Delinea

WHITEPAPER

The Future of Workplace Passwords:

Not Dead, but Evolving

Executive Summary

With all the buzz around passwordless authentication, it's easy to believe that passwords are dead and buried. Google, Apple, Microsoft, and the media are driving the vision of an automated sign-in process that's simple for consumers to use and difficult for criminals to crack. It's a compelling proposition, considering how the rise of identity theft and data breaches can be commonly traced to weak or easily stolen passwords.

Much of the story has centered on consumer passwords for websites and apps. But, as we've seen in the past, the adoption of new workplace solutions often trails consumer technology. For example, advances like user-friendly interfaces and one-click installation have set high consumer expectations for technology while many people are still struggling with outdated tools and processes at work.

With this in mind, we set out to understand how passwords are evolving in the workplace. We surveyed 300 IT and cybersecurity leaders across the United States, representing companies of different sizes and industries. They shared their perspectives on passwords' current and future state, including the potential for passwordless authentication.

We found that, to adapt an infamous quote, reports of the death of the password appear to have been greatly exaggerated.

Instead, our results show that passwords are evolving into something new. While passwords may never disappear completely, they will be supplemented by different, better forms of authentication. Password management still has a critical role in workplace security for the foreseeable future.

Read on to learn how:

- Organizations currently manage password risk with a mix of solutions
- Compliance and insurance requirements drive demand for password management
- Companies view the login experience of the future
- Multi-Factor Authentication (MFA), biometrics, and AI are supporting the password evolution
- Legacy tools and enterprise risks require security strategies that passwordless authentication can't solve

Dangers of poor password hygiene

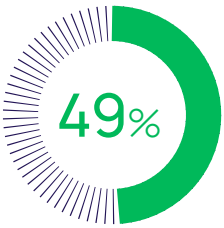
- **Unauthorized access**
  Weak passwords are easily cracked, making it easier for malicious hackers to gain unauthorized access to accounts, systems, and sensitive information.
- **Data breaches**
  Weak passwords can lead to data breaches, where sensitive personal or business information is exposed or stolen.
- **Account compromise/takeover**
  If people reuse passwords across multiple accounts and one is compromised, attackers can use the same password to access other accounts.
- **Credential theft**
  Malicious hackers can use stolen credentials to impersonate people online, potentially accessing financial accounts or committing fraud.
- **Compromised data**
  Poor password hygiene can compromise trade secrets or employee or customer information, leading to financial and legal consequences.
- **Malware distribution**
  Malicious hackers may gain access to accounts to spread malware, using a user's account as a launching pad for attacks on the organization.
- **Phishing attacks**
  Weak passwords make it easier for attackers to trick people into revealing login credentials through phishing emails or websites.
- **Legal and regulatory consequences**
  Some industries and regions have regulations that require strong password policies. Non-compliance can result in legal penalties.
- **Reputation damage**
  A security breach due to poor password hygiene can damage your reputation with partners, customers, and shareholders, and possibly result in lawsuits.
- **Financial loss**
  Significant loss as a result of a security breach is common due to many of the factors outlined above, including hefty penalties, loss of customers, and lawsuits.

Scary workplace-related password stats

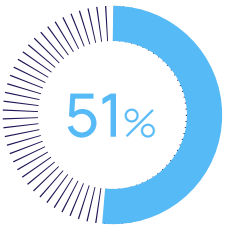
$480

Employers spend **$480 per employee** on time wasted due to password issues.

source: Beyond Identity



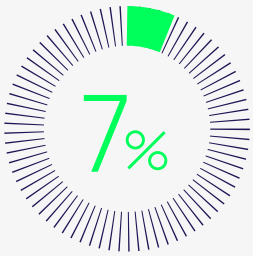
IT security professionals



individuals

49% of IT security professionals and **51% of individuals** share passwords with colleagues to access business accounts.

source: Yubico and Ponemon Institute



If they urgently terminate an employee, **only 7% of IT security and cybersecurity leaders** are extremely confident they can transfer passwords and credentials, terminate access, and maintain business continuity.

