Enterprise Strategy Group™ by TechTarget

Workforce Identity Management:

A Mature Approach to Managing Identities Proves to Be a Game Changer for Organizations

APRIL 2024

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

TABLE OF CONTENTS

Research Methodology and Respondent Demographics and Maturity Model Details

BACK TO CONTENTS

Research Objectives and Highlighted Findings

Objectives

This eBook, and the primary research survey that underpins it, seeks to understand whether, and to what degree, the technologies and strategies in place at organizations to manage end users' identities have a direct impact on outcomes related to their experience and productivity, enterprise risk, organizational agility, and more.

Moreover, the research explores commonalities among the organizations with the most mature approaches to workforce Identity management to uncover practical best practices that organizations should strive to adopt in order to improve their own outcomes.

Highlighted Findings

Leaders in workforce Identity maturity drive significant advantages in *business* outcomes. They are:

3.9x as likely
to say their Identity solutions enable business agility.

3.6x as likely
to say their Identity solutions enable employee productivity.

Leaders in workforce Identity maturity drive significant advantages in *security* outcomes. They are:

3.4x as likely
to say their Identity solutions help significantly with incident response.

3.2x as likely
to say their Identity solutions help to significantly mitigate threats.

Why Now Is the Time for Organizations to Maximize Their Identity Maturity

Three Trends That Underscore the Criticality of Identity Maturity

Before discussing the concept of workforce Identity maturity and whether it is helping organizations, it is important to understand the landscape organizations are operating within.

Research from TechTarget's Enterprise Strategy Group shows there are three distinct trends taking place in the market today that create a compounding effect on the complexity of effectively and efficiently managing workforce identities:

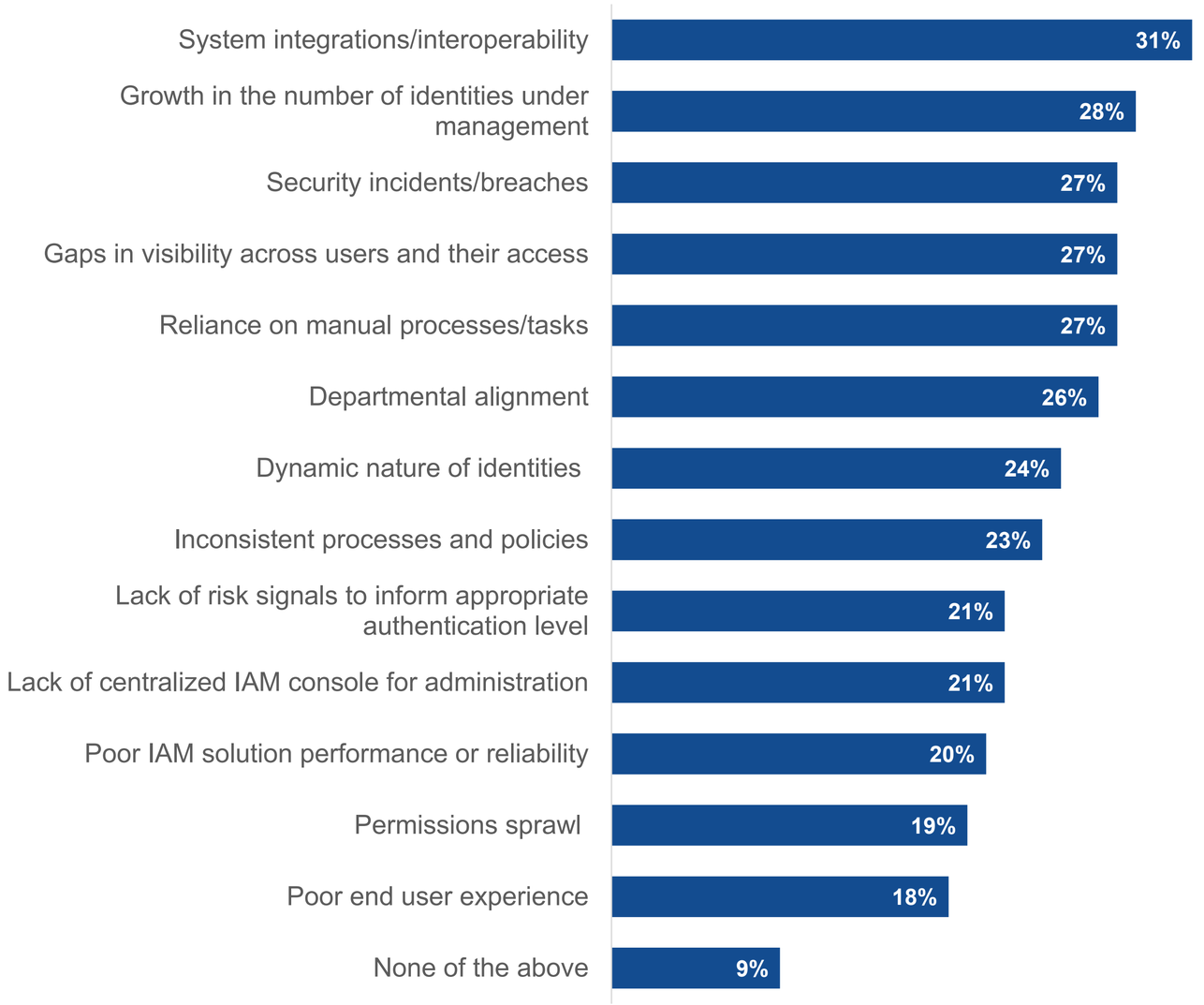
1. **The number of identities under management is increasing.** 83% of respondents expect the number of identities under management at their organization to increase over the next 12 months, outnumbering the percentage of organizations that expect identities to contract by 21 to 1. In another finding, growth of identities was the second most frequently mentioned challenge organizations face with respect to Identity management today.

2. **Continued cloud adoption creates complexity.** Enterprise Strategy Group research shows public cloud adoption is poised to continue: 35% of organizations have a cloud-first approach to new application deployments versus 16% that have an on-premises-first approach, and the proportion of organizations hosting the majority of their apps in the cloud is poised to increase from 17% to 27% over the next few years.[1] This is a problem for Identity-focused teams, as 73% of respondents say public cloud use has increased the complexity of Identity management at their organization.

3. **Remote work is a continuing trend.** On average, respondents estimate half of their organization's employees work either in a hybrid manner or remotely, with 77% saying their organization's approach to remote work makes Identity management more complex.

This market landscape illustrates why it is so critical for organizations to seriously inspect their Identity practices and technologies as well as take action where it is warranted.

Challenges organizations are facing with workforce Identity management.



[1] Source: Enterprise Strategy Group Research Report, *2024 Technology Spending Intentions Survey*, February 2024.

BACK TO CONTENTS

Establishing the Workforce Identity Maturity Model

The Current State of Workforce Identity Maturity

Okta has developed a comprehensive framework for strengthening security and governance, raising productivity, and increasing efficiency through Identity.

To validate that this framework delivers on its promise when enacted by organizations, Enterprise Strategy Group created a survey to assess organizations' alignment with Okta's maturity model. It did so by translating the principles of the framework into eight categorical survey questions. The answers to these questions enabled us to determine how well aligned an organization is to best practices advocated for in Okta's maturity model. Enterprise Strategy Group then segmented respondents (and the organizations they represent) as having attained one of four levels of workforce Identity maturity. The organizations that are most mature are designated as Strategic, followed by Advanced, Scaling, and Fundamental.

Enterprise Strategy Group's analysis employed a point-based scoring system in which organizations were evaluated as having (or not having) mature Identity attributes and practices. They could then earn (or not earn) maturity points as a result. A maximum of 100 maturity points could be earned.

Attributes and practices assessed include:

- The presence of a comprehensive Identity strategy (10 points)
- Breadth of single sign-on (SSO, 10 points) and multifactor authentication (MFA) deployment (10 points)
- Use of adaptive and/or passwordless authentication (10 points)
- Federation of directory services (10 points)
- Identity and access management (IAM) solutions' integration with key business applications (10 points)
- Identity-related workflow automation (25 points)
- Adoption of identity governance administration (IGA, 7.5 points) and privileged access management (PAM) solutions (7.5 points)

In the aggregate, just 20% of organizations were evaluated as having achieved Strategic status (earning more than 80 of the 100 available maturity points. Additionally, 24% of organizations were evaluated as Advanced (earning more than 70 and up to 80 maturity points), 26% were rated as Scaling (earning more than 60 and up to 70 maturity points), and 30% were rated as Fundamental (earning 60 maturity points or fewer).

More specifics about the questions asked, possible responses, and associated maturity scores can be reviewed in the "Research Methodology and Respondent Demographics and Maturity Model Details" section of this eBook.

Organizations, by workforce Identity maturity.

BACK TO CONTENTS

"Organizations looking to increase their level of maturity should first and foremost **seek to drive more alignment with these principles**."

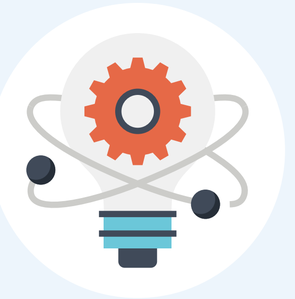
What Distinguishes a Workforce Identity Maturity Leader From Its Peers?

Okta's Workforce Identity Maturity Model is multifaceted, spanning strategies, processes, and Identity solutions. Key differences between Strategic organizations and other maturity cohorts are summarized to the right.

Taken together, these three organizational attributes determine where any given organization lands on the Workforce Identity Maturity Model. Organizations looking to increase their level of maturity should first and foremost seek to drive more alignment with these principles.

Strategic organizations develop a comprehensive approach to Identity.

Strategic organizations deploy Identity solutions both more broadly (i.e., with more solution capabilities) and more deeply (i.e., covering a greater proportion of their environments).



Strategic organizations focus on ecosystem integrations and intelligent automation.

