State of Authentication Report

Strengthening security posture with next generation technology is an imperative.

SECUREAUTH
Welcome to Better Identity.

Contents

Executive Summary

Survey Findings

EXECUTIVE SUMMARY

Time to Move Beyond Traditional MFAs

SecureAuth's inaugural State of Authentication report is based on a detailed research survey conducted independently by ViB Research. The report is based on a survey of 285 IT and security professionals from mid to large enterprises in North America. It provides insight into the current state of authentication and the latest innovation adoption trends like invisible MFA, device trust, and passwordless technologies.

Authentication Security is Top Priority

Authentication has become one of the top priorities with 84% of the respondents, placing authentication and access management in their top 3 to 5 cyber security priorities. Another 11% placed it in their top 10.

Traditional MFA is Popular, but Susceptible to Attacks

While credential-related attacks continue to be the top vector for cyberattacks, the research showed that most companies are still stuck in the world of legacy MFAs. However, it was reassuring to see that most respondents have MFA practices in place instead of using simple passwords. Despite the prevalence of traditional MFA, respondents do have many security-related concerns about traditional or "legacy" MFA, including:

- Over half think the technology is susceptible to cyberattacks. 21% feel traditional MFA cannot be used as an effective hacker deterrent because adoption rates are too low in operational terms.
- Most respondents have little confidence in using traditional MFAs to thwart credential-related cyberattacks. When asked, "Given that most attacks occur through credentials, how confident are you that traditional MFA is enough to thwart attacks?" only 5% are very confident with another 40% somewhat confident. Not a strong vote of confidence for traditional MFAs.
- Traditional MFA has users authenticate using verification factors like one-time passwords (OTPs) and personal identification numbers (PINs) transmitted over SMS text messages, emails or phone calls. While these MFA techniques were

considered revolutionary when they debuted in the late 1990s, they are increasingly viewed as "better than nothing," but problematic from a security perspective. Most respondents picked one-time-passwords or OTPs with 38% selecting that as one of the methods. The next most popular passwordless technologies were PINs (27%) and biometrics, which was tied with security keys at 26%.

Given the weaknesses associated with traditional MFAs that are easily exploitable with "MFA bombing", "man-in-the-middle" and other attacks, it's time to kill the traditional MFAs and move on to passwordless technologies that not only enhance security but also provide a much smoother user experience.

Passwordless Adoption Becoming Reality

The idea of authenticating users and managing access without passwords is a dream for IT and security professionals. As one respondent put it, "Passwordless security is the future and we believe we should be moving toward this goal.". The good news is that most respondents are looking to move to a passwordless world as quickly as possible. A whopping 65% are planning on implementing passwordless technologies in the next 24 months. Nearly a third are planning to do so in the next six months, and another third are looking at the 12-24 month horizon. The survey asked respondents to explain what was standing in their way. The top reason was having too many competing priorities (55%), followed by not knowing enough about the technology (46%), and lack of budget (24%). As more security professionals are getting educated on the importance of passwordless authentication especially when executed on a continuous basis, there seems to be a big momentum towards this type of solution.

> "Passwordless security is the future and we believe we should be moving toward this goal."
>
> —A Survey Respondent

Surprising Finding: 76% of Respondents Use More than One IdP

Some surprising results showed that many enterprises use multiple IdP products, a trend that bucks the usual consolidation of cyber security tools. 76%

of respondents use more than one IdP in their organization. They reported this redundancy due to failover, use case requirements, and preferred best of breed approach reasons. As over 80% of cyberattacks focus on credentials, it makes sense that practitioners need to have a back-up system in case their primary IdP product goes down or is compromised by an attack.

Device Trust: Woefully Underused

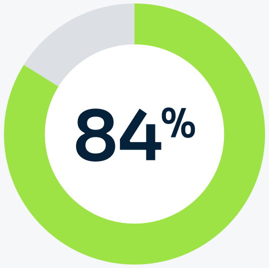
Further to the challenges in managing people external to the organization, the survey probed respondents on where they had implemented device trust technologies. As threats grow more sophisticated and legacy forms of access become more deficient, security managers have recognized that establishing trust with a user's device is critical to preserving a strong security posture. Hackers can easily impersonate legitimate users with stolen credentials, so it is the user's device that becomes a critical element in authentication. Indeed, without device trust, an attacker can penetrate an MFA control before the login stage. Device trust technologies track characteristics of a device that are unique to the user. These might include factors like geolocation and keystrokes or even patterns of movement. That way, if a user who lives in Dallas seems to be logging in from Berlin, a device trust solution will block the log in and issue an alert. An attack is most likely underway, unless the user has actually gone to Berlin. Unfortunately, device trust isn't used at all according to 25% of the respondents. And under half use it for mobile security and only 25% use it for Mac workstation safeguarding. It's an area where organizations can make great strides in shoring up their security posture by adding this valuable technology.

Conclusion

The majority of respondents realize that although traditional MFA is better than nothing, it's susceptible to cyberattacks and causes too much friction for users. The only way forward is to move towards a passwordless continuous authentication platform that powers a next generation version of MFA: invisible MFA. This will enable a strong security posture and Zero Trust Architecture while providing a frictionless user experience.

