

2023

The State of Authentication Security

Real-World Insights & Best Practices for Password Management



Introduction

Authentication security remains a cornerstone of any cybersecurity strategy, yet it is an area fraught with challenges. With increased sophistication in cyber threats, an expanding attack surface, and a growing number of vulnerabilities, organizations are grappling with ensuring secure and user-friendly authentication. Despite the emergence of advanced practices, there are still significant gaps where traditional methods must still be fortified, particularly in password-based authentication.

This survey set out to explore these challenges, to identify common practices, and to provide insight into how organizations can bolster their defenses. Based on responses from 483 cybersecurity professionals, the survey offers fresh insights into the state of authentication security in today's organizations.

Key findings from the survey include:

- **Current Authentication Practices:** The survey reveals that usernames and passwords are still the most prevalent authentication methods for organizations. Nearly 70% of organizations are still relying on username and password combinations for their employees and only 50% have adopted software tokens, such as one-time passwords, following cyberattacks.
- **Authentication-Related Cyberattacks:** A combined 47% of cyber attacks were focused on password credential vulnerability, using password spraying, credential stuffing, and brute force attacks. This will only continue to grow, as both the Verizon DBIR Report and the IBM Cost of a Data Breach Report find that compromised credentials are the top cause of a data breach.
- **Security Incidents & Impact:** Unauthorized access to systems impacts businesses significantly, causing reallocation of IT resources for incident response and remediation (28%), system or service downtime (26%), increased helpdesk workload (24%), and data breaches or leakage (22%), all resulting in significant financial loss and additional IT workload for businesses.
- **Password Management:** Most organizations still follow older password management strategies. 74% of organizations continue to require forced password resets every 90 days or less, generating a burden for employees. Periodic password reset is something organizations can eliminate for better security and to align with NIST to follow updated password policy recommendations.
- **Security Awareness & Standards:** Organizations are still learning about the updated NIST Guidelines for authentication. 54% learned about it less than a year ago and 33% are still unaware of the updated password recommendations.

This research was made possible through the support of Enzoic, a leading provider of authentication security solutions. Their invaluable support has enabled us to explore this crucial topic and provide actionable insights to organizations striving to improve their cybersecurity posture.

We believe the results of this survey offer a comprehensive overview of the state of authentication security today and that readers will find this report insightful and practical in their pursuit of stronger authentication security measures.

Thank you,

Holger Schulze



Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS



State of Authentication Security

An abstract graphic consisting of several concentric, semi-transparent circular bands of varying shades of gray, centered in the lower half of the page.

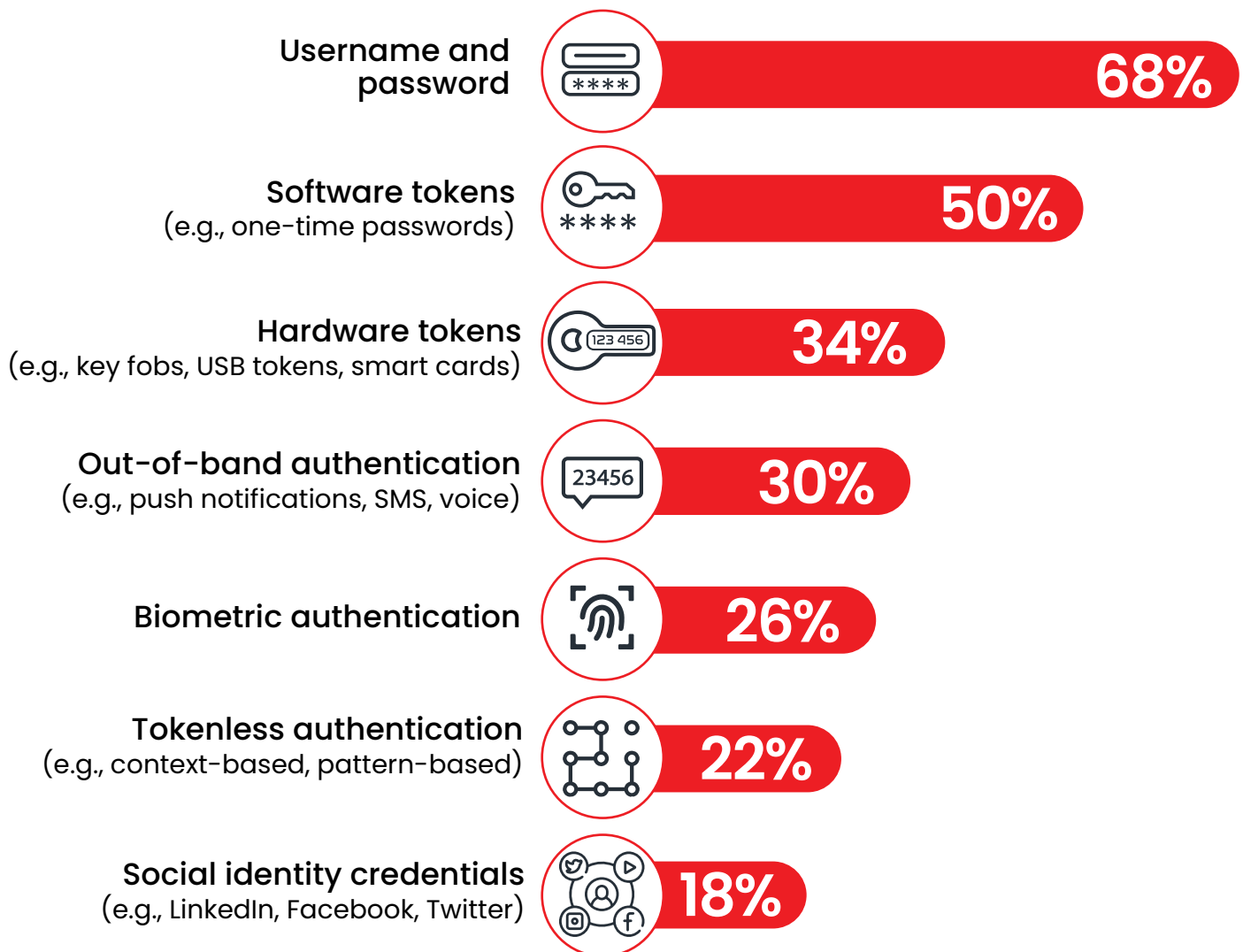
Compromised Passwords Can Weaken Authentication

