

Managing Non-human Identities for an Effective Cybersecurity Program

Todd Thiemann | Senior Analyst

ENTERPRISE STRATEGY GROUP

SEPTEMBER 2024



Research Objectives

Enterprise IT cybersecurity and operations teams are recognizing the risk associated with the large and growing volume of non-human identities (NHIs). Modern application architectures with complex relationships and ephemeral resources have resulted in a proliferation of non-human access to communicate and exchange data. NHI management is an emerging space with unique characteristics and lifecycle requirements when compared with the more established human identity and access management (IAM) domain. Inadequate security for non-human identities poses significant security risks given the significant access and privileges provided to non-human identity infrastructure. Specifically, poor security for NHIs can lead to data breaches, operational disruptions, and compliance violations. As cloud adoption and automation continue to grow, effective non-human identity management has become essential for maintaining security, facilitating business operations, and supporting digital transformation initiatives.

To gain further insight into these trends and issues, TechTarget’s Enterprise Strategy Group surveyed 367 IT, cybersecurity, and DevOps, platform, and cybersecurity engineering professionals at organizations in North America (US and Canada) involved with or responsible for the technologies and processes that secure non-human identities and machine workloads.

THIS STUDY SOUGHT TO:

Assess the state of the market for locating, securing, and managing non-human identities.

Understand the challenges in gaining visibility and lifecycle control over non-human identities.

Explore the consequences of inadequate visibility and security for non-human identities.

Determine how enterprises intend to invest to address risks associated with non-human identity management and security.





Key Findings



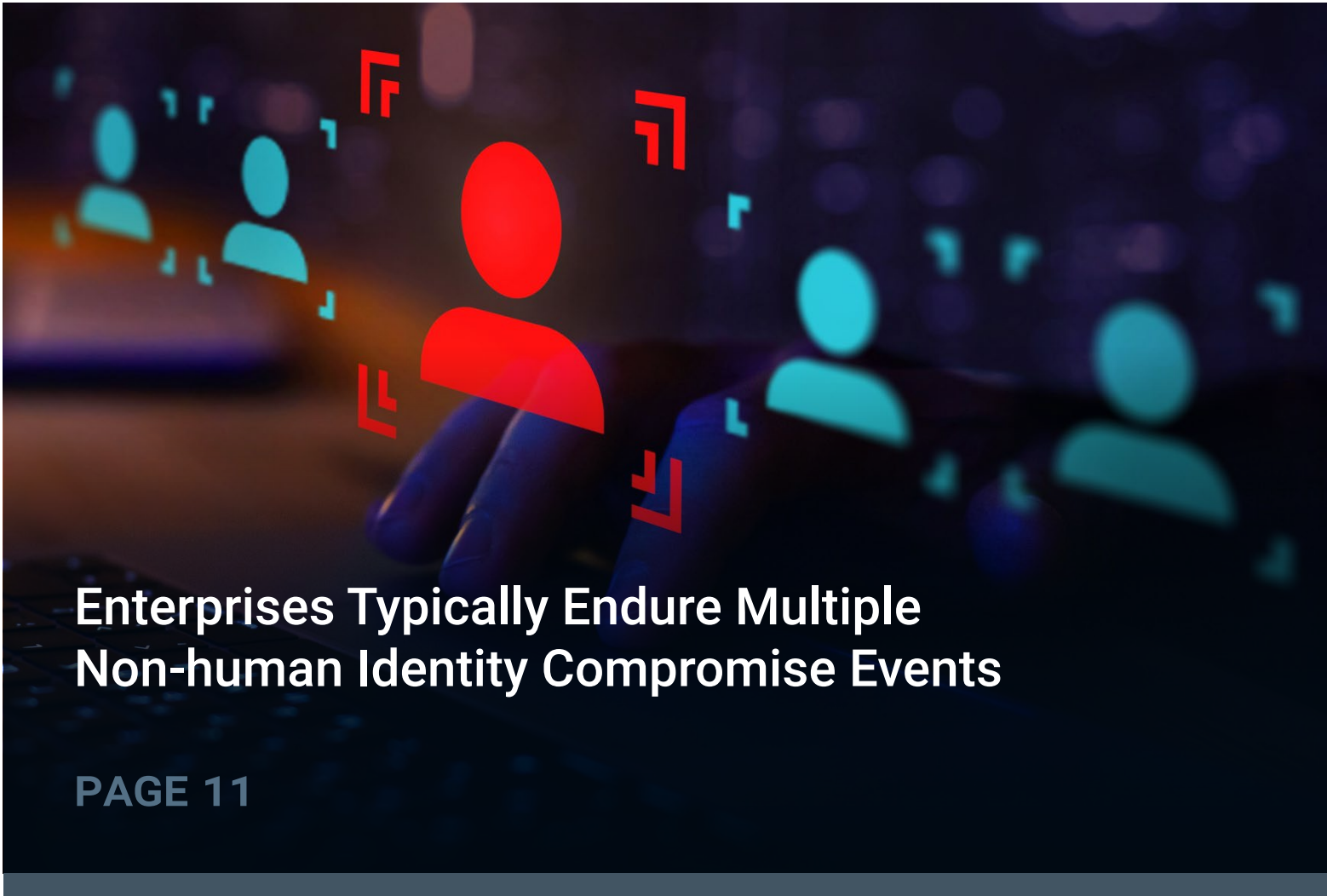
Non-human Identity Volume Is Large and Increasing Quickly

PAGE 4



Enterprises Typically Deploy Multiple Solutions for Each NHI Problem Area

PAGE 8



Enterprises Typically Endure Multiple Non-human Identity Compromise Events

PAGE 11



Non-human Identity Management Has Diverse Constituents, and Compromises Get Board-level Attention

PAGE 15



Enterprises Are Investing Disproportionately to Solve for Non-human Identity Security

PAGE 19



**Non-human Identity Volume Is Large
and Increasing Quickly**

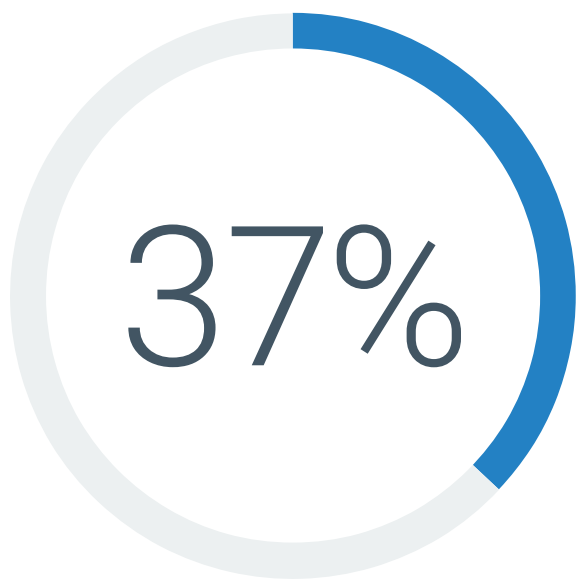
Flux in How to Refer to the Space, but Plurality Prefer ‘Non-human Identity’

The industry has yet to settle on the optimal way to refer to managing digital credentials or sets of permissions that represent an automated actor for machines, service accounts, digital certificates, applications, and other automated systems. However, the plurality of respondent organizations (38%) prefer the term “non-human identity management.”

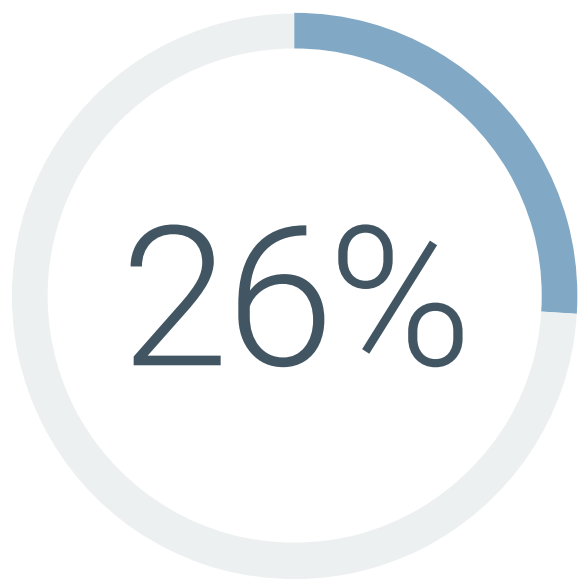
Term organizations prefer for referring to the management of identities that are not tied to human users.



