

# The State of Identity Security

Opening Doors for the Right Entities  
and Locking Out the Bad Actors

**Melinda Marks** | Practice Director

**Todd Thiemann** | Senior Analyst

ENTERPRISE STRATEGY GROUP

MARCH 2024

# Research Objectives

Organizations continue to rely on identities that are susceptible to compromise, abuse, misuse, and theft. Risk is compounded by over-permissive, static access rights that provide little to no visibility into access trends or, most importantly, who is accessing what and how they are doing so.

Despite the transformation to a dynamic, amorphous perimeter, a multitude of identity security solutions and managed identity services exist. Unfortunately, organizations have been slow to pivot their security programs to an approach that incorporates identities as a foundational aspect of their cybersecurity strategy.

However, CISOs and security professionals are beginning to understand the importance of securing identities. With a decade of evidence on the risks and a plethora of identity security solutions, identity is shifting from the domain of IT operations into cybersecurity.

To gain further insight into these trends, TechTarget’s Enterprise Strategy Group surveyed 372 IT, cybersecurity, and application development professionals at organizations in North America (US and Canada) responsible for or involved with identity security technologies and processes.

## THIS STUDY SOUGHT TO:

**Define** the scope, scale, and growth of identities organizations must manage.

**Determine** whether organizations have suffered identity-related breaches, and if so, why and how often.

**Establish** who is responsible for securing identities, including the key stakeholders influencing and making identity security purchasing decisions.

**Highlight** the manner in which security concerns are driving a shift in responsibility for identity from IT operations to cybersecurity.




KEY FINDINGS



Machine and Workload Identities  
Outnumber Workforce Identities

PAGE 4



Multiple Account or Credential  
Compromise Is the Norm

PAGE 7



MFA and Passwordless  
Authentication Implementations  
Are Becoming Extensive

PAGE 13



Cloud Provides Identity  
Challenges While ITDR and  
ISPM Gain Momentum

PAGE 16



Identity Security Is  
a Team Sport

PAGE 19



Investment in Identity Security  
Is Growing

PAGE 21



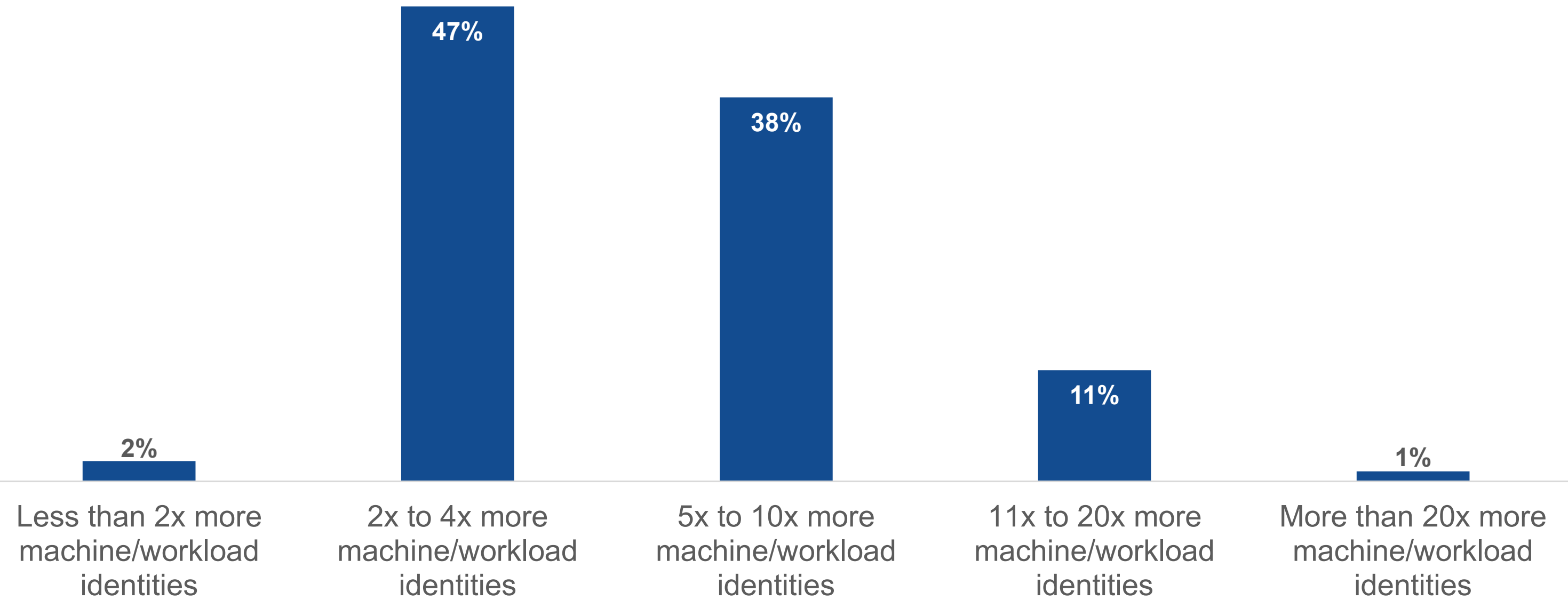
# **Machine and Workload Identities Outnumber Workforce Identities**

## Machine and Workload Identities Outnumber Workforce Identities

The majority of organizations agree (44%) or strongly agree (29%) that protecting machine/workload identities has been a challenge.

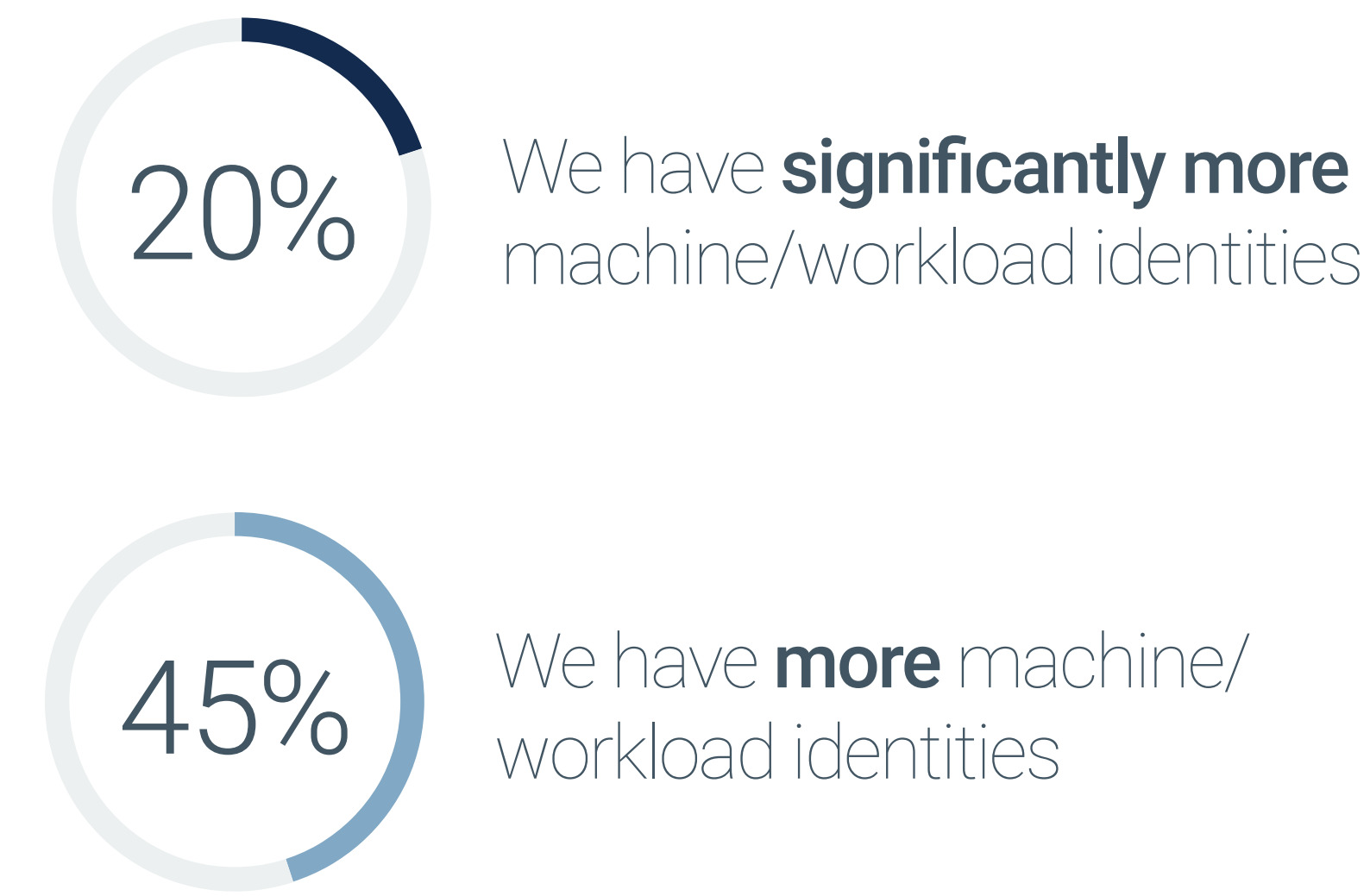
This is because nearly two-thirds (65%) of organizations report that their machine/workload identities outnumber their workforce identities. Specifically, half of organizations estimate they have at least five times more machine than workforce identities. That means, on average, there are approximately 6.1 machine/workload identities for every workforce identity.

Approximately how many more machine/workload identities does your organization support relative to its workforce identities?



73%  of organizations report that **protecting machine/workload identities** has been a challenge.

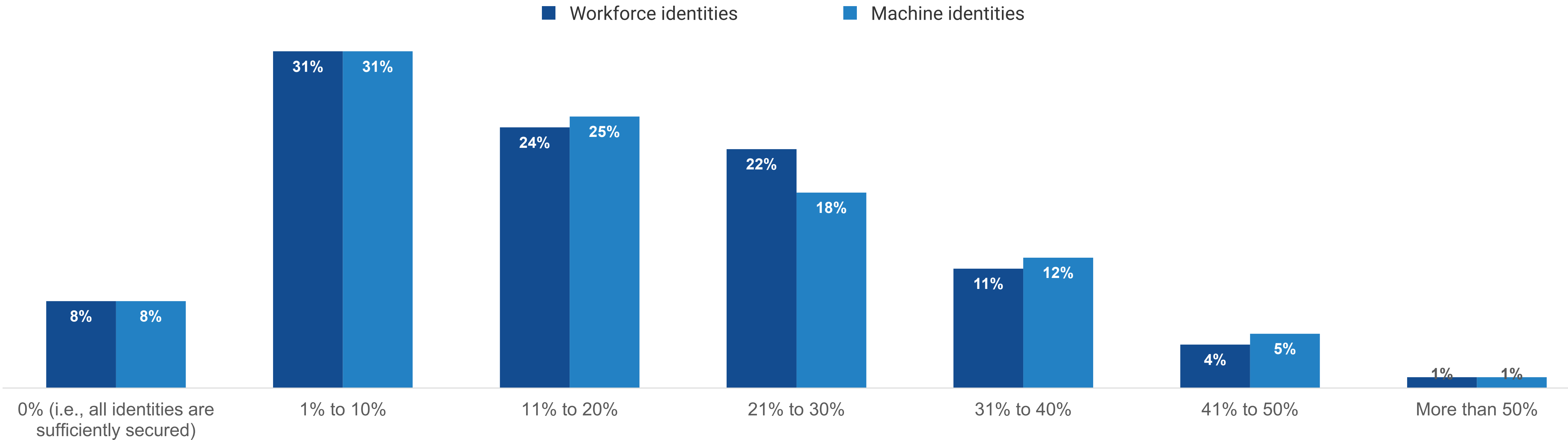
How does the number of machine/workload identities in your organization compare to the number of workforce identities?



