Delinea

BENCHMARKING SECURITY GAPS & PRIVILEGED ACCESS

Global survey of cybersecurity leaders

WHITEPAPER

Executive Summary

Much has changed in the IT security industry this past year. Threats like data breaches and ransomware are increasing, organizations are facing unprecedented employee turnover, and work is commonly hybrid or remote. IT security leaders have escalating challenges and not enough time or resources to address them.

Given that numerous studies have found credentials are the most common attack vector, we wanted to know what IT security leaders are doing to reduce the risk of an attack. Specifically, we set out to learn as much as possible about organizations' adoption of Privileged Access Management (PAM) as a security strategy. We explored questions such as: How are they confirming identities and leveraging access controls? How are they forcing attackers to take more risks and catch them in the act? And, how well are those strategies embedded in their organization?

Our intent was not only to understand which PAM capabilities organizations adopt, but also how people close to the process feel about their progress, what obstacles stand in their way, and what they expect for the future.

Who we asked

More than 2,000 IT security leaders around the world shared their insights to create this report. The broad reach of this study provides an opportunity to compare the PAM-related activities and attitudes of IT security practitioners with varying levels of responsibility, in different countries, industries, and companies of all sizes.

What we learned

The results of the research show vast differences between where people want to be in their security journey and where they actually are.

This report explores three key findings:

1. **Despite good intentions, over 60% of companies have a long way to go to protect privileged identities and access.**
2. **Human accounts are getting security attention, while machine identities are vulnerable.**
3. **Plans for next year focus on incremental security controls, but are missing the big picture to drive real change.**

Research reveals differences among key groups

Job level

IT security leadership and rank-and-file practitioners report conflicting perceptions and priorities, which may be blocking security initiatives from being successful.

Company size and industry

While you might suspect that larger enterprises would be better prepared than smaller businesses, or that certain industries would be more mature than others, the findings of this study indicate that isn't the case. Neither company size nor industry variables impacted the results in terms of PAM best practices and cyber preparedness.

Geography

The research exposes a gap between countries which have adopted PAM best practices and those which haven't, with organizations in the Middle East and Africa less prepared for privilege-based cyberattacks. This gap reflects what Wendy Nather, Head of Advisory CISOs at Cisco, referred to at RSA as "the security poverty line."

How to use this report

The findings of this report give you a benchmark for your own security journey.

In addition, expert insights help you put the findings into context. They shed light on where you should be spending your time and give you a head start on planning your next moves.

Before we dive into the key takeaways, let's set some context. Consider the mindset and perspective of the survey respondents.

Eighty-four percent of them experienced an identity-related breach or an attack using stolen credentials in the previous year and a half.

The impact of these breaches varied, with the loss of sensitive data the most frequently cited.

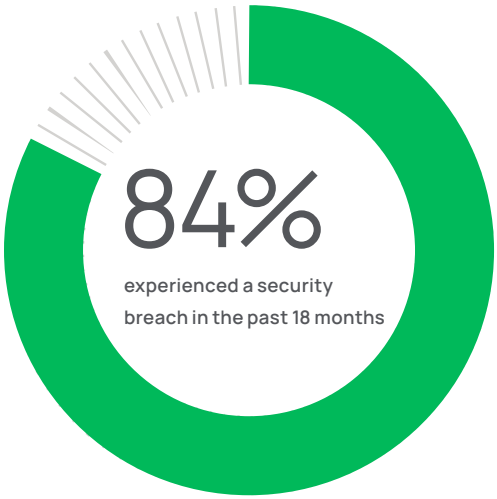
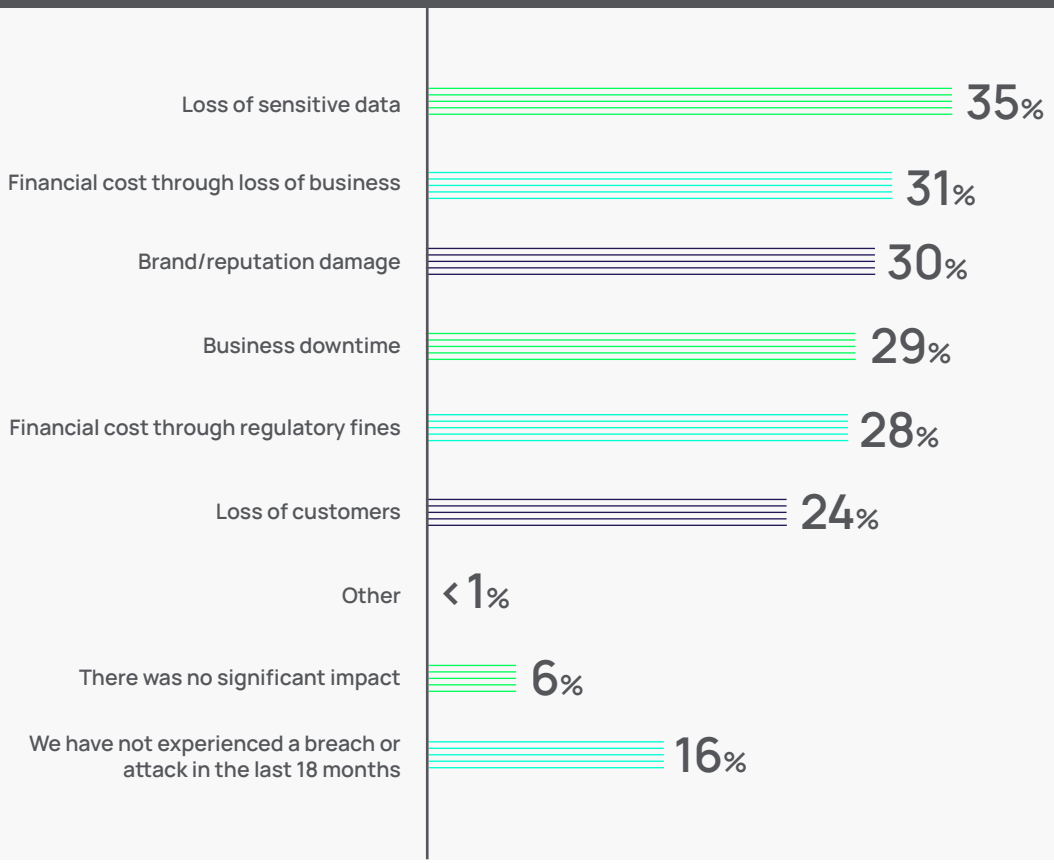


FIGURE 1 | If your organization has experienced an identity-related breach or an attack using stolen credentials in the last 18 months, what was the most significant impact of this breach?



