ESG Enterprise Strategy Group | Getting to the bigger truth.™

RESEARCH HIGHLIGHTS

Trends in Identity and Access Management: Cloud-driven Identities

Doug Cahill, VP and Group Director

OCTOBER - 2020

CONTENTS

Research Objectives

The broad adoption of public cloud services demands a retooling of identity and access management programs. Perimeter security must evolve from a traditional castle and moat model to one that focuses on cloud identities inclusive of service accounts, as well as individual users and the data they access. To protect sensitive cloud-resident data, cybersecurity and IT operations teams need to work with their line-of-business teams on strengthening identity programs with both the user experience and risk in mind.

In order to gain insight into these trends, ESG surveyed 379 IT and cybersecurity professionals at organizations in North America (US and Canada) personally responsible for evaluating or purchasing identity and access management and cloud security technology products and services. This research aimed to understand the problem space, organizational responsibilities, compliance implications, and plans for securing user access to a wide portfolio of cloud services. The study will also look at the current and planned use of various authentication methods, privileged access management, device profiling, unified directories, user activity analytics, and service account protection.

This study sought to:

Understand how cloud adoption is influencing identity and access management (IAM) strategies.

Gain insight into IAM challenges and threats associated with cloud usage.

Assess which IAM and IGA technologies organizations are prioritizing to secure access to a range of public cloud services.

Examine the buying intentions and organizational responsibilities regarding IAM and IGA offerings.

Key Research Findings

The complexion of public cloud usage is increasingly business-critical, but in a hybrid, multi-cloud context. No longer relegated to tertiary use cases, both SaaS applications and internally developed cloud-native applications deployed on IaaS/PaaS platforms serve as the backbone of front, middle, and back office operations. The expanding adoption of public cloud services is resulting in an appreciable projected increase in cloud-resident data.

The need to secure access to a diverse range of applications makes maintaining IAM consistency the top challenge. As a result of several factors, including increasing levels of cloud usage and remote employees, maintaining consistency across public and private clouds is the top identity and access management challenge. While most respondents report they can enumerate accounts and permissions associated with their organization’s use of cloud services, nearly a third report they have cloud identities with permissions greater than what is required.

Cloud-related cybersecurity incidents highlight the connection between data and identities. Cloud environments are actively under attacks as evidenced by the three-quarters of respondents who reported a cloud-related cybersecurity incident or attack over the last 12 months. The prevalence of shadow IT, the improper use of sanctioned cloud applications, and sharing data with third parties create a visibility gap, resulting in many organizations being unsure of whether they have lost cloud-resident data.

Organizational convergence and vendor consolidation are underway to enable a shift from a siloed to unified approach. To gain consistency across disparate environments, a unified identity and access management strategy that can be applied across hybrid, multi-clouds is the highest IAM priority moving forward. IT and cybersecurity teams will increasingly seek solutions that enable the implementation of unified identity and access management measures across disparate environments.

Zero-trust is driving a focus on MFA, device profiling, and user monitoring, an expansion of IDaaS use cases. Friction in the end-user experience has been an impediment to broader use of multi-factor authentication (MFA) to secure access to a range of cloud services and systems. As a result, many organizations are now planning to use device trust in their access policies with the proper configuration of devices being the attribute to verify device trust.

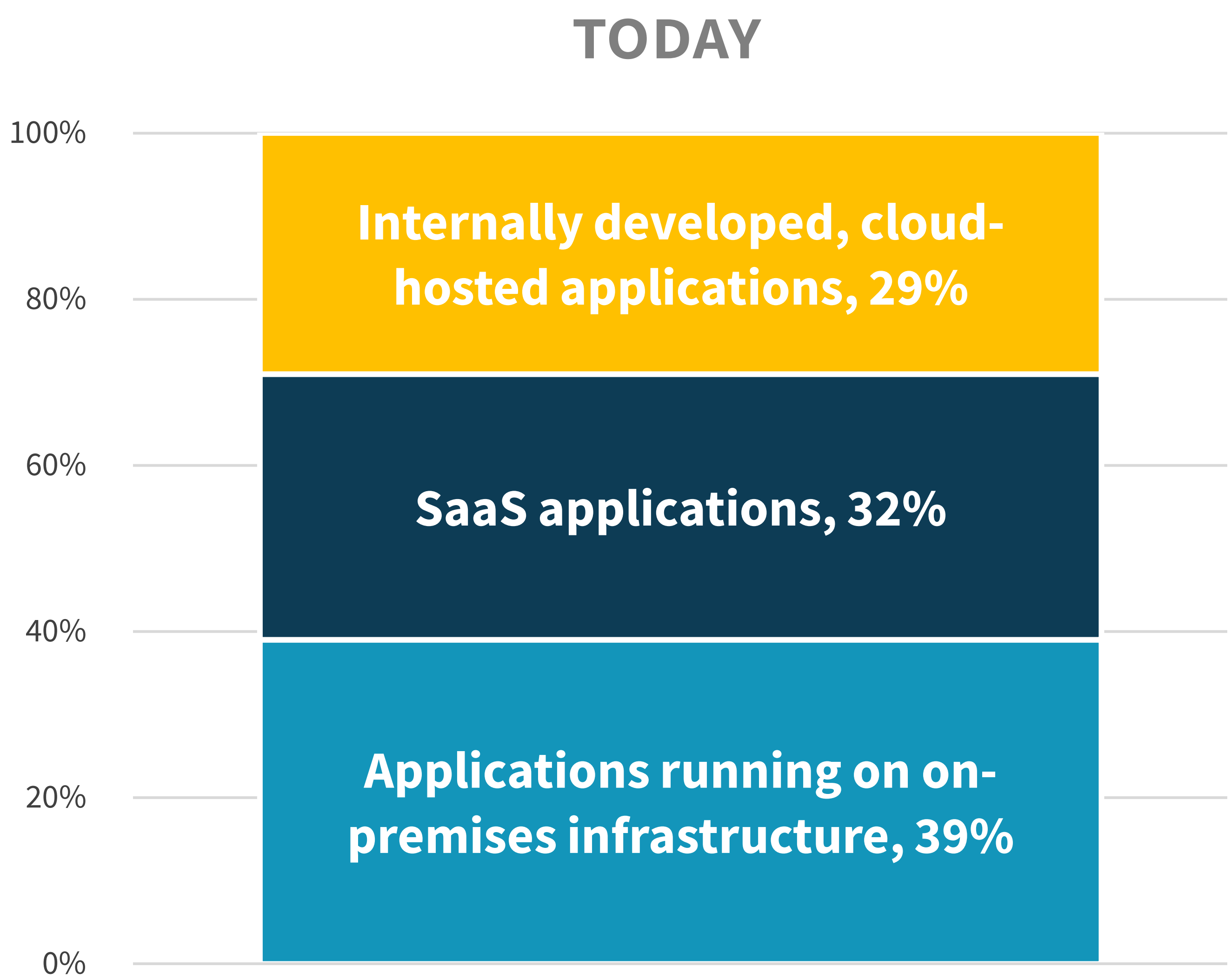
Back to Contents

The complexion of public cloud usage is increasingly business-critical, but in a hybrid, multi-cloud context.

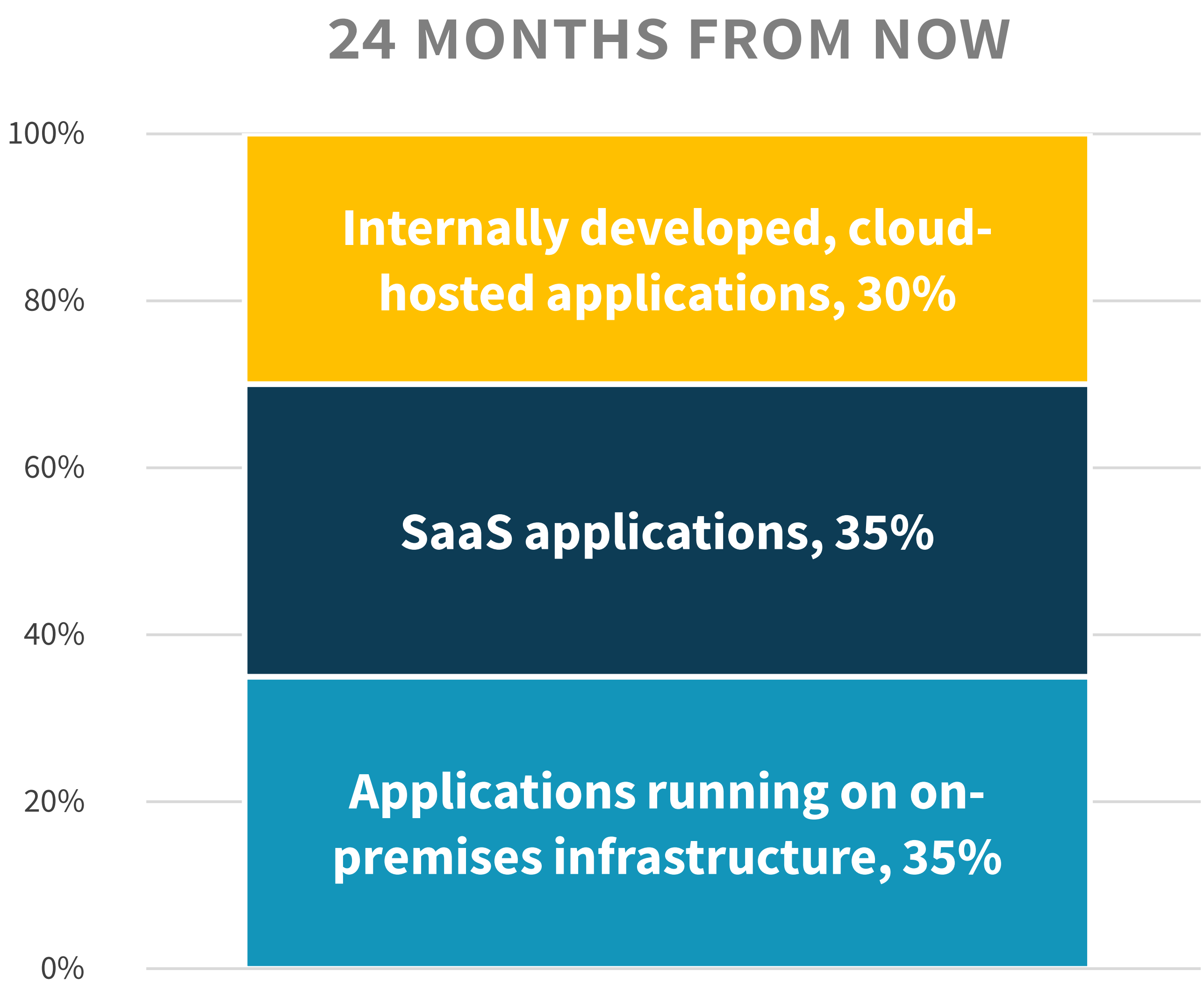
Business-critical Applications Span Hybrid, Multi-clouds

No longer relegated to tertiary use cases such as dev and test or archiving, organizations now rely on public cloud services for essential workloads. Both SaaS applications and internally developed cloud-native applications deployed on IaaS/PaaS platforms serve as the backbone of front, middle, and back office operations. On-premises applications will, however, continue to be essential, highlighting the hybrid, multi-cloud composition of the modern data center.