# Machine, Workload, and Workforce Identities Are Insufficiently Secured

Regardless of the ratio of machine to workforce identities, the fact is that these credentials make enticing targets for bad actors intent on finding an ingress to corporate networks and systems. As such, it is concerning that only 8% of organizations believe that all of their workforce and/or machine identities are sufficiently secured. Conversely, nearly one in five organizations estimate that more than 30% of all machine/workload and workforce identities aren't sufficiently secured.

Approximate percentage of identities that are insufficiently secured.



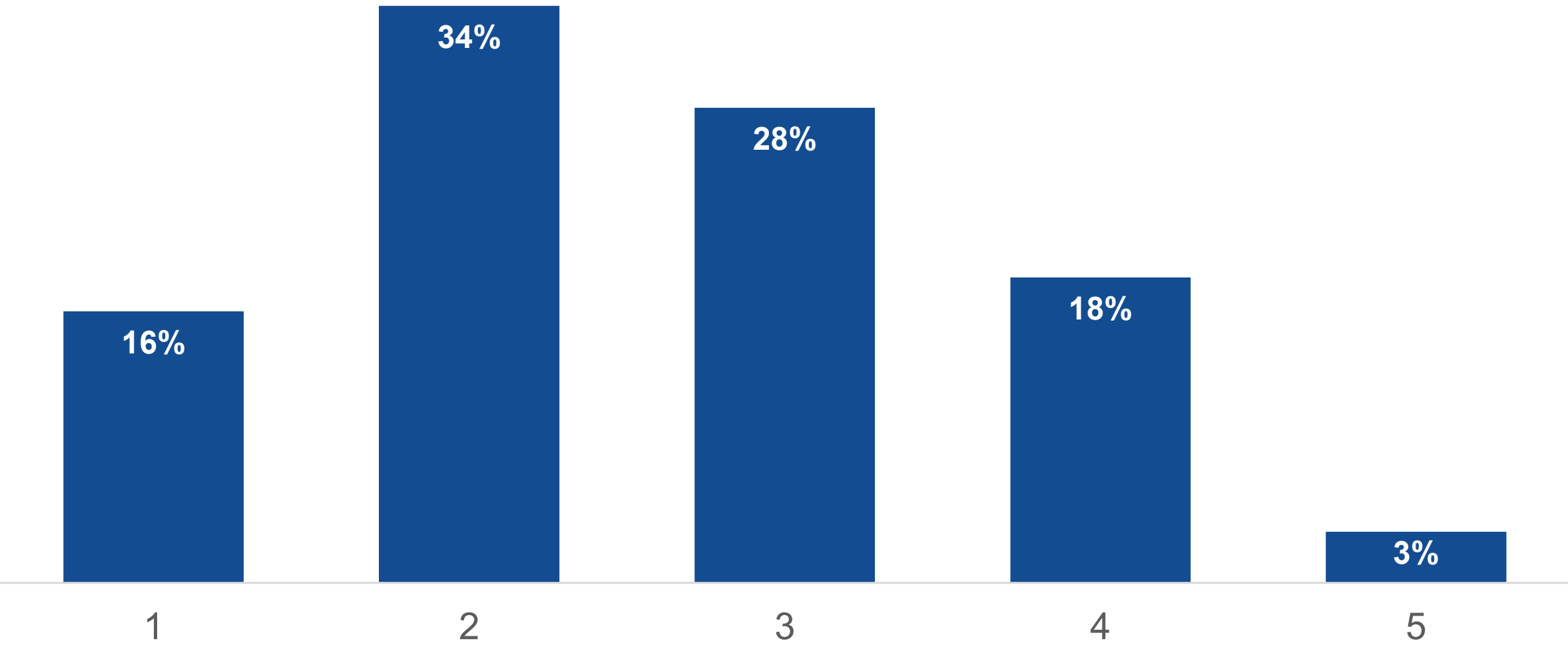


**Multiple Account or Credential  
Compromise Is the Norm**

# Multiple Workforce Account/Credential Compromise Is Common

Despite a threat landscape that continues to grow larger and more complex, organizations keep relying on identities that are susceptible to compromise, abuse, misuse, and theft. This is compounded by the fact that employees don't have sufficient training on or an understanding of cyberthreats. Indeed, half of organizations know (24%) or suspect (26%) they have had workforce accounts or credentials compromised in the last year. Among those organizations that know or suspect that employee accounts or credentials have been breached within the past 12 months, the majority (82%) have suffered multiple incidents over this period, with more than one in five citing at least five such occurrences.

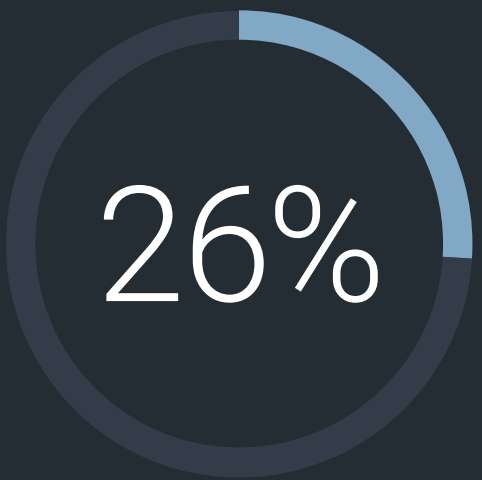
Number of times workforce accounts or credentials have been compromised in the past 12 months.



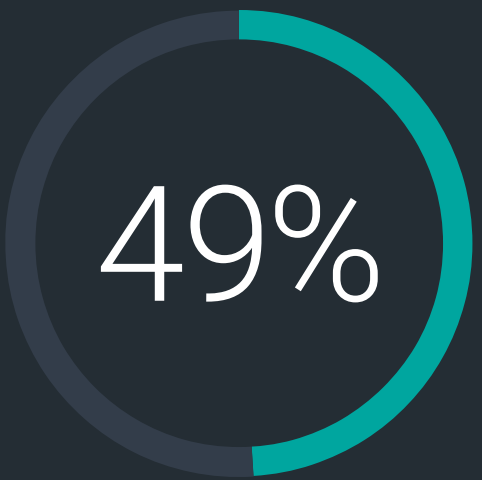
Have workforce accounts or credentials been compromised in the past 12 months?



**Yes**, we know we've had workforce accounts or credentials compromised



**Maybe**, we suspect we've had workforce accounts or credentials compromised



**No**, we know that we have not had workforce accounts or credentials compromised

# Top Contributors to Credential Compromise Include Passwords and Social Engineering

Storing and managing passwords, phishing, and social engineering attacks are the biggest contributors to credential compromise when it comes to employees. Operational issues of managing employee accounts and offboarding processes also cause problems. This justifies the rapid transition to strict and mandatory policies, including multifactor and passwordless authentication.

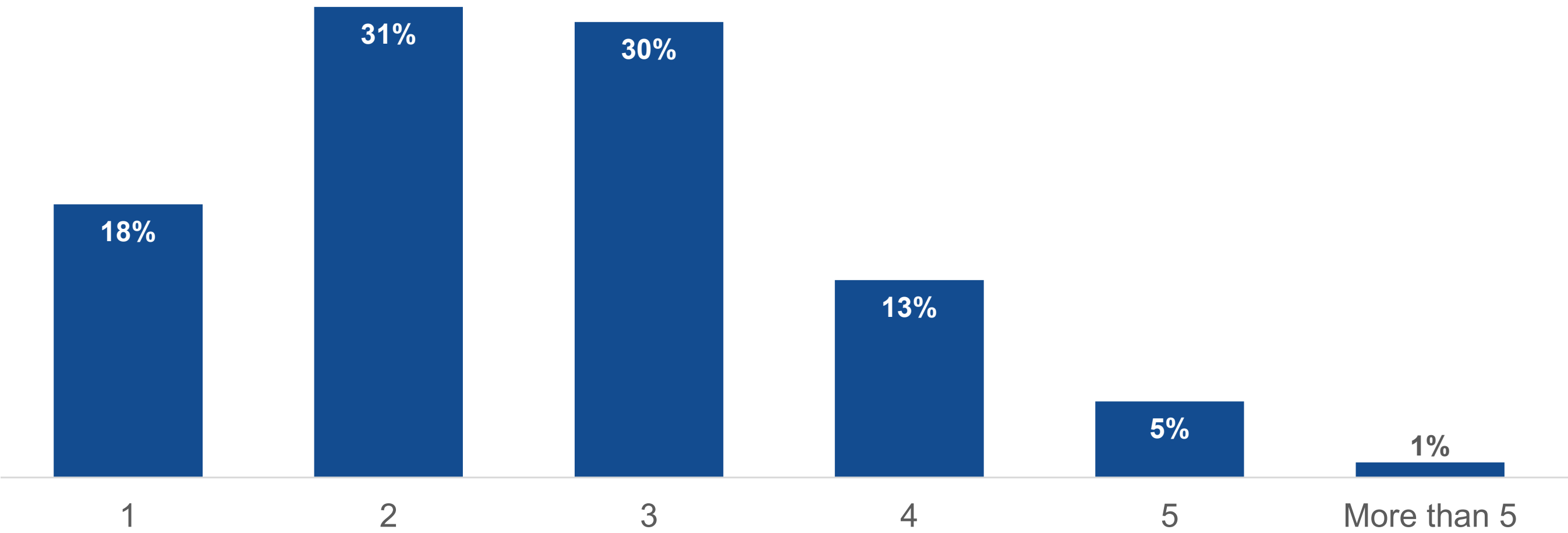
## Factors contributing to the compromise of workforce accounts or credentials.



## Multiple Machine/Workload Account/Credential Compromise Is Common

Compromise of machine accounts or credentials is also common. While more than one-quarter (26%) of organizations know this has happened in the last 12 months, of greater concern is the 23% of respondents that suspect but don't know for sure that they've experienced machine/workload account/credential compromise. This reflects a potential lack of security controls and tooling to understand the machine/workload identity estate. Most of these organizations report experiencing multiple machine accounts or credentials being compromised, including 19% experiencing four or more compromise events in the last 12 months.