BACK TO CONTENTS

Strategic Organizations Develop a Comprehensive Approach to Identity

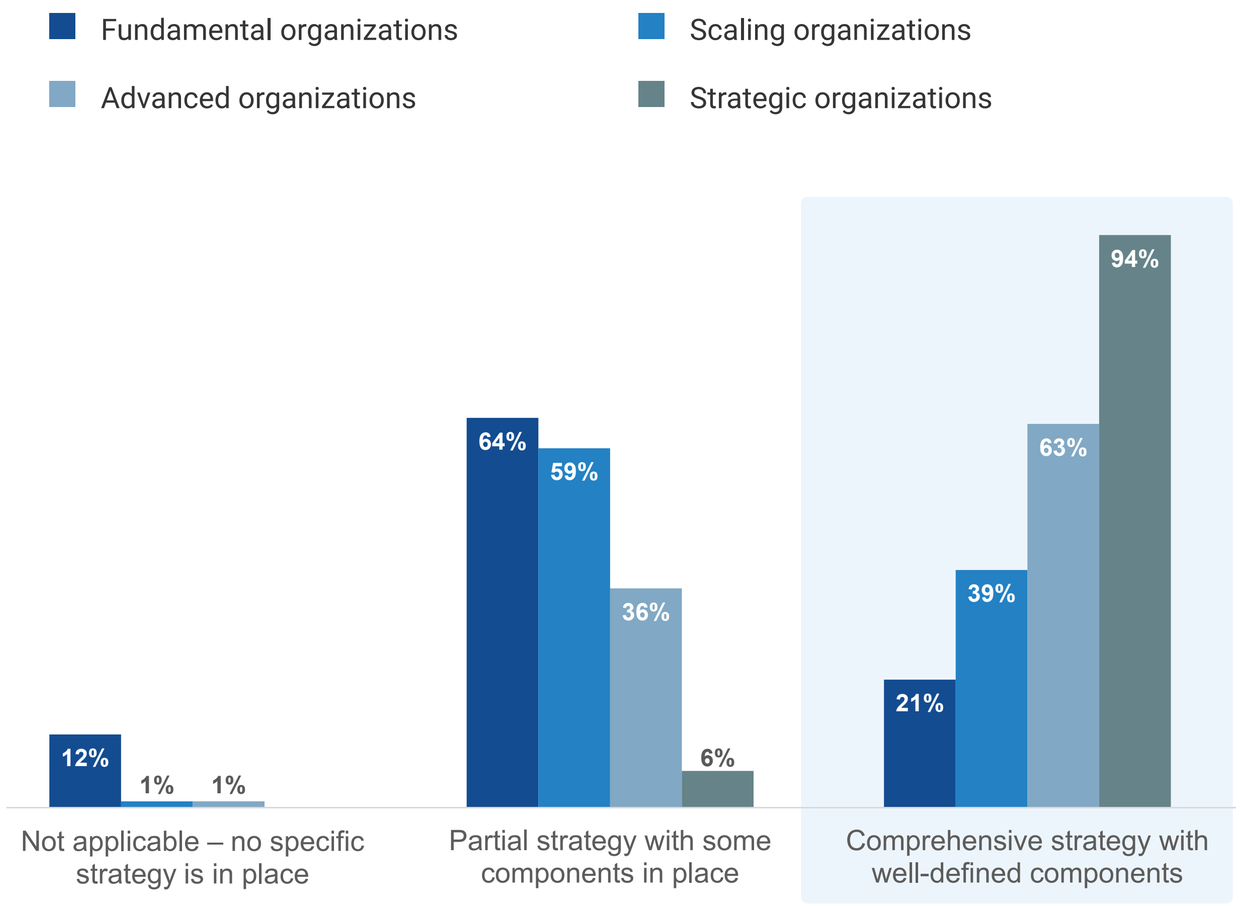
94% of organizations that reached Strategic status reported they have a comprehensive Identity strategy that includes well-defined technology roadmaps, budget expectations, and executive approval. By contrast, 63% of Advanced organizations, 39% of Scaling organizations, and just 21% of Fundamental organizations reported the same.

Such a strategy ensures alignment between Identity initiatives and overarching business objectives:

- Clear budget expectations enable effective resource allocation, ensuring adequate funding for critical Identity capabilities.
- Executive approval helps foster stakeholder engagement and collaboration across departments. It also helps align the organization's Identity strategy with the overarching business strategies prioritized at the highest levels of the organization.

A well-defined, forward-looking technology roadmap related to Identity solutions helps make sure the controls in place will be able to meet the future needs of the organization.

Which best describes your company's Identity strategy?



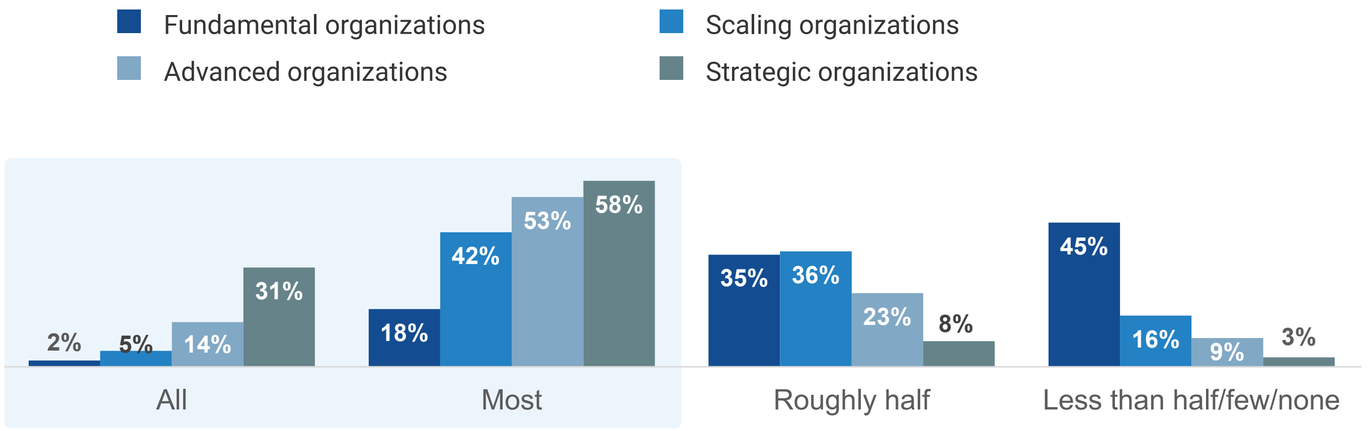
BACK TO CONTENTS

Strategic Organizations Deploy Identity Solutions More Broadly and More Deeply

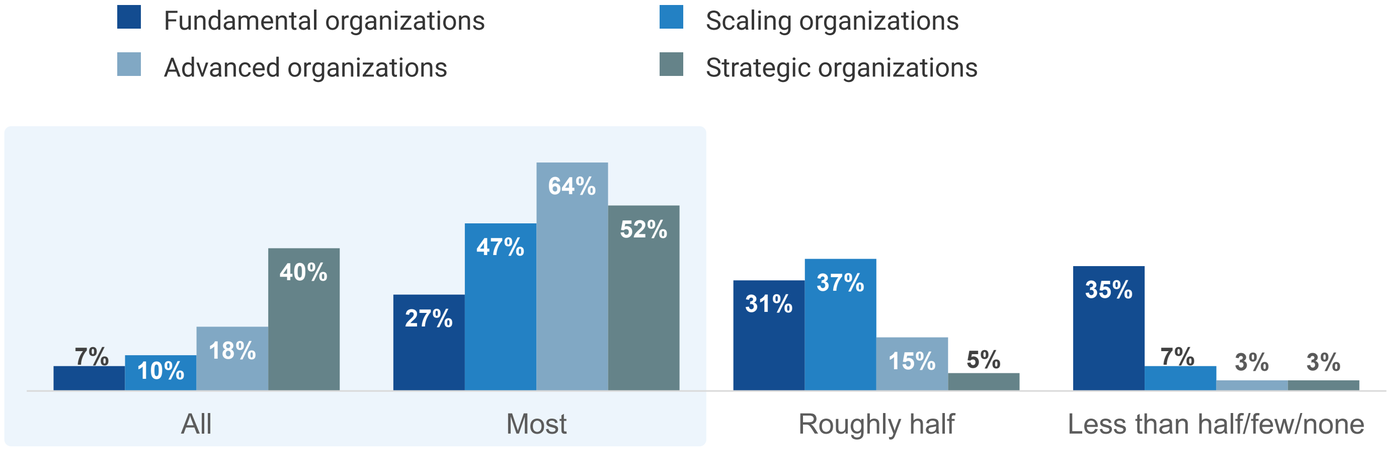
Strategic organizations were much more likely than their peers to employ several Identity capabilities and do so more completely. For example:

- 89% of Strategic organizations make most or all of their business-critical applications accessible via SSO, while just 20% of Fundamental organizations can say the same. SSO enables users to access applications with one set of credentials, enhancing convenience and productivity while minimizing frustrating and inefficient password reset processes.
- 92% of Strategic organizations protect all or most of their business-critical applications with MFA. Just 34% of Fundamental organizations can say the same. Furthermore, more than 9 out of 10 Strategic organizations report that their authentication solutions include passwordless or adaptive capabilities (versus roughly half of Fundamental organizations). MFA significantly reduces the risk of unauthorized access by verifying users with multiple authentication factors (e.g., their password and a biometric factor or one-time code). With greater coverage and the ability to adapt MFA requirements based on the level of risk represented, Strategic organizations gain a significant security advantage.
- Strategic organizations are much more apt than their peers to have adopted IGA (77% versus 13% of Fundamental organizations) and PAM solutions (61% versus 10% of Fundamental organizations). IGA and PAM aid organizations with regulatory compliance while also helping to protect organizations from both insider threats and external threats by providing oversight of user access rights and permissions as well as restricting and monitoring privileged user access, respectively.

The proportion of business-critical applications accessible via SSO.



The proportion of business-critical applications protected by MFA.