» Business-critical application deployments



Percent of business-critical applications running on each today



Percent of business-critical applications running on each in 24 months

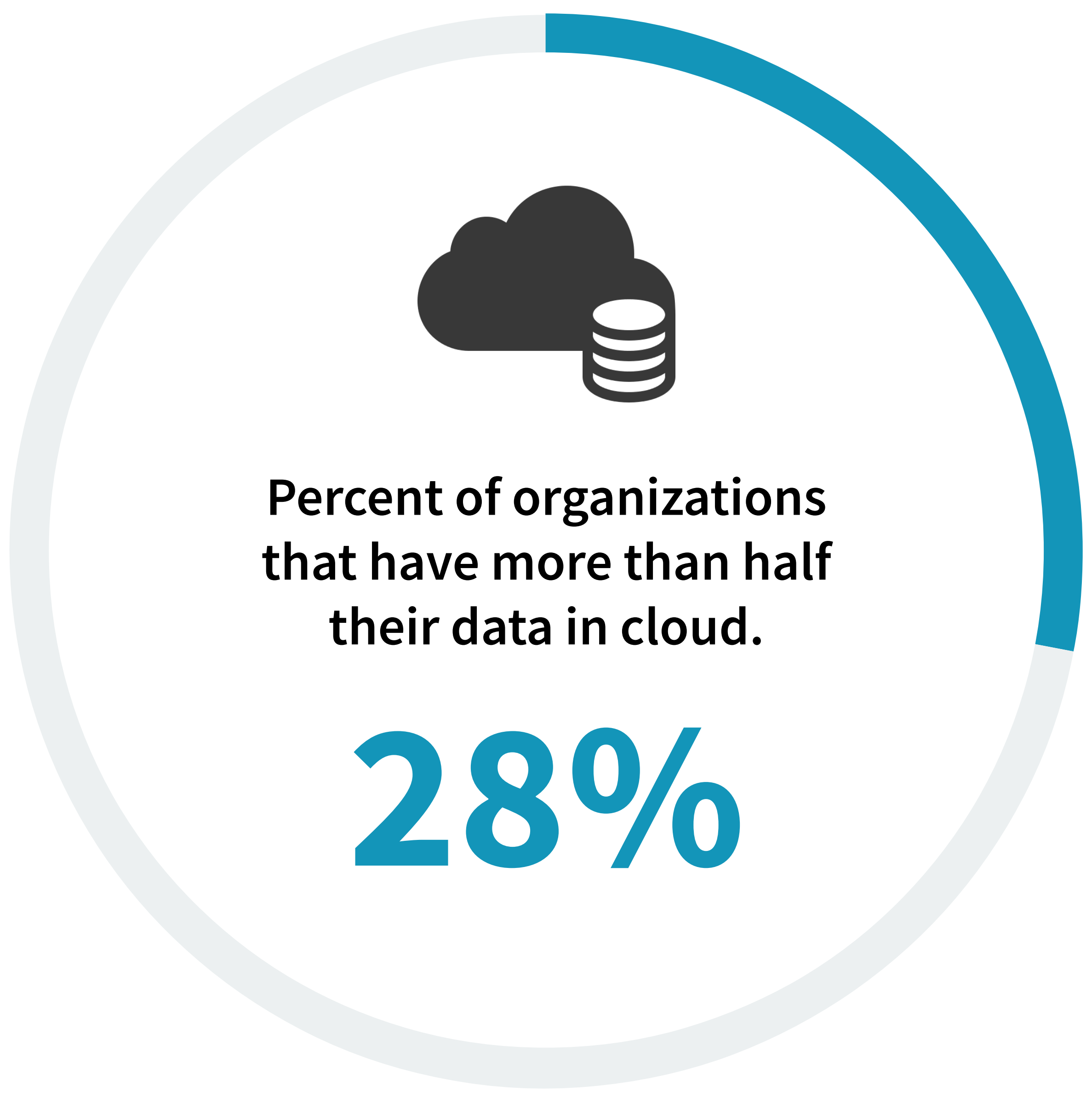
Back to Contents

As Data Shifts to Public Clouds, Sensitive Data Is Being Stored with a Variety of Cloud Services

The expanding adoption of public cloud services is resulting in an appreciable projected increase in cloud-resident data. In fact, the percentage of organizations that store more than half of their data in public clouds is expected to more than double in the next 24 months. The use of public cloud for business-critical purposes is further evidenced by the amount of cloud-resident data that respondents consider sensitive. Those organizations that share most of their cloud-resident data is sensitive note the amount of that data is relatively proportional across different types of cloud services.

> *The percentage of organizations that store more than half of their data in public clouds is expected to* ***more than double in the next 24 months.*** ”

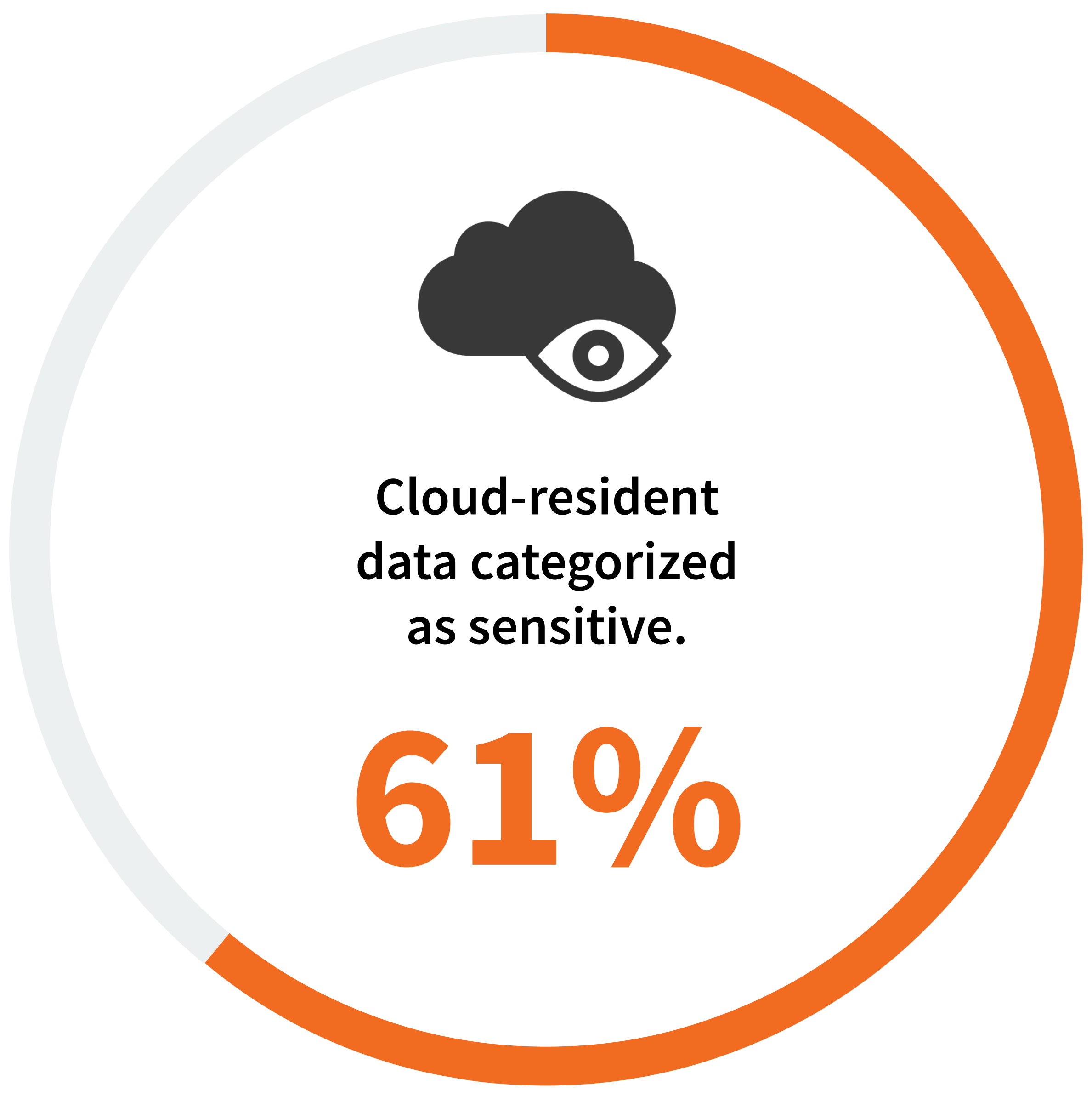
TODAY



Percent of organizations that have more than half their data in cloud.

28%

24 MONTHS FROM NOW



Cloud-resident data categorized as sensitive.

61%

Back to Contents

The need to secure access to a diverse range of applications makes maintaining IAM consistency the top challenge.