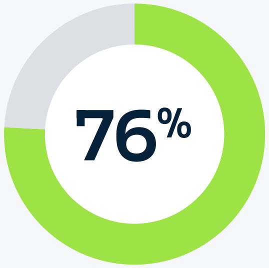
EXECUTIVE SUMMARY

High Level Findings



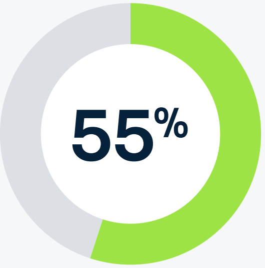
Authentication Priority

Authentication and access management are significant areas of focus, with **84% of respondents placing it among their top 3 or 5 priorities for 2023.**



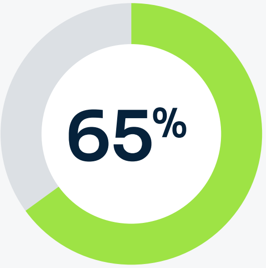
Multiple IdPs

The vast majority of enterprises (76%) reported using multiple identity platforms (IdPs), a situation that – despite high costs and administrative complexity – is a necessary evil to allow for failover, use case requirements, and product innovation.



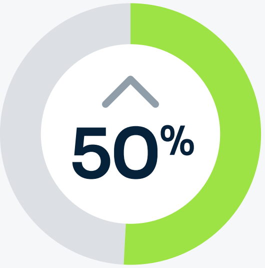
Traditional MFA is Dead

Respondents are concerned about security risks associated with traditional MFA, with **55% worried that relying on SMS texts and phone calls makes them susceptible to cyberattacks.**



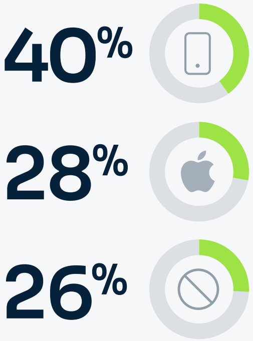
Passwordless Being Embraced

The majority of enterprises **(65%) plan to adopt passwordless technologies in the next 24 months.** Lack of budget, fewer resources, and conflicting priorities hinder faster progress.



Cyber Insurance Trends

Cyber insurance carriers are beginning to mandate the use of new MFA technologies. However, **over half of respondents are not sure or are concerned that they will lose their coverage if they continue with traditional MFA.**



Lack of Device Trust

Device trust is woefully under-used throughout organizations, as only **40% of mobile devices** and **28% of Mac workstations** are enabled, with a whopping **26% claiming not to use device trust at all.** This leaves enterprises vulnerable to attack as a user's digital journey always begins with a device.

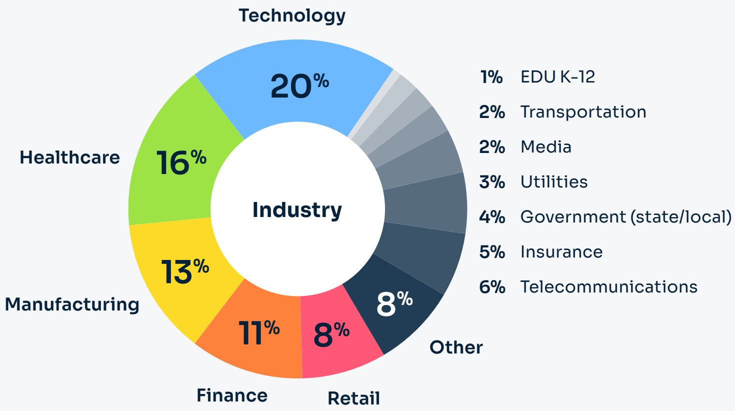
EXECUTIVE SUMMARY

Demographic Overview of Survey Respondents

This report is based on a survey of 285 security and IT professionals working across a range of industries in North America. Overall, we see an even distribution of respondents across company size, titles, and industries.

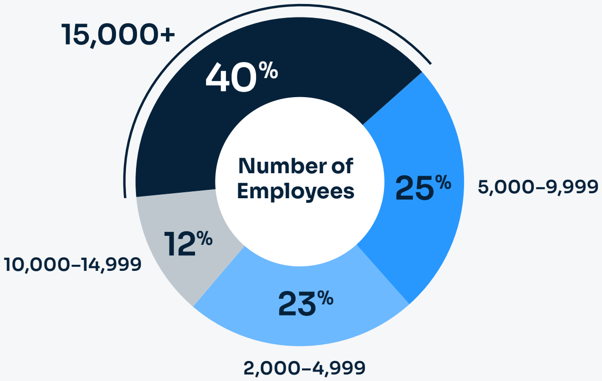
By Industry

We had a diverse breakdown of verticals including 20% work in the technology industry, 16% in healthcare, 13% in manufacturing, 11% in finance, and 8% in retail.



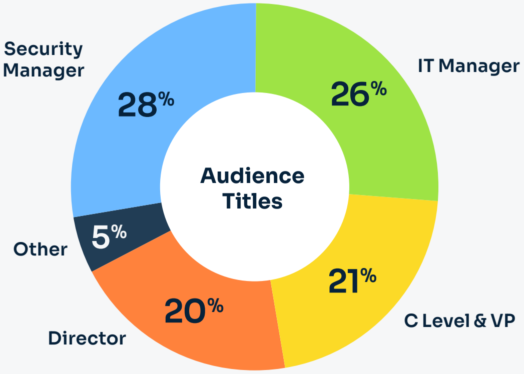
By Company Size

40% of the respondents work in organizations with over 15,000 employees, while 12% work at companies with 10,000-14,999 employees. 25% are at companies with between 5,000 and 9,000 employees, and 23% represent firms with 2,000-4,999 employees.