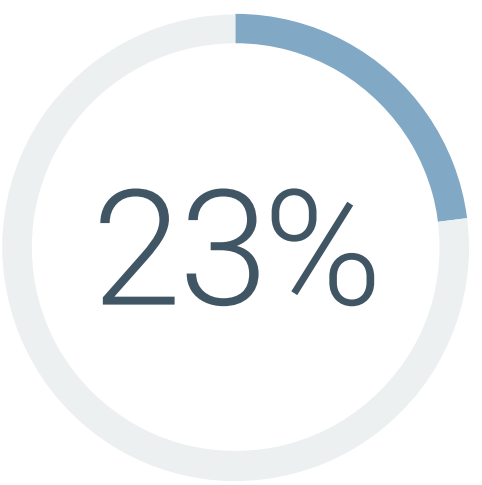
Number of times machine/workload accounts or credentials have been compromised in the past 12 months.



Have machine/workload accounts or credentials been compromised in the past 12 months?



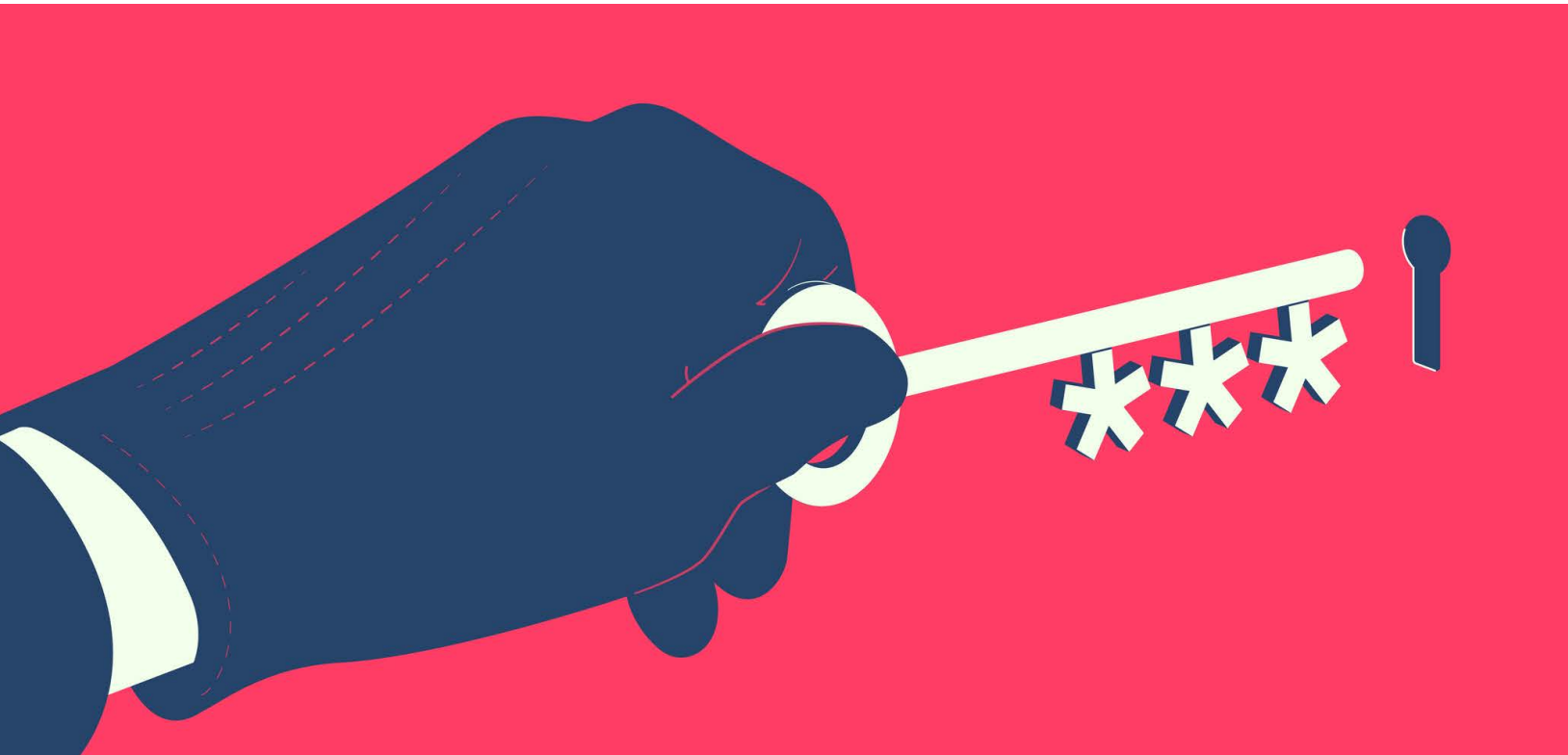
**Yes**, we know we've had accounts or credentials compromised



**Maybe**, we suspect we've had accounts or credentials compromised



**No**, we know that we have not had accounts or credentials compromised



# Poor Secrets Management Is the Most Common Contributor to Machine/Workload Account/Credential Compromise

Secrets hard-coded in applications or stored in spreadsheets, combined with social engineering attacks compromising shared keys, are the biggest factors contributing to increased risk.

Factors contributing to the compromise of machine/workload accounts or credentials.

48%



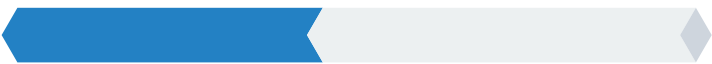
Exposed secrets embedded in an application

46%



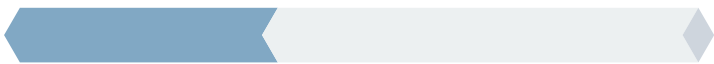
Exposed keys or secrets stored in files, spreadsheets, etc.

45%



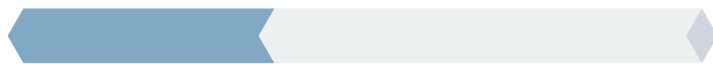
Social engineering attacks that exposed shared keys

38%



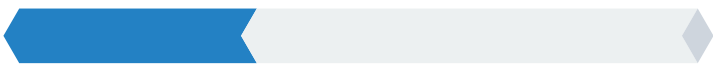
Expired certificates

37%



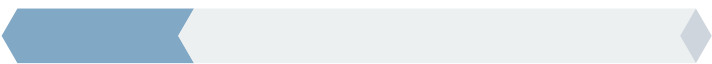
Unknown/unmanaged “shadow” identities

35%




Unknown revoked certificates

26%



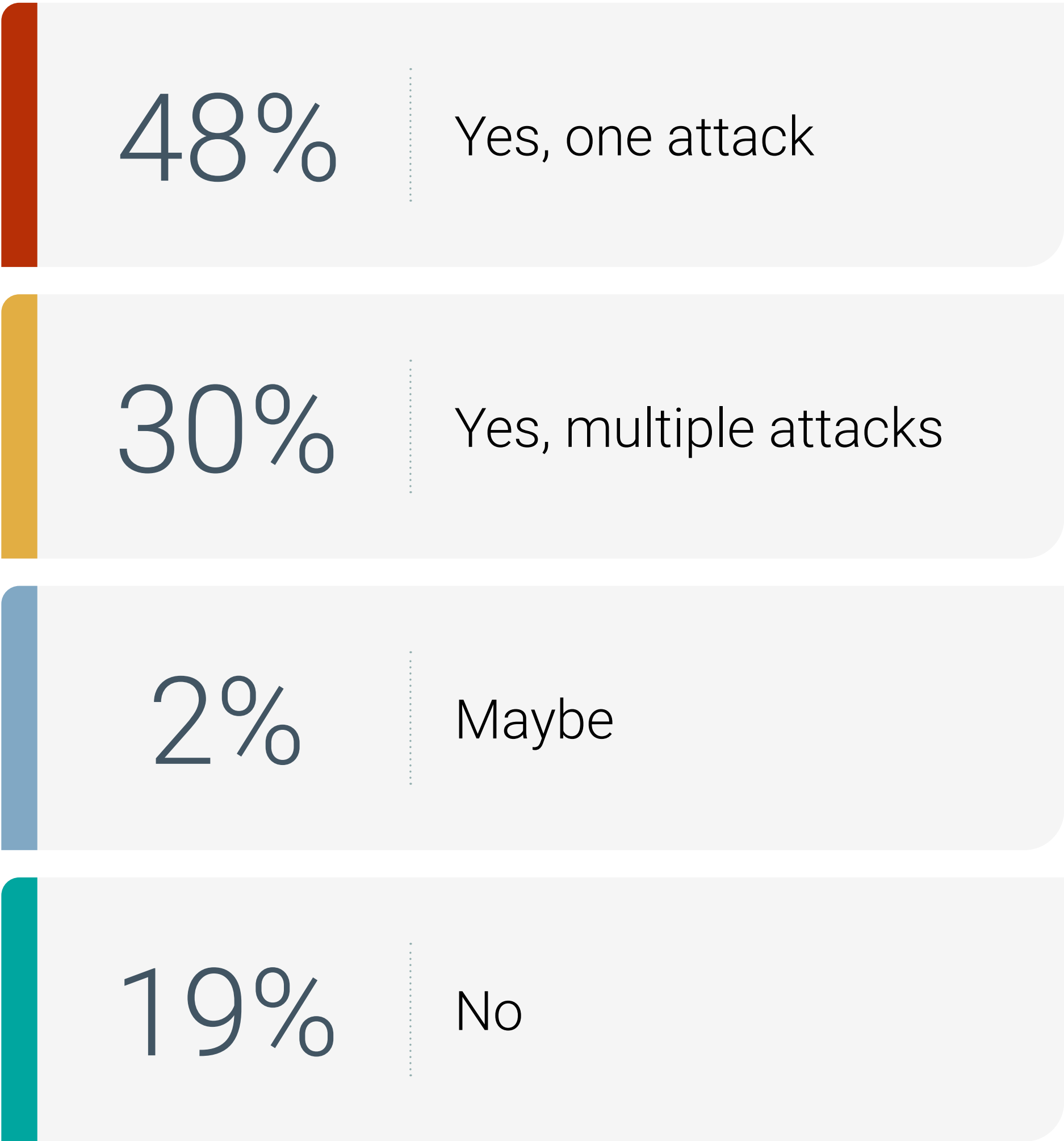
CA compromise



### Machine, Workload, and Workforce Identities Are Insufficiently Secured

Regardless of the ratio of machine to workforce identities, the fact is that these credentials make enticing targets for bad actors intent on finding an ingress to corporate networks and systems. As such, it is concerning that only 8% of organizations believe that all of their workforce and/or machine identities are sufficiently secured. Conversely, nearly one in five organizations estimate that more than 30% of all machine/workload and workforce identities aren't sufficiently secured.

Have compromised accounts or credentials in the past 12 months led to successful cyberattacks?