Maintaining Consistent IAM Policies Across Environments Is Challenged by Heterogeneity and Remote Workers

Complexity has long been a principal enemy of cybersecurity. The differences between cloud environments and the devices used to access resources further promotes complexity while introducing additional cost. The increase in remote work has exacerbated this issue with IT and cybersecurity teams now charged with providing secure access from heterogeneous devices to a heterogenous mix of applications. As a result, maintaining consistency across public and private clouds is the top identity and access management challenge.

» Most common cloud-specific identity and access management challenges.

33%

Maintaining security consistency across our own data center and public cloud environments

32%

An increase in remote users as a result of the coronavirus pandemic requires access to a diverse range of applications

» Organizations agree

81%

Specialized cloud IAM controls increase cost and complexity

80%

The differences between cloud applications, infrastructure, and DevOps tools and the rest of our apps require a different set of IAM policies and technologies

77%

Heterogeneity of end-user devices types and operating systems makes using devices as an identity attribute challenging

Overly Permissive Cloud Identities Create a Visibility Gap

The interwoven relationship between identities and data is highlighted by a disconcerting visibility gap. A majority of organizations report it is difficult to know which users and which service accounts have access to their company's cloud-resident sensitive data. The root cause is permissions. While most respondents report they can enumerate accounts and permissions associated with their organization's use of cloud services, nearly a third report they have cloud identities with permissions greater than what is required. As a result, the top type of misconfigured cloud services discovered over the last 12 months are over-permissioned accounts and roles.

*Average organization says **30% of their cloud identities are overly permissive.***

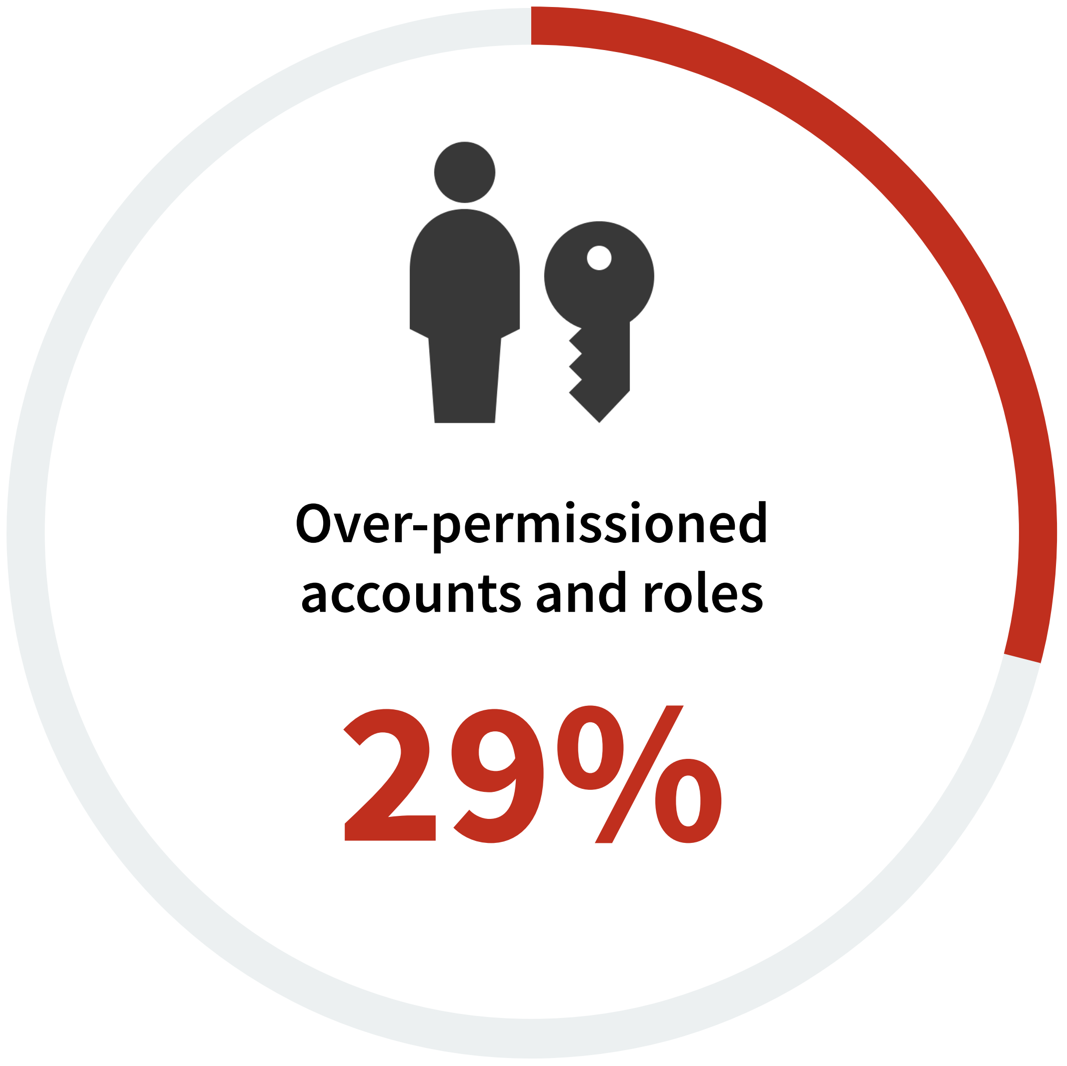
52%

say it is difficult to map **service account** access to cloud-resident sensitive data

52%

say it is difficult to map **user account** access to cloud-resident sensitive data

MOST COMMON TYPE OF MISCONFIGURED CLOUD SERVICE:



Over-permissioned accounts and roles

29%

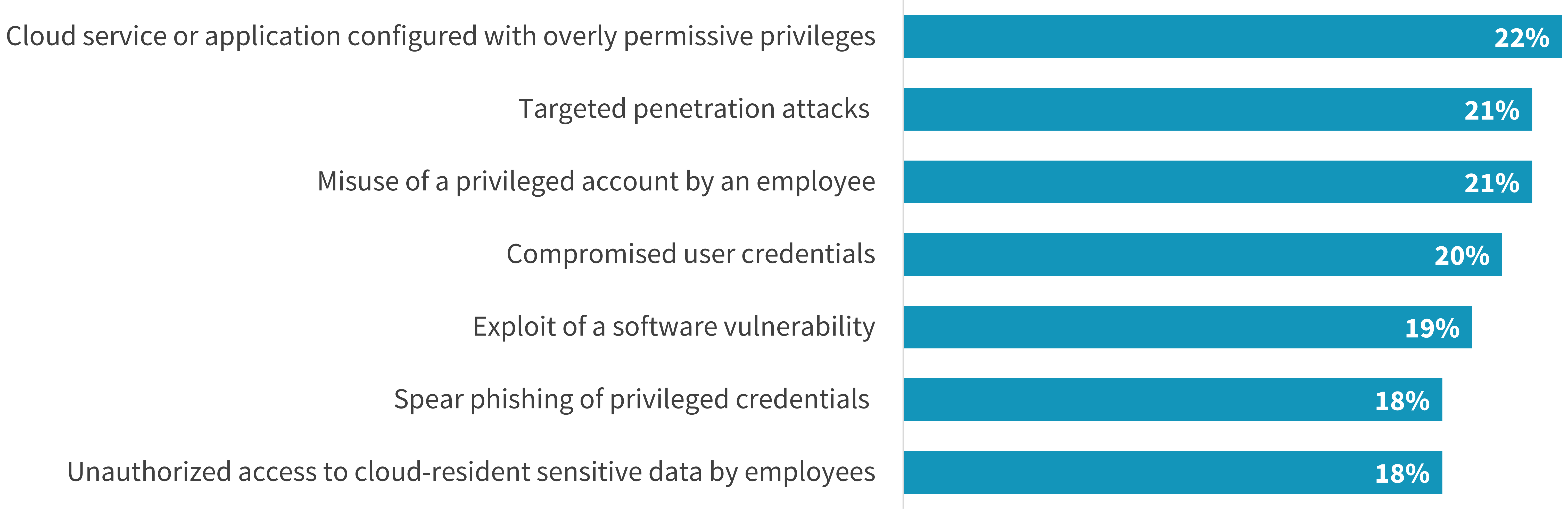
Back to Contents

Cloud-related cybersecurity incidents highlight the connection between data and identities.

The Most Common Types of Attacks Against Public Cloud Entail Exploiting an Identity

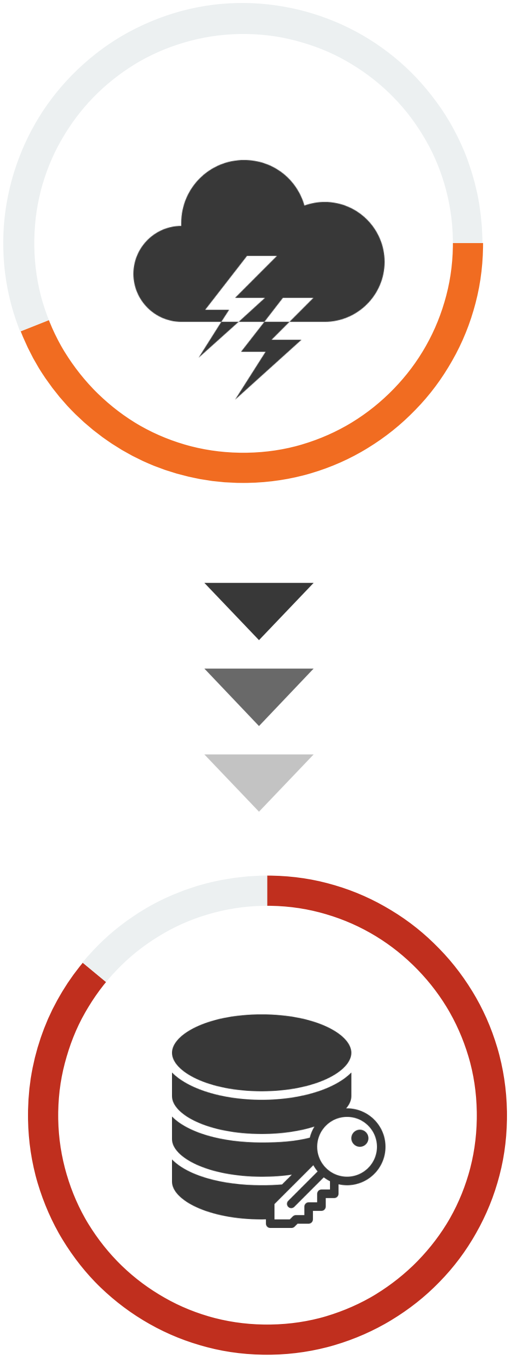
Cloud environments are actively under attacks as evidenced by the three-quarters of respondents who reported a cloud-related cybersecurity incident or attack over the last 12 months. Over-permissioned roles and the misuse of privileged accounts have ramifications, with each contributing to cybersecurity incidents and attacks against cloud applications and infrastructure. The identity theme continues with compromised user credentials and spear phishing of privileged cloud credentials revealing cyber adversaries are actively targeting privileged cloud accounts. But employees also present a risk by exposing sensitive data via authorized access.

