Enterprise Strategy Group™

Identity Security at a Crossroads: Balancing Stability, Agility, and Security

Todd Thiemann | Principal Analyst

ENTERPRISE STRATEGY GROUP

JULY 2025

This Enterprise Strategy Group eBook was commissioned by Teleport and is distributed under license from TechTarget, Inc.

Research Objectives

Workforce identity security is in a state of flux, with changing enterprise infrastructure, an expanding application portfolio to integrate, and sprawling cloud deployments that are exposing unsolved problems, inefficient processes, and fragmented solutions. Enterprises are coming to terms with new identity-driven cyberthreats and recognizing the underappreciated non-human identity (NHI) or machine identity attack surface that includes emerging agentic AI deployments. Pain points, key solutions under consideration, decision dynamics for identity solutions, and how enterprises are optimizing or unifying their identity infrastructure are all changing rapidly.

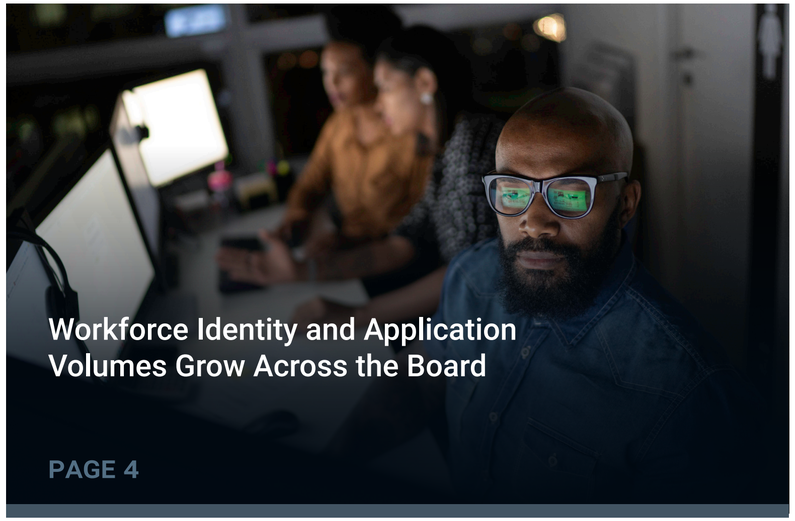
To gain further insight into these trends, Enterprise Strategy Group surveyed 370 IT and cybersecurity decision-makers at organizations in North America (US and Canada) involved with or responsible for workforce identity and access management (IAM) and identity security processes and technologies.

THIS STUDY SOUGHT TO:

- **Understand** the scope, scale, and growth of identities that organizations must manage.
- **Determine** the maturity of non-human/machine identity security and the state of agentic AI deployment.
- **Identify and quantify** the major pain points for leaders managing workforce identity security.
- **Uncover** the strategies used to optimally manage identity security in the face of proliferating enterprise applications, compliance obligations, identity threats, and a diverse identity security tool ecosystem.

Note: Totals in figures and tables throughout this eBook may not add up to 100% due to rounding or organizations choosing more than one answer to select questions.

Key Findings



Workforce Identity and Application Volumes Grow Across the Board

PAGE 4

The Workforce Identity Security Tool Portfolio Is Expansive and Typically Includes Multiple Tools for Each Identity Domain

PAGE 7

Identity Governance and Administration Deployments Are Hindered by Manual Processes and Regularly Discover Excessive Privileges

PAGE 11

Enterprises Are Concerned About Security Risk for Non-human Identities and Agentic AI

PAGE 17

Identity Security Tools Proliferate, but Plans Abound to Rationalize While Achieving Better Outcomes

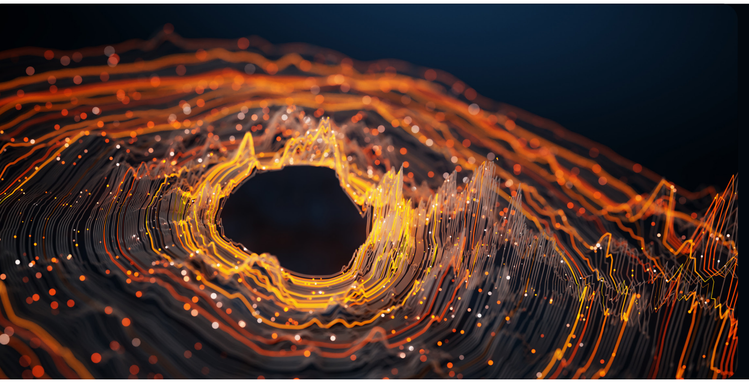
PAGE 20

Identity Security Is a Top Priority With Budgets Primed to Increase, and Agentic AI Management and Security Are the Focus

PAGE 23

BACK TO CONTENTS

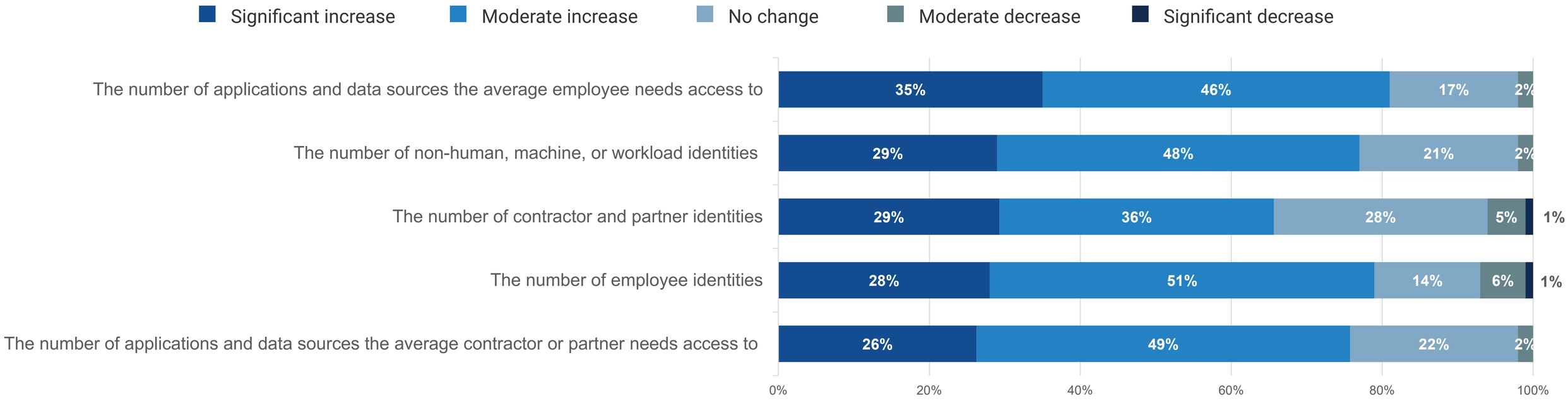
Workforce Identity and Application Volumes Grow Across the Board



The Enterprise Identity Estate Is Expected to Grow

Enterprises grow and change, and identity teams are preparing for that changing status quo. Identity security leaders expect the volume of applications and data sources, non-human (machine) identities, and human identities to increase.

Anticipated change in elements of workforce identity over the next 12 months.