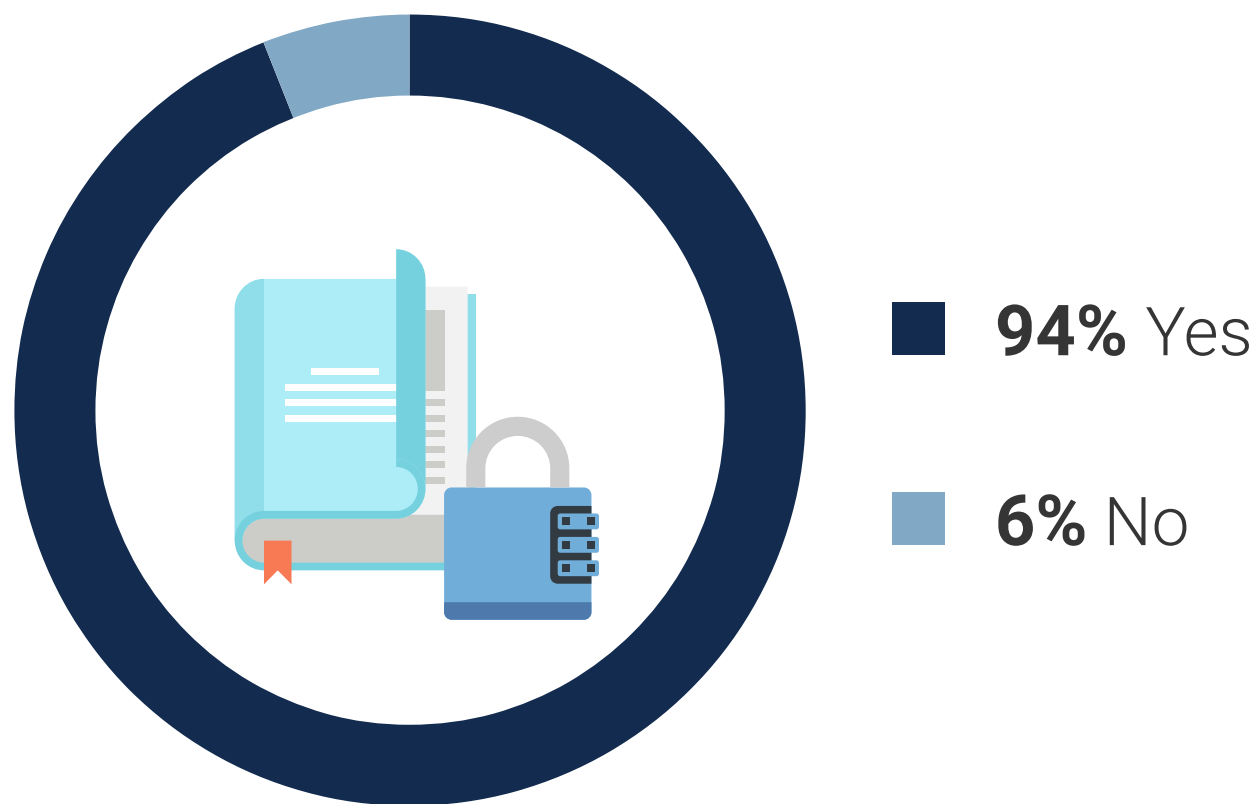
A person is shown from the chest up, wearing a blue button-down shirt. They are holding a smartphone in their right hand, which has a black watch on the wrist. They are looking at a laptop screen. The background is a bright, out-of-focus window with greenery outside, creating a bokeh effect. The text is overlaid on the bottom left of the image.

**MFA and Passwordless  
Authentication Implementations  
Are Becoming Extensive**

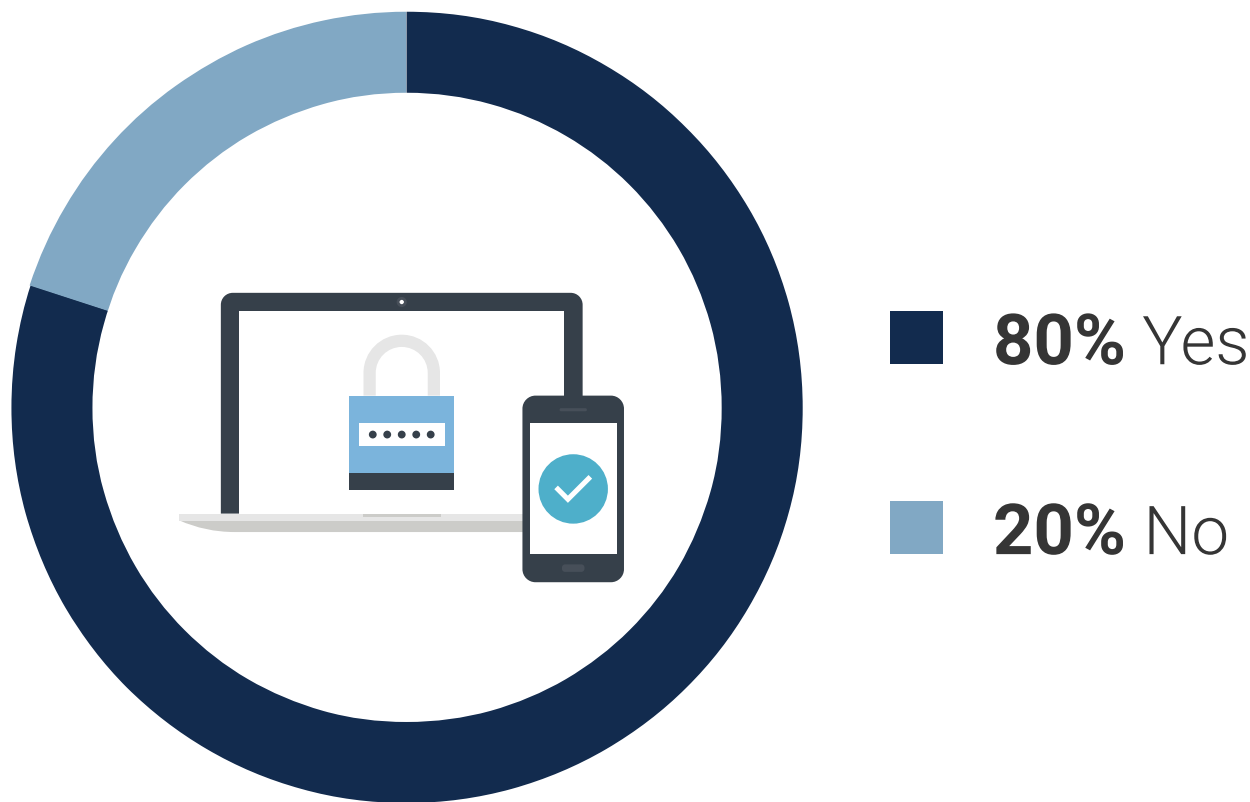
## Taking Action to Remedy Issues With Passwords

That the simplest form of privileged access management, multifactor authentication (MFA), is strictly enforced is a good start toward securing critical accounts and associated credentials from attack. Among those organizations currently leveraging multifactor authentication, a majority (94%) are enforcing strict MFA policies for privileged users. Additionally, 80% of these organizations report making multifactor authentication mandatory for their entire workforce, which is a significant increase from previously conducted Enterprise Strategy Group research.<sup>1</sup> With mechanisms like password cracking, social engineering, and MFA push-bombing increasingly being used to weaponize passwords against organizations' security posture, it follows that two-thirds have made passwordless authentication mandatory for their entire workforce.

Does your organization enforce strict multifactor authentication (MFA) policies for privileged users?



Does your organization make multifactor authentication (MFA) mandatory for its entire workforce?



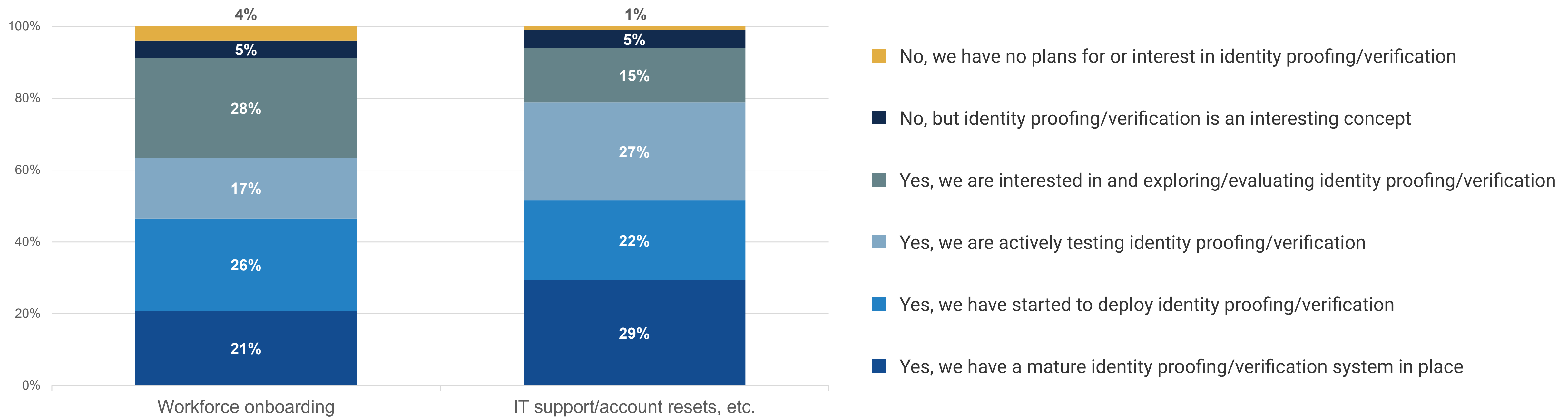
Does your organization make passwordless authentication mandatory for its entire workforce?




# Organizations Turning to Out-of-band Identity Verification for Critical Operations

Most likely due to well-publicized attacks, the use of identity proofing and verification is gaining traction. This method focuses on the supporting evidence of validity to affirm that the identity is a real person. Specifically, more than half of organizations report having a mature identity proofing system in place (29%) or actively deploying one (22%) to support IT. In terms of employee onboarding, usage levels are similar, with nearly half (47%) confirming the usage of identity verification technology.

Are organizations using identity proofing and/or verification solutions for IT support and workforce onboarding?



The background is a composite image. On the left, a city skyline is partially obscured by thick, white clouds. On the right, a person's profile is shown in silhouette, looking towards the left. The person's face is superimposed over the city skyline, with the buildings appearing to be part of their facial structure. The overall color palette is muted, with blues, greys, and whites.