source: Bravura Security

1 | Workplace passwords aren't dead, but evolving into something new

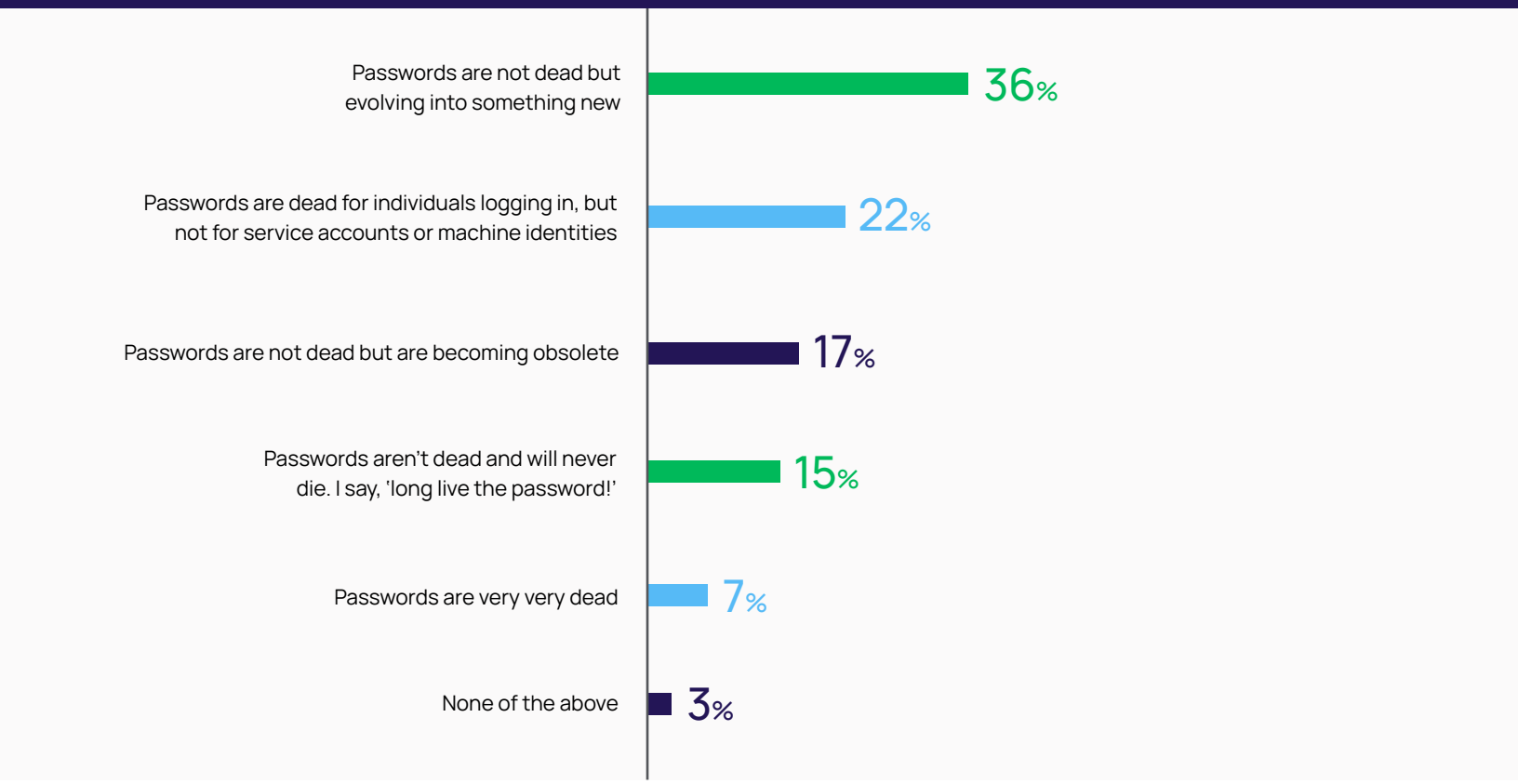
Survey respondents are feeling the winds of change but aren't quite ready to make a move away from passwords.

a. Most say passwords are alive and well

One-third of respondents believe passwords aren't dead but are evolving. On the extremes, a few respondents say they've happily left passwords behind, while several others say they'll never let passwords go.

One in four believe passwords are dead for humans but not for machines. According to Gartner, machine identities are defined as containers, virtual machines, applications, services, along with mobile devices, IoT/OT devices, desktops, and code signing. Machine identities are separate from human identities and are used to establish trust and authenticate with other machines on a network. Considering that the number of machine identities has far surpassed human identities, ensuring these connections are secure is a crucial part of zero trust and identity-first security strategies.

Figure 1 | Which, if any, of the following BEST describes your opinion in relation to passwords in the workplace?



b. Most organizations rely on a mix of password solutions to mitigate risk

The good news is organizations are taking measures to reduce the risks related to poor password management. Most survey respondents have multiple solutions in place.

We found that:

- **Privileged Access Management (PAM) leads the pack.** PAM, which includes functionality such as password management, Role-Based Access Control (RBAC), session monitoring, and reporting, is more popular than simple solutions like password managers, which are primarily designed for consumers.
- Unfortunately, over 50% of respondents answered that their organizations still partially rely on insecure **manual processes such as spreadsheets** for creating, storing, and changing passwords.
- For 43% of respondents, their organizations put the **onus on employees** to manage their own passwords using the tools and methods they prefer. Insider risk increases with this approach, as users are more likely to make mistakes and neglect to follow best practices, resulting in IT and security teams losing visibility and control.

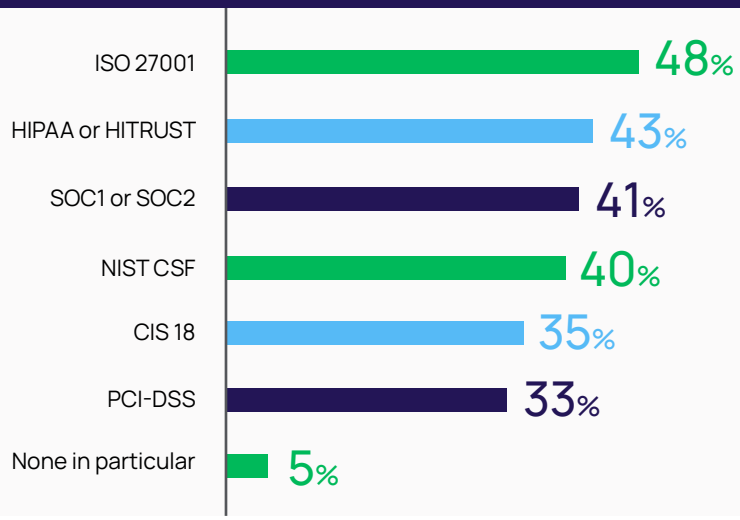
Figure 2 | How, if at all, is your organization currently managing workplace passwords?

c. Compliance and insurance requirements are likely driving demand for password management

Any company assessed by auditors or regulators will need to demonstrate proof of password management controls. We found that 95% of the companies surveyed must meet at least one set of compliance requirements, with many having to meet more than one requirement.