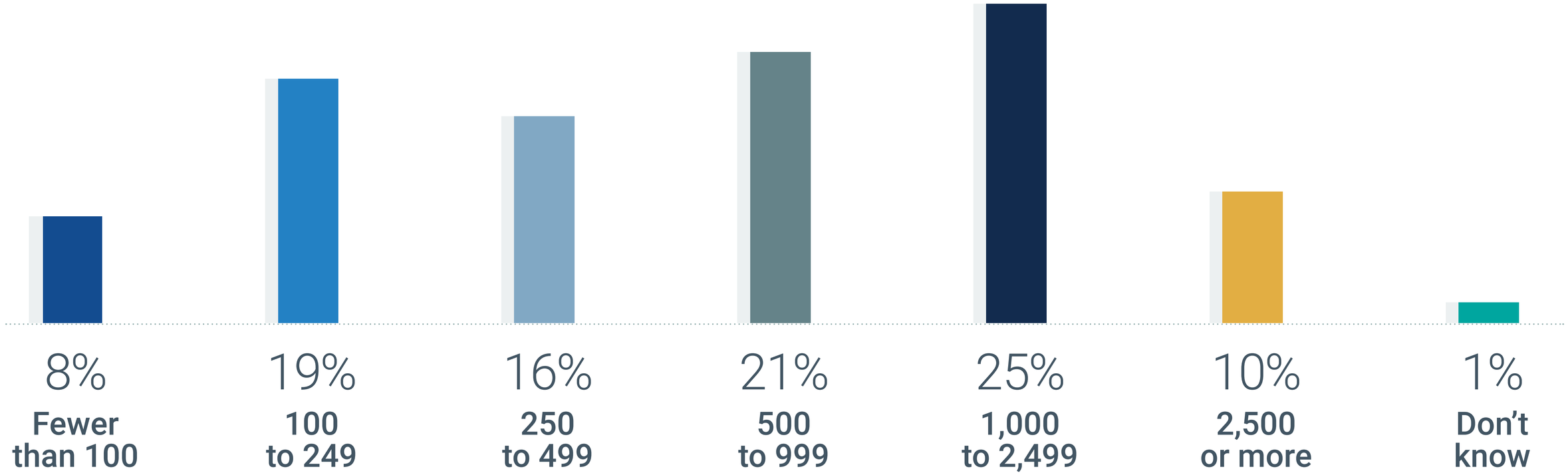


BACK TO CONTENTS

Enterprises Manage Voluminous Application Portfolios

Identity teams need to maintain visibility, ensure appropriate access, and manage policies across a broad ecosystem of business applications. More than one-third (35%) of organizations report having at least 1,000 applications in use worldwide.

Number of business applications in use.



BACK TO CONTENTS

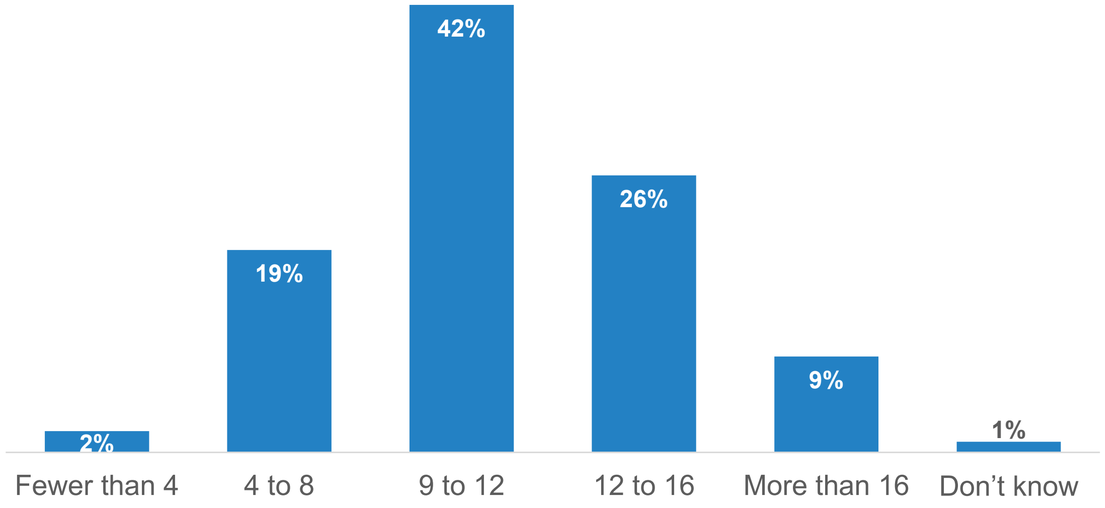
The Workforce Identity Security Tool Portfolio Is Expansive and Typically Includes Multiple Tools for Each Identity Domain

Workforce Identity Tools Proliferate

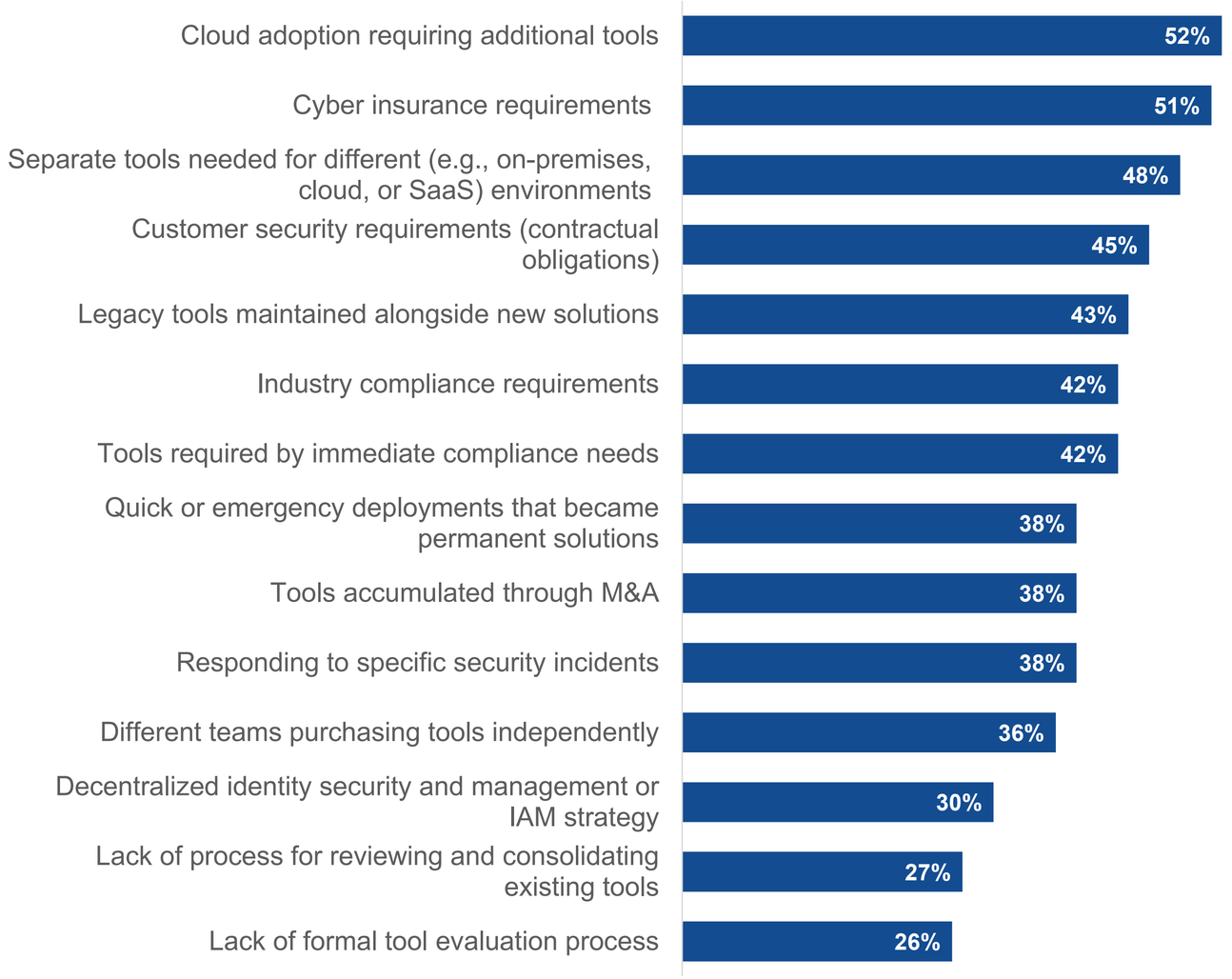
Workforce identity teams use an average of 11 tools, and the proliferation of tools leads to operational complexity, poor visibility, and identity silos. While tools are essential to solving identity challenges, tool fragmentation can result in inefficiencies and gaps in coverage.

The lead factors contributing to this tool proliferation are cloud adoption, cyber insurance requirements, and separate tools needed for different compute environments (i.e., on-premises, SaaS, and cloud environments).

Approximate number of different workforce identity tools and technologies in use.



Factors contributing to organizations accumulating more than four identity security tools.

