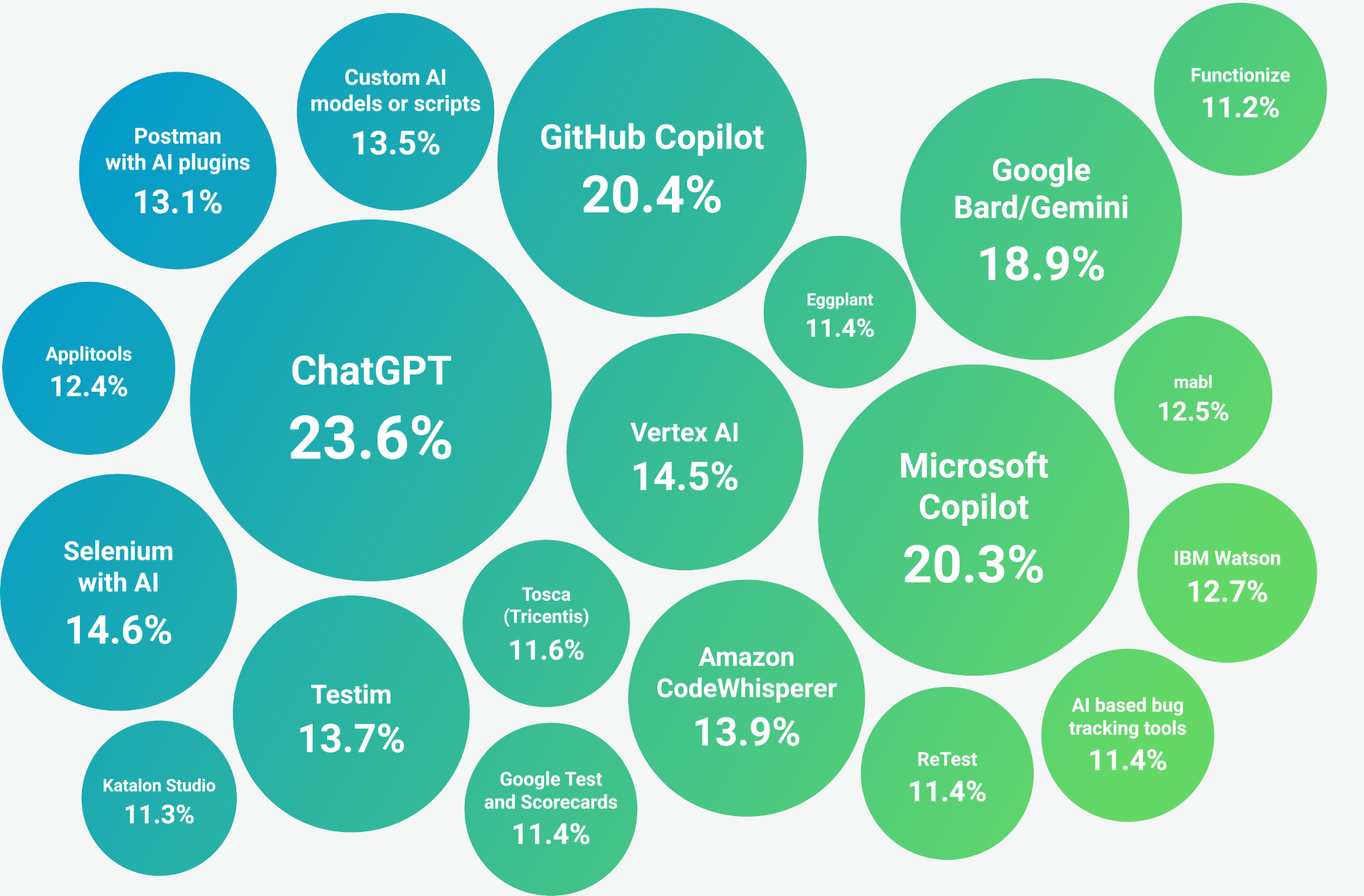


AI in QA

AI is becoming a bigger part of QA, but most teams are still working out how to use it effectively. Across the industry, organizations are trying a mix of AI tools to improve testing speed, coverage, and efficiency. While the opportunity is clear, the results are uneven. Some teams are seeing real benefits, while others are dealing with challenges like integration complexity, data privacy concerns, and rising costs.

This section examines how QA teams are using AI today, the impact it is having, and what is getting in the way of broader success. It looks at which tools are most common, how teams describe the results of AI-driven testing, how AI-generated code is increasing testing demand, and what barriers are slowing adoption. Overall, the data suggests that AI is becoming more common in QA, but consistent value still depends on how well it is implemented.

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



No single AI tool dominates QA, with ChatGPT leading adoption

The absence of a dominant AI tool in QA is itself a signal. Unlike other technology shifts where one or two platforms quickly captured most of the market, AI adoption in testing is sprawling and experimental. Teams are reaching for whatever is closest—general-purpose LLMs, IDE assistants, purpose-built testing plugins—rather than following an industry-wide playbook. That reflects how early this transition still is: organizations know AI belongs in their QA workflow, but most haven't yet determined where it creates the most durable value.