» Most common cloud-related cybersecurity incidents and attacks in last 12 months.



Identities Play a Central Role in the Loss of Cloud-resident Sensitive Data

The prevalence of shadow IT, the improper use of sanctioned cloud applications, and sharing data with third parties create a visibility gap, resulting in many organizations being unsure of whether they have lost cloud-resident data. Most confirm that the cloud-resident data their organization lost was sensitive or could have been. The lack of knowledge of what data was lost highlights the need for data discovery and classification. At the same time, the other top causes of data loss from cloud stores include user negligence, use of personal devices, over-permissive credentials, and stolen credentials, highlighting the connection between cloud identities and protecting sensitive data.

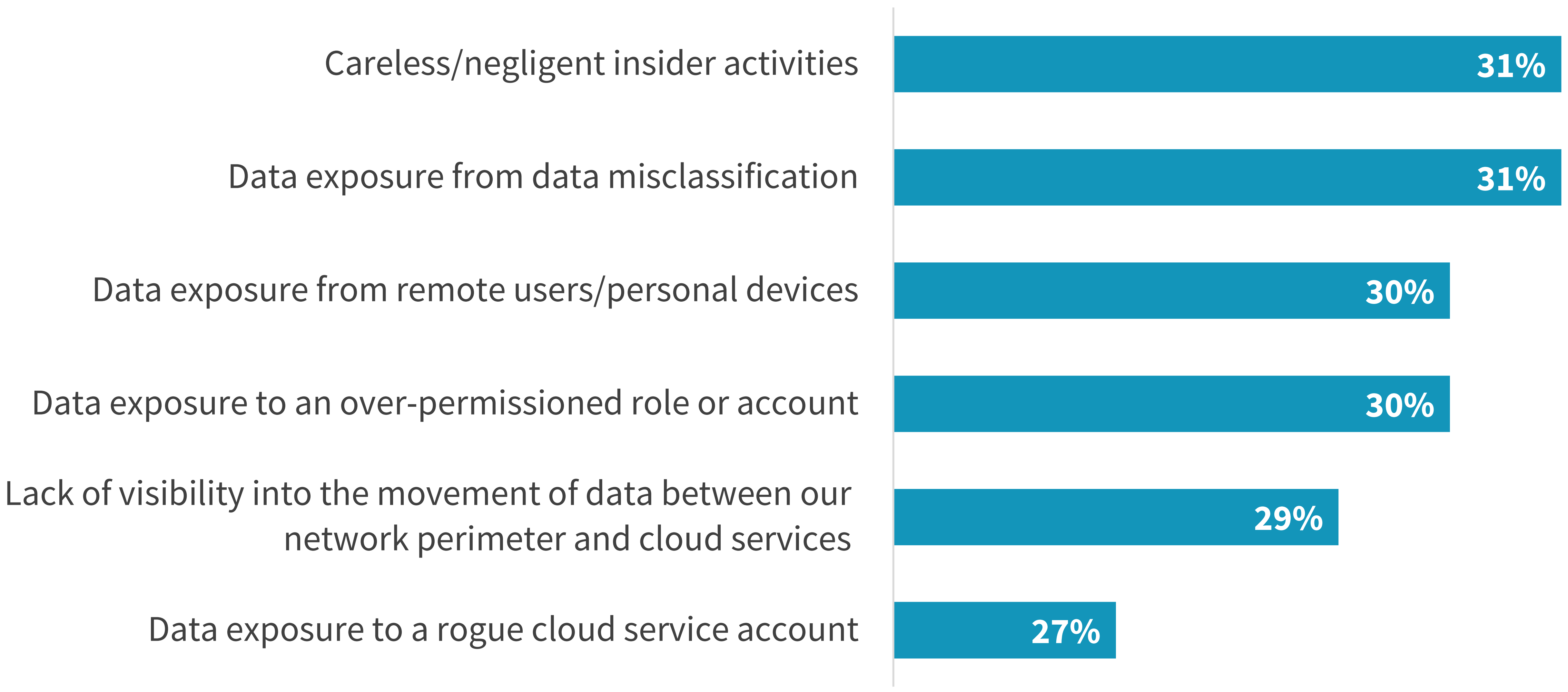


44%

of organizations have lost or suspect they have lost **cloud-resident data** due to a cybersecurity incident.

86%

of those organizations know or suspect lost cloud-resident **data was sensitive.**



» **Biggest contributors to public cloud-related data loss.**

Organizational convergence and vendor consolidation are underway to enable a shift from a siloed to unified approach.

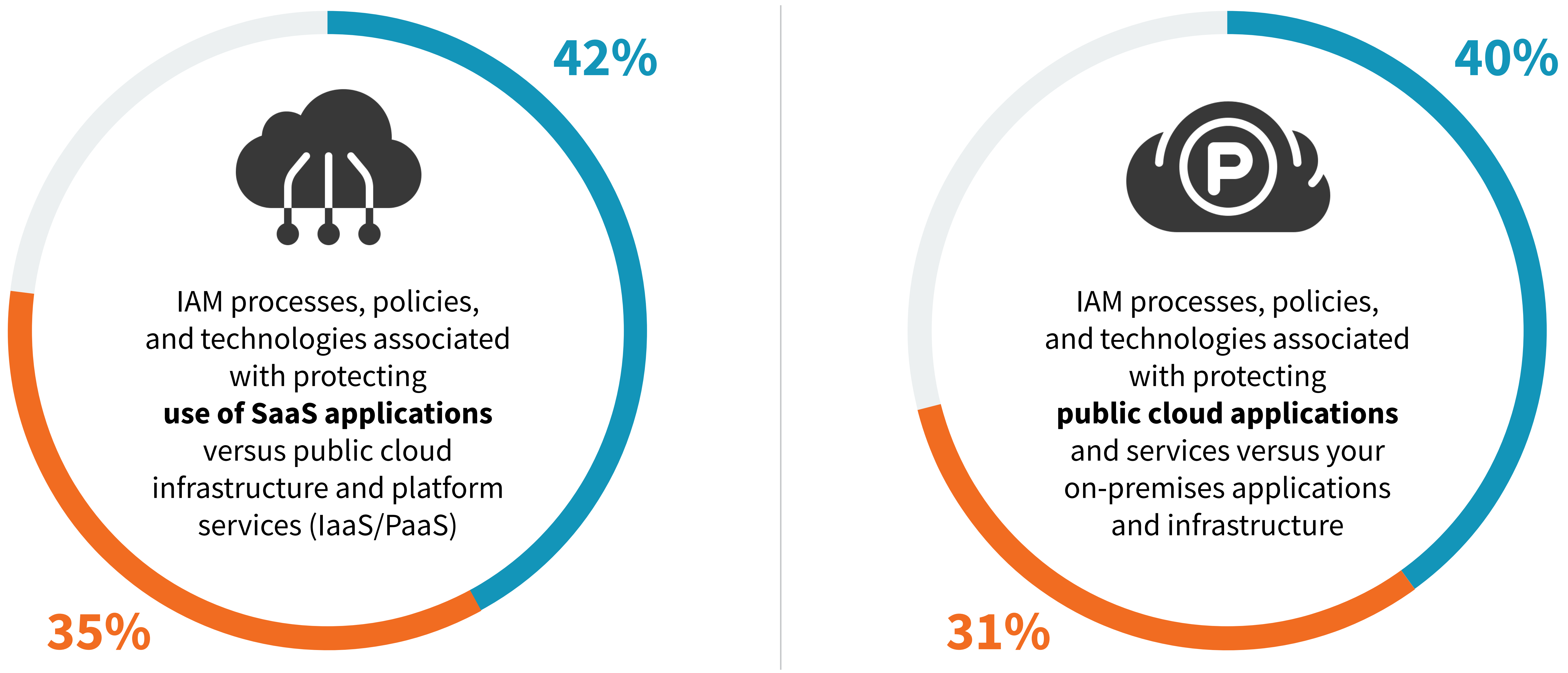
Implementing an IAM Strategy that Spans Public and Private Clouds Requires Organizational Alignment

To gain consistency across disparate environments, a unified identity and access management strategy that can be applied across hybrid, multi-clouds is the highest IAM priority moving forward. To do so, organizations must shift from silos of separate teams that employ separate controls to secure access to separate environments to a converged approach. Such a converged organizational model to unify identity and access management is well underway for both SaaS and cloud-native applications as well as across the totality of cloud and on-premises resources.