Adopting secure authentication methods is crucial for maintaining robust cybersecurity and usability. The predominant authentication method, used by 68% of organizations, is the traditional username and password. The next most popular methods involve software tokens, such as one-time passwords (OTPs), used by 50% of organizations, hardware tokens (34%), and out-of-band authentication such as push notifications (30%). The low adoption rate of 26% for biometric authentication among organizations might reflect concerns regarding its reliability and the necessity for backup methods.

To best protect their digital assets, organizations that use the predominant authentication method, passwords, must prioritize updating practices to reflect more modern password policies. Multi-factor authentication (MFA) can be a compensating control, but is intended to enhance, not replace, strong password measures. By closely monitoring the dark web and eliminating exposed credentials used in your environment, organizations can effectively guard against a common entry point for attackers.

► Which authentication methods does your organization employ?

Multiple answers allowed

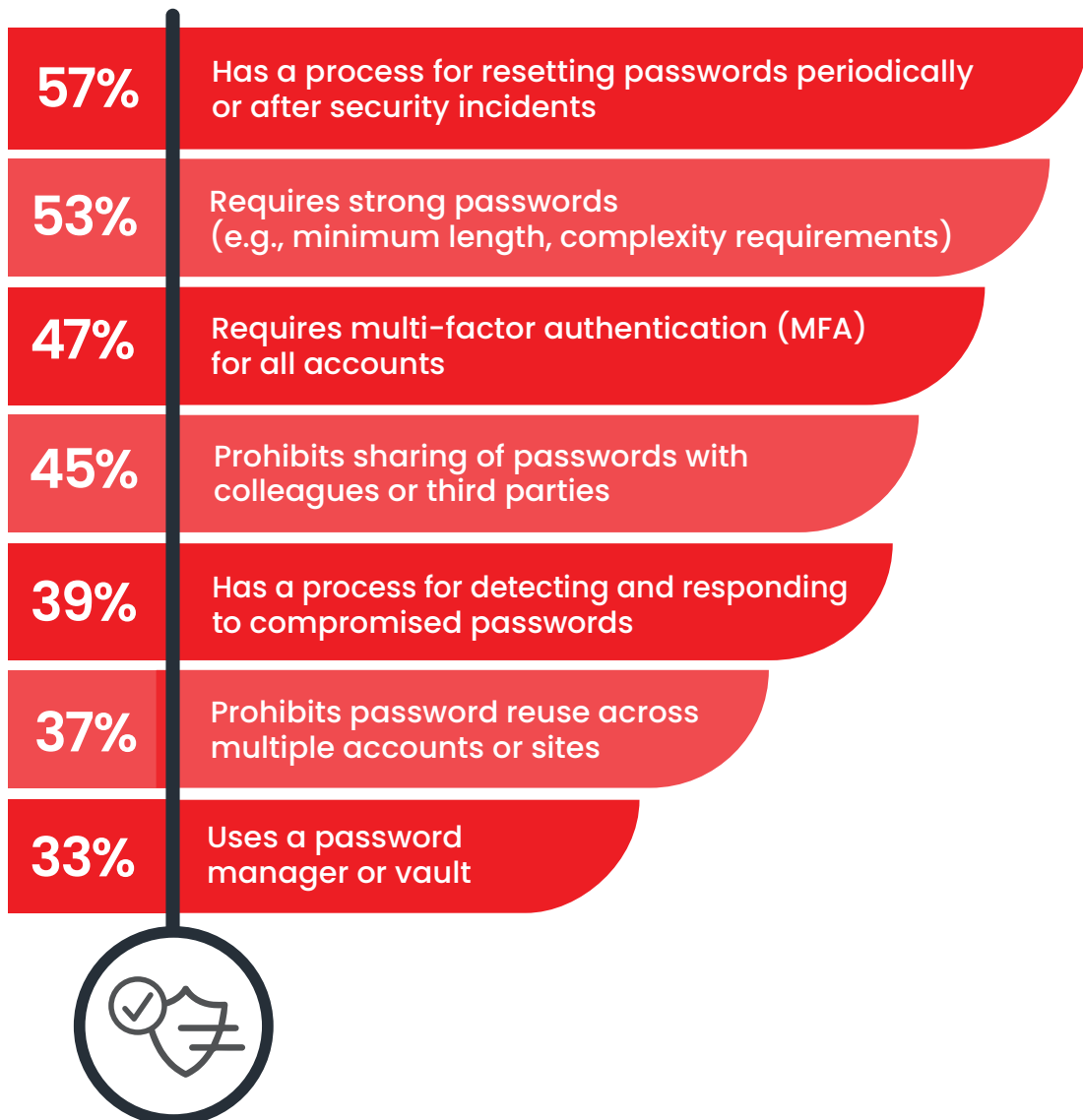


Authentication Policies

Authentication policies play a vital role in securing an organization's digital assets. A defense-in-depth strategy should encompass a range of measures, from effective password requirements to multi-factor authentication (MFA). Among survey respondents, the most implemented policy measures include a defined process for resetting passwords periodically or after security incidents (57%), requiring strong passwords (53%), and requiring MFA for all accounts (47%). However, less than half of organizations (39%) have a process for detecting and responding to compromised passwords, which is an essential part of an effective authentication policy.

These results highlight that organizations should prioritize comprehensive authentication policies that go beyond basic password rules. For example, using services to enhance the ability to detect and respond to compromised passwords in combination with additional security layers.

▶ Which of the following elements are part of your organization's authentication policy for passwords and other shared secrets?



Password Management Effectiveness