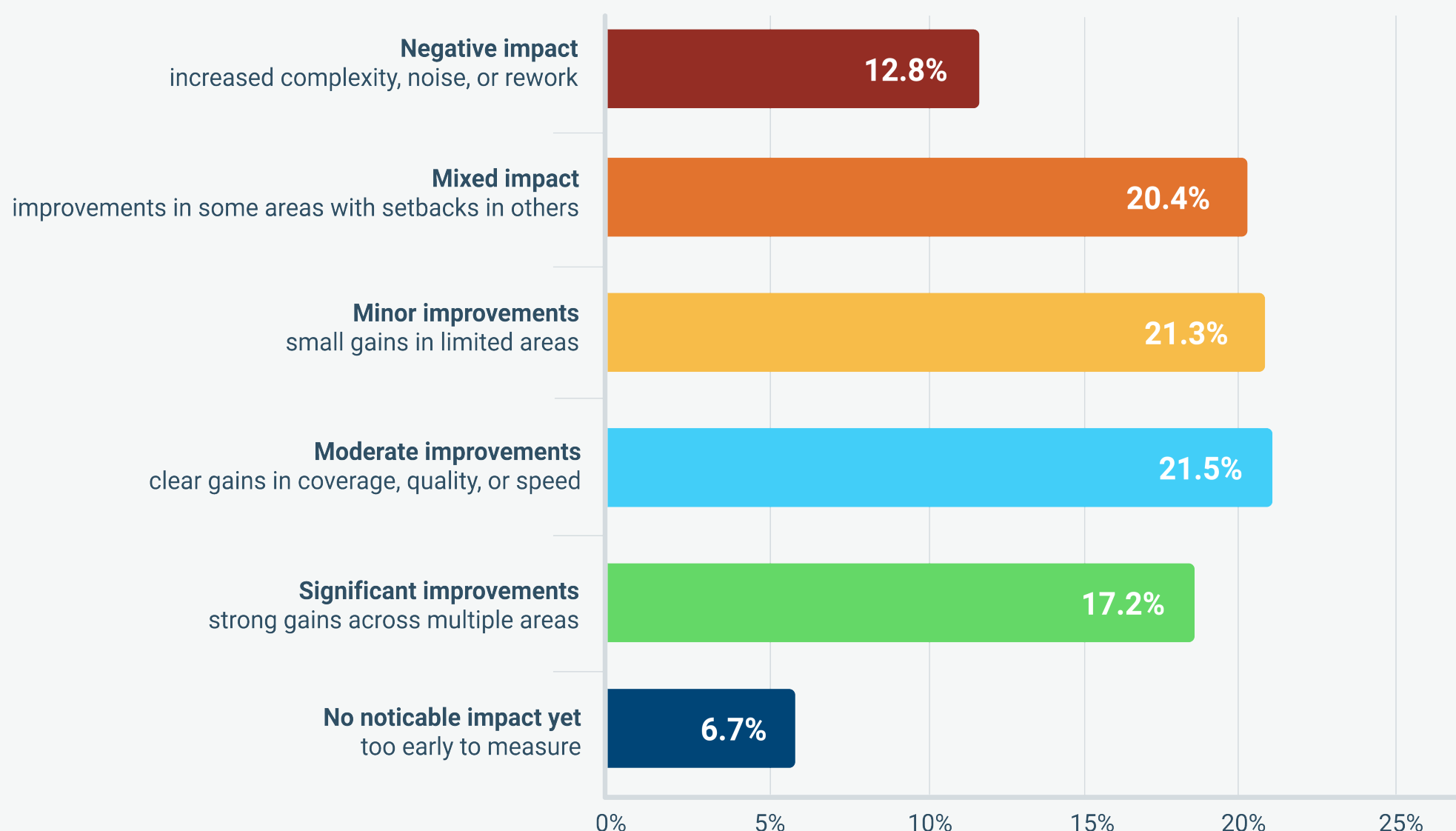
This matters because fragmented adoption can create new problems alongside new efficiencies. Different teams may use different tools for different tasks, which can lead to siloed workflows, inconsistent practices, and more complexity to manage. At the same time, the spread of adoption shows strong interest in AI across the testing lifecycle. The bigger opportunity now is not just using more AI, but using it in a way that is more connected, consistent, and easier to scale.

- **AI adoption is broad but fragmented**
- **Most teams are still experimenting**
- **Standardization has not yet emerged**

“The real breakthrough won't be ‘AI writes test cases’ or ‘AI replaces testers.’ It will be AI that understands the system, the risks, and the change impact, then tells QA what to test, when, and how deep.”

- Survey Respondent

How would you describe the impact of AI-driven testing on QA coverage, quality, and/or speed?



Most teams report minor, mixed, negative, or no noticeable impact from AI-driven testing

The results here push back on the more triumphant narratives around [AI in testing](#). Despite heavy investment and widespread adoption, teams are not reporting a step-change in quality outcomes. The distribution of responses—spread across incremental improvement, mixed results, and even negative impact—suggests that AI testing tools perform unevenly across environments, use cases, and levels of implementation maturity. For every team seeing meaningful gains, there is another absorbing the overhead of AI integration without a clear return.

