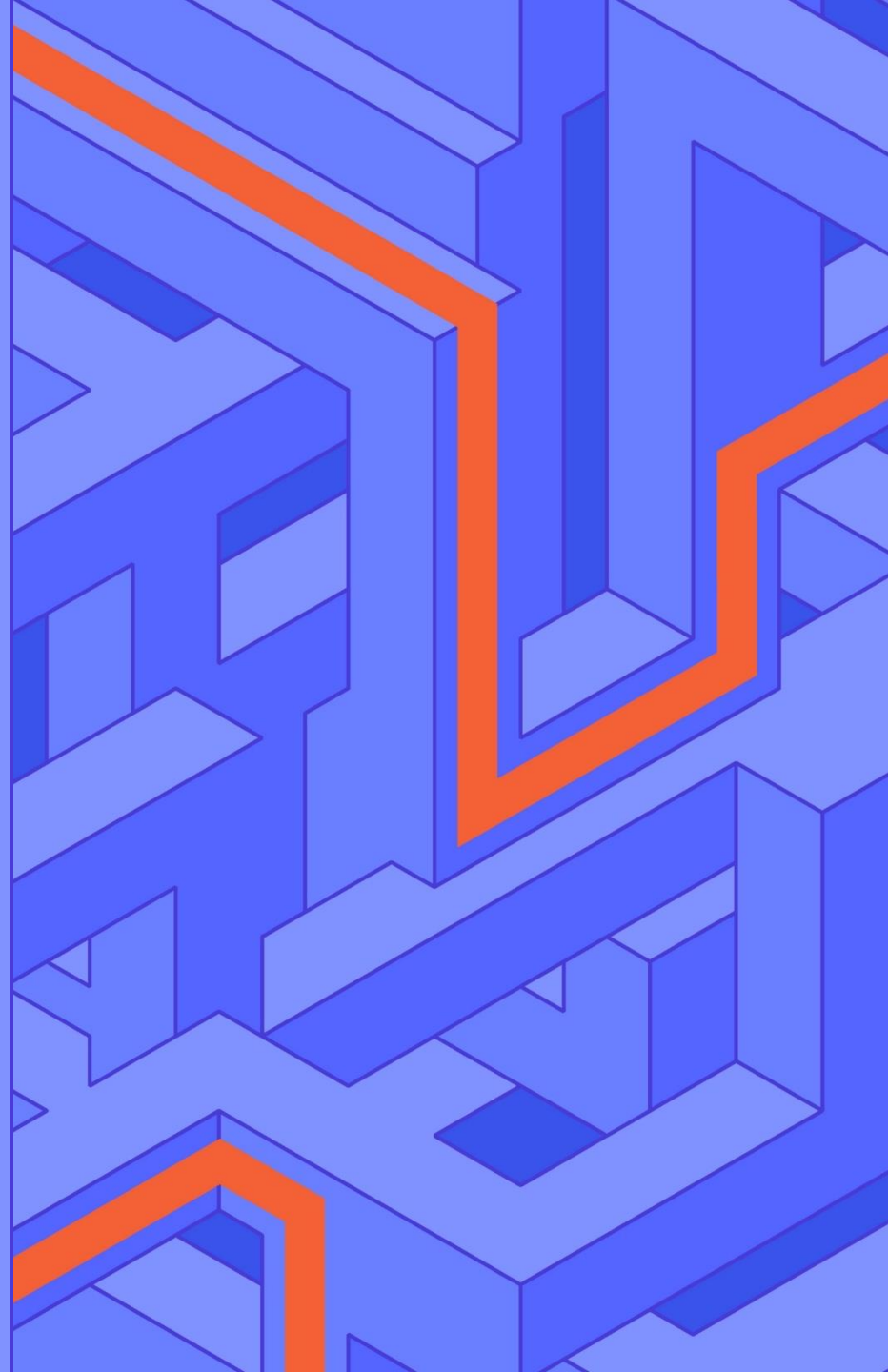
SPECTEROPS | OMDIA

Trends in Identity Attack Path Management

Executive Summary

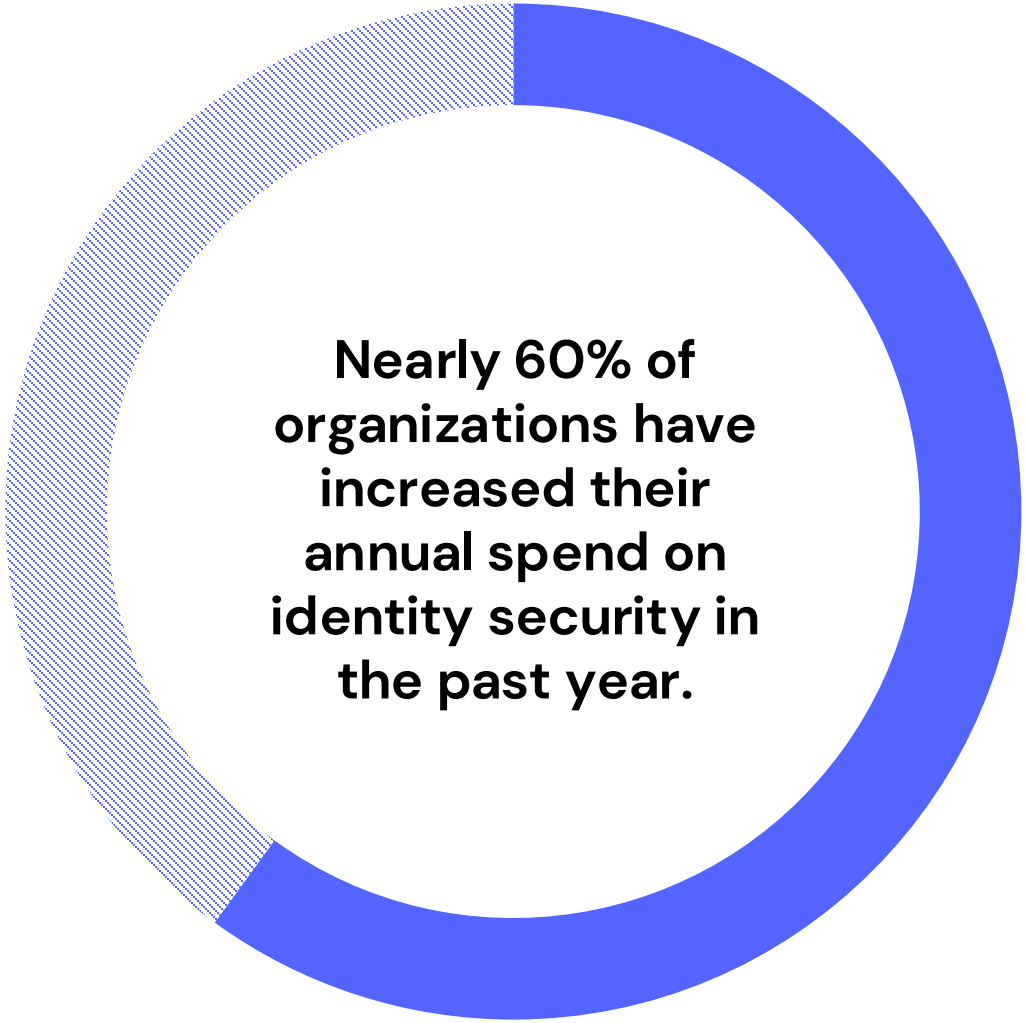


Key findings

Identity security is a top priority in an increasingly complex threat landscape.

Nearly 60% of organizations have increased their annual spend on identity security in the past year, and enhancing visibility into attack paths is ranked as the third-highest cybersecurity priority over the next year.

Organizations are shifting toward proactive identification and mitigation of vulnerabilities – emphasizing the need for an integrated, risk-based solution to address evolving threats. The scale of the problem is immense, with
100% of respondents reporting at least one security incident in the past 12 months.



Key findings

The foundations for identity-based attack path management solutions are wholly in place.

Organizations aren't just sitting idle: **59% report they are actively researching or have already implemented an identity-based attack path management solution**.

There is measurable opportunity for startups to innovate more quickly and deliver real-time attack path visibility to help meet this need.

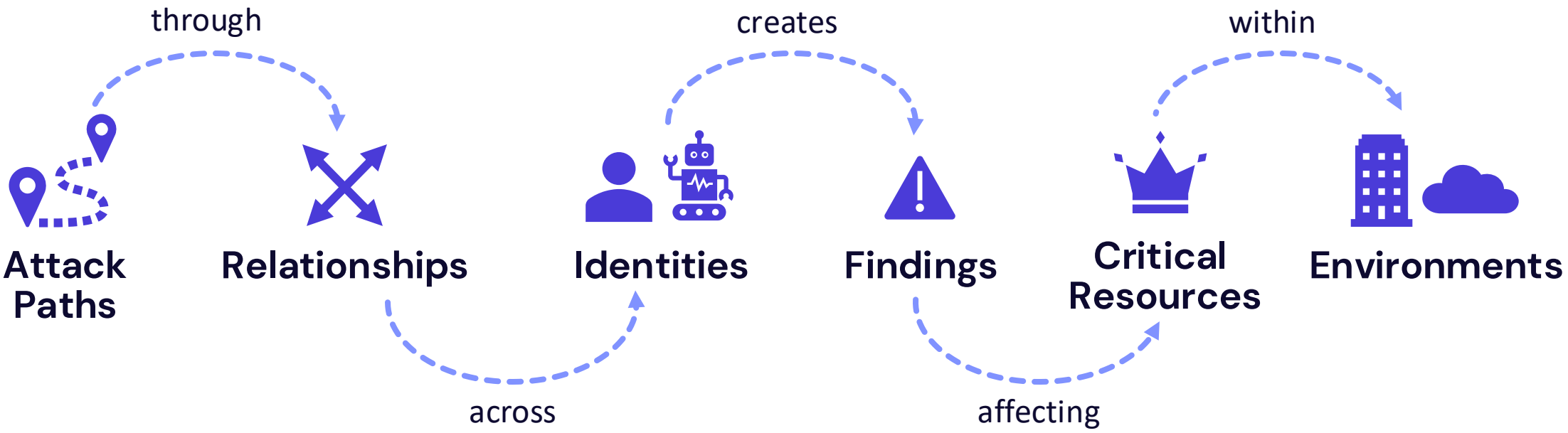
The need for integration drives collaboration between IT and security teams.

More than half of organizations rank APM integration with other security tools as a top priority for the next year.

This increase in integration demands a higher level of collaboration between IT and security teams – which respondents tell us is a main benefit they expect a successful APM process to have.

Attack Paths are chains of abusable privileges and user behaviors that create connections between identities and resources.