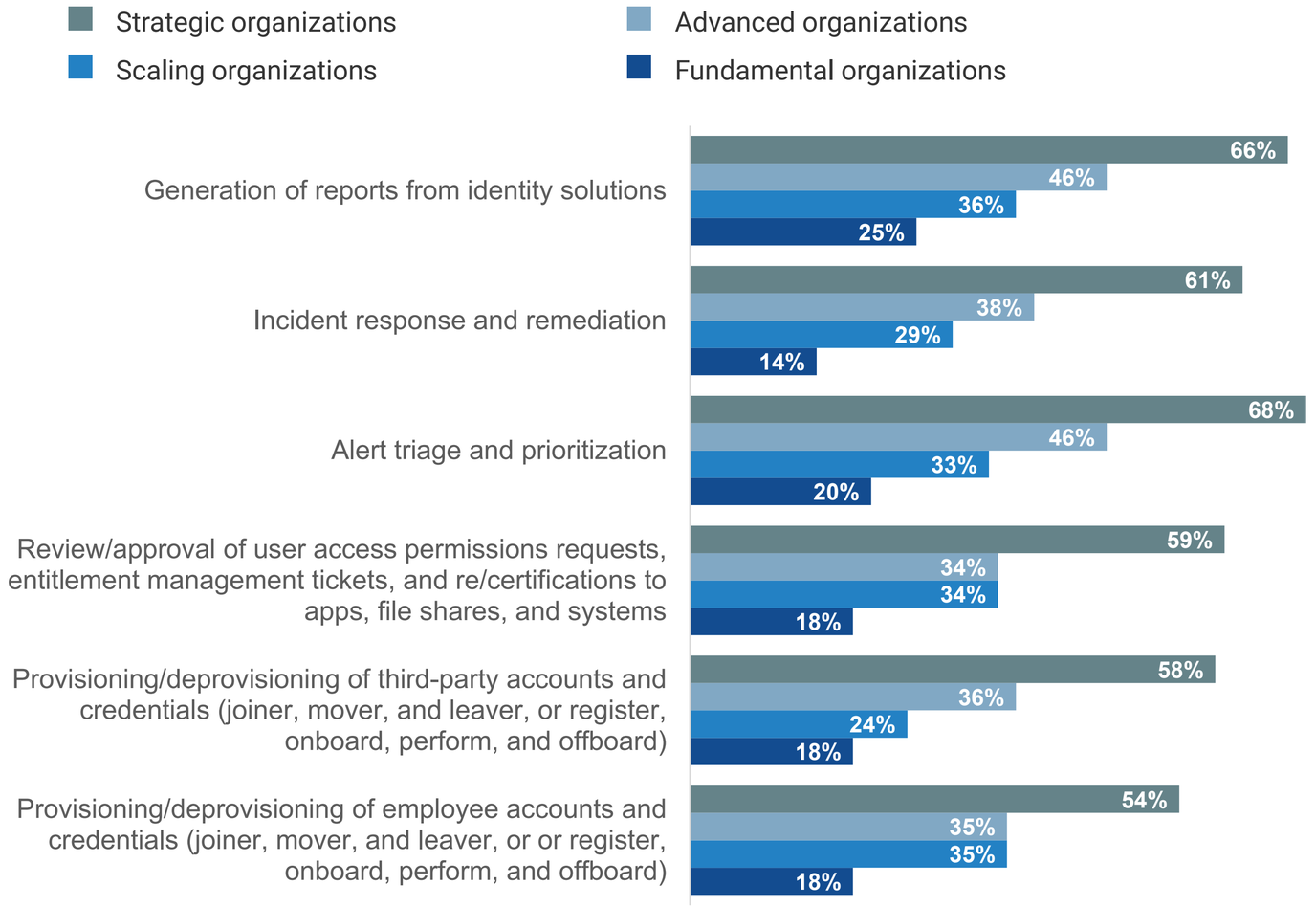
BACK TO CONTENTS

Strategic Organizations Focus on Ecosystem Integrations and Intelligent Automation

Strategic organizations are leaning into an approach to Identity that emphasizes ease of integration and workflow automation, delivers greater efficiency, and reduces the risk of human error:

- 91% of Strategic organizations have completely federated their various directory services, while only 20% of Fundamental organizations can say the same. This interconnection of identity repositories enables seamless, yet secure, authentication and authorization across disparate systems and platforms.
- Strategic organizations tend to invest in Identity solutions that ship with preconfigured connectors to a variety of business applications, making integration quick and simple. For example, 94% said their primary IAM solution had a vendor-provided connector to their collaboration tools, 93% said it included a connector to their CRM solution, and a similar percentage reported the inclusion of such a connector to their back-office finance (88%) and HR (92%) apps.
- Strategic organizations have much more heavily automated, common Identity-related tasks like creating reports (66% versus 25% of Fundamental organizations), responding to Identity-related incidents (61% versus 14), triaging Identity-related alerts (68% versus 20%), and more. This degree of automation helps Strategic organizations keep pace with their growing environments and enforce consistency regardless of environment (on premises or cloud) and user location (in-office or remote).

Percentage of respondents reporting each Identity-related workflow is highly automated at their organization.



BACK TO CONTENTS

The Direct Impacts of a Mature Approach to Workforce Identity

Strategic Organizations See Identity Solutions as Enabling the Business

In the survey, respondents were asked what impact their Identity solutions were having across a wide variety of business operations. Respondents could report that Identity solutions enable, have no impact on, or hinder agility, compliance efforts, collaboration, end-user experience, remote work, and more.

When the maturity model is applied to the answers to this question, it quickly becomes clear that not all organizations achieve the same level of business enablement from their Identity solutions. Strategic organizations were much more likely than their Fundamental counterparts to say their solutions are delivering strong enablement, including being:

3.9x AS LIKELY

to say their solutions strongly enable agility (59% versus 15%).

4.2x AS LIKELY

to say their solutions strongly enable collaboration (59% versus 14%).

3.6x AS LIKELY

to say their solutions strongly enable productivity (57% versus 16%).

The percentage of respondents reporting their Identity solutions strongly enable each area of their business.

BACK TO CONTENTS

Strategic Organizations Say Their Approach to Identity Enhances Security

While the prior data underscores the business enablement advantage Strategic organizations achieve, respondents were also asked about the relationship between their approach to Identity and cybersecurity operations. Here again, respondents could say their Identity strategies are helping, have no impact on, or are hindering tasks like incident response, threat detection and mitigation, and even the adoption of Zero Trust strategies.

As with business enablement, it is clear that Strategic organizations are achieving an advantage. Strategic organizations were much more likely than their Fundamental counterparts to say their solutions are significantly helping security teams, including being:

3.4x AS LIKELY

to say their approach to Identity significantly helps their move toward Zero Trust (61% versus 18%).

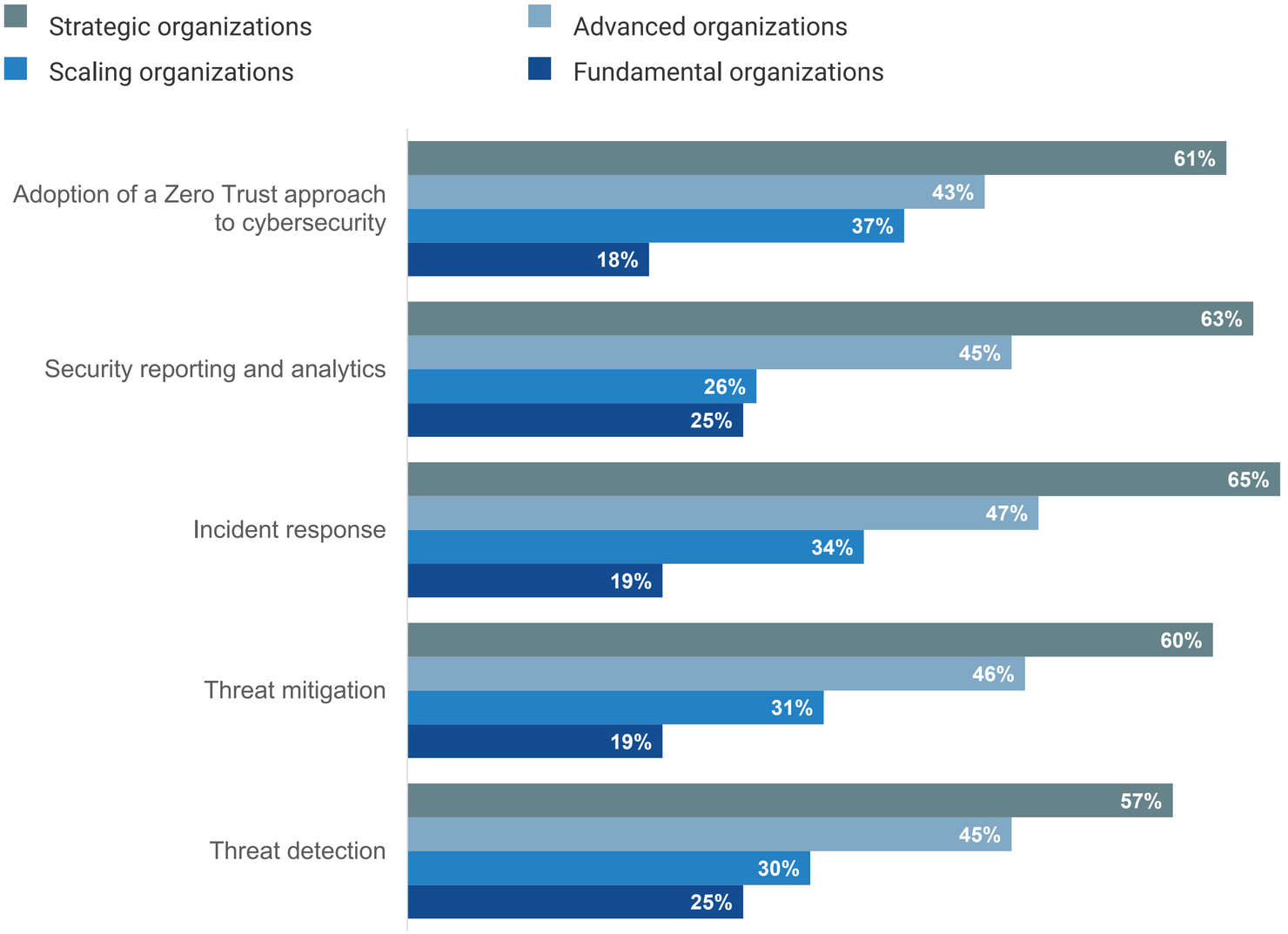
3.4x AS LIKELY

to say their approach to Identity significantly helps with incident response (65% versus 19%).