Adapting to passwordless methods while remaining compliant can be complex since so many compliance frameworks call out password management requirements. Auditors are used to looking for observable password-based controls. Even if you remove passwords from your workflow, you'll still need to demonstrate to auditors that you're properly authenticating users and providing them with the appropriate level of access.

Figure 3 | What, if any, compliance frameworks do you currently need to meet?



Compliance governs the password

Common password security practices required by compliance regulations and standards include:

- Implementing strong password policies for complexity and character length
- Enforcing regular password changes
- Implementing Multi-Factor Authentication (MFA) for critical systems
- Storing passwords securely using encryption
- Monitoring and auditing password-related activities
- Conducting employee training on password security best practices

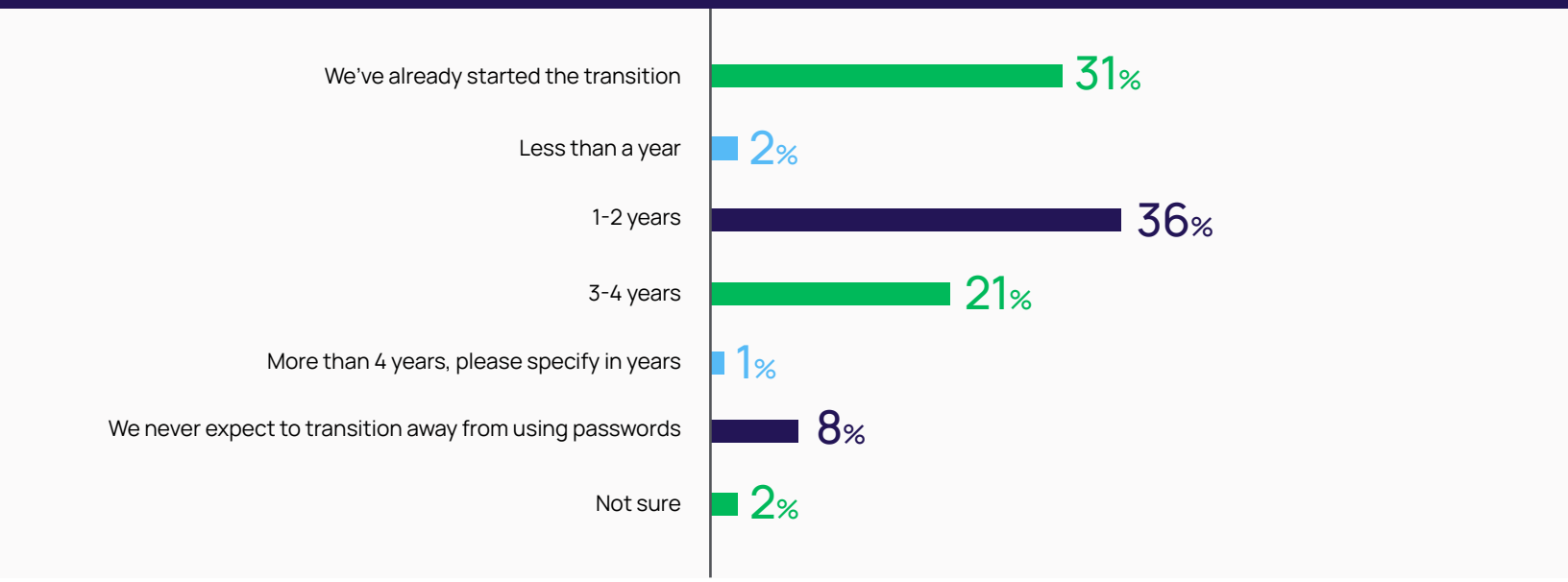
Most compliance bodies offer broad guidance and leave the details to you. Others are extremely specific, namely PCI which increased the character requirements from 7 to 12 in its latest version.

Learn more about compliance and audit requirements at **delinea.com/solutions/security-compliance-audit**

d. Most workplaces are years away from passwordless authentication

Going passwordless doesn't seem to make the priority list for companies right now, perhaps due to competing initiatives and changing economic conditions. While 30% of respondents say they've already started the transition to passwordless authentication, the majority anticipate that they won't begin the transition for at least a year, with some saying three to four years.

Figure 4 | What timeline, if any, does your organization have for beginning the transition away from passwords?



