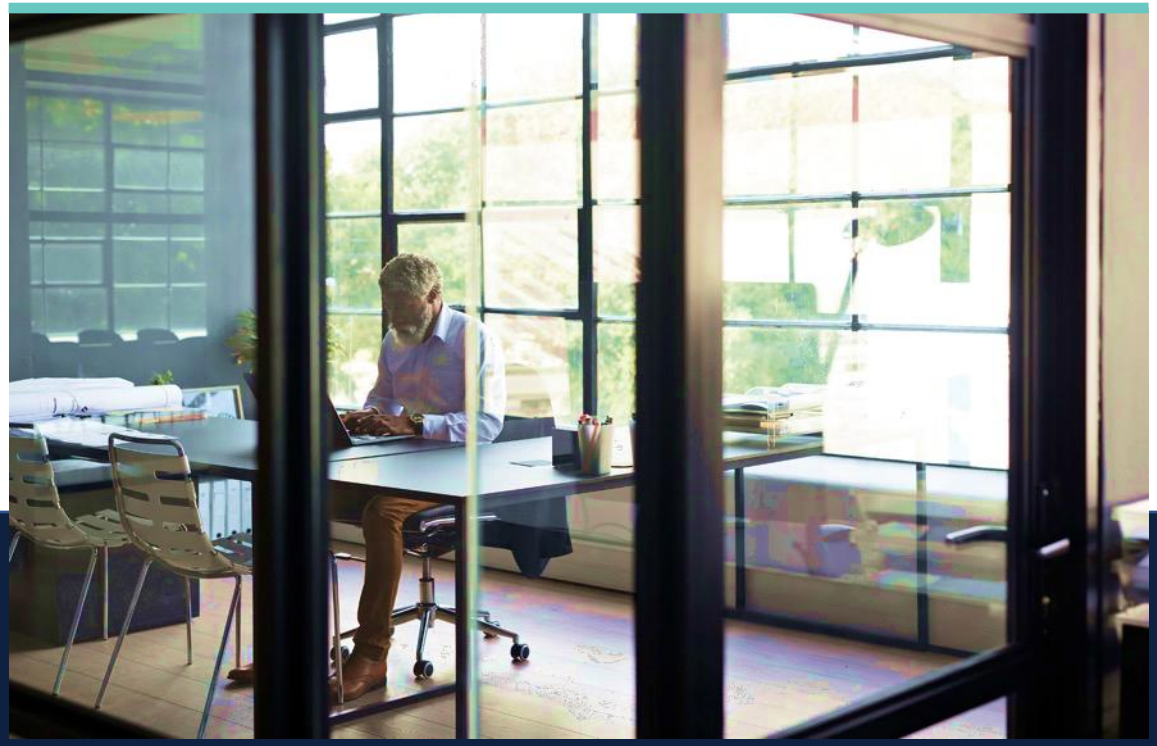
WIZ

PULSE REPORT GATEPOINT RESEARCH

# NAVIGATING THE FUTURE OF AI SECURITY

## SUMMARY RESULTS



DECEMBER 2024

# WHO DID WE SURVEY?

Between September and November 2024, Gatepoint Research invited selected executives to participate in a survey themed *Navigating the Future of AI Security.*

Candidates from several industries were invited via email and 100 executives have participated to date.

Management levels represented are all senior decision-makers: 16% hold the title CxO or are VPs, 15% are directors, 11% are senior or department managers, 58% are data, system, or application architects or engineers.

100% of responders participated voluntarily; none were engaged using telemarketing.

