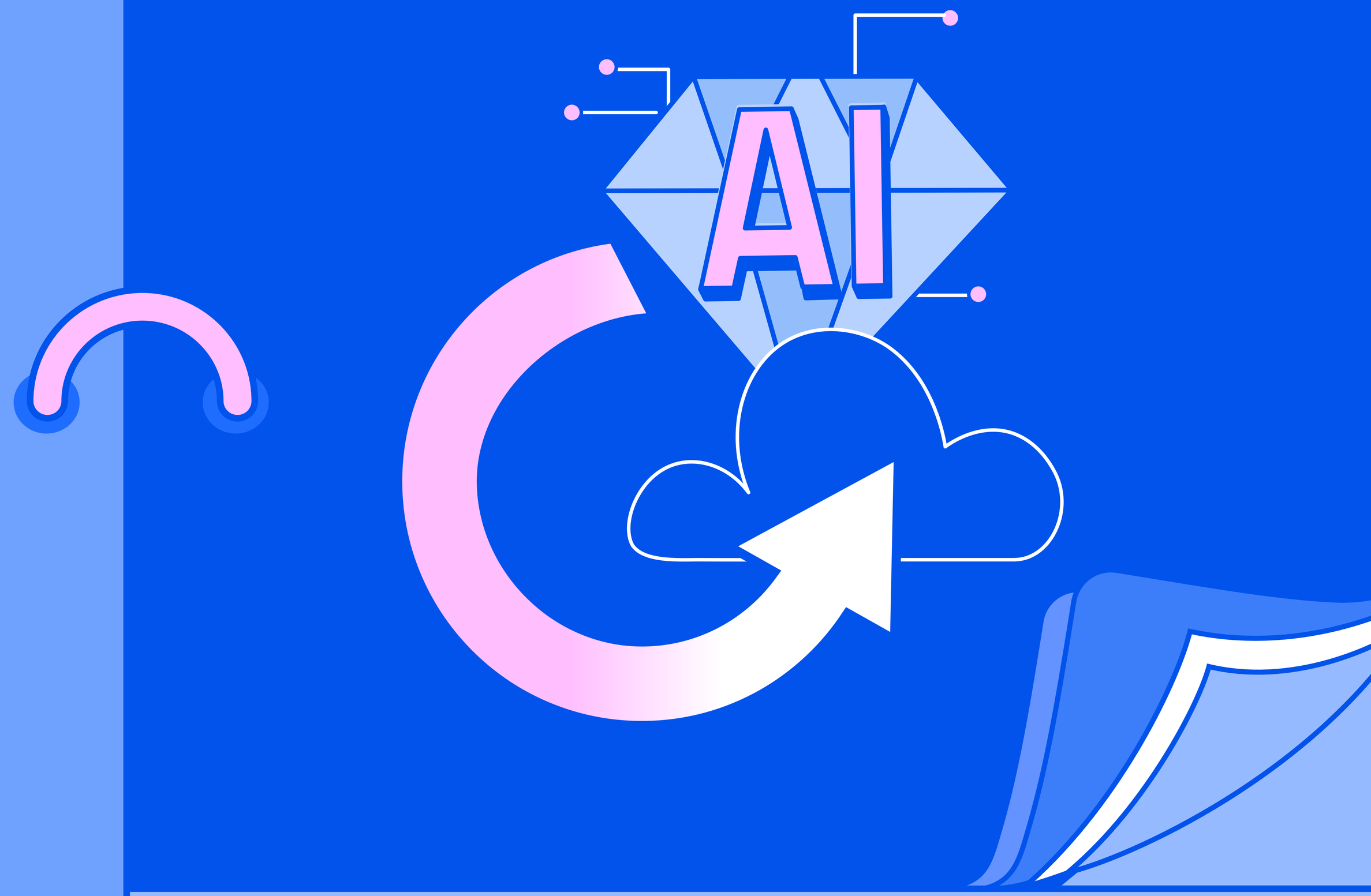
AI Security Readiness:

# Insights From 100 Cloud Architects, Engineers, And Security Leaders



# Table of Contents

# Introduction

In late 2024, Gatepoint Research invited a select group of professionals to participate in a survey titled Navigating the Future of AI Security. The 100 respondents spanned 96 unique organizations, and included engineers, architects, CxOs, VPs, directors, and managers across various industries. They were asked to report on their cloud adoption journeys, current cloud architectures, AI usage patterns, top AI security challenges, and the strategies they've implemented to manage those risks. In this ebook, we explore AI adoption and security trends from that survey data.

# Executive Summary

The AI adoption is nearly universal, but security isn't keeping up.

According to our survey, 87% of respondents are using AI services. This aligns with Wiz's State of AI in the Cloud 2025 report, where we found that over 85% of respondents are currently using either managed or self-hosted AI services or tools. However, the adoption of security best practices is not keeping pace.