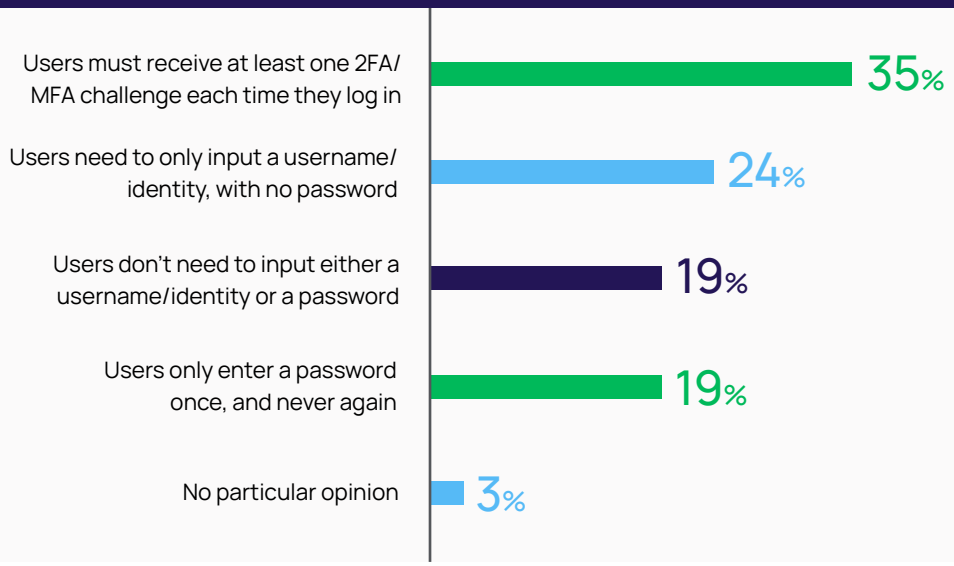
2 | The difference between passwordless experience and passwordless implementation

At the moment, companies seem to have a clearer picture of the passwordless *experience* than how they will proceed with passwordless *implementation*. With a passwordless experience, people authenticate to resources without any shared secret. Even if users aren't required to enter a password, the mechanics of password authentication are still happening behind the scenes. Full passwordless implementation, in which the authentication system doesn't maintain any shared secret at all, is much more difficult to achieve.

a. Expect the user experience to change

In the future, what should you expect when logging into workplace tools? Well, that depends on where you work. For some companies, it may mean a fully hands-off, automated process. For most, it will mean a few more steps for identity verification.

Figure 5 | In your opinion, what best describes the user experience of gaining access to workplace systems without passwords?



b. Hopes are high for biometrics

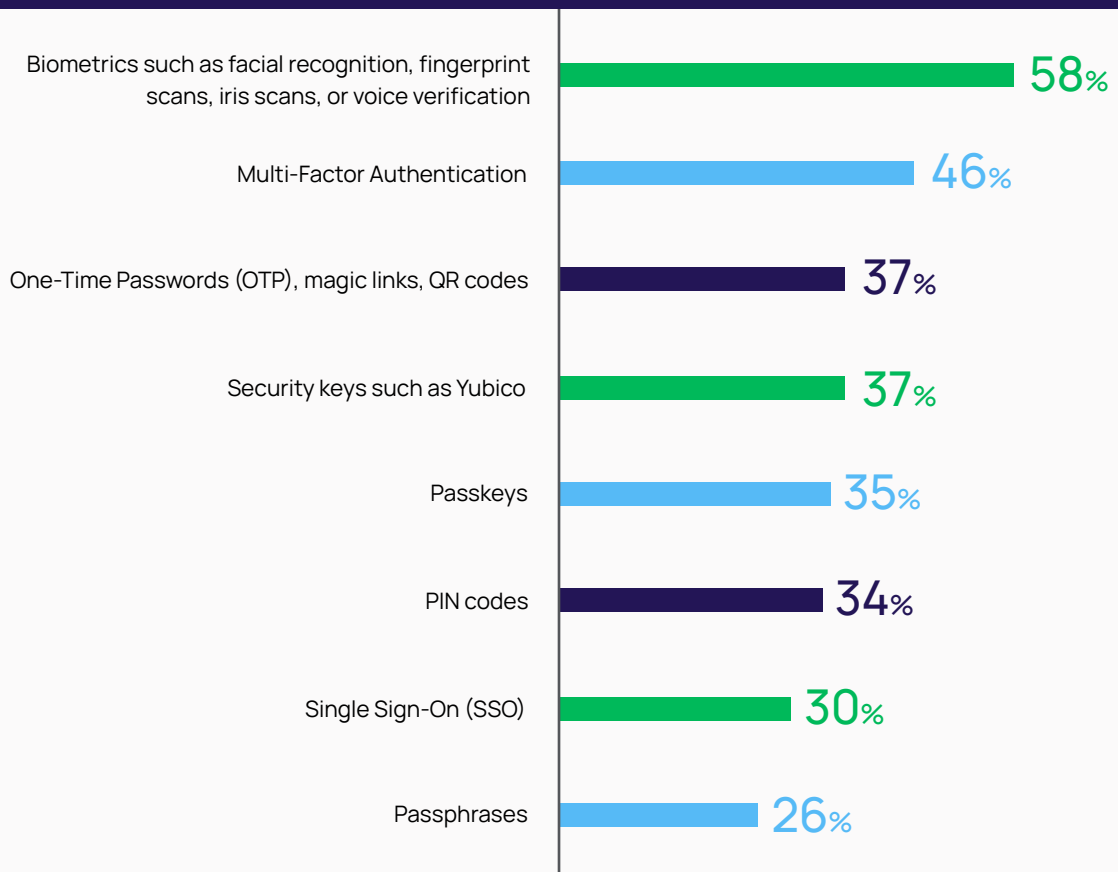
When it comes to technical implementation, there are many potential technical solutions vying to replace or supplement the traditional password. Most respondents expect that biometrics, such as fingerprint recognition, facial recognition, and even behavioral biometrics (e.g., typing patterns), is the way forward.