3.2x AS LIKELY

to say their approach to Identity significantly helps to mitigate threats (60% versus 19%).

The percentage of respondents reporting their Identity solutions significantly help each area of security operations.



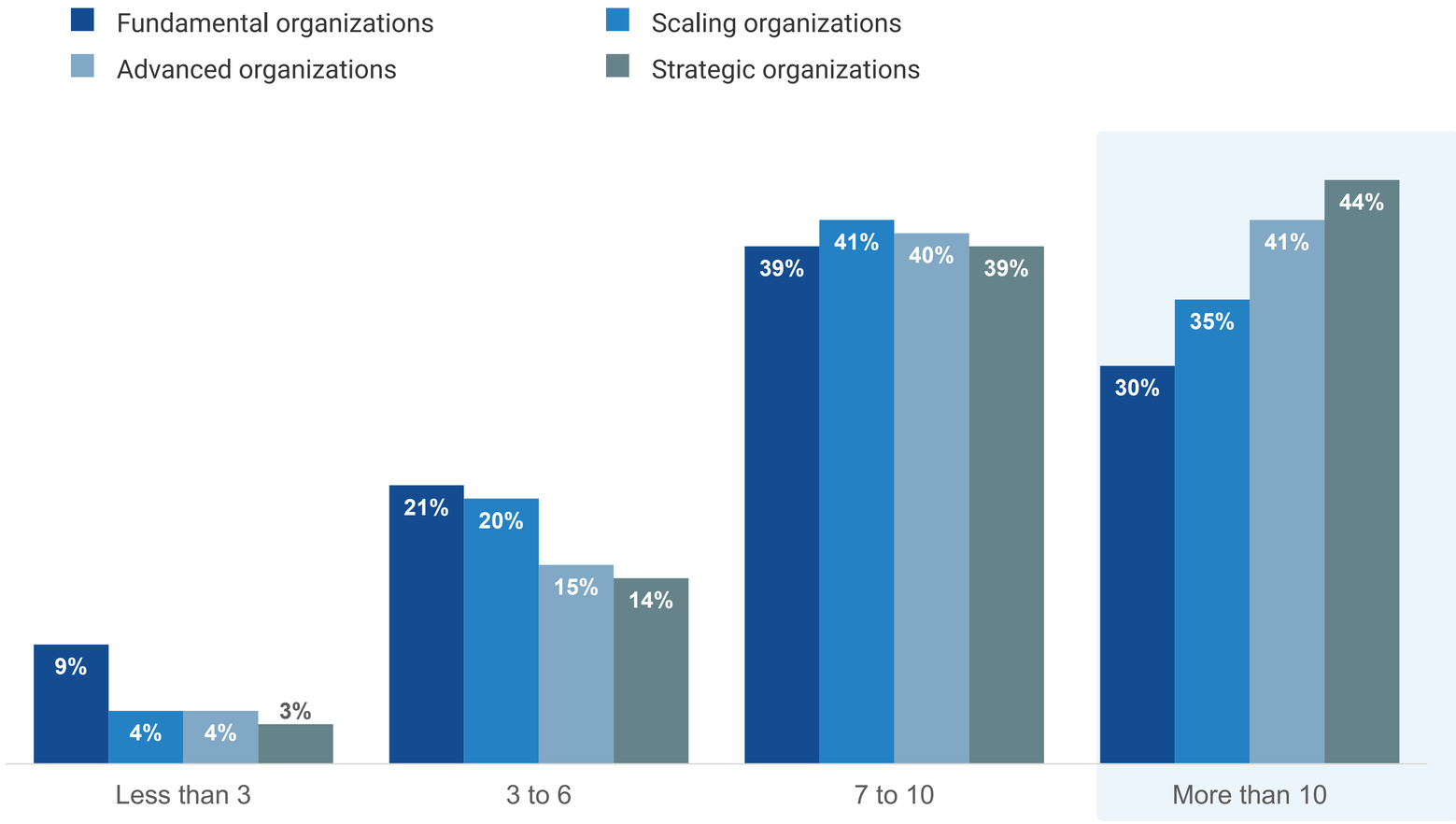
BACK TO CONTENTS

Strategic Organizations Are Supercharging Operational Efficiency

Respondents were asked to quantify the efficiency savings enabled by the Identity solutions they've invested in over the last 24 months. Specifically, they were asked to consider improvements in areas like security efficiencies, IT operations, and end-user productivity.

In the aggregate, nearly all organizations reported material gains: 90% estimated saving more than three full-time equivalents (FTEs) as a result of their investments. But once again, Strategic organizations saw the biggest results, with the plurality reporting their recent Identity-related investments had saved them more than 10 FTEs.

How many full-time equivalents have been saved by Identity-related investments made in the past 24 months?



BACK TO CONTENTS

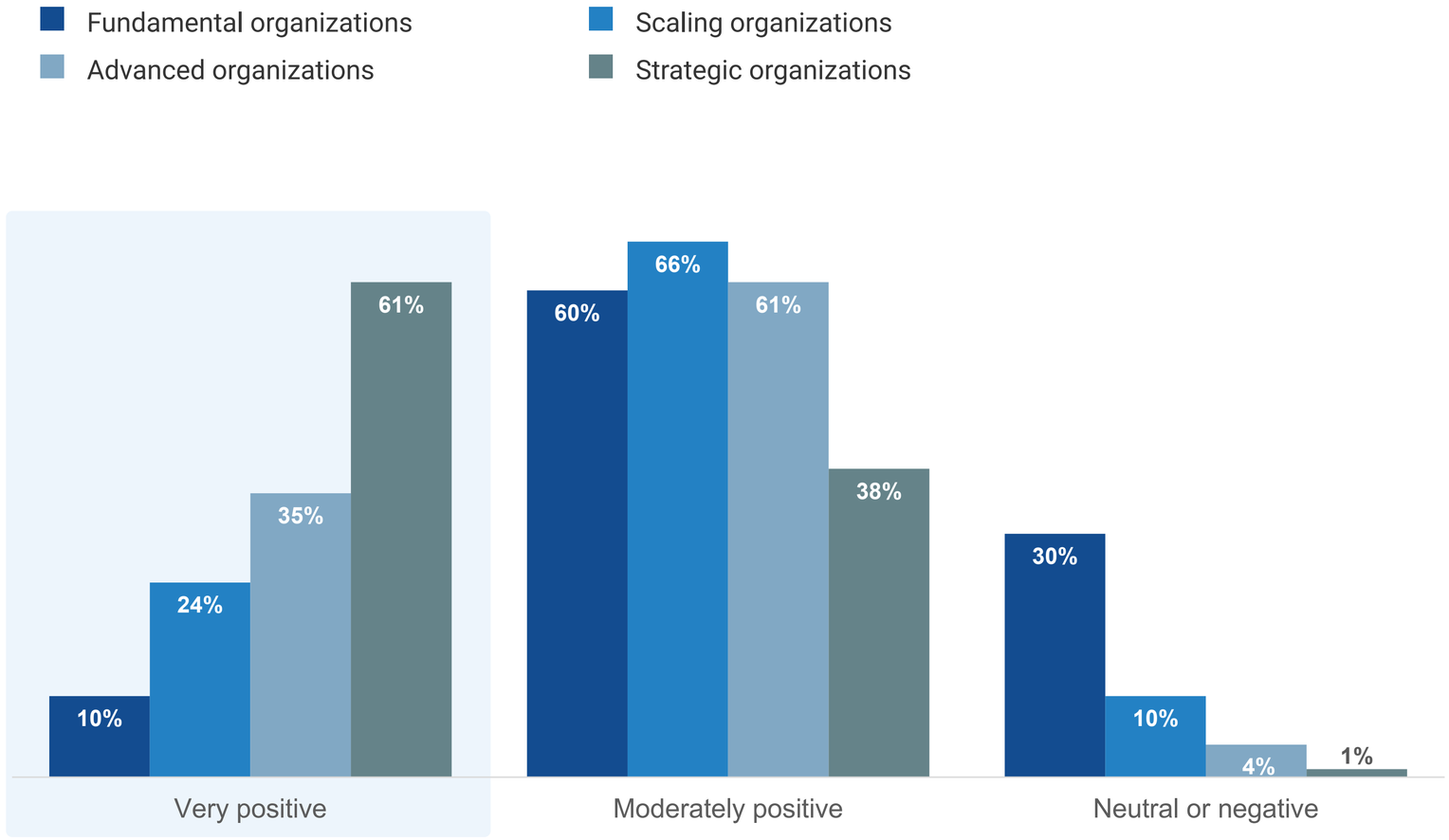
6.1x AS LIKELY

as Fundamental organizations to **be achieving a very positive ROI** from their Identity investments.

Strategic Organizations Receive Market-leading ROI From Identity Solutions

Finally, respondents were asked to characterize the ROI they have received on the Identity-related solutions they've invested in over the prior few years. While 86% of all respondents say their organization is achieving a positive return on the investments they've made in Identity solutions, it should not be surprising, given the data previously discussed, that Strategic organizations were much more apt to report their ROI has been "very positive." In fact, they are 6.1x as likely as Fundamental organizations to be achieving a very positive ROI from their Identity investments.

How would you describe the ROI your organization has received on recent Identity-related solutions?