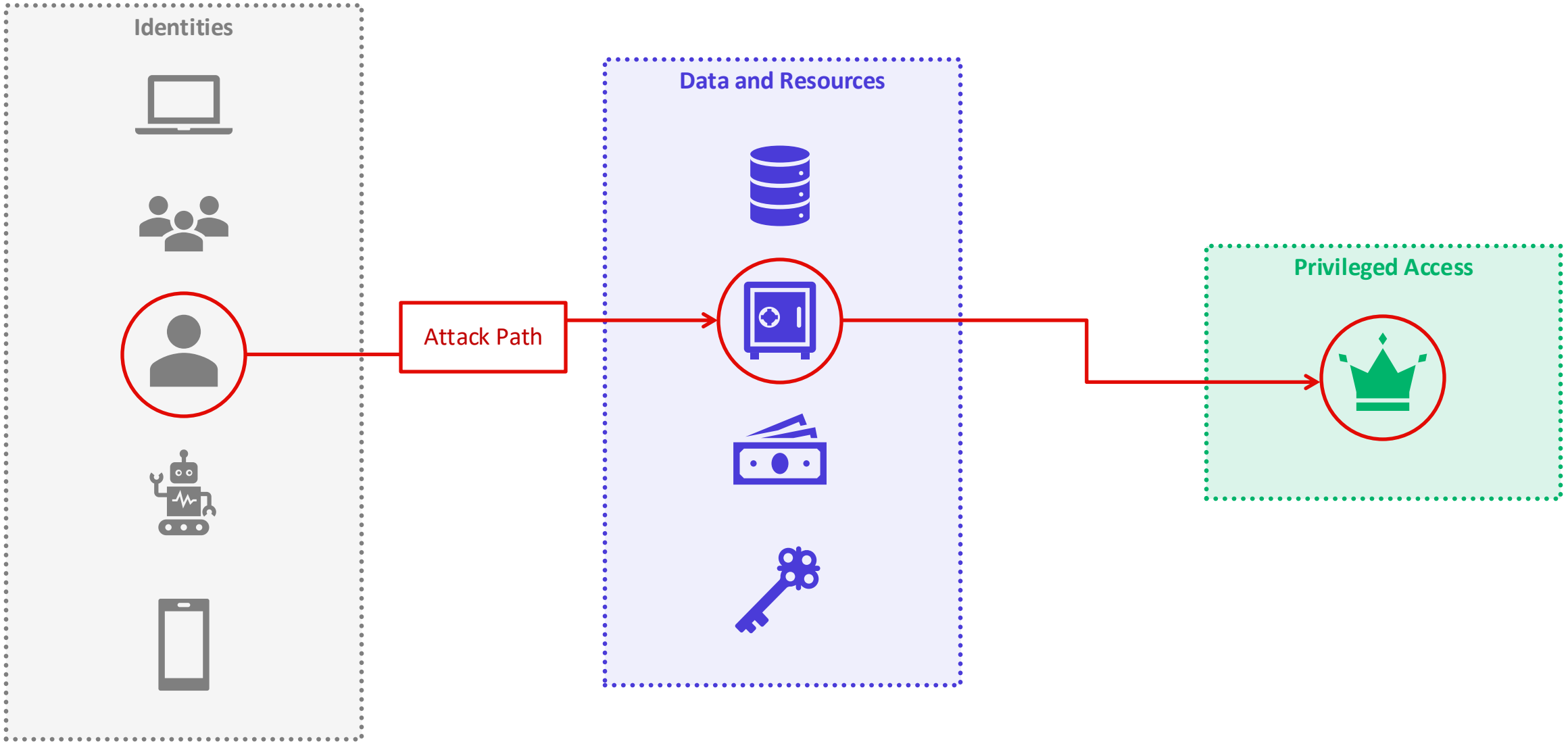
Understanding the problem



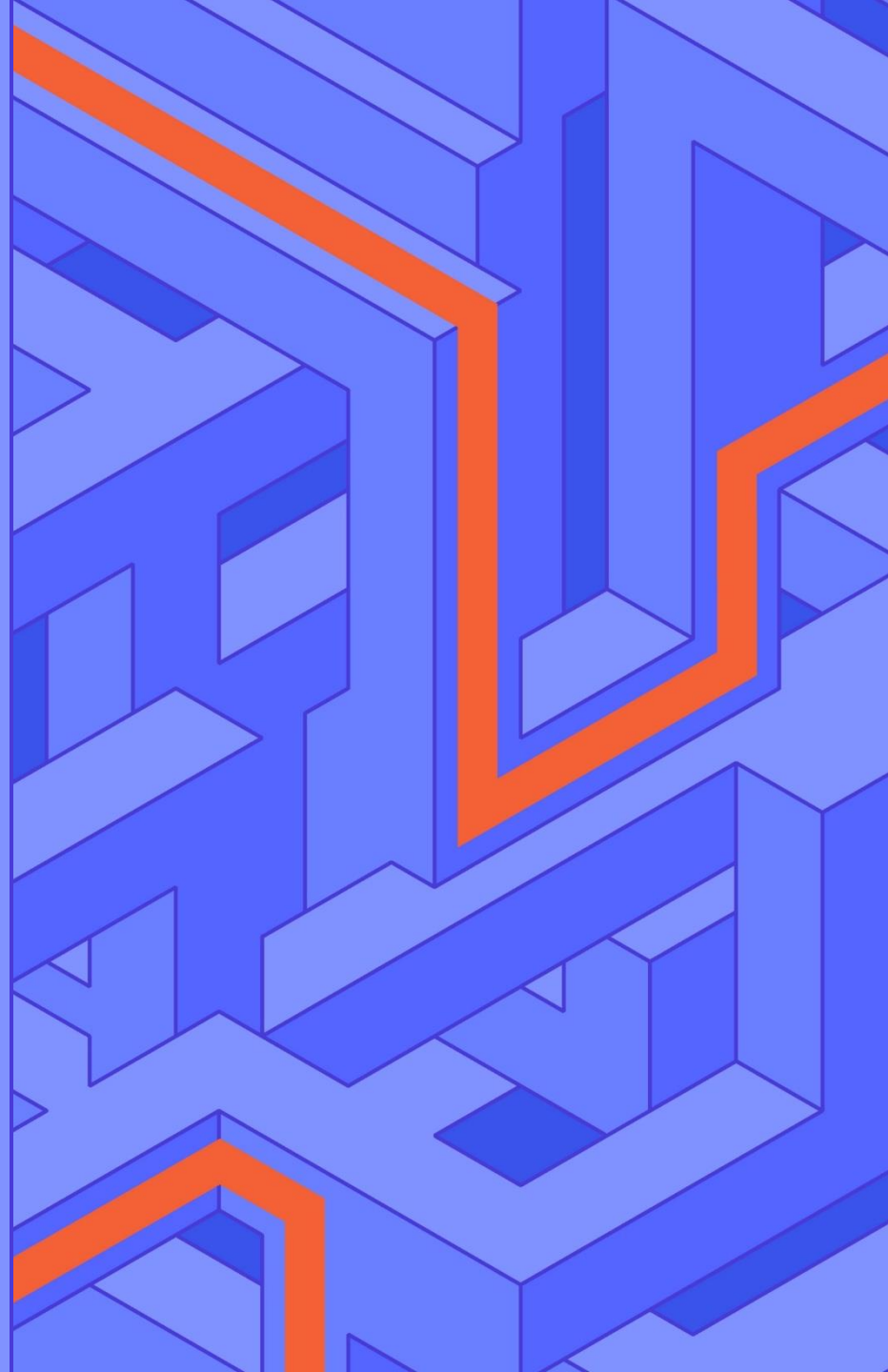
5K Identities = 5 Million Attack Paths **5M**

More Identities

More Attack Paths

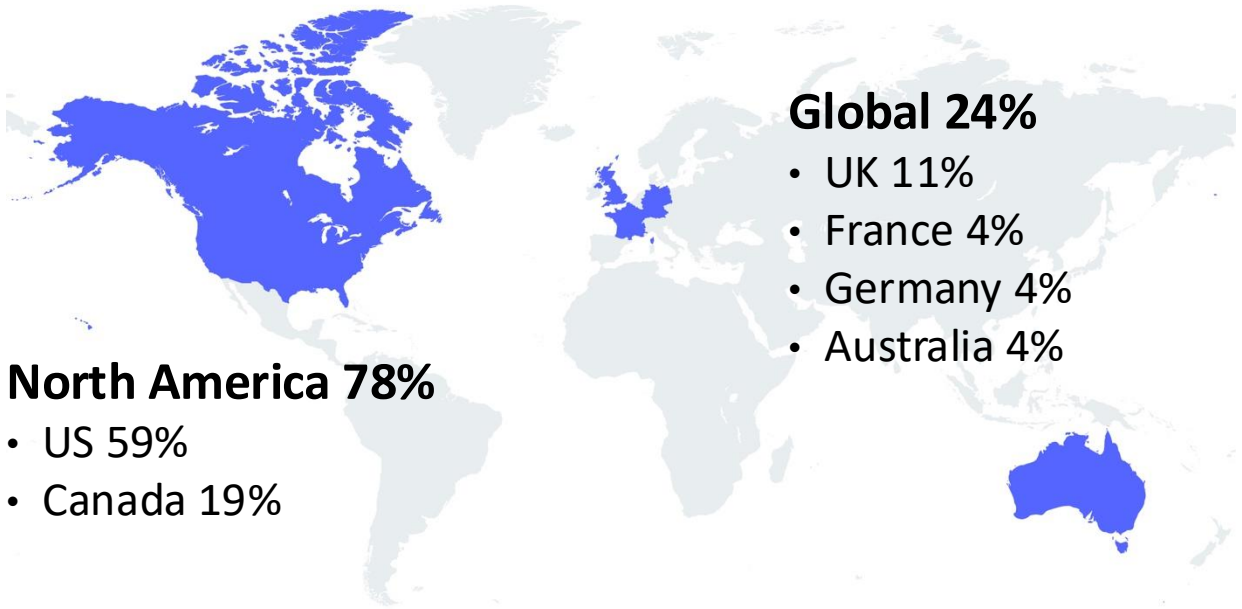

Identities
Attack Path
Data and Resources
Privileged Access

Demographics



Respondent firmographics

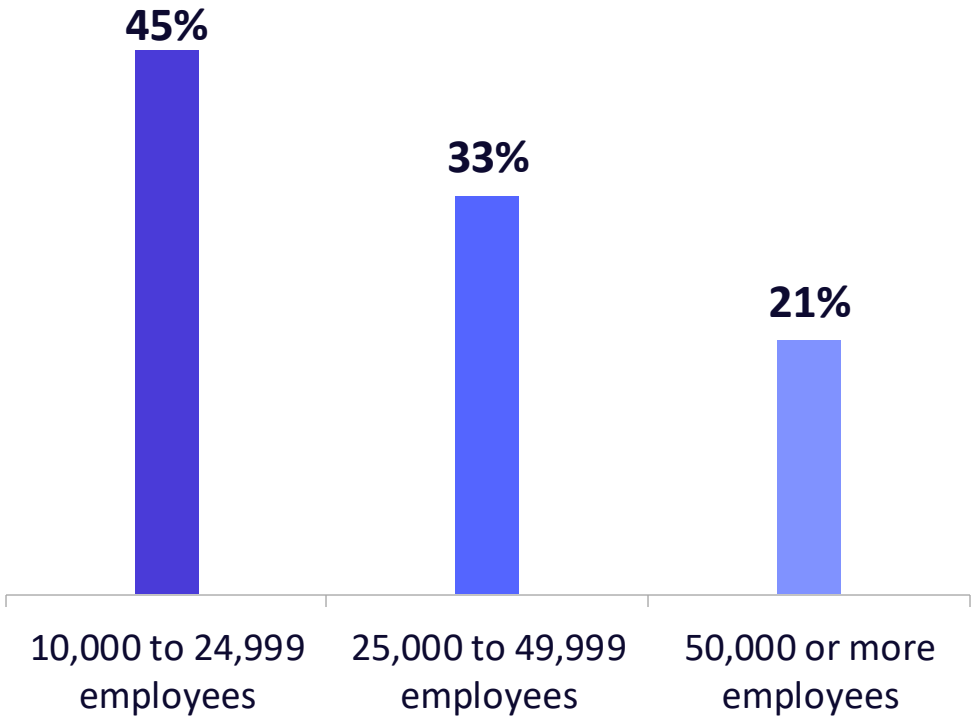
Geography



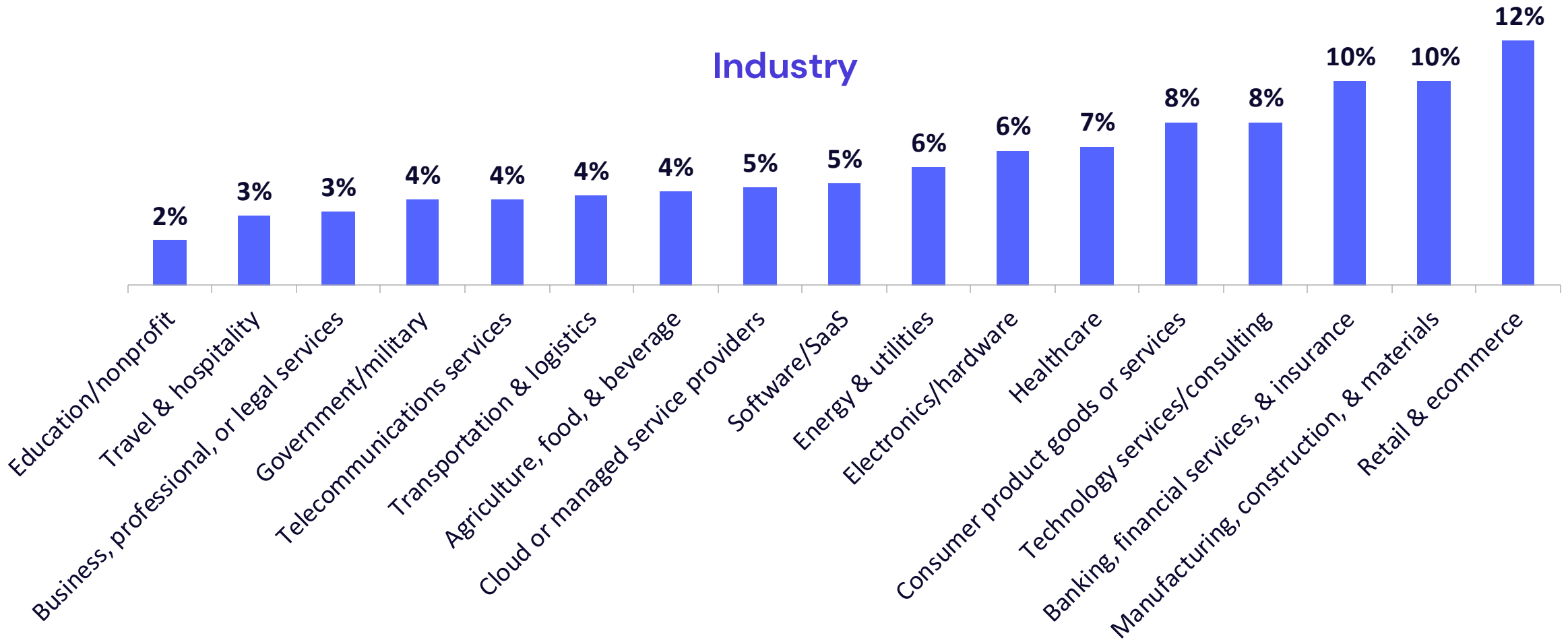
North America 78%
- US 59%
- Canada 19%

Global 24%
- UK 11%
- France 4%
- Germany 4%
- Australia 4%

Company Size



Respondent firmographics

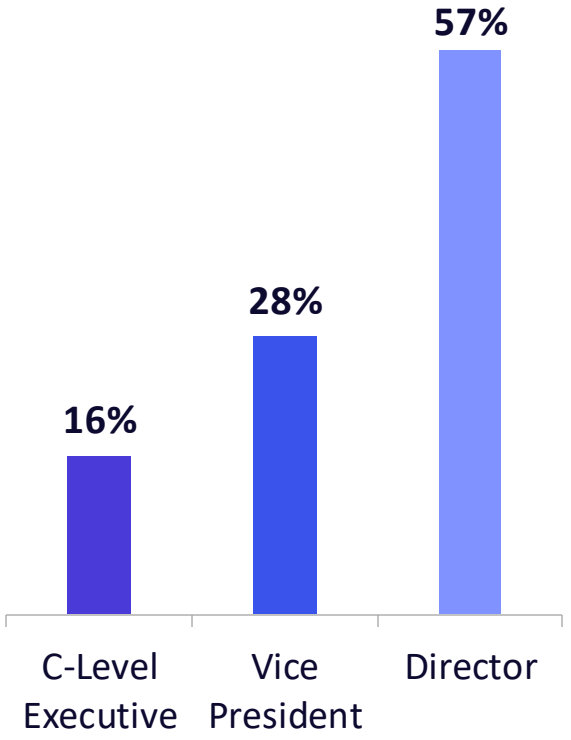


Respondent demographics

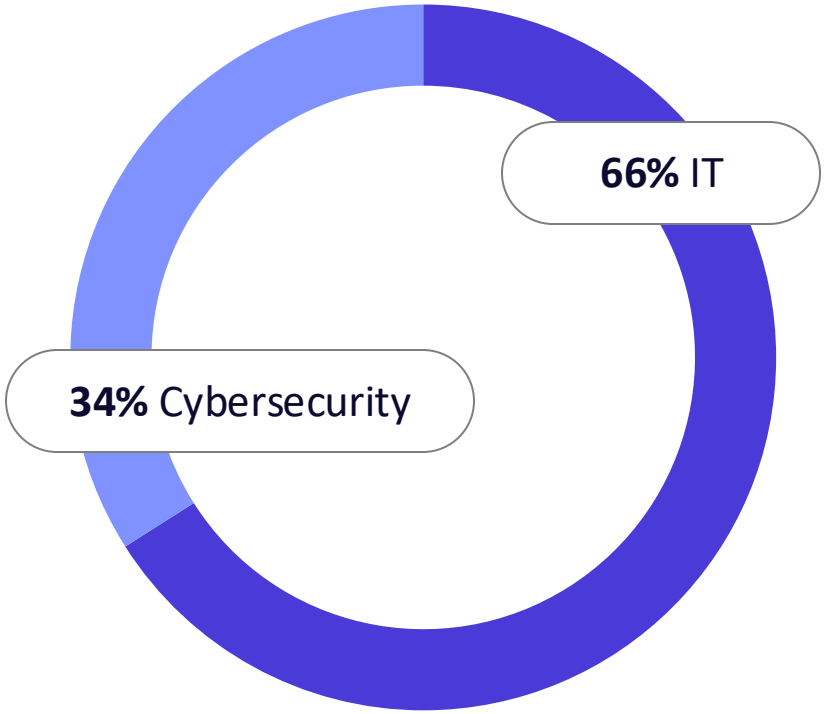
Respondents must have **decision-making capability** (final decision maker, part of a team, or a decision influencer) for at least one of the following in order to qualify:

- Domain/system management strategy
- Domain/system solution procurement
- Cybersecurity strategy
- Cybersecurity purchasing decisions
- Identity and access management (IAM) decisions
- Microsoft, Windows, or directory services strategy