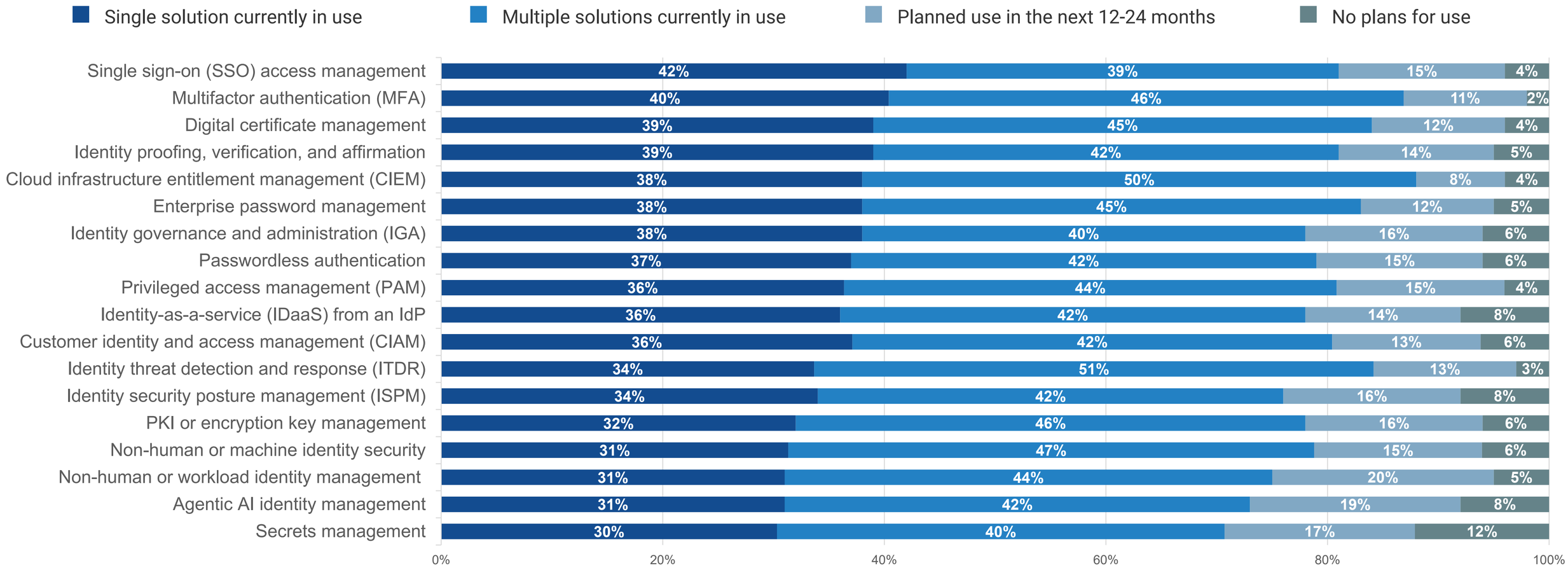


BACK TO CONTENTS

Enterprises Typically Have Multiple Solutions Across Each Area of Identity Security

Identity security teams have deployed a plethora of tools to solve identity security, but the resulting complexity provides an opportunity for improved efficiency and sets the stage for future rationalization.

Identity solutions currently in use or expected to be in the next 12-24 months.

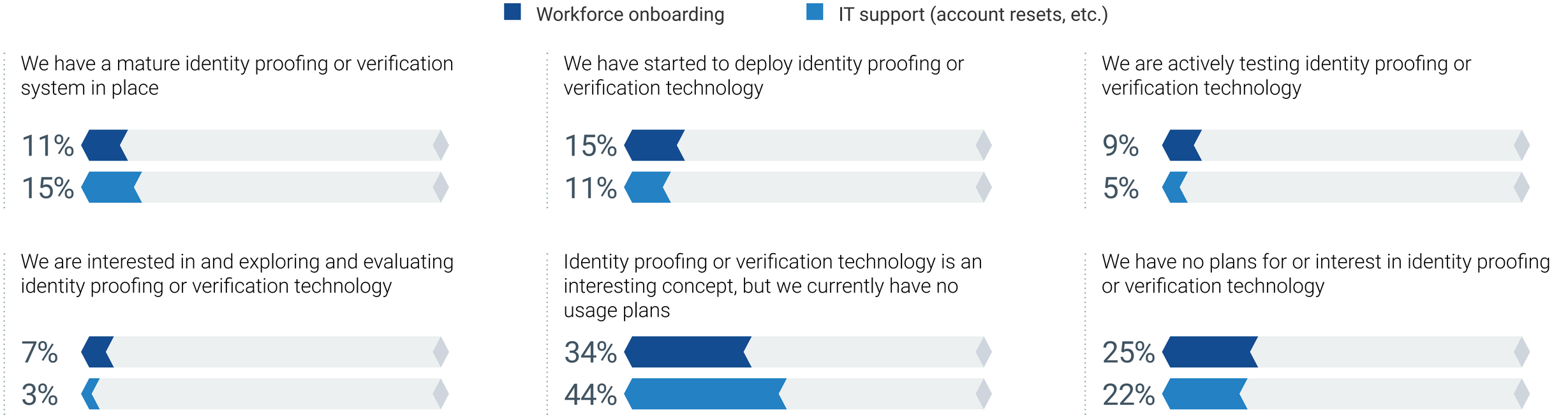


BACK TO CONTENTS

Workforce Identity Proofing Is on the Radar

While most enterprises recognize threats posed by adversaries impersonating job candidates or employees, solution adoption to counter the threat is in the early stages. Specifically, only slightly more than a quarter (26%) of organizations have identity proofing solutions in place for onboarding and IT support, but a majority is currently considering or evaluating solutions.

Usage status for identity proofing and/or verification technology.



BACK TO CONTENTS

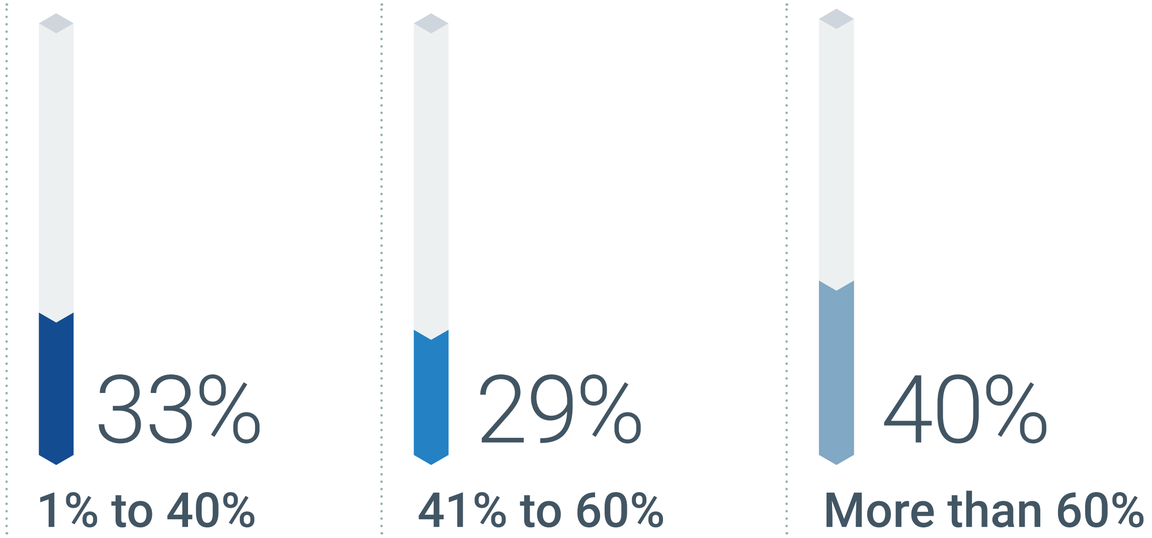
Identity Governance and Administration Deployments Are Hindered by Manual Processes and Regularly Discover Excessive Privileges

There Is Plenty of Room for Improved Identity Governance and Administration (IGA) Deployment Progress in Light of Several Key Obstacles