BACK TO CONTENTS

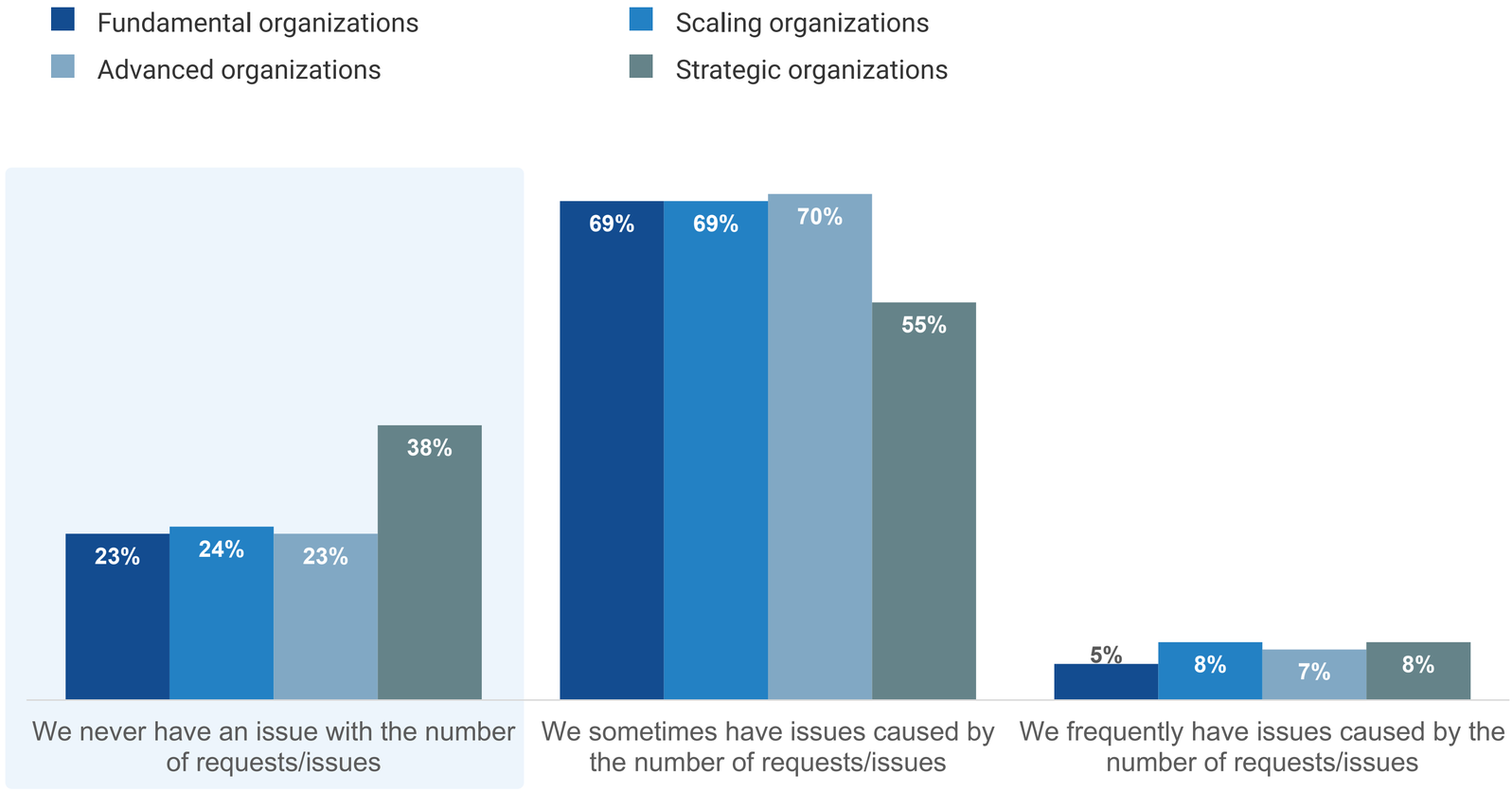
Additional Outcomes Leaders in Workforce Identity Maturity Achieve

Strategic Organizations Report Their Identity Management Teams Can Keep Up With Requests More Effectively

As discussed in the previous section of this eBook, Strategic organizations are much more apt than their less mature counterparts to directly credit their Identity solutions with providing value. The research went on to question respondents about a number of aspects of their operations. The correlations observed in these questions further bolster the argument that organizations should prioritize deploying capabilities that are aligned to a more mature approach to Identity.

Respondents were asked to describe the number of Identity-related requests and issues they handle from end users, and Strategic organizations more often reported they never have an issue with the volume of requests. The ability to keep up with end-user demand is a critical capability, as more nimble Identity teams can respond to end-user requests faster, increasing both user satisfaction and productivity.

How often Identity-related requests and issues overwhelm administrators.

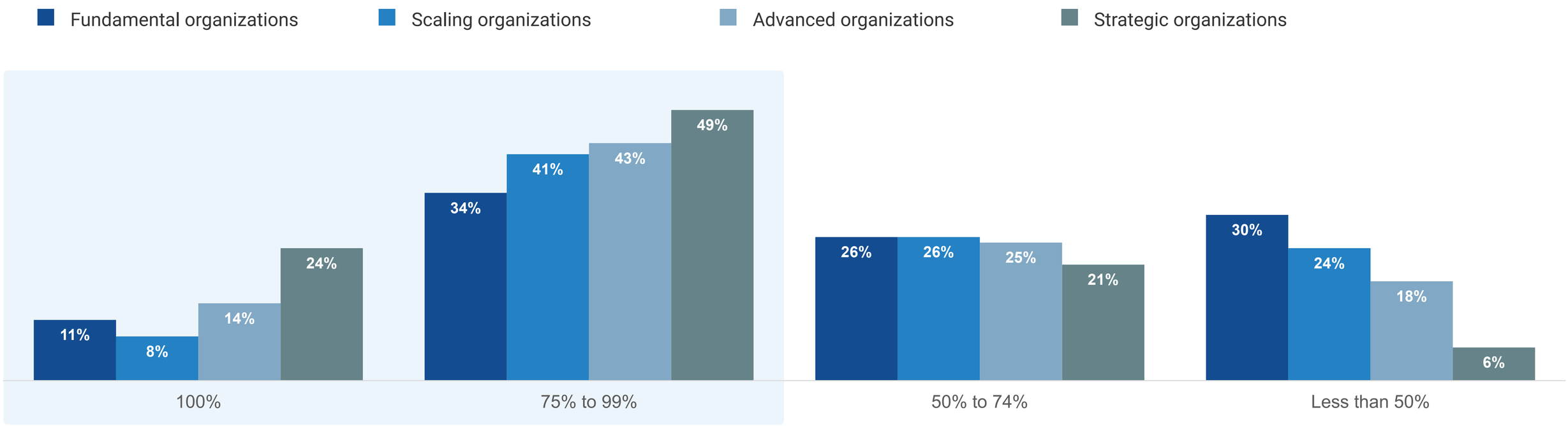


BACK TO CONTENTS

Strategic Organizations Can Keep Pace With Security Alerts More Easily

The data also makes it clear that workforce Identity maturity is correlated with an improved ability to keep up with security alerts. Respondents were asked to quantify how many Identity-related alerts generated by their security controls their staff are able to triage and investigate. Respondents at Strategic organizations more often said they triage and respond to 75% or more of alerts occurring in their environments (73% versus 45%). On the flip side, alert fatigue and a deluge of false positives at Fundamental organizations make them much more likely to not investigate the majority of their alerts (30% versus 6% of Strategic organizations).

What percentage of Identity-related security alerts are actually triaged and responded to?



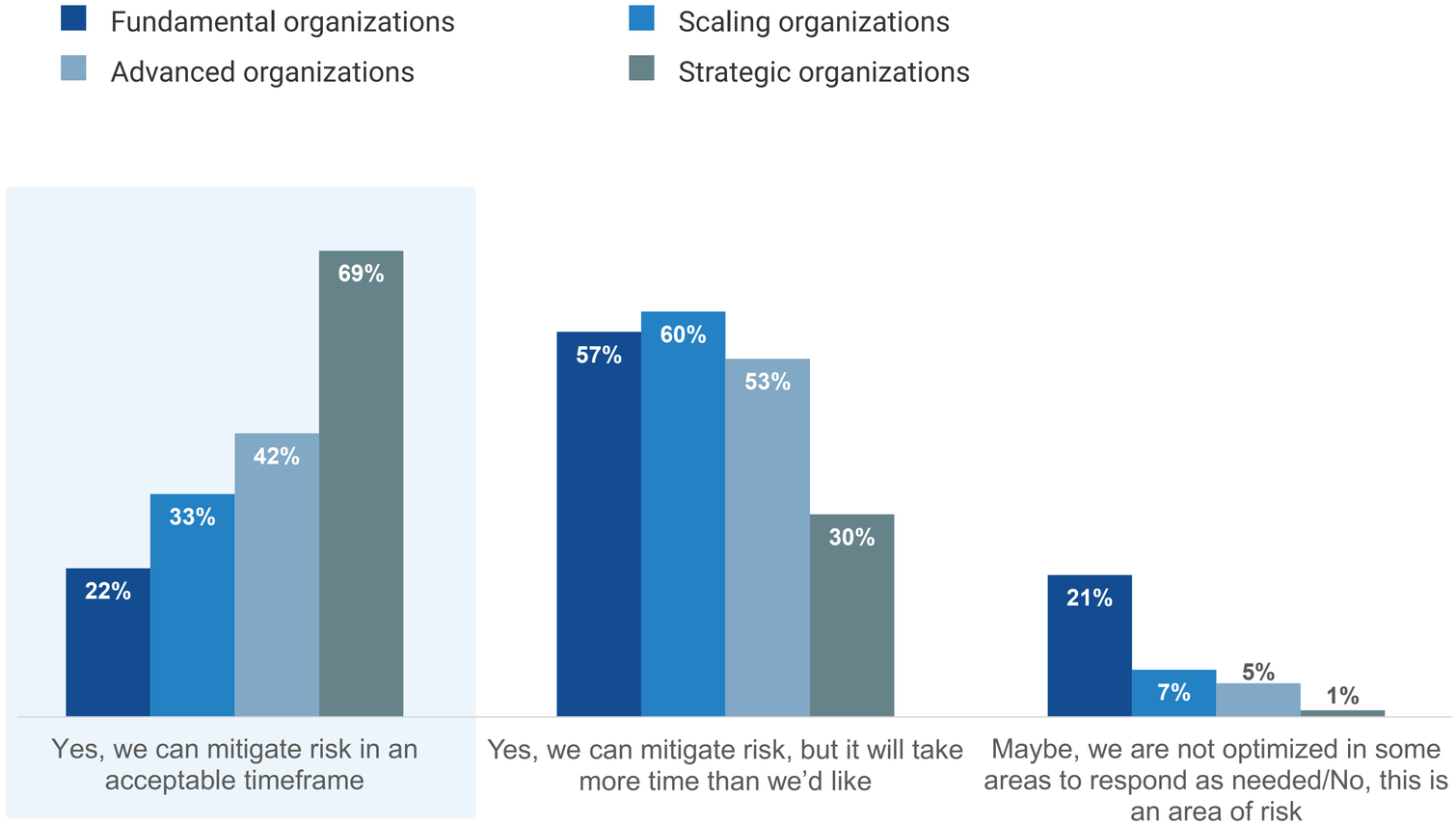
BACK TO CONTENTS

Strategic Organizations Are More Confident in the Agility of Their Response to Identity-related Risks

Finally, respondents were asked a hypothetical question: “If made aware of a critical workforce Identity-related incident or attack that affects sensitive data, do you feel your organization has the people, skills, processes, and technology to mitigate risk?”