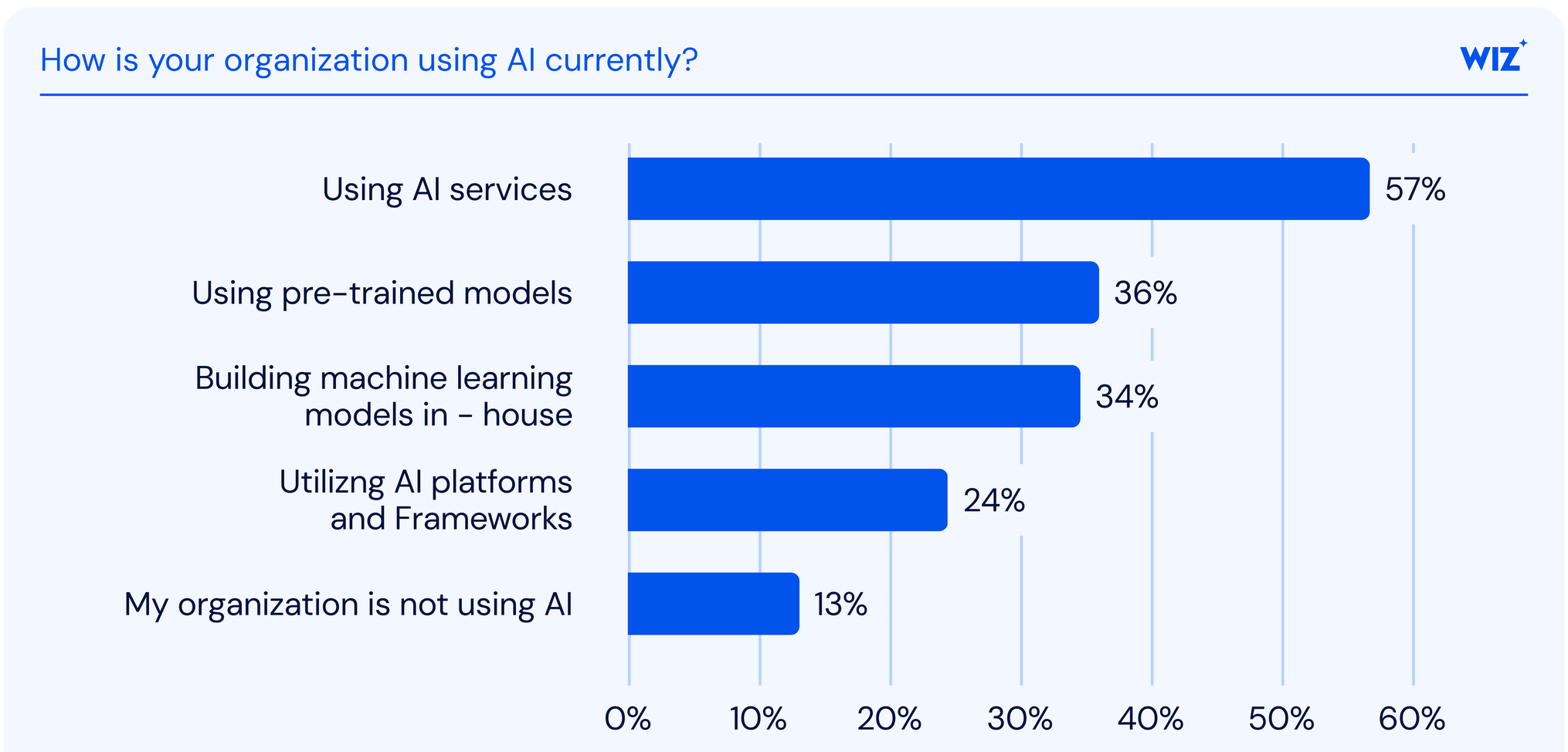
31% of respondents cite a lack of AI security expertise as their top challenge. The rate of innovation in AI can't afford to wait for security to upskill. This gap increases risk exposure and makes tooling and automation critical.

While traditional security approaches like EDR and vulnerability management remain prevalent (adopted by 70% and 65% of respondent respectively), only 13% of respondents have adopted AI-specific posture management (AI-SPM). Shadow AI is also on the rise—25% of respondents don't know what AI services are running in their environment, raising further concerns about visibility and governance.

