Enterprise Strategy Group™
by TechTarget

PASSWORDLESS
in the Enterprise

Jack Poller, Senior Analyst

JUNE 2023

Research Objectives

Traditional authentication methods aren't working. With the availability of cheap cloud GPUs to crack passwords and tens of billions of known accounts/passwords, it's clear that passwords aren't secure. MFA hasn't been a viable replacement as it's susceptible to social engineering, phishing, and other attacks while introducing user friction and degrading the user experience.

Successful attacks are cultivating the need for a new authentication method. Recent prominent MFA-based breaches and friction in the end-user experience have reached the ears of app developers, IT, and cybersecurity leadership. Organizations are now searching for alternative methods to address the risks and challenges of MFA and password-based authentication.

IAM vendors need to demystify passwordless authentication. While the concept has received tremendous publicity as a panacea, organizations struggle to understand which passwordless methods are the best fit for different use cases. Passwordless vendors are jockeying to differentiate themselves in this crowded space to demonstrate they're the best fit for prospective customers.

To gain insights into the authentication landscape generally and the evolution of passwordless technology specifically, TechTarget's Enterprise Strategy Group (ESG) surveyed 377 IT, cybersecurity, and application development professionals responsible for identity and access management programs, projects, processes, solutions/platforms, and services in North America.

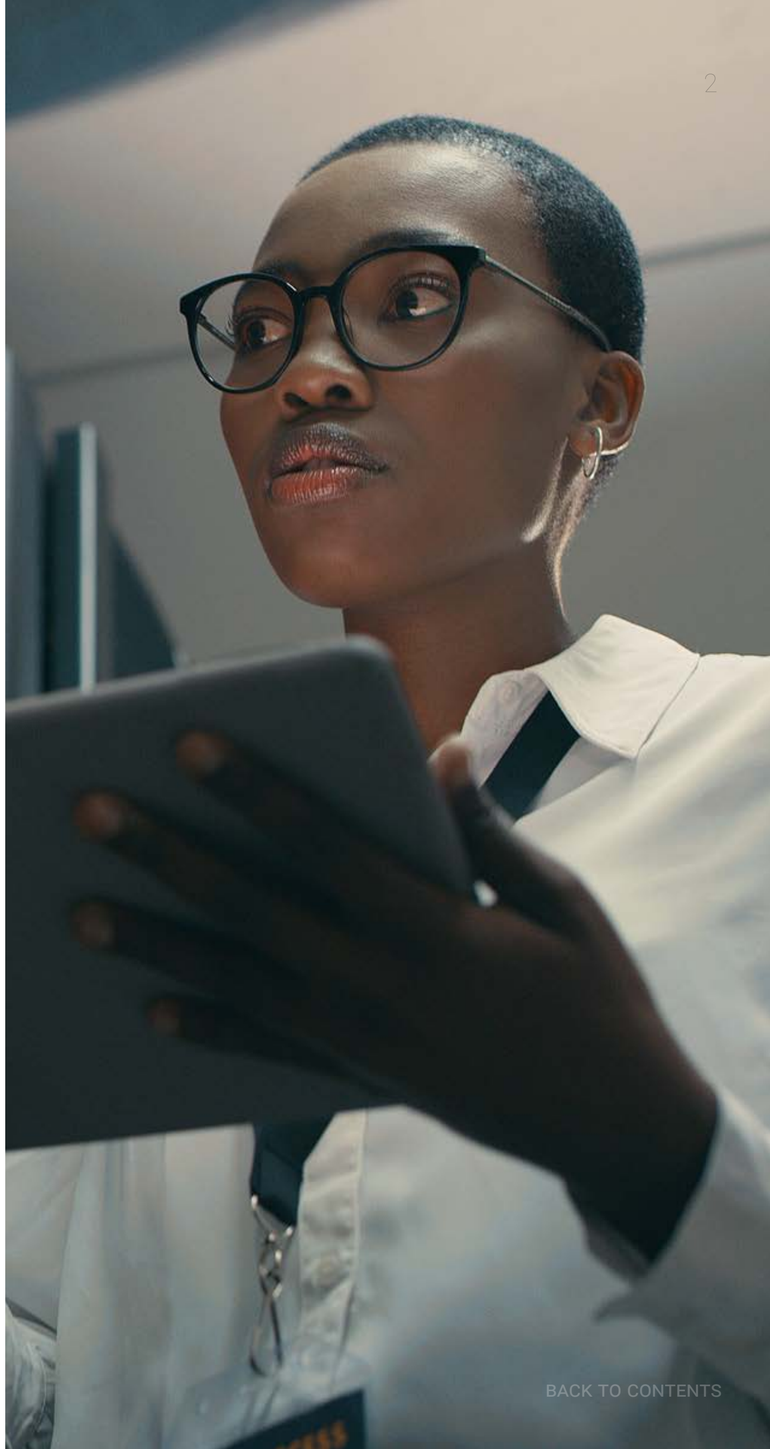
This study sought to:

Examine the impact of cyber-attacks on authentication and cybersecurity.

Gain insights into top authentication challenges and user experiences with and attitudes toward modern authentication.

Determine organizational desires to address authentication challenges with phishing-resistant passwordless authentication.

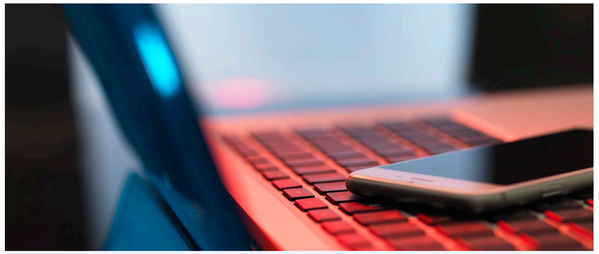
Establish passwordless authentication spending intentions and priorities.



BACK TO CONTENTS

KEY FINDINGS

CLICK TO FOLLOW



Workforce Authentication Failures Are Common and MFA Is *Still* Not Mandatory

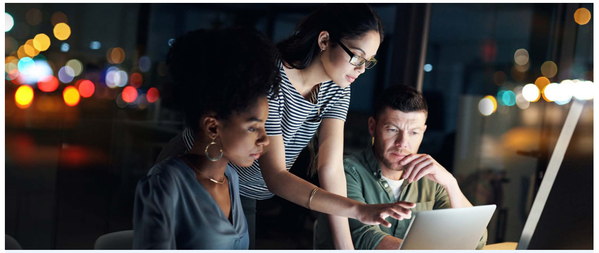
PAGE 4

Two-thirds Have Started Their Workforce Passwordless Journey

PAGE 7

Phishable MFA for Customers Is the Norm

PAGE 10



Customer Passwordless Is Gaining a Foothold

PAGE 14

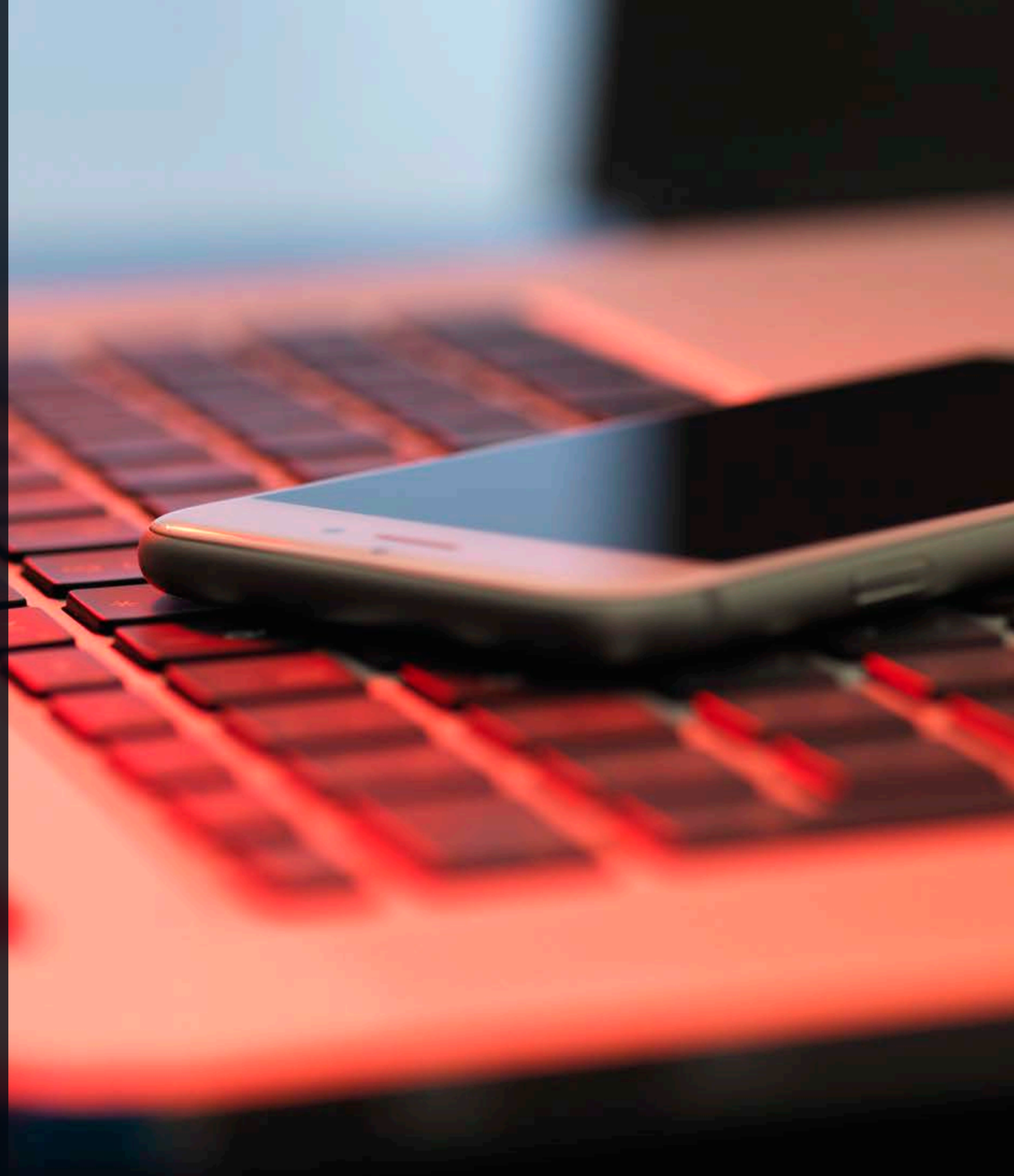
Multiple Account or Credential Compromise Is the Norm