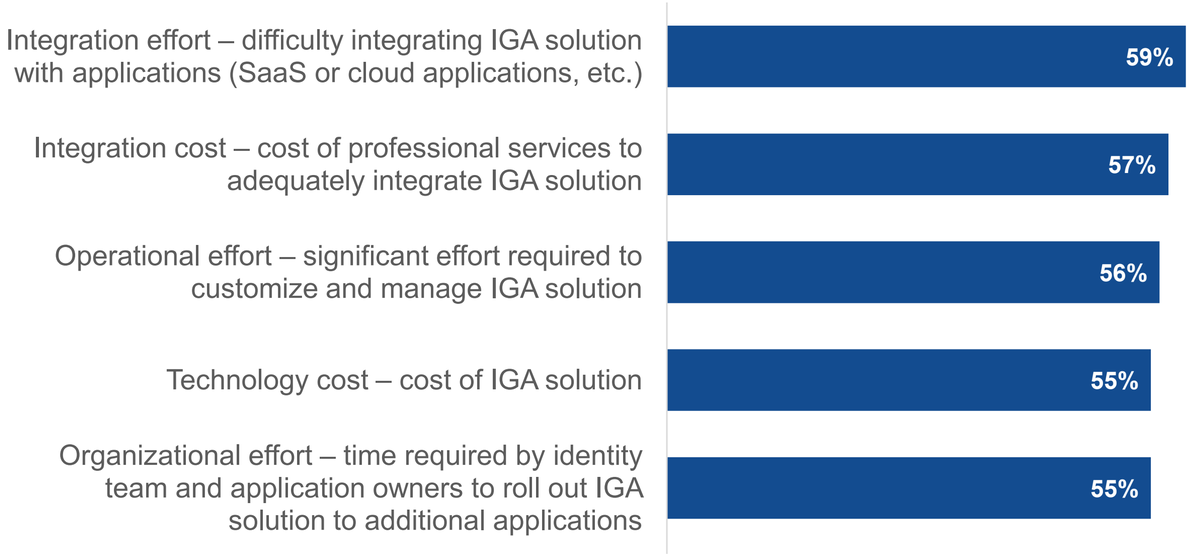
IGA is a work in progress. Organizations may have integrated their critical applications into their IGA systems, but on average, only 54% of the available applications are reportedly adequately integrated with their IGA solutions.

This is because IGA rollouts can be lengthy projects that affect an entire organization and its application portfolio. Integration overhead, operation resourcing, and costs all combine to a similar degree in inhibiting a broader rollout of IGA.

Percentage of applications that are adequately integrated with IGA.



Factors that have inhibited a full IGA rollout.



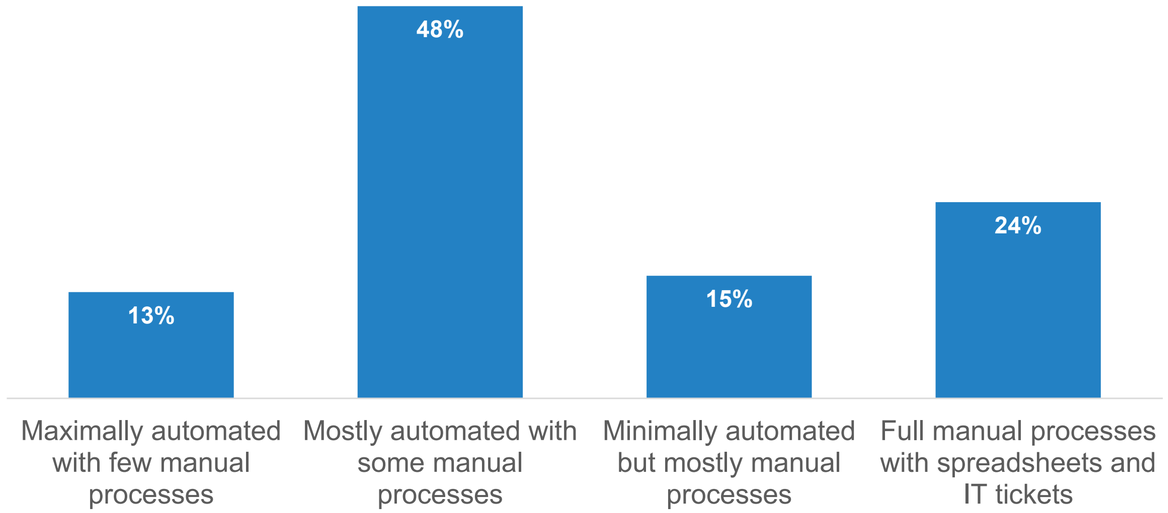
BACK TO CONTENTS

A Significant Volume of Manual IGA Processes Remains

Much remains to be done in automating IGA processes. While IGA technology has proliferated, 39% of organizations have either fully manual processes or minimally automated IGA processes.

What identity-related workflows and tasks are most commonly responsible for manual processes? Over half of respondents pointed to provisioning and deprovisioning workforce accounts, with entitlement and user access reviews also causing problematic levels of manual work. While IGA is widely deployed, organizations recognize the opportunity for efficiency improvements.

Degree to which IGA processes are automated.



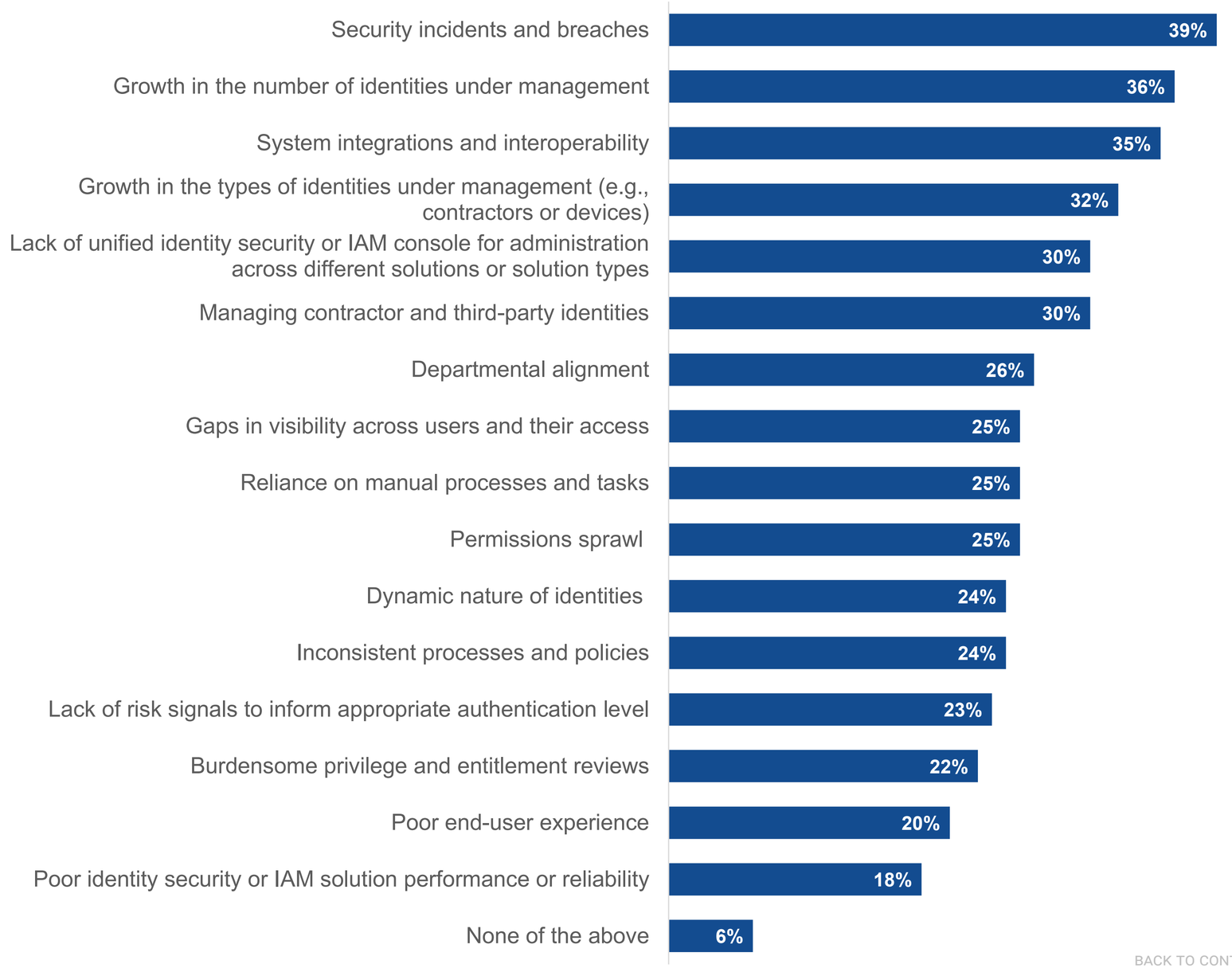
Identity-related workflows and tasks that cause a problematic level of manual work.

BACK TO CONTENTS

Breaches, Sprawl, and Integration Friction Lead Workforce Identity Security Challenges

Identity security teams face a plethora of challenges, but the major issues are responding to security incidents, the growing number of workforce identities for employees and third parties, managing integrations, and the challenge of swiveling between identity security tools.

