8%
Other	0.8%

Some security pros say AI improves security, but others say it's creating new risks

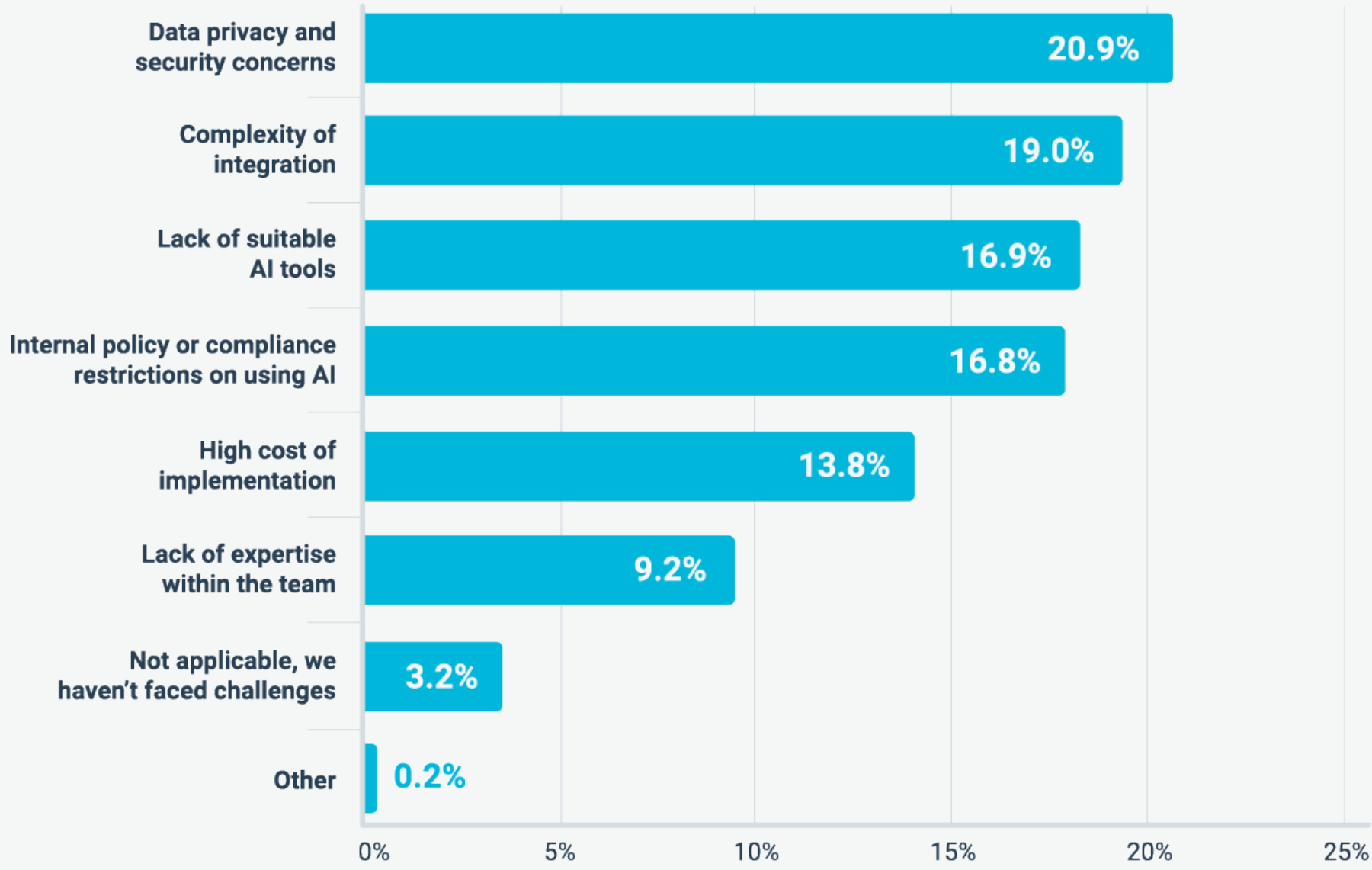
The impact of **AI-generated code** on security posture is both measurable and mixed. Some teams report clear benefits: 20.6% cite more advanced testing capabilities, and 14.3% report overall improvements. At the same time, 12.9% report new security concerns, reflecting uncertainty around the risks AI introduces.

This split highlights the dual nature of AI in security. It enables faster testing, broader coverage, and new approaches to detection, but also introduces unfamiliar vulnerability patterns, inconsistencies, and blind spots in traditional validation methods. The result is not a net-positive or net-negative shift, but a more complex and dynamic security landscape that requires new approaches to risk management.

AI is increasing what teams can do while raising the baseline level of risk they must manage. Traditional validation methods are not always equipped to detect AI-specific vulnerabilities, leaving potential gaps in coverage. At the same time, the surge in code volume amplifies overall exposure, making it easier for issues to slip through unnoticed. To keep pace, security strategies must evolve and adapt to new risk patterns introduced by AI-driven development.

- **AI delivers both improvements and new risks**
- **Traditional security approaches may fall short**
- **AI-aware testing strategies are now essential**

What challenges have you faced in integrating AI into your security process?



Organizations cite data privacy as the top barrier, with AI integration complexity close behind

While AI adoption is widespread, integrating it effectively into security processes remains a challenge. The most commonly cited barriers are data privacy concerns (20.9%) and integration complexity (19%), pointing to issues of trust and implementation rather than technical capability.

These challenges highlight a gap between experimentation and operationalization. Many teams are exploring AI tools, but embedding them securely and seamlessly into existing workflows is proving difficult. Concerns around **sensitive data exposure**, regulatory compliance, and tool interoperability are slowing adoption and limiting how far organizations are willing to go.

- **Trust and complexity limit AI adoption**
- **Privacy and compliance are major concerns**
- **Secure, integrated AI solutions are needed**