Secure password management provides a crucial foundation for securing IT environments. This involves creating and implementing strong password policies, monitoring adherence, and responding quickly to incidents.

While 53% of organizations believe their password management practices are very effective, implementing password policies and controls that meet or exceed industry best practices, a significant 45% consider their practices to be only somewhat effective, acknowledging areas for improvement and minor incidents. Just 2% find their practices ineffective, highlighting the need for continuous improvement in this domain.

Organizations should strive for best-in-class password management, implementing strong policies and investing in solutions that strengthen these controls. Tools that automatically check for compromised credentials can significantly enhance these practices. Regular audits and adjustments to password management best practices, based on industry developments and standards, should also be part of an ongoing cybersecurity strategy.

▶ How effective are your organization's current password management practices?



53%

Very effective:

The organization has implemented password policies and controls that meet or exceed industry best practices, and has not experienced any major security incidents related to password management.



45%

Somewhat effective:

The organization has implemented some password policies and controls, but there are areas for improvement. Password-related security incidents have occurred, but they have been relatively minor and were resolved quickly.



2%

Not effective:

The organization has either not implemented any password policies and controls, or the ones that are in place are not effective at preventing security incidents. The organization has experienced multiple security incidents related to password management, which have resulted in significant harm to the business.

Rise in Helpdesk Requests

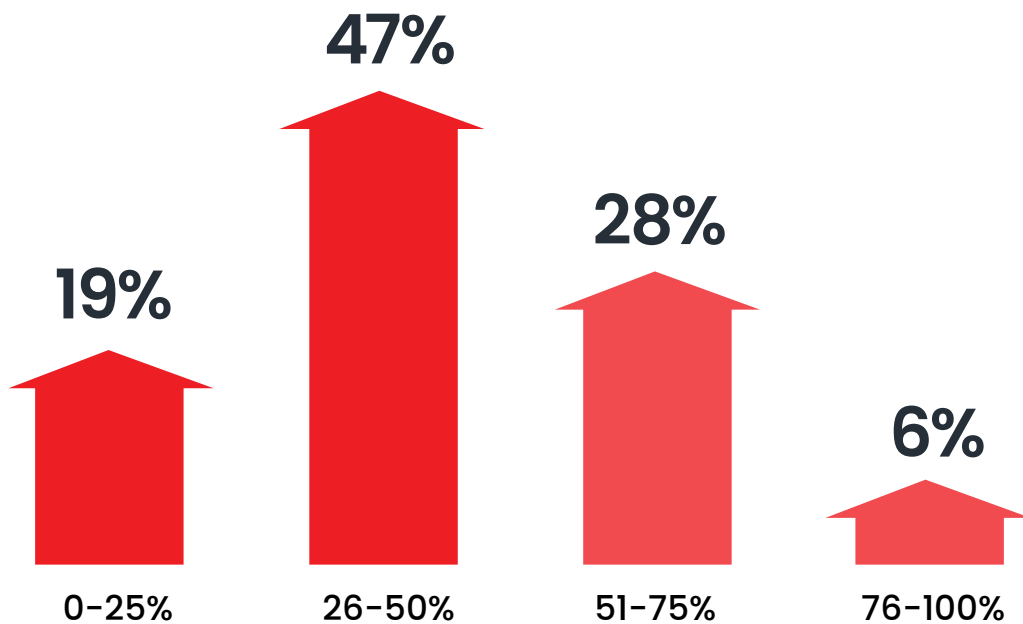
Password resets and hardware security key issues are common helpdesk requests, yet they can become a drain on IT resources and can impact user productivity. The survey reveals a notable increase in such requests compared to the previous year. Most organizations (66%) experienced up to a 50% increase in helpdesk requests, while a third (34%) saw an even higher rate of growth in support requests.