PAGE 18

Investment in Strong Authentication Is Growing

PAGE 22

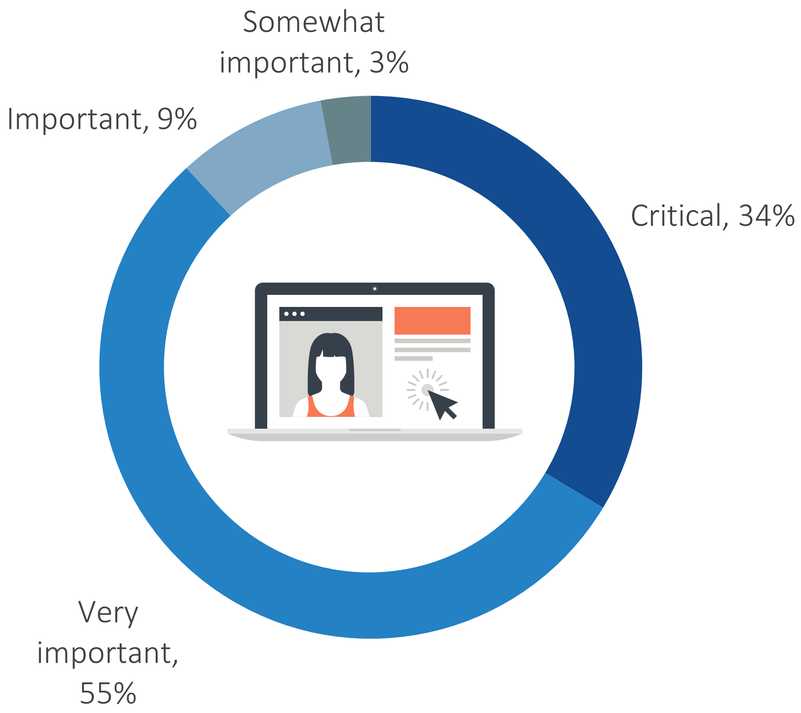
Workforce Authentication Failures Are Common and MFA Is *Still* Not Mandatory



Significant Portions of Workforce Identities Are Insufficiently Secured

With the rise of ransomware and the realization that the majority of attack paths involve the compromise of an identity, organizations recognize that strong authentication is critically important. Indeed, nearly nine in ten consider authenticating employee identities critical (34%) or very important (55%). However, securing workforce identities is a challenge organizations have yet to overcome, recognizing that a significant portion of their workforce identities are insufficiently secured.

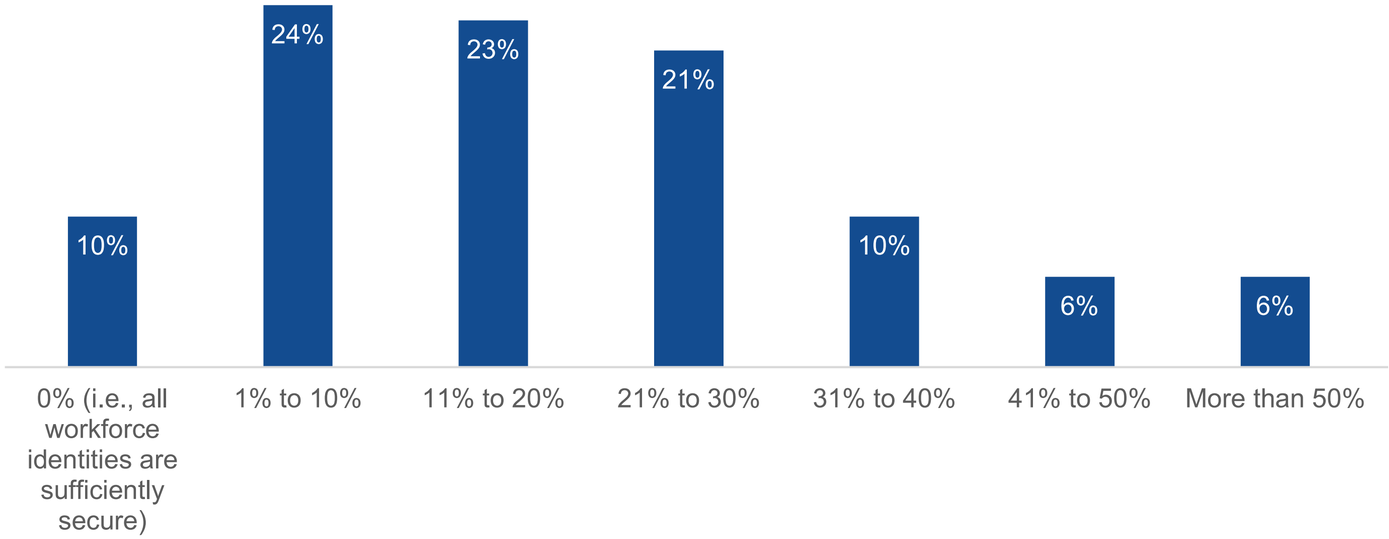
Priority level for authenticating workforce identities.



Percentage of workforce identities believed to be **insufficiently** secured.

43%

say that more than one in five of their workforce identities are **insufficiently** secured.



BACK TO CONTENTS

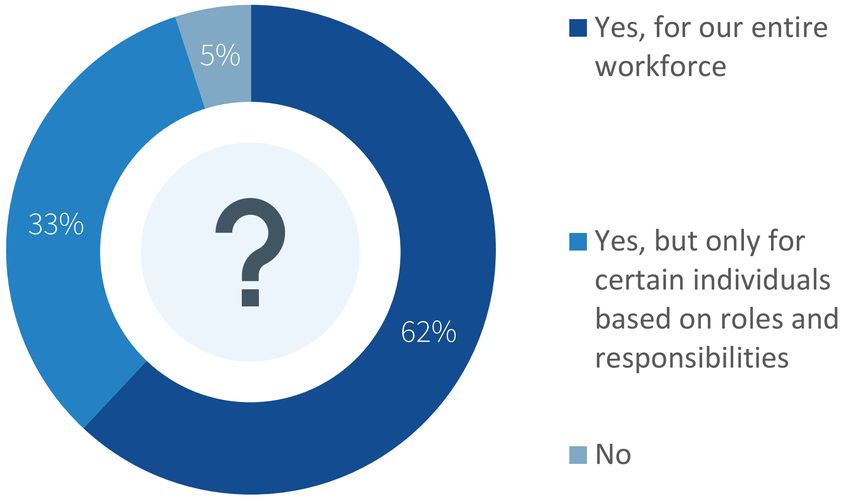
> “Almost two-fifths **fail to authenticate** at least 25% of the time.”

MFA *Still* Not Mandatory for the Entire Workforce

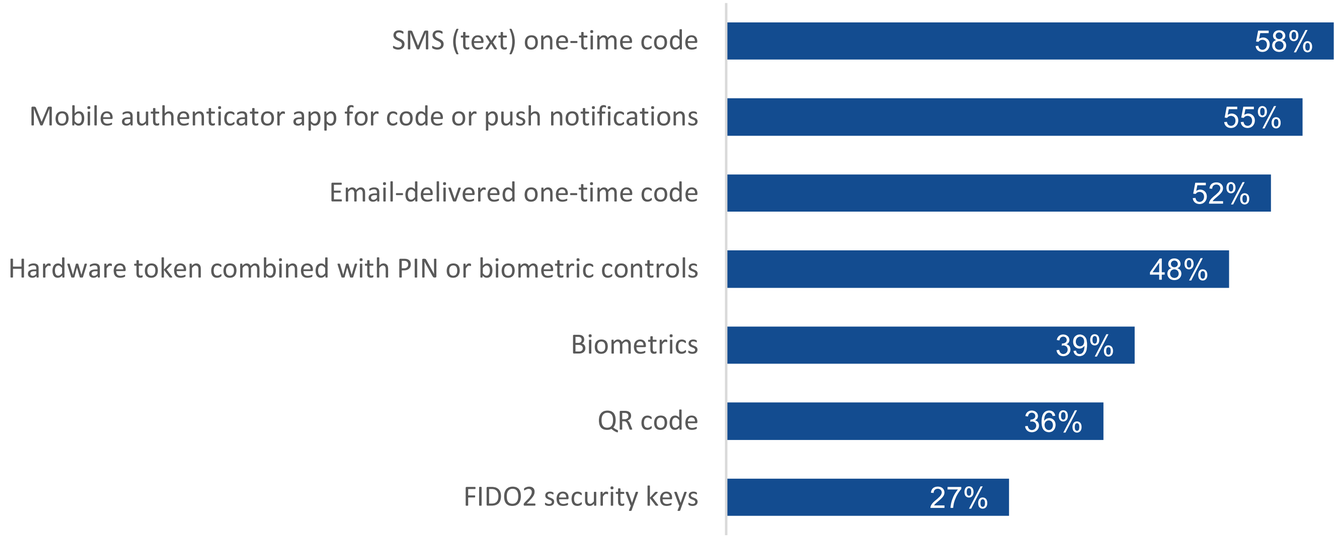
Users already have too many accounts with hard-to-remember, complex passwords, introducing friction into the user experience. More friction comes from multifactor authentication, and this friction causes login failures. In fact, almost two-fifths fail to authenticate at least 25% of the time.

But friction and login failures shouldn’t stop organizations from strengthening their authentication process. It’s surprising that despite all the known identity risks and the protection afforded by MFA, more than one-third don’t make MFA mandatory for the entire workforce. Equally surprising is that SMS, mobile apps, and one-time email codes are the most common MFA factors, even though they’re easily phishable.

Is multifactor workforce authentication mandatory?



Additional factors of workforce multifactor authentication.