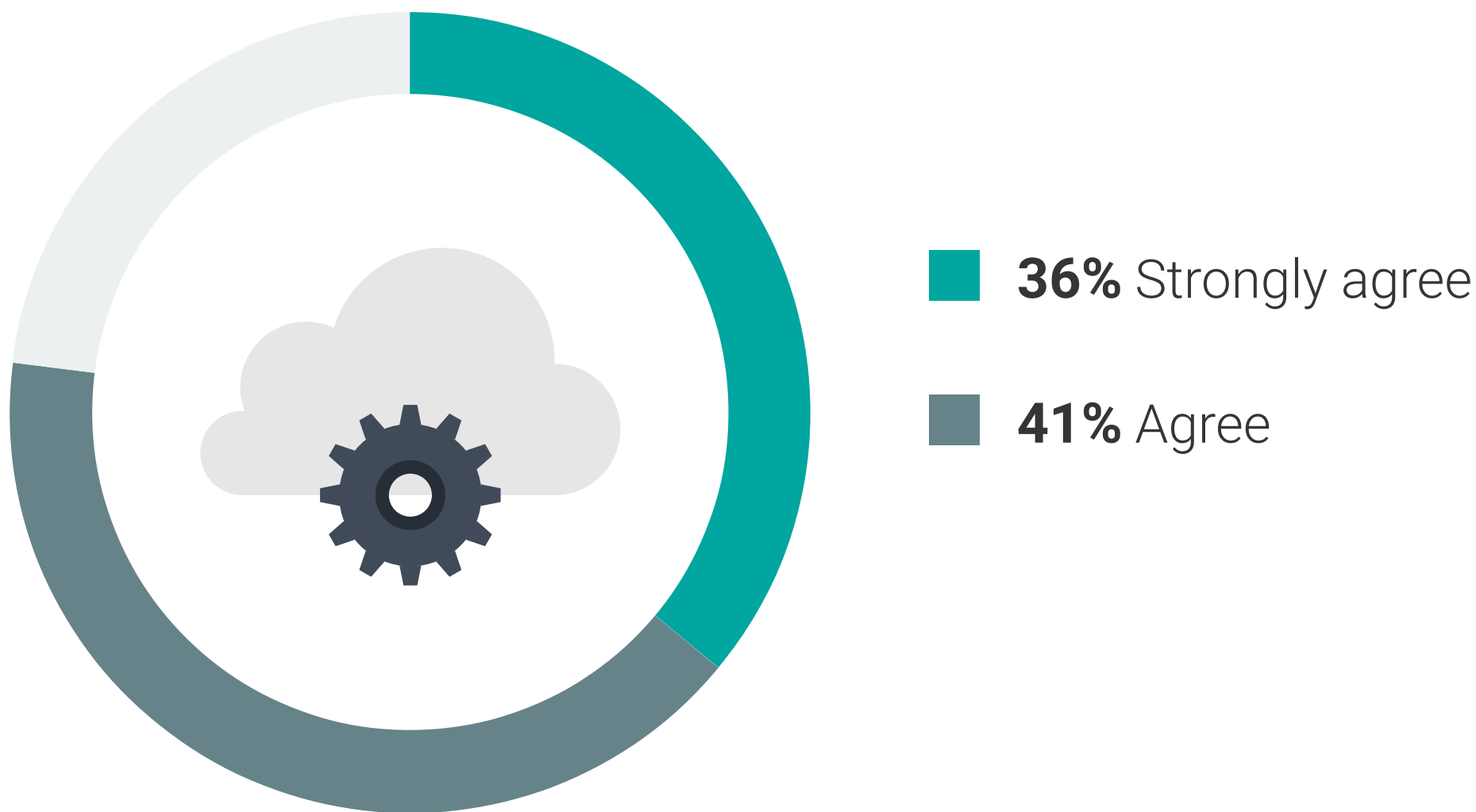
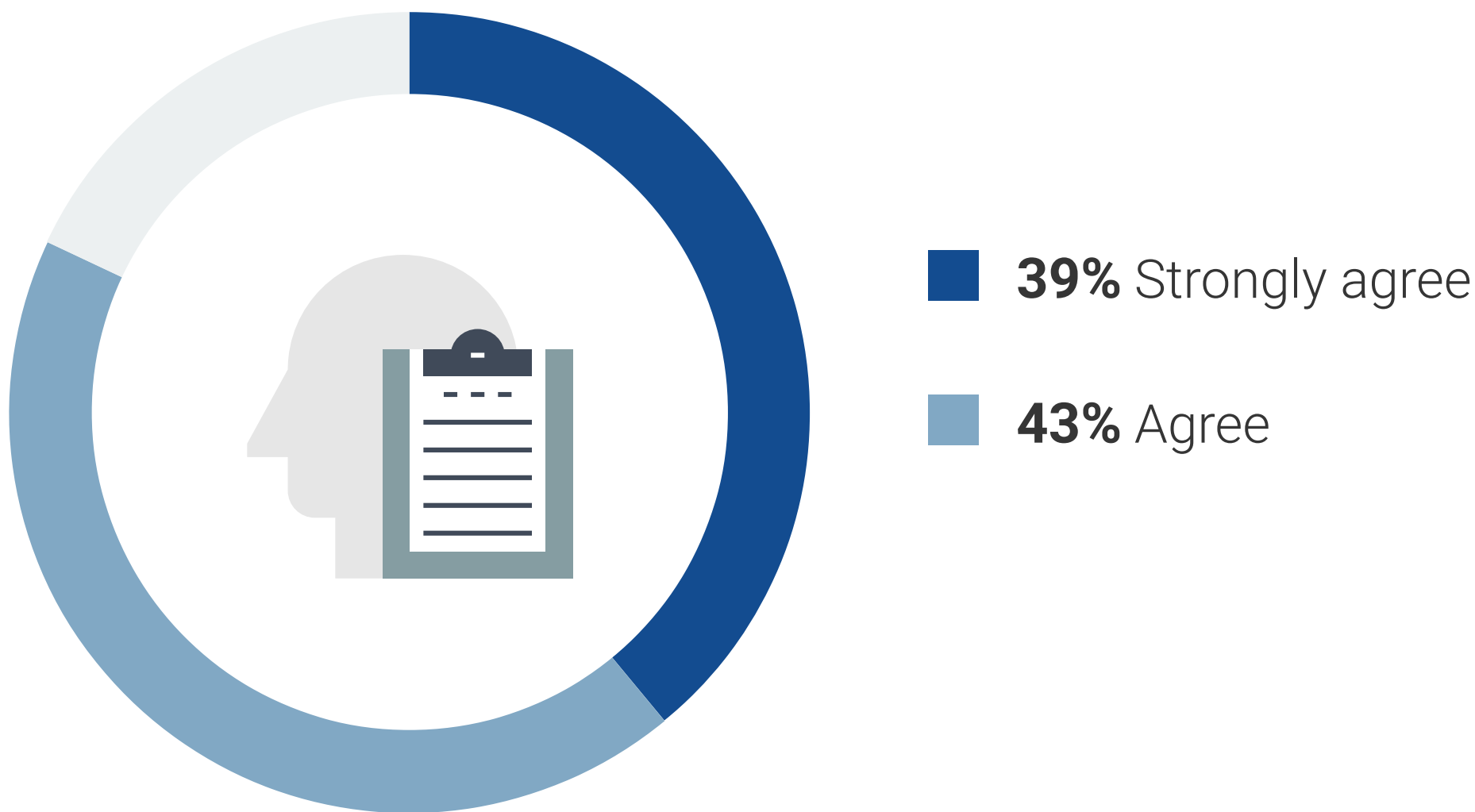
# **Cloud Provides Identity Challenges While ITDR and ISPM Gain Momentum**

## The Cloud Makes Identity Security More Challenging

As has been the case in many other areas of cybersecurity, the increased usage of public cloud services has made identity security more challenging. Indeed, the usage of public cloud services has forced many organizations to establish new policies and purchase new technologies specifically for cloud-related identities, separate from policies and technologies in place for on-premises infrastructure.

The differences between on-premises and cloud-resident infrastructure require a different set of identity security policies and technologies.

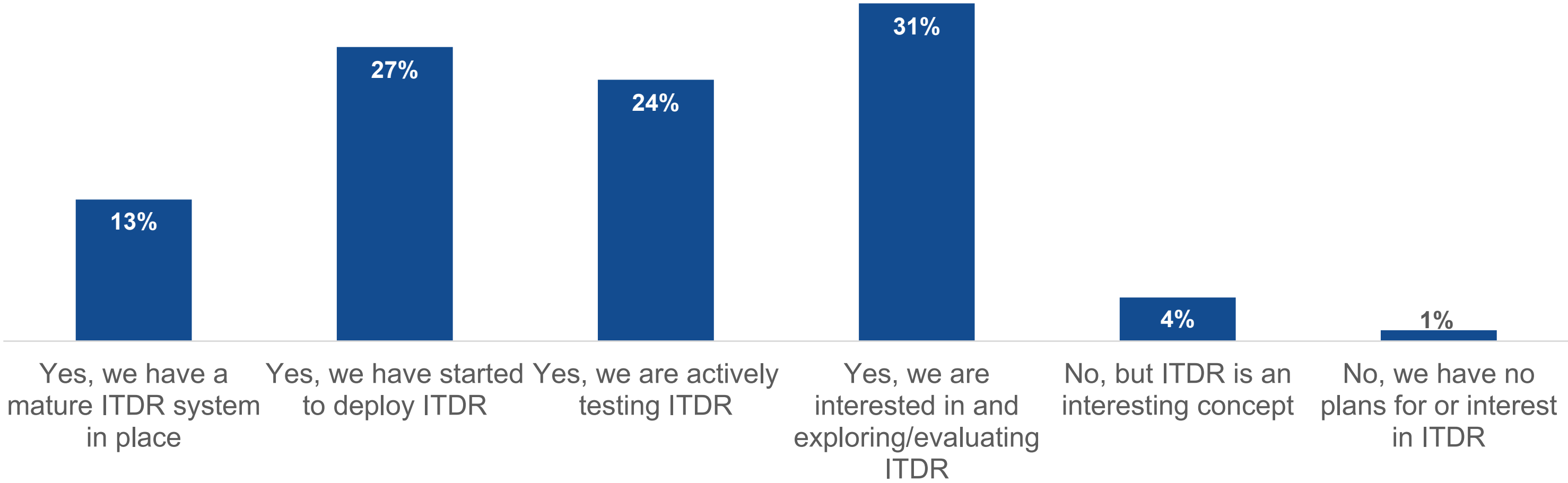
The increase in our use of public cloud (SaaS, IaaS, and/or PaaS) has made securing our identities more challenging.



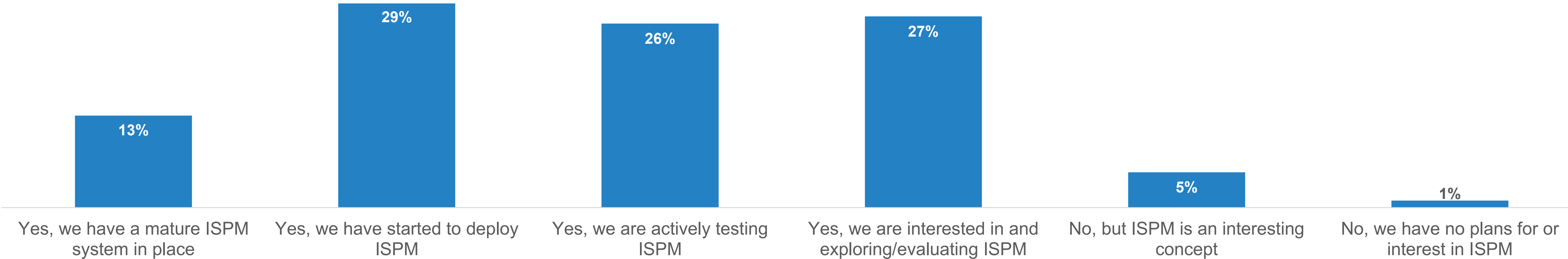
## Two-thirds Have Started the Journey Toward Deploying ITDR and ISPM

Identity threat detection and response (ITDR) is a practice that focuses on threat intelligence, tools, and processes to identify, reduce, and respond to identity-based threats and protect identity systems. Identity security posture management (ISPM) is a practice that combines identity attack surface management and risk reduction (such as detecting partial or incomplete offboarded accounts or an excessive number of privileged accounts and prioritizing remediation actions) with identity threat prevention, detection, and response. While both are still in their relative infancy, 13% of organizations report having mature systems in place and more than one-quarter have started deploying ITDR (27%) and ISPM (29%).