Level



Department

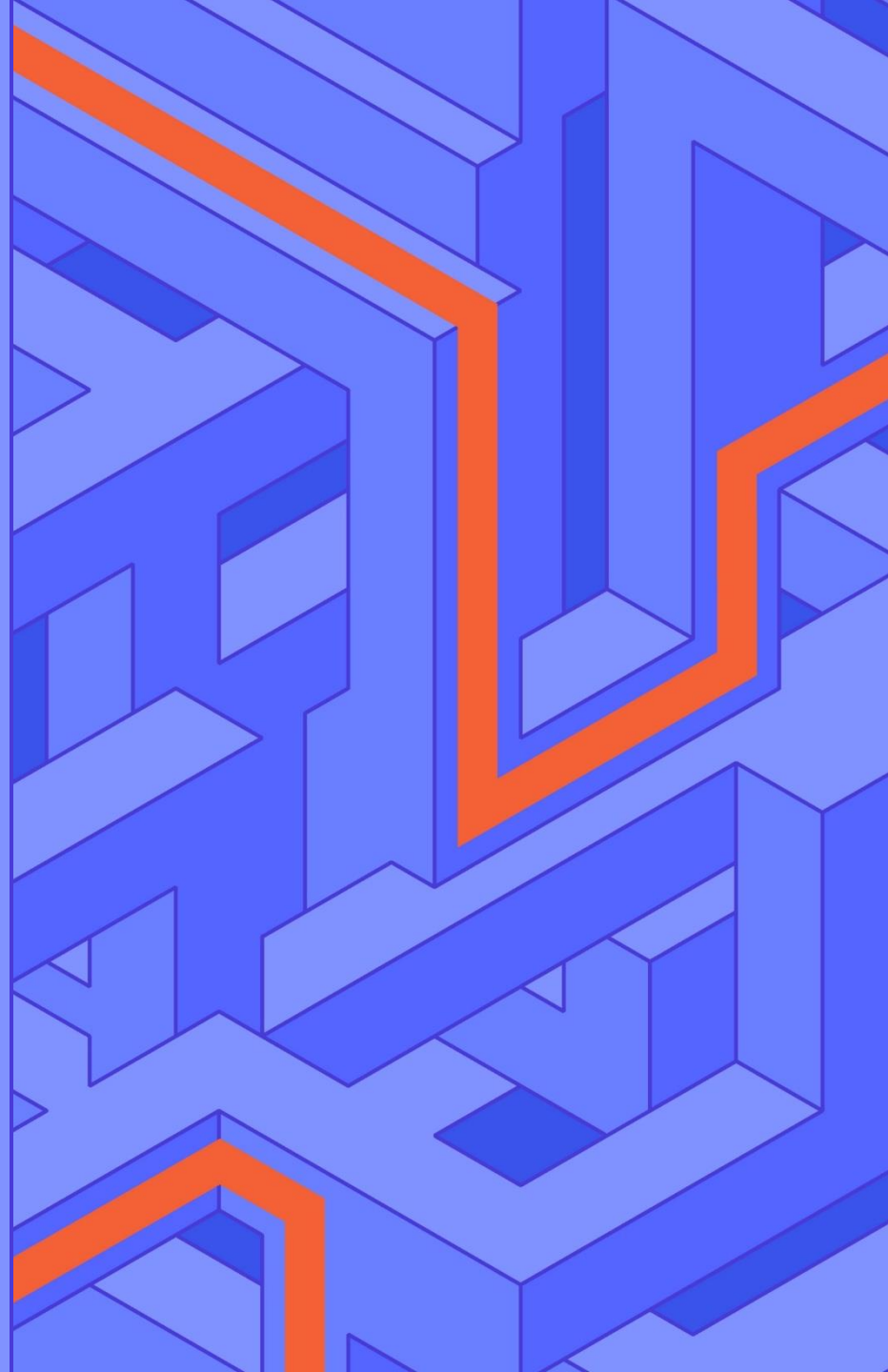


Overall Priorities and Journey

Data Review

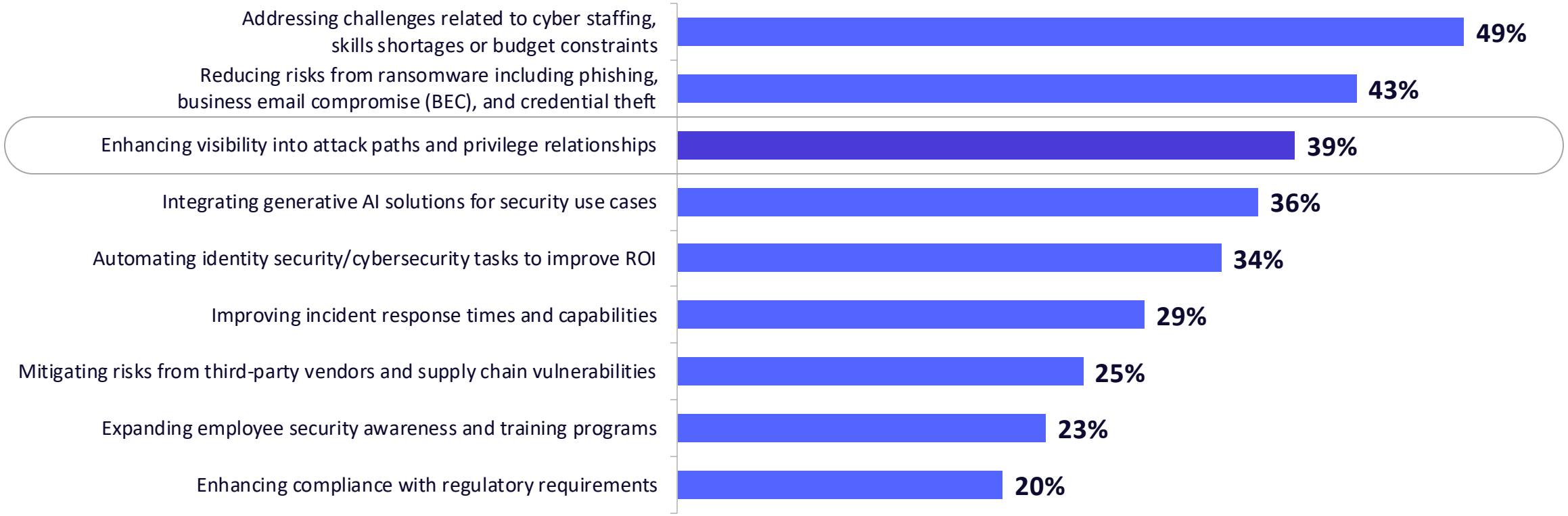
The data within this report shows the rising concern around identity security, and gives some insights into the time, budgets and key implementation concerns Identity and Security leaders have when starting or continuing their Attack Path Management journey.

For example, the rise of identity risk is their top priority over the next 3-5 years. Furthermore, the problem is expanding, and many leaders are already looking for solutions and beginning to create strategies for success.



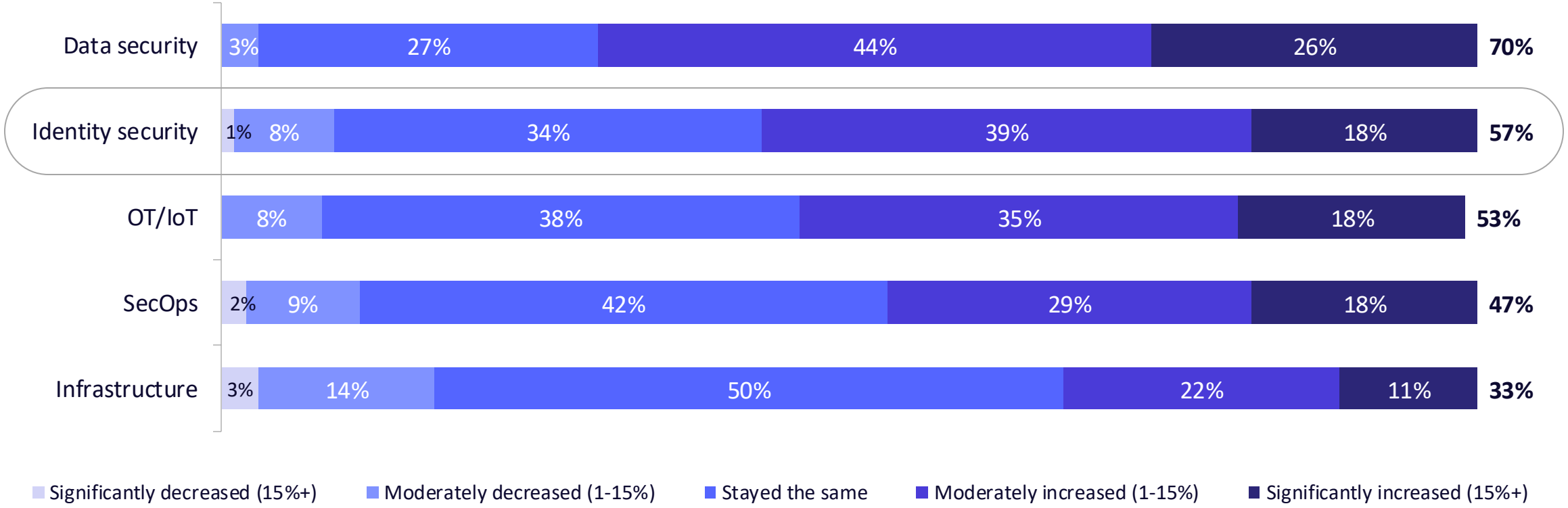
Top Priorities? Attack path visibility is second only to staffing/skills and security incident reduction

What are your organization's top cybersecurity priorities over the next 12 months?



Almost 60% of organizations have increased their identity security spend over the past year

For each of the following security technology categories, how has your organization's spending changed compared to this time one year ago?

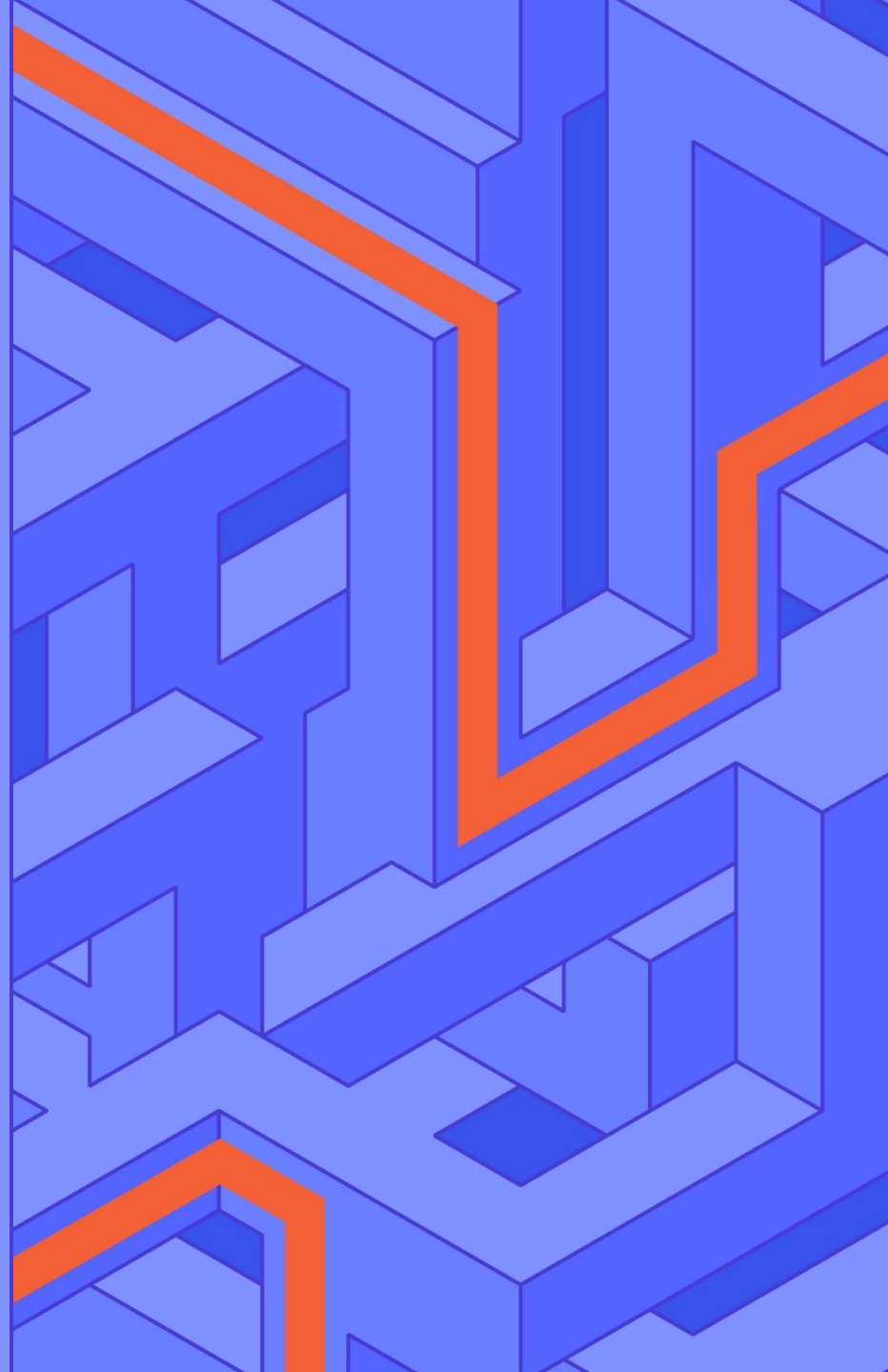


Current State of Identity Practices

Data Review

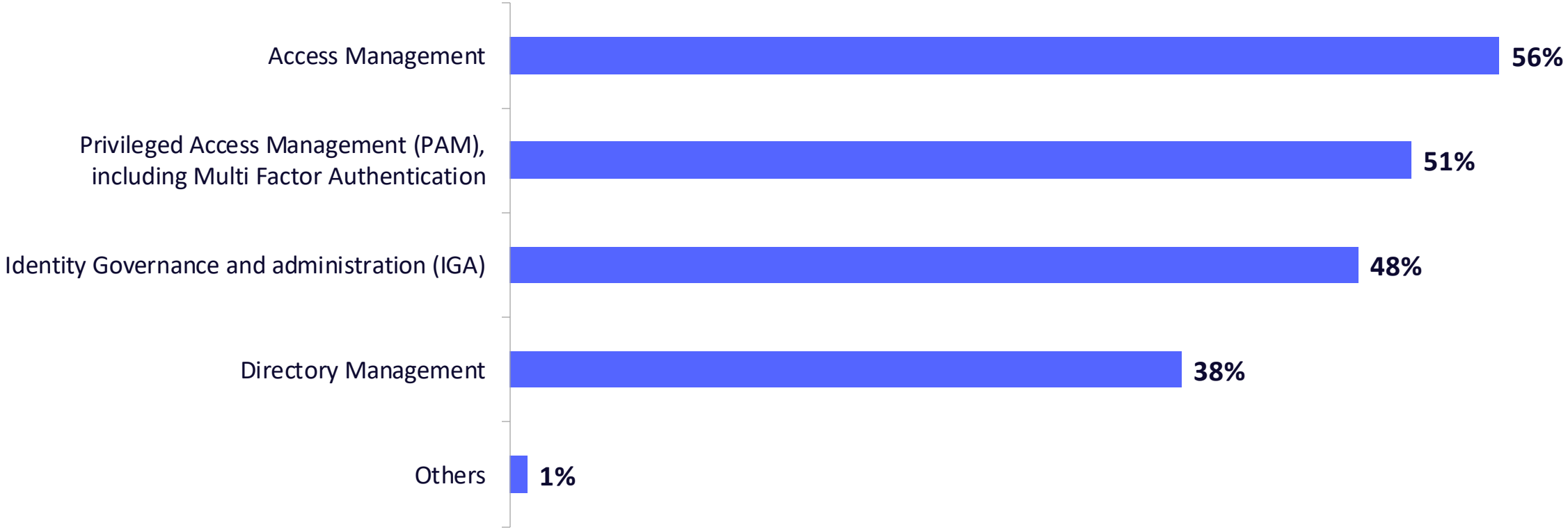
How are organizations mitigating attack paths? Most currently use EDR tools, followed by PAM and IAM. But these tools, while necessary to combat other problems with identity, have gaps in coverage when it comes to Attack Path Management.