BACK TO CONTENTS

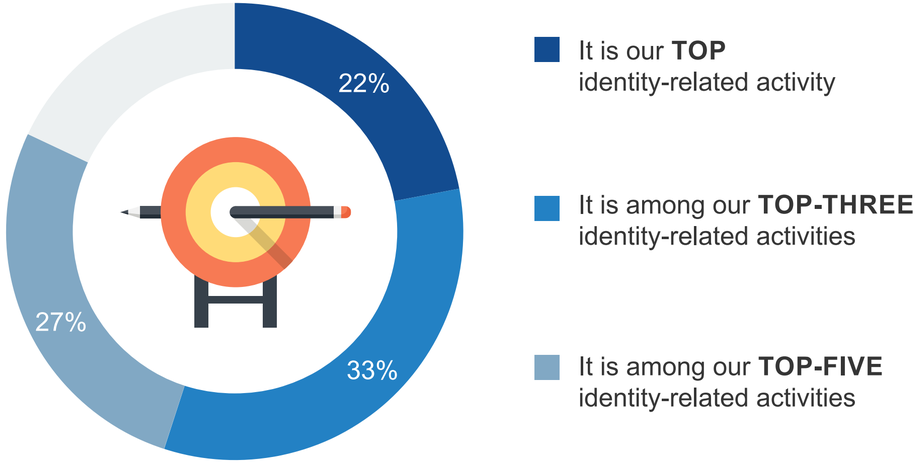
Two-thirds Have Started Their Workforce Passwordless Journey

Two-thirds Have Started Their Workforce Passwordless Journey

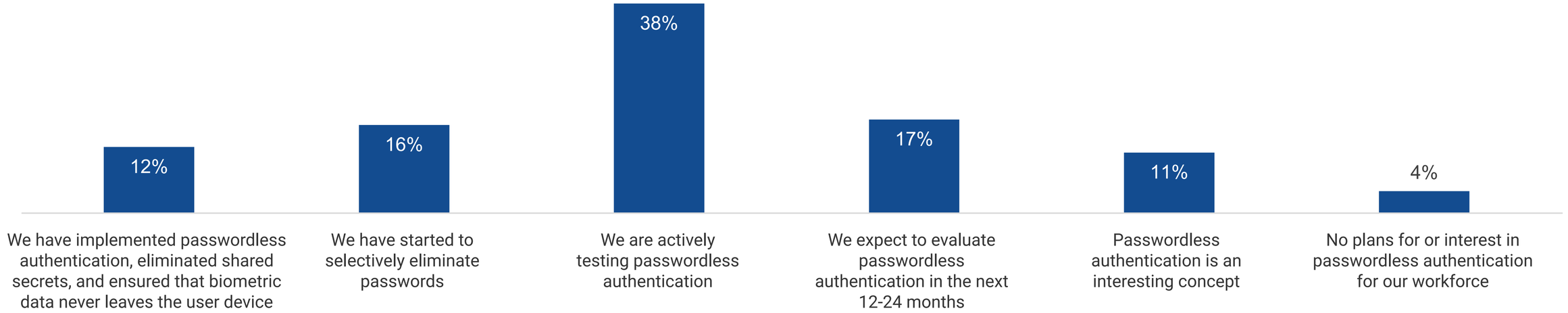
The volume of authentication-related compromises (password cracking, social engineering, MFA push-bombing, etc.) demonstrates how much password-based authentication is a threat to an organization's security. This is why organizations believe passwordless authentication for their workforce is a strategic activity, with **more than half (55%) of organizations ranking passwordless among their top-three identity-related activities.**

For two-thirds of organizations, passwordless authentication is more than a good idea. These organizations have started testing and deploying passwordless authentication, and 12% have even successfully eliminated passwords for a portion of their workforce.

Priority level for using passwordless workforce authentication methods.



Usage of or plans for passwordless workforce authentication methods.



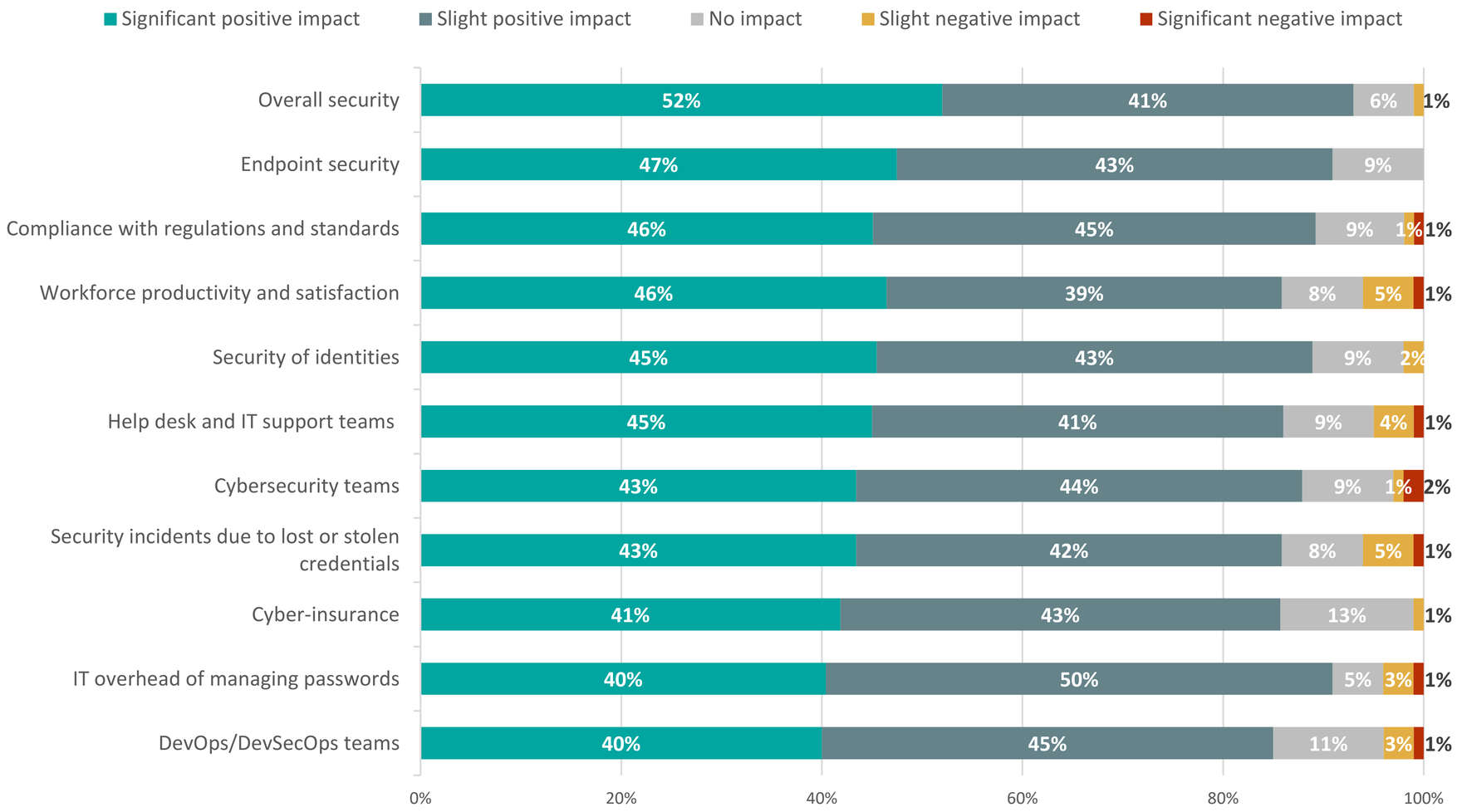
BACK TO CONTENTS

Workforce Passwordless Is Making a Positive Impact

While organizations expect and experienced an improvement in overall security when deploying passwordless authentication for their workforce, passwordless provides many other benefits such as:

- Compliance with new standards and regulations, including zero trust.
- Reduced user login friction by eliminating the need to remember passwords and the hassle of MFA as well as bringing about the concomitant increase in workforce productivity and satisfaction.
- Reduced calls to help desk/IT for password resets and account lockouts.
- Eligibility to obtain cyber-insurance or reduce rates.

Impact that passwordless **workforce** authentication has had (or will have) in certain areas.



BACK TO CONTENTS

Phishable MFA for Customers Is the Norm

Significant Portions of Customer Identities Are Insufficiently Secured

While all organizations are justifiably concerned with ensuring proper authentication of their workforce, those with customer-facing applications have additional concerns: account takeover attacks that enable access to customers' confidential information for nefarious activities. Of grave concern is access to financial accounts leading to fraudulent purchases and outright theft of customers' funds.

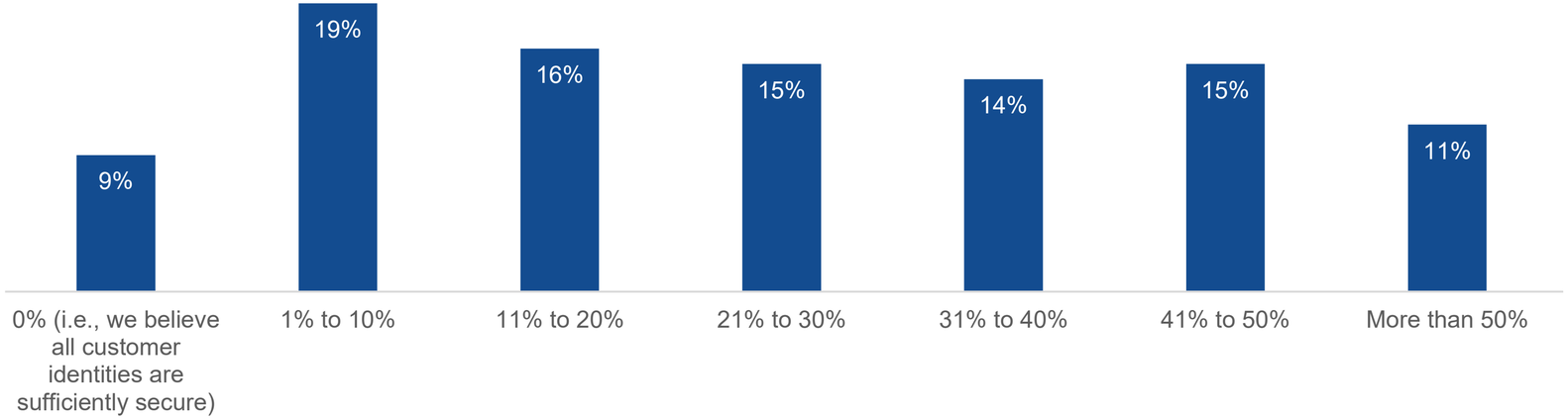
Unfortunately, respondents say that a significant portion of their customer identities are insufficiently secured.

Strengthening authentication to secure accounts and prevent identity theft can reduce the risk of fraud and theft of billions of dollars of funds, merchandise, services, and data. Therefore, the vast majority of organizations are prioritizing their customer authentication practices, with more than one-third (36%) designating authentication as a critical activity.