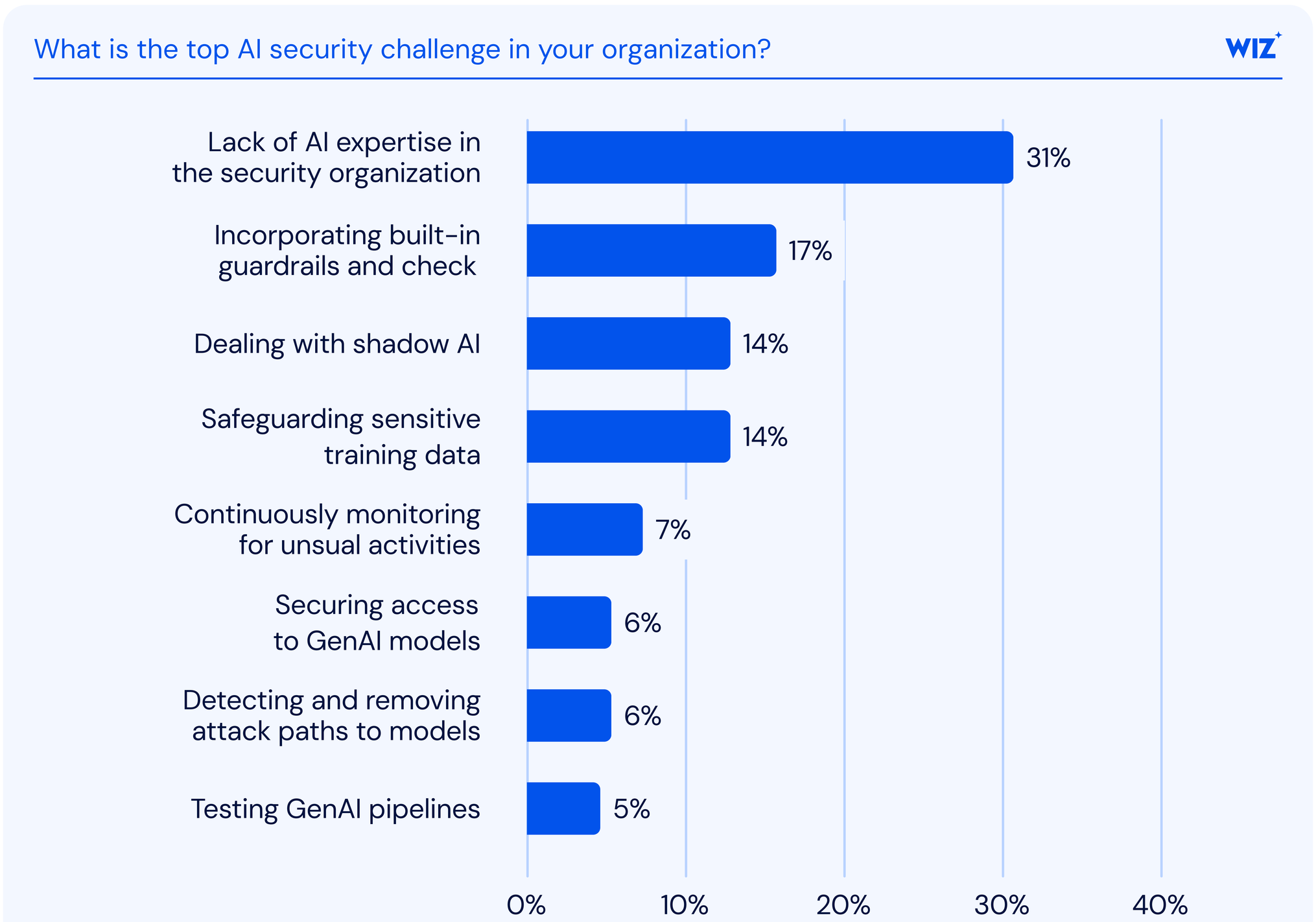
Security teams must act quickly. A hybrid approach that blends traditional cloud security with AI-native protections is no longer optional—it's essential.

## 1 AI Adoption is Outpacing Security Expertise

**Survey Data Insights:** Only 13% of respondents reported no use of AI in their organizations at all. That leaves a whopping 87% of that do use AI services, most of which rely on managed offerings like OpenAI and Amazon Bedrock. This mirrors findings from Wiz's State of AI in the Cloud 2025 report, where 85% of organizations indicated some form of AI use, whether managed or self-hosted.



At the same time, nearly a third of survey respondents (31%) said that a lack of AI security expertise is their biggest challenge.