To make biometric-based authentication a reality in the workplace, software will need to demonstrate a high rate of success. In independent testing, many biometrics currently don't deliver on their promises of accuracy. In practice, each company and software vendor will need to determine how strict or lenient the authentication is to balance ease of use with accuracy.

After biometrics, many workplaces expect to rely on MFA as part of the password evolution, requiring people to confirm their identities with something they have or something they know. It's encouraging news for MFA solutions that have been battling MFA fatigue — in which users push back against additional steps in the login process.

Though FIDO2-based passkeys are the technical solution heralded by consumer tech giants, interestingly, IT and cybersecurity decision-makers didn't rate it as a top solution for workplace authentication.

Figure 6 | What technical solutions, if any, are you replacing/expecting to replace passwords with?

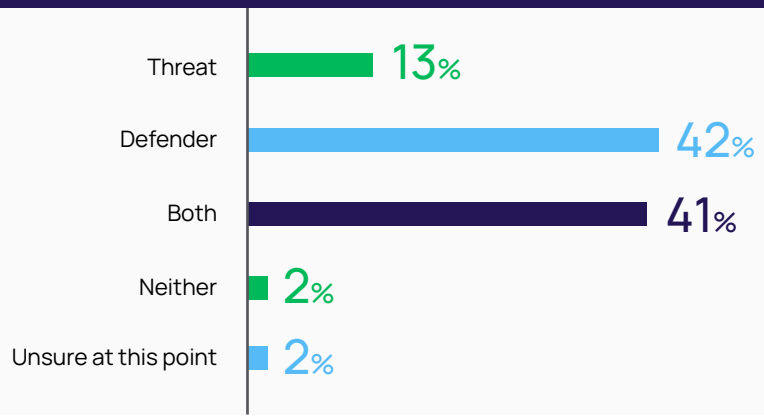


c. More respondents see AI as a defender, rather than a threat

It seems everyone has an opinion about how the explosion of generative AI will impact cybersecurity. On one hand, AI capabilities are making it easier for threat actors to create realistic-sounding phishing emails to snare their victims, and the use of public AI tools in the workplace increases the risk of private information being exposed. On the other hand, AI holds the potential for IT and cyber teams to more easily and accurately detect threats and respond immediately.

In the case of privileged access, more survey respondents see AI as a defender than a threat. This is particularly true for larger companies.

Figure 7 | Do you think Artificial Intelligence is a threat to or a defender of privileged access?