***28% say building an IAM strategy** that can span heterogeneous public and private cloud is one of their organization’s highest cloud security priorities.”*

🟦 We have different teams but we plan to merge these responsibilities in the future

🟧 We have already centralized and unified IAM responsibility



IAM processes, policies, and technologies associated with protecting **use of SaaS applications** versus public cloud infrastructure and platform services (IaaS/PaaS)

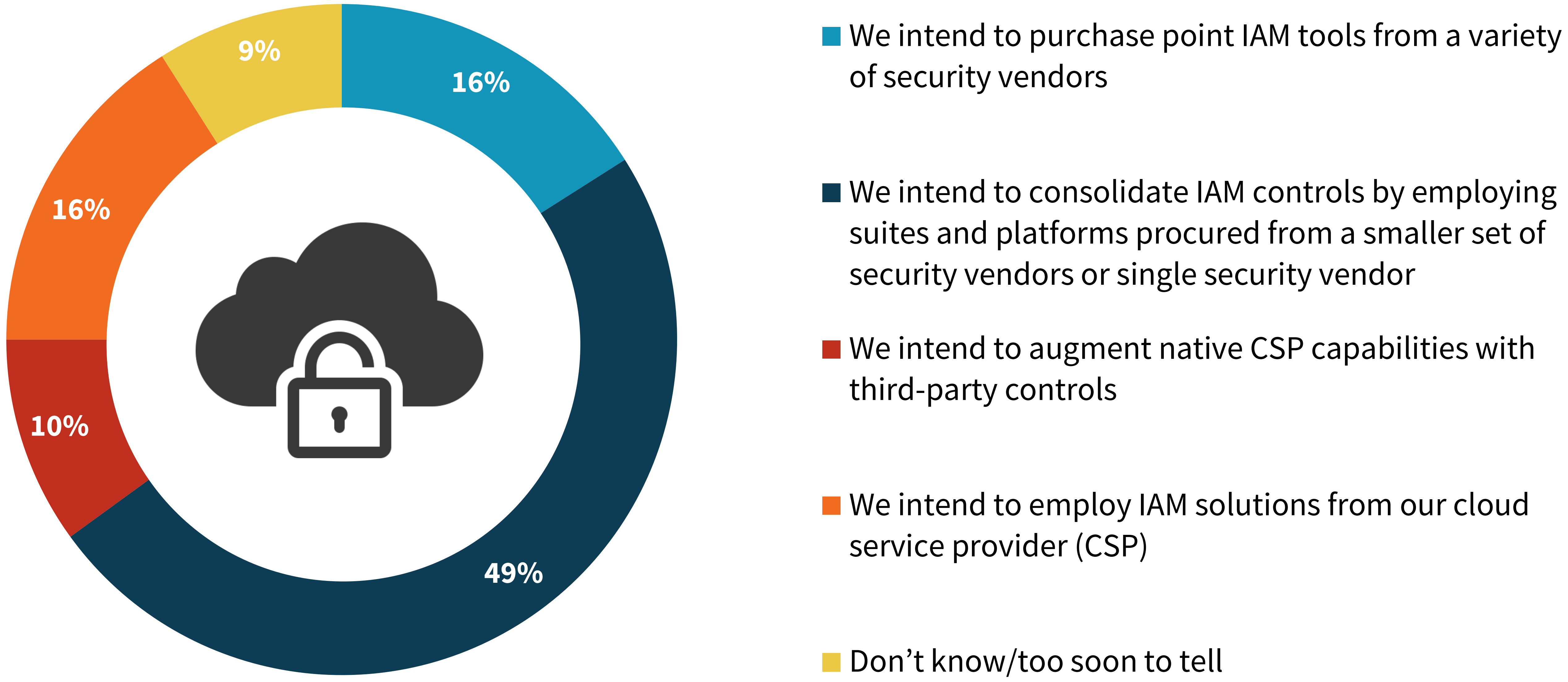
IAM processes, policies, and technologies associated with protecting **public cloud applications** and services versus your on-premises applications and infrastructure

Back to Contents

Vendor Consolidation Will Result in the Emergence of Identity and Access Management Platforms

IT and cybersecurity teams will increasingly seek solutions that enable the implementation of unified identity and access management measures across disparate environments. This will require consolidating separate controls into cloud-ready identity and access management suites that employ a cloud-native platform. Nearly half of the organizations that participated in ESG's research indicated an intent to move in this direction.

» **Likeliest strategy for securing access to public cloud applications and infrastructure services.**

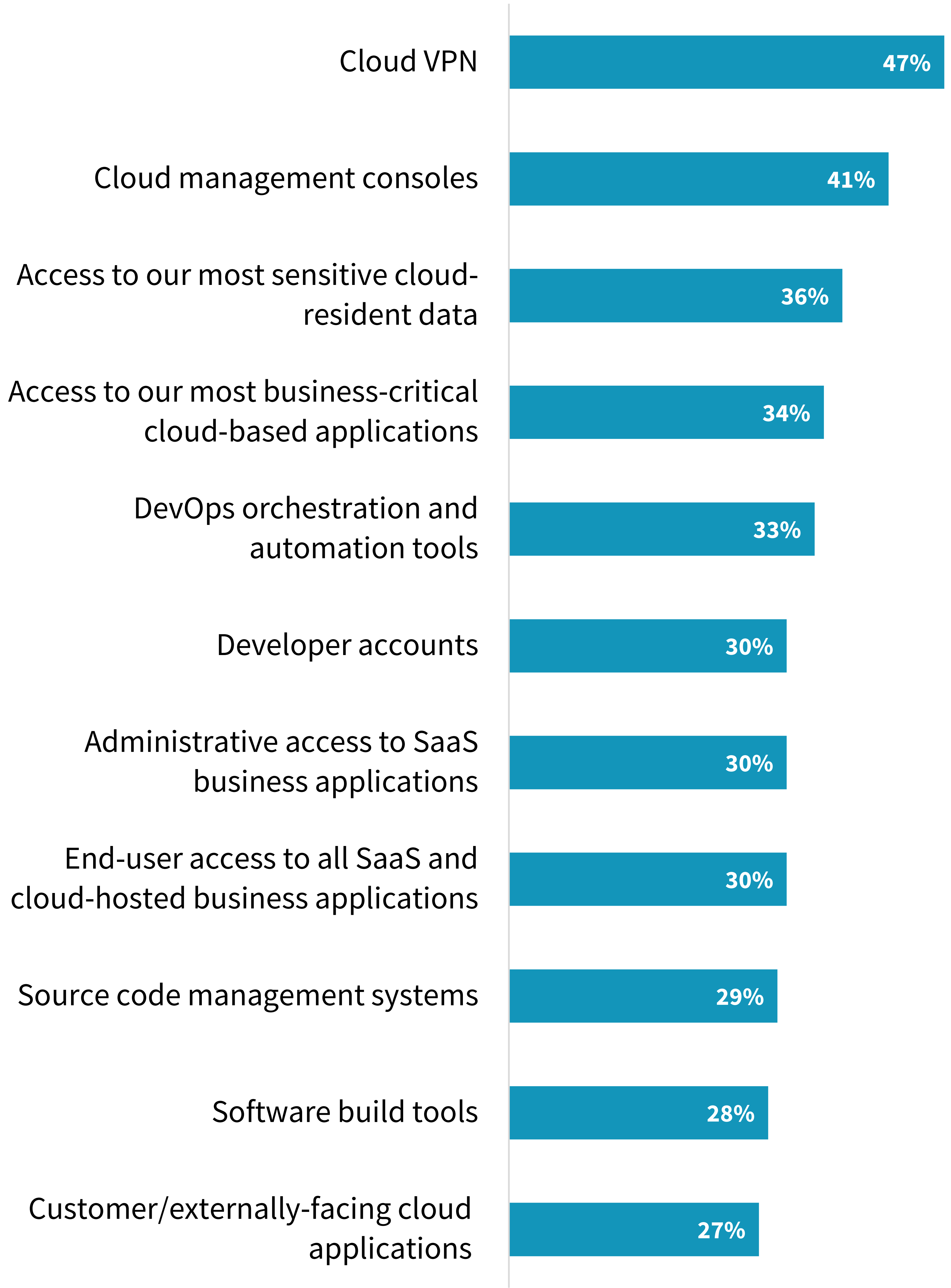


Zero-trust is driving a focus on MFA, device profiling, and user monitoring, an expansion of IDaaS use cases.

A Context-based Approach to MFA Promises to Expand Usage

A zero-trust approach to access management requires initially and continually verifying identities. Friction in the end-user experience has, however, been an impediment to broader use of multi-factor authentication (MFA) to secure access to a range of cloud services and systems. In fact, only 41% of organizations employ MFA to secure access to cloud management consoles. Fortunately, the interest in an adaptive approach that triggers a secondary challenge based on detecting anomalous user activity promises to expand the use of MFA to a broader range of critical cloud resources.

» **Most common cloud-related cybersecurity incidents and attacks in last 12 months.**