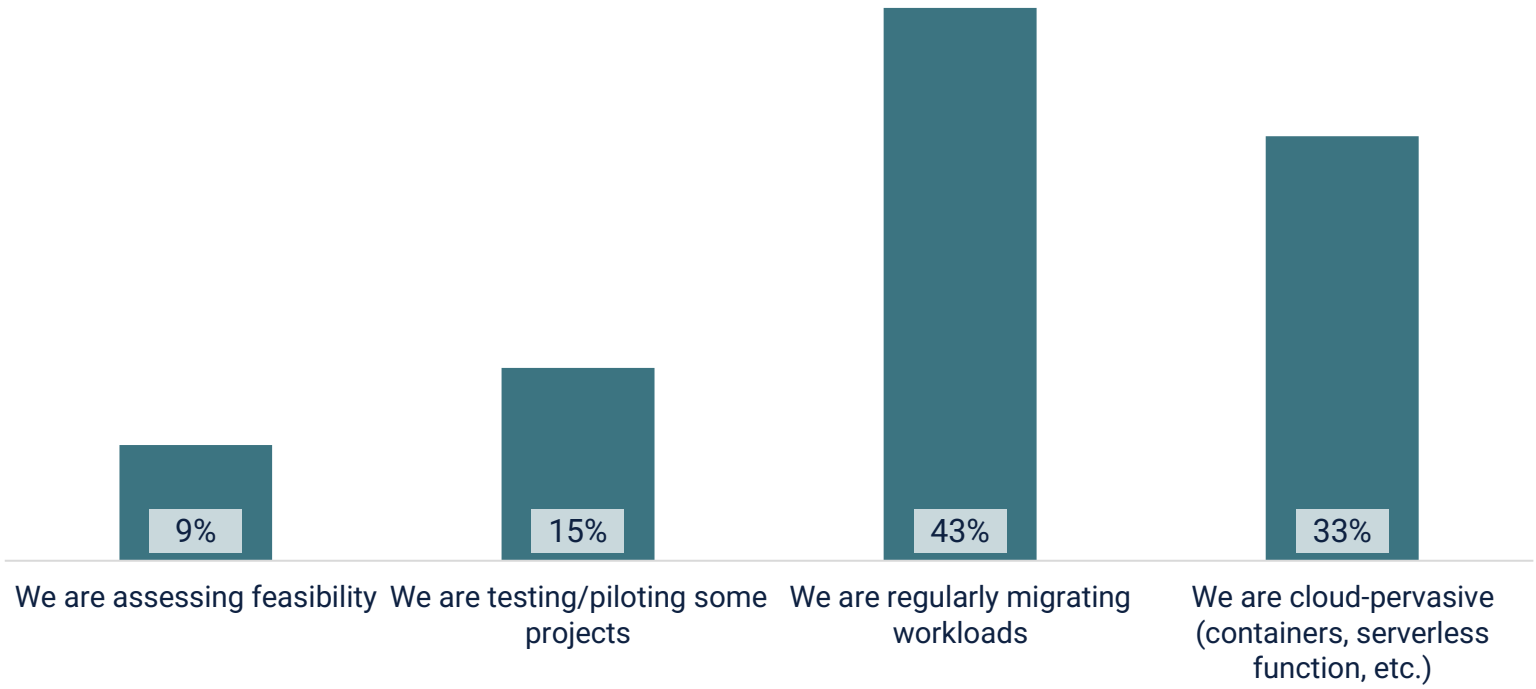
# EXECUTIVE SUMMARY

Many organizations are still progressing in their cloud adoption journey, with hybrid cloud architecture being the most common setup. While endpoint detection and response (EDR) and vulnerability management are widely used for cloud security, broader cloud-native security solutions like CNAPP and CSPM are less prevalent. Artificial intelligence is increasingly utilized, with managed services and custom AI models enabling both convenience and customization, though a lack of AI-specific expertise remains a challenge. To secure AI, organizations prioritize data privacy, threat visibility, and ease of integration, supported by practices like tenant isolation and regular audits.

This survey asks respondents to report:

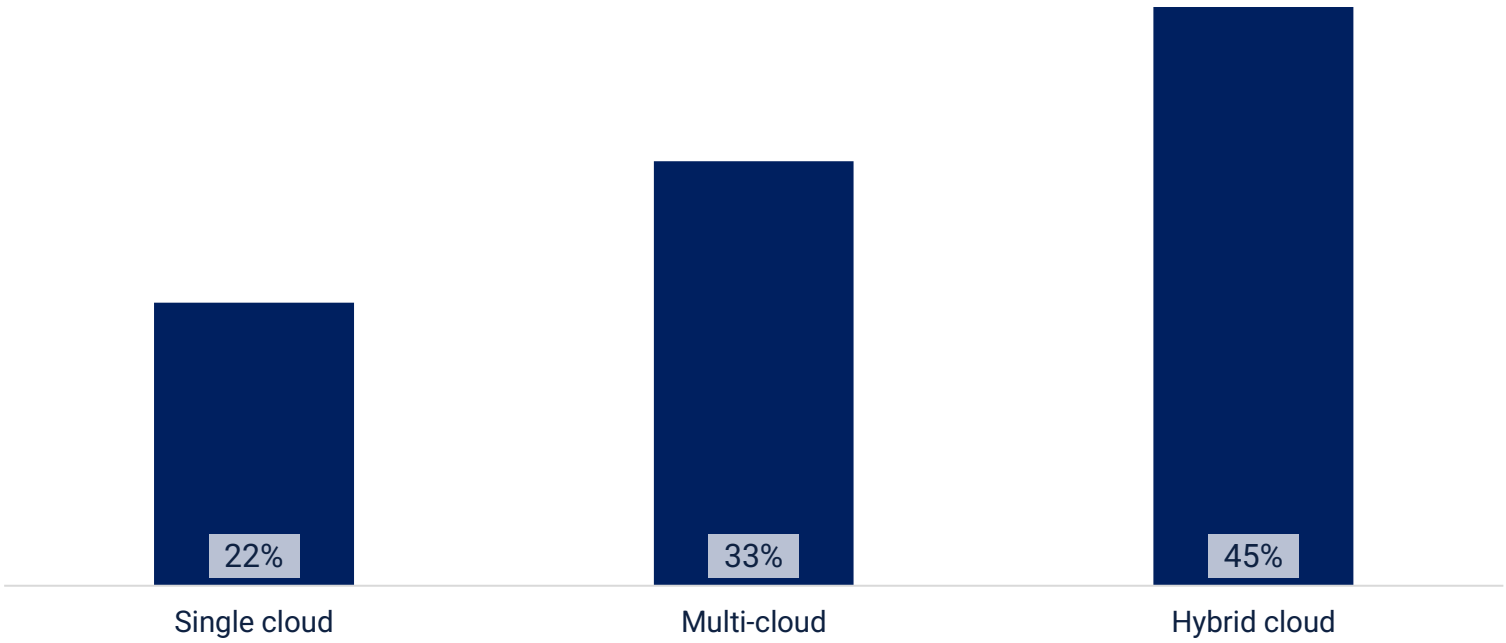
- Where are you at in your cloud journey? What does your cloud architecture currently look like?
- How is your organization using AI currently?
- What is the top AI security challenge in your organization?
- What strategies are you implementing to manage AI security risks?