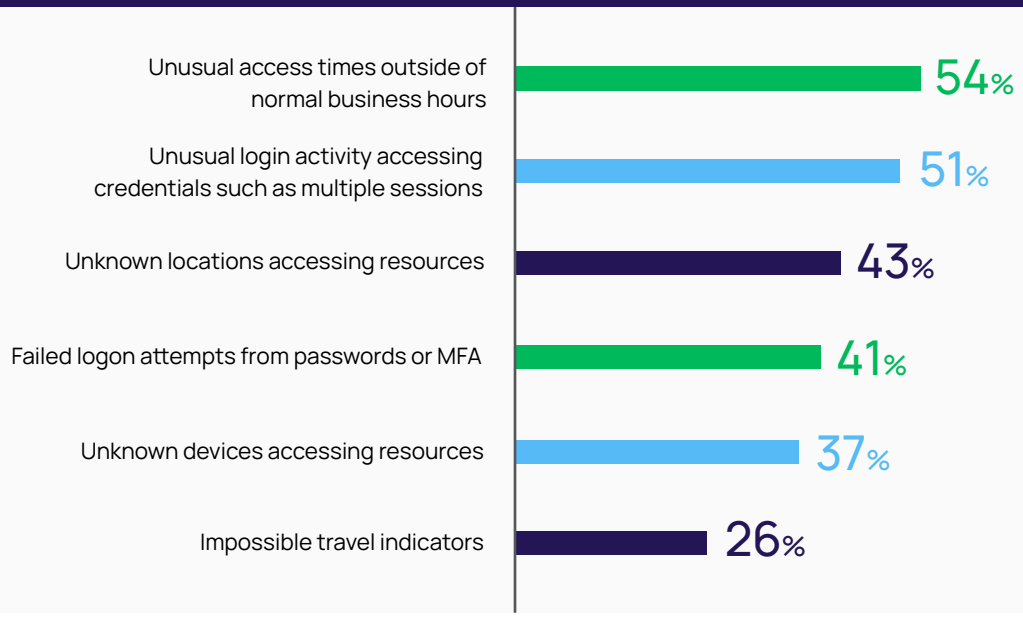


d. Behavioral analytics can identify credential-based attacks

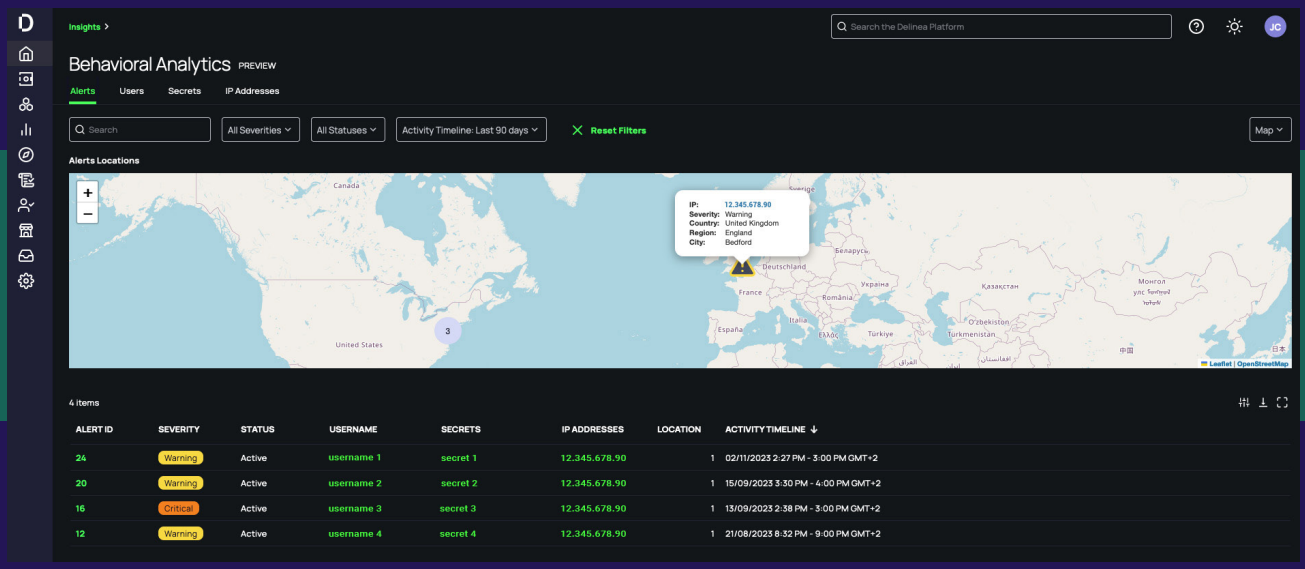
As passwords evolve, risk-averse decision-makers are going to need a safety net. While authentication processes like biometrics and MFA will provide some assurances, nothing is 100%. There will still be cases when unauthorized people gain access.

If that happens, companies need to know the signs of credential-based attacks so they can stop attackers in their tracks. Behavior-based analytics can identify suspicious credential activity and alert security teams to investigate the red flags. Survey respondents say there are many indicators of compromise they would like to know before it's too late.

Figure 8 | What, if anything, are the best ways to help you detect suspicious credential activity?



What Are FIDO2-Based Passkeys?



The emerging standard for passkeys is FIDO2, developed by a consortium of technology companies known as the FIDO Alliance. FIDO2 is meant to make the user authentication process more secure, with a solution that's easy for people to adopt.

- Use of public key cryptography and biometrics make FIDO2 significantly more secure than traditional password-based authentication methods.
- FIDO2 removes the need for users to remember complex passwords and change them regularly.
- FIDO2's design makes it resistant to phishing attacks, as authentication keys are tied to specific websites, and user consent is required for each authentication attempt.
- Users can keep their authentication credentials on their devices and not share them with online services.

FIDO2 consists of two main components:

- **Web Authentication (WebAuthn):** Supported by all major browsers, WebAuthn allows people to use biometrics or external security devices like USB security keys to prove their identity when logging into online services.
- **Client-to-Authenticator Protocol (CTAP):** External security devices interact with a user's computer or mobile device during the authentication process, ensuring that private keys are stored securely and never leave the security device

3 | The password evolution won't be smooth

Compared to consumer technology, workplaces have more complex requirements and decision-making processes that are tied to password-based practices. IT and cyber decision-makers need to consider not just the cost of purchasing new tech, but also the change management aspects of technology and process adoption, especially as their organizations grow.