Non-human
identity management



Workload
identity management



Machine
identity management

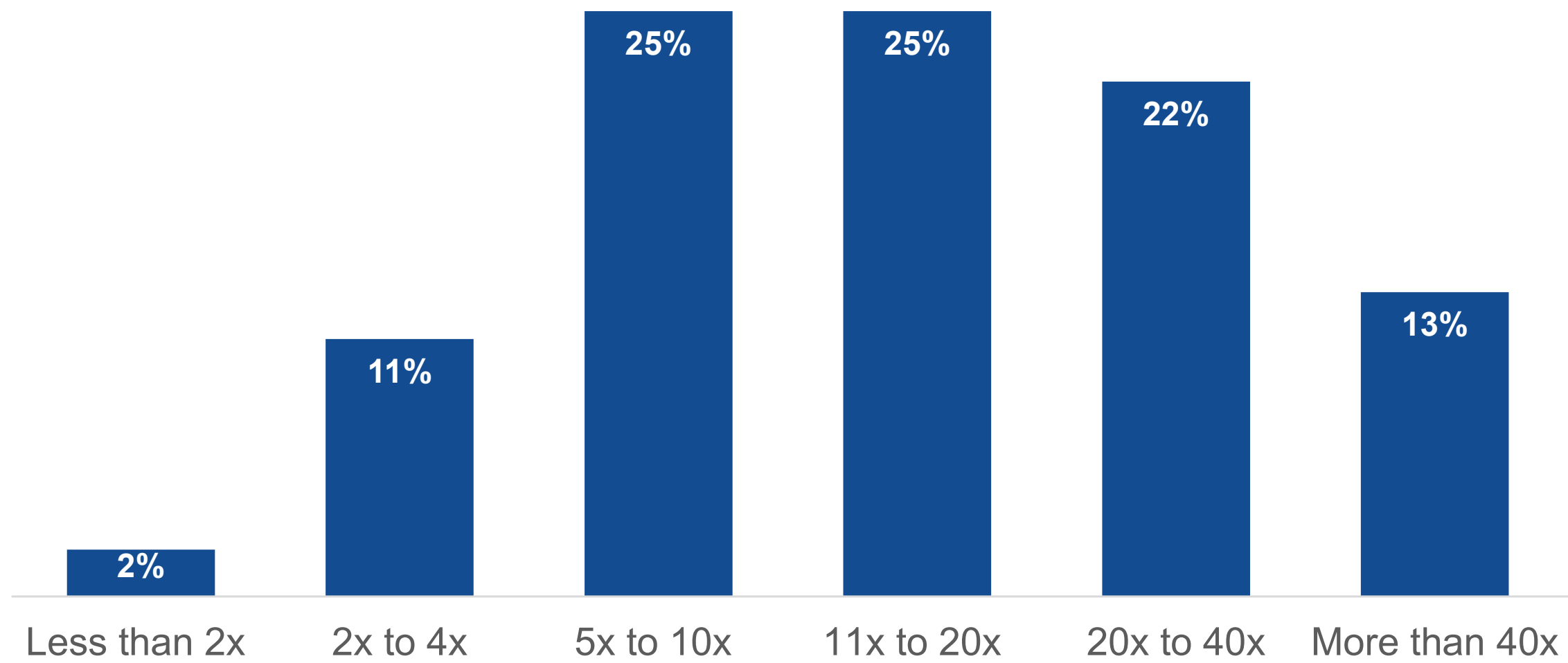
“The industry has yet to settle on the optimal way to refer to managing digital credentials or sets of permissions that represent an **automated actor for machines, service accounts, digital certificates, applications, and other automated systems.**”

Non-human Identities Significantly Outnumber Human Identities, and This Volume Is Expected to Increase

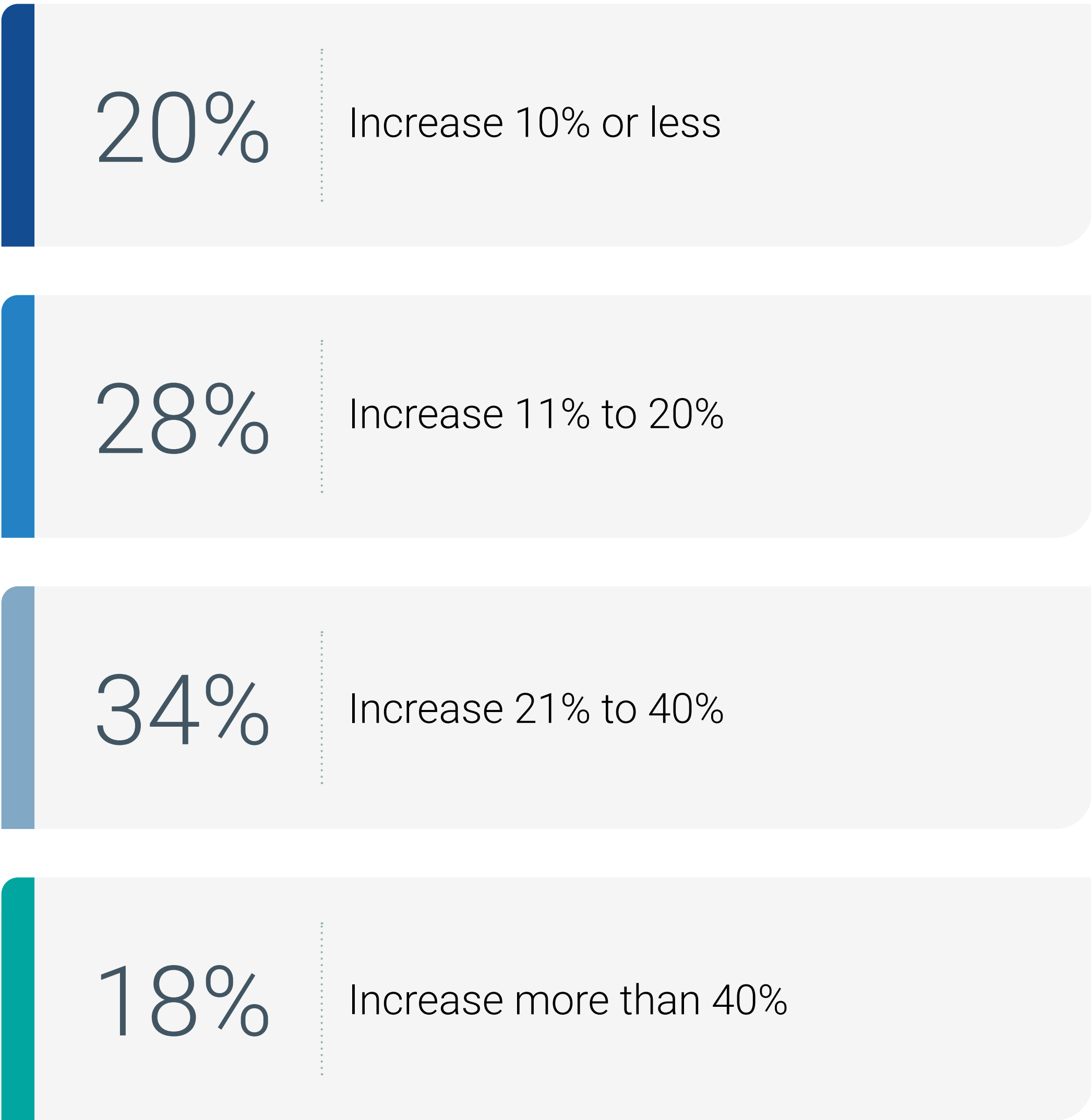
When asked to gauge the number of non-human identities they must manage relative to the number of human identities, the average organization estimated that number to be approximately 20x larger. It’s worth noting that many of these analyses *probably* understate the problem as respondents typically do not have complete visibility into the variety of NHIs across their organization.

More than half (52%) of organizations expect the total number of non-human identities under management to increase by more than 20% over the next 12 months. The proliferation of non-human identities requires solutions that can accommodate expected growth.

Approximate number of non-human identities organizations manage relative to human identities.



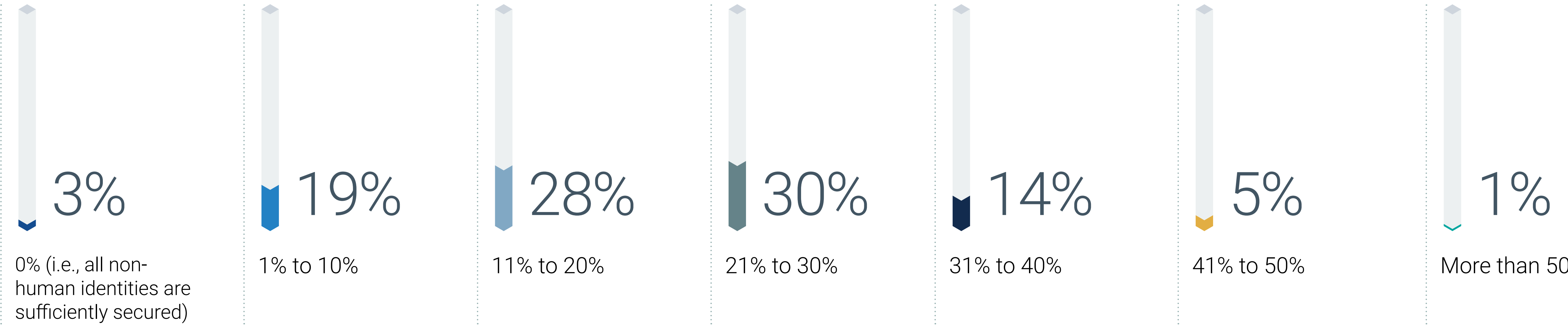
Expected change in the total number of NHIs organizations have under management over the next 12 months.