# Where are you at in your cloud journey?



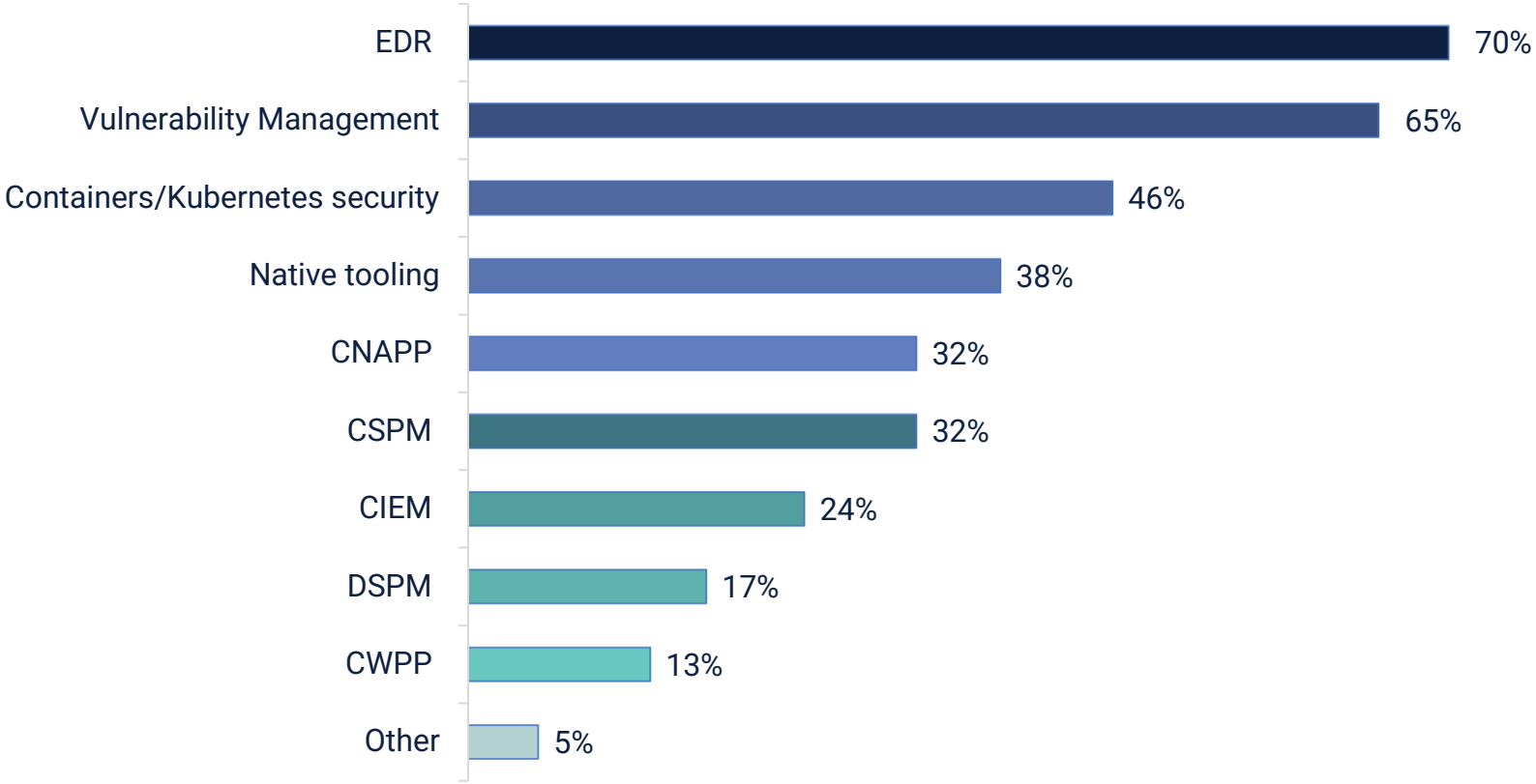

*Only a third of surveyed organizations are currently cloud-pervasive. Many (43%) are consistently transferring applications, data, and processes to the cloud, and just over a quarter are in the beginning stages of their cloud migration journey.*