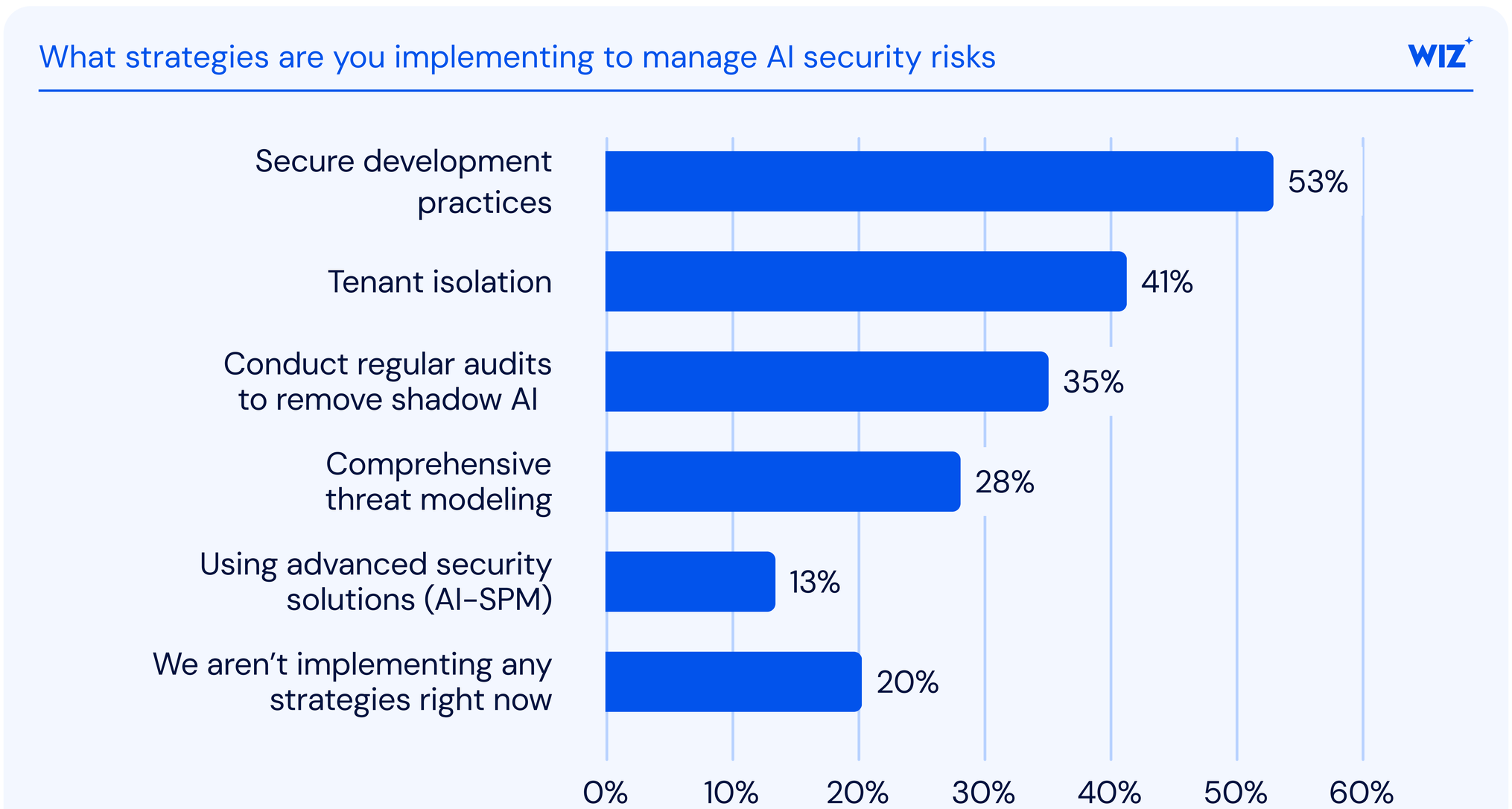



**Why This Matters:** The rapid adoption of AI services is not being matched by the development of in-house expertise to secure them. Security teams are being asked to protect systems they may not fully understand, and this expertise gap creates a growing risk surface.

**Call to Action:** Organizations must prioritize structured AI security frameworks and invest in upskilling programs to build internal knowledge. Until then, tooling that helps close the visibility and control gap is critical.

## 2 AI Security Requires Both Traditional and Advanced Solutions

**Survey Data Insights:** Only 13% of respondents report using AI-SPM solutions today. Meanwhile, more traditional controls are widely deployed: 53% have implemented secure development practices, 41% use tenant isolation, and 35% perform audits to uncover shadow AI.






**Why This Matters:** Traditional security practices still have a key role to play in securing AI systems. Protecting the software development lifecycle (SDLC), enforcing isolation between tenants, and conducting regular audits are all critical foundations. However, they are not enough on their own. As AI usage grows, so too does the sophistication of associated risks—and current strategies aren't equipped to address the speed or scale of adoption.

One area that deserves greater attention is tenant isolation. In a multi-tenant GenAI architecture, improper segmentation can expose data between workloads and users. As highlighted in Wiz's blog on GenAI tenant isolation, AI workloads often run in environments where shared infrastructure or dependencies create implicit trust boundaries.