To reduce the burden on helpdesks and the negative impact on user productivity, organizations should consider implementing self-service password reset tools and offering comprehensive user training. The requirements of NIST 800-63b, which advise against imposing password complexity requirements and advocate for removing periodic password resets in favor of only mandating resets when compromised credentials are detected, also play a pivotal role in this. According to Forrester Research, the average password reset costs \$70 in helpdesk labor, highlighting the cost savings of embracing a contemporary password policy. By adopting the NIST guidelines, organizations can see a dramatic reduction in helpdesk calls while improving account security.

► Compared to the previous year, what is the estimated increase in your helpdesk requests for password resets or hardware security key issues this year?

66%

experienced up to a 50% increase in helpdesk requests



Percent increase in helpdesk requests

Time-Based Password Changes

Regular password changes have traditionally been used to maintain security by ensuring even compromised passwords are only valid for a limited period. However, the practice is increasingly being questioned due to user behavior and the rise of other security measures.

Three quarters of organizations (74%) require password changes every 90 days or sooner. A quarter (26%) require changes every 180 days or longer. Notably, no organization reported that they do not require time-based password changes. Historically, routine password changes were the norm, often advised as a method of strengthening security. However, a paradigm shift has occurred within contemporary cybersecurity frameworks.

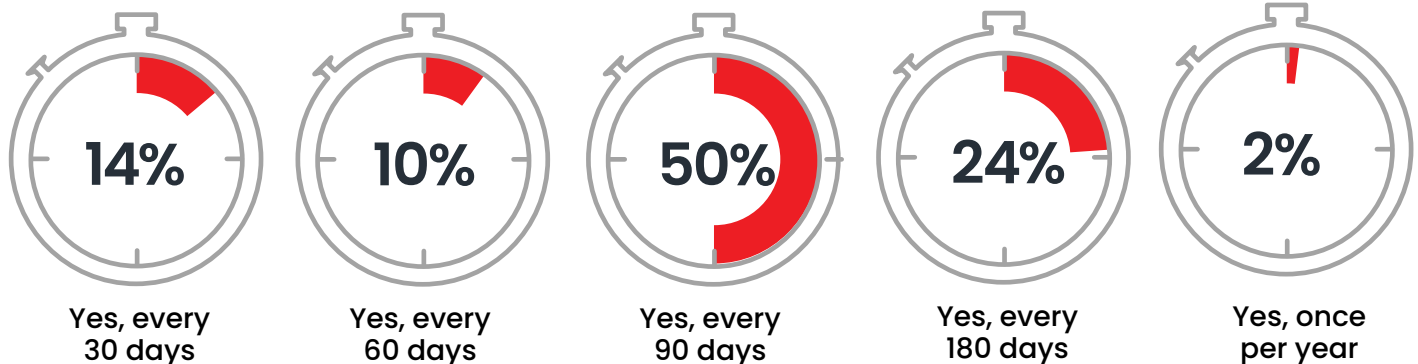
Companies aiming to align with the most recent regulatory frameworks should be aware that current recommendations lean away from routine password resets, as these have been shown to promote poor password practices for users. Instead, the focus is on changing passwords for compromised accounts. For enhanced user experience, security, and cost-efficiency, it's important to reconsider periodic password resets.

With account security evolving, organizations should now explore a more comprehensive approach. While periodic password changes were believed to mitigate certain risks, they inadvertently encourage detrimental user behaviors, such as creating incremental or weak passwords. To truly fortify account security, organizations are encouraged to adopt security strategies such as checking passwords against lists of known compromised credentials.

► Does your organization require time-based password changes?