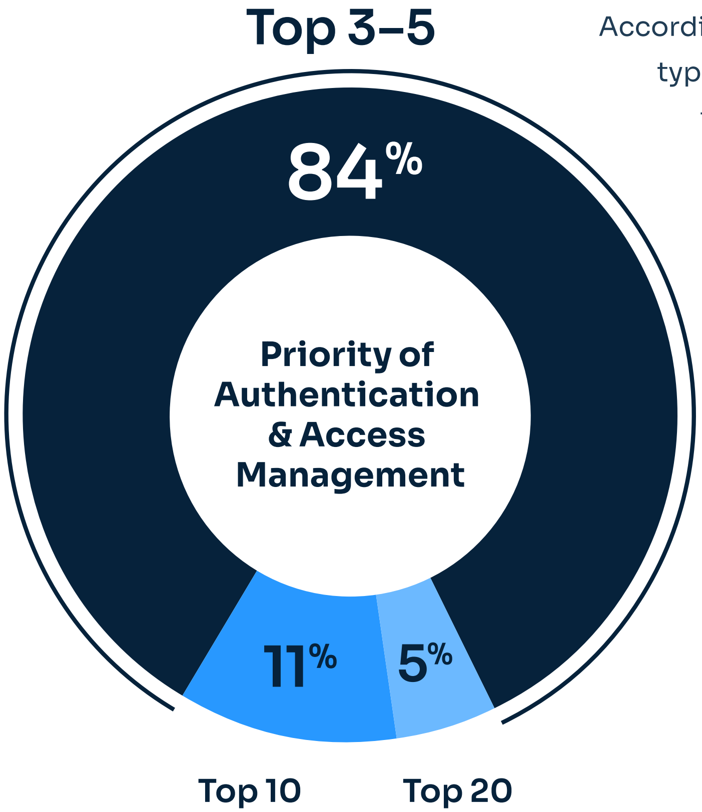


By Title

C-level and VP titles accounted for 21% of the respondents, with 20% being directors. IT Managers at 26% and Security Managers with 28% rounded out the audience.



Authentication Tops Cyber Security



According to the Cyber Resilient Organization Report, organizations typically deploy 45 cybersecurity tools to protect their environments from attack. That's a lot of software and budget dollars.

When asked what their top cyber security priority was, authentication emerged in at least the top 5 for 84% of respondents. This top 3-5 priority is for all cyber security products, not just ones in IAM (identity and access management).

Another 11% placed it in their top 10. A mere 5% put them in the top 20.

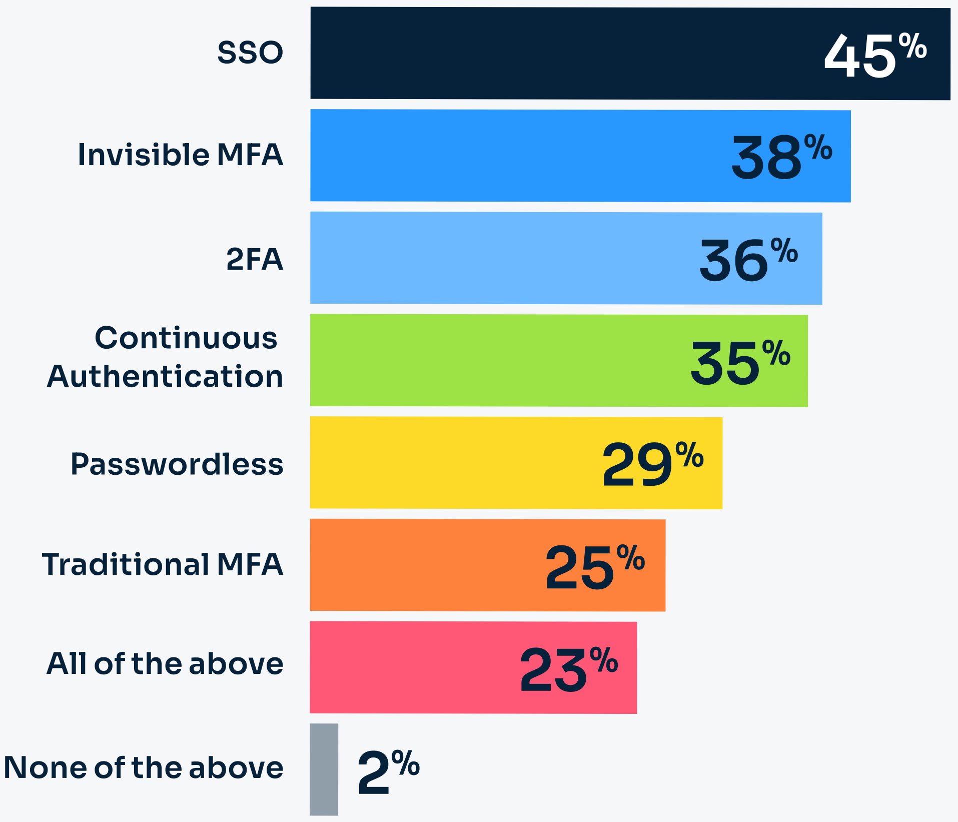
These results demonstrate the importance of authentication and access management for IT and security teams in an extremely crowded market and threat landscape.

Invisible, Continuous & Passwordless Authentication Technologies are Priority

In terms of specific priorities within authentication for 2023, the biggest item on the agenda appeared to be single sign on (SSO), referenced by 45% of respondents as a priority.

However, intelligent/phishing-resistant MFA and risk-based continuous authentication, which are more modern alternatives to traditional MFA, garnered 38% and 25%, respectively.