Challenges organizations face when managing workforce identities.



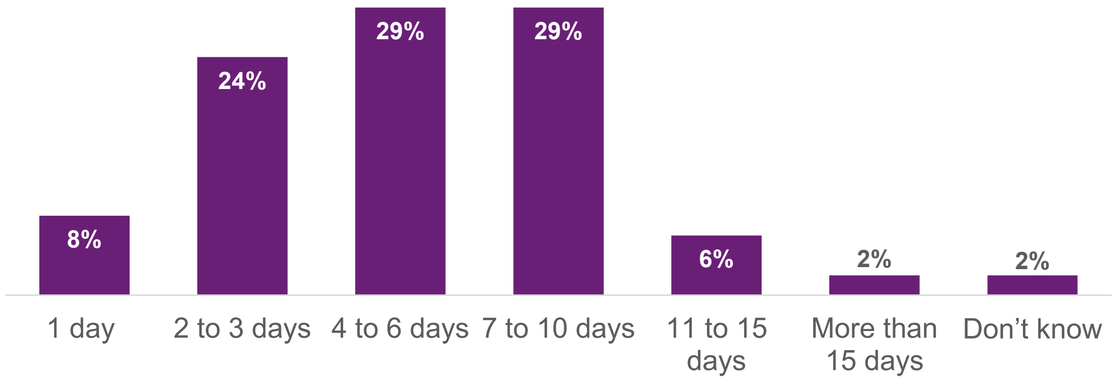
BACK TO CONTENTS

Providing Application Access and Permissions for New Hires and Resolving Identity-related Security Alerts Consume Precious Time

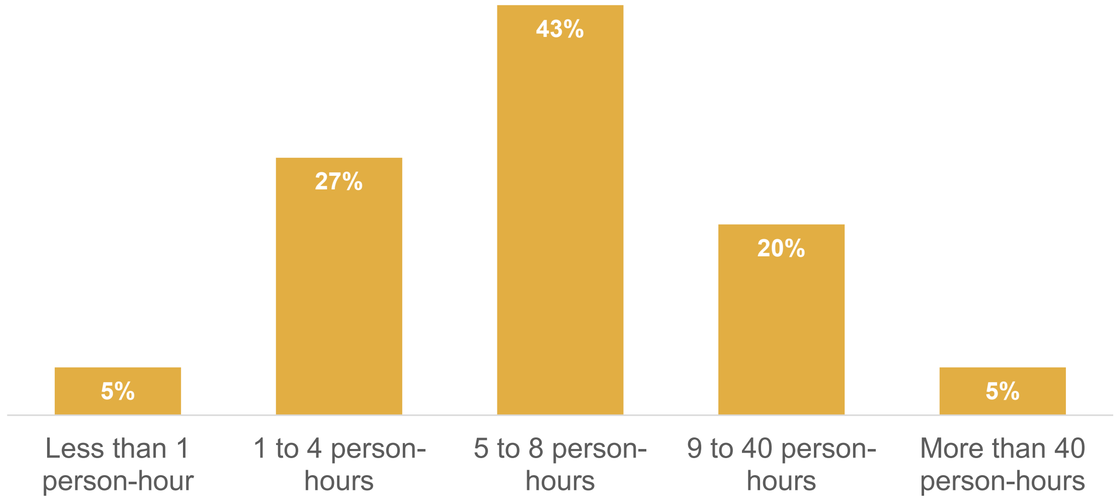
Providing new employees with appropriate access is ideally a “day one” occurrence, but most organizations find it is a “next week” situation, taking about six days on average. This latency creates a cost and frustration point for the business as employees cannot be productive as they wait for access to their applications.

Beyond onboarding employees from an identity and access perspective, resolving security alerts is also a complex process. That is particularly the case for identity-related security alerts. Indeed, one-quarter of organizations report typically spending at least nine hours investigating and remediating a single critical identity-related security alert. A time-consuming investigation process risks expanding the incident blast radius. Identity alert investigation and response is ripe for improvement: Today, a single alert consumes more than a person-day to resolve.

Length of time it typically takes to grant full application permissions while onboarding new employees.



Time in person-hours spent investigating and remediating a single critical identity-related security alert.



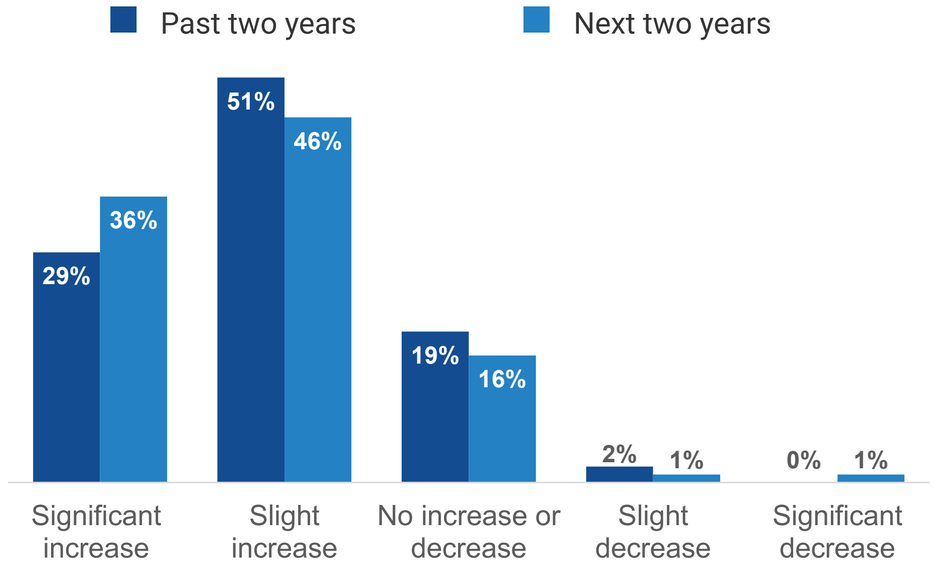
BACK TO CONTENTS

The Scope of User Access Reviews Has Increased, Revealing Excessive Permissions Are a Pervasive Issue

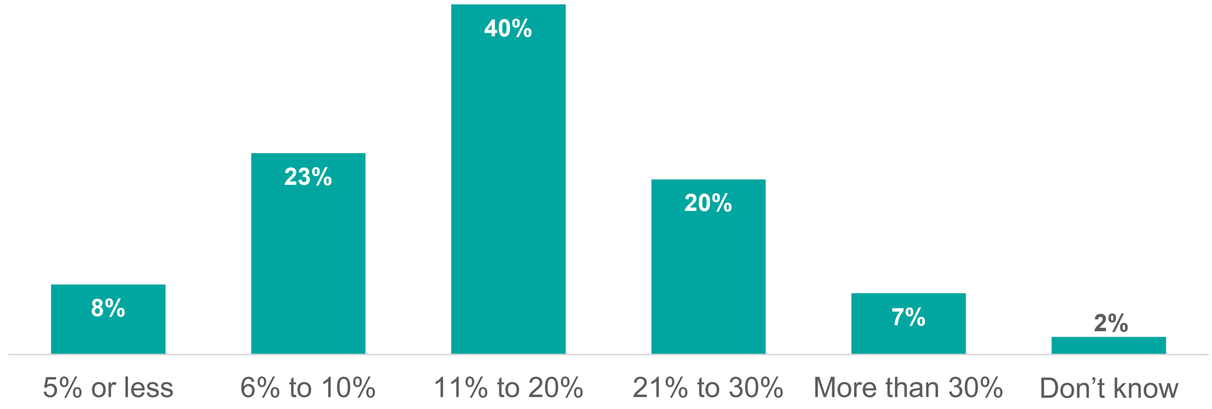
Organizations have increased the scope of access and privilege entitlement reviews over the past two years and expect that trend to continue over the next two years. There is considerable room to streamline the activity so decision-makers can evolve beyond rubber-stamping approvals to move the process along to conducting thorough, context-driven evaluations.

Organizations revoke an average of 16% of entitlements during user access and privilege entitlement reviews. While reviews can be rubberstamp approval exercises for some, it is a rigorous process for most, with four in 10 respondents revoking 11-20% of entitlements during their review process.

Change in scope of user access and/or privilege entitlement reviews.



Percentage of entitlements identified for revocation during periodic user access and/or privilege entitlement reviews.