74%

of organizations require password changes every 90 days or sooner



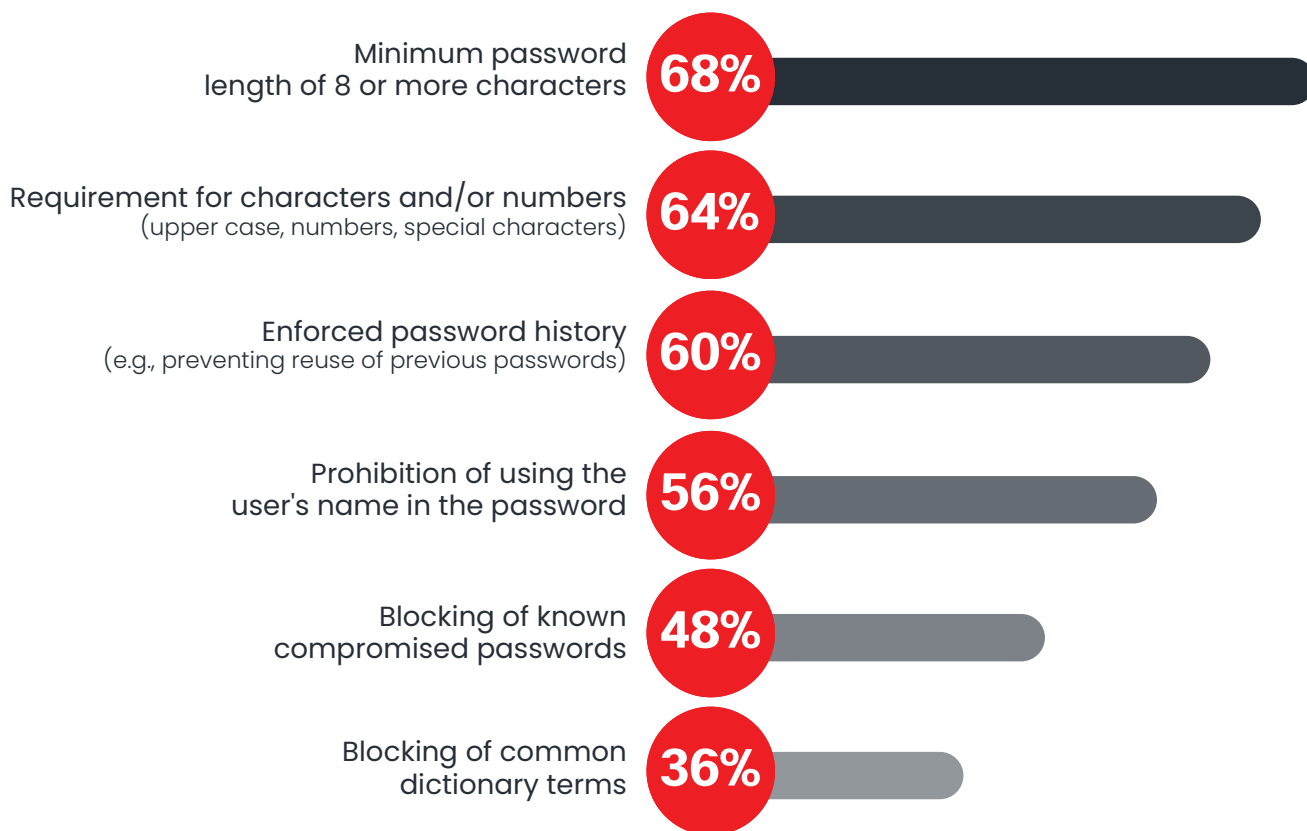
Enforcing Password Requirements


Password requirements are a cornerstone of a robust authentication policy. They encourage the use of strong, hard-to-crack passwords, thereby reducing the risk of unauthorized access. The survey shows that most organizations enforce a minimum password length of 8 or more characters (68%), requirements for use of characters and/or numbers (64%), or prevention of previously used passwords (60%). Still, only 48% block known compromised passwords, and just 36% block common dictionary terms, suggesting a gap in their password security measures.

The emphasis on password complexity becomes moot if compromised account credentials are not addressed first. For a truly robust authentication policy, organizations need to shift their focus from merely enforcing password requirements to actively identifying and preventing the use of exposed and predictable passwords. This proactive approach ensures that even if users comply with all password requirements, their credentials are not already available to potential adversaries or easily guessable through rudimentary attacks.


Many organizations are following older password policies and less than half are checking for compromised passwords. These results emphasize the need for organizations to adopt a more comprehensive approach to password security. This can include integrating real-time services to block known compromised passwords and common dictionary terms, thereby enhancing defenses against credential stuffing and brute force attacks. However, abstain from enforcing arbitrary password complexity requirements such as mixtures of uppercase letters, symbols, and numbers, as these restrictions often lead to weaker passwords, consequently diminishing your security posture rather than enhancing it.

► What password requirements does your organization currently enforce?