The responsibility to make sure next year is better than last rests on the shoulders of the people who answered this survey. So, let's find out what they said...

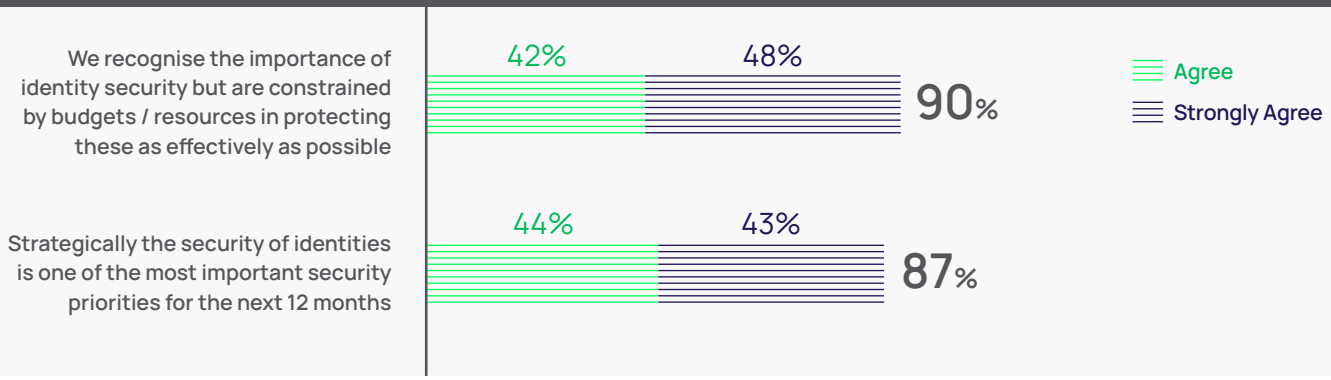
KEY TAKEAWAY 1

Despite good intentions, over 60% of companies have a long way to go to protect privileged identities and access

Most organizations recognize that protecting privileges and identities is a top priority to reduce risk.

Ninety percent of respondents agree that identity security is important to meeting business goals. Eighty-seven percent agree that securing identities is a top priority for the next 12 months.

FIGURE 2 | To what extent do you agree with the following?

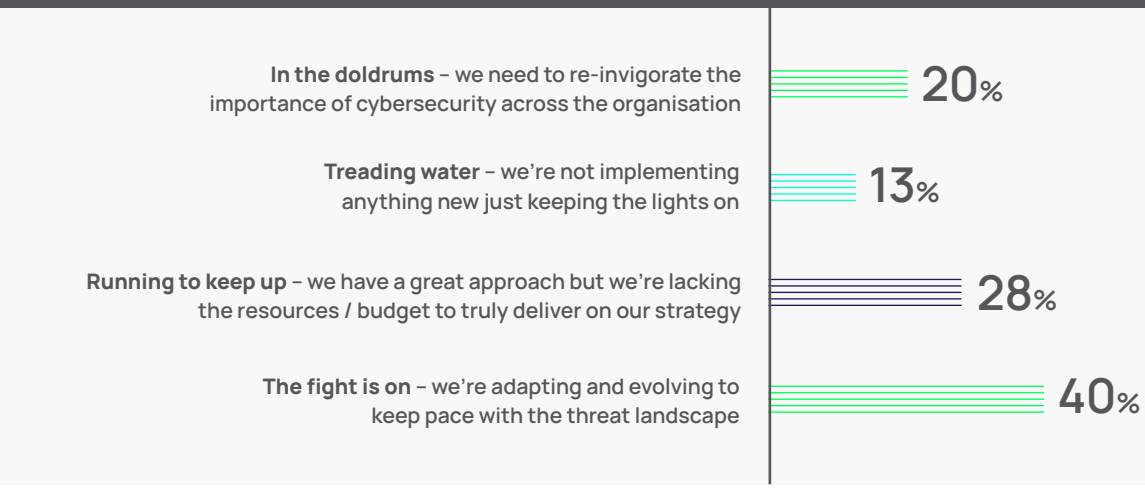


This high level of awareness among IT and security professionals is likely due to the attention Garter Research and other analysts and influencers have given to privilege and identity security in the past few years. For example, Gartner included PAM as a top security project in 2018 and 2019 for security leaders to implement. In 2022, Gartner recognized Identity System Defense as #2 among seven security priorities, highlighting the importance of securing credentials and privileged access.

Unfortunately, while most organizations talk the talk, they aren't walking the walk.

Only 40% of respondents say their security strategy is keeping pace with the threat landscape. The bulk are falling behind, treading water, or running to keep up.

FIGURE 3 | Which of the following best describes your overall security strategy right now?