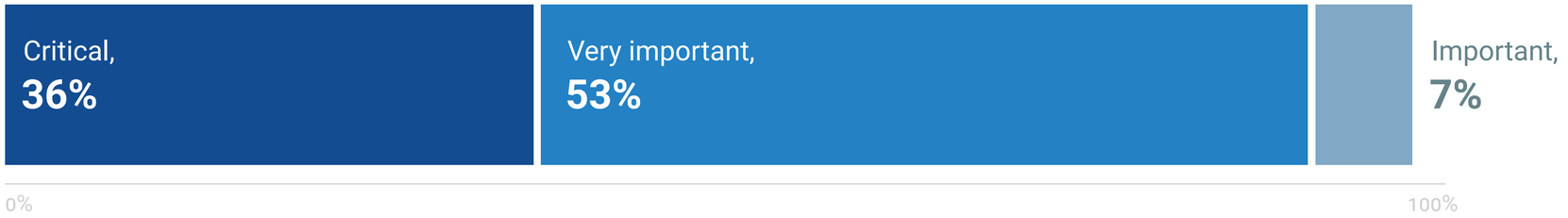
Percentage of customer identities believed to be **insufficiently** secured.

45%

say that more than one in five of their customer identities are **insufficiently** secured.



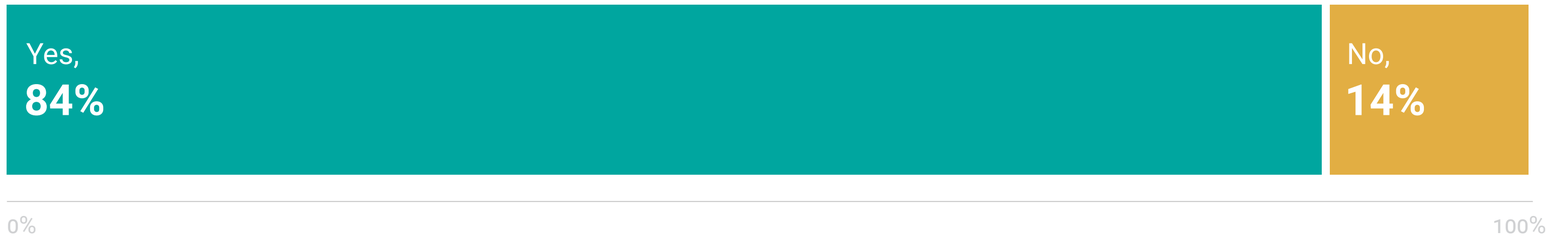
Priority level for authenticating customer identities.



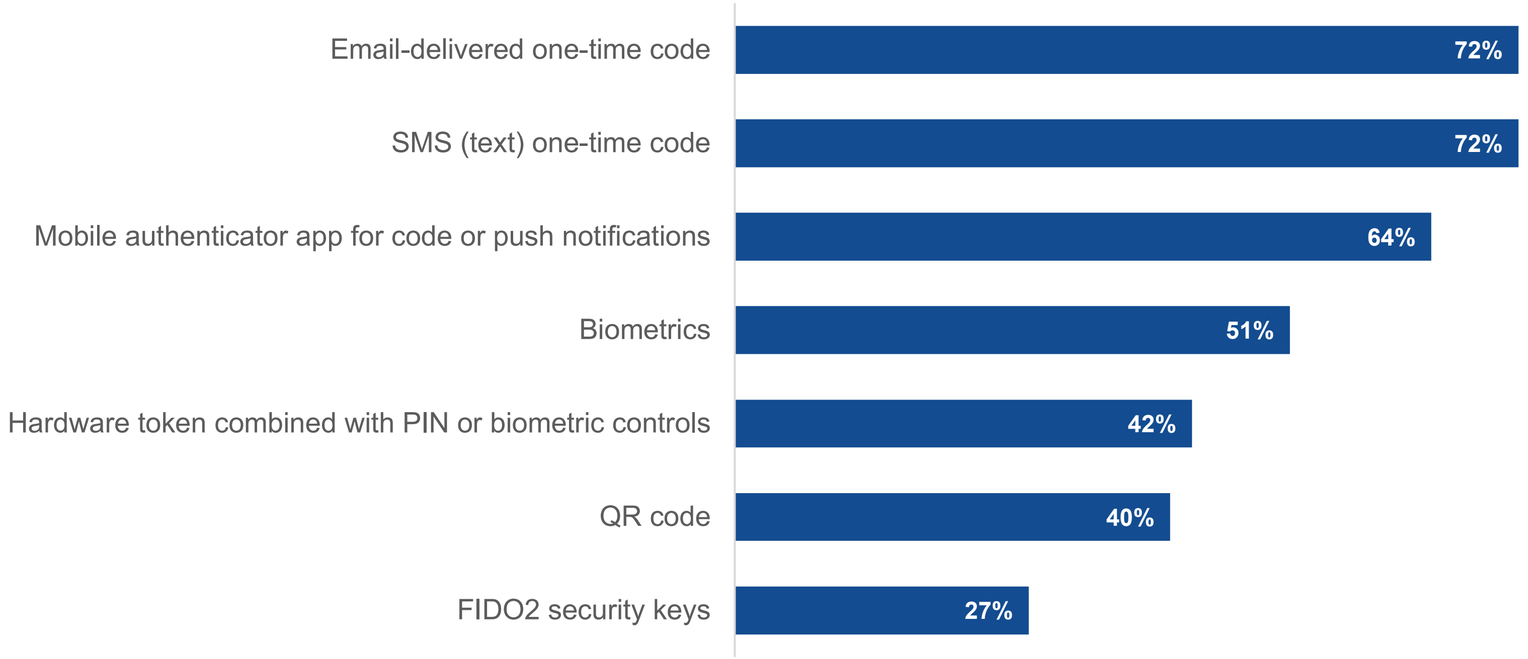
An additional 5% said somewhat important or not important at all.

BACK TO CONTENTS

Is multifactor customer authentication mandatory?



Additional factors of customer multifactor authentication.



MFA Is Mandatory for Most Customers, But Phishable Factors Are Still in Use

The cost and risk of lost or stolen data, business, and funds from compromised accounts is motivating the vast majority organizations to strengthen authentication by making MFA mandatory for their customers.

Unfortunately, organizations haven't gone far enough, and still rely on the weakest forms of MFA. SMS, mobile apps, and one-time email codes are the most common MFA factors, even though they're very susceptible to social engineering attacks.

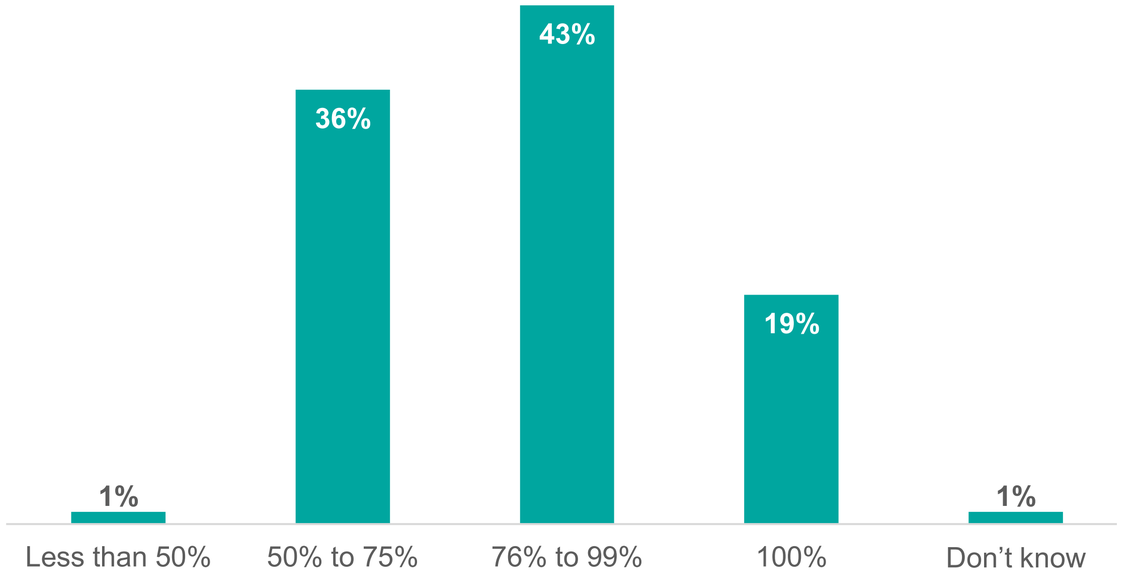
BACK TO CONTENTS

MFA Issues Can Impact Revenue and Customer Retention

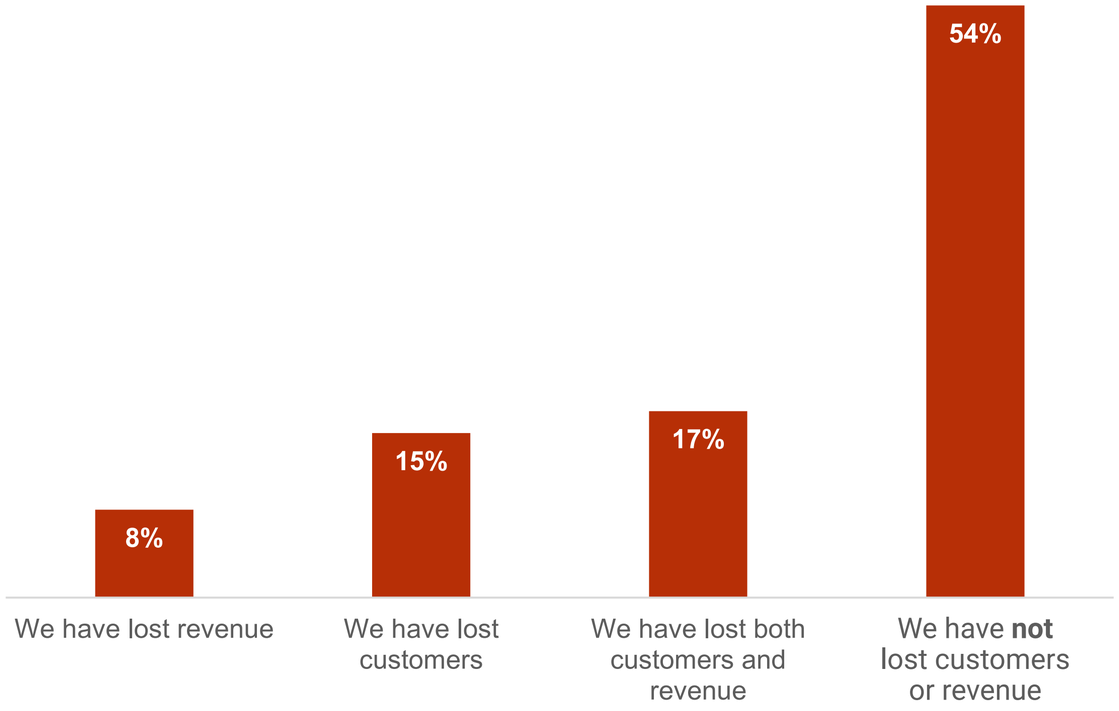
Trying to remember and correctly type long and complex passwords or depending on unreliable email, SMS, or other MFA techniques leads to authentication failures. Indeed, more than one-third (37%) of respondents say their customers fail to authenticate at least 25% of the time.