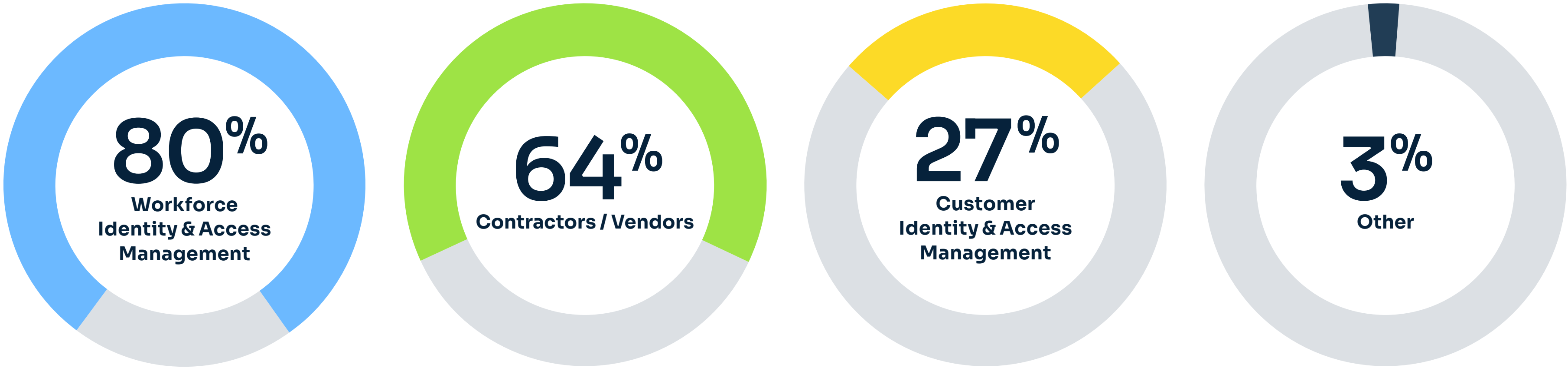
When combined with passwordless technologies, at 25%, **84% of respondents appear to be looking beyond traditional authentication technologies** in the near future.



SURVEY FINDINGS CURRENT IDPS IN ENTERPRISES TODAY

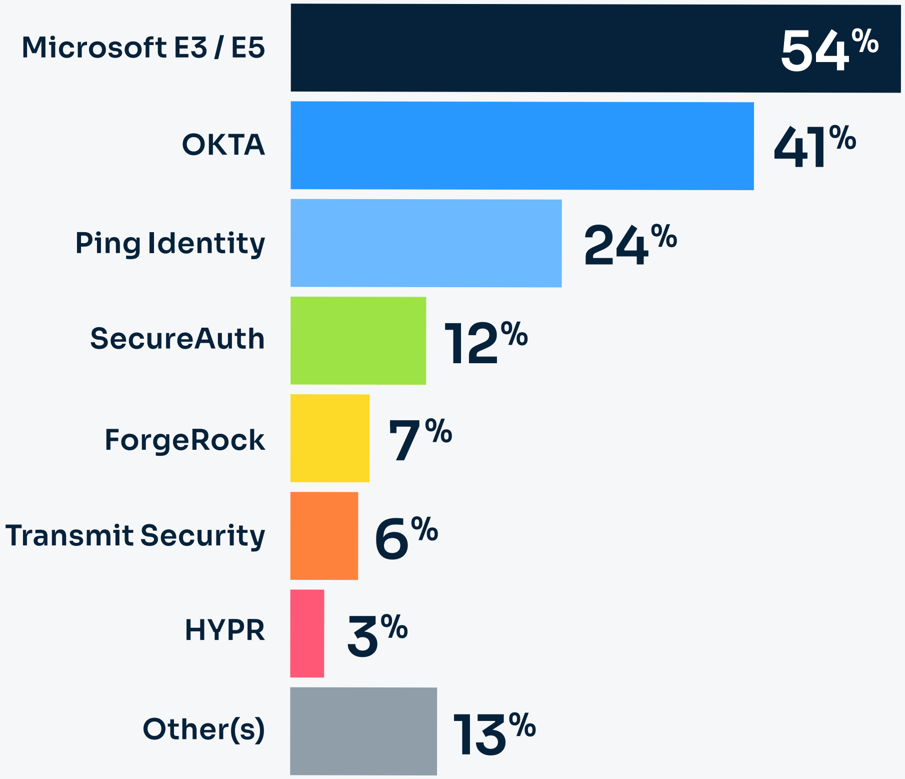
Workforce and Contractors Lead Authentication Use Cases

Survey respondents use authentication solutions for a range of purposes. Workforce access management was the top choice, with 80% of respondents saying this was one of their use cases. Over a quarter use an authentication solution for customer identity and access management, while nearly two thirds put authentication solutions to work managing access for contractors and vendors.



Variety of Authentication Products Are Used

When asked what identity provider products they use, 54% of respondents indicated Microsoft E3 and E5. The next most popular was Okta (41%), followed by Ping Identity (24%) and SecureAuth (12%). The predominance of Microsoft is not surprising, given the pervasiveness of Windows in the corporate world. However, an issue arises when one considers that a separate question in the survey found that 28% of respondents appear to have Mac computers, which are not optimally protected by Microsoft security products.

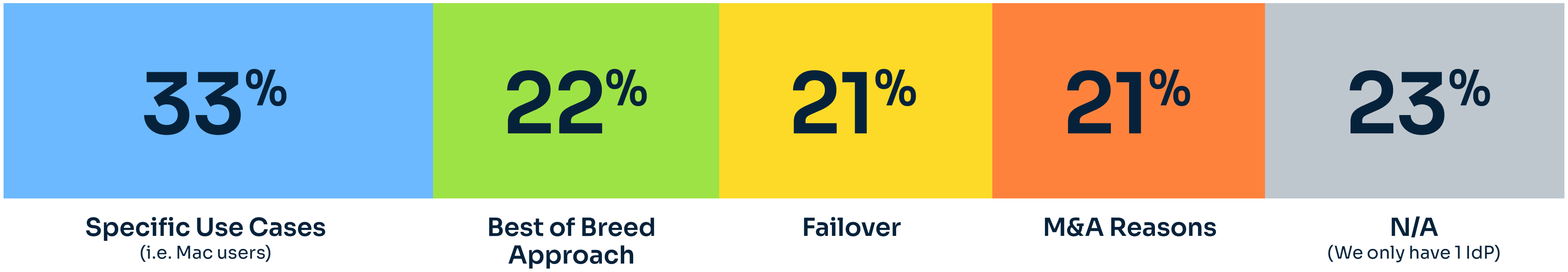


SURVEY FINDINGS **MULTIPLE IDPS EXIST FOR AUTHENTICATION & ACCESS MANAGEMENT**

76% of Enterprises Use Multiple IdPs

Some surprising results showed that many enterprises use multiple IdP products, a trend that bucks the usual consolidation of cyber security tools. 76% of respondents use more than one IdP in their organization. They reported this redundancy due to failover, use case requirements, and preferred best of breed approach reasons. As over 80% of cyberattacks focus on credentials, it makes sense that practitioners need to have a back-up system in case their primary IdP product goes down or is compromised by an attack.