Non-human Identities Are Perceived to Be *Insufficiently* Secured

The average organization believes that more than one in five of their non-human identities are insufficiently secured. Not only is the number of non-human identities growing, but organizations also recognize them as a vulnerable part of the attack surface.

Percentage of non-human identities organizations estimate are insufficiently secured.



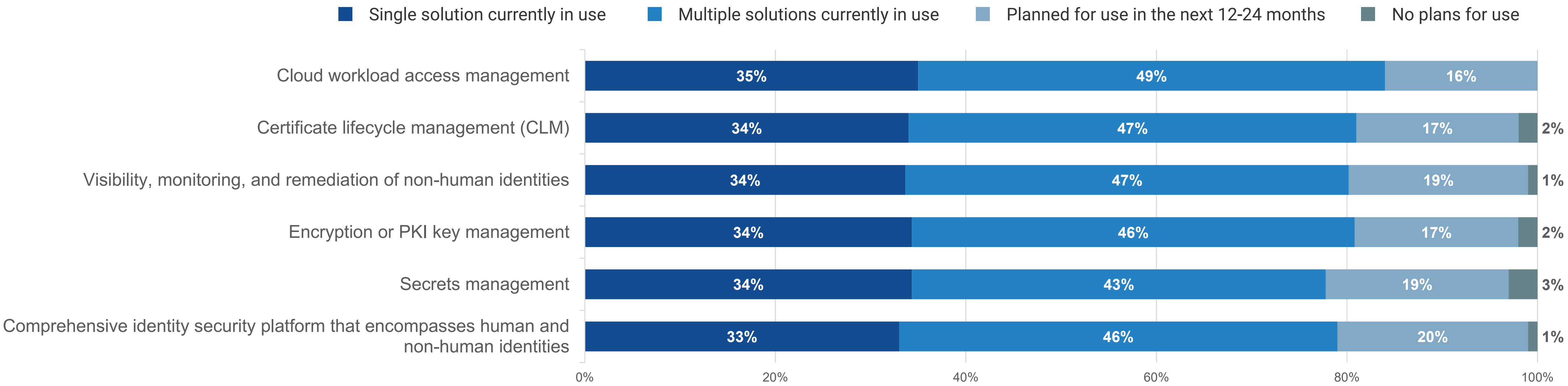


**Enterprises Typically Deploy Multiple
Solutions for Each NHI Problem Area**

Most Enterprises Invest in Multiple Solutions for the Various Aspects of Non-human Identity Management

Practically all organizations leverage at least one non-human identity management solution, and many have multiple solutions in place. While this does suggest a defense-in-depth approach, it also reveals a lack of motion toward platform unification at this point.

Usage of and plans for NHI technologies.

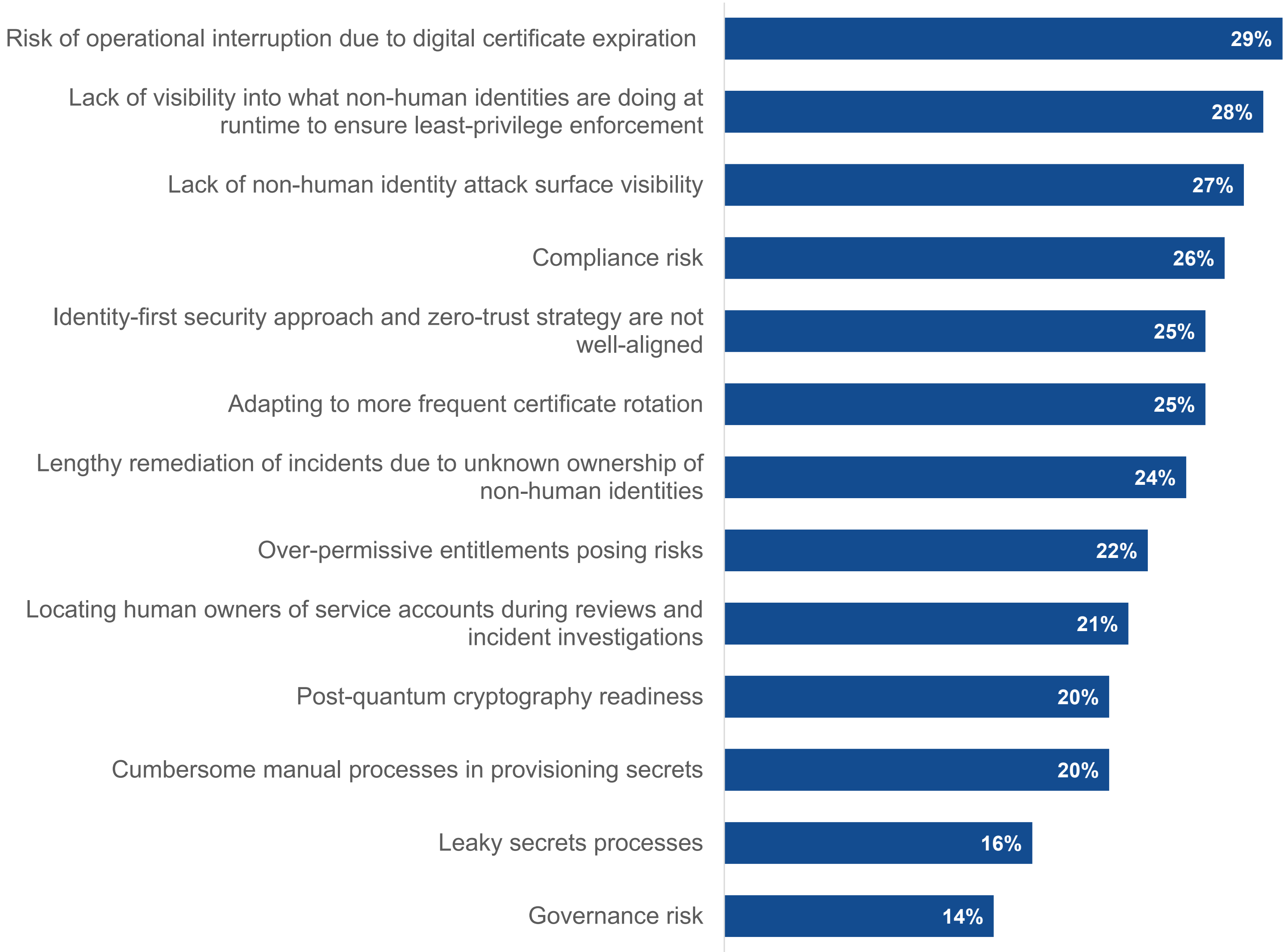




Avoiding Operational Interruptions and Visibility Are Leading Concerns

What concerns do organizations have with non-human identity management? Operational risk and a lack of visibility are most commonly cited, but compliance and other security concerns, such as identity and zero-trust alignment and certificate rotation, are not far behind.

Current concerns with non-human identity management.