Part of mitigation is remediation—but there's not always a clear path. Remediations are usually identified by the security team, but at many organizations they are implemented by the IAM team or an IT Ops team. Organizations can benefit by designating an intra-team manager that ensures all sides are informed of critical issues, aware of remediations planned, and kept up to date on successes.



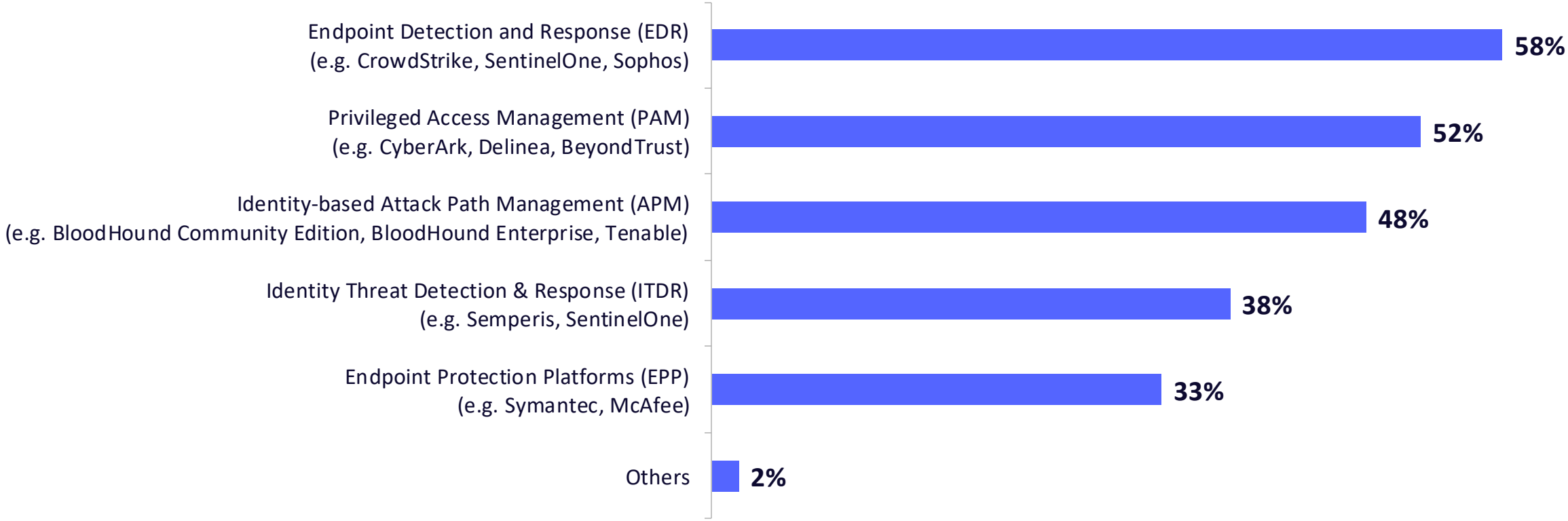
Access management and PAM are foundational components of an identity security stack

Which products are currently deployed as components of your identity security stack?



EDR and PAM are the most commonly-used approaches to securing identity directory services

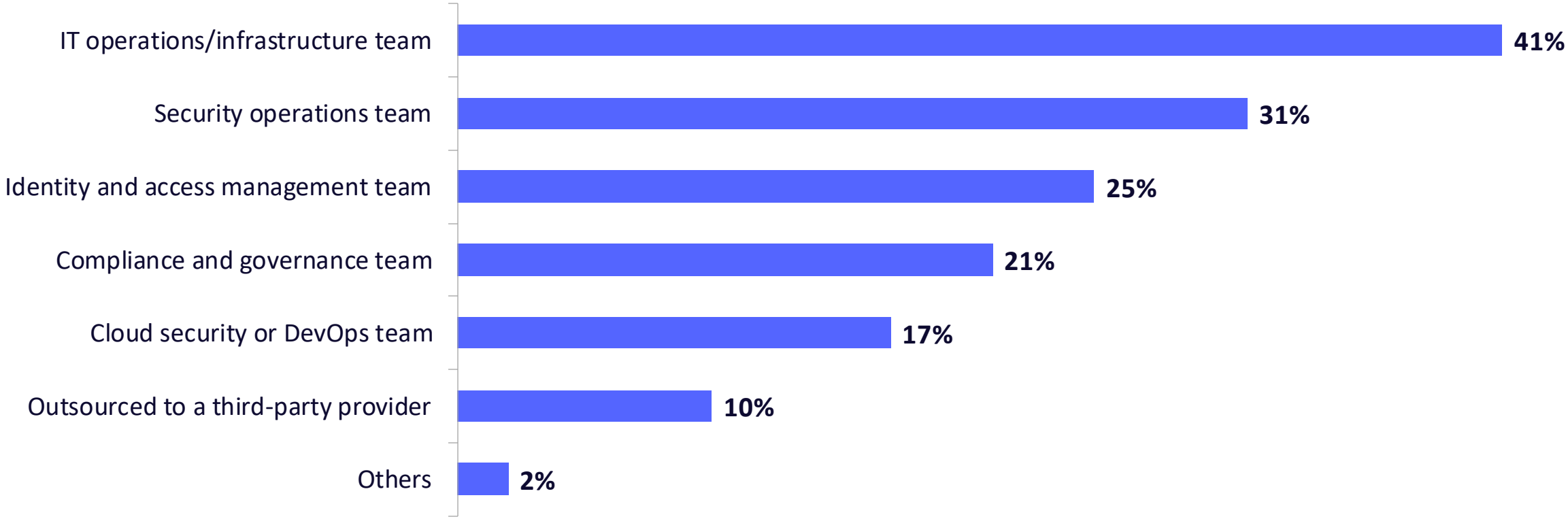
What products do you currently use to secure your identity directory services?



Breaches are inevitable, but impactful breaches are avoidable.

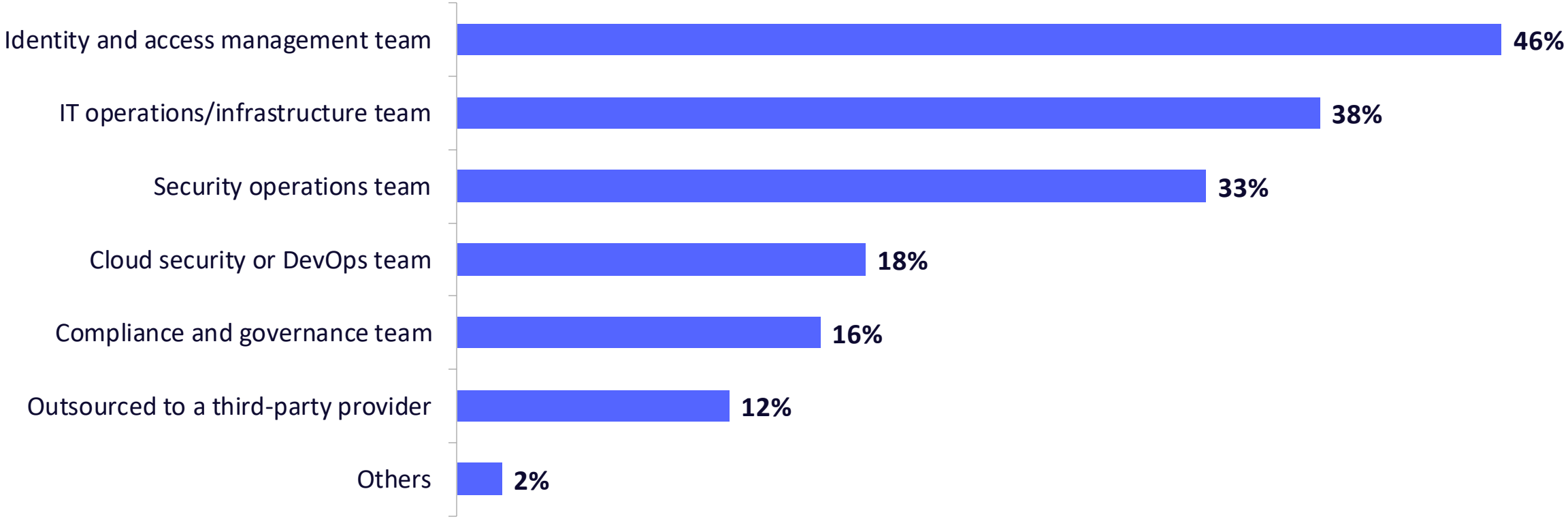
Infrastructure/operations teams are usually responsible for identity directory services…

Who is primarily responsible for identity directory services at your organization?



...whereas identity management typically gets its own specialized team

Who is primarily responsible for identity management at your organization?

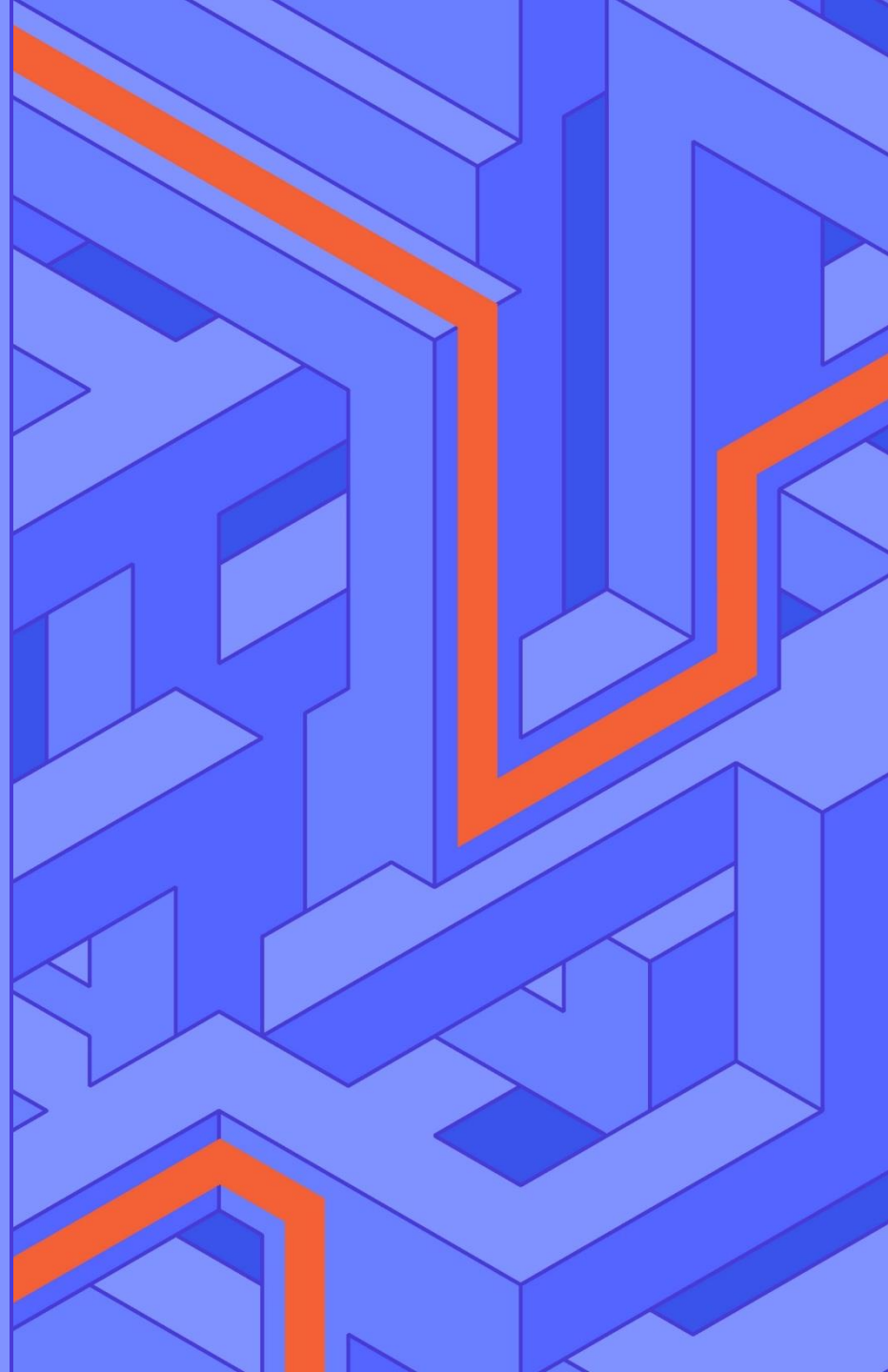


Challenges and Risks

Data Review

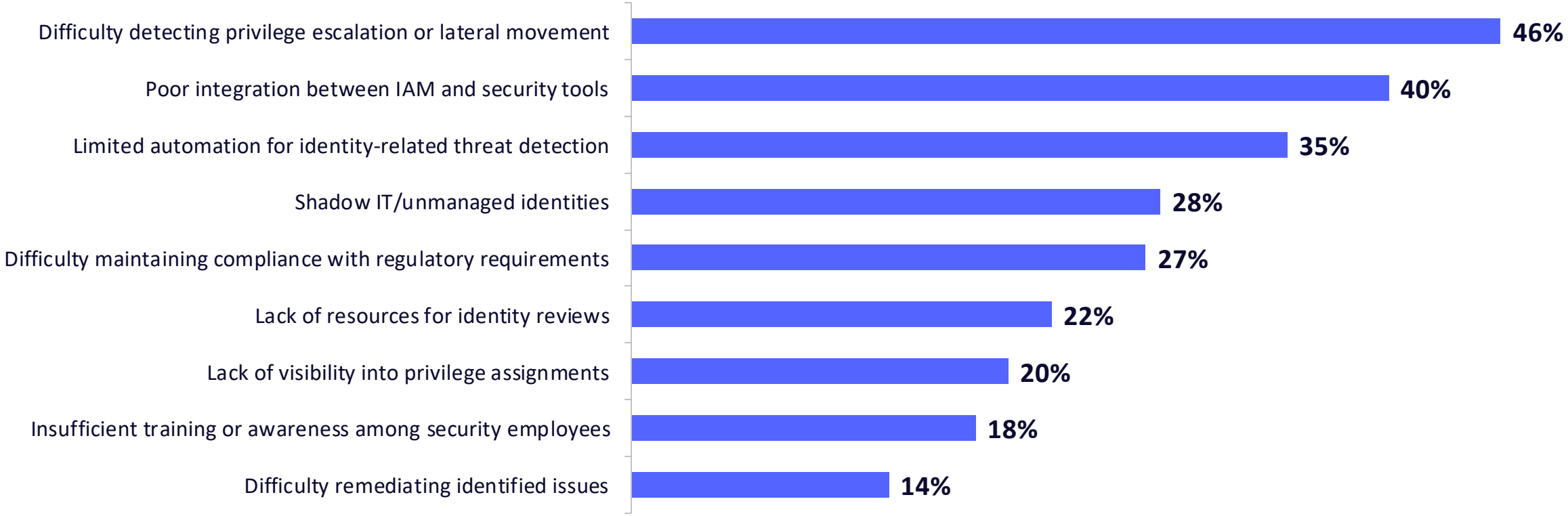
It’s apparent that most CIOs and CISOs are actively working on implementing attack path management, but there is no standard industry process for doing so. A lack of integration with other security tools and poor collaboration between IT and security teams seems to be holding many organizations back.