Are organizations using identity threat detection and response (ITDR)?



Are organizations using identity security posture management (ISPM)?



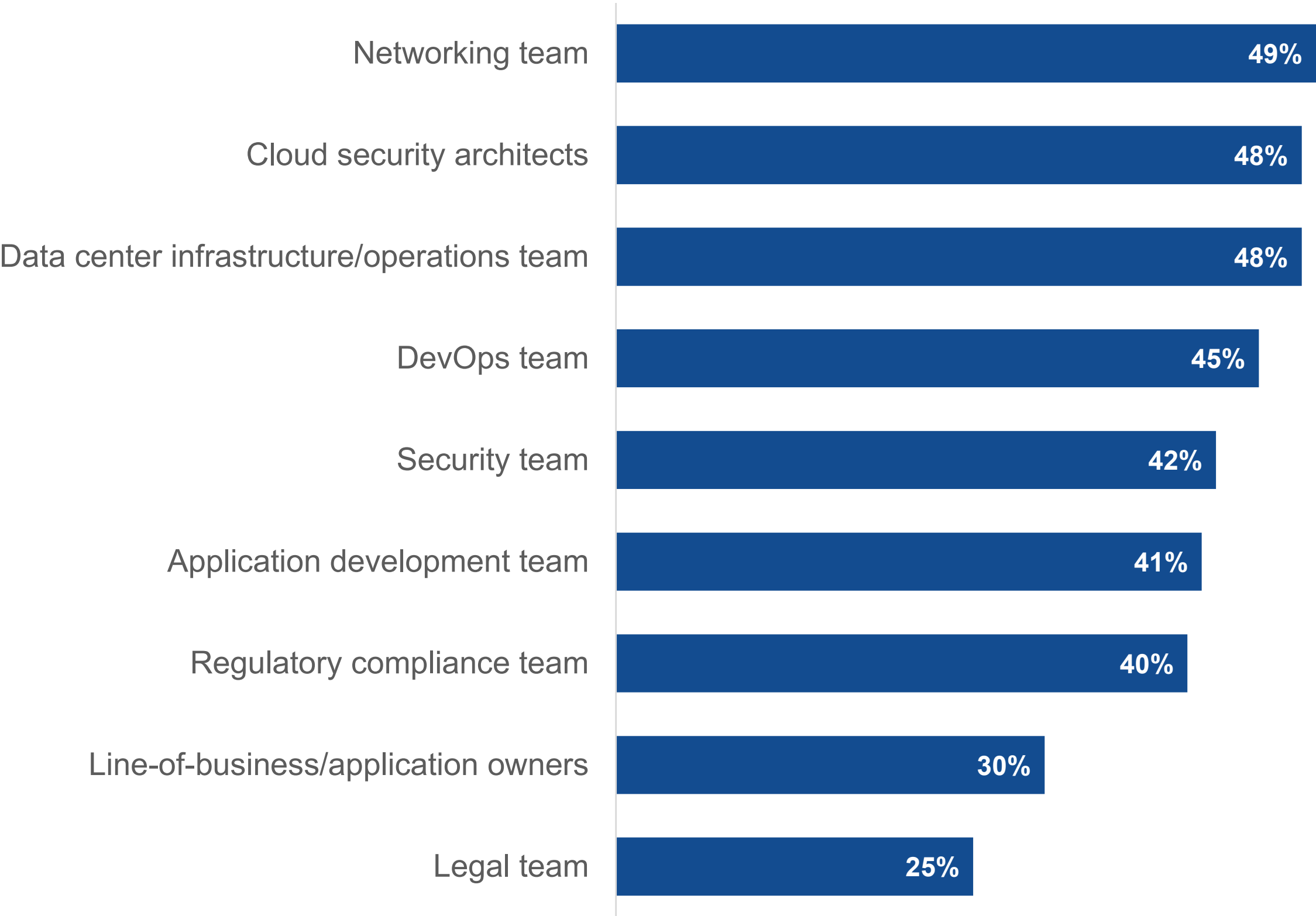


**Identity Security Is  
a Team Sport**

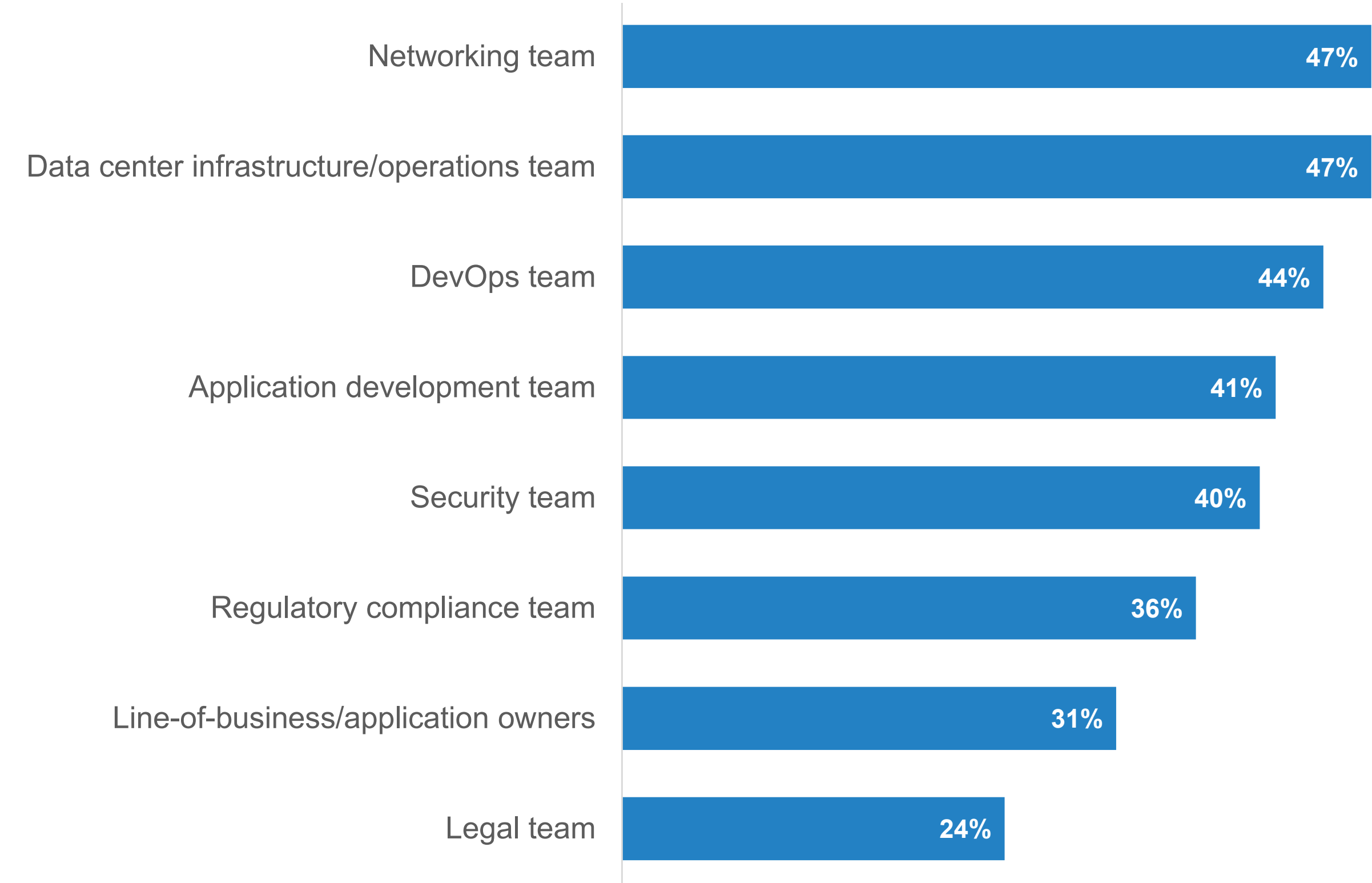
# Identity Security Takes a Village

Identity security involves multiple teams for both setting policies and making purchase decisions. These groups include the networking team, security, IT and operations, DevOps, developers, compliance, and even legal teams. This underscores the importance of solutions that drive efficiency for collaboration across teams.

Groups involved in creating identity security policies.



Groups involved with purchasing decisions for identity security products and services.