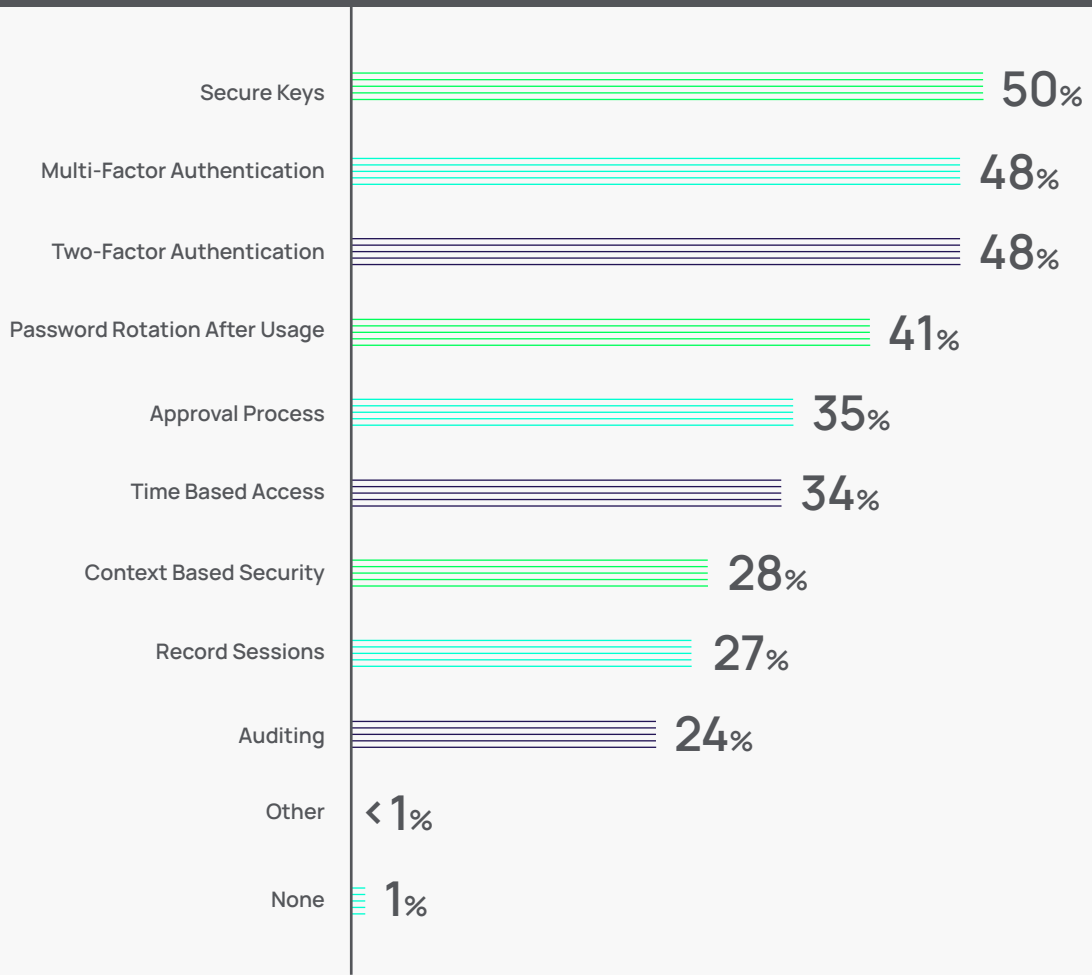


Delinea

Most haven't adopted best practices and solutions in their PAM journey.

More than half of organizations surveyed haven't implemented ongoing security policies and processes for access management, such as MFA, password rotation or approvals, time-based or context-based access, or privileged behavior monitoring such as recording and auditing.

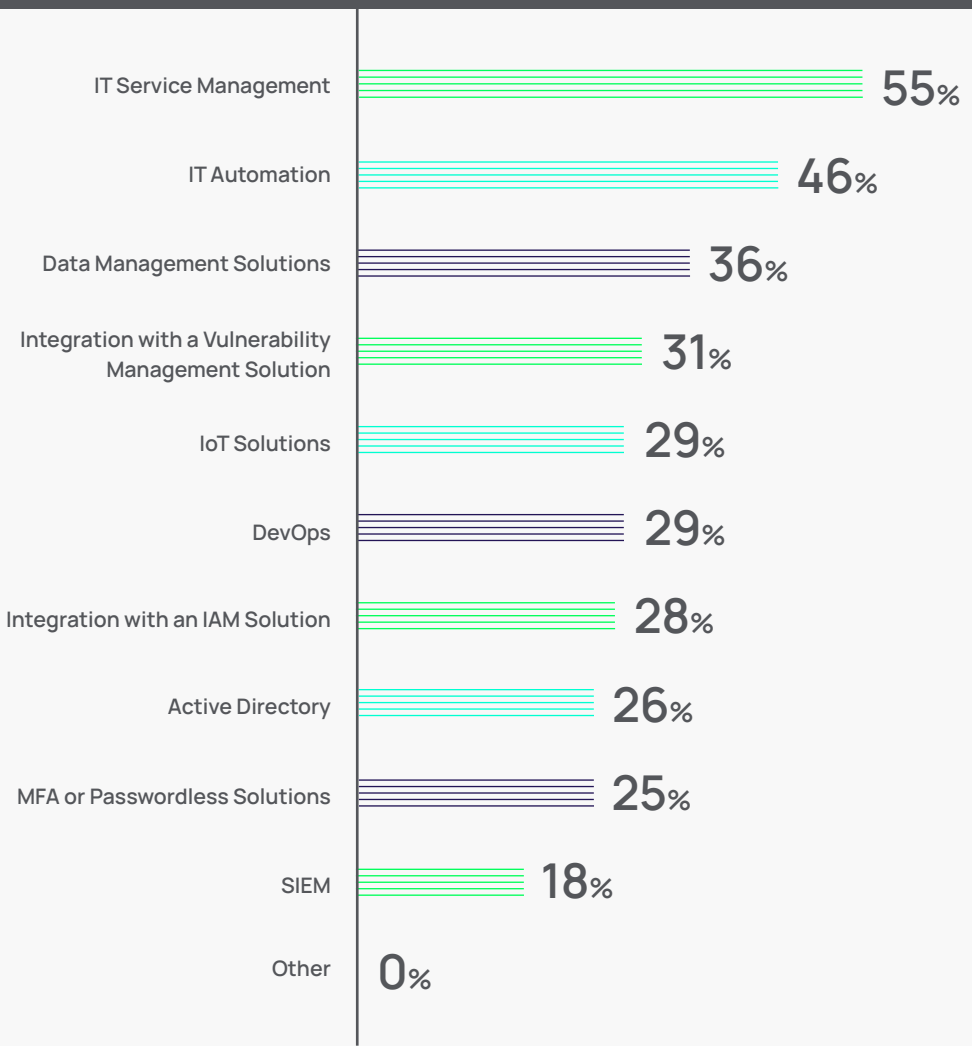
FIGURE 4 | What types of security controls are in place to protect privileged access?



At most organizations, PAM practices aren't bolstered by supporting tools or embedded into everyday workflows.

Shockingly, only 28% have integrated PAM with Identity Access Management (IAM) solutions. Integration between IAM and PAM ensures that appropriate access controls are in place for privileged identities, including segregation between authentication and authorization, which makes it more difficult for attackers to abuse users' privileges. Rarely are PAM practices connected to Active Directory and Security Information and Event Management (SIEM).

FIGURE 5 | What types of integrations have you done with Privileged Access Management?