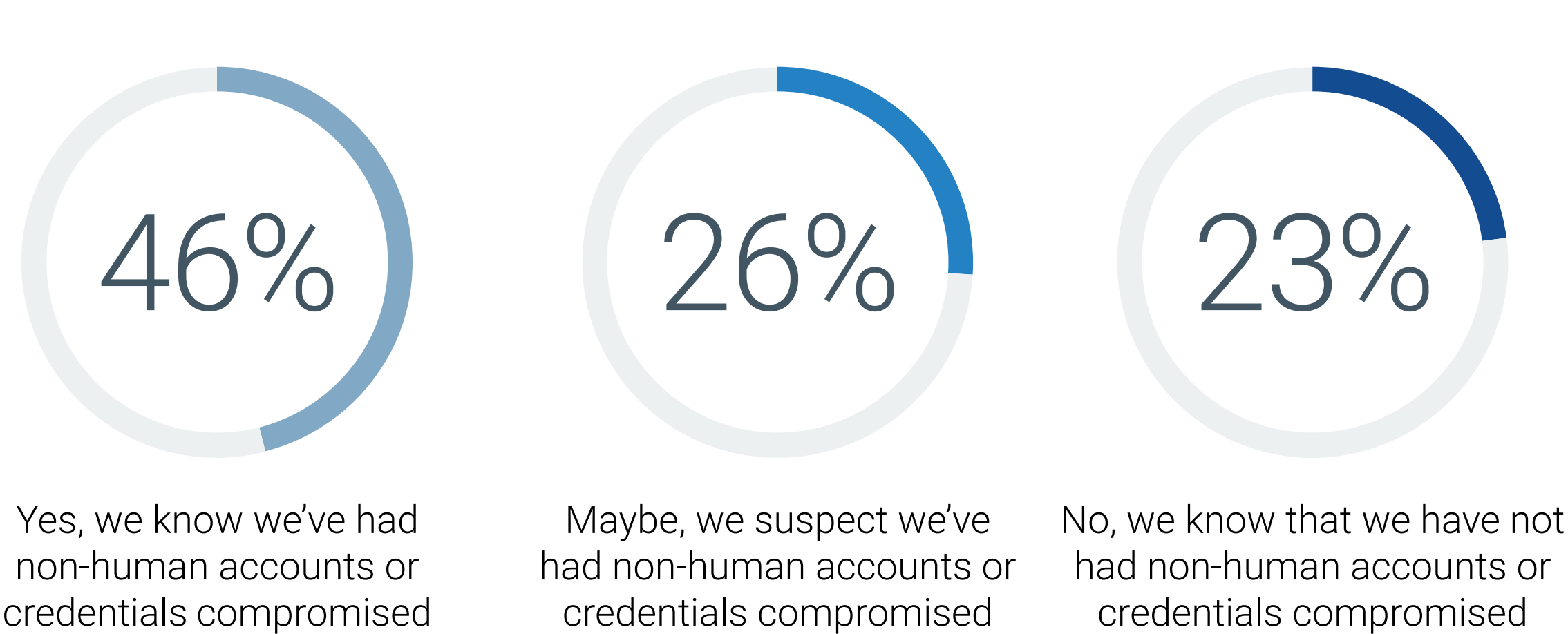
**Enterprises Typically Endure Multiple
Non-human Identity Compromise Events**

Nearly Three in Four Enterprises Suspect They Have Exposed NHIs

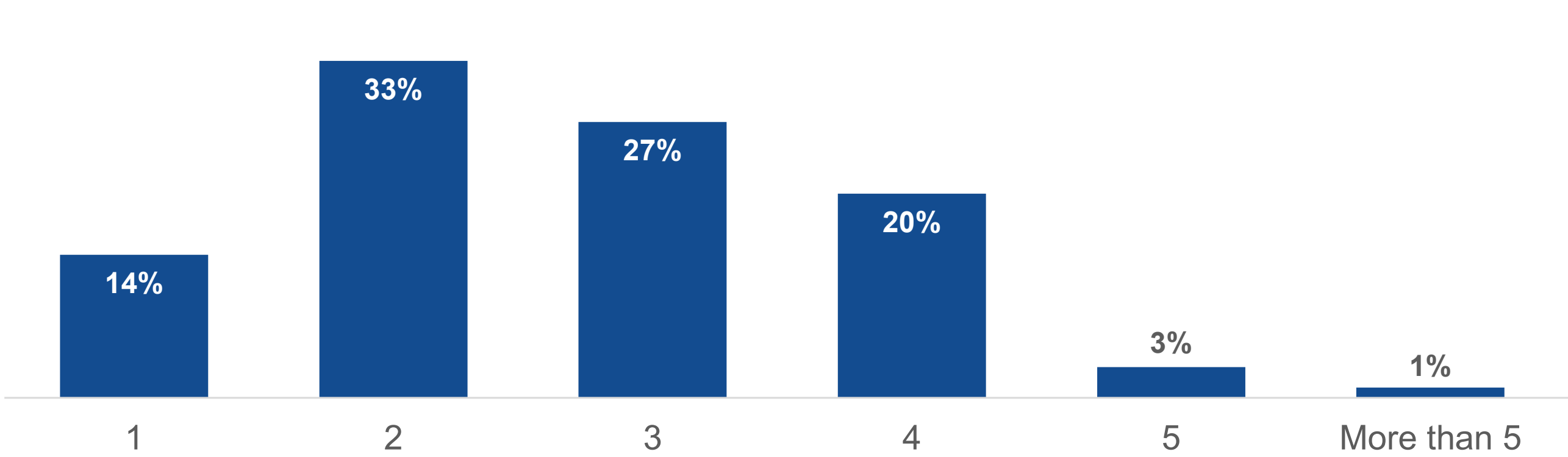
Nearly half (46%) of respondents know their organization has experienced a breach of non-human identities, and another 26% suspect that they have had NHI accounts or credentials compromised. Those that have avoided NHI compromises are more likely to be *completely* confident in their ability to discover NHIs.

Enterprises that have experienced a compromised NHI have averaged 2.7 instances in the past 12 months.

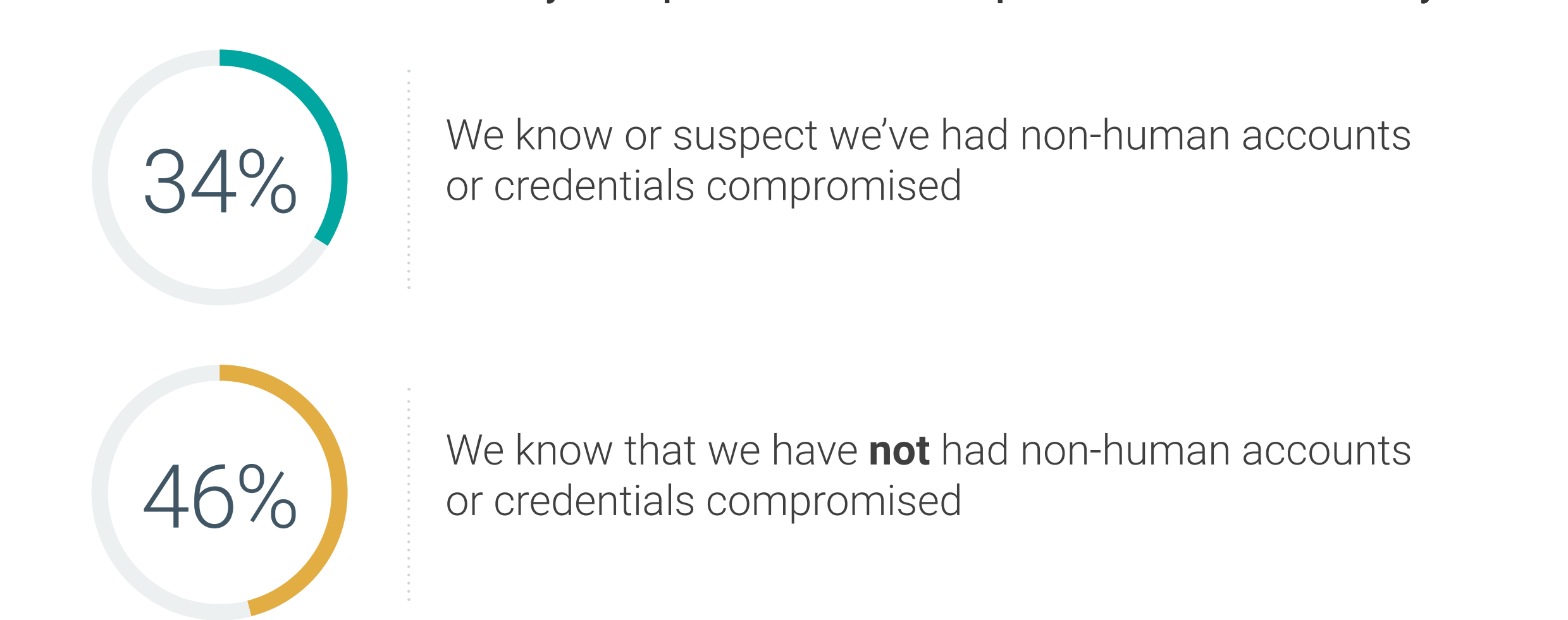
Have organizations experienced any compromises of NHI accounts or credentials in the last 12 months?



Number of times NHI accounts or credentials have been compromised in the last 12 months.