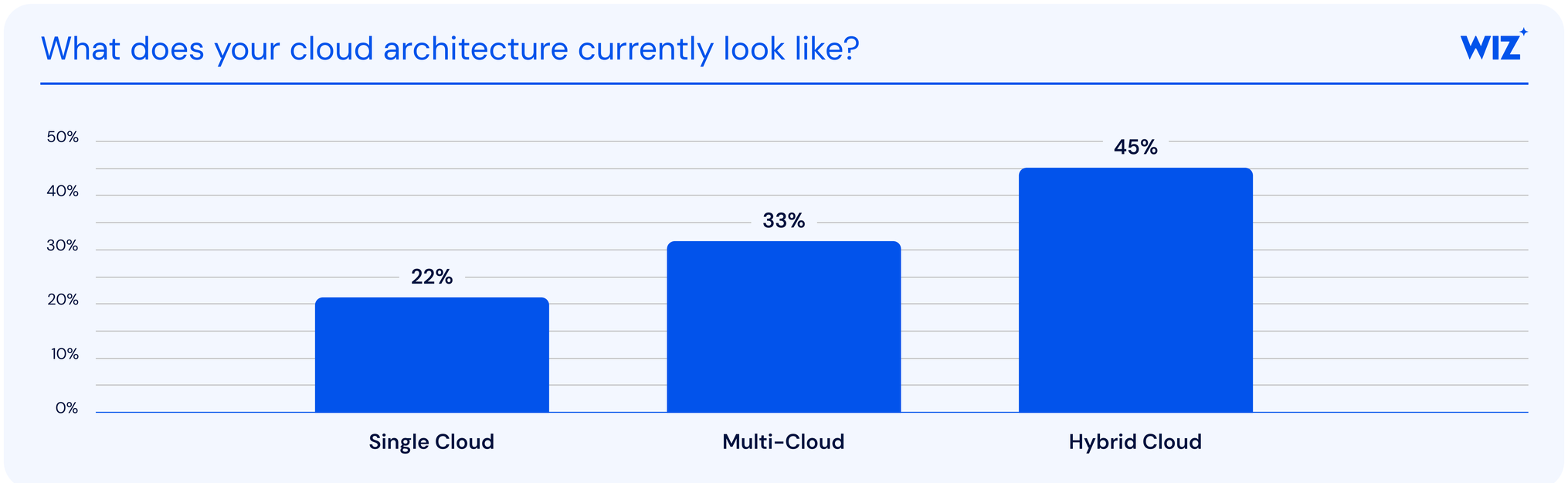
If these boundaries aren't explicitly defined and enforced, attackers may be able to move laterally between tenants or access sensitive outputs from unrelated workloads. The blog also outlines architectural design patterns to mitigate these risks, including granular IAM, scoped permissions, and environment-specific model registries.

In Wiz's State of AI report, we highlighted the rise of open-source models like DeepSeek-R1, which surpassed 130,000 downloads. With more organizations turning to self-hosted models, it's clear that manual discovery and auditing processes are no longer sufficient.

**Call to Action:** Security programs must take a layered approach: foundational best practices need to be complemented with AI-specific protections. Organizations should adopt CSPM and CNAPP to address broader cloud posture while leveraging AI-SPM for discovering and securing AI-specific risks like shadow usage, model exposures, and data leakage. Isolation must be explicit, not assumed —especially in GenAI environments. Security programs must take a layered approach: foundational best practices need to be complemented with AI-specific protections. Organizations should adopt CSPM and CNAPP to address broader cloud posture while leveraging AI-SPM for discovering and securing AI-specific risks like shadow usage, model exposures, and data leakage.

## 3 Cloud Security Architectures Are Increasingly Complex

**Survey Data Insights:** Many respondents (45%) say they operate in hybrid cloud environments, while 33% use multi-cloud setups. Only 22% have a single-cloud architecture. Despite this complexity, security tooling remains rooted in endpoint-focused strategies—EDR is deployed by 70% of respondents, while only about a third use cloud-native platforms like CNAPP or CSPM.