BACK TO CONTENTS

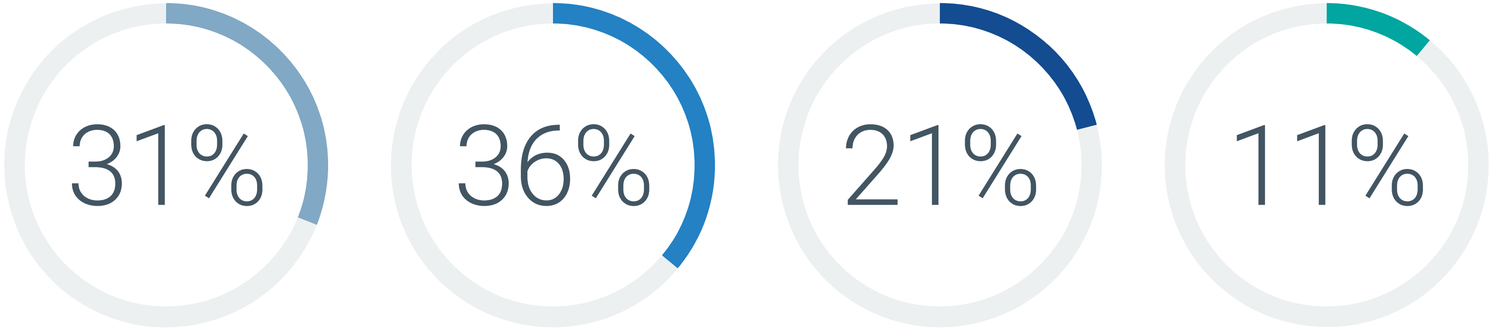
Enterprises Are Concerned About Security Risk for Non-human Identities and Agentic AI

Organizations Are Concerned About the Security Risk Posed by Non-human Identities but Cite Multiple Methods of Gaining Visibility Into NHIs

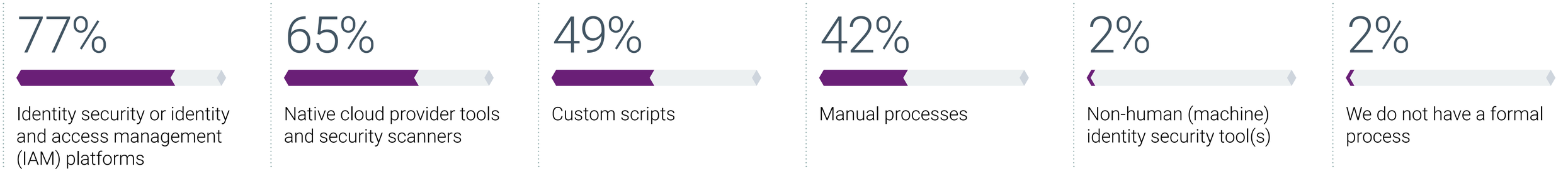
Organizations recognize the security risk associated with non-human identities (NHIs), and 67% are either very concerned or concerned about the potential for damage relating to NHIs.

Organizations use a variety of methods to discover their non-human identity footprint, with a strong preference for using existing security tools to provide visibility into their NHI estate. Very few organizations have deployed a specific NHI security tool.

Level of concern about security risks specifically related to non-human identities.



How organizations discover and inventory NHIs across their infrastructure.

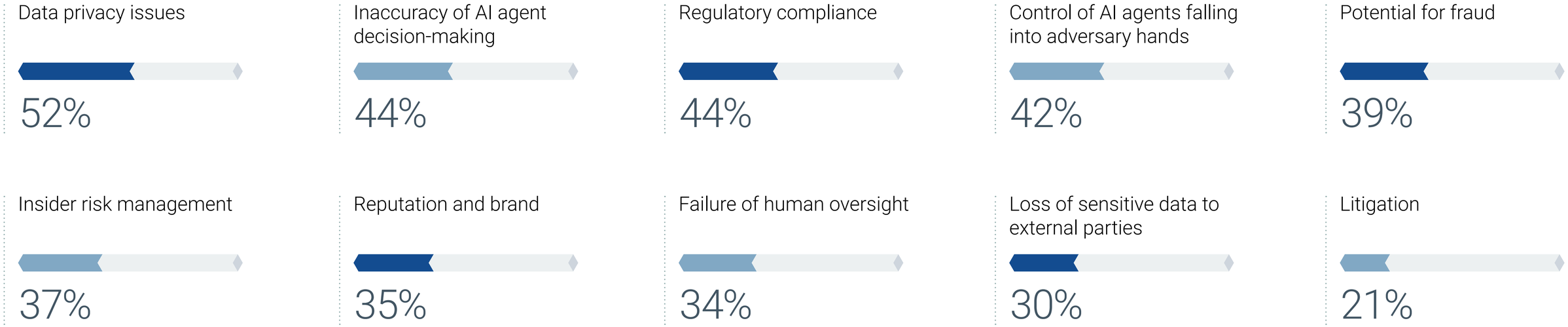


BACK TO CONTENTS

Agentic AI Adoption Raises a Host of Risks

Data privacy issues are the lead concern with AI agents, and inaccurate decisions due to generative AI's probabilistic nature, compliance, and loss of AI agent control are not far behind. While risks are recognized by identity leaders, it may take some public agentic AI security incidents to motivate business leaders to adequately invest in securing their agentic AI infrastructure.

Security and business risks of using AI agents that concern organizations.



BACK TO CONTENTS

Identity Security Tools Proliferate, but Plans Abound to Rationalize While Achieving Better Outcomes

A Range of Motivations Drive Security Portfolio Evolution

Organizations first and foremost want better security outcomes from their identity security portfolios and see the proliferation of tools leading to identity security gaps that need to be closed. Change also comes from cloud migrations and data breaches that can motivate firms to solve new identity security challenges that an existing tool set may be insufficient to tackle.

Organizations' motivations to evolve existing security portfolios.

44%

Better security outcomes - current multivendor solution orchestration and complexity may leave identity security gaps

41%

Cloud migration - transitioning tools to cloud-based platforms for scalability and potential reduced costs

40%

Data breach prevention - an experienced data breach relating to identities exposed the need to improve identity security

38%

Operational efficiency - simplified management and automation will enable teams to do more

36%

Data integration for visibility and analytics - consolidating vendors will provide comprehensive visibility and improved analysis

30%

Compliance and governance - fewer vendors will streamline audits and provide consistent policy enforcement

24%

Cost savings - consolidating vendors will reduce costs and optimize utilization

22%

Cross-team collaboration - fewer tools will be used by a broader swath of the IT and security team

1%

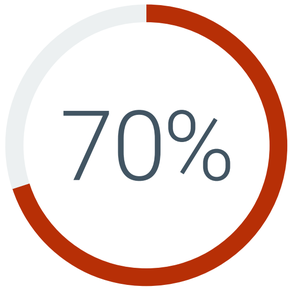
No changes planned

BACK TO CONTENTS

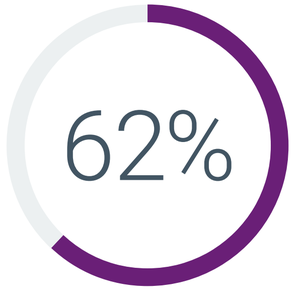
Organizations Experience Flux in Identity Security Program Evolution

Change is the operative word in identity security. While more than two-thirds (70%) of respondents report that their organization intends to expand usage of an existing tool, 62% expect to deploy a specific new tool for a new use case, and 38% anticipate replacing an existing core identity security solution with another vendor's offering. Identity security teams are ruthlessly trying to improve their programs and prune what is not working.

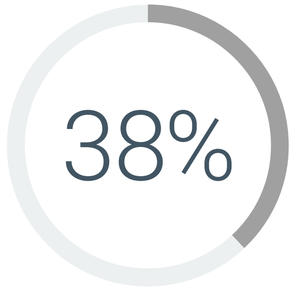
Organizations' plans to evolve identity security programs in the next 12-18 months.



Expand usage of an existing identity security tool to cover a new identity security use case (e.g., vendor providing PAM tool expanding to cover IGA, vendor providing access management tool expanding to include PAM, etc.)