# What does your cloud architecture currently look like?



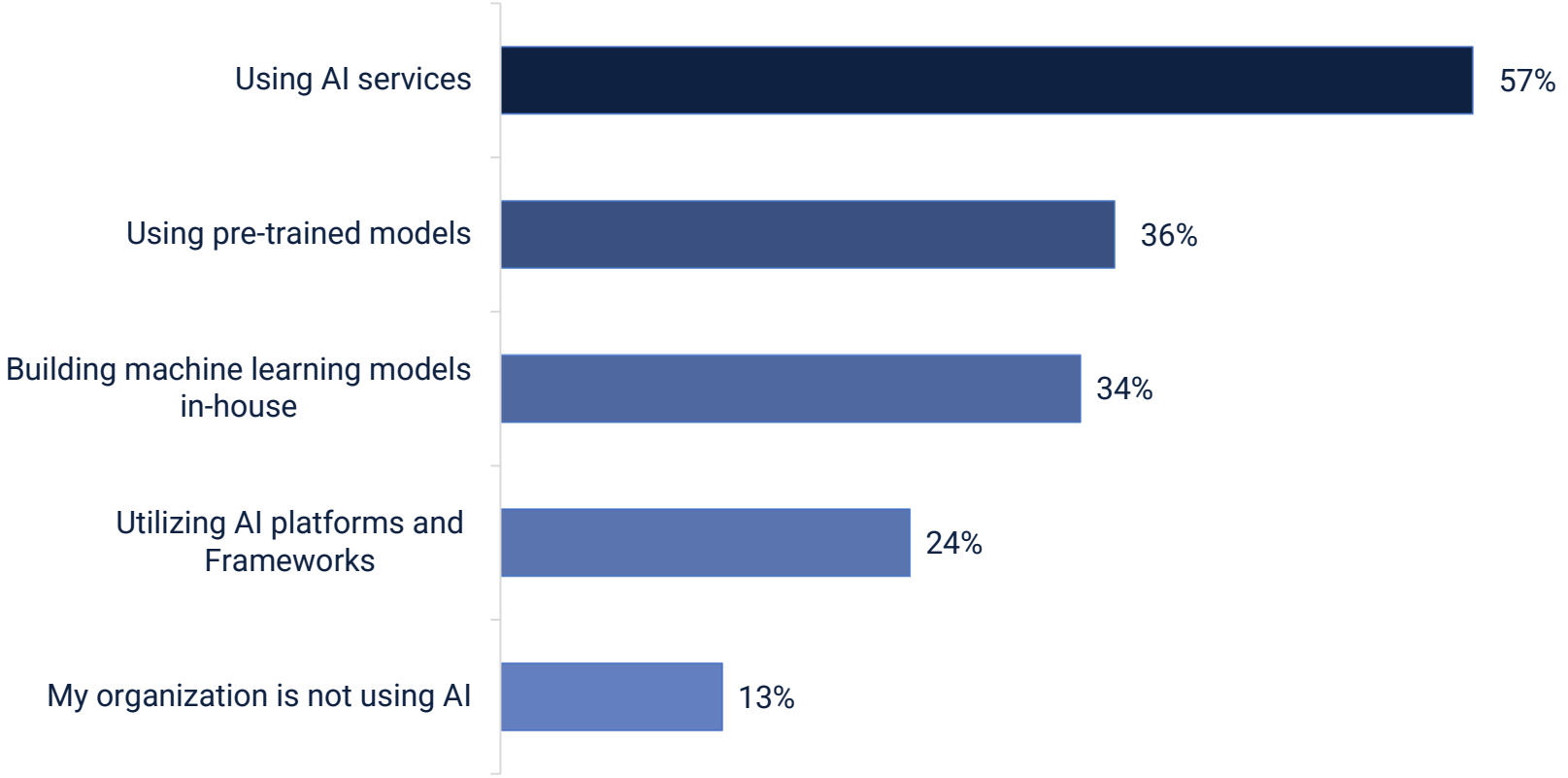

*Hybrid cloud architecture is most prevalent among respondents, cited by 45%. A third use multi-cloud architecture and 22% utilize single cloud.*