Risks and Consequences of Inadequate Authentication Security

An abstract graphic consisting of several concentric, semi-transparent circular arcs in shades of gray, centered in the lower half of the page.

Fallout After Unauthorized Access

Unauthorized access to sensitive data, apps, and systems can have far-reaching impacts, from severely disrupting business operations to causing reputational damage. Organizations that experienced unauthorized access incidents reported that the reallocation of IT resources for incident response and remediation was the most immediate negative impact (28%), indicating a disruptive shift in focus and resources. This is followed by system or service downtime (26%), increased helpdesk workload (24%), and data breaches or leakage (22%), all damaging operational efficiency and trust.

Organizations must prioritize strengthening their security posture to eliminate unauthorized access and avoid the severe consequences. Implementing robust measures like secure communication protocols and real-time detection of compromised credentials can significantly reduce the risk.

► **What negative consequences has your organization experienced due to unauthorized access to sensitive data, applications, or systems in the past 12 months?**
Multiple answers allowed



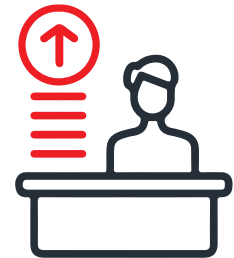
28%

Reallocation of IT resources for incident response and remediation



26%

System or service downtime



24%

Increased helpdesk workload
(e.g., password resets, account lockouts)

22%

Data breaches or leakage

20%

Negative publicity and reputational damage

18%

Disruption of business operations

18%

Customer attrition or dissatisfaction

Loss of revenue or business opportunities 14% | Loss or compromise of intellectual property 12% | Legal disputes, lawsuits, or liabilities 12% | Decreased employee productivity 10% | Regulatory fines or penalties 8% | Other 2%

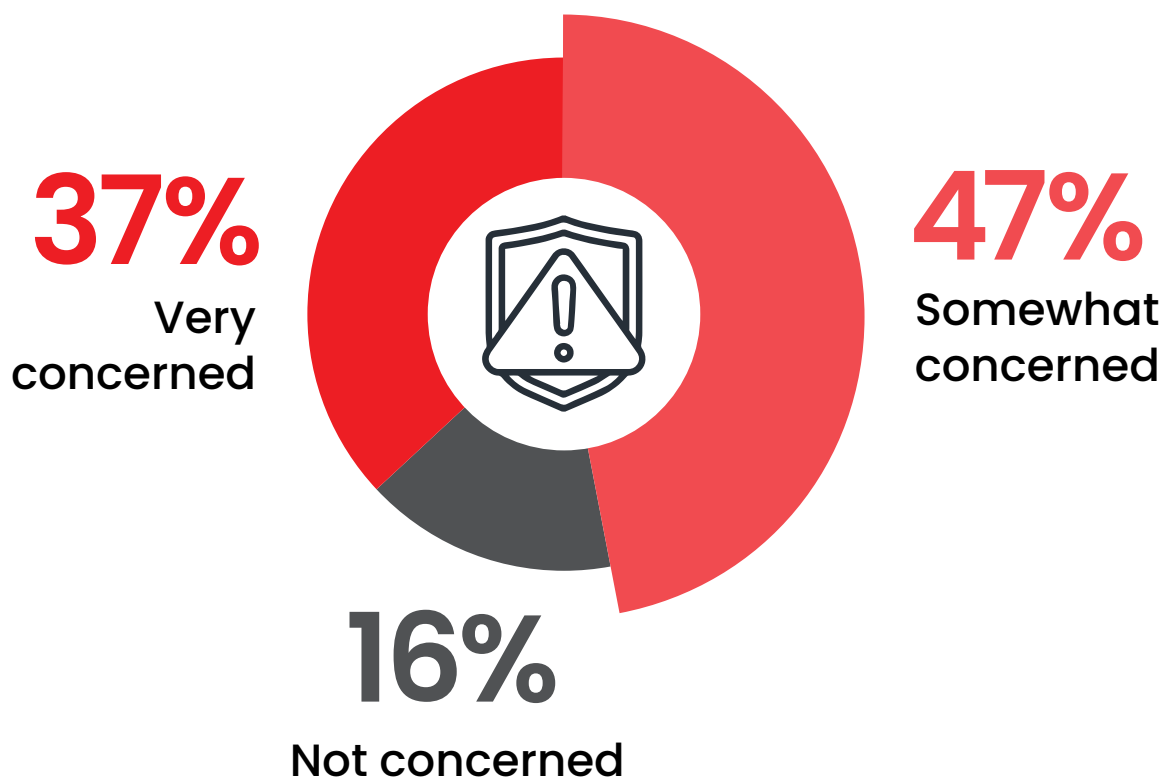
Password Security Concerns

Perceptions of risk can influence how organizations prioritize their cybersecurity efforts. When it comes to password security, understanding the threat landscape and potential vulnerabilities is key.