Based on these findings, there is a high likelihood that more organizations will become cyber victims, until security gets the investment and prioritization required to reduce the risks. It's only a matter of time before attackers steal privileges and bring an organization to its knees.

Why it matters

On the surface, these results are concerning. But, in fact, they indicate an increase in organizations' PAM capabilities compared to previous research. A few years ago, Thycotic (now Delinea) found that **86% of organizations struggled to implement even basic PAM security controls**.

The good news is organizations are heading in the right direction. They've begun their journey and have the fundamentals in place. We now need to ask: Will they be able to implement PAM security fast enough to prevent, detect, and defend against a cyberattack?

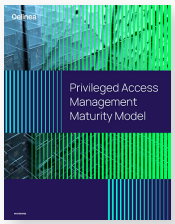
Cyber criminals look for the weakest link. They'll avoid companies with defenses that cause them to risk exposing themselves. With plenty of other fish in the sea, you don't need to be the one that gets caught.

Recommendations

If these results are hitting a little too close to home, it's time to get started strengthening your privilege security and access management.

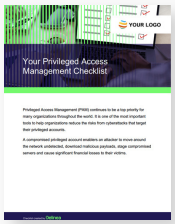
To embed PAM into your organization's security culture, integrate security best practices into workflow and communications systems users rely on every day (e.g. help desk ticketing, account provisioning and deprovisioning, incident and disaster response) to reduce friction and improve adoption.

Resources



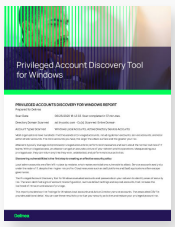
Benchmark your PAM maturity.

Find out which phase of PAM maturity you're in — Starting Point, Foundational, Advanced or Expert — with the Delinea PAM Maturity Model.



See which PAM best practices you have in place and which ones you still need to master.

Prepare your plan with the Delinea Privileged Access Management checklist.



Identify areas of privilege security risk.

The Delinea Privileged Account Discovery Tool for Windows evaluates privileged accounts and passwords on your network. The scan identifies signs of account misconfiguration, such as default settings and expired accounts, that increase the likelihood of intrusion and abuse of privileged accounts.

KEY TAKEAWAY 2

Human accounts get the security attention, while machine identities are vulnerable

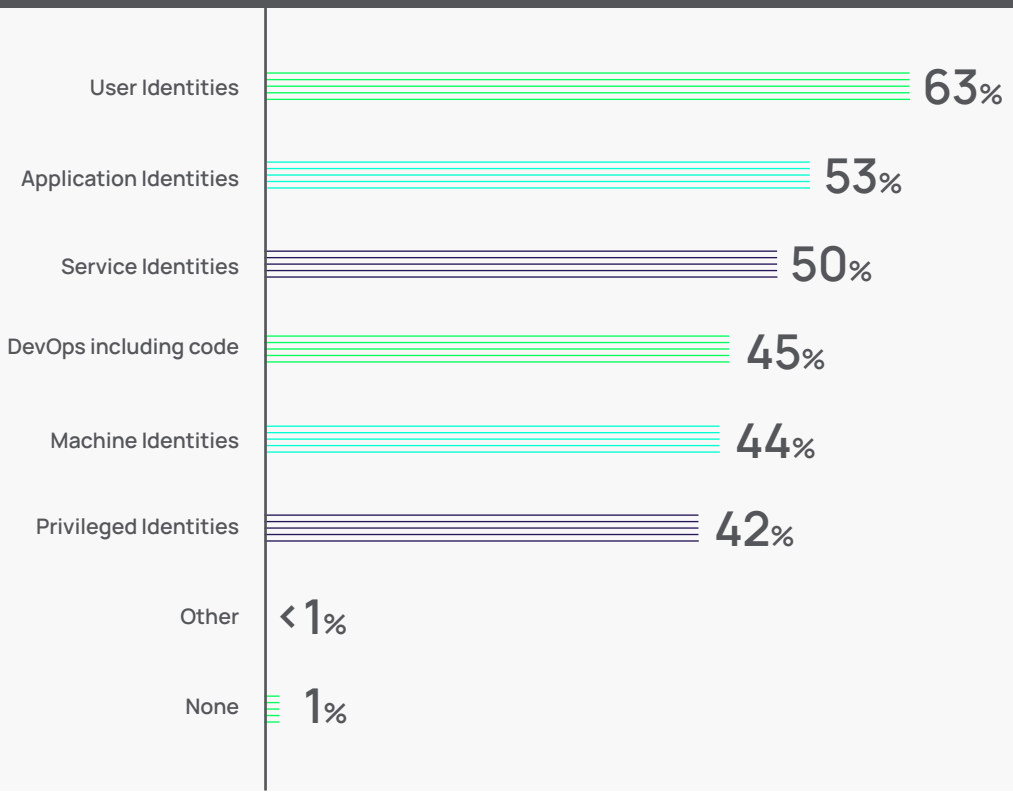
Privileged identities include humans, such as domain and local administrators, as well as non-humans, such as service accounts, application accounts, code, and other types of machine identities that connect and share privileged information automatically. Cyber criminals can leverage all types of accounts to gain initial access and elevate privileges.

The research found that most organizations implementing privileged access security measures have prioritized the human side. In fact, 63% of organizations have deployed privileged access security measures for user identities.

Among the types of human accounts most protected by these measures are IT admins and security teams, followed by developers. Typically, these types of accounts involve people logging onto web applications, databases, and other infrastructure for configuration, troubleshooting, and hands-on operational support.

However, organizations have been slower to protect non-human privileged identities, leaving them exposed and vulnerable to attack. Just about half are protecting application and service identities, and less than half include DevOps and machine identities in their PAM strategy.

FIGURE 6 | To what type of identities have you deployed privileged access security measures?



Why it matters

Most organizations have hundreds, if not thousands, of privileged accounts. The more privileged accounts, identities, passwords, and credentials you have, the larger your attack surface and the greater your risk. Yet, most organizations are only protecting and managing a small portion.

Many wrongly assume that Active Directory is the source of truth for the number of privileged accounts. The reality is, many privileges are outside of Active Directory, such as those in code, cloud platforms, SaaS applications, and Unix or Linux-based systems.

The lack of attention to machine-based identities is particularly concerning for two reasons: They're growing at a faster pace than human identities and they pose greater risk if compromised.