Why do you have multiple IdPs for authentication and access management?

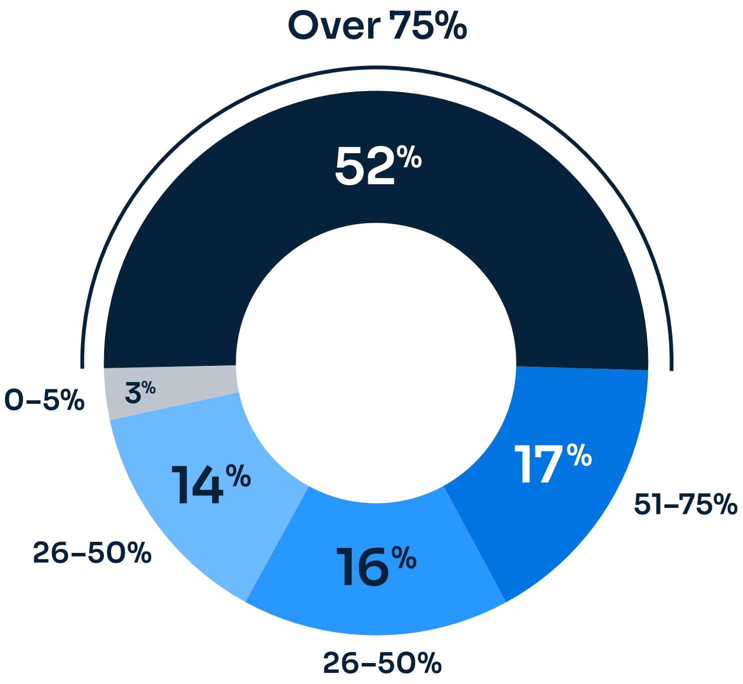


Majority Are Behind the Curve with Traditional MFA

Traditional MFA has users authenticate themselves using verification factors like one-time passwords (OTPs) and personal identification numbers (PINs) transmitted over SMS text messages, emails or phone calls. While these MFA techniques were considered revolutionary when they debuted in the late 1990s, they are increasingly viewed as "better than nothing," but problematic from a security perspective. There have been enough troubling incidents that IT and security professionals view traditional MFA as deficient—a technology that must be upgraded to next-gen secure methods such as passwordless continuous authentication solutions driven by a behavior-based risk engine. In addition to the weaknesses in traditional MFAs from security point of view, they add a lot of friction for users causing productivity issues.

While traditional MFAs are vulnerable, they are better than simple passwords that are super easy to crack. So, it's good to see that a lot of companies have at least adopted the MFA technology. **Over 50% of respondents say that 75%+ of their organizations have deployed MFA.** A further 15% have deployed MFA in 51-75%. Only 3% have MFA in 5% or fewer of their organizations.

What percentage of your organization has deployed traditional MFA?



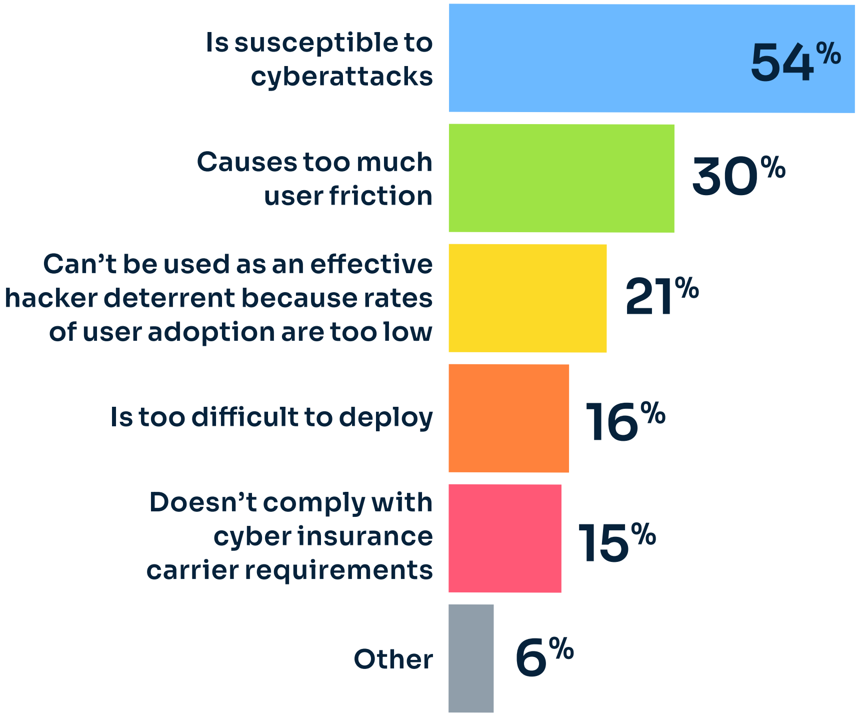
Traditional MFA Methods are Prone to Attack & Cause User Friction

Respondents do have many security-related concerns about traditional or "legacy" MFA. Over half think the technology is susceptible to cyberattacks. 21% feel traditional MFA cannot be used as an effective hacker deterrent because adoption rates are too low.