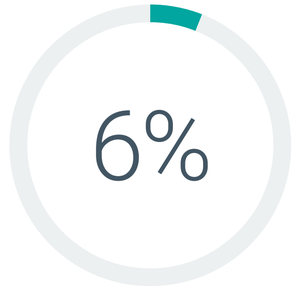


Implement a new identity security tool for a specific use case (e.g., cloud IGA, cloud PAM, identity threat detection and response, identity security posture management, etc.)



Replace an existing core identity security enterprise solution (e.g., IGA, PAM, access management, etc.) with a solution from another vendor

Replace existing identity security point solution(s) (e.g., ITDR, ISPM, etc.)



No changes planned

BACK TO CONTENTS

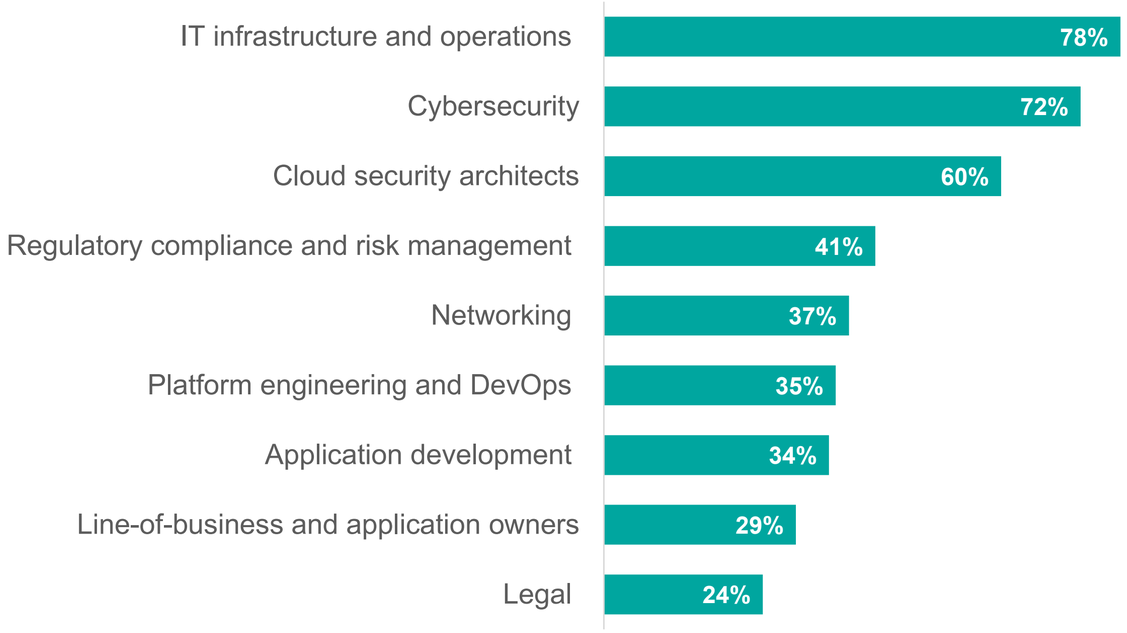
Identity Security Is a Top Priority With Budgets Primed to Increase, and Agentic AI Management and Security Are the Focus

Who Drives Identity Security Policies and Acquisition Processes?

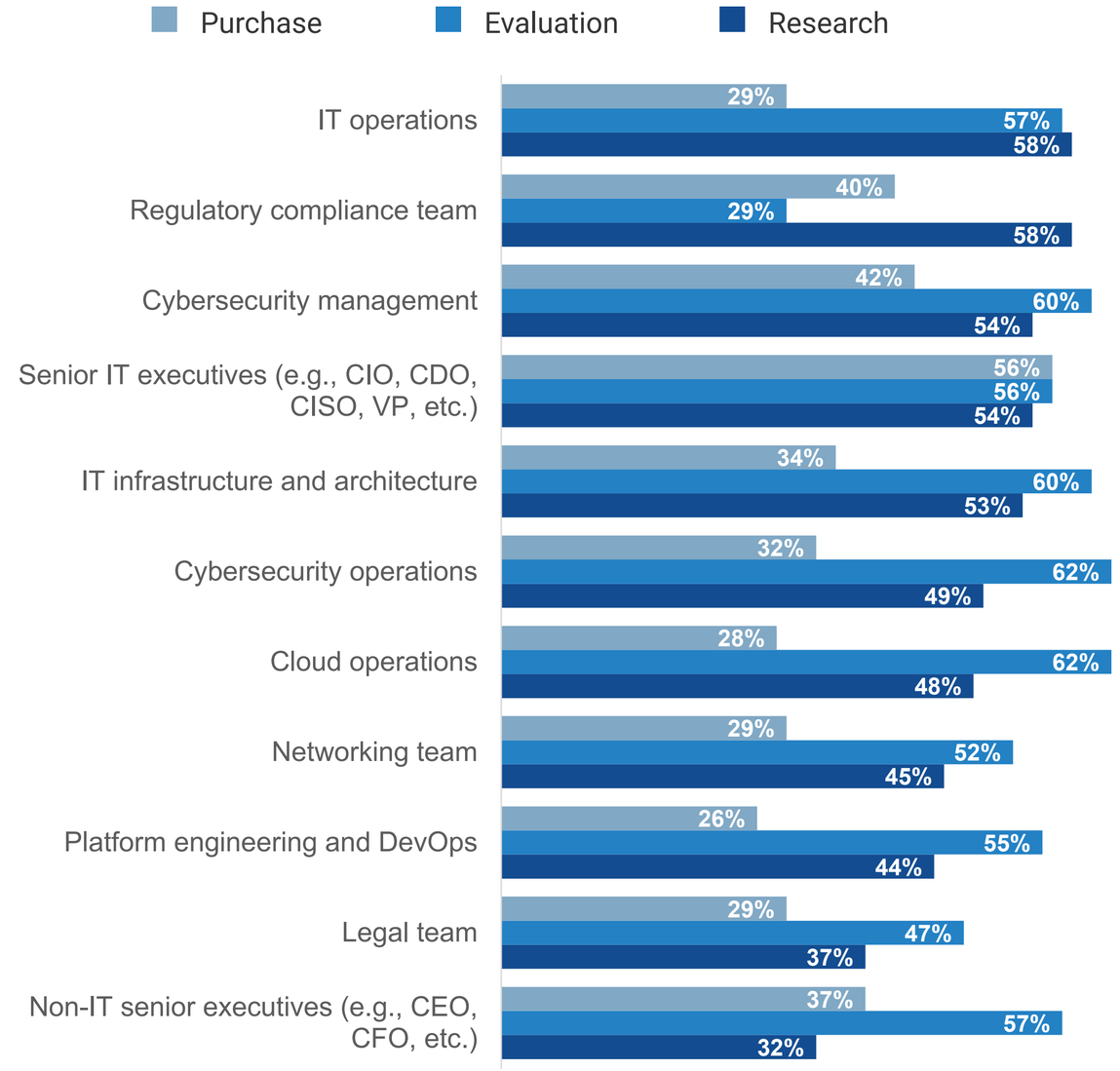
While IT and cybersecurity are the groups most commonly involved in establishing identity security policies, cloud security teams are involved for 60% of respondent organizations.

While many players are involved in research and evaluation, purchasing authority originates with the senior executives (e.g., CIO and CISO) and is distributed to compliance and cybersecurity teams.

Groups directly involved in creating organizations' identity security policies.



Individuals or groups that influence the decision-making stages of identity security technology purchases.