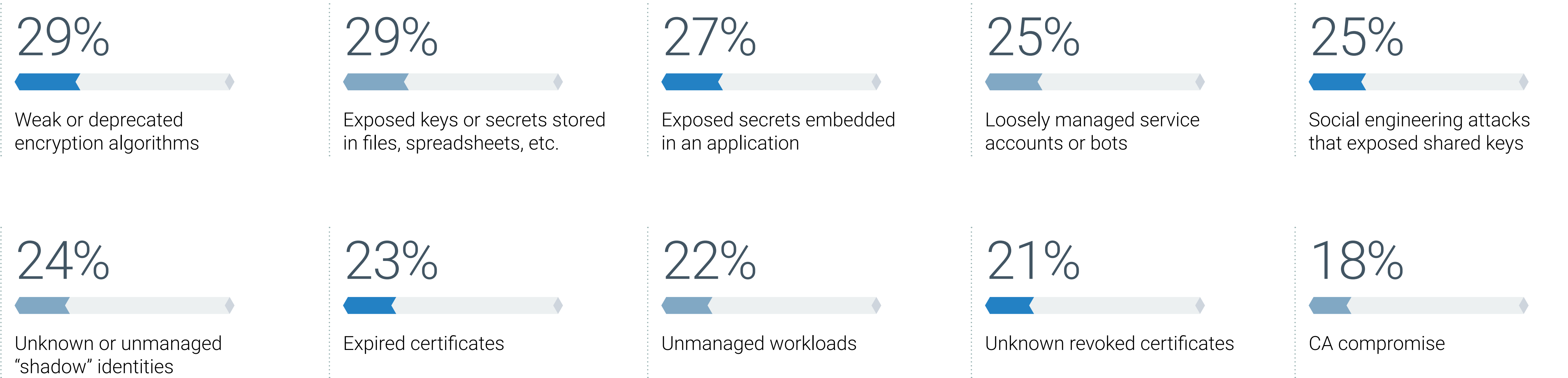
Percentage of organizations that are completely confident that they can discover workload identities based on whether they've experienced NHI compromises within the last year.



Multiple Factors Lead to Non-human Identity Compromises

What factors contributed to the compromise (whether confirmed or suspected) of organizations’ non-human accounts or credentials? At least one-quarter of organizations cited weak encryption algorithms, exposed keys or secrets, and/or loosely managed service accounts.

Factors that contributed to the compromise, or suspected compromise, of NHI accounts or credentials.

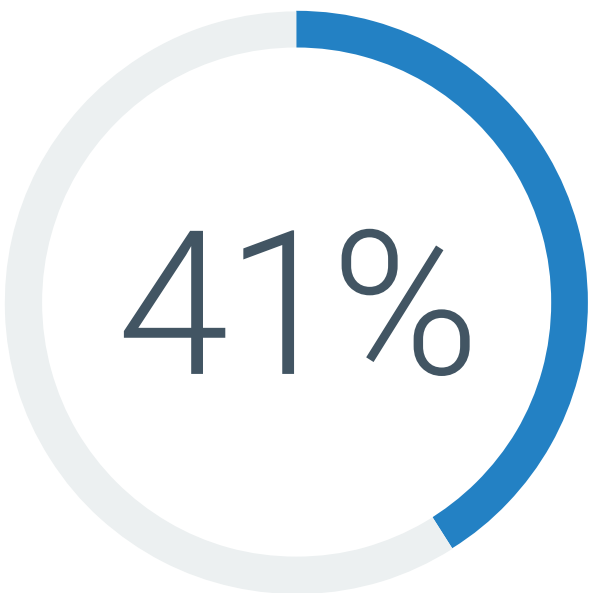


Compromised NHI Accounts Frequently Lead to Successful Cyberattacks With Multiple Ripple Effects

Two-thirds of enterprises have endured a successful cyberattack resulting from compromised non-human identities, with a quarter of enterprises encountering multiple attacks.

Businesses suffer manifold impacts as a result of successful cyberattacks spawned from NHI compromises, from reputational damage through compliance fines to more expensive cyber insurance rates. Security teams frequently see increased budgets and investment but can also encounter leadership changes as a result of successful cyberattacks.

Have organizations' compromised NHI accounts or credentials over the last 12 months led to a successful cyberattack?

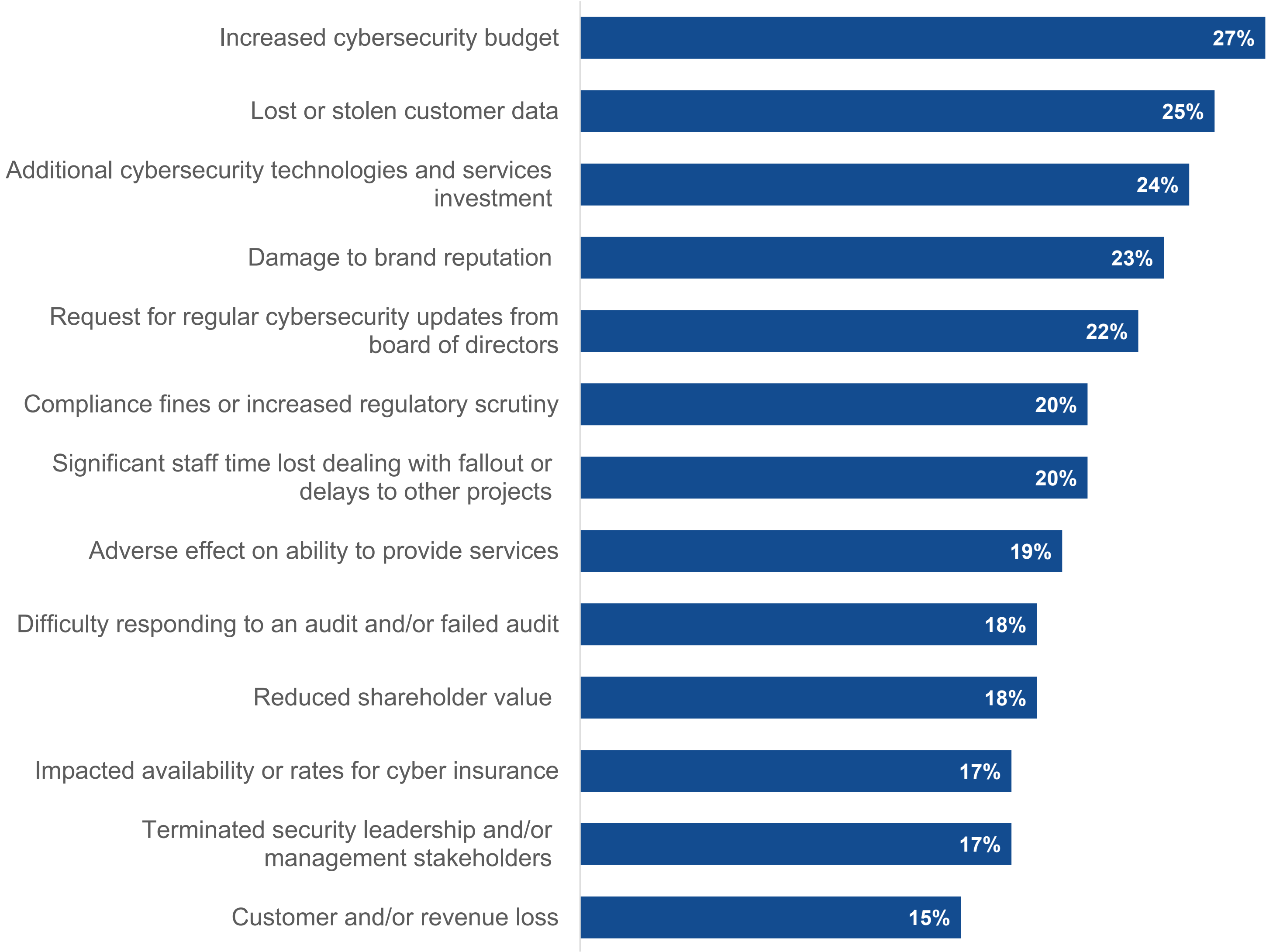


Yes, one attack



Yes, multiple attacks

Business impacts stemming from successful cyberattacks tied to the compromise of a NHI account or credential in the last 12 months.