Within these respondents, interestingly Insurance companies were the most concerned about weakness of these methods against hackers, followed closely by Finance, Healthcare, Retail, and Technology companies.

Besides lack of protection against cyberattacks, friction for users is another big issue. 27% of respondents say that traditional MFA causes too much friction with users.

Do you believe traditional MFA with SMS/phone/KBA type of authentication does the following?

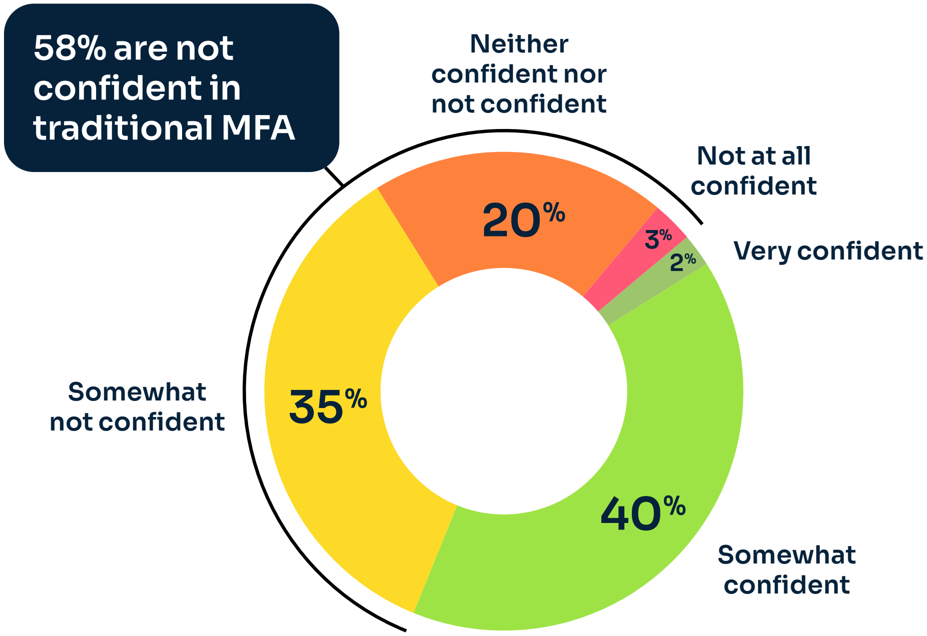


Respondents Not Confident that Traditional MFA Can Thwart Attacks

Most of the respondents lack confidence in using traditional MFAs to thwart credential related cyberattacks. When asked on their confidence level, only 5% are very confident with another 40% somewhat confident. Not a strong vote of confidence for traditional MFAs.

Despite MFA technologies being widely deployed, confidence in using these solutions to help protect the infrastructure is not very high. Not surprisingly, most companies having started initiatives to move away from traditional MFAs to phishing resistant technologies including invisible MFA, passwordless authentication, and other solutions.

How confident are you that traditional MFA is enough to thwart attacks?

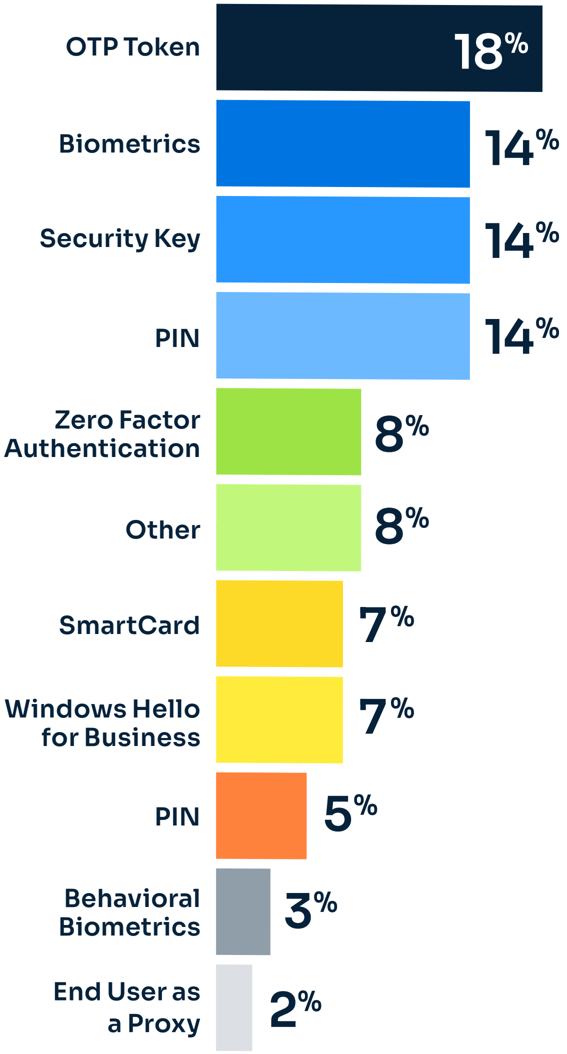


For Respondents Adopting Passwordless Technologies, Most Methods Used are Vulnerable to Attack

In terms of passwordless technology, companies are using various different types of technologies for authentication.

Most respondents picked One-Time-Passwords or OTPs with 38% selecting that as one of the methods. The next most popular passwordless technologies were PINs (27%) and biometrics, which was tied with security keys at 26%. Respondents showed a preference for proven, tangible passwordless solutions like PINs and OTPs over newer, more subjective approaches like biometrics and knowledge factors. Unfortunately, many of these including biometrics are vulnerable with hackers using various techniques to intercept or replicate users' credentials.

Which of the following technologies you are using achieve your passwordless goals?