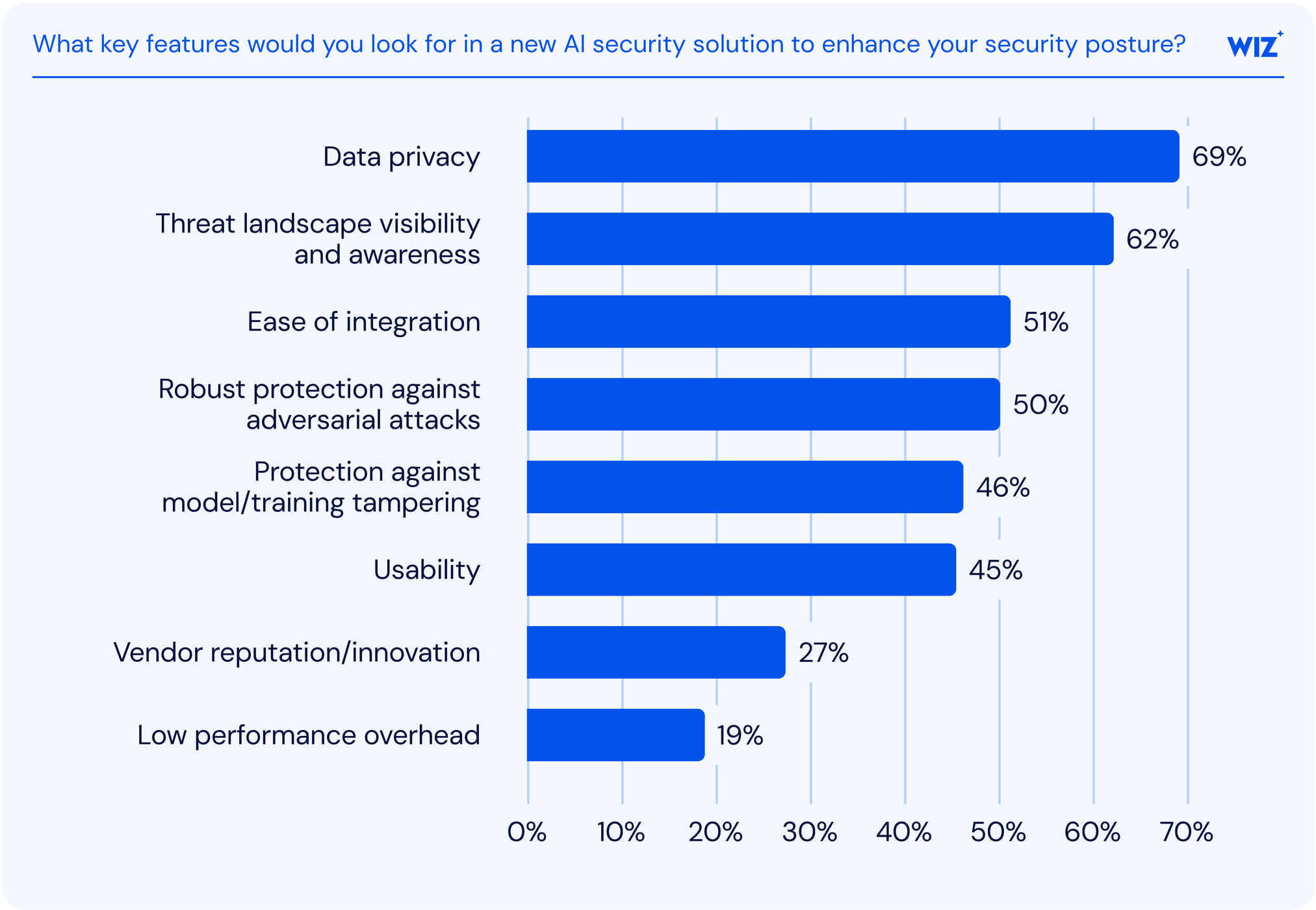



**Why This Matters:** AI workloads don't live in a vacuum. They span containerized services, serverless compute, and APIs across different cloud providers. Yet most security controls in use are designed for a more centralized IT model. This disconnect creates visibility gaps, increases misconfiguration risk, and exposes sensitive AI models and training data to threats.