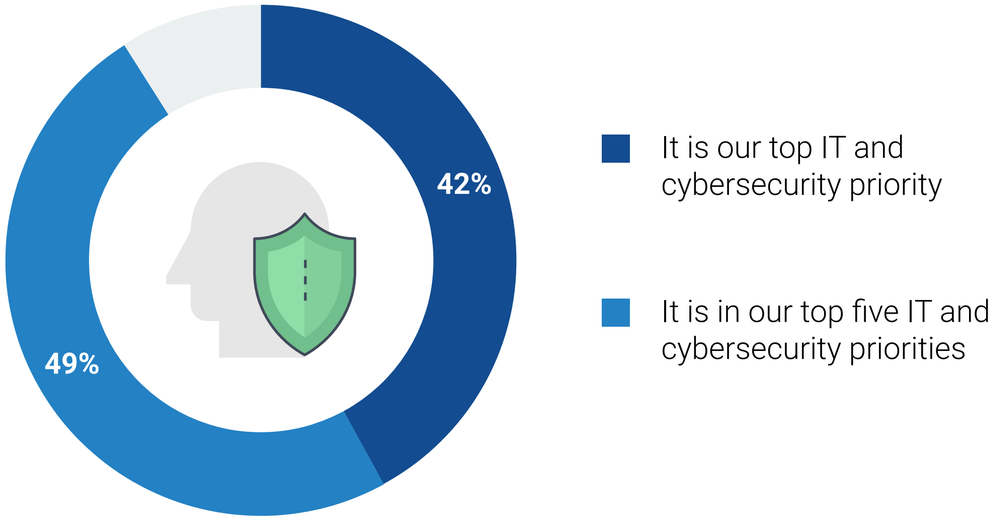
BACK TO CONTENTS

Modernizing Workforce Identity Security Is a Top Priority for a Majority of Organizations, and Spending Plans Reflect That

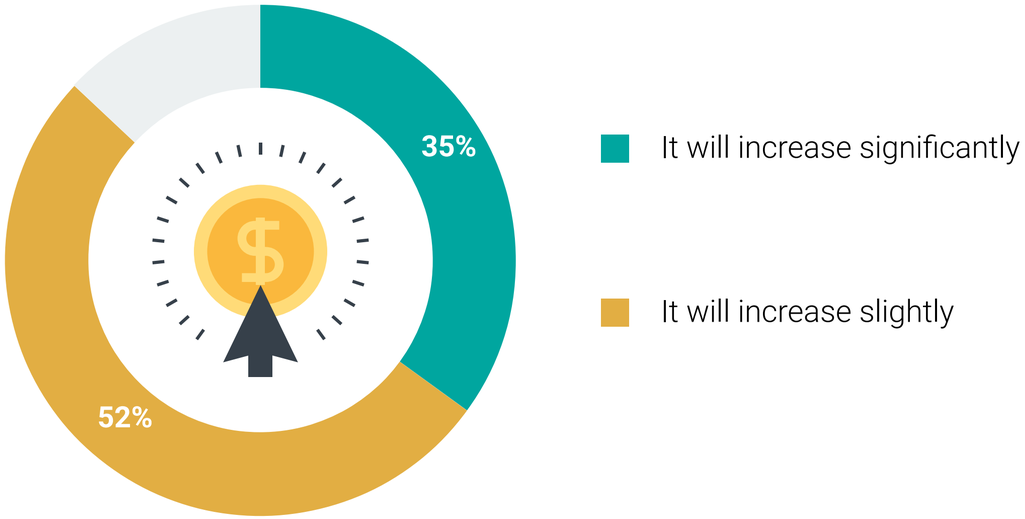
Executives and their teams have the bandwidth and budget for a limited number of projects in any given year. Workforce identity security is one of those projects as enterprises recognize the need to improve their identity security processes and technology. Specifically, 91% of organizations would classify their identity security initiatives as a top-five IT and cybersecurity priority, with 42% singling it out as their top overall IT and cybersecurity priority.

Given the relative importance of identity security, it follows that budgets are growing year over year, with 87% of organizations reporting plans to increase their spending on workforce identity security, including more than one-third anticipating significantly increasing their spending.

Priority level for identity security over the next 12 to 24 months.



Expected spending changes for workforce identity solutions over the next year.



BACK TO CONTENTS

Investment Priorities for Workforce Identity Security Highlight Goals for Protecting Agentic AI and Infrastructure

Agentic AI holds the prospect to dramatically improve how enterprises operate, and identity teams are prioritizing security and management for that infrastructure as their lead investment priority. Rounding out the top three priorities are managing cloud entitlements and investing in identity threat detection and response.

Expected areas of increased identity security investment in the next 12 months.

BACK TO CONTENTS

Teleport

ABOUT

Teleport is the Infrastructure Identity Company, modernizing identity, access, and policy for infrastructure, improving engineering velocity and infrastructure resiliency against human factors and compromise.

The Teleport Infrastructure Identity Platform implements trusted computing at scale, with unified cryptographic identities for humans, machines and workloads, endpoints, infrastructure assets, and AI agents. Our identity-everywhere approach vertically integrates access management, zero trust networking, identity governance, and identity security into a single platform, eliminating overhead and operational silos. For more information, visit www.goteleport.com or follow @goteleport.

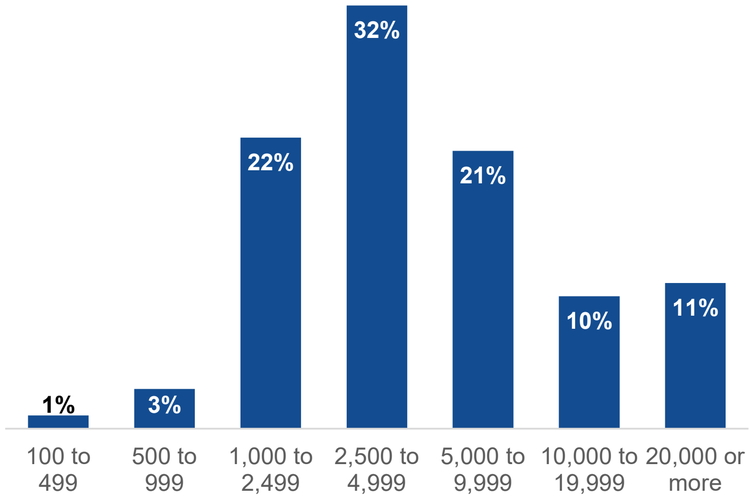
LEARN MORE

RESEARCH METHODOLOGY AND DEMOGRAPHICS

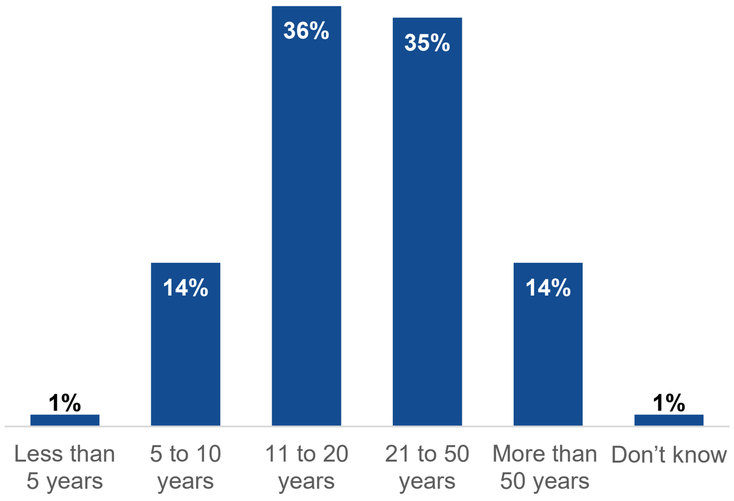
To gather data for this report, Enterprise Strategy Group conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America (United States and Canada) between May 5, 2025 and May 23, 2025. To qualify for this survey, respondents were required to be familiar with their organization's workforce identity access management (IAM) and identity security processes and technologies. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 370 IT and cybersecurity professionals.

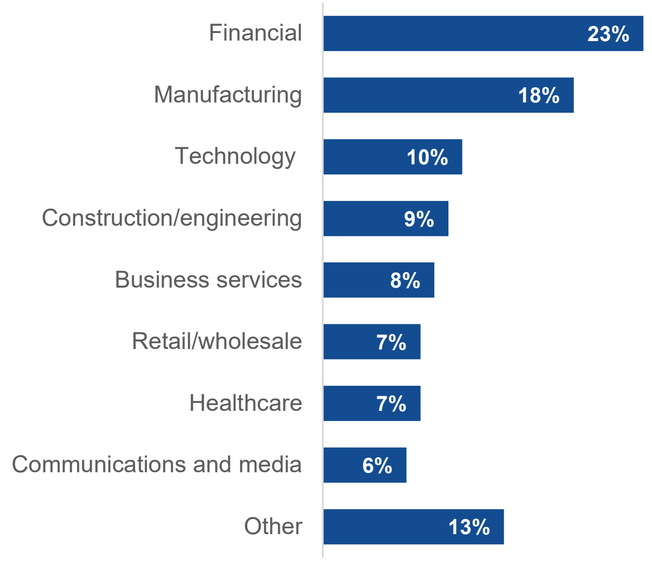
Respondents' organizations by number of employees.



Respondents' organizations by years in operation.



Respondents' organizations by industry.



BACK TO CONTENTS

Enterprise Strategy Group, now part of Omdia, provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.