Whether it's to check the latest social media posts, talk to doctors, access bank accounts, or make purchases, customers want quick and easy access to their accounts. Friction, especially that introduced by MFA, can cause such aggravation that customers abandon their transactions, leading to lost revenue, or worse, abandon the vendor altogether.

Customer authentication success rate.



Impact of customer attitudes toward or issues with MFA.



BACK TO CONTENTS

Customer Passwordless Is Gaining a Foothold

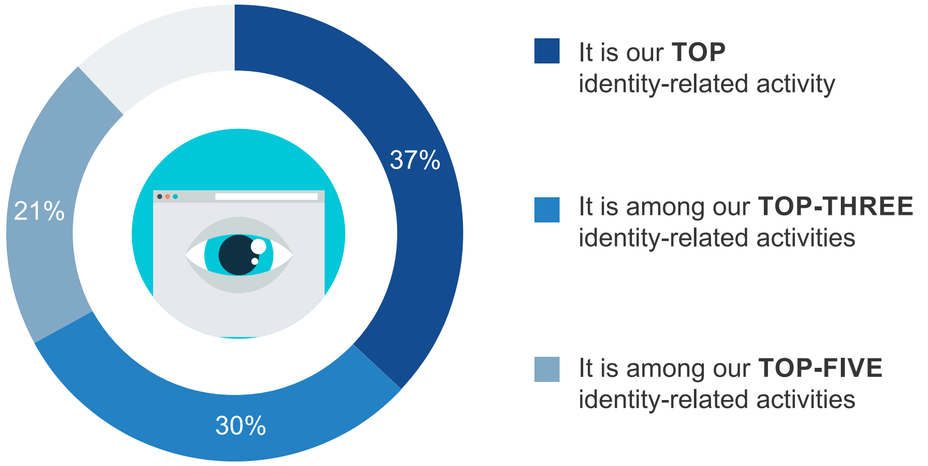
Passwordless for Customers Is a Strategic Activity

The significant volume of authentication failures, MFA friction leading to loss of revenue and customers, and the massive volume of password hacking, credential stuffing, MFA push-bombing, and other account takeover attacks have organizations with customer-facing applications looking to strengthen and simplify the authentication process.

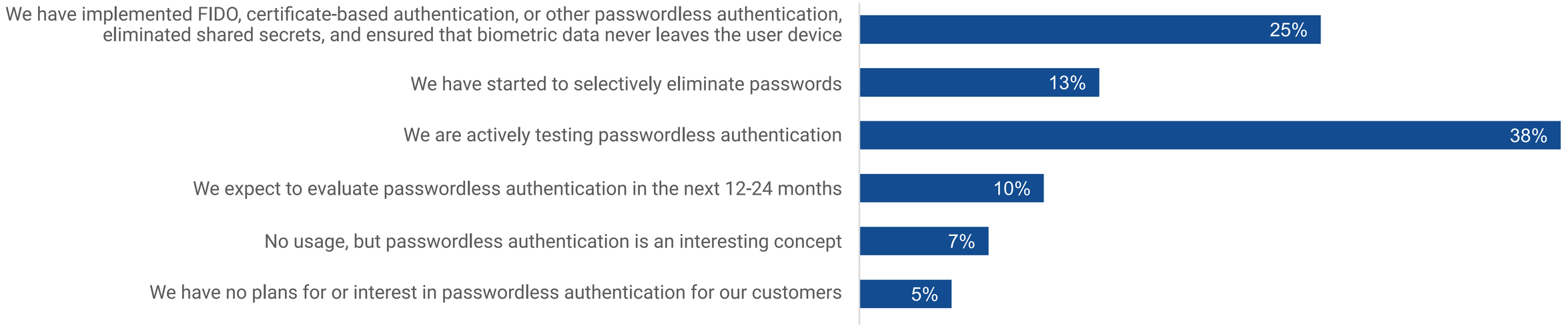
For two-thirds of organizations, moving to passwordless authentication is a strategic activity, with more than one-third ranking passwordless authentication as their top overall identity-related activity.

And that has translated into significant progress in deploying passwordless. While more than half of organizations are testing or selectively eliminating passwords for customer authentication, fully one-quarter have implemented FIDO, certificate-based, or other passwordless authentication, completely eliminating shared secrets from their customer authentication process.

Priority level for using passwordless customer authentication methods.



Usage of or plans for passwordless workforce authentication methods.



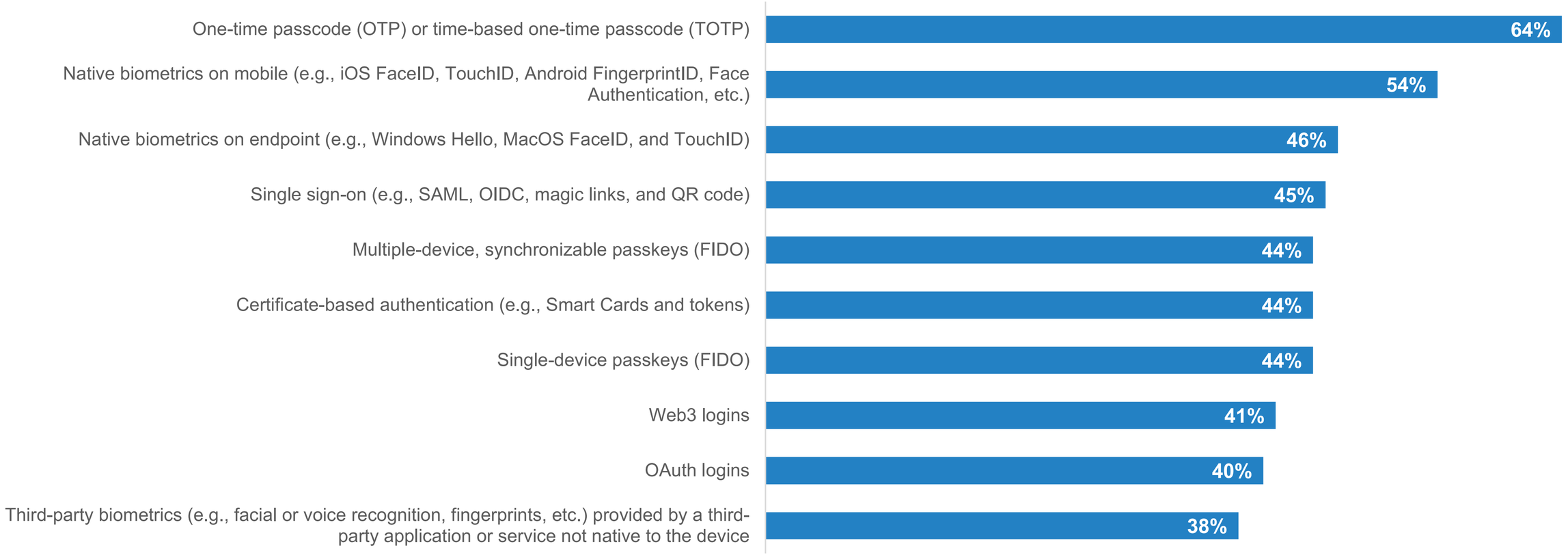
BACK TO CONTENTS

Customer Authentication Leverages OTP and Mobile Biometrics

Eliminating passwords can be confusing for customers, so organizations are most commonly using the simplest or most ubiquitous forms of passwordless authentication: One-time codes, native biometrics on mobile devices, and single sign-on (SSO).

In May 2022, Apple, Google, and Microsoft jointly announced support for FIDO passwordless authentication. This guarantee that all major devices and browsers will support FIDO is driving rapid adoption of FIDO for customer-facing apps.

Types of passwordless solutions currently used for customers.



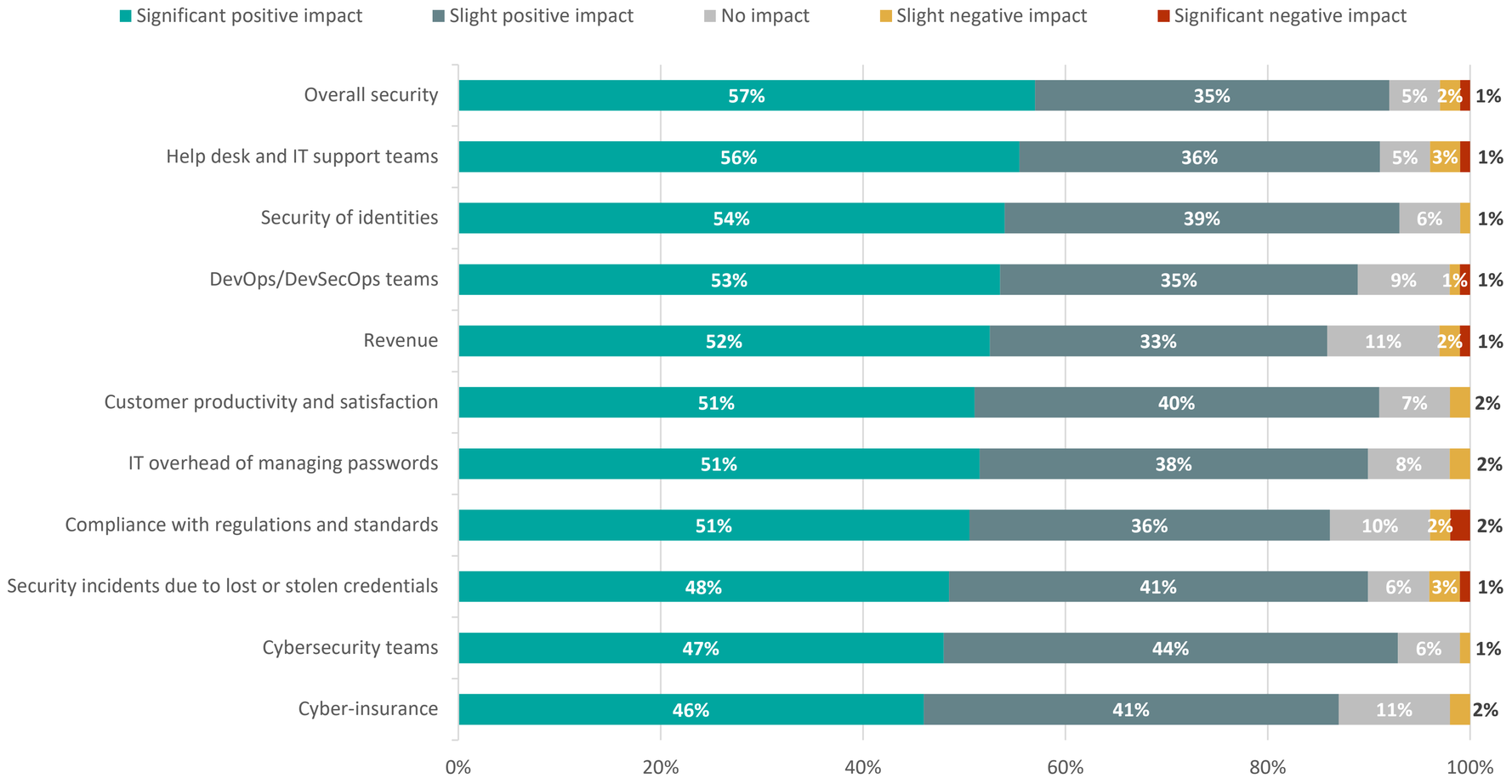
BACK TO CONTENTS

Customer Passwordless Is Making a Positive Impact

In addition to the expected risk reduction that comes from deploying passwordless authentication for customer-facing apps, organizations expect and experience a multitude of benefits including:

- Reduced calls to help desk/IT for password resets and account lockouts.
- Reduced burden on DevOps/ DevSecOps having to design, develop, deploy, and secure passwords and MFA.
- Reduced MFA-induced revenue loss.
- Increased customer productivity and satisfaction by eliminating the friction from passwords and MFA.
- Eligibility to obtain cyber-insurance or reduce rates.

Impact that passwordless **customer** authentication has had (or will have) in certain areas.



BACK TO CONTENTS

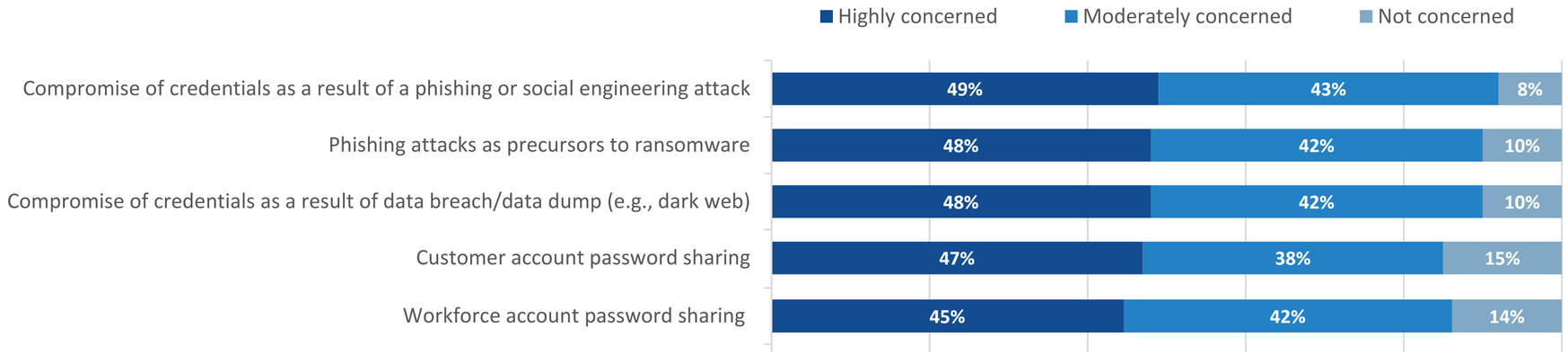
Multiple Account or Credential Compromise Is the Norm

The Angst Surrounding Authentication Is Justified as Phishing and Password Sharing Result in Compromise

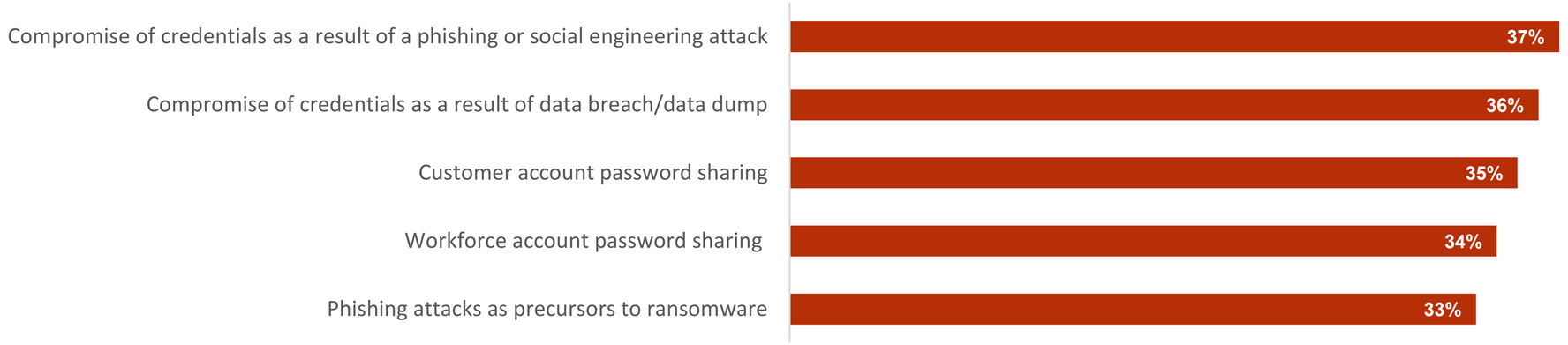
Phishing, credential data breaches, and password sharing provide the greatest angst for those responsible for identities and authentication. But that's not all: They're almost equally concerned about the multitude of other ways in which accounts can be compromised.

The good news is that security and identity professionals are dialed in to the problems as their top threat concerns match the top attacks they actually experience.

Level of concern for specific authentication-related threats.



Top five contributors to the compromise of accounts or credentials.



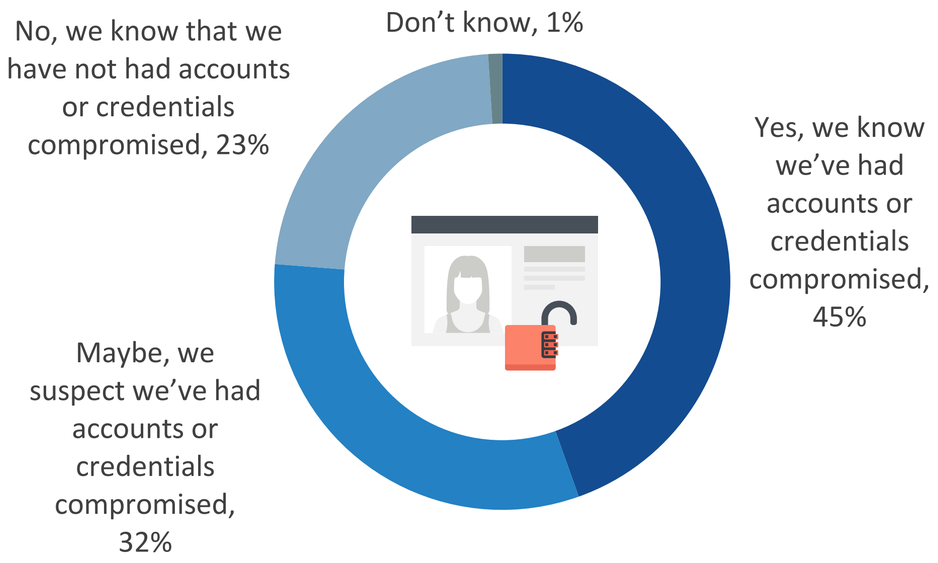
BACK TO CONTENTS

Multiple Account/Credential Compromise Is the Norm

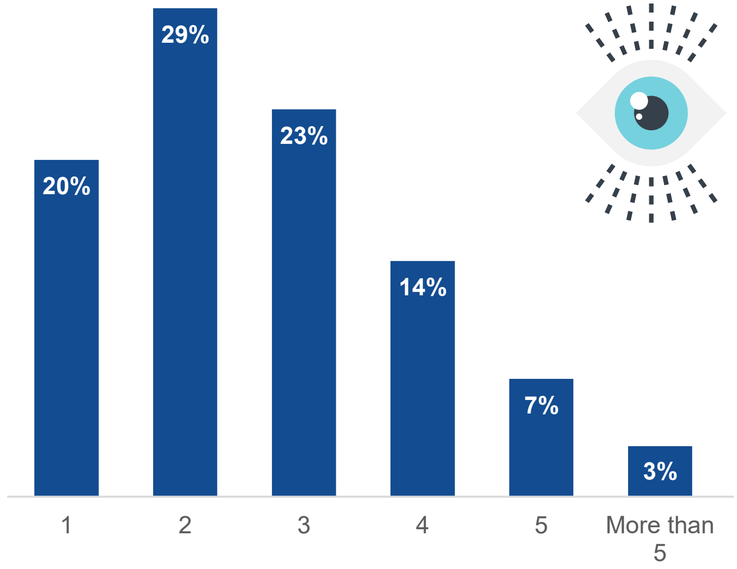
Organizations face challenges defending against the multitude of disparate attack vectors targeting both weak authentication methods and the human element. The result is that almost half (45%) of respondents know they've experienced account or credential compromise. Of great concern, however, is the one-third of organizations that suspect they've suffered account or credential compromise but don't know for sure because they don't have the proper tooling in place.

Unfortunately, organizations are failing to learn from and respond to account or credential compromises, and more than three-quarters (76%) of those victimized have experienced multiple account compromise events in the last 12 months alone.

Have organizations experienced any account or credential compromises in the last 12 months?



Number of account or credential compromises experienced in the last 12 months.