a. Legacy tech slows the pace for password evolution

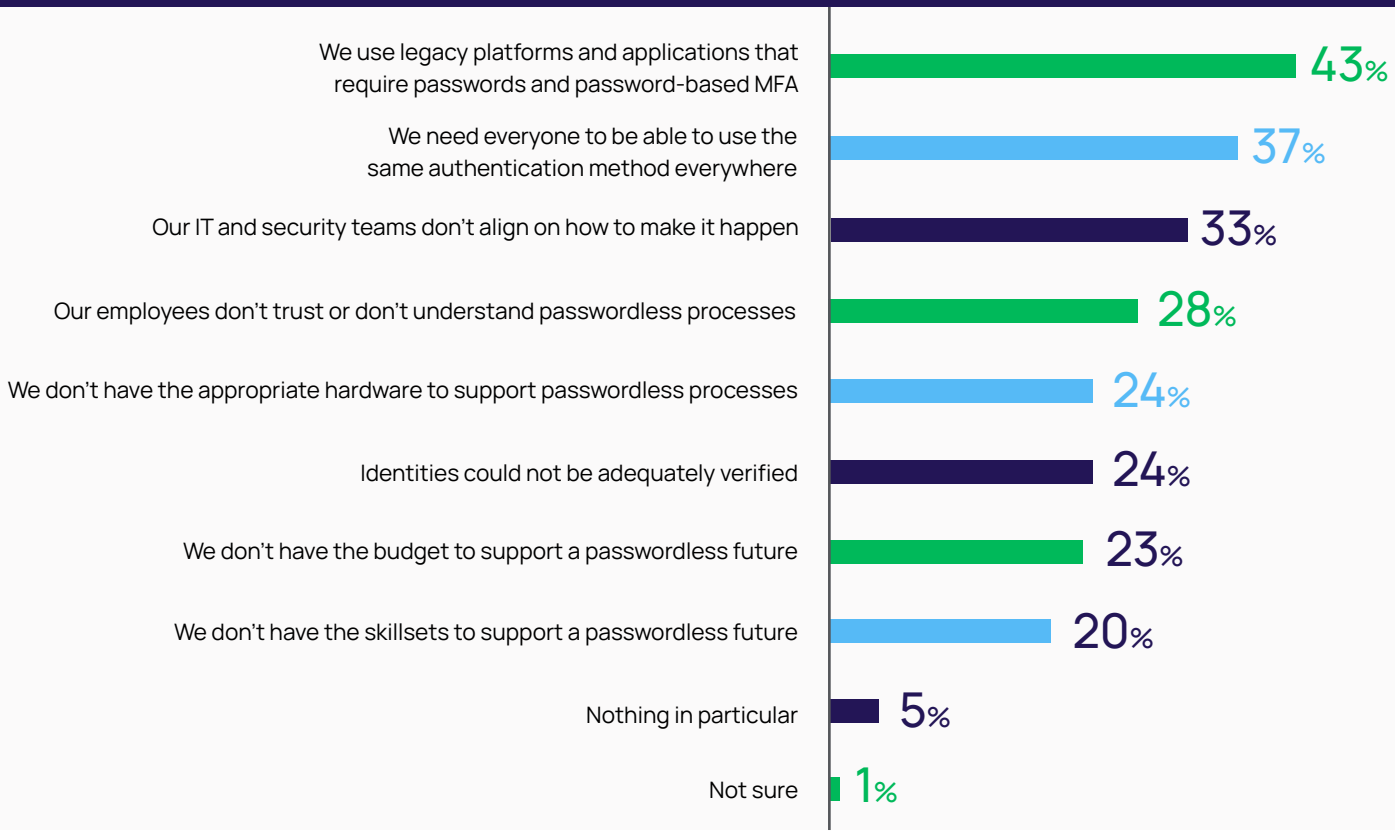
In the case of passwordless authentication, we found that resources aren't a problem for most of the companies surveyed. Most respondents believe they have the skills and budget necessary.

Respondents say that legacy technology, as well as the need for consistent processes that can be governed across an organization, are defining the pace of password evolution. Legacy technology and processes are holding back the race to passwordless authentication. Organizations often become dependent on specific vendors or technologies, which can limit flexibility to change processes. These legacy systems and applications may not have the necessary infrastructure or APIs to integrate with modern passwordless solutions.

Ensuring a consistent user experience across various devices and operating systems can be challenging because passwordless authentication methods may not be compatible with all devices and platforms.

Synchronization problems are real. With users bringing their own devices, it may be difficult to verify identities for users across systems.

Figure 9 | What, if anything, do you believe stands/would stand in the way of your workplace going passwordless?



b. Passwordless authentication isn't a silver bullet security solution

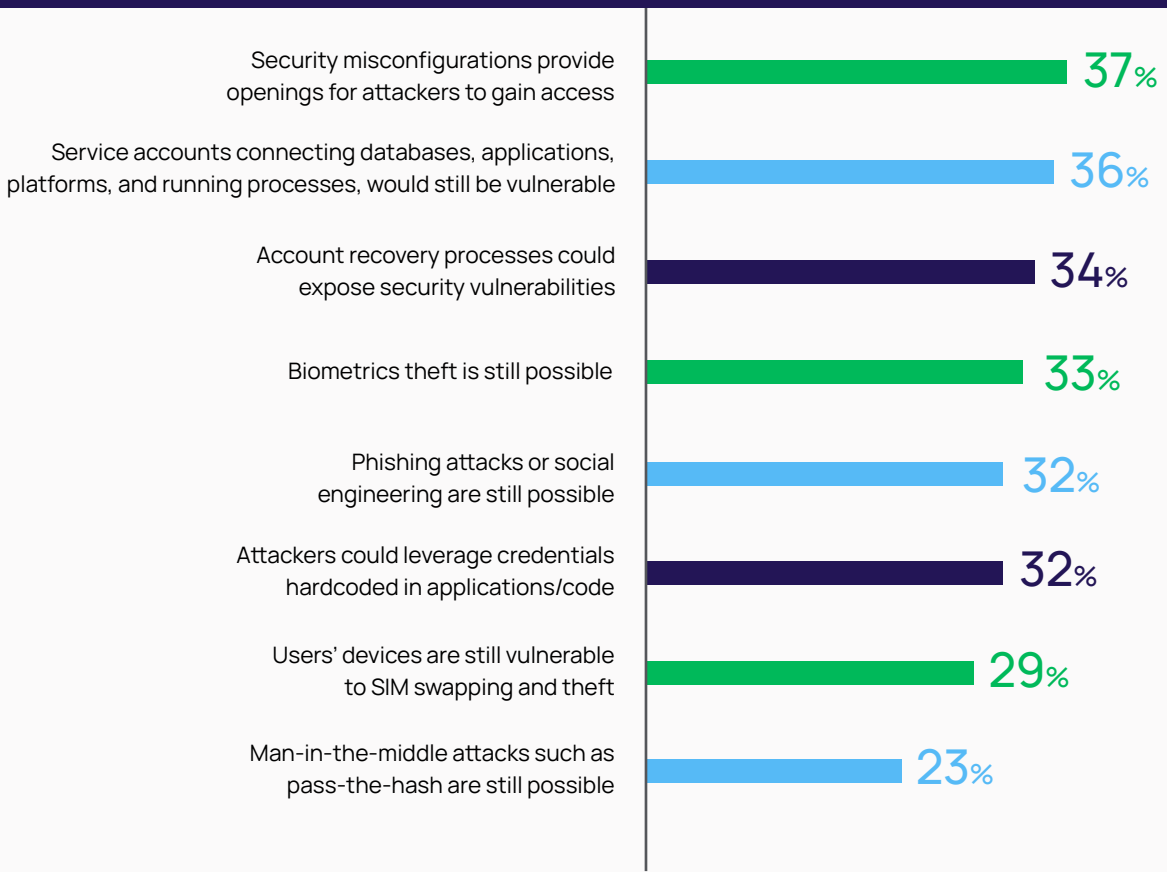
While passwordless authentication can mitigate some types of attacks, such as password cracking and credential stuffing, IT and cybersecurity leaders recognize many critical security challenges it won't solve.