Those at Strategic organizations were much more bullish about their capabilities: 69% responded that they believe they could mitigate risk effectively and within an acceptable timeframe—3.1x the rate of respondents at Fundamental organizations.

Can your organization mitigate critical Identity-related incidents with agility?



BACK TO CONTENTS

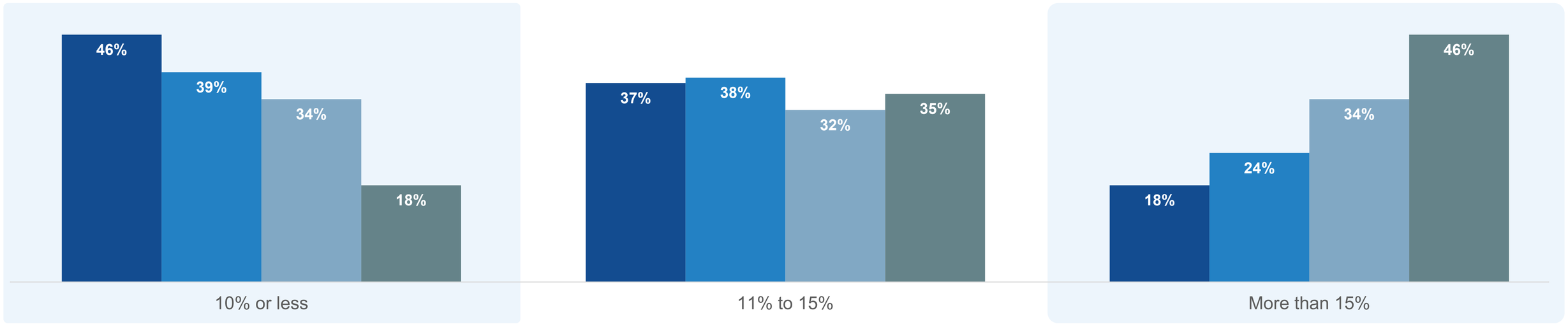
Learning From the Leaders

Strategic Organizations Tend to Allocate More Funding for Identity Solutions

Beyond the specific actions and best practices advocated for within the maturity model, the research uncovered a few key distinctions between Strategic organizations and their less-mature peers.

In the survey, respondents were asked approximately how much of their annual IT technology budget (i.e., excluding salaries) is dedicated to Identity solutions. Relative to Fundamental organizations, Strategic organizations allocate an average of ~47% more of their IT budget to Identity tools (16% versus 10.9%).

Percentage of IT technology budgets allocated to Identity solutions.



BACK TO CONTENTS

"Relative to Fundamental organizations, Strategic organizations were more likely **to say five of the six department heads listed were engaged**."

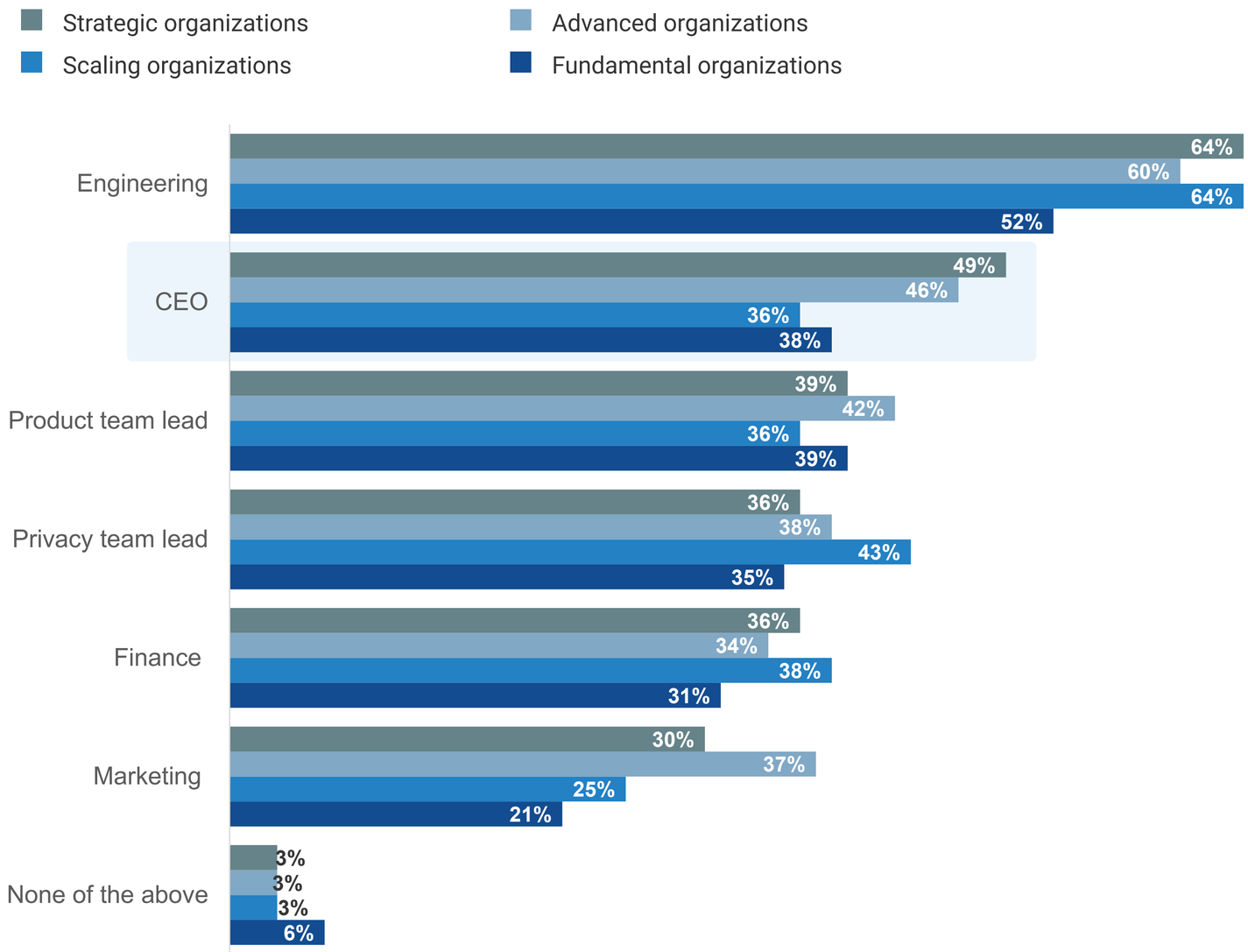
Executives at Strategic Organizations Are More Involved

Executive engagement is another differentiator between Strategic organizations and their peers. Respondents were asked which department heads outside of IT and security are actively engaged in developing and executing Identity strategies.

While there are several differences in the data, the most noteworthy is that 49% of CEOs at Strategic organizations are involved versus 38% of those at Fundamental organizations. In fact, relative to Fundamental organizations, Strategic organizations were more likely to say five of the six department heads listed were engaged.

This higher level of executive engagement is helpful to securing budget and ensuring policies and best practices are adopted throughout the organization.

What functional leaders are actively involved in your organization's Identity strategy?



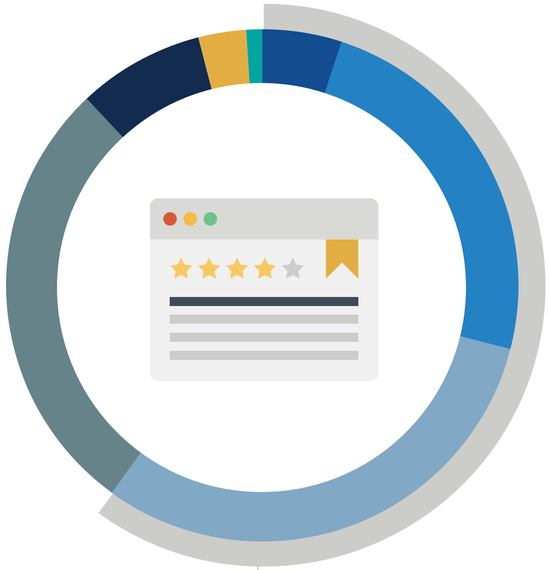
BACK TO CONTENTS

When Evaluating Your Organization, Objectivity Is Critical

The research shows that organizations tend to overestimate their Identity capabilities. In the survey, respondents were asked to subjectively self-assess their organization's Identity maturity level. Four responses were offered, from "very mature" to "very immature." Enterprise Strategy Group compared this self- assessment to the maturity model outputs and found that 60% of respondents graded their organization at a higher level than the maturity model.

This type of bias underscores the importance of objectivity to mitigate skewed decision-making and flawed strategies.

Visualizing how much organizations tend to overrate their maturity.