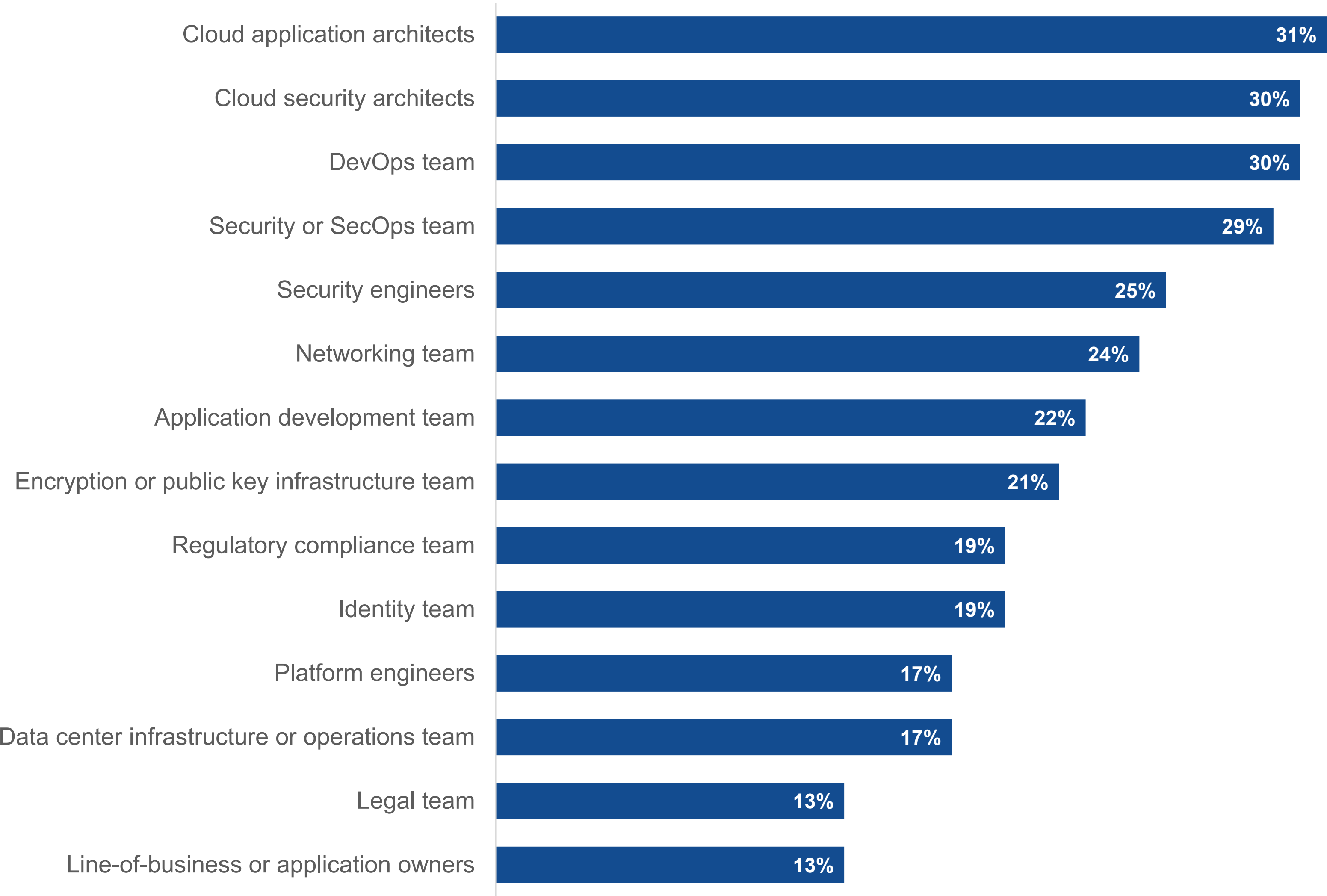
Non-human Identity Management Has Diverse Constituents, and Compromises Get Board-level Attention



Technology Personas Drive Management Policies for Non-human Identities and Workloads

Cloud architects, DevOps, and SecOps teams are most commonly involved in processes to create policies around non-human identities and workloads. Nearly one in five organizations say their identity team is involved.

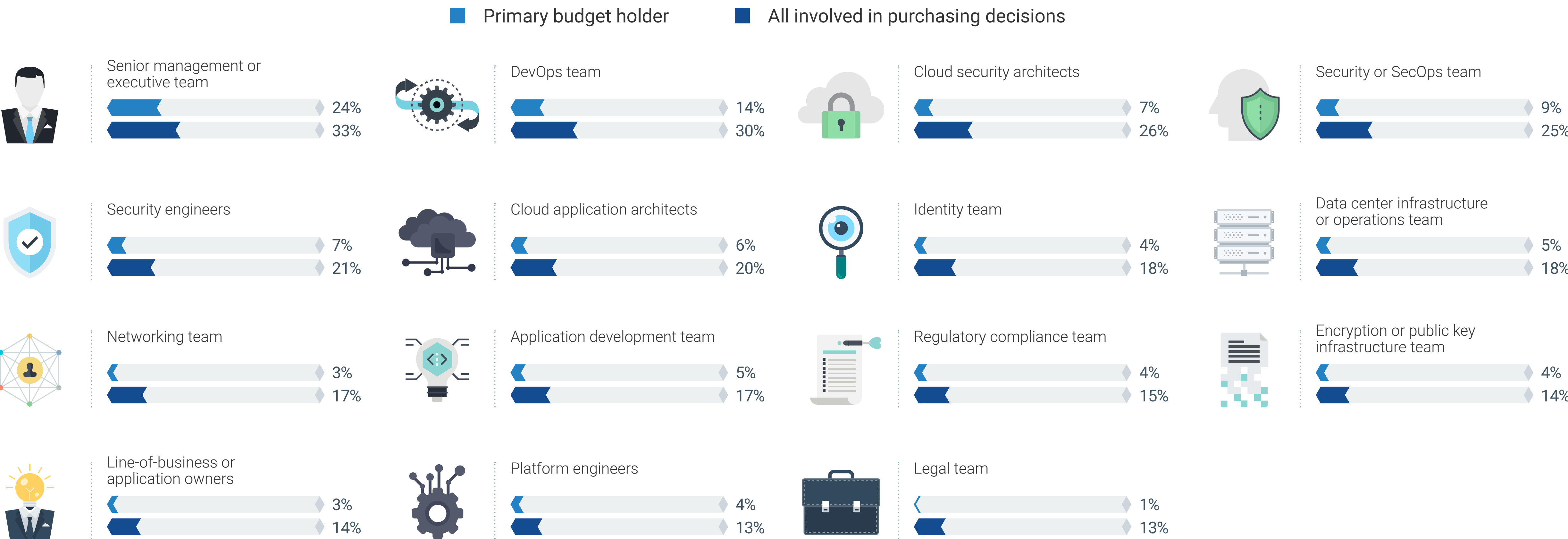
Groups directly involved in creating management policies for non-human identities and/or workloads.



Diverse Constituency of Decision-makers, but Security Is Well-represented as Budget Holder

Technology teams in DevOps, cloud security, SecOps, and cloud applications contribute to evaluating, recommending, and purchasing solutions, but the security personas (32%) are the most common budget holders. Senior management and executive teams continue to be highly frequent influencers and budget holders since cybersecurity has gained more visibility in the C-suite and with boards of directors in the wake of high-profile incidents and their adverse impacts on business operations.

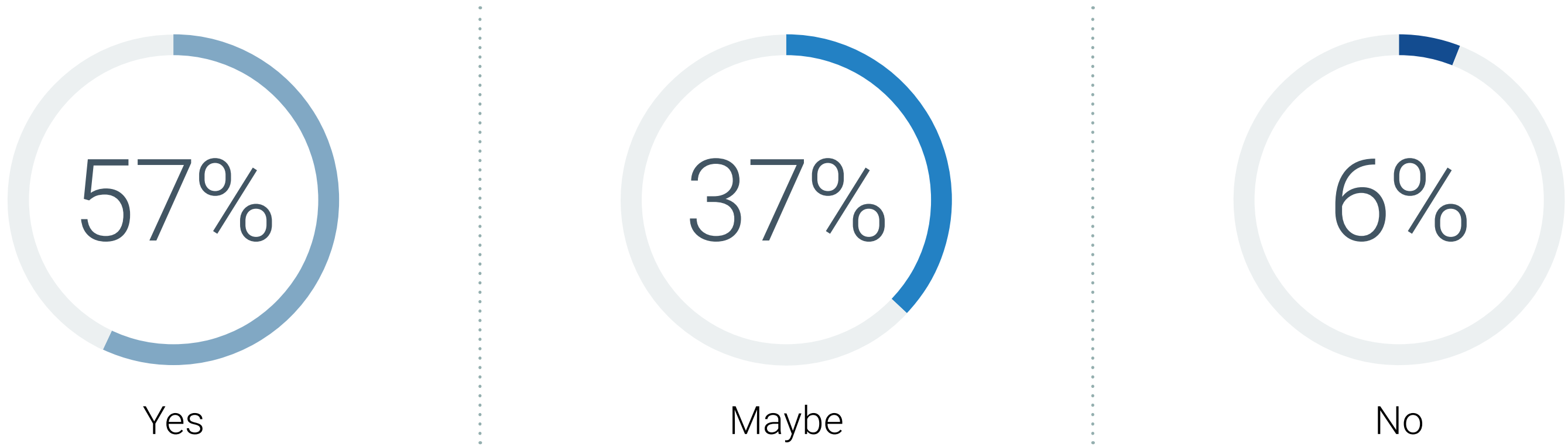
Groups involved with purchasing decisions and group that holds budget for NHI management products and services.