# What type of cloud security do you have in place?



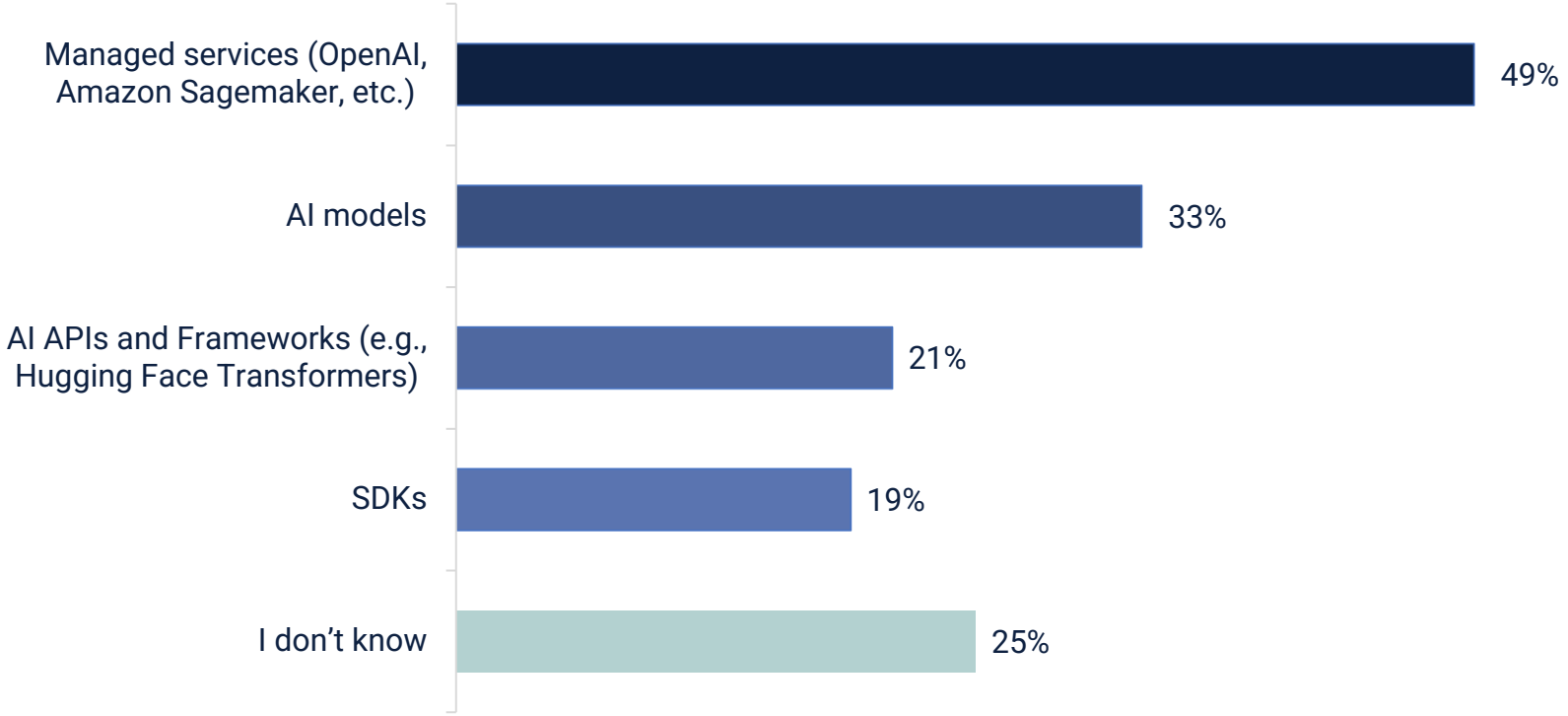

*Endpoint detection and response (EDR) (70%) and vulnerability management (65%) are the most popular types of cloud security currently in use. The use of products designed to broadly secure cloud ecosystems that focus on cloud-native challenges (CNAPP, CSPM, etc.) are not as widespread.*