5%
Overrated by 3 levels

24%
Overrated by 2 levels

31%
Overrated by 1 level

28%
Accurately self assessed maturity level

8%
Underrated by 1 level

3%
Underrated by 2 levels

1%
Underrated by 3 levels

"Enterprise Strategy Group compared this self-assessment to the maturity model outputs and found that **60% of respondents graded their organization at a higher level than the maturity model."**

BACK TO CONTENTS

How Okta Can Help

Okta Workforce Identity Cloud provides easy, secure access for your workforce so you can focus on other strategic priorities—like reducing costs and doing more for your customers.

LEARN MORE

RESEARCH METHODOLOGY AND RESPONDENT DEMOGRAPHICS

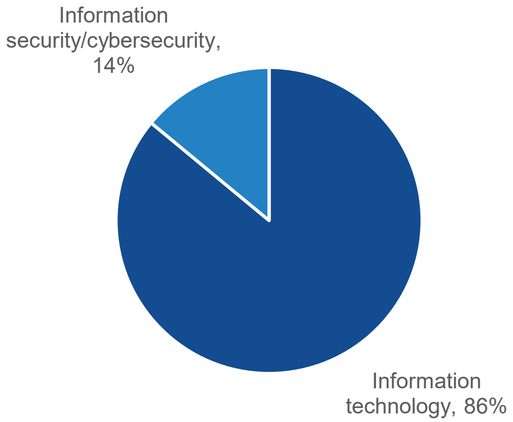
To gather data for this eBook, Enterprise Strategy Group conducted a comprehensive online survey of 600 IT and security practitioners and decision-makers with responsibility and/or influence over their organization's Identity-related technology investments (e.g., IAM, MFA, SSO, etc.).

Organizations represented span all private- and public-sector organizations in North America (U.S., Canada; 50% of respondents), Western Europe (U.K., Germany; 26%), and Asia (Australia, New Zealand, Singapore; 25%). The survey was fielded between November 13 and November 29, 2023.

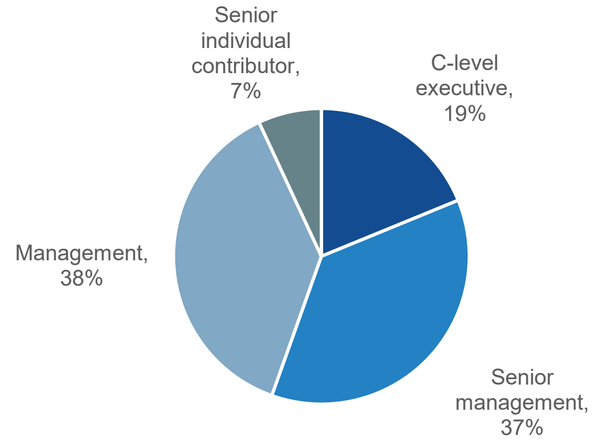
The margin of error at the 95% confidence level for this sample size is + or - 4 percentage points.

Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

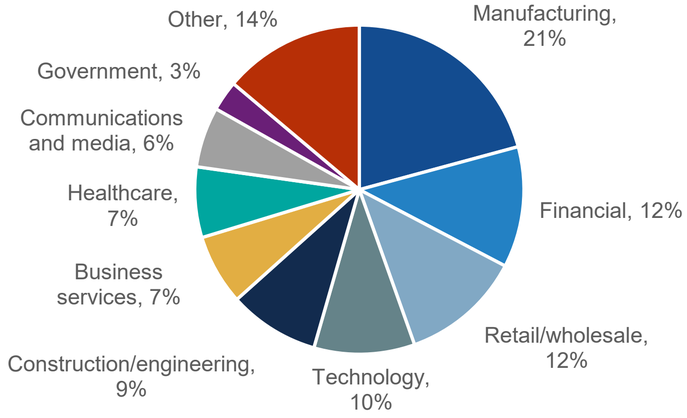
Respondents by job function.
(Percent of respondents, N=600)



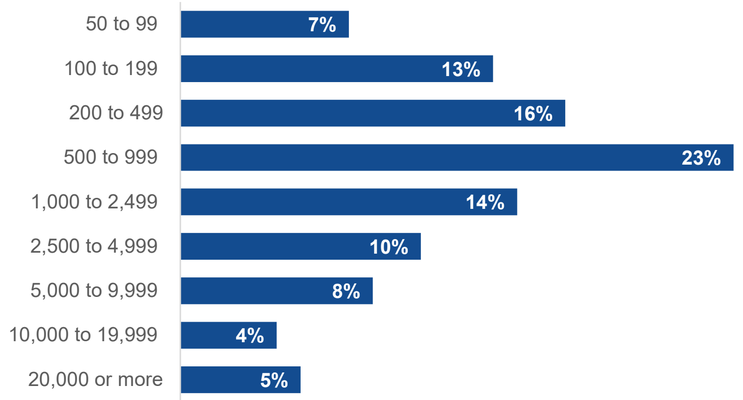
Respondents by seniority.
(Percent of respondents, N=600)



Respondents by industry.
(Percent of respondents, N=600)



Respondents by number of employees.
(Percent of respondents, N=600)



BACK TO CONTENTS

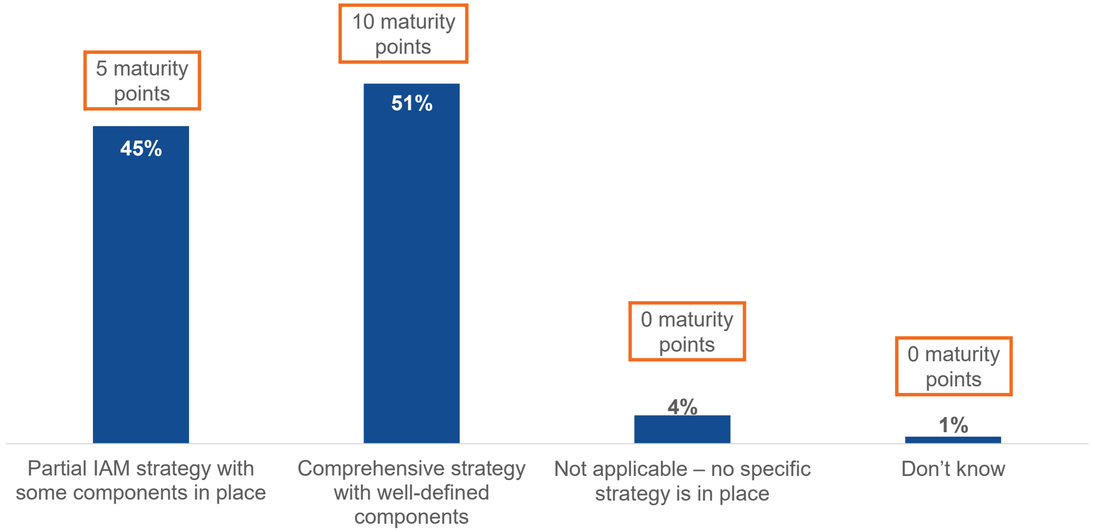
MATURITY MODEL DETAILS

To evaluate how mature an organization's Identity practices are, Enterprise Strategy Group developed a maturity model that evaluated eight multifaceted questions about the technologies and processes in place.

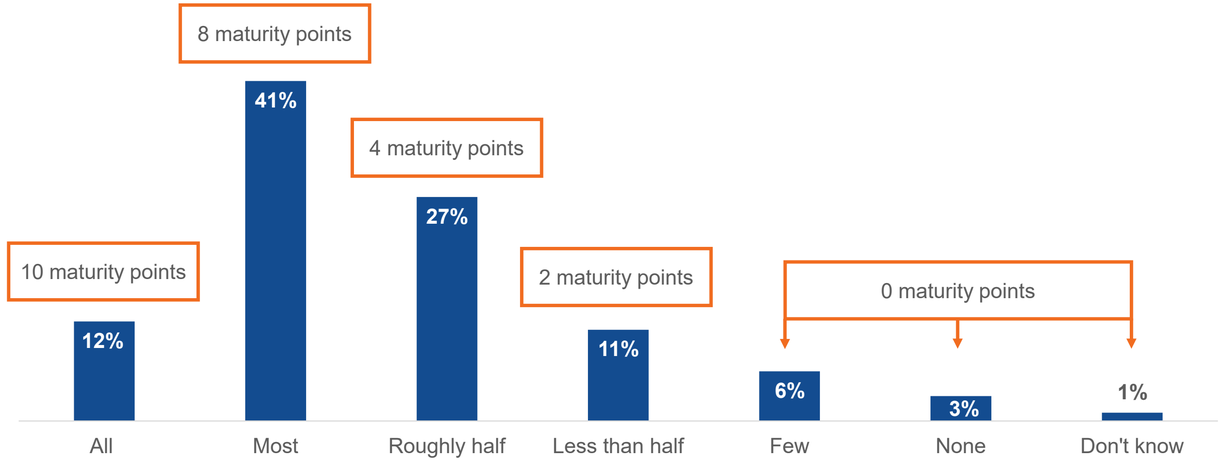
Based on the answers to these questions, organizations with a mature approach earned more maturity points, and those with an immature approach earned fewer points. Respondents' organizations could earn between 0 and 100 maturity points. Strategic organizations were defined as those organizations earning more than 80 maturity points, Advanced organizations as those that earned more than 70 and up to 80 maturity points, Scaling organizations as those that earned more than 60 and up to 70 maturity points, and Fundamental organizations as those that earned 60 points or less.

The questions Enterprise Strategy Group asked to assess maturity are shown in the following figures, along with the number of maturity points ascribed to each response.