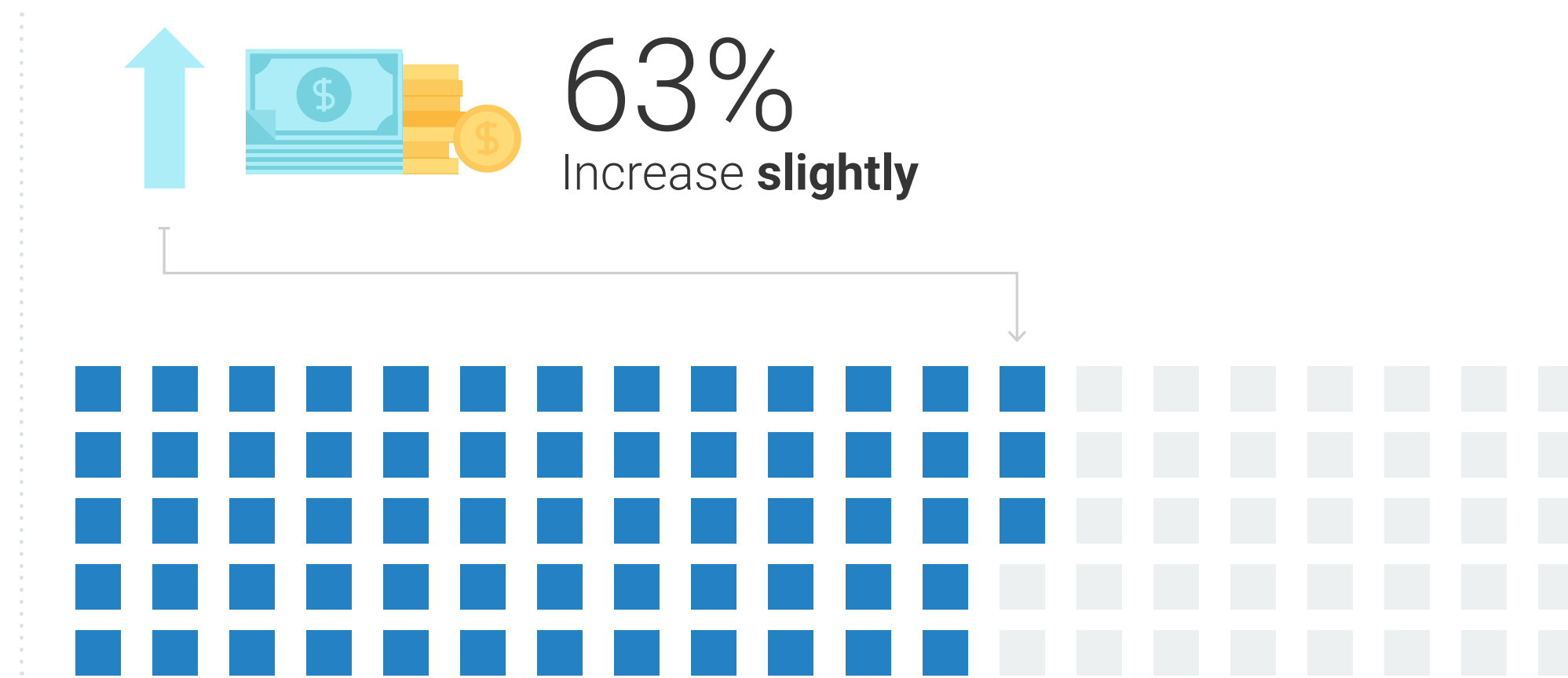
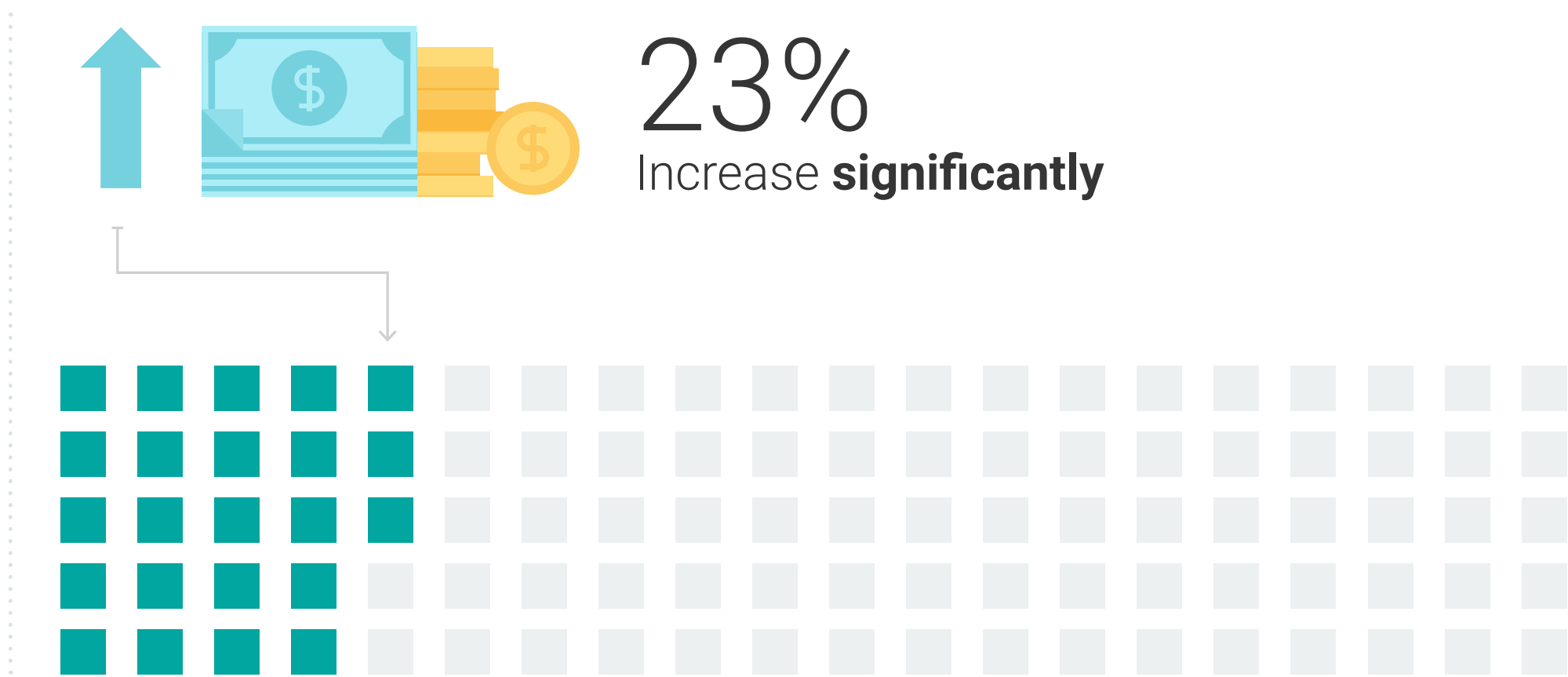


# Investment in Identity Security Is Growing

# Identity Security to Garner a Larger Share of the Cybersecurity Budget, With ITDR, CIEM, and ISPM Topping Investment Priorities

Relative to other areas of IT and cybersecurity, the vast majority of organizations expect to increase their spending on identity security technology solutions either slightly (63%) or significantly (23%). Increasing identity security budgets reflects a growing understanding of the importance of protecting permissions and access against attacks and lateral movement to secure assets and data.

Expected spending change for identity security over the next 12 months.



# ITDR, CIEM, and ISPM Top the List of Identity Security Investment Areas

Now that most organizations have addressed baseline authentication challenges with mandatory MFA and passwordless authentication, they're setting their sights on ITDR, CIEM, and ISPM. The bulk of threats leverage compromised identities, and these areas represent the greatest value in countering threats.

Identity security spending priorities over the next 12 months.



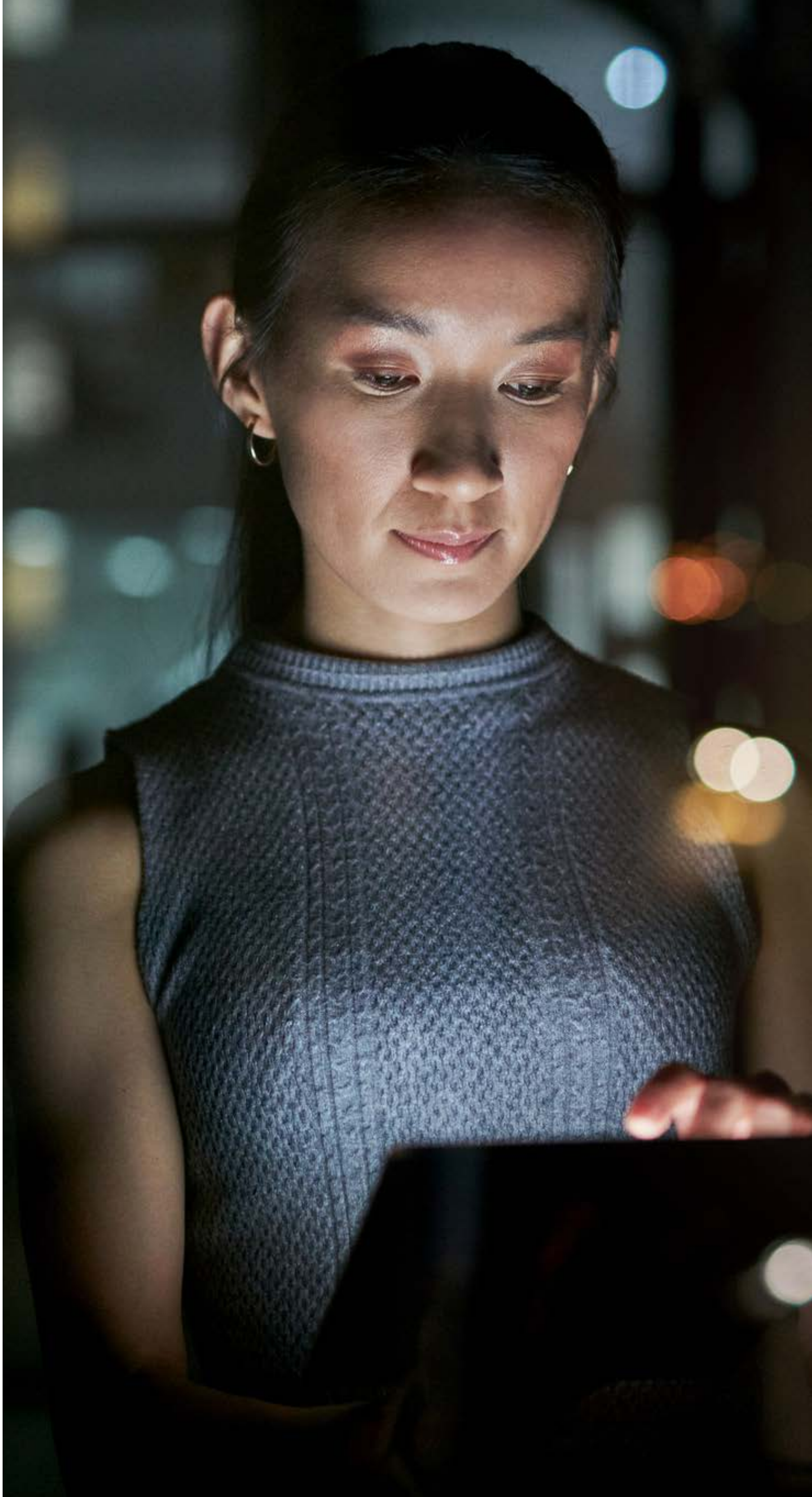


ABOUT

Portnox is a leader in delivering cloud-native zero trust access control and cybersecurity solutions, empowering IT teams to tackle modern security challenges with confidence. The Portnox Cloud offers a unified platform for zero trust security, integrating passwordless authentication, risk monitoring, compliance enforcement, and endpoint remediation. Trusted by organizations worldwide, it provides complete visibility and control over every device the moment it requests access.

Portnox is committed to simplifying zero trust security while maintaining enterprise-grade protection. With always-on security essentials, we help businesses stay ahead of sophisticated cyber threats. Our “set it and forget it” approach ensures simplicity and power, giving IT professionals the tools to secure their environments without losing time or peace of mind. Backed by industry recognition, we’re on a mission to make zero trust security effective, approachable, and hassle-free.