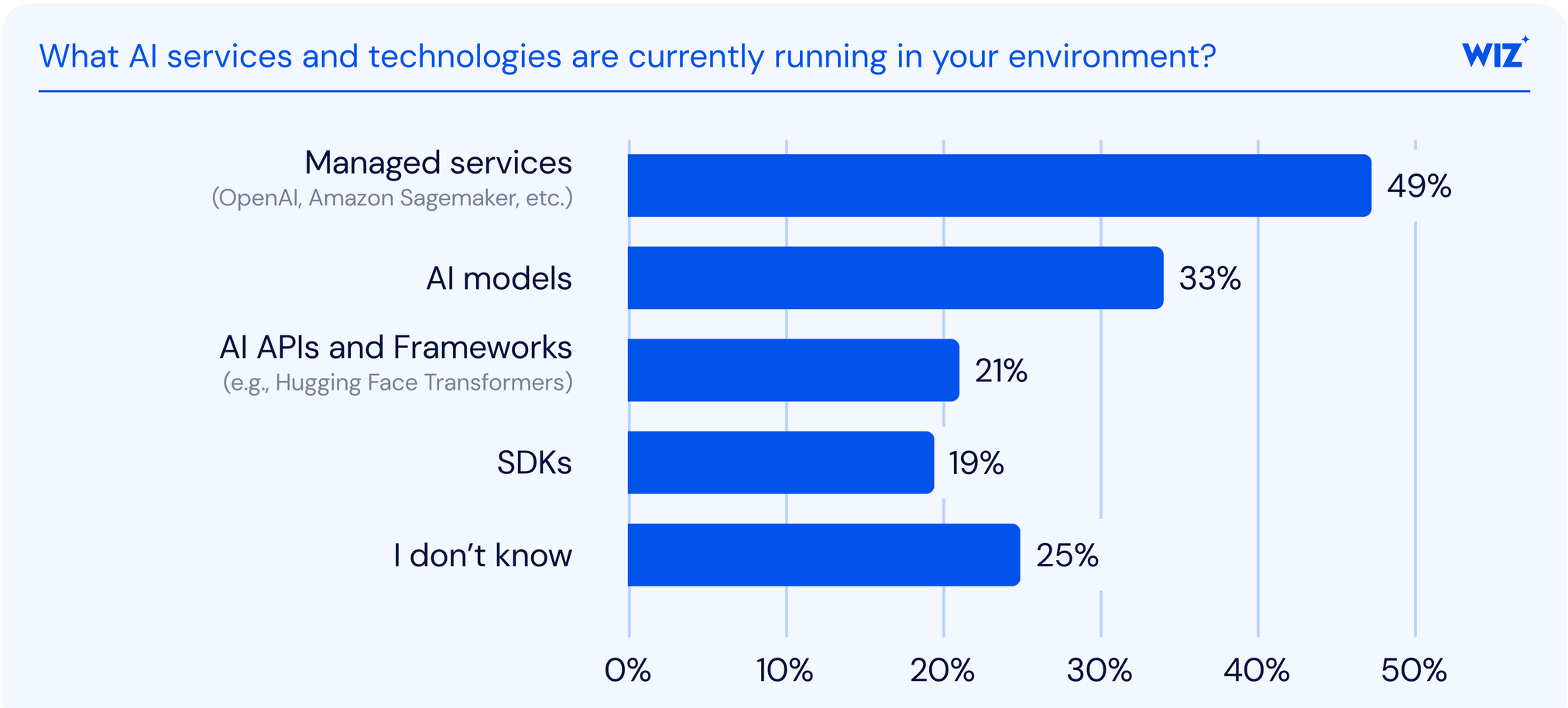
**Call to Action:** Organizations should prioritize security tools built for modern, distributed environments. CNAPP and CSPM offer visibility into cloud-native services and AI workloads running across environments. A holistic approach to cloud security that includes AI posture management is crucial to addressing today's risks.

## 4 AI Security Challenges Are Not Just Technical—They're Operational

**Survey Data Insights:** When asked about top priorities for AI security solutions, respondents pointed to data privacy (69%), threat visibility (62%), and ease of integration (51%).




However, 25% also admitted they don't know what AI services are in use in their environments.

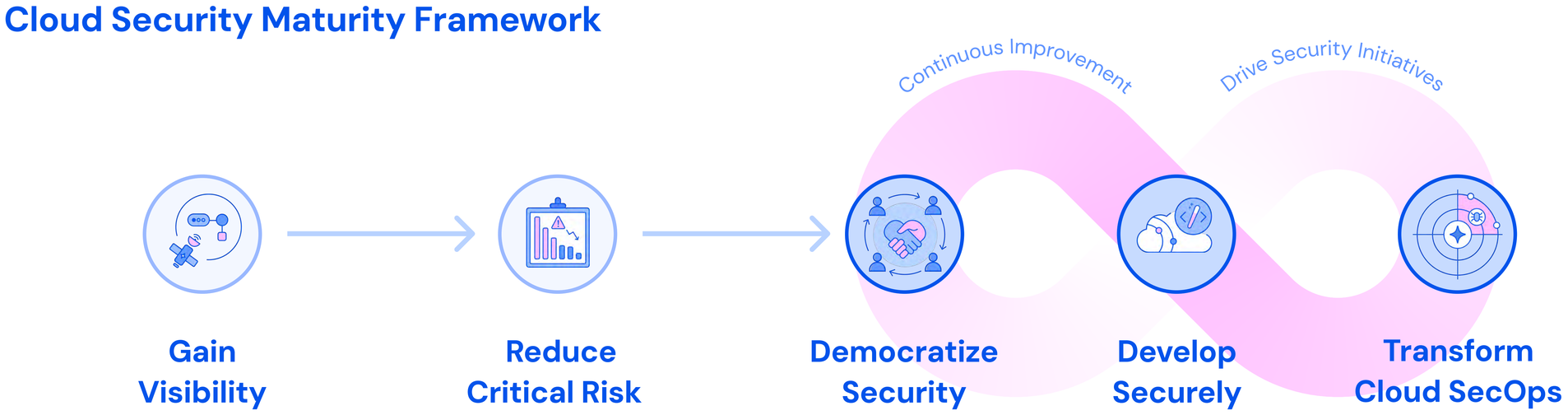


**Why This Matters:** While many organizations understand what they want from AI security, fewer know how to operationalize it. Tools that are difficult to integrate stall adoption. Worse, a lack of visibility into deployed services—or shadow AI—makes it impossible to defend against threats you can't see. This isn't just a technology problem. It's a workflow and awareness issue, often compounded by decentralized AI experimentation.