# How is your organization using AI currently?



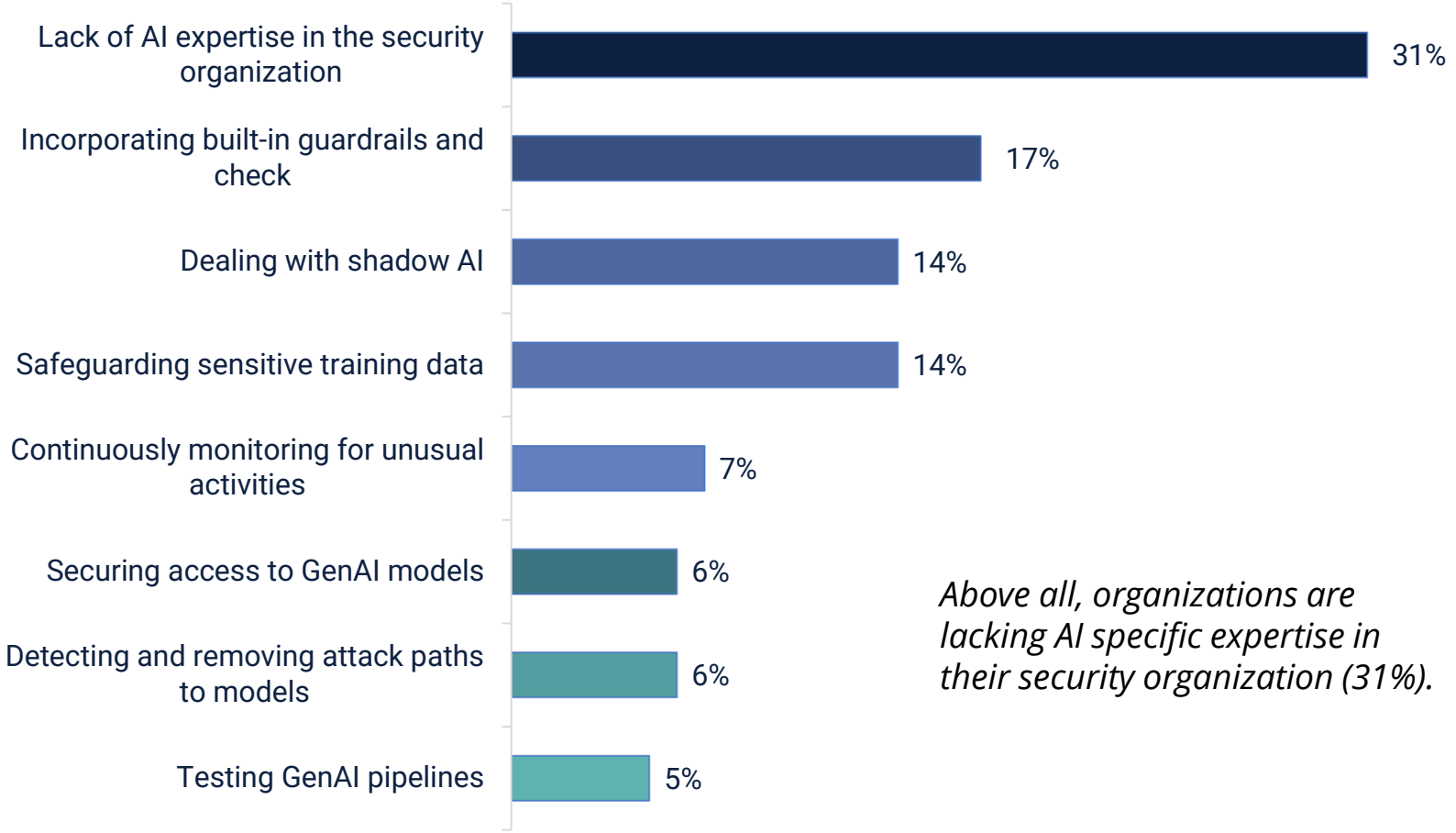

*Use of Artificial Intelligence is becoming more widespread: only 13% report their organization does not use AI. AI is most commonly used through services such as OpenAI, Amazon Bedrock, etc. (57%).*