LEARN MORE

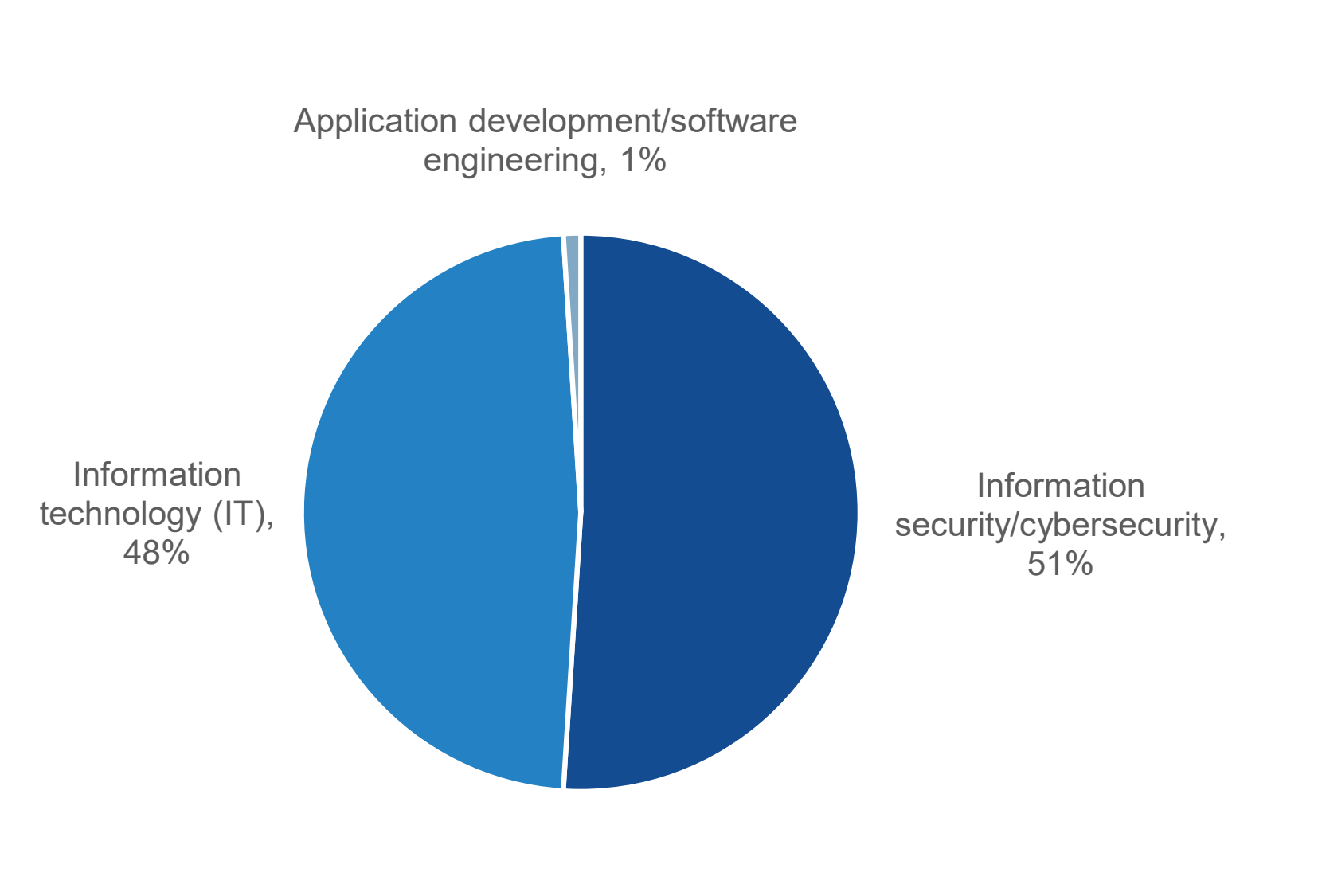


RESEARCH METHODOLOGY AND DEMOGRAPHICS

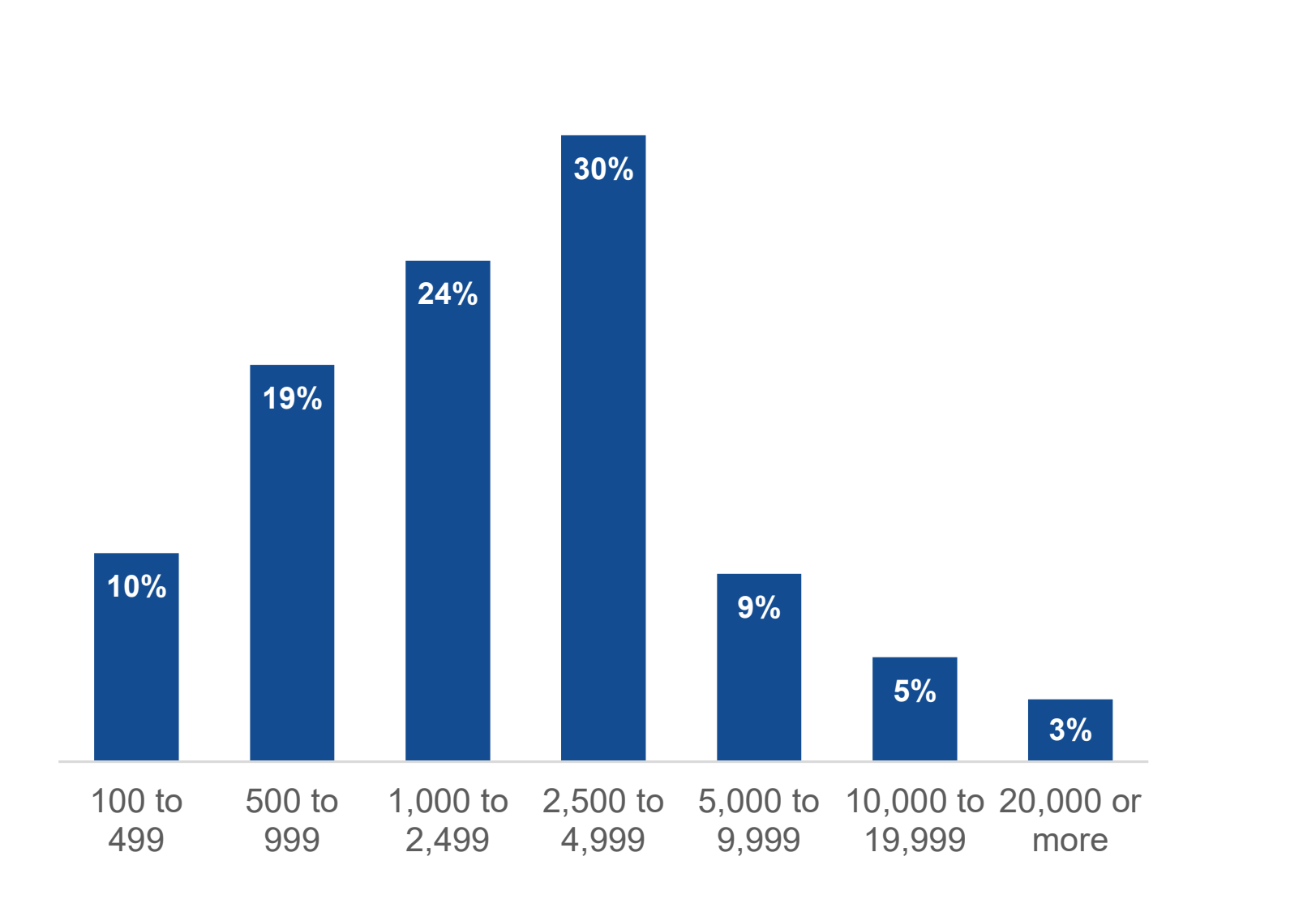
To gather data for this report, TechTarget’s Enterprise Strategy Group conducted a comprehensive online survey of IT, cybersecurity, and application development professionals from private- and public-sector organizations in North America between January 12, 2024 and January 21, 2024. To qualify for this survey, respondents were required to be responsible for or involved with identity security technologies and processes. 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 372 IT, cybersecurity, and application development professionals.

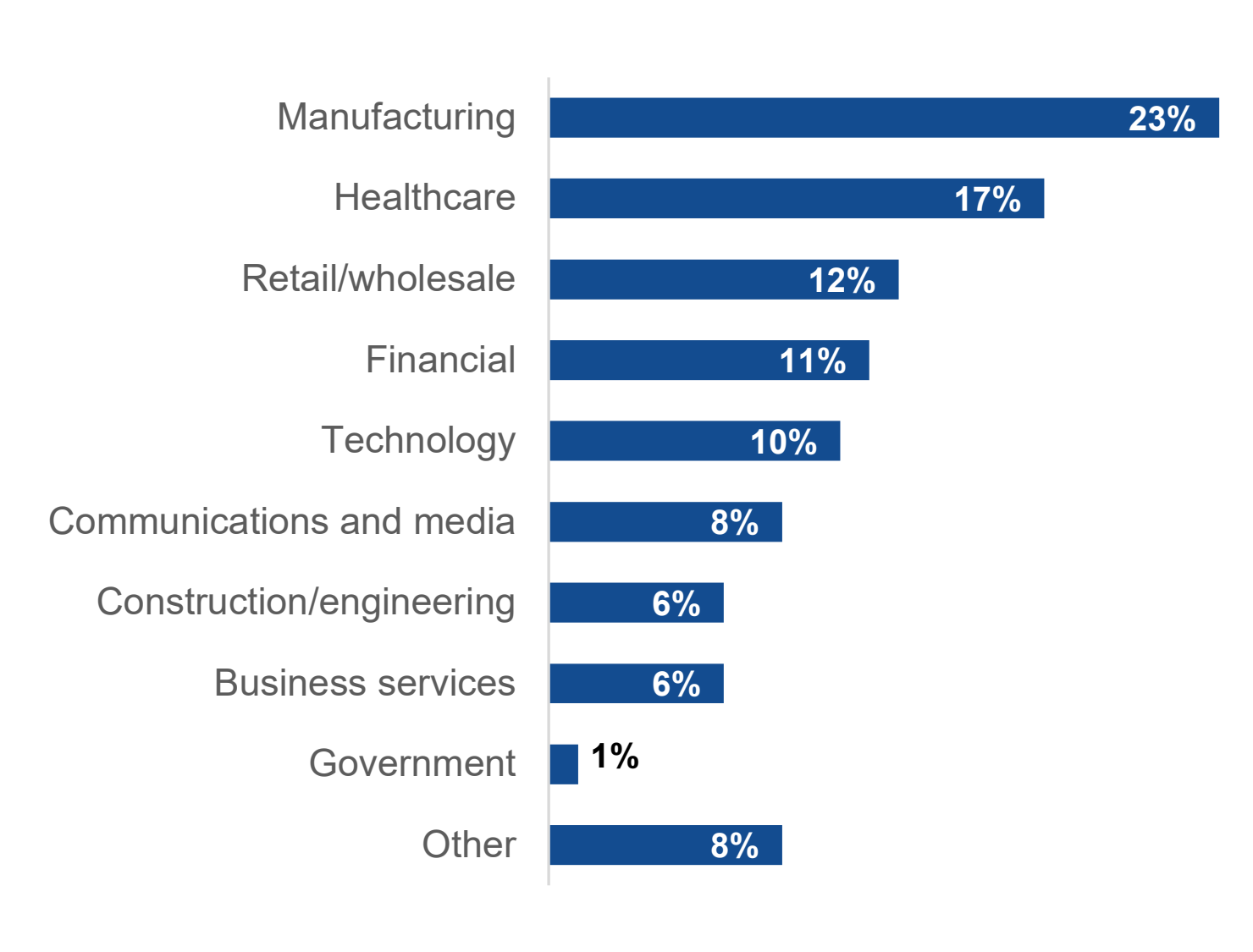
Respondents by job function.



Respondents by number of employees.



Respondents by industry.



All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

This publication is copyrighted by TechTarget, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at [cr@esg-global.com](mailto:cr@esg-global.com).



**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.

© 2024 TechTarget, Inc. All Rights Reserved.