Machine identities and application-based privileges tend to go unmanaged, unprotected, and unchanged. These privileges are commonly misconfigured from the start, and it's easy to lose track of privileged accounts that aren't tied to humans.

When attackers target user privileges, they tend to create more noise and are more likely to be detected. However, when they attack machine and application identities they can easily hide, moving around the network and enumerating sensitive systems to determine the best place to strike and cause the most damage. Non-human accounts are the easiest entry points for an attacker to maintain persistent access without the worry that someone will rotate their password.

Recommendations

It's not enough to protect only a few privileged accounts and leave the others open to attack. Attackers only need to be successful at finding one unprotected account to carry out malicious activity.

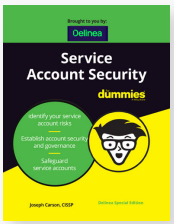
Instead of restricting the definition of "privileged user" to domain administrators and other IT superusers, consider all types of users and systems with access to any type of sensitive or critical data. They must all be prevented from being "over privileged," or granted too much access for too long.

If you're among the organizations rapidly adding machine identities to support digital transformation, cloud migrations, and rapid development cycles, make sure you include them in your PAM strategy.

Keep in mind, not all privileges are equal in the risks they pose to the organization. Prioritize privileges that, if compromised, risk bringing the business to a complete halt. Secure them first.

A risk-based approach allows you to make an impact right away. Based on their level of risk, each type of account may require a different level of protection. For example, some privileges may require additional layers of approval before being granted, or continuous monitoring to make sure behavior is as expected. From there, you can add additional layers of security or types of privileged identities to your PAM strategy in phases.

Resources



Learn about service account governance.

Get control of service account sprawl and develop a strategy to protect service account access properly with Service Account Security for Dummies.

Measure the state of privileged access entitlements in your service accounts.

Run a free service account discovery to expose areas of the highest risk.

KEY TAKEAWAY 3

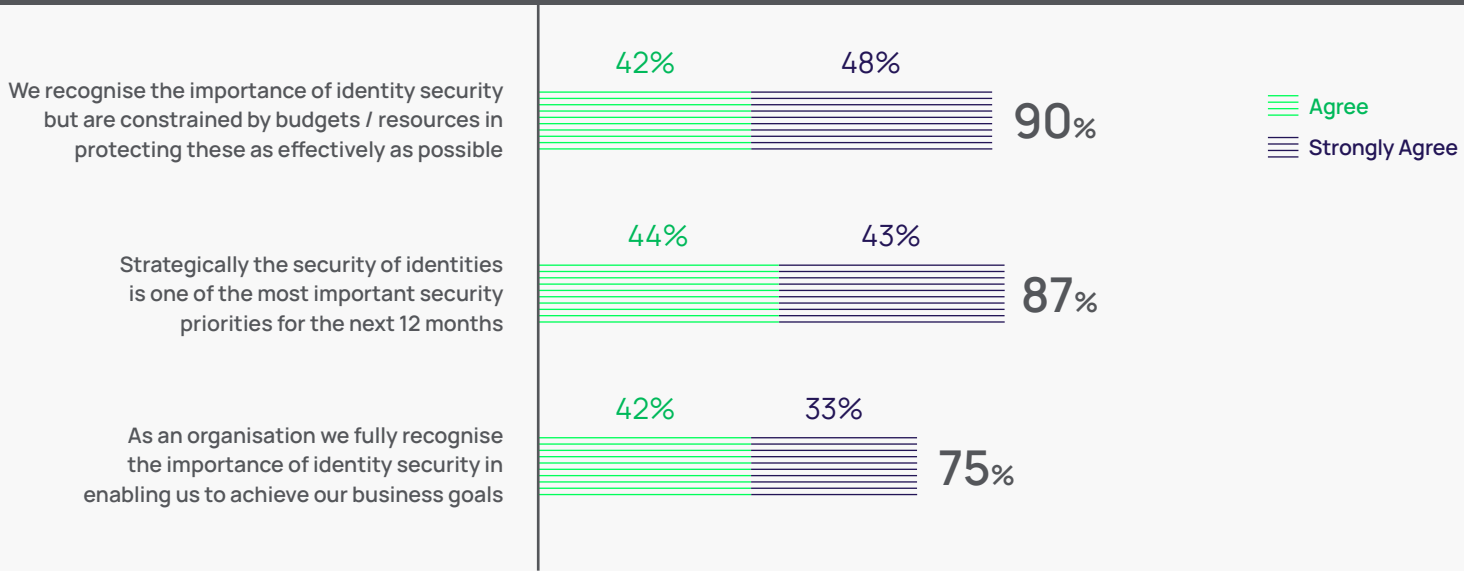
Plans focus on incremental security controls, but miss the big picture to drive real change

Let's start with the good news.

Organizations are looking ahead and making plans to invest in additional measures to improve security.

Almost 90% recognize the importance of identity security as a top priority to help achieve business goals, and 87% plan to act to secure privileged identities within the next 12 months.