While identity risk is a growing concern, so is the adoption of new tools. Even though leaders seem to understand the risks and benefits of APM, the perceived complexity and possible shortcomings of APM tools may be scaring potential users away.



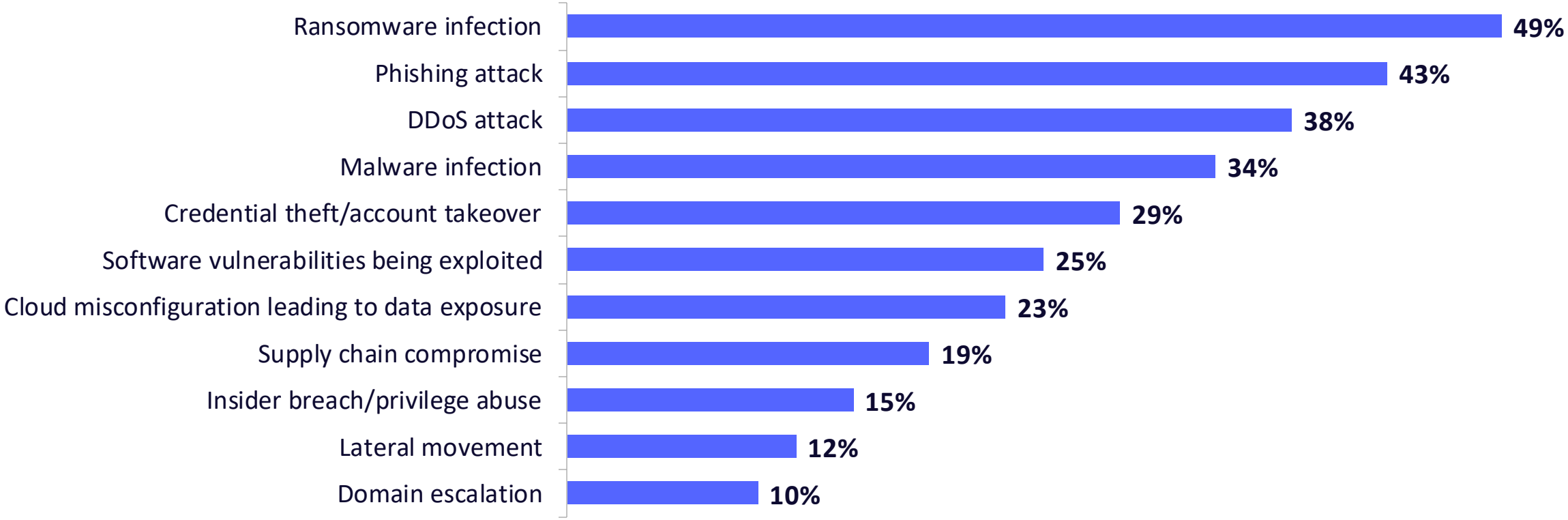
Detecting privilege escalation, integration, and automated threat detection are major hurdles to managing identity risk

What challenges does your organization experience with managing identity risk?



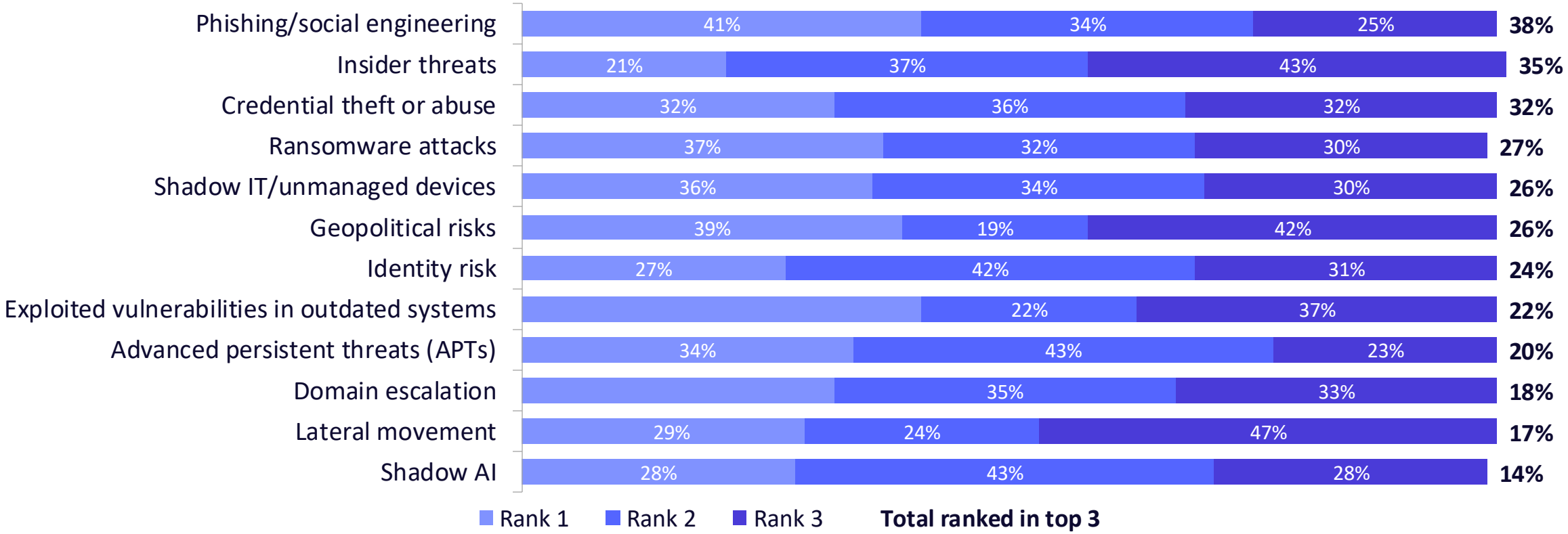
All respondents reported at least one security incident in the past 12 months

Which of the following security incidents has your organization experienced in the past 12 months?



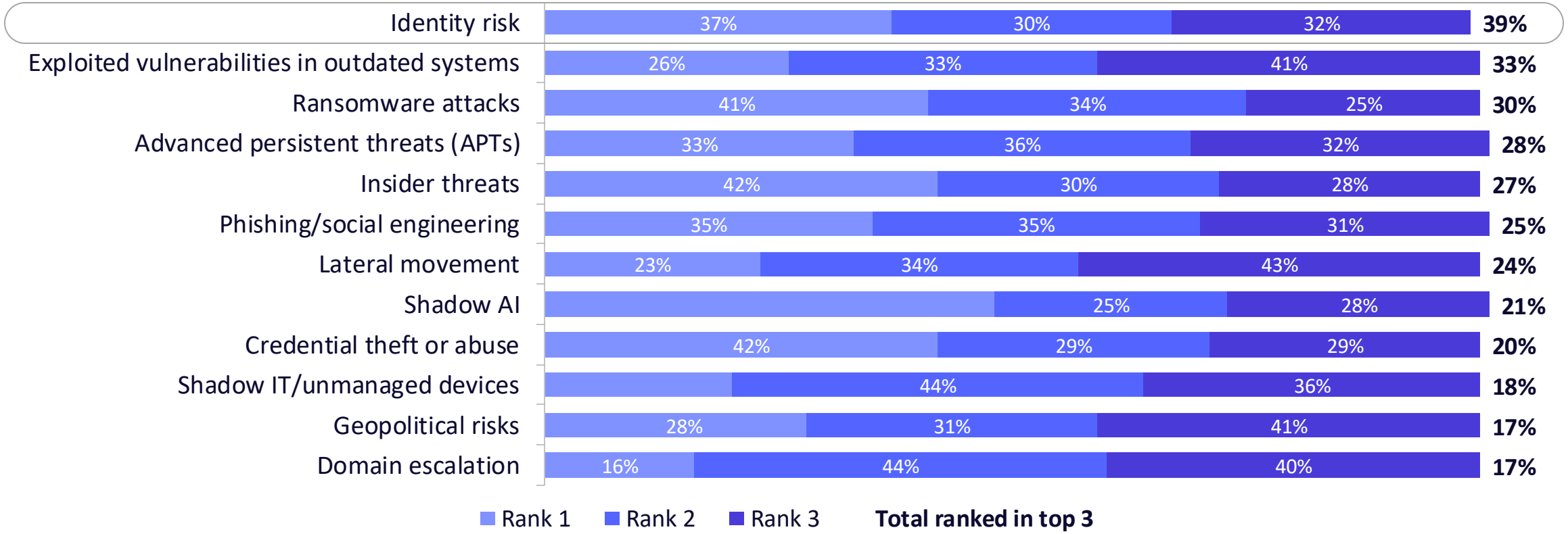
Phishing, insider threats, and credential theft/abuse dominate the current threat landscape

What are the top three most critical threats/vulnerabilities to your organization today?



Identity risk, exploiting outdated systems, and ransomware emerge as most critical in the near future

What are the top three most critical threats/vulnerabilities to your organization in 3-5 years?

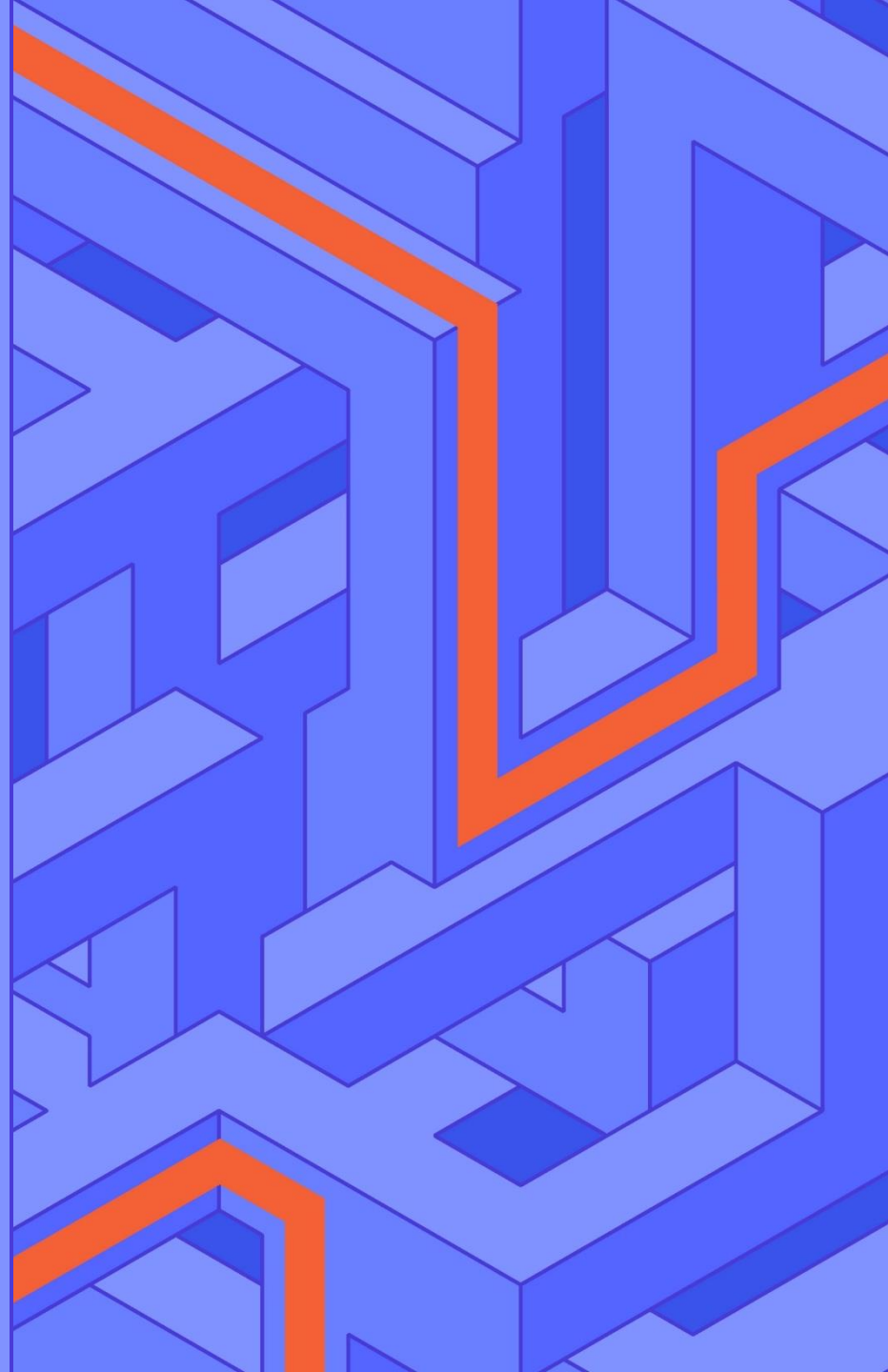


Understanding Identity-Based Attack Paths

Data Review

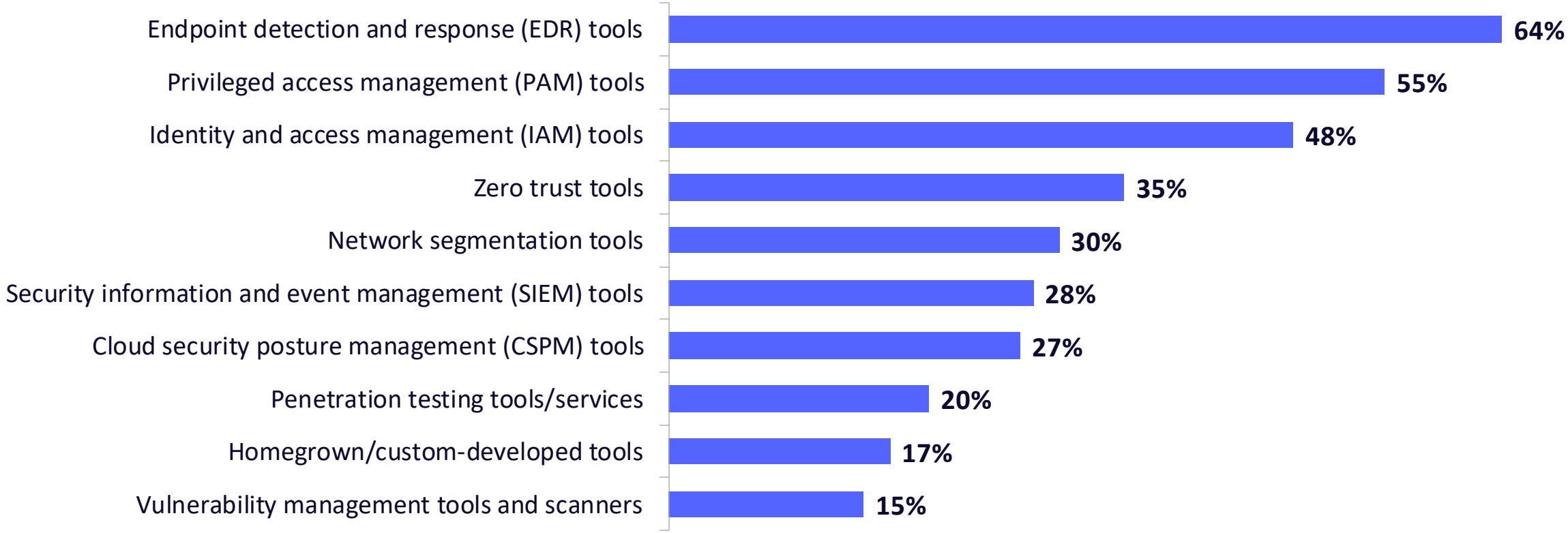
Organizations may be following a specific Attack Path Management methodology (such as what we at SpecterOps suggest) or they might be solving a part of the problem with a similar technology. Nonetheless, organizations are doing what they can to mitigate attack paths here and now.