76%
experienced **multiple account or credential compromises.**

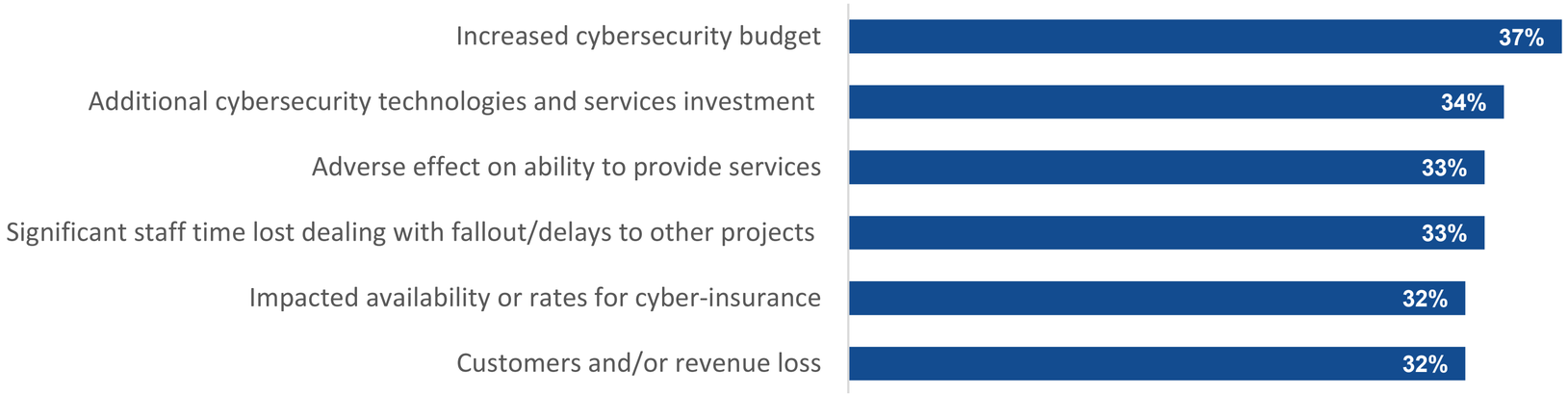
BACK TO CONTENTS

Account or Credential Compromise Is a Precursor to Successful Cyber-attacks, Which Are Too Common

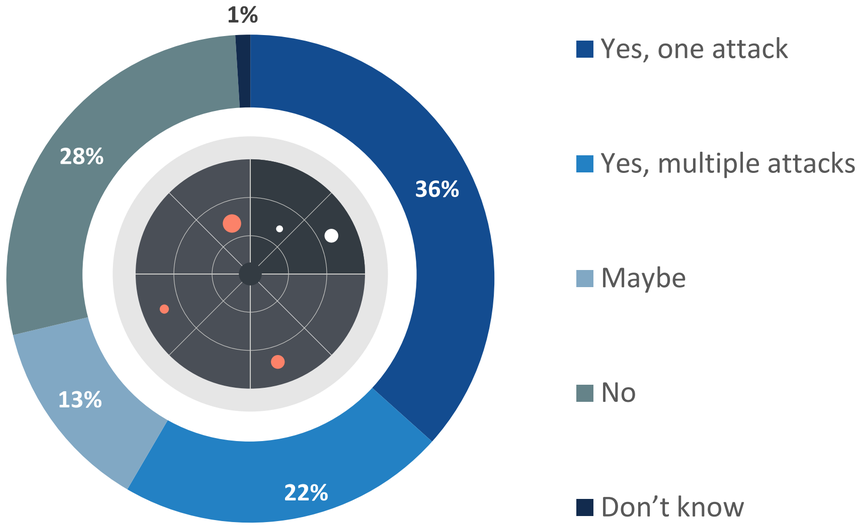
Organizations face direct risks from account or credential compromise: theft of account information, financial accounts, or payments, and purchase fraud. Credential compromise also presents an indirect risk: traditional cyber-attacks further penetrating the organization. **Unfortunately, 59% have experienced such attacks, with almost one-quarter suffering from multiple attacks.** Also of concern is the 13% who think they've had a successful credential-related attack but don't know for sure.

Cyber-attacks targeting identities impact the organization's ability to conduct operations, and delay projects as resources are diverted to deal with the fallout. Because these attacks negatively impact revenue and customer retention, security leadership and management stakeholders may be terminated. While these attacks are disruptive, they have also helped drive organizational commitment to improving cybersecurity through increased budgets and deployment of additional controls.

Top business impacts of successful cybersecurity attacks stemming from compromised accounts or credentials.



Have compromised accounts or credentials led to a successful cybersecurity attack?



> **"Unfortunately, 59% have experienced a successful cybersecurity attack,** with almost one-quarter suffering from multiple attacks."

BACK TO CONTENTS

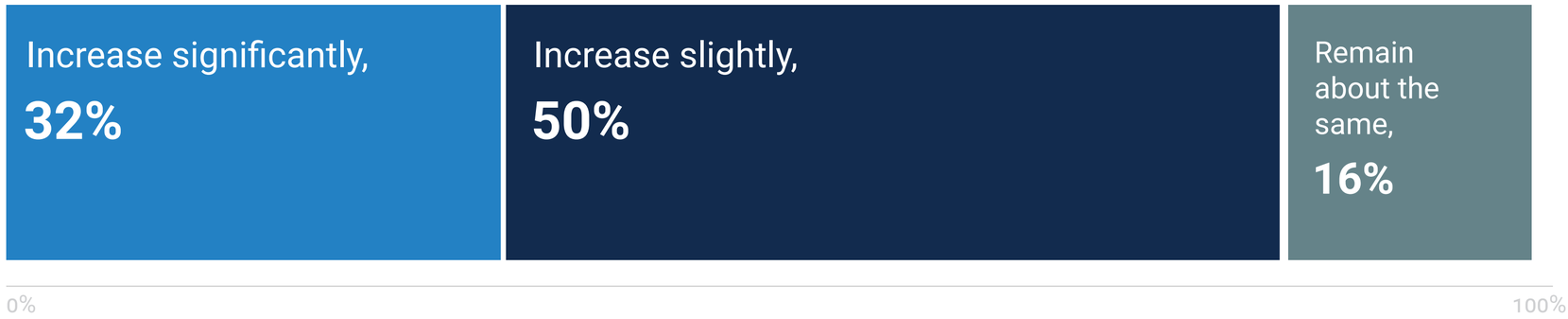
Investment in Strong Authentication Is Growing

Authentication to Garner Larger Share of Identity Budget

Organizations have experienced the negative impacts of passwords and MFA: user friction, account lockouts, account compromises, account takeovers leading to loss of data, loss of revenue, loss of customers, cyber-attacks, and other damages. This has increased the collective awareness of security, IT operations, and DevOps groups that authentication is a critical component of both an organization's overall cybersecurity strategy and its user and customer experience.

Therefore, organizations are earmarking their cybersecurity budgets to include identity security. Specifically, 82% of organizations expect to increase their spending on authentication to some extent over the next 12 months, with one-third classifying these increases as significant.

Expected spending change on authentication technologies over the next 12 months.



An additional 1% said it will decrease slightly.

82%

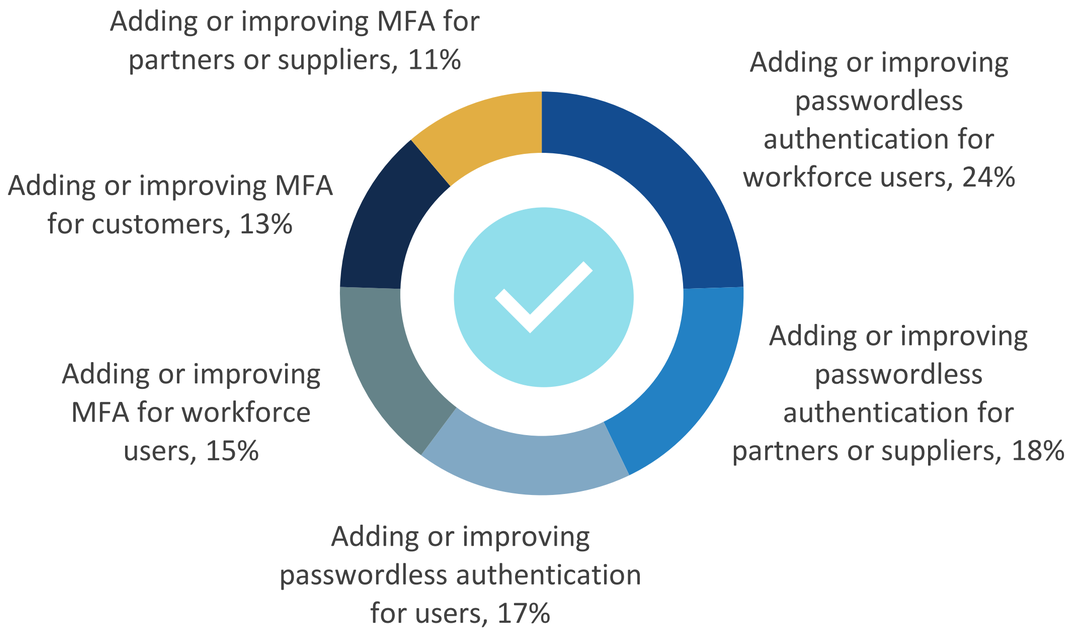
of organizations **expect to increase their spending** on authentication to some extent over the next 12 months.

BACK TO CONTENTS

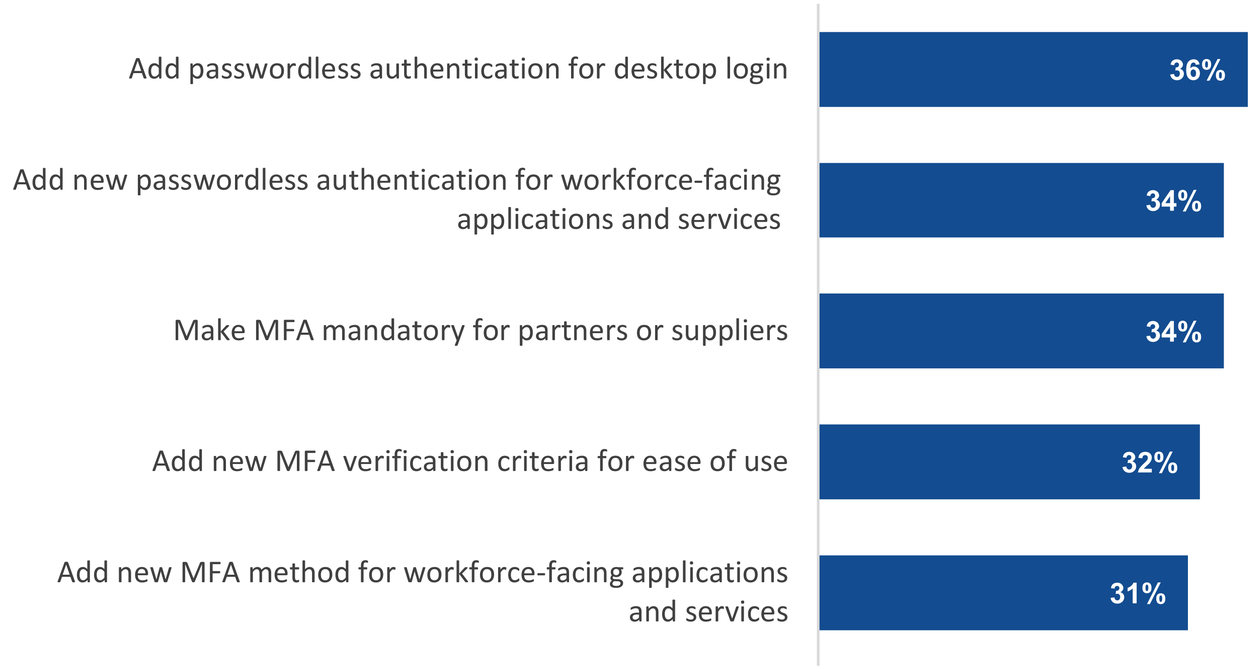
Passwordless Tops the Action Priority List and the Investment List

Organizations clearly understand that password-based authentication is susceptible to hacking and phishing. While making MFA mandatory for both the workforce and customers can reduce risk, many MFA methods themselves can be compromised by social engineering. Additionally, they can introduce friction to the login process, which can lead to a poor user experience, loss of revenue, and loss of customers. Thus, organizations are prioritizing the move to passwordless authentication for their workforce. Likewise, additional funds will be invested in adding or improving passwordless authentication for the workforce, partners, suppliers, and customers.