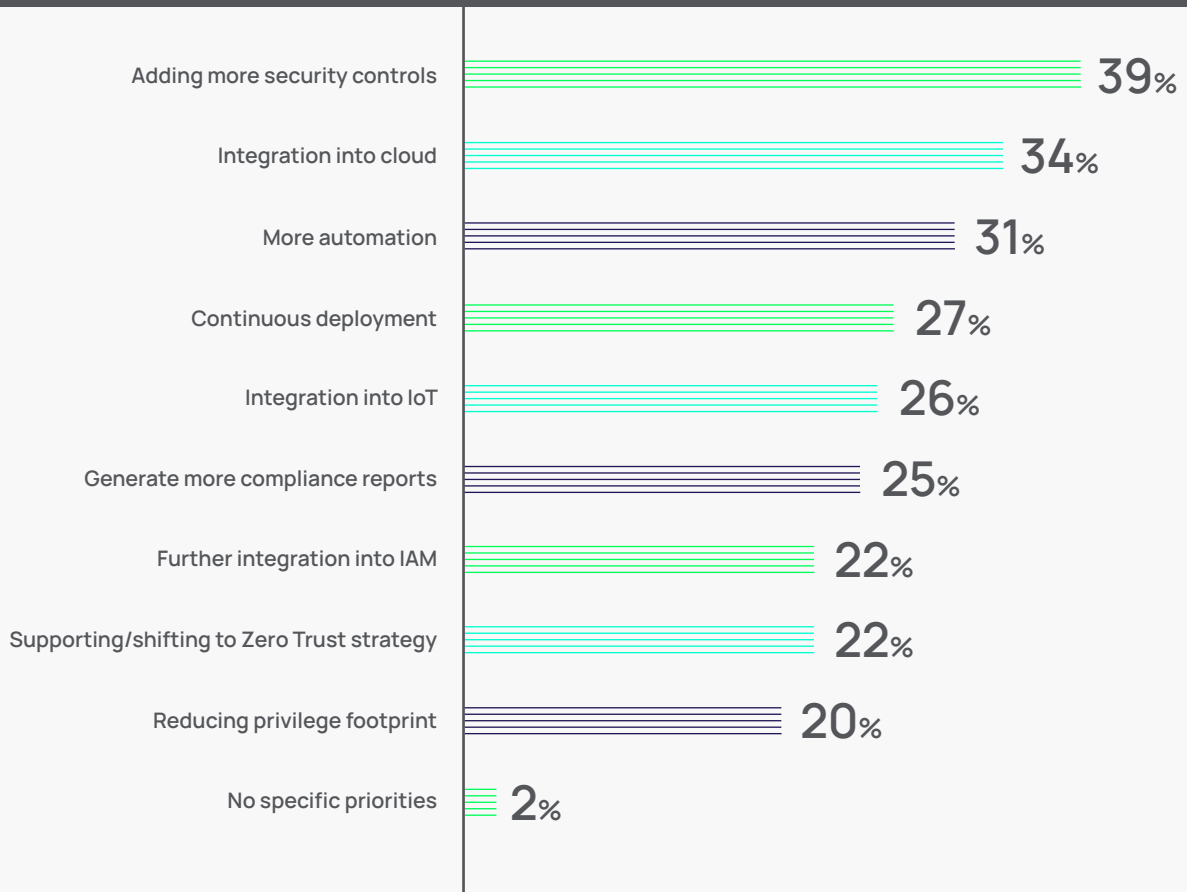
FIGURE 7 | To what extent do you agree with the following?



In fact, the survey respondents say their top priority in the next year is to add more security controls to protect privileges.

Organizations have specific security measures and PAM capabilities they intend to implement. Top priorities include adding more security controls (39%), cloud integration (34%) and more automation (31%).

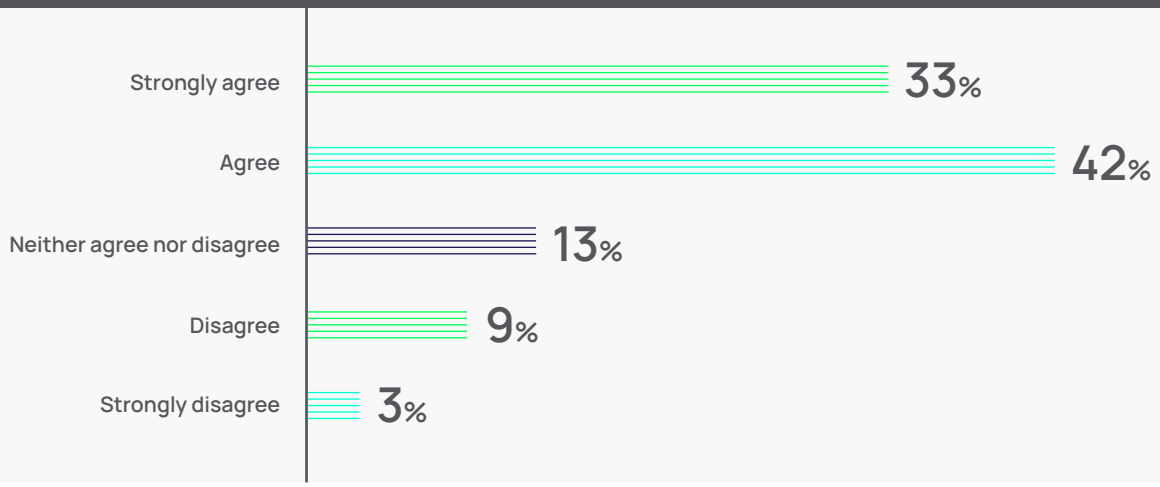
FIGURE 8 | What are your priorities over the next 12-18 months in relation to privileged access security to protect identities?



Now, the bad news.

75% of organizations believe they will fall short of protecting privileged identities because they won't get the support they need.

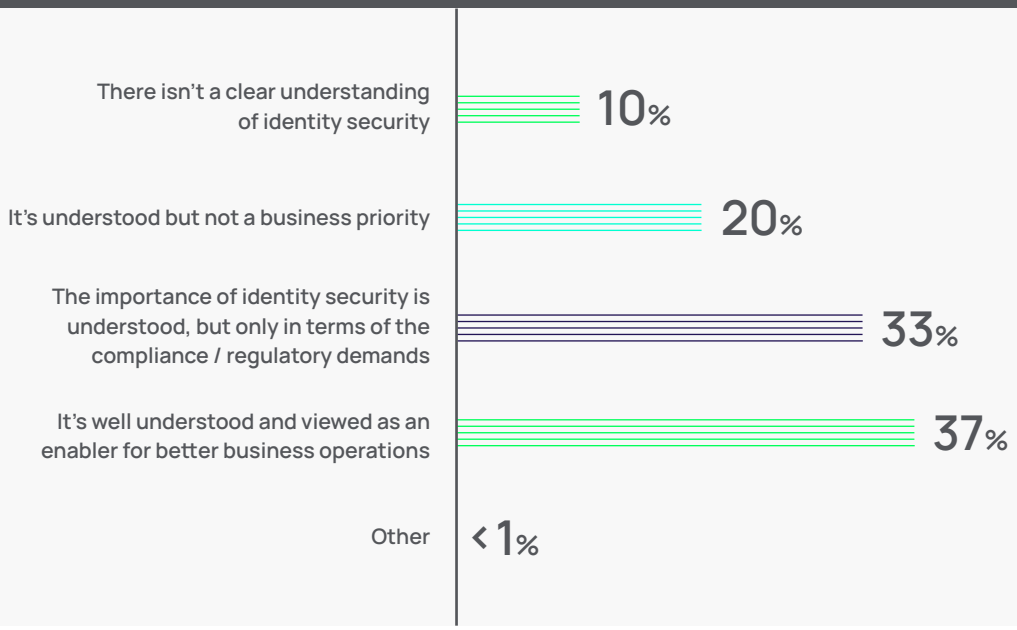
FIGURE 9 | To what extent do you agree with the following? We recognize the importance of identity security but are constrained by budgets / resources in protecting these as effectively as possible.