The following data shows that organizations are implementing Identity Security tools and strategies, how they prioritize remediation, and what struggles they still face.



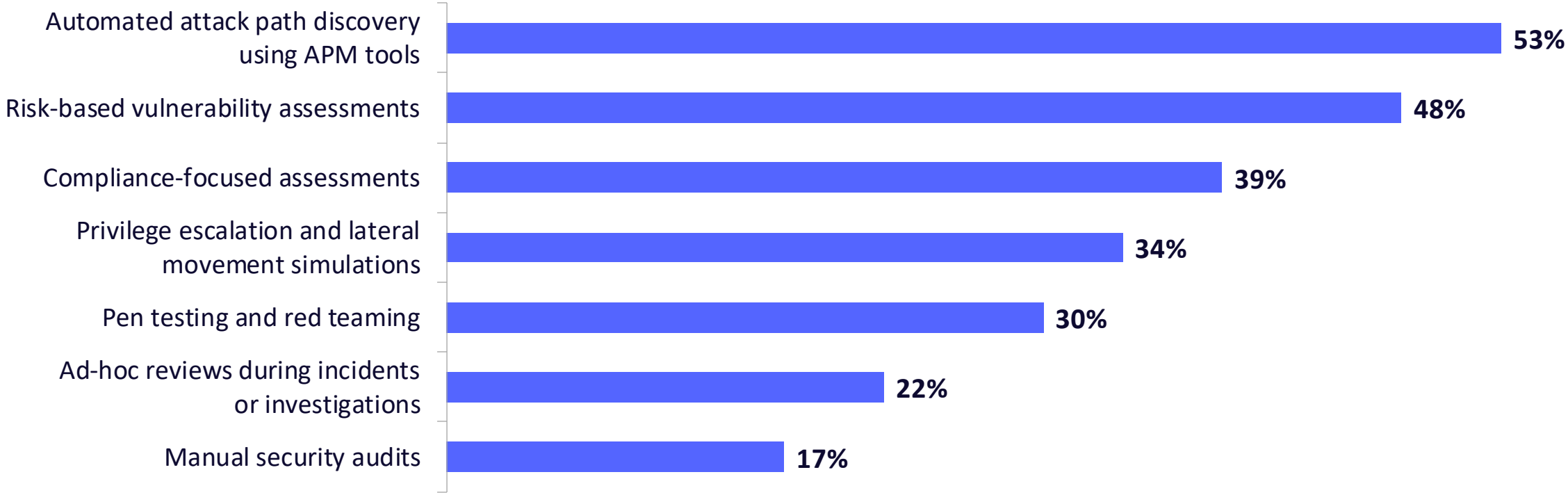
Organizations most commonly use EDR, PAM, and IAM to mitigate identity-based attack paths

Which of the following tools does your organization use for mitigating identity-based attack paths?



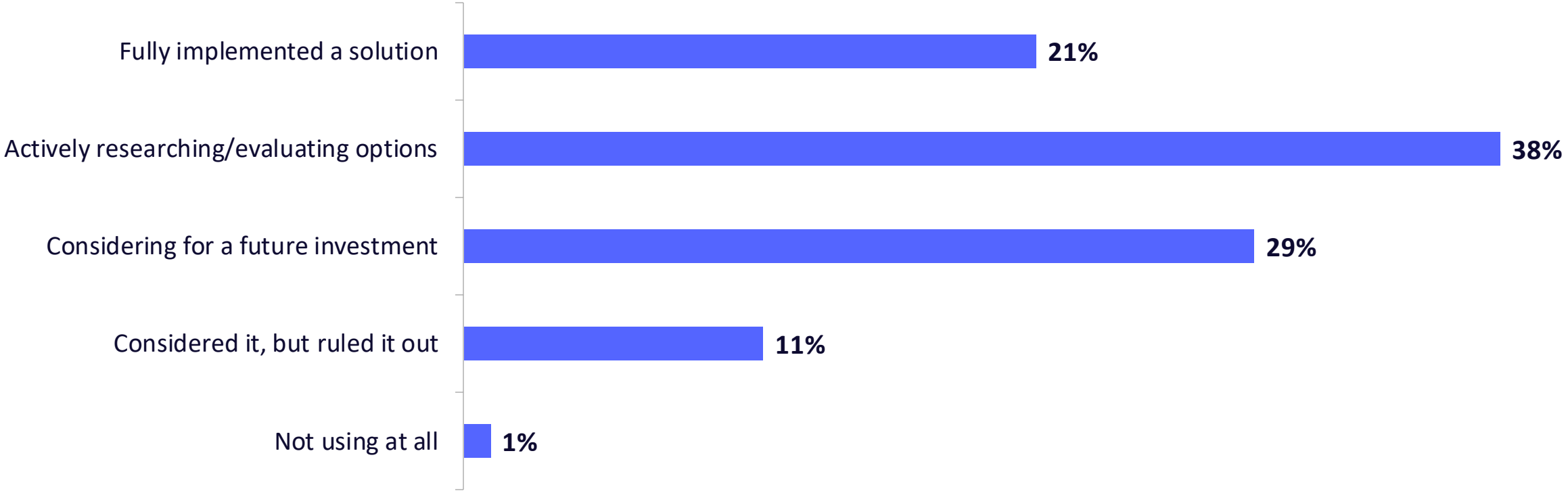
Automated attack path discovery, risk-based vulnerability assessments, and compliance-focused assessments are key to examining attack paths

What types of assessment does your organization use to examine identity-based attack paths?



59% of organizations are actively researching or have already implemented an identity-based attack path management solution

Which of the following best describes your organization's current use of identity-based attack path management solutions?

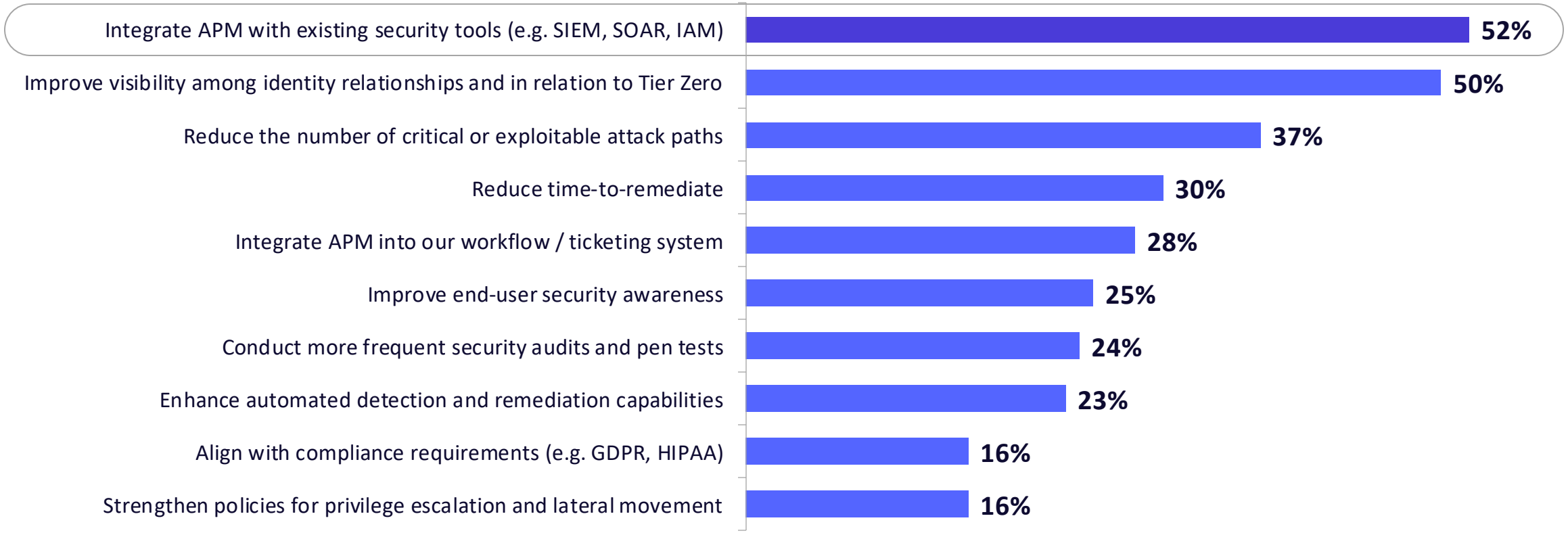


Organizations report myriad benefits from their APM implementation

What benefits would you expect to experience from an ideal identity-based attack path management process?

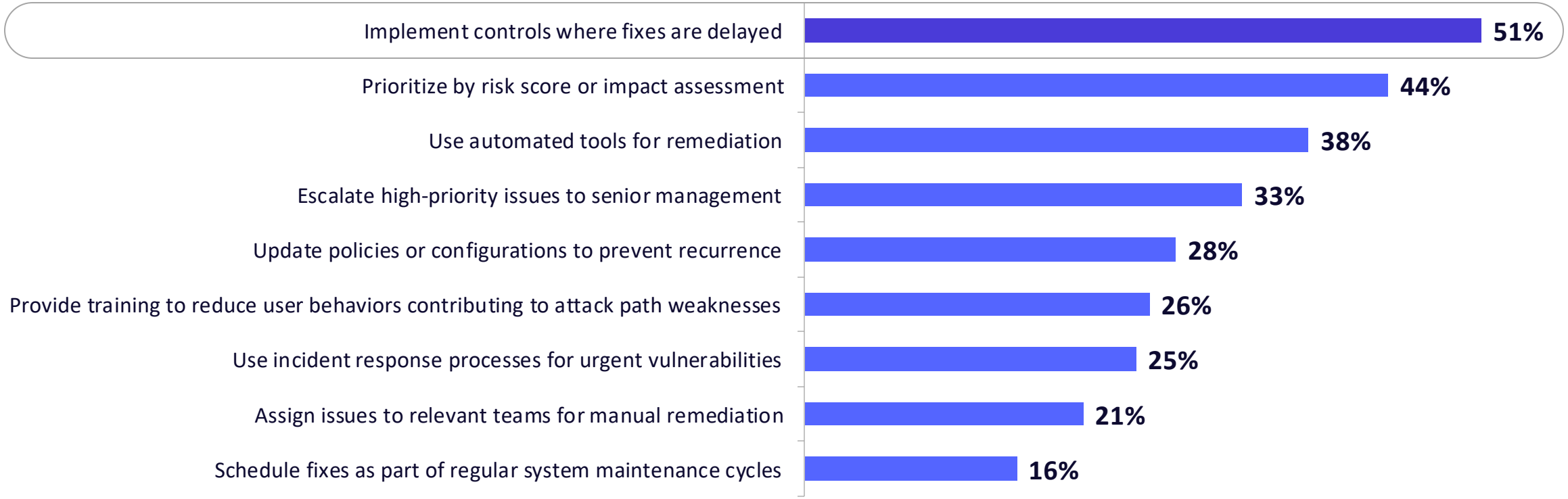
Top APM program priorities include integration and improving visibility

What are your overall goals for your APM program over the next 12 months?



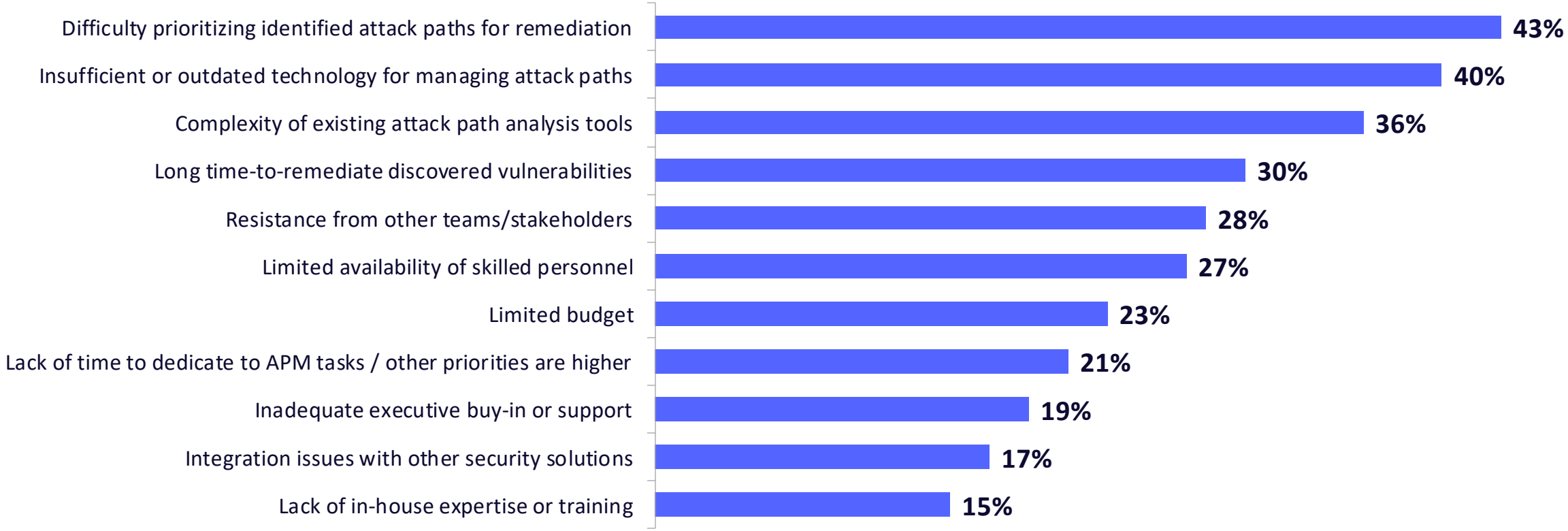
Remediation typically includes implementing controls and prioritizing by risk score/impact assessment

Once attack paths and misconfigurations have been identified in your Attack Path Management solution, what is your team's process (or planned process) for remediation?