# What AI services and technologies are currently running in your environment?



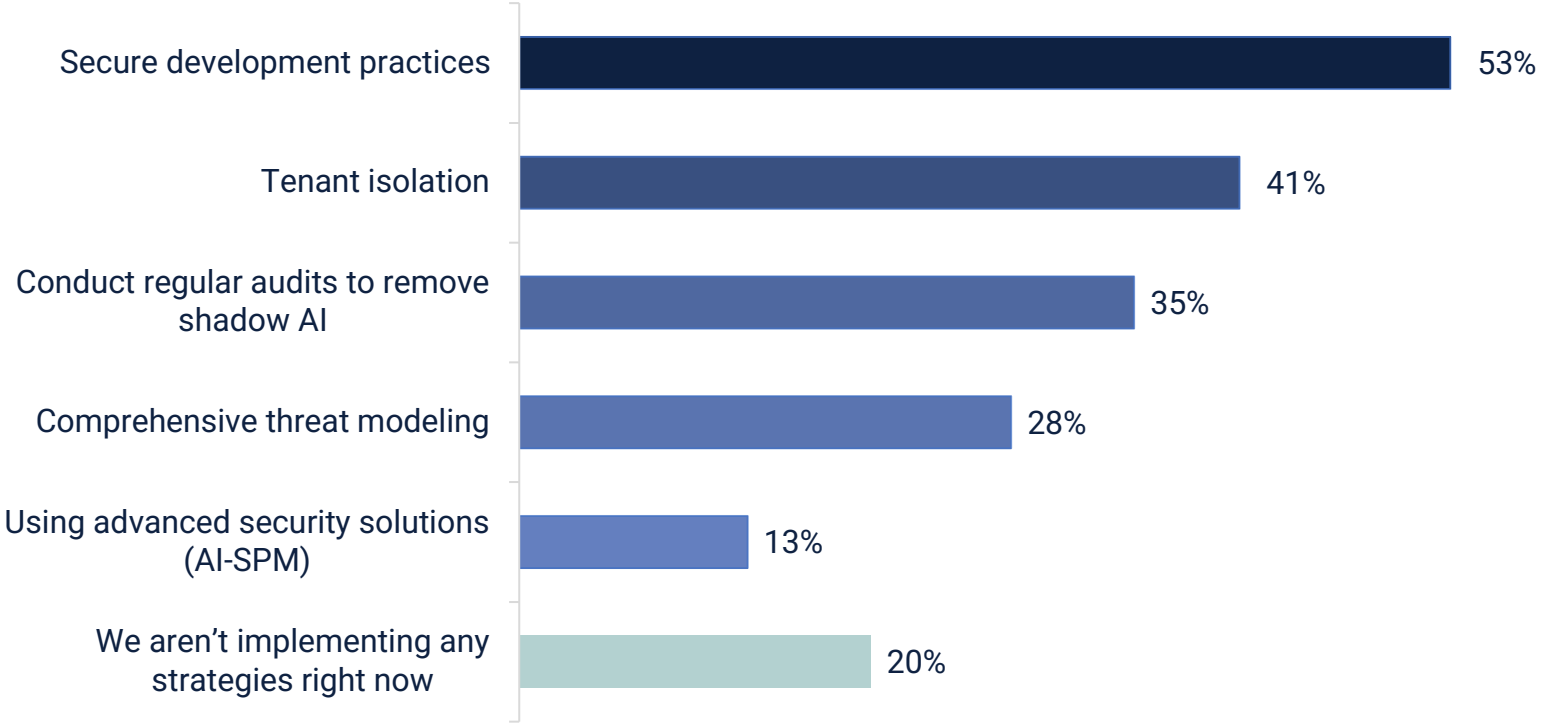

*Organizations are leveraging both convenience and customization in their environment through managed services (49%) and custom AI models (33%).*