Passwordless Adoption Hindered by Competing Priorities, Lack of Knowledge and Budget

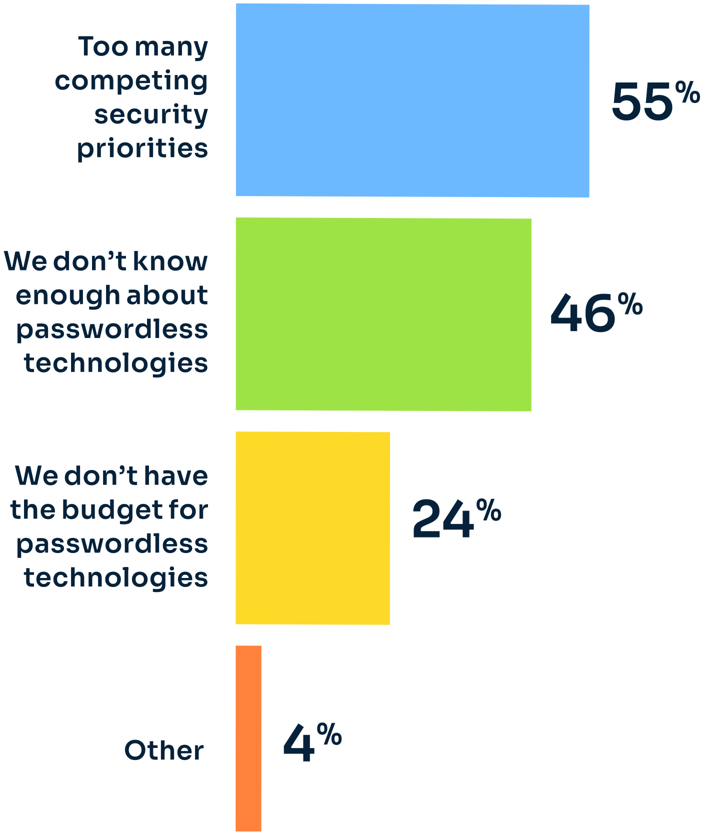
The idea of authenticating users and managing access without passwords is a dream for some in the IT and security fields.

For respondents, while the vision of using next-gen authentication solution to rid the world of passwords is appealing, the reality is a bit daunting.

The survey asked respondents to explain what was standing their way. The top reason was having too many competing priorities (55%), followed by not knowing enough about the technology (46%), and lack of budget (24%).

As more security professionals are getting educated on the importance of passwordless authentication especially when executed on a continuous basis, there seems to be a big momentum towards this type of solution.

If not using passwordless technologies, what has held you back from adopting?



65% Plan on Adopting Passwordless Technologies in the Next 2 Years

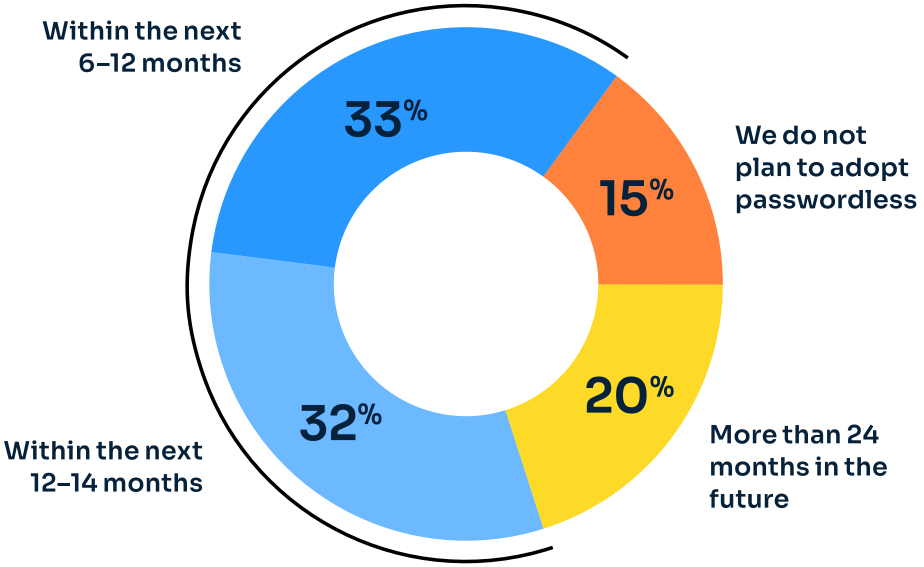
It was very encouraging to see that most organizations are planning on implementing passwordless technologies. Only 15% of the respondents are not ever planning on adopting passwordless technologies.

A whopping 65% are planning on implementing passwordless technologies in the next 24 months. Nearly a third are planning to do so in the next six months, and another third are looking at the 12-24 month horizon. In IT terms, that is also a fairly immediate plan, especially in large organizations.

Looking at specific industries, Technology companies led the group for adoption in 6-12 months followed closely by Government, Manufacturing, Finance, and Insurance.

Although passwordless is a good step, organizations need to look at the next level of the maturity curve with continuous authentication with invisible MFA to eliminate friction and significantly enhance security.

If you don't already use passwordless technologies, what are your plans for adopting them?