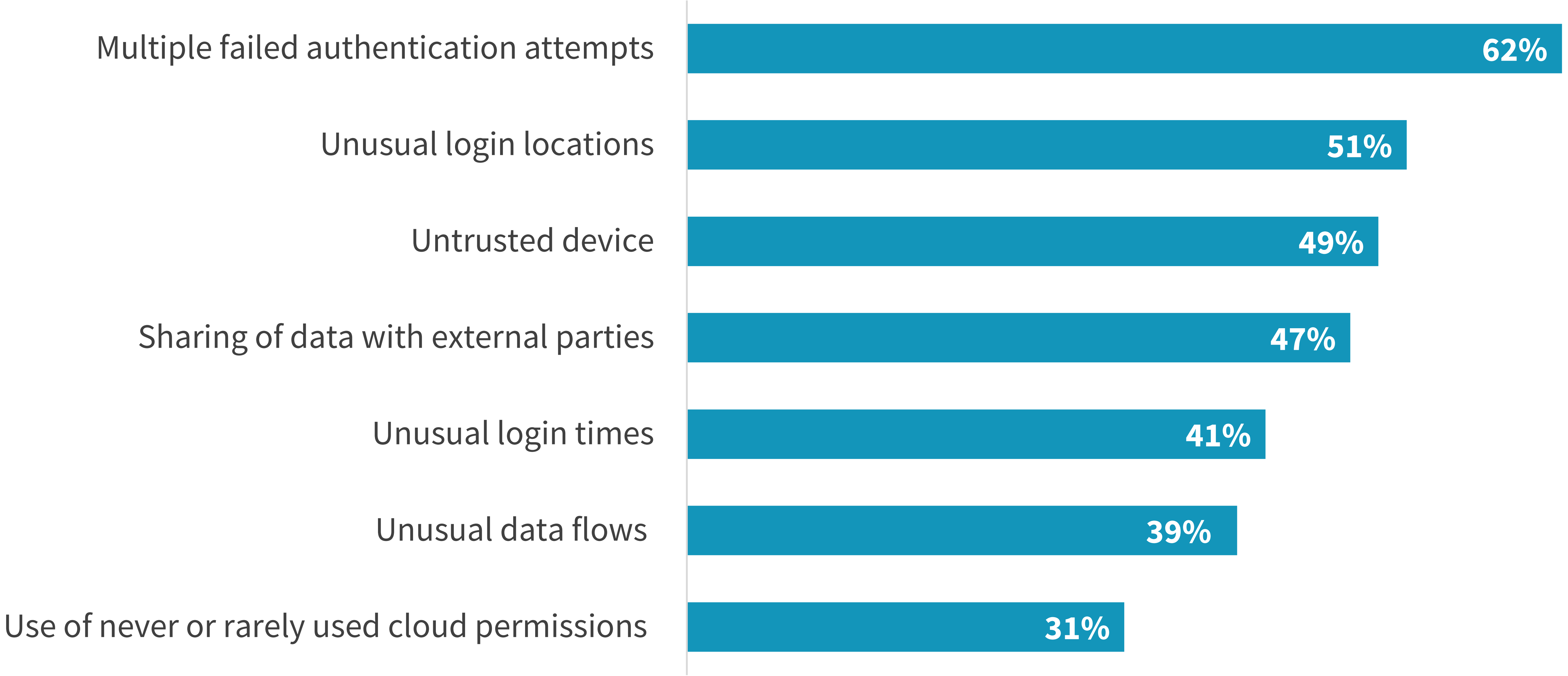
79%

are interested in an **anomaly, context-based approach to MFA.**

User Monitoring Focuses on Indicators of Account Takeover (ATO) Attacks

A problematic increase in account takeover (ATO) attacks via which credentials are stolen and then employed for a subsequent step in the kill chain (such as is the case in business email compromise (BEC) attacks) is driving the need to monitor user activity. Such indicators of an ATO attack that research respondents currently or plan to monitor for include multiple failed authentication attempts, which could be indicative of brute force credential stuffing, as well as unusual login locations, which could indicate the use of stolen credentials. Finally, the use of untrusted devices is also an important aspect of monitoring user activity.

» **User actions taken to monitor cloud applications for TDR purposes.**

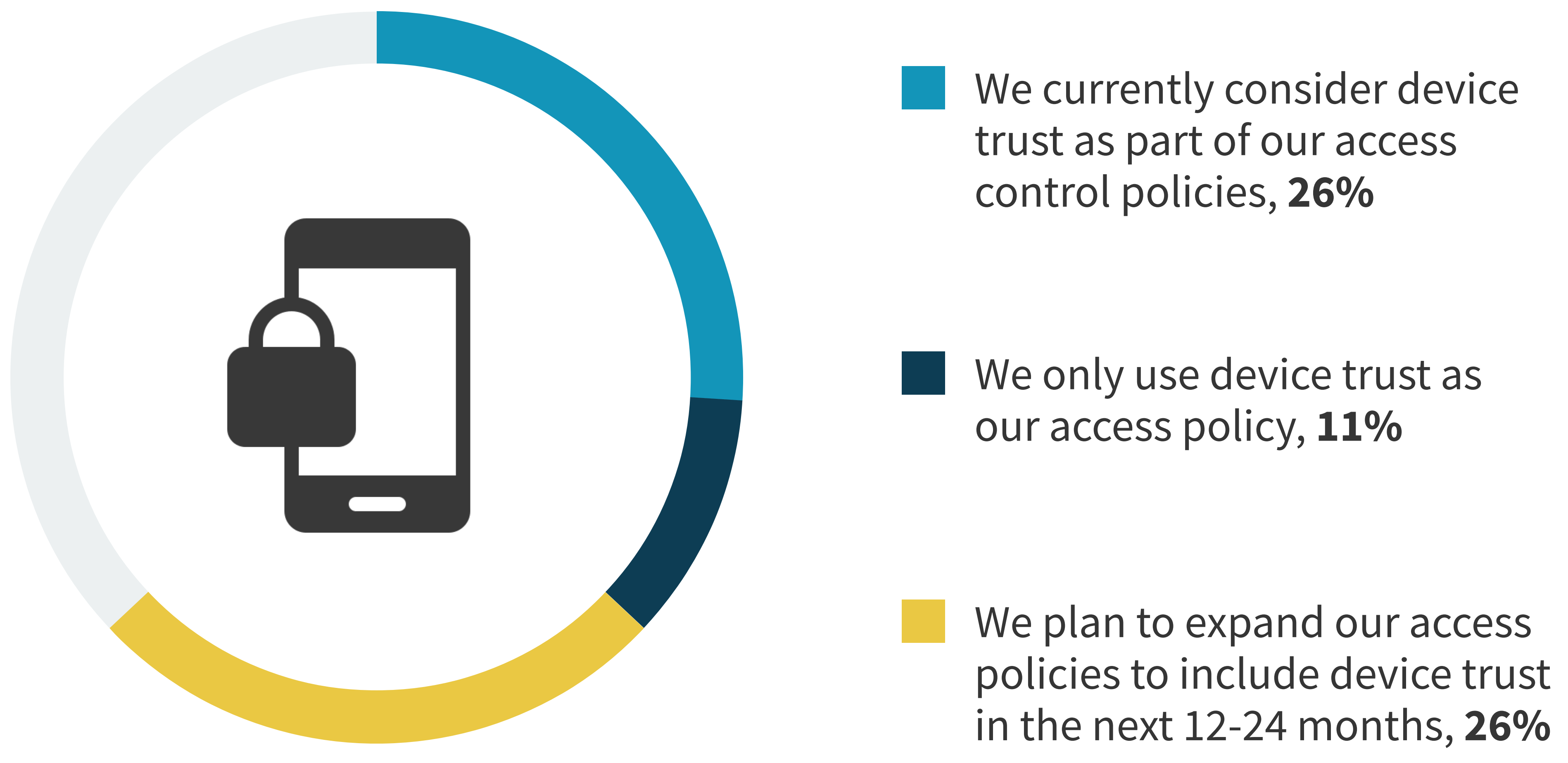


Back to Contents

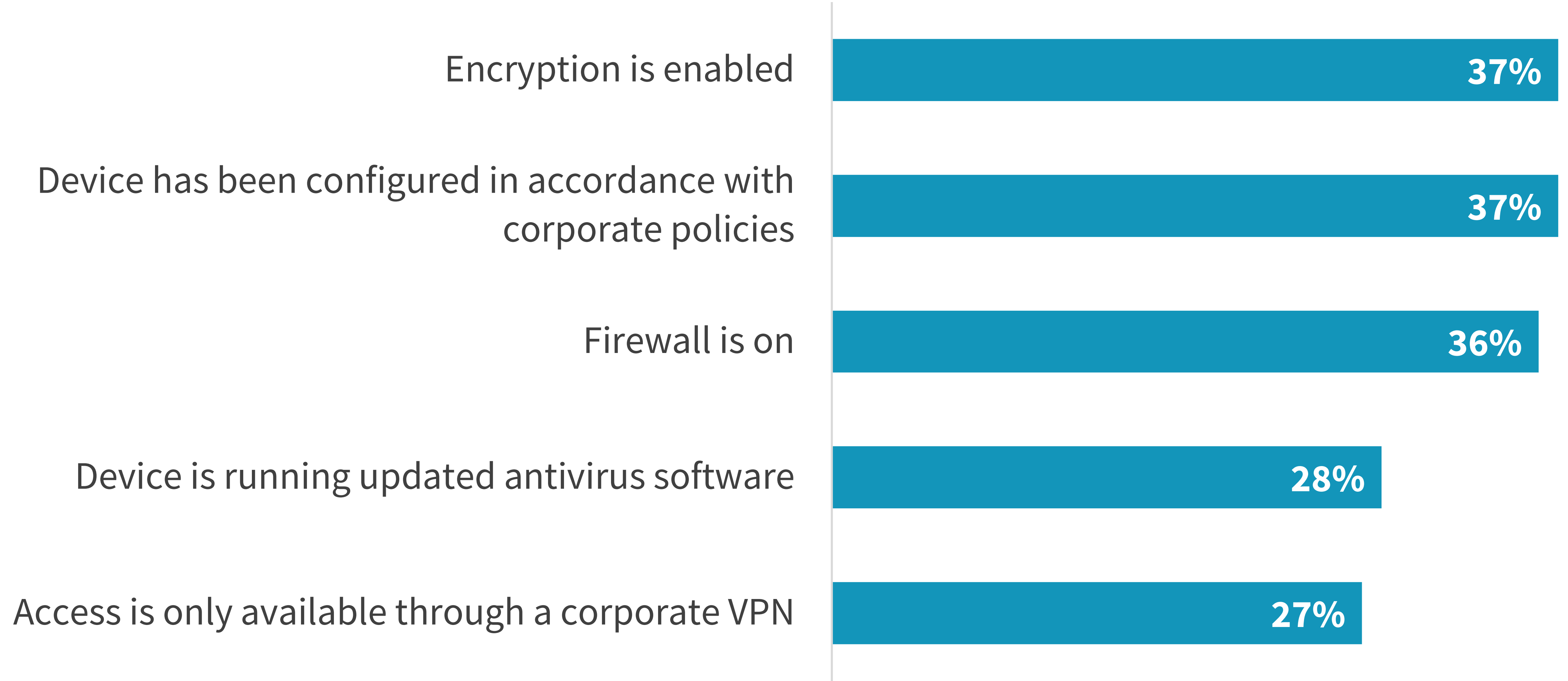
Device Posture Is an Important Aspect of Trust-based Authentication

The “don’t trust, continuously verify” approach of a zero-trust strategy necessitates the use of multiple factors to grant access to corporate resources, including the posture of the device used to access those resources. The increase in work-from-home mandates, which has resulted in the use of new and unmanaged devices by remote employees, has put additional focus on the need to consider the trustworthiness of devices in establishing identity. Many organizations are now planning to use device trust in their access policies with the proper configuration of devices being the attribute to verify device trust.

» Use of “device trust” for authentication.