Non-human Identity Security: The Board Will See You Now

Non-human identity compromise has the potential to be significantly disruptive to business operations. Indeed, a majority (57%) of non-human identity compromises definitively got board-level attention, while 37% of respondents indicated their organization’s board may have delved into the details of the incident.

Did a successful cyberattack tied to the compromise of a non-human account in the past 12 months get board-level attention?



“A majority (57%) of non-human identity compromises **definitively got board-level attention**, while 37% of respondents indicated their organization’s board may have delved into the details of the incident.”



**Enterprises Are Investing Disproportionately
to Solve for Non-human Identity Security**

Non-human Identity Security Spending Is Primed to Increase

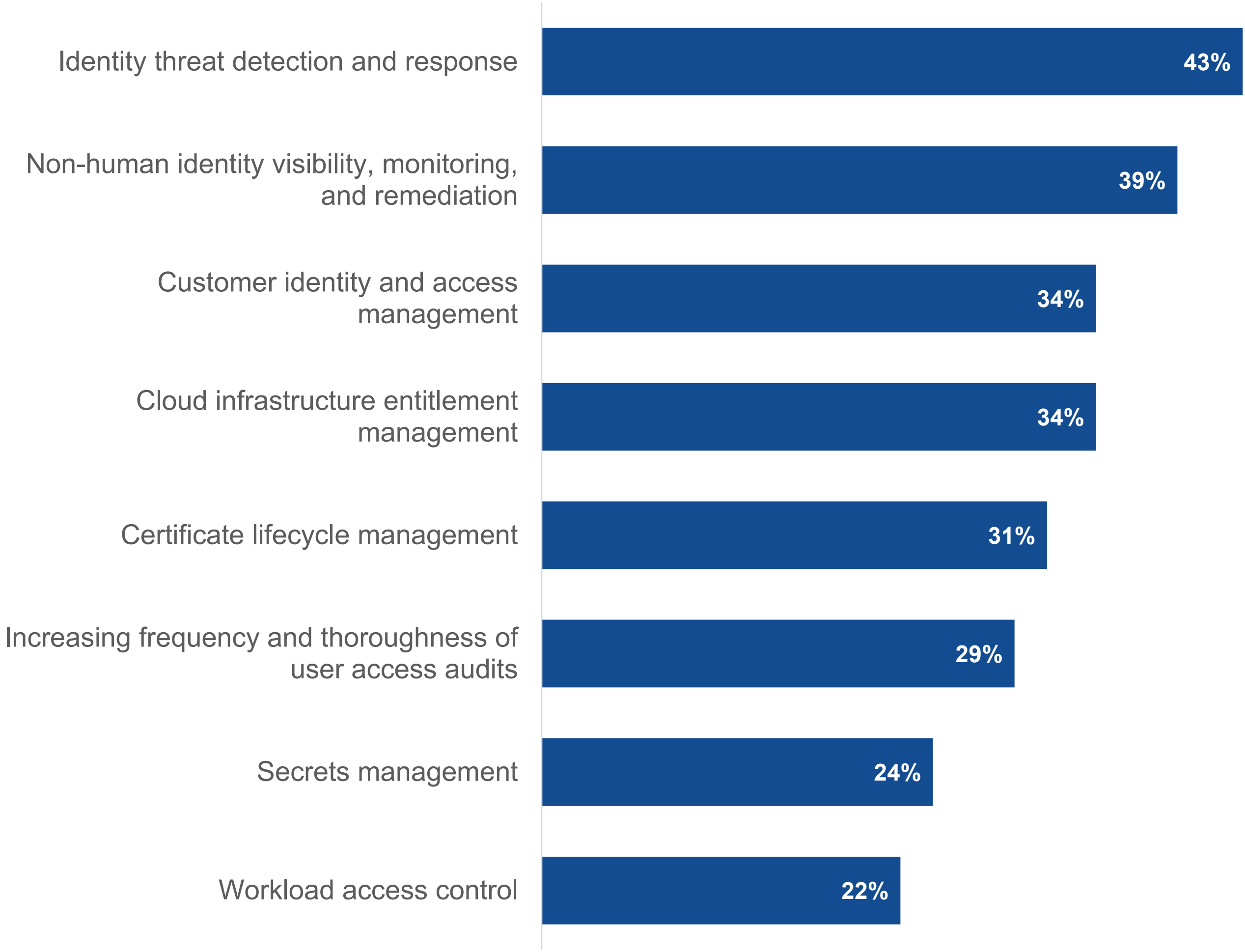
A notable 83% of organizations expect to spend relatively more on non-human identity security, with nearly one in five expecting to spend *significantly* more.

Enterprises invest in solutions to solve specific problems, and non-human identity management involves diverse problems. More than four in ten organizations expect to increase spending on identity threat detection and response solutions, while 39% will prioritize investments in technologies designed to address visibility, monitoring, and remediation for non-human identities.

Expected change in spending on NHI security over the next 12 months.



Areas organizations expect most of their NHI security investment to go to over the next 12 months.





ABOUT

Anetac has built a world-class Dynamic Identity Vulnerability and Security SaaS Platform that offers continuous visibility of the ever-evolving machine identity account landscape. Anetac automates the discovery of all machine and human identities; including service accounts, APIs, and tokens, and provides a map of their access chains to detect over privileged accounts. The Anetac platform also provides insights into password compliance and works across on premise, cloud, and hybrid environments. Founded in Los Altos, California in 2023, Anetac proactively solves the disconnect of static scanning tools with an innovative, streaming approach that dynamically addresses identity security posture management problems.