Why? It comes down to budget and executive alignment.

Only 37% say that identity security is well understood by their company's board, and viewed as an enabler for better business operations.

FIGURE 10 | Thinking about the Board / C-Suite's awareness of identity security across the organization, which of the following best describes their understanding of its importance?



Why it matters

Incremental security changes can only move the needle so much to reduce cyber risk. Privilege access security must be a company-wide endeavor that's embedded in all areas of the business.

When leadership doesn't understand the likelihood or business impact of a cyberattack, they tend to consider security a check-the-box activity for compliance, and they're less apt to invest in layered defenses.

Recommendations/next steps

If more executive boards understood the business value of PAM, they would be more likely to provide the needed support and budget.

To obtain budget and resources and gain PAM adoption, it's essential to get executive buy-in. While compliance and regulatory requirements may get the board's attention, IT and security leaders must also show them that PAM isn't simply a check-the-box exercise.

Explain additional benefits in terms of business value, for example:

- Increasing productivity for IT and business users
- Meeting cyber insurance requirements and lowering premiums
- Building trust with customers and partners

Resources

Get practical recommendations from IT security pros

Cyberedge's Cyberthreat Defense Report explores what enterprise IT security pros around the world are thinking and doing to reduce risk.

See how to get started with Privileged Access Management

The Privileged Access Management for Dummies eBook gives you, your IT staff, and business stakeholders a practical understanding of Privileged Access Management and its security implications.

Conclusion

While organizations have made progress toward a more secure future, they have a long way to go. Ad-hoc, incremental changes aren't going to get the job done. In fact, they can give you a false sense of security and leave you with a lot of technical debt you'll need to unravel.

You can't protect what you don't know. In addition to privileges for domain admins, make sure you understand the security risk and plan to manage privileges for service accounts, applications, and other types of machine identities.

No organization is the same. Every path to PAM maturity is different. Determine which aspects of cybersecurity you can tackle now, and make sure you plan ahead. Even if you only have the resources or budget to afford limited protections today, start with the basics and make sure you choose a solution that grows with you. Get the right system in place to gather data and insights so you can understand where to prioritize your efforts and have the most impact on reducing your risk.

Methodology

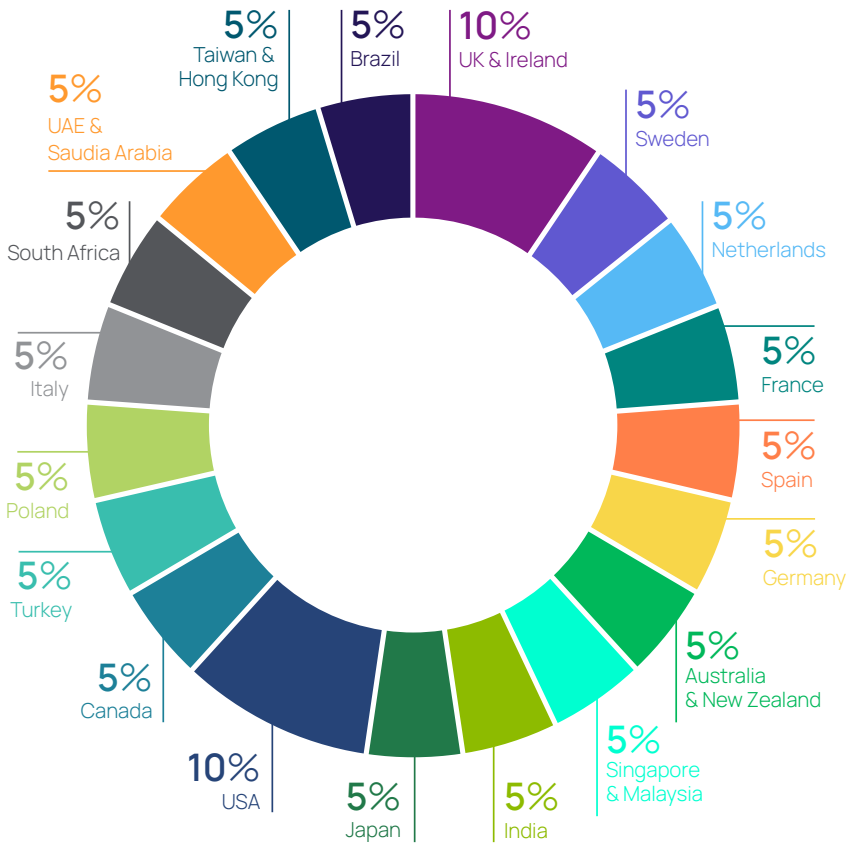
The results from this survey are from an online survey Sapio Research fielded on behalf of Delinea during June 2022.

At an overall level results are accurate to ± 2.1% at 95% confidence limits assuming a result of 50%.