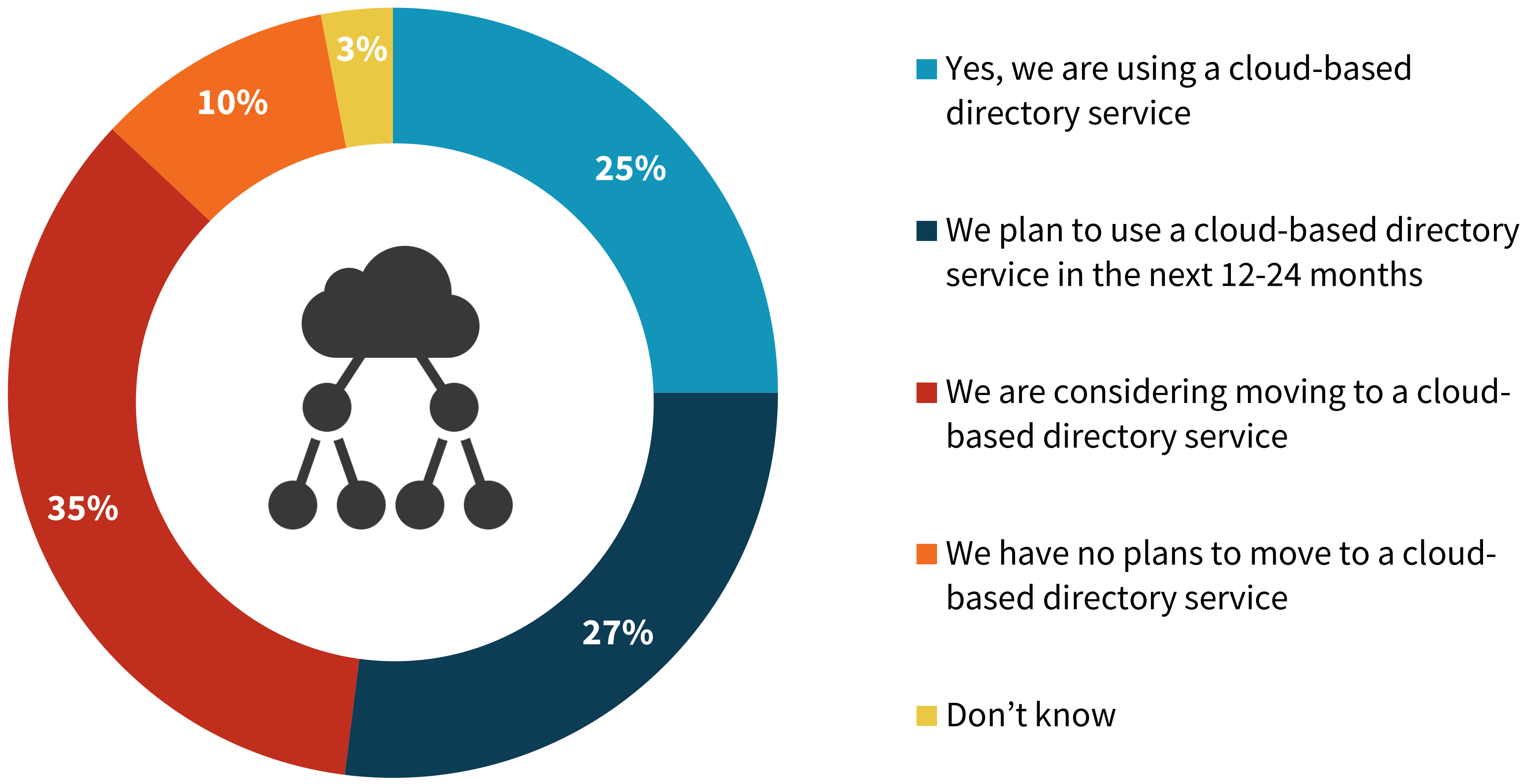
» Top attributes for establishing “device trust.”



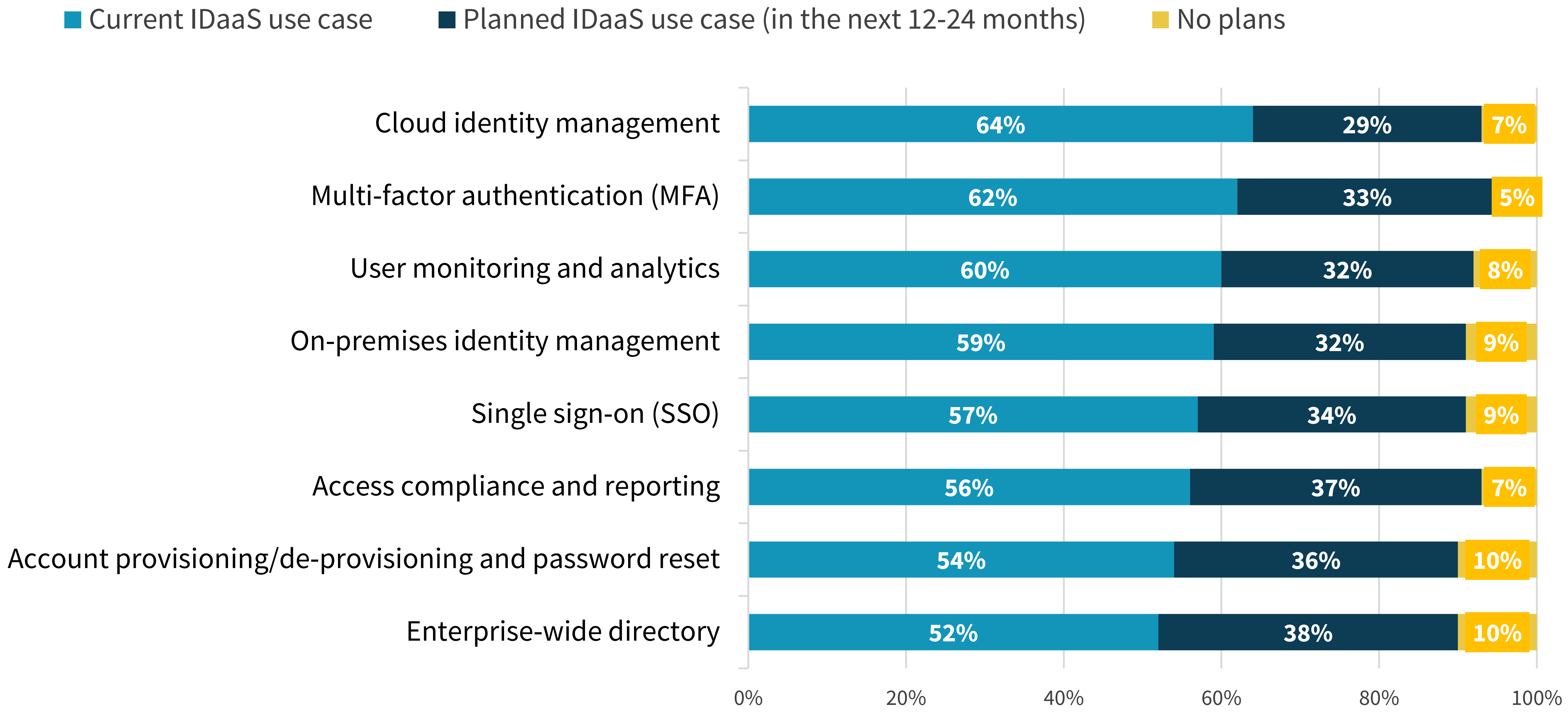
An Expansion of IDaaS Use Cases and a Shift to a Cloud-based Directory Highlights the Need for Cloud-ready IAM Controls

Plans to move to a cloud-based directory service are consistent with the adoption of other cloud-delivered security-as-a-service offerings driven by improved operational efficiency, a shift to OpEx economics, and the scale enabled by a cloud-native implementation. Consistent with the intent to employ a cloud-based directory service is a clear expansion of identity-as-a-service (IDaaS) use cases, including leveraging IDaaS to implement an enterprise-wide directory to unify access to cloud and on-premises applications.

» Plans for a cloud-based directory service.



» Use cases for identity-as-a-service.



JumpCloud®

JumpCloud has reimagined directory services to transform how IT delivers workers secure and easy access to technology. The rise of cloud, web apps, and remote work made it hard for IT to secure employees while supporting their need to work however and wherever they want: as a result IT teams have wrestled with an increasing number of identity, access, and device management products as they try to recreate what Active Directory achieved in an on-premise centric world. The JumpCloud Directory Platform gives IT and devops a modern solution to securely manage and connect users to IT resources regardless of platform, provider, protocol, or location. With JumpCloud, organizations increase employee productivity and protect identities, while enabling convenient connection.

Read this technical guide to learn how on-premises domain controllers increasingly expose organizations to risk, and get a strategy to implement modern, cloud-based infrastructure to manage and secure your environment.