Areas expected to benefit from an increase in authentication technologies over the next 12 months.



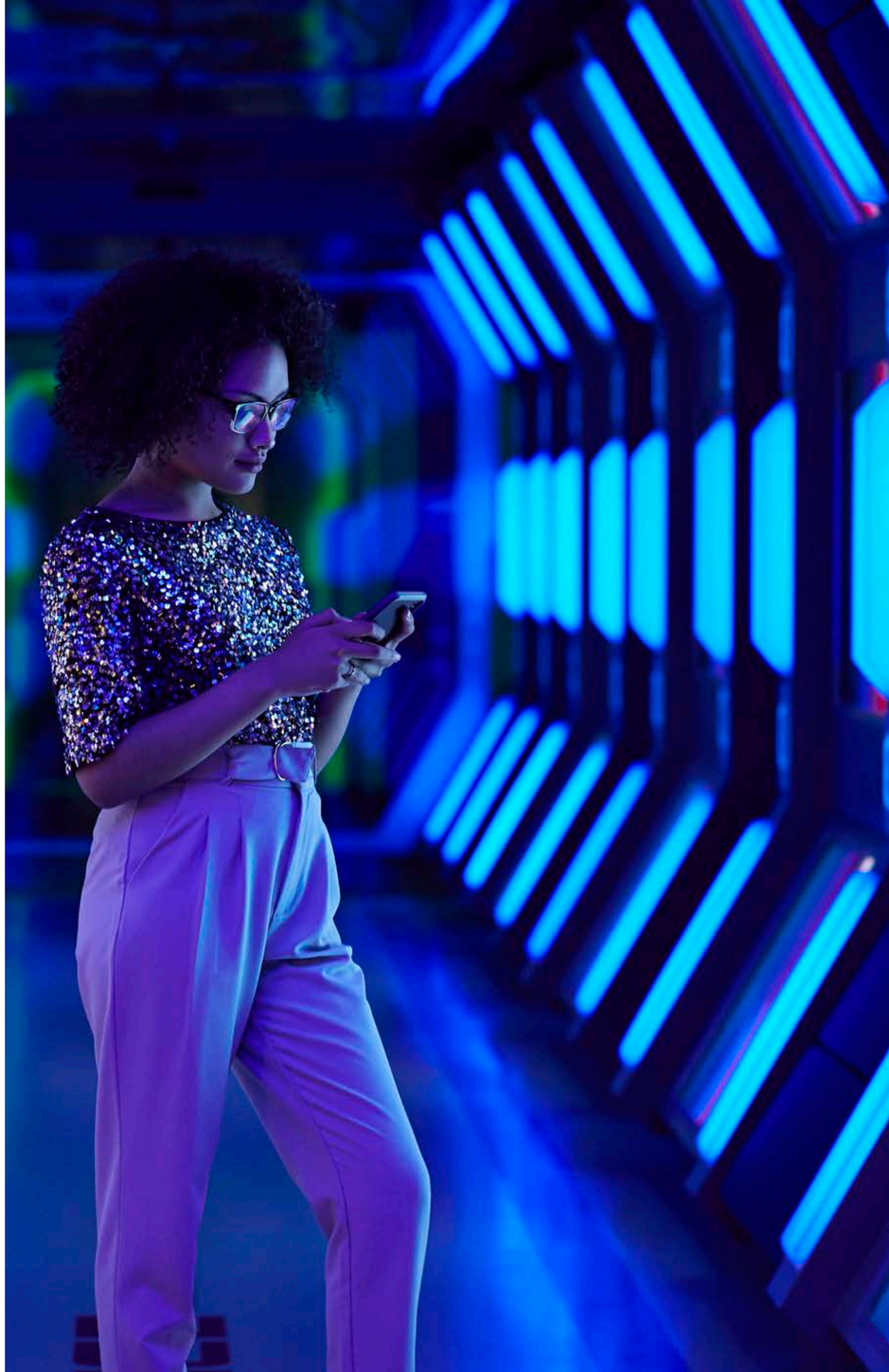
Likeliest actions to be taken with authentication technologies over the next 12-18 months.



BACK TO CONTENTS

Nok Nok is a leader in passwordless customer authentication and delivers the most innovative FIDO (Fast IDentity Online) solutions for the passwordless authentication market today. Nok Nok empowers organizations to significantly improve their user experience and security, and reduce operating expenses, while enabling compliance with the most rigorous privacy and regulatory requirements. The Nok Nok™ S3 Authentication Suite integrates into existing security environments to deliver proven, FIDO-enabled passwordless customer authentication. As a founder of the FIDO Alliance and an innovator of FIDO standards, Nok Nok is an expert in next-level, multi-factor authentication. Nok Nok's global customers and partners include AFLAC Japan, BBVA, Carahsoft, Fujitsu Limited, Hitachi, Intuit, Mastercard, MUFG Bank, NTT DATA, NTT DOCOMO, Standard Bank, T-Mobile, and Verizon.

LEARN MORE



ABOUT ENTERPRISE STRATEGY GROUP

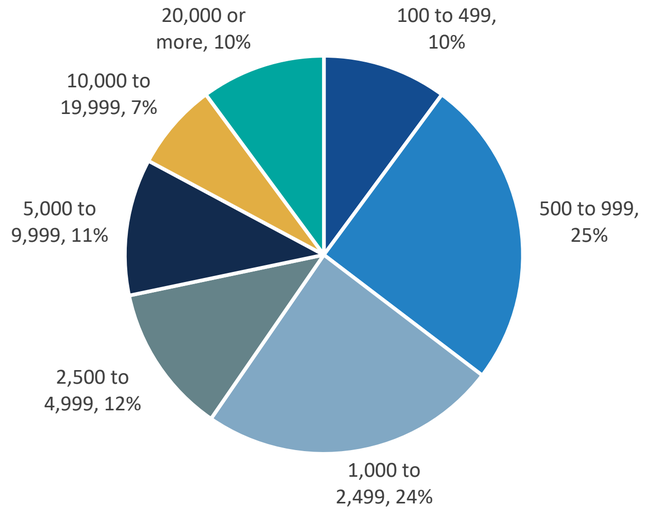
TechTarget's Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.

Respondent Demographics and Research Methodology

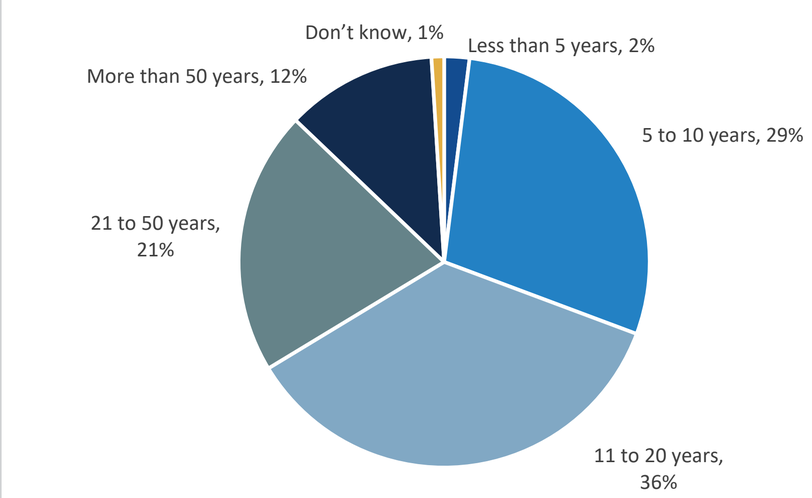
To gather data for this report, ESG conducted a comprehensive online survey of IT, cybersecurity, and application development professionals from private- and public-sector organizations in North America (United States and Canada) between April 5, 2023, and April 19, 2023. To qualify for this survey, respondents were required to be personally responsible for evaluating and purchasing identity and access management programs, projects, processes, solutions/platforms, 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 377 IT, cybersecurity, and application development professionals.

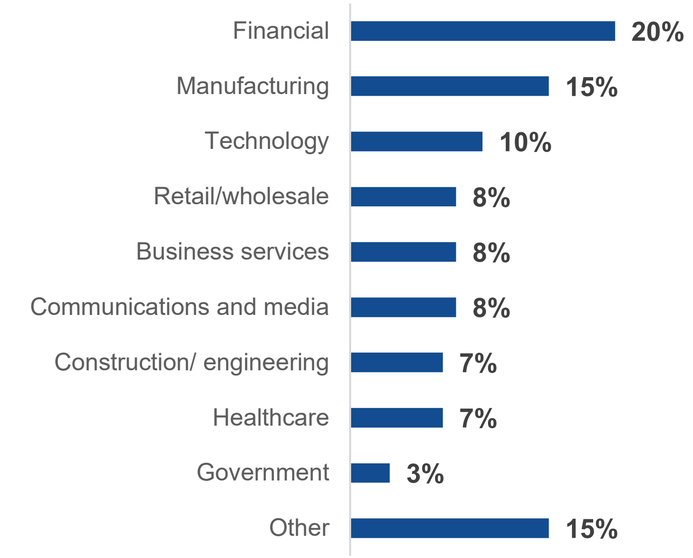
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY AGE OF COMPANY



RESPONDENTS BY INDUSTRY



BACK TO CONTENTS

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.