Human error is still a concern. Survey respondents are most worried about misconfigurations leading to unauthorized access, for example an S3 bucket that is left open and accessible to all.

In addition to humans, respondents are concerned about machines. Machine identities and service accounts often rely on passwords and other poorly understood or documented authentication mechanisms. If one of those mechanisms breaks due to a change in the authentication process, critical business operations may fail.

These risks will require security resources and attention, regardless of the password evolution path companies choose.

Figure 10 | If users no longer had to use passwords, what, if any, top security risks do you believe your organization would still face?



Conclusion and recommendations

The results of this survey demonstrate that workplace password management practices are evolving, even though organizations haven't yet radically moved away from traditional passwords. We expect automated solutions for managing passwords will continue to play a critical role in the security landscape for some time and become especially important as they layer controls for authentication, access, and enforcement.

As consumer technology brands and the FIDO Alliance create demand for passwordless authentication, companies are bound to hear that employees expect the same type of seamless experience at work. As biometrics become more accurate, legacy technology gets replaced, and Artificial Intelligence creates a stronger safety net, enterprises will likely become more comfortable with a passwordless future.

You can take steps today to prepare so that your organization's technology ecosystem and workforce are ready for the password evolution.

#Deletethesheet

If your organization is like most and still using passwords, make sure to store them in an encrypted password vault, instead of spreadsheets and sticky notes. Don't put the onus on people to choose their own password management process. You'll end up with inconsistent, manual processes that leave passwords and privileged accounts unmanaged and vulnerable to attack. Transition to an automated process that enforces unique, complex passwords, limits password sharing, and rotates passwords regularly and unexpectedly.

Increase trust in authentication

Implement Multi-Factor Authentication (MFA) throughout the access chain from the moment of initial login to privilege elevation. Risk-based authentication responds adaptively to changes in state. For example, you can move to a heightened monitoring state at risky moments, such as reorganizations and layoffs. Continuous authentication monitors user behavior throughout a session. Access can be revoked if suspicious activity is detected, or additional verification can be required.

Manage access, not just passwords

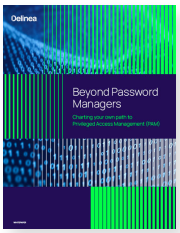
Privileged Access Management (PAM) solutions offer a higher level of security than password managers. In addition to securing passwords and other secrets in a central vault, they include granular access controls. Instead of standing, broad access, users receive just-in-time, just-enough access based on their roles or responsibilities.

In addition to password vaulting, PAM provides extensive monitoring and auditing capabilities. This helps detect and respond to security incidents, as well as aids in compliance with regulatory requirements. PAM solutions can identify suspicious or anomalous privileged activities in real-time and trigger alerts or automated responses, helping you proactively address potential security threats.

Improve cyber awareness

Even if you have all the right cybersecurity solutions in place, it's still critical to invest in education and training to ensure that employees understand the importance of protecting credentials, verifying identities, and managing access. With the proper education and practical training, employees can evolve from the weakest link in the cybersecurity chain to a positive driving force.

Related resources



Beyond the Password

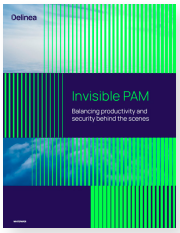
See why consumer-grade password managers aren't sufficient to protect privileged accounts in the enterprise.

delinea.com/resources/password-managers-to-privileged-access-management

MFA Everywhere

Just because someone can present the correct password doesn't guarantee they are the user you think they are. Multi-Factor Authentication (MFA) mitigates risk throughout the chain of access control points.

delinea.com/resources/verify-privileged-users-with-mfa-everywhere-whitepaper



Invisible Privileged Access Management

Reduce password fatigue and empower happy employees. With native integrations, Privileged Access Management sits behind the scenes and synchronizes all privileged identities, roles, permissions, and activities.

delinea.com/resources/invisible-pam-whitepaper

PAM for Dummies

A fast, easy read to get up to speed on privileged access management and security basics.

delinea.com/resources/privileged-access-management-for-dummies-pdf

FREE TOOL

Weak Password Finder: See how easy it is to crack weak AD passwords and take action to protect them.

delinea.com/resources/weak-password-finder-tool-active-directory

FREE TRIAL

Try the industry-leading PAM solution, Secret Server, free for 30 days.

delinea.com/products/secret-server#trial

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**