Prioritization difficulties and outdated technology are roadblocks to implementation

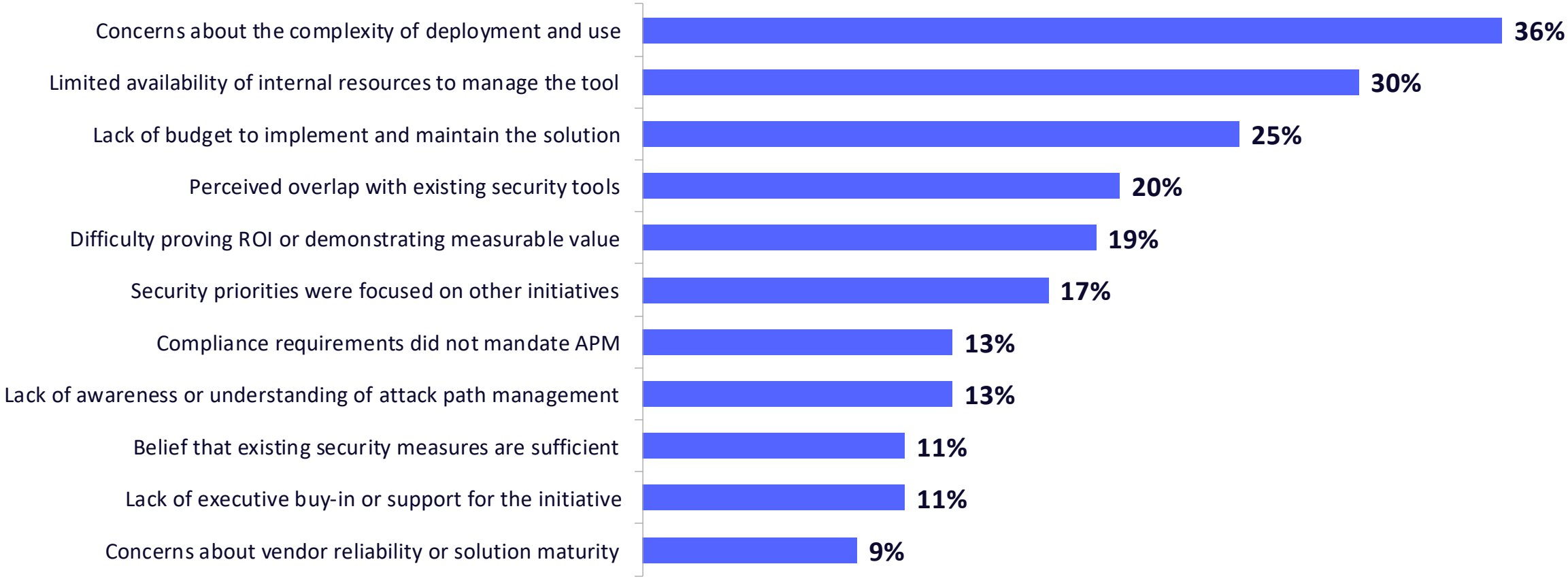
What challenges did you experience, or anticipate experiencing, in implementing your APM process?



N=64 cybersecurity decision makers who are not using, or not interested in using, an identity-based attack path management solution

Internal challenges hinder wider adoption of APM solutions

Why did you ultimately decide not to use an Attack Path Management solution?

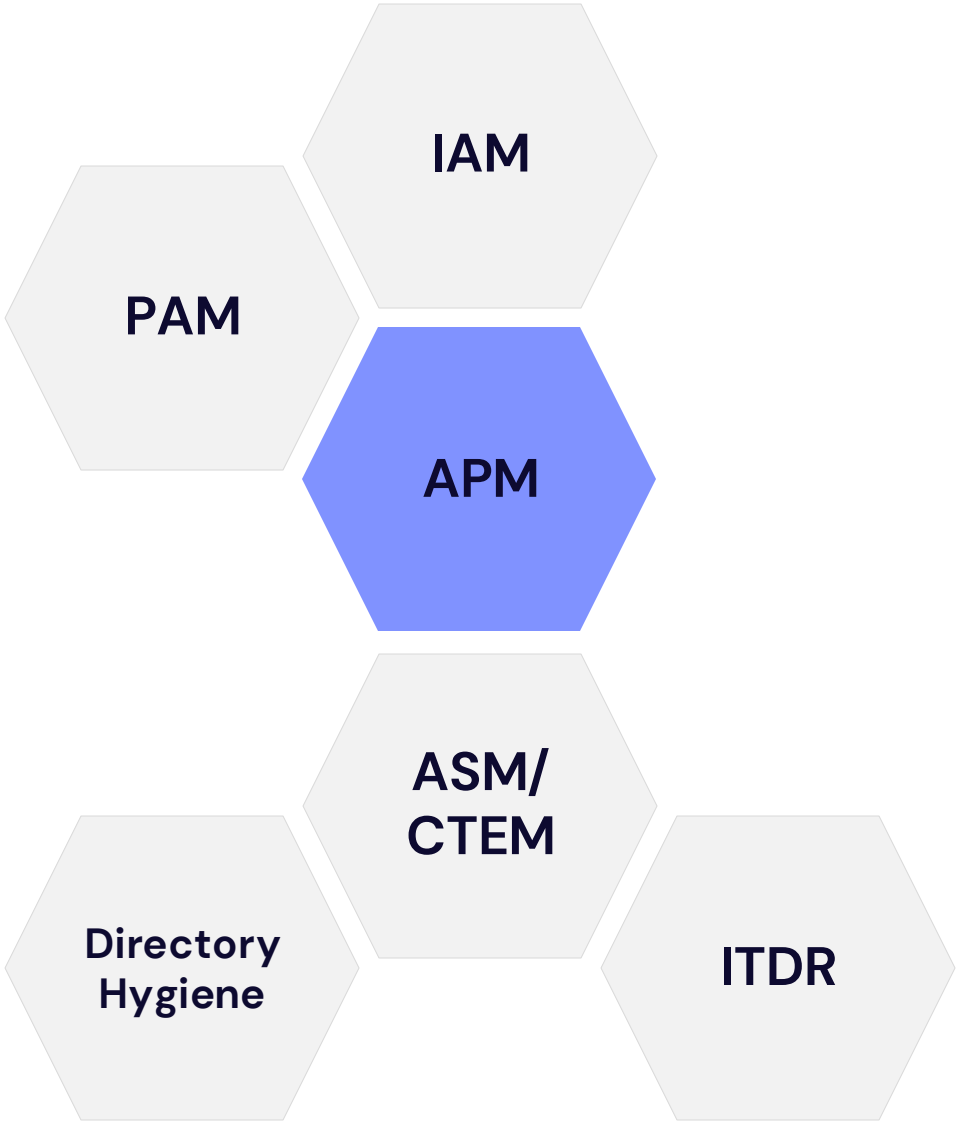


Source: Gartner - Demystifying the Hype: Identity Security, Posture Management, Threat Detection and Response - Felix Gaehtgens

Other identity solutions

Powerful but address other problems

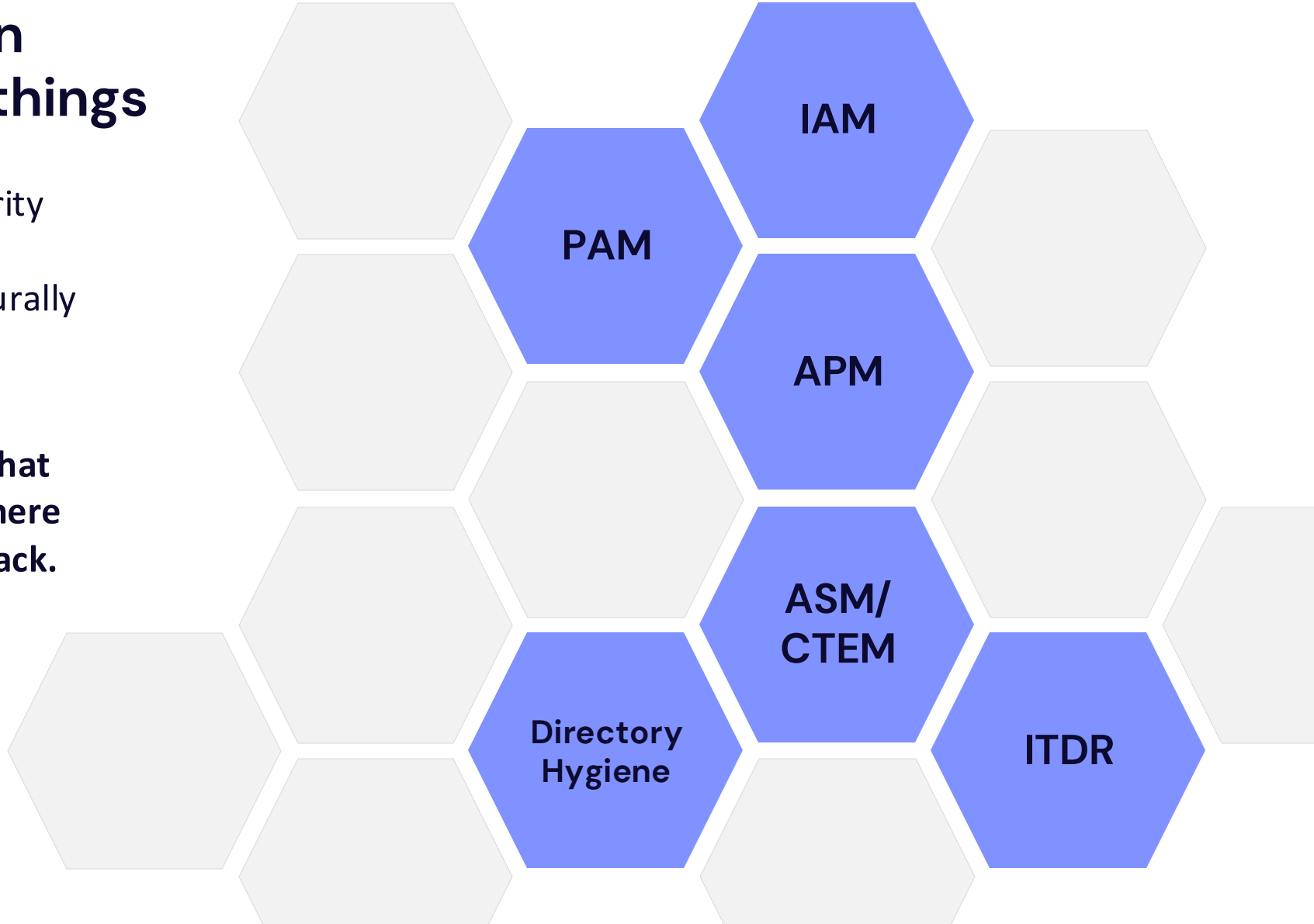
- An **authentication tool** protects identities from unauthorized access and from being manipulated and misused.
- A **privileged access management (PAM) tool** also protects identities and provides additional protection to identities that become privileged, which could lead an attacker directly to critical assets.
- An **identity governance or management (IAM) tool** will help control technology access by managing/governing every identity across the organization.



Source: Gartner - Demystifying the Hype: Identity Security, Posture Management, Threat Detection and Response - Felix Gaehtgens

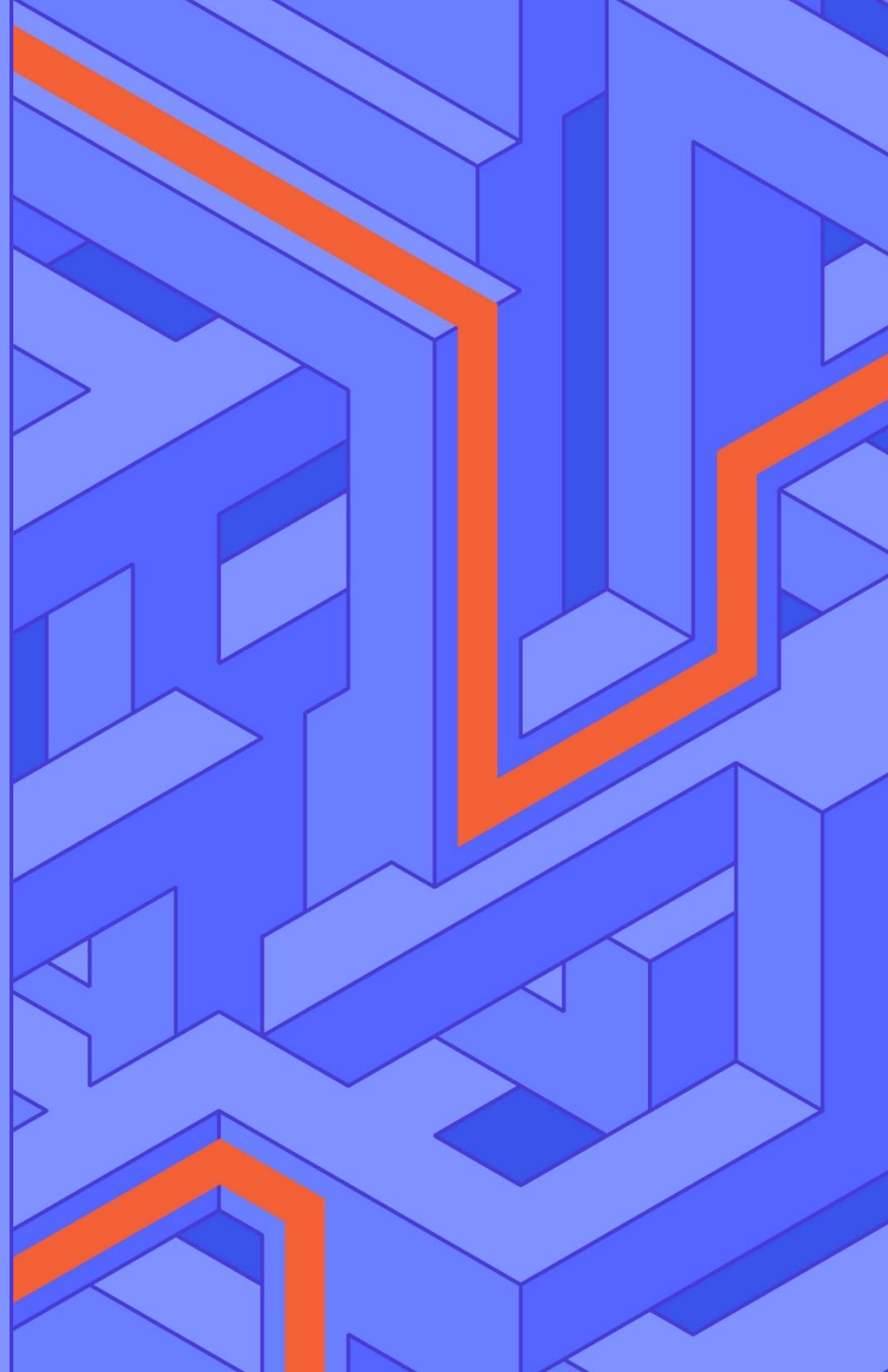
“Identity Security” can mean many different things

- Vendors under the Identity Security umbrella will have increasingly disparate capabilities, which naturally causes confusion for IT and security teams.
- **It’s important to ask a vendor what they really DO to understand where it fits in your identity security stack.**