**Call to Action:** To bridge the gap, security tools must be designed to fit into existing cloud and DevOps workflows without requiring major change management. Automation should drive discovery and risk reduction, not add overhead.

## 5 Evaluating Security Maturity

Wiz's **Cloud Security Maturity Framework** outlines how modern teams evolve from simply gaining visibility to fully transforming how security is embedded across development and operations. It's a model built to help organizations continuously adapt—as threats evolve, architectures grow more complex, and innovation accelerates.




### Where Does AI Security Maturity Fall Within the Cloud Security Maturity Framework?

AI security isn't its own standalone journey—it's a thread that weaves through every stage of broader cloud security maturity. As organizations progress through the phases of the **Wiz Cloud Security Maturity Framework,** their ability to manage AI-specific risk evolves alongside.

#### Phase 1 Gain Visibility

**AI maturity stage: Experimental AI (High Risk)**

At this stage, AI is being used—often rapidly—but without centralized visibility or governance. Security teams may be unaware of how many models, APIs, or services are in use. There's limited context around what data AI systems touch or how they behave in production. Shadow AI is common.

**Focus areas:** Discovery, inventory, shadow AI detection, foundational posture visibility

#### Phase 2 Reduce Critical Risk

**AI maturity stage: Early AI Governance (Elevated Risk)**

AI workloads begin reaching production, but are often protected with general-purpose tooling like EDR or VM. AI-specific risks—like model exposures, tenant crossover, or poisoned training data—remain largely unaddressed. Risk is elevated, not just because of the tech, but because the business is increasingly dependent on AI outputs.

**Focus areas:** Tenant isolation, secure SDLC for AI apps, prioritizing risks with AI context

### Phase 3 Democratize Security & Develop Securely

**AI maturity stage: AI-Integrated Security (Reduced Risk)**

Security is embedded into development workflows. Teams use CSPM/CNAPP to monitor infrastructure and AI-SPM to track model usage, exposure, and behavior. Developers are equipped with guidance and guardrails. Shadow AI is automatically surfaced and governed.

**Focus areas:** Discovery, inventory, shadow AI detection, foundational posture visibility

### Phase 4 Transform Cloud SecOps

**AI maturity stage: Proactive, Automated AI Security**

Security operations can identify AI-driven risks in real time, respond automatically, and continuously improve policies based on AI-specific learnings. AI security isn't a niche skill—it's part of the core SecOps toolkit, enabled by automation and integrated context.

**Focus areas:** Runtime policy enforcement, automated response, AI-aware threat modeling

Most organizations remain in **phase 1 or 2.** AI is becoming mission-critical, but security programs haven't kept pace. Moving to **phase 3 and beyond** requires deliberate planning and investment. Organizations should benchmark their maturity and map out the steps needed to embed AI risk management into broader cloud security strategies.

## 6 Recommendations: How to Close the AI Security Gap

- **Adopt tools that continuously scan for new services, models, and shadow AI**
  Manual audits can't keep up with the scale and speed of AI usage growth. Automated discovery is essential for maintaining visibility and control as environments evolve rapidly.
- **Integrate security early in the development lifecycle**
  Waiting until deployment is too late to catch risky behavior. Shifting security left allows teams to address misconfigurations and vulnerabilities during design and build phases—before they reach production.
- **Ensure security controls follow AI workloads across environments**
  AI services don't stay put—they span containers, APIs, and cloud platforms. Security must move with them, providing consistent policy enforcement regardless of infrastructure.
- **Equip security teams with AI-specific training and tools**
  Even the best tools fall short if teams don't understand the risks they're solving for. Upskilling programs and better collaboration between security and data teams are essential for effective governance.

## 7 Future-Proofing AI Security

AI is evolving quickly—and so are the risks. Staying secure means keeping a constant pulse on how AI is used and adapting defenses in real time. Regulations are coming, and attackers are already targeting exposed models and endpoints. In complex, hybrid environments, visibility gaps make AI harder to protect.

Security can't be reactive. It must be continuous and proactive. That means building automation, visibility, and policy enforcement into every stage of the AI lifecycle. Teams that invest in AI security posture today will be better equipped to scale innovation safely tomorrow.