A majority of respondents express concern about weak and compromised passwords in their environment, with only 37% being very concerned and 47% somewhat concerned. Despite compromised credentials being the primary cause of data breaches and posing substantial financial risk, as highlighted in Verizon's DBIR Report and IBM's Cost of a Data Breach Report. This lack of urgency is striking given that these incidents are notoriously difficult to identify and often result in higher-than-average financial repercussions.

IBM's Cost of a Data Breach Report reinforces the gravity of the situation, revealing that compromised credentials took the longest to identify among all attack vectors. This led to an even greater financial impact, surpassing that of other types of breach categories. Despite these alarming statistics, there is a clear disconnect between the perceived and actual risks associated with weak and compromised passwords. Organizations must reconcile this discrepancy by aligning their cybersecurity measures with the realities of the threat landscape, prioritizing actions that mitigate the most significant risks. Only then can they effectively protect against the often-devastating consequences of compromised credentials.

- ▶ **How concerned are you about the security risk of weak and compromised passwords used in your organization's environment?**

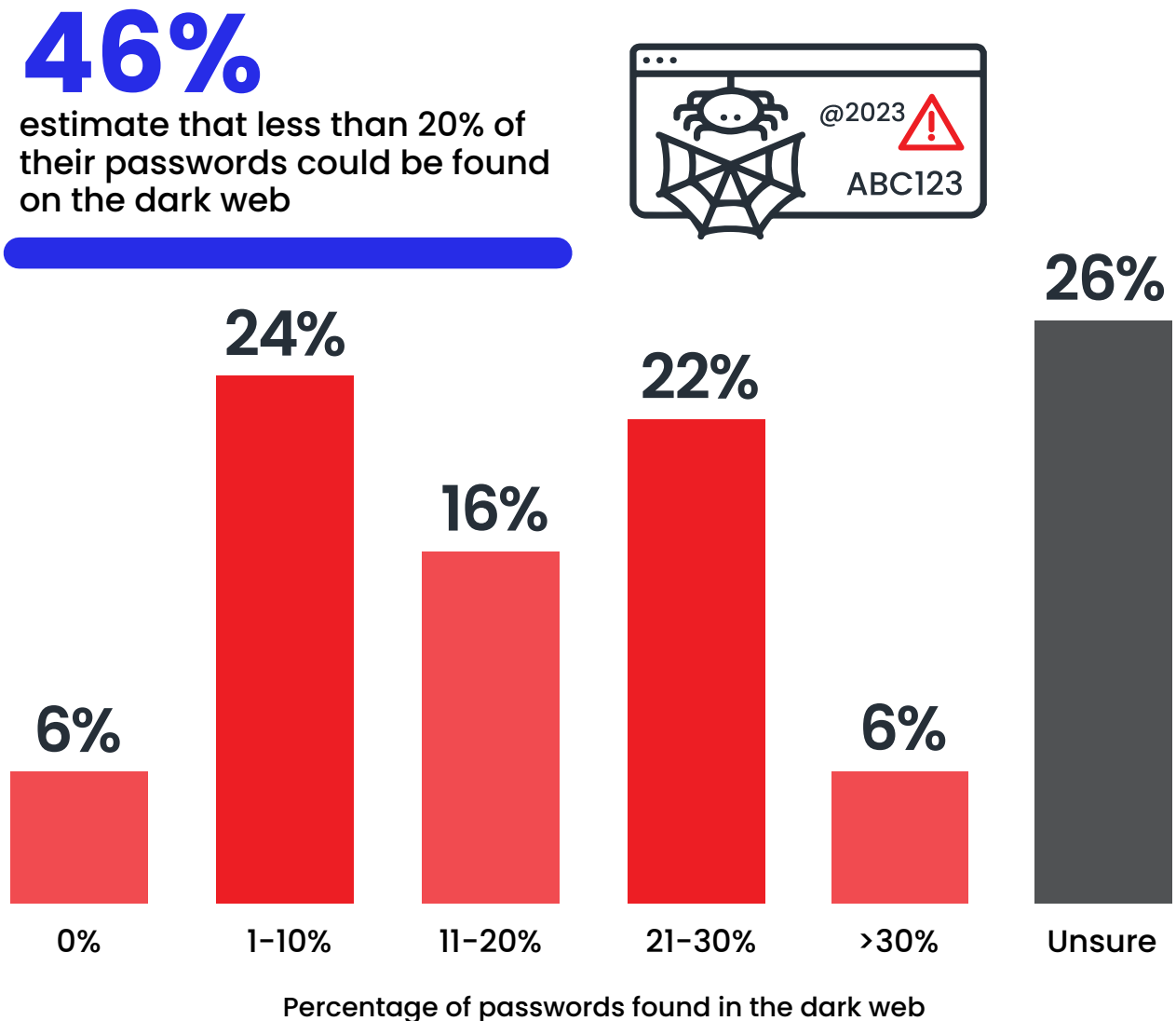


Dark Web Password Exposure

The dark web's role in propagating cybercrime, particularly in relation to stolen or compromised credentials, is a significant concern. Understanding the extent of potential exposure on the dark web can inform an organization's risk profile. A substantial portion of respondents feel that their exposure is alarmingly high, with 28% estimating that more than 20% of their passwords are exposed on the dark web. 46% believe that less than 20% of their passwords could be found on the dark web. A concerning 26% are unsure about their exposure.