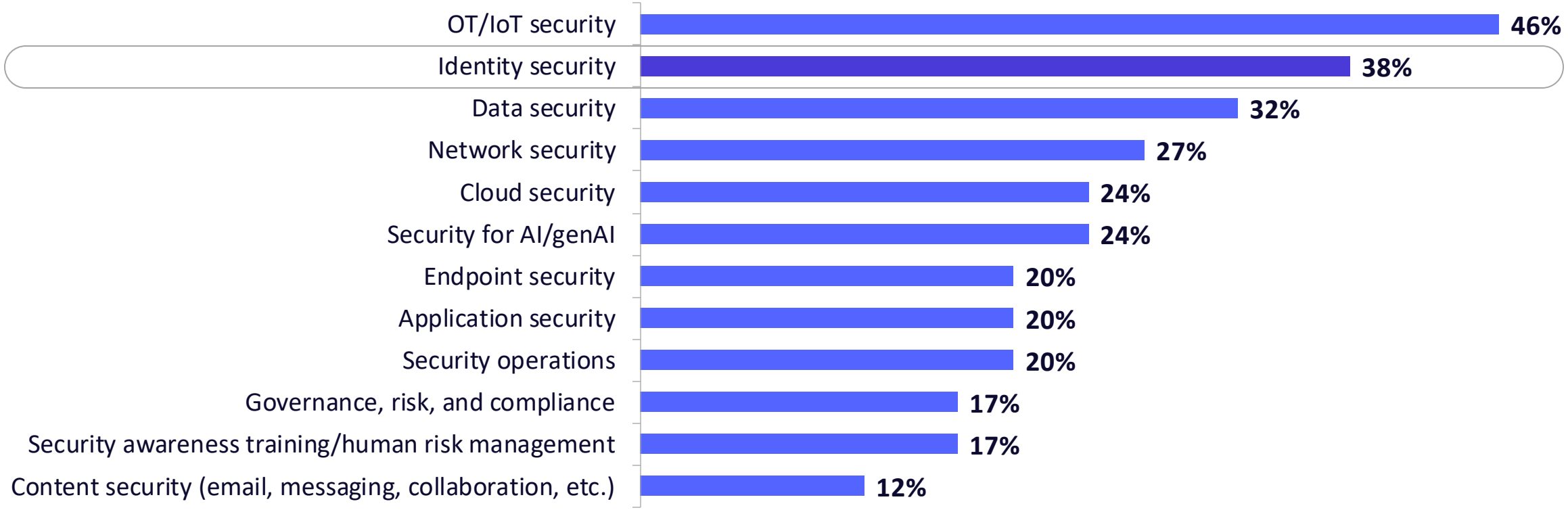
Looking Ahead

Data Review



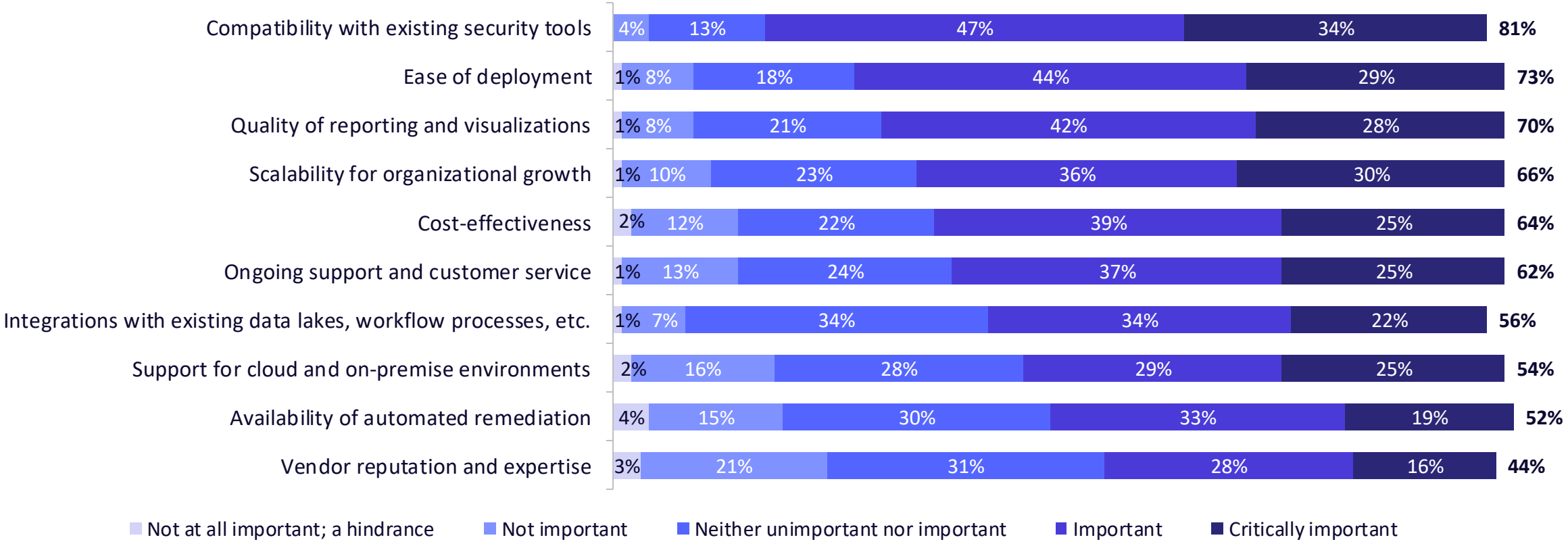
Start-up innovation is most needed in OT/IoT, identity security, and data security

In which areas does your organization see the greatest need for innovative cybersecurity technology from start-ups (i.e. beyond the major vendors)?



The most important vendor selection criteria include compatibility with existing tools, ease of deployment, and quality of reports

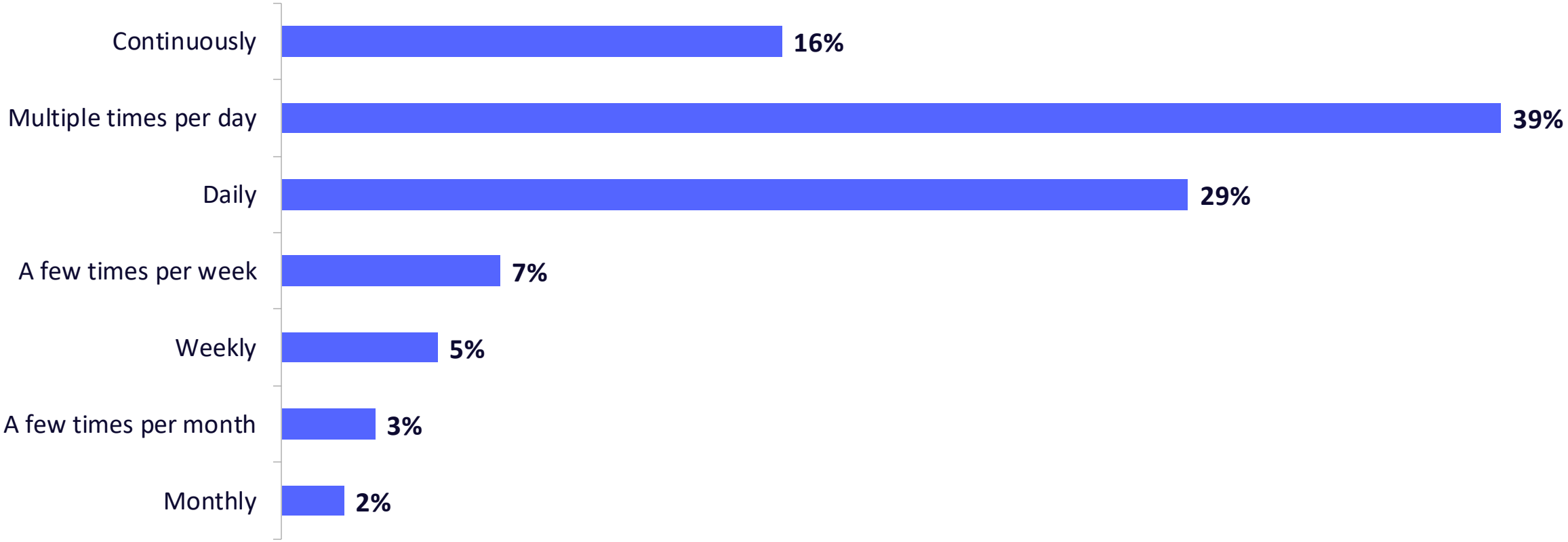
How important are each of the following criteria when selecting an identity-based APM partner/solution?



N=109 cybersecurity decision makers who have implemented an identity-based attack path management solution

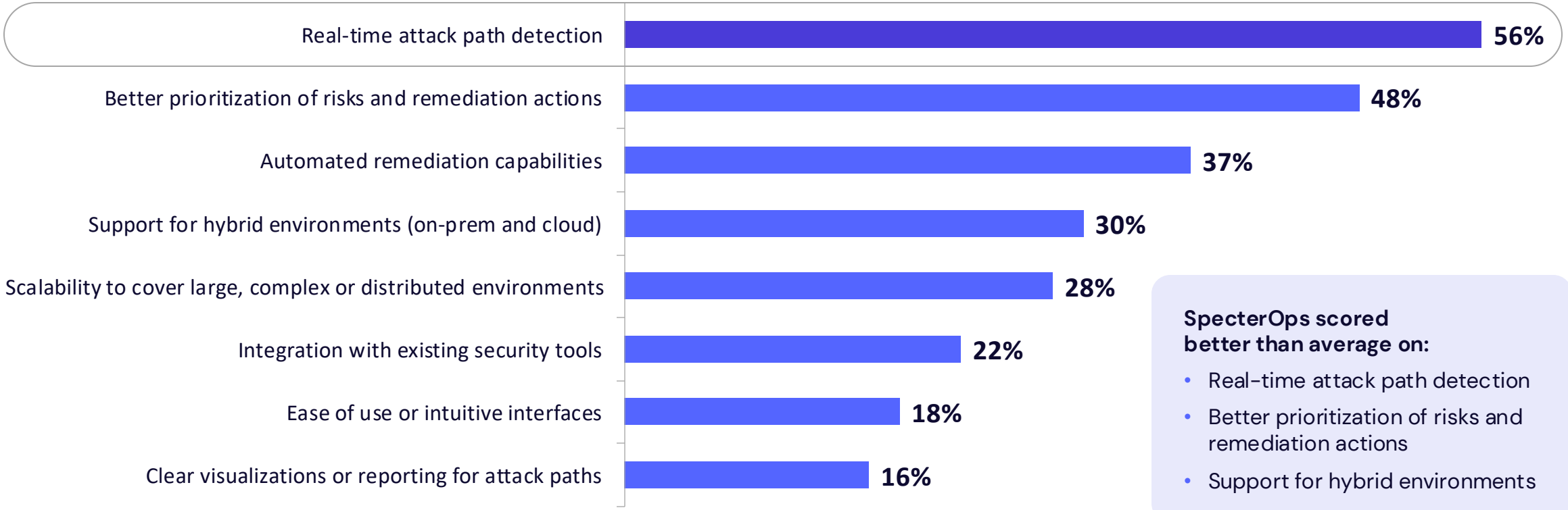
84% of organizations evaluate attack paths at least daily

In what capacity does your organization evaluate Attack Path Management in your identity environments?



Effectiveness is hindered by vendors' lack of real-time attack path detection and risk prioritization

What challenges or gaps in your current Attack Path Management solution hinder your effectiveness?



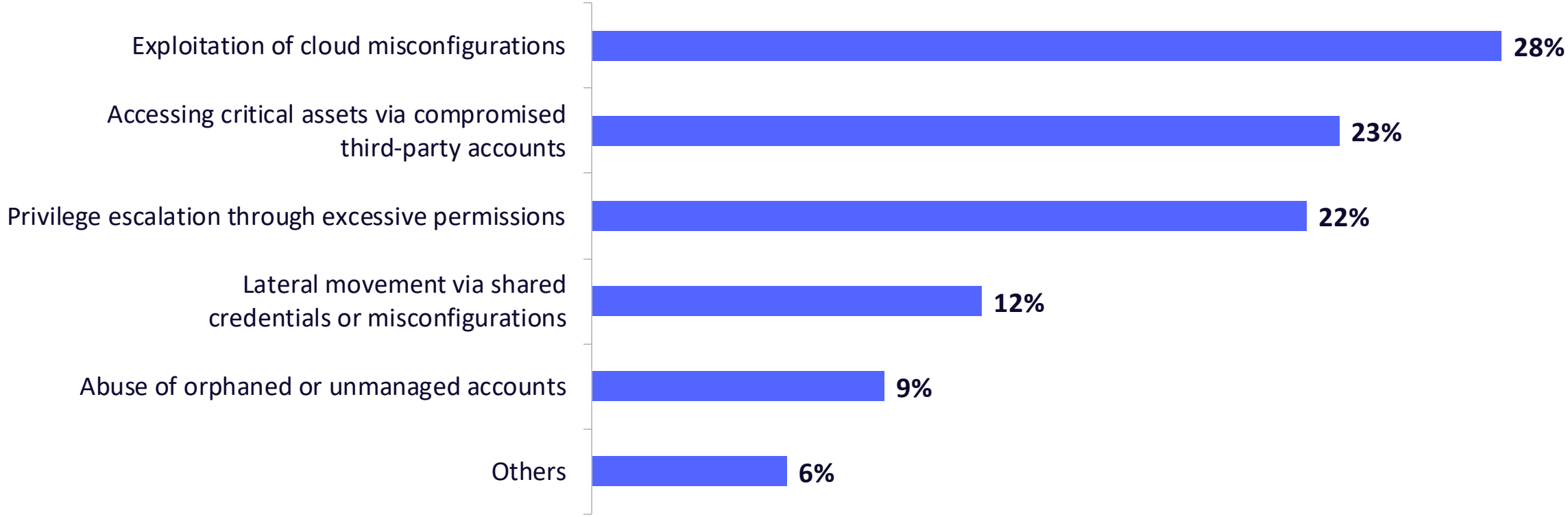
SpecterOps scored better than average on:

- Real-time attack path detection
- Better prioritization of risks and remediation actions
- Support for hybrid environments

N=109 cybersecurity decision makers who have implemented an identity-based attack path management solution

Over one quarter of organizations report exploitation of cloud misconfigurations as the most concerning attack path

What is the most concerning attack path your teams have uncovered using an Attack Path Management tool?



Additional information

About this survey

The source for all respondent data in this report came from a commissioned study conducted by Omdia on behalf of SpecterOps. In January 2025, Omdia conducted an online survey of 518 cybersecurity and IT decision makers regarding attack path management. Survey participants included respondents in director-level positions and higher, in the US, Canada, UK, France, Germany, and Australia. Surveys were fielded in a double-blind methodology to ensure anonymity.

About SpecterOps

SpecterOps is a leader in Identity risk reduction. Possessing deep knowledge of adversary tradecraft, the company enables global organizations to detect and remove critical attack paths before sophisticated attackers can take advantage of them – a practice called Identity Attack Path Management. SpecterOps built and maintains widely used open-source security toolsets, including BloodHound, the company's foundational tool that enables attack path management in Active Directory, Entra ID and hybrid environments. BloodHound has been recommended by the U.S. Department of Homeland Security, PricewaterhouseCoopers and many others. BloodHound Enterprise is the company's managed SaaS for identity and security teams, allowing for attack path prioritization, remediation guidance, and reporting to show improvements over time.

SPECTEROPS | OMDIA

Thank you

For more information on the practice of Identity Attack Path Management as well as BloodHound Enterprise powered by SpecterOps, head to specterops.io