Maturity input: Does the organization have a comprehensive Identity strategy? (N=600)

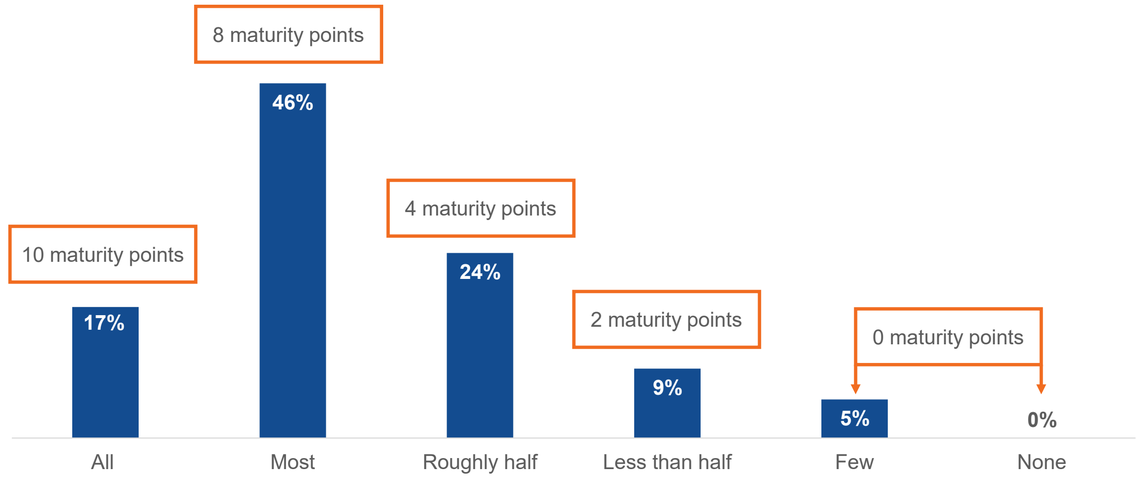


Maturity input: What is the breadth of SSO among business-critical apps? (N=600)

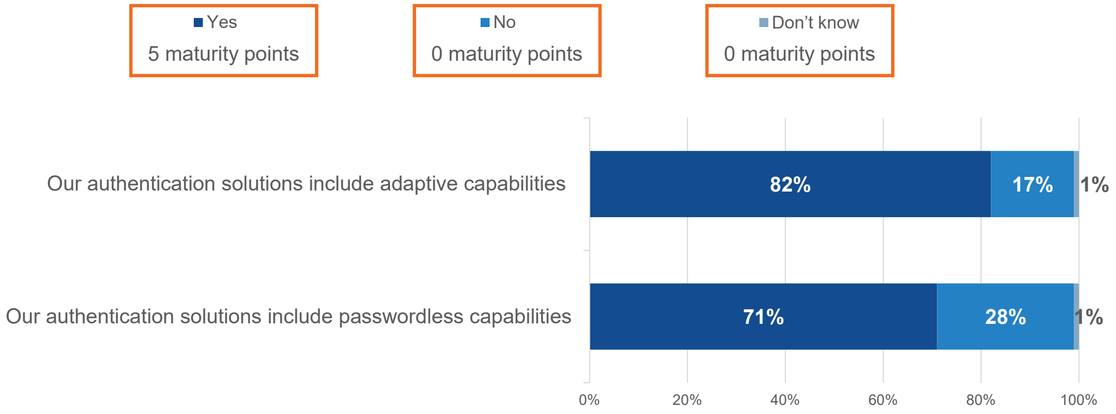


BACK TO CONTENTS

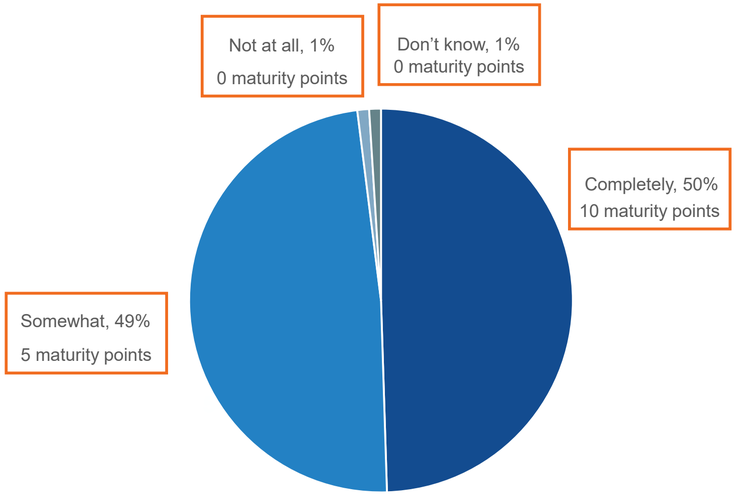
Maturity input: What is the breadth of MFA across business-critical apps? (N=600)



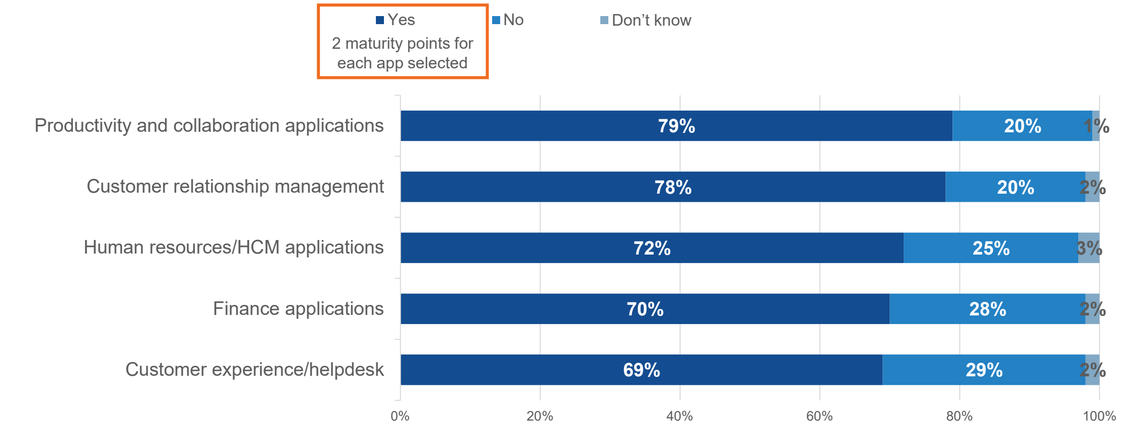
Maturity input: Does authentication include adaptive and/or passwordless capabilities? (N=598)



Maturity input: Has the organization federated its directory services? (N=547)

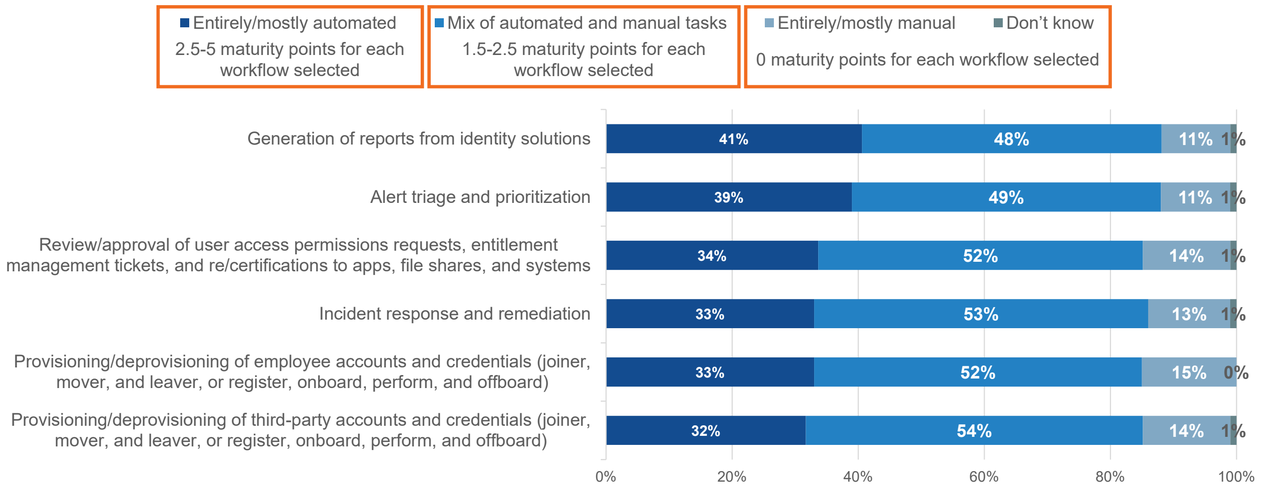


Maturity input: Does the organization leverage IAM solutions that easily integrate with key business applications? (N=600)

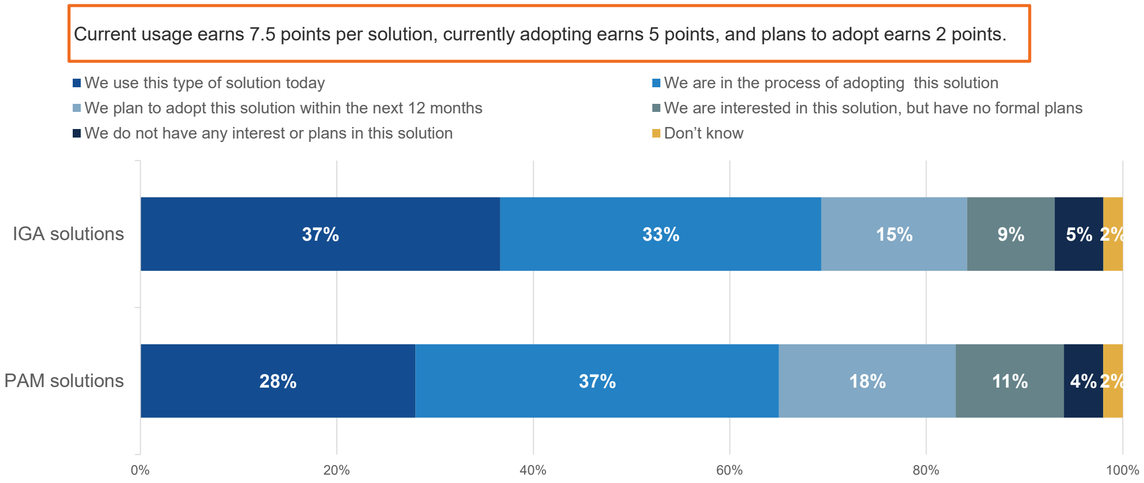


BACK TO CONTENTS

Maturity input: Has the organization automated Identity tasks to reduce risk associated with manual work or custom scripting? (N=600)



Maturity input: Has the organization adopted IGA and PAM solutions to round out their IAM solution set? (N=600)



BACK TO CONTENTS

Enterprise Strategy Group™
by TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.