LEARN MORE

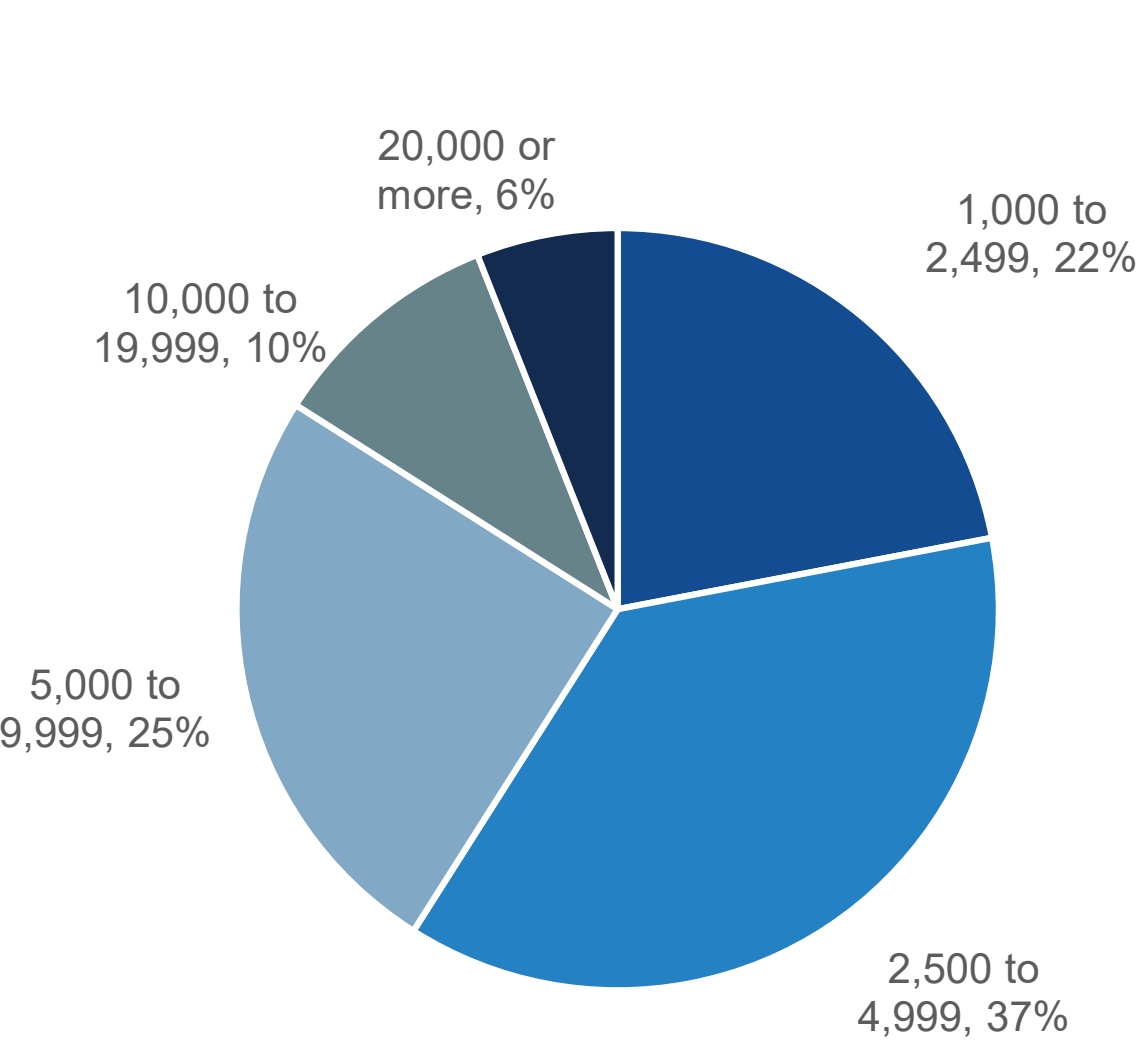


RESEARCH METHODOLOGY AND DEMOGRAPHICS

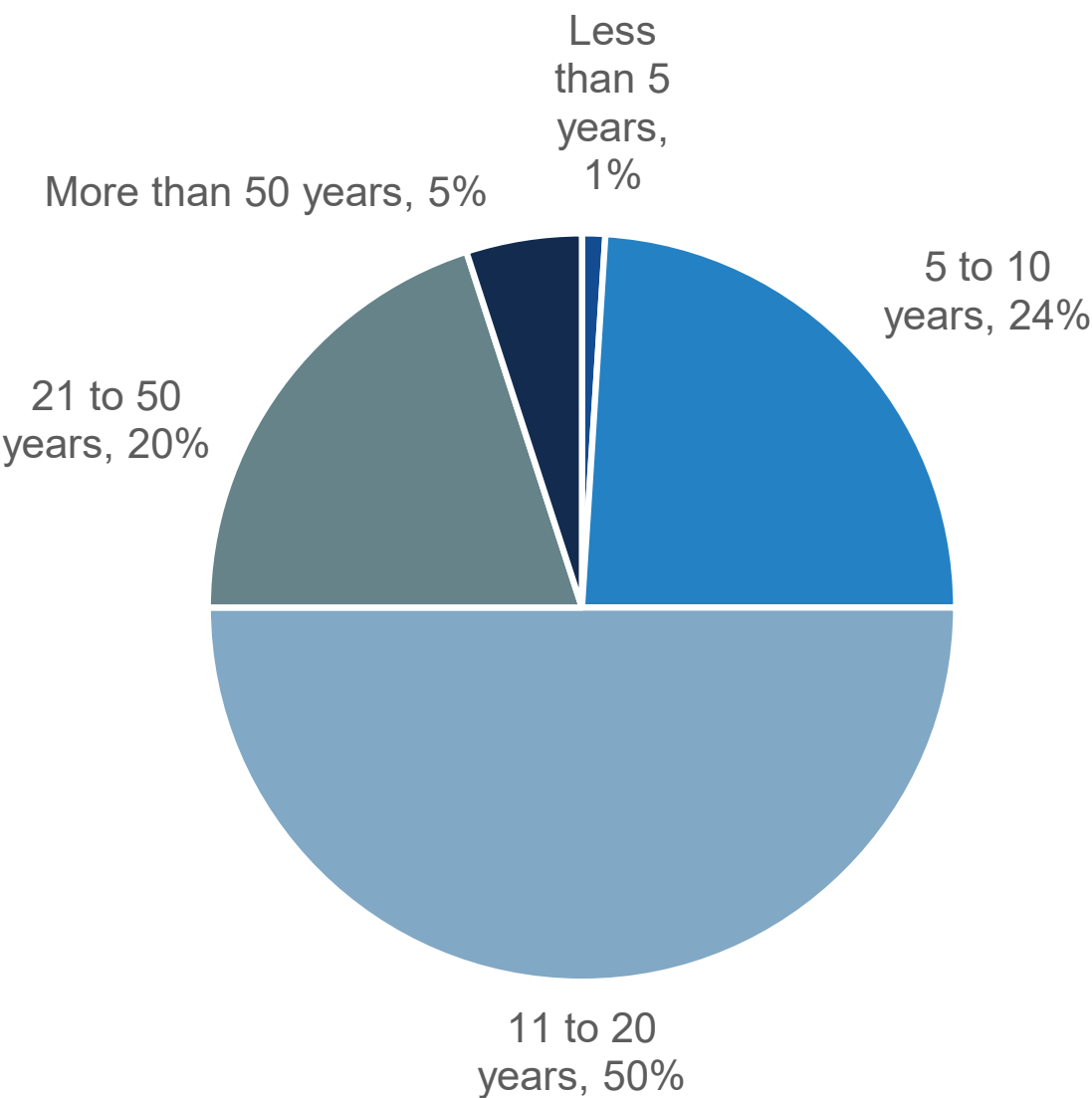
To gather data for this report, Enterprise Strategy Group conducted a comprehensive online survey of IT, cybersecurity, and DevOps, platform, and security engineering professionals from private- and public-sector organizations in North America (United States and Canada) between July 17, 2024 and July 28, 2024. To qualify for this survey, respondents were required to be involved with the technologies and processes that secure non-human identities, including machine identities, workload identities, certificates, and service accounts. 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 367 IT, cybersecurity, and DevOps, platform, and security engineering professionals.

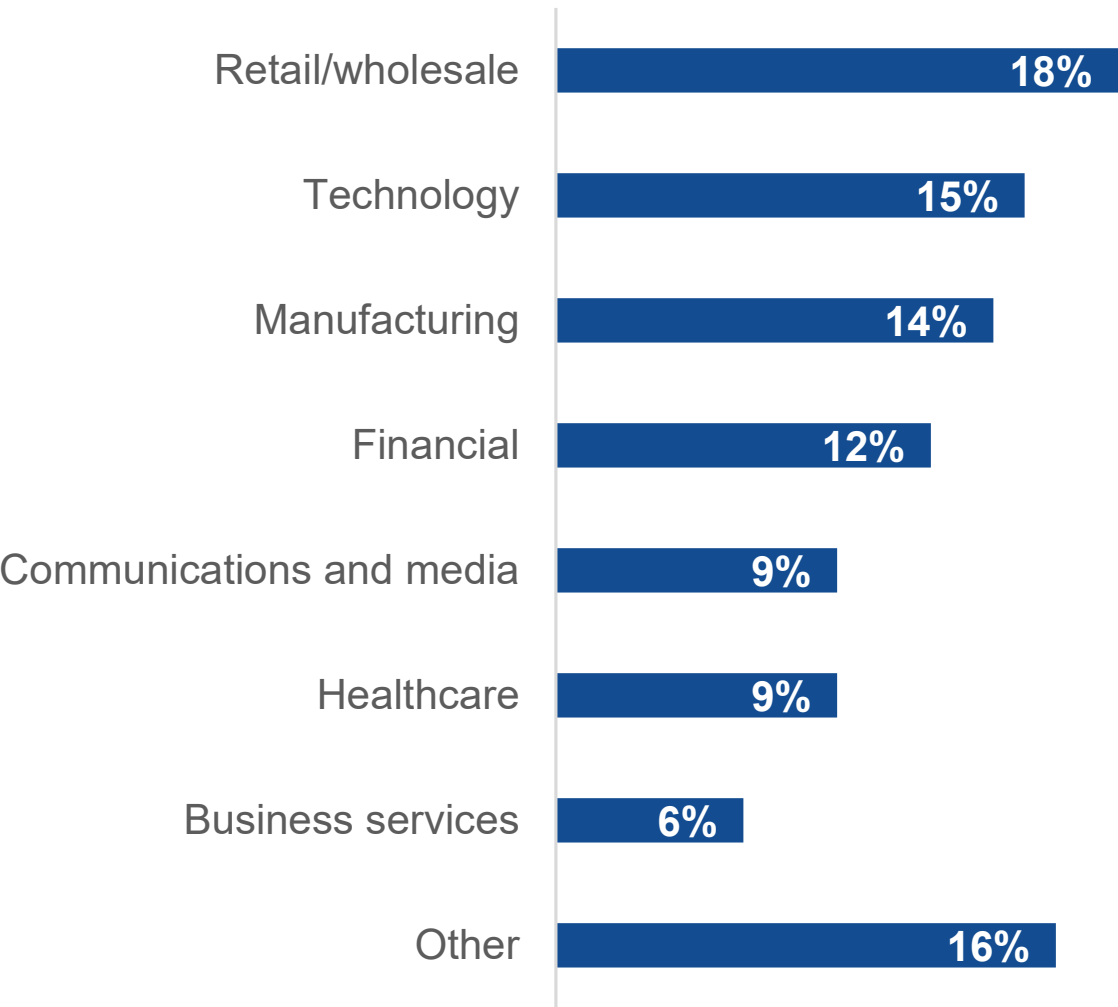
Respondents by number of employees.



Respondents by company age.



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.



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.