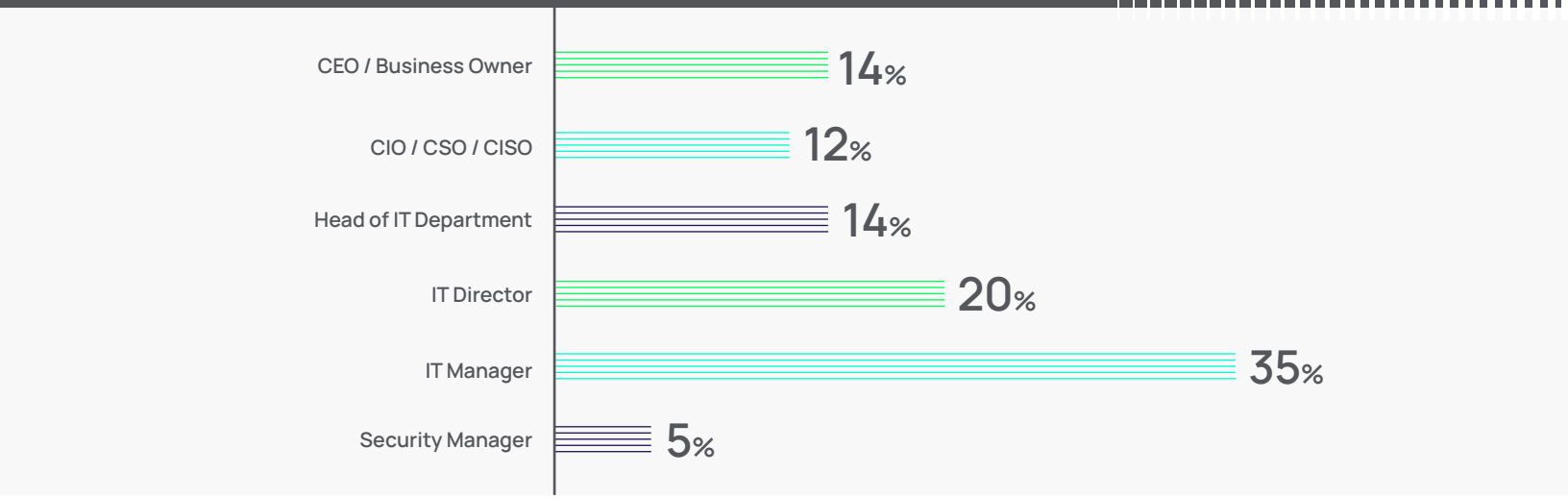
Sapio Research is a London-based B2B and consumer market research agency with an experienced team of researchers offering qualitative and quantitative research services and tools to help clients gain deeper insights. https://sapioresearch.com/

2,100 IT and security professionals in 23 countries responded representing a cross-section of decision makers.

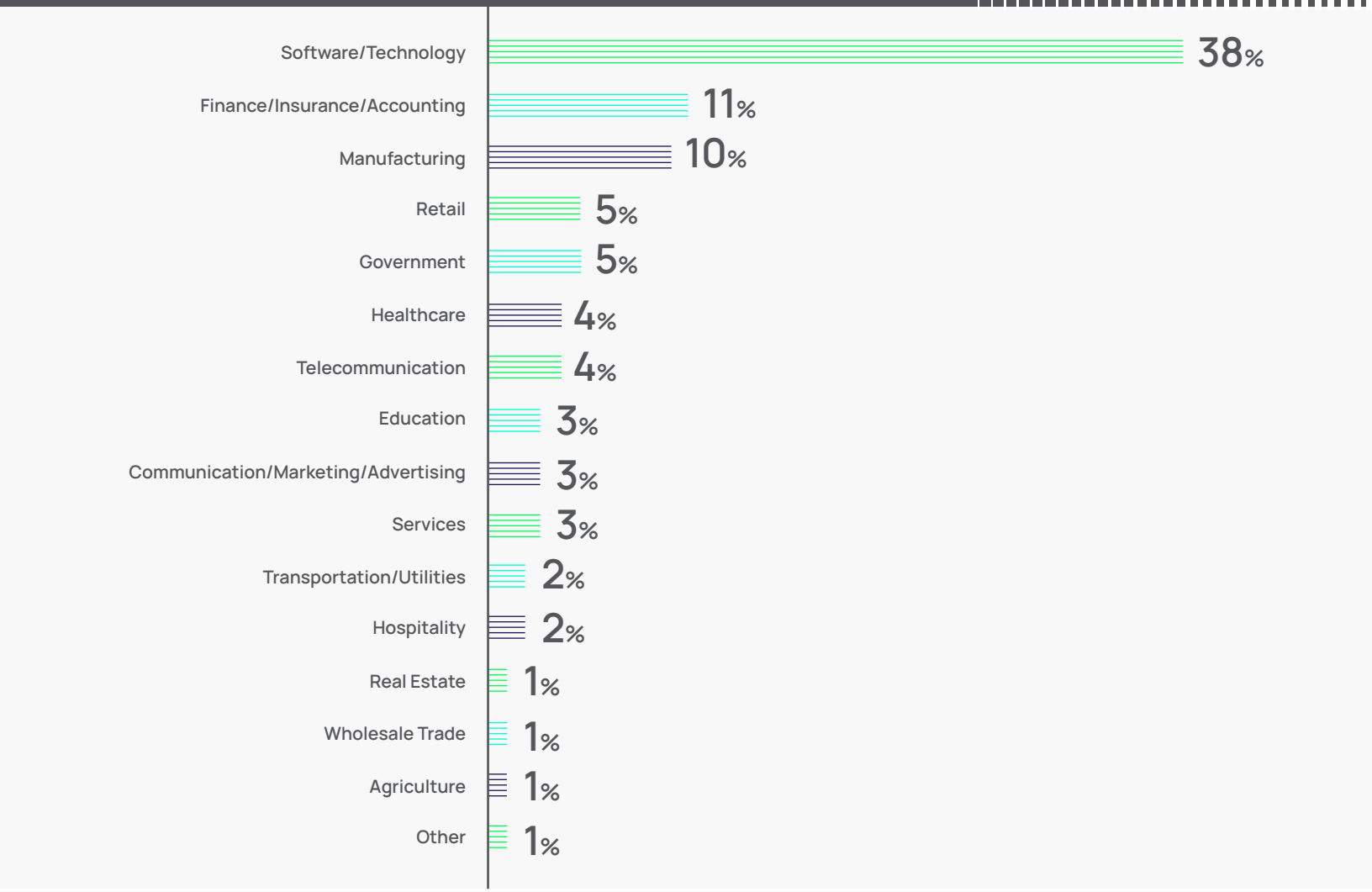
Where are you based?



Which of the following best describes your job role?



Which of the following most closely describes your industry?



Delinea

Defining the boundaries of access

Delinea is a leading provider of Privileged Access Management (PAM) solutions for the modern, hybrid enterprise. The Delinea Platform seamlessly extends PAM by providing authorization for all identities, controlling access to an organization's most critical hybrid cloud infrastructure and sensitive data to help reduce risk, ensure compliance, and simplify security. Delinea removes complexity and defines the boundaries of access for thousands of customers worldwide. Our customers range from small businesses to the world's largest financial institutions, intelligence agencies, and critical infrastructure companies. **delinea.com**