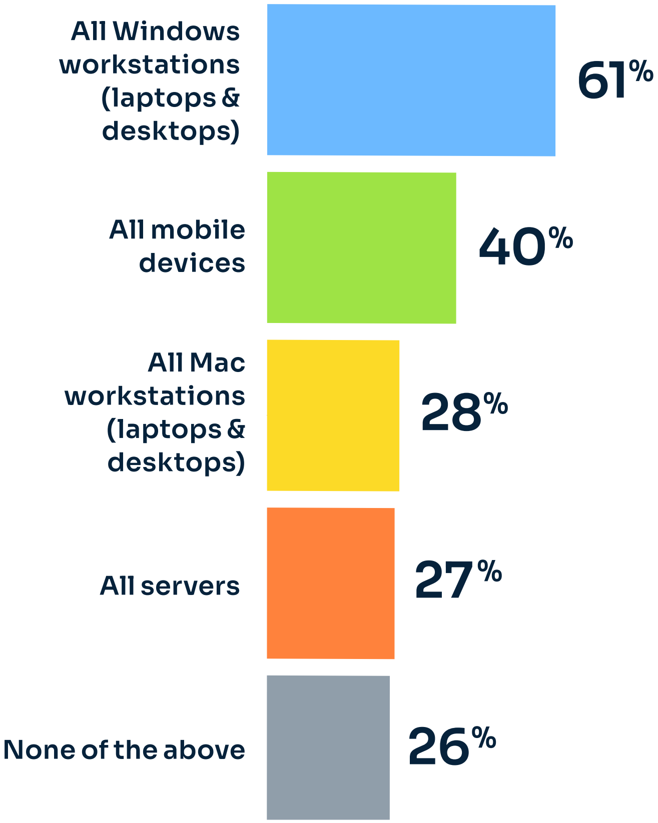
Device Trust Woefully Underused to Aid in Credential Attacks

To implement an effective continuous authentication process, it's important to have Device Trust on end points. Device trust technologies track characteristics of a device that are unique to the user.

The survey probed respondents on where they had implemented device trust technologies. As threats grow more sophisticated and legacy forms of access become more deficient, security managers have recognized that establishing trust with a user's device is critical to preserving a strong security posture. Without device trust, an attacker can penetrate an MFA control before the sign in stage.

Over six in ten respondents have implemented device trust for all Windows workstations. Four in ten have done so for all mobile devices. 28% have device trust for Mac workstations, and 27% have it for all servers. The discrepancy between device trust for Windows versus Mac highlights a difficulty facing security managers.

Where have you implemented Device Trust technologies in your organization?



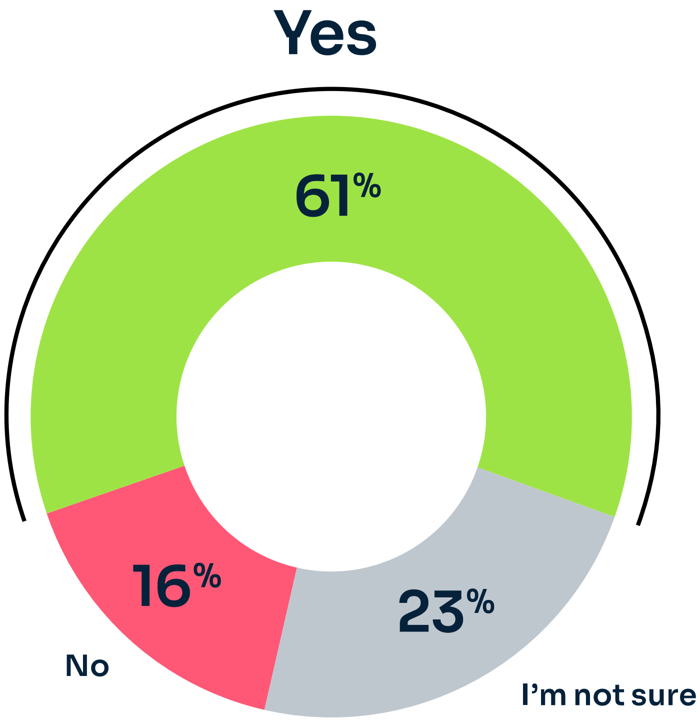
Cyber Insurance is a Priority

Cyber insurance is a high priority for respondents. Asked, “Is cyber insurance a priority for you? (i.e., do you need to purchase/ renew it for your organization?)” 59% said “yes.” Only 17% said “no,” while 24% said were “not sure.” This is not a surprising result. Most businesses are intent on reducing residual cyber risk, and insurance is an effective way to achieve this outcome.

However, getting the right kind of cyber insurance coverage, and the best rates, requires adhering to a range of parameters specified by the carrier. Overall, cyber insurance is getting increasingly expensive while providing less coverage. Organizations that want good coverage and low premiums will need to demonstrate strong controls over authentication and access. This will almost certainly mean the adoption of the latest innovative MFA technologies.

If a carrier deems a prospective policy holder to be deficient in its authentication and access management capabilities, it may deny coverage or insist that the customer improve its authentication and access management before they will underwrite the policy. Indeed, some cyber insurance carriers are starting to mandate that policy holders replace traditional MFA with more advanced and secure techniques, such as device trust-based invisible MFA, behavioral methods, and passwordless technologies.

Is Cyber Insurance a priority?



ABOUT SECUREAUTH

Welcome to Better Identity

We believe more security shouldn't equal more obstacles.

And, with Identity Management solutions from SecureAuth, leading companies worldwide find it easier than ever to create experiences that are as welcoming as they are secure.

Our AI-driven risk engines help you bring dynamic — and often invisible — authentication for your audiences. Making you more effective than ever at eliminating bad actors or incorrect authorizations. While providing your employees and customers the simple and seamless access they deserve.

Make all your authentication user experiences a secure and accessible "front door" to your company.

Visit **SecureAuth.com** to learn how.

SECUREAUTH

ViB

About ViB Research

This vendor-neutral research study was independently conducted by ViB (Virtual Intelligence Briefing) Research.

Respondents are precisely screened and targeted from ViB's community of more than 10M technology practitioners and decision makers who share their opinions by engaging in high quality surveys across IT domains including Identity Management.

ViB's best-in-class survey design and analysis methodology is designed to deliver accurate insights from engaged community members who are motivated to share their experiences for the community's greater good.

The Effective Margin of Error™ is estimated to be +/- 3.7%. Learn more about ViB's research capabilities at vibriefing.news/services/market-research