# What is the top AI security challenge in your organization?



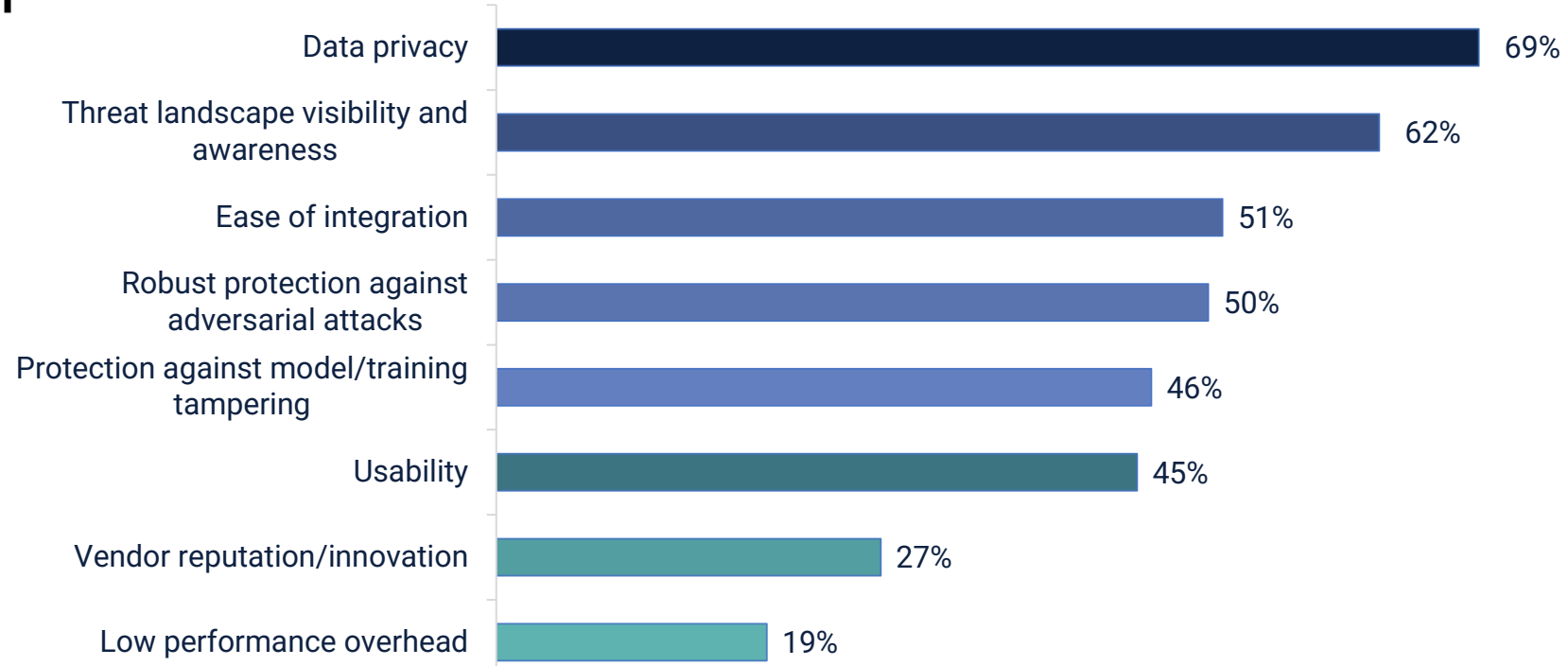

*Above all, organizations are lacking AI specific expertise in their security organization (31%).*

# What strategies are you implementing to manage AI security risks?




*Over half are using secure development practices to manage AI security risks. Tenent isolation (41%) and regular audits to remove shadow AI (35%) round out the top three security strategies currently in use.*

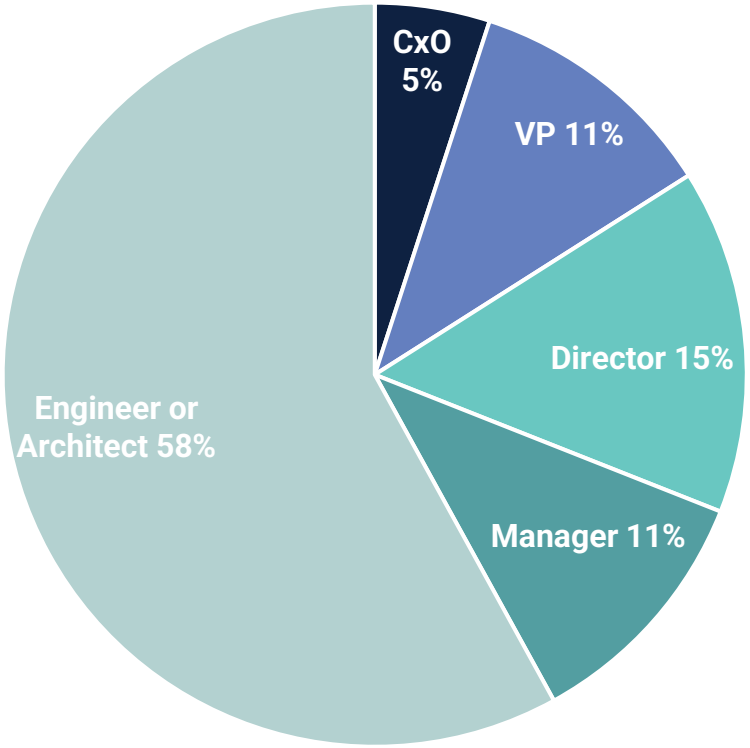
# What key features would you look for in a new AI security solution to enhance your security posture?




*When it comes to AI security solutions, organizations want data privacy features (69%) and threat landscape visibility and awareness (62%) over all others. At least half say they want a solution that is easy to integrate (51%) and robust protection (50%).*

# JOB LEVEL

*31% of respondents to this survey hold executive or director-level positions in their organization.*



## About the Company

Wiz offers a cloud security platform that ensures comprehensive protection for everything built and run in the cloud. It provides full-stack visibility across AI services, virtual machines, containers, and serverless without agents. By creating a single prioritized risk queue, Wiz helps teams proactively reduce the attack surface, enabling coordinated security from development to runtime

Learn more at wiz.io