Adding AI to the testing process does not guarantee better outcomes alone. While 60% of teams report at least some improvement, only 17.2% say those gains have been significant. This suggests that AI is creating value in specific areas, but not yet in a way that is broad, consistent, or transformative across QA. The next opportunity is not just wider adoption, but a more thoughtful approach to applying AI in ways that deliver more reliable results.

- **Most gains are still incremental**
- **Outcomes remain uneven across teams**
- **Significant impact is still limited**

“AI is showing what is wrong within QA—implementing it on top of an unstable architecture, and AI really highlights the cracks in their systems.”

- Patrícia Duarte Mateus, TestRail Solution Architect

How has AI code generation impacted your security posture today?



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

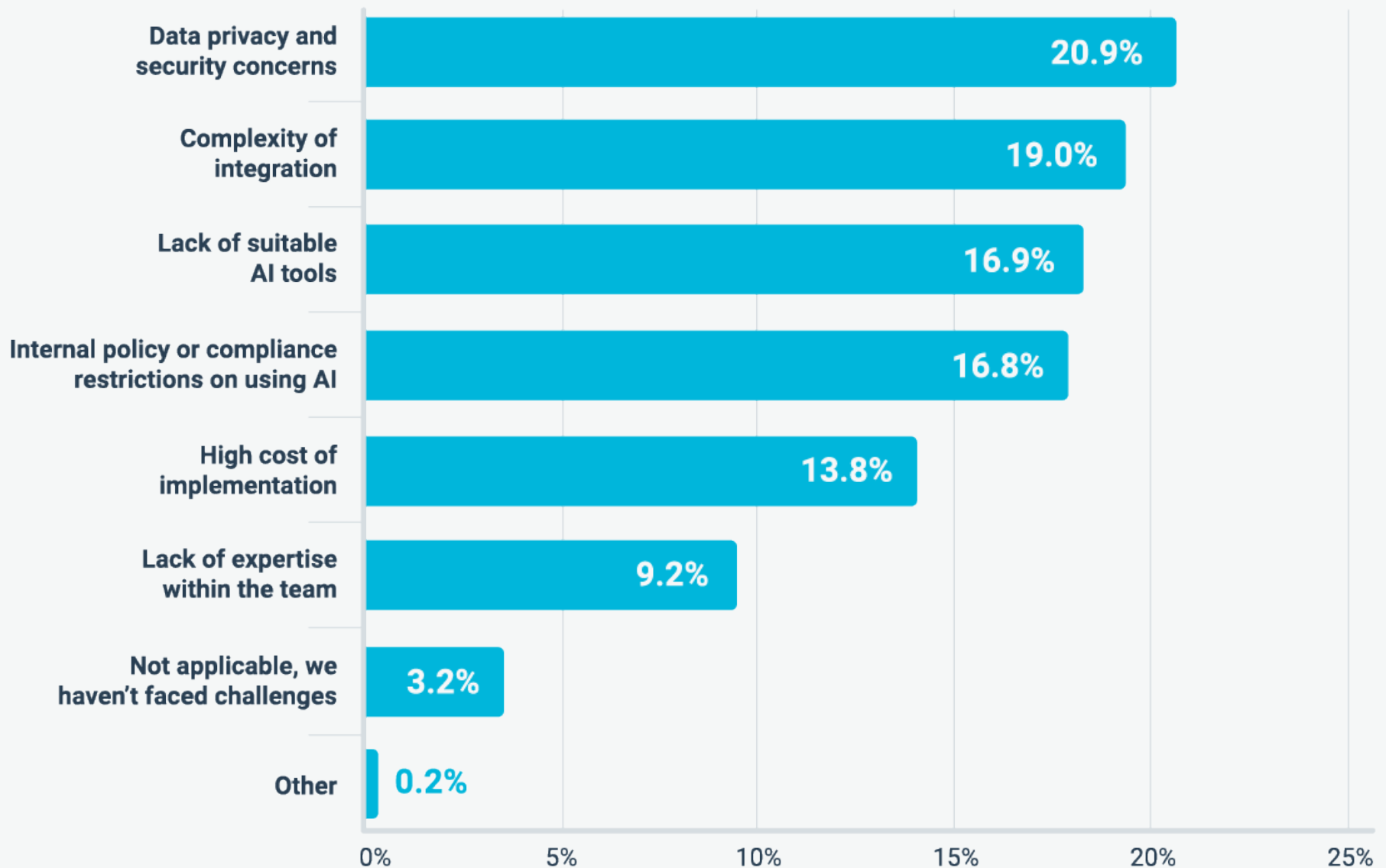
The impact of [AI-generated code](#) on security posture is both measurable and mixed. Some teams report clear benefits: 20.6% cite more advanced testing capabilities, and 14.3% report overall improvements. At the same time, 12.9% report new security concerns, reflecting uncertainty around the risks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