Given the potentially high stakes involved with credential exposure on the dark web, organizations should not leave this to guesswork but should instead use sophisticated services that can provide real-time alerts on compromised credentials.

▶ **What percentage of the passwords in your environment do you believe could be found on the dark web?**

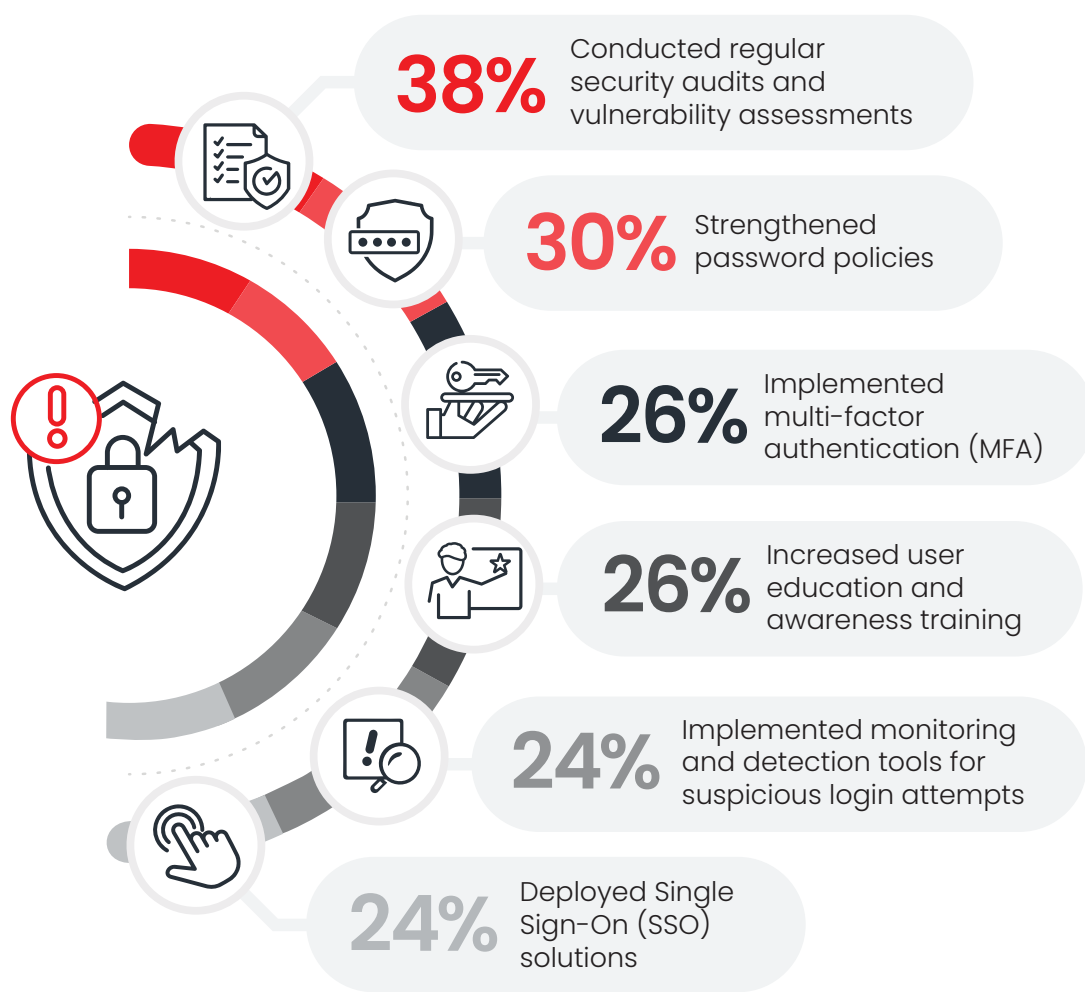


Post-Attack Authentication Reinforcement

The importance of strengthening authentication security measures following a cyberattack can't be overstated. Robust authentication is a fundamental aspect of cybersecurity, protecting user identities and ensuring only authorized individuals gain access to sensitive information. A notable 38% of organizations conducted regular security audits and vulnerability assessments following an attack, highlighting a proactive approach to security. A combination of implementing multi-factor authentication (26%), strengthening password policies (30%), and increasing user education and awareness (26%) were the next most common responses.