LEARN MORE

About ESG

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

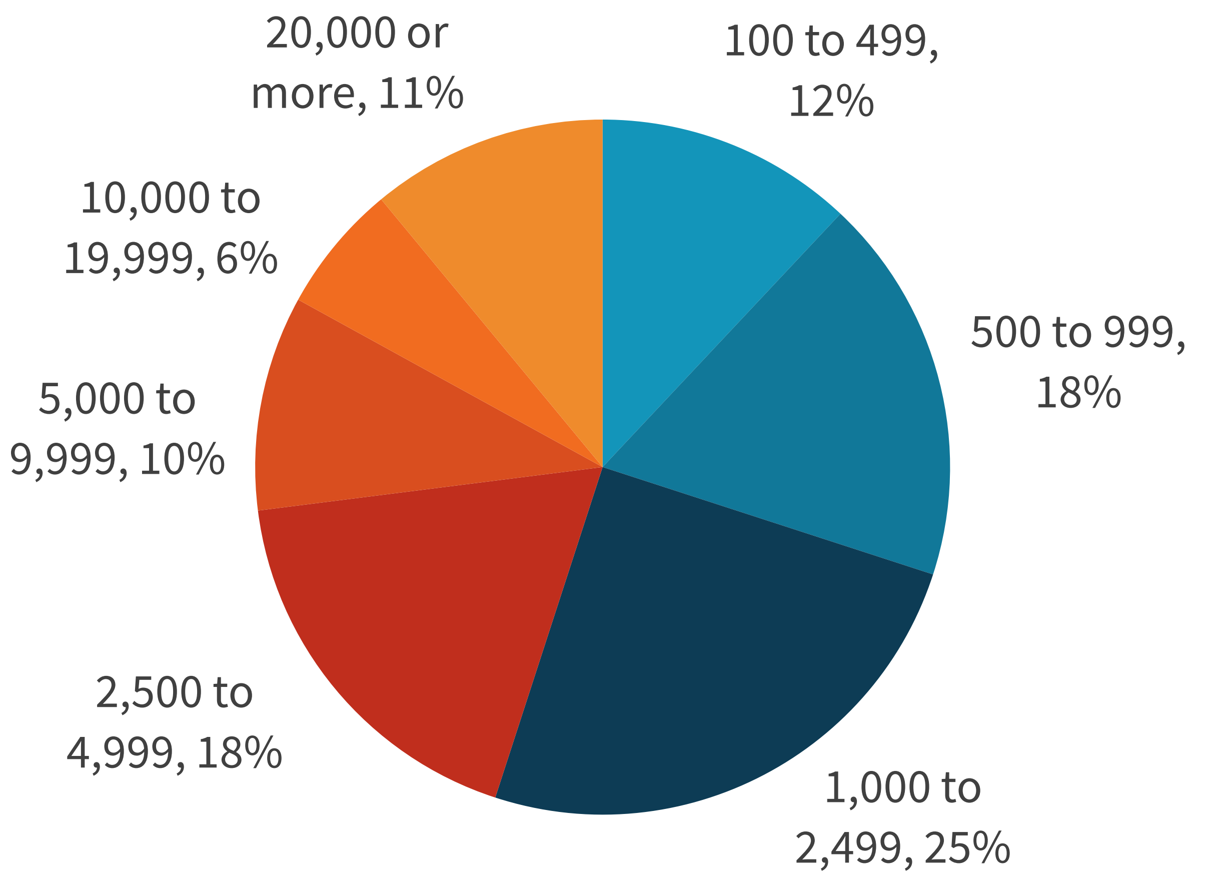
Back to Contents

Research Methodology

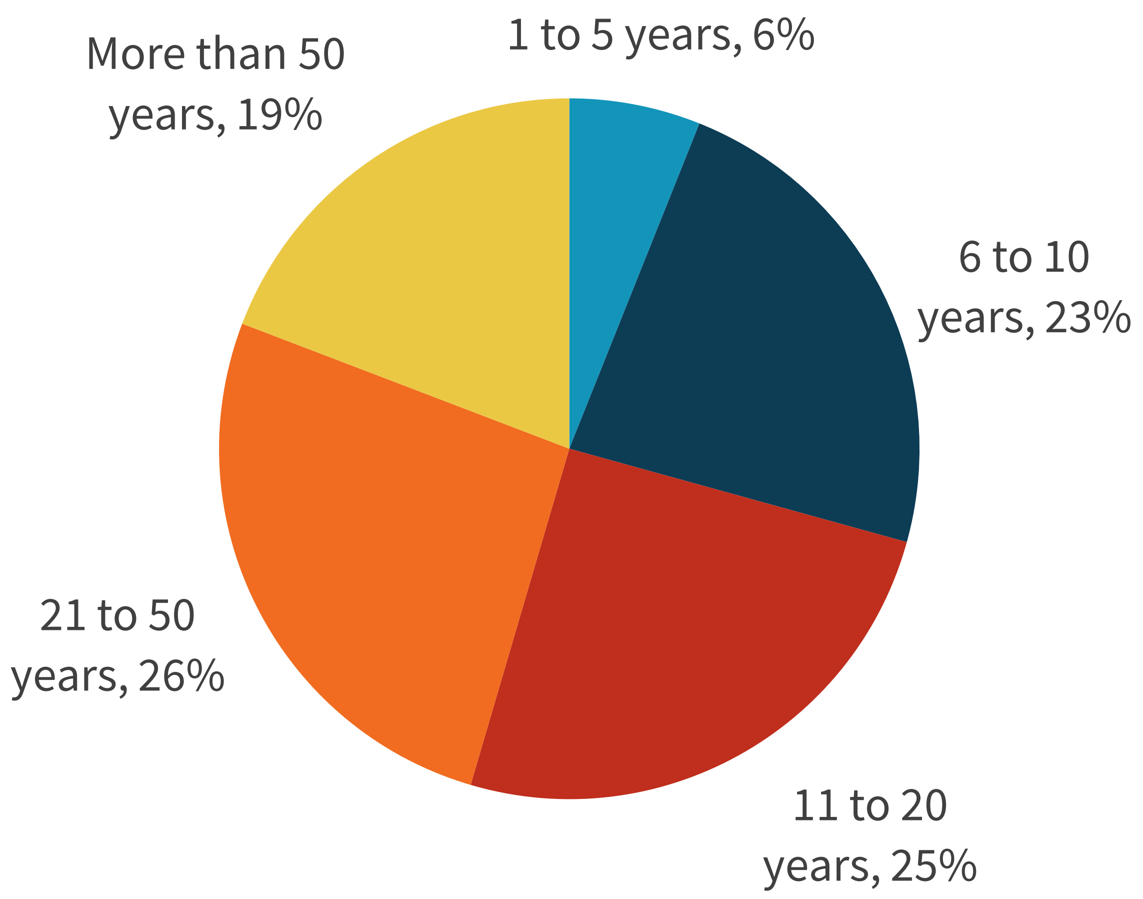
To gather data for this report, ESG conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America (United States and Canada) between July 31, 2020 and August 25, 2020. To qualify for this survey, respondents were required to be IT professionals personally responsible for evaluating or purchasing identity and access management and cloud security technology products and services. 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 379 IT and cybersecurity professionals.

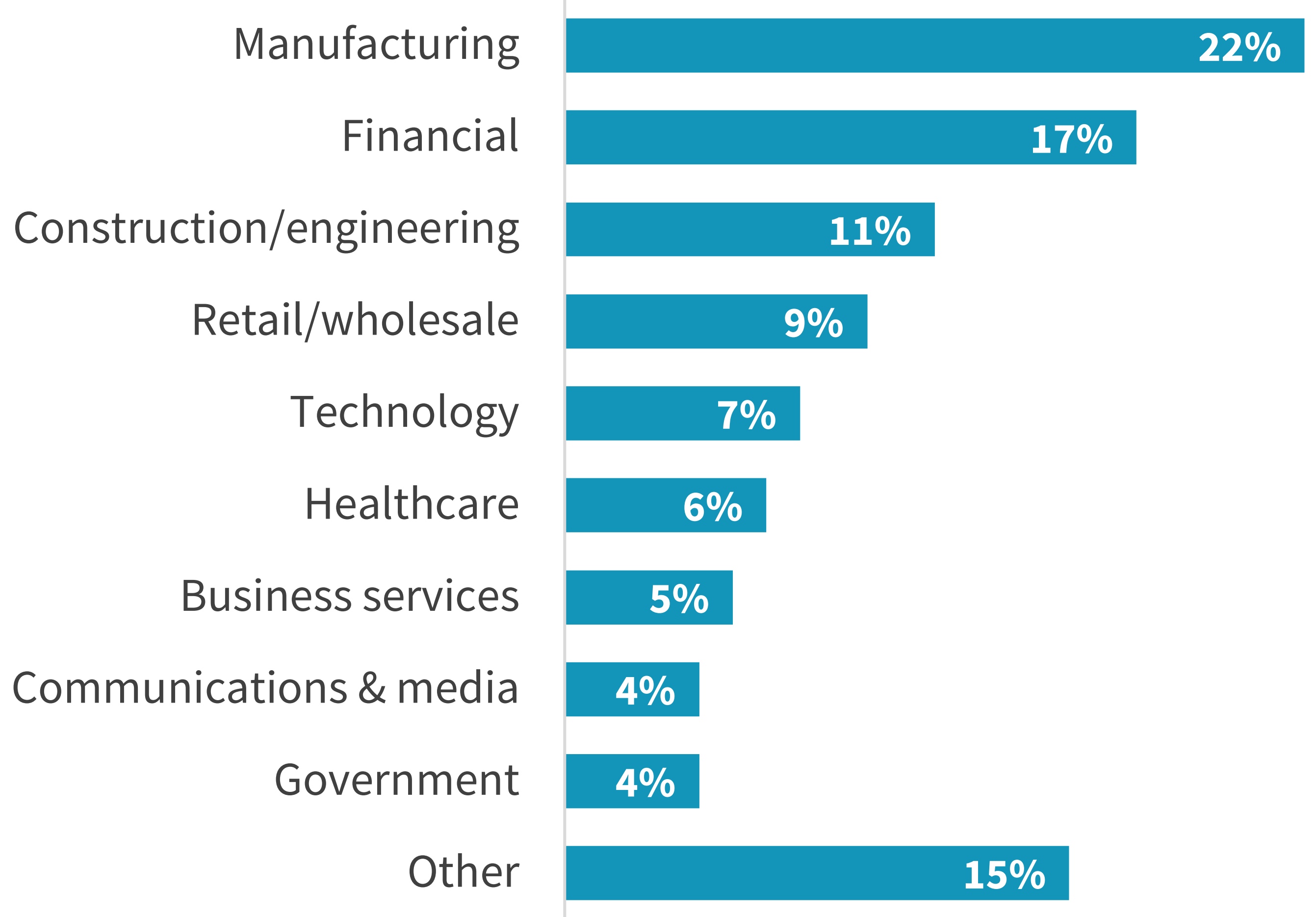
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY AGE OF COMPANY



RESPONDENTS BY INDUSTRY



Back to Contents

Version 2 二版
www.version-2.com
Hong Kong | Taiwan | Singapore | Macau | Mainland China

Hong Kong & Macau
Tel : (852) 2893 8860
Email : sales@version-2.com.hk

Taiwan
Tel : (886) 02 7722 6899
Email : sales@version-2.com.tw

Singapore, Malaysia & SEA
Tel : (65) 6296 4268
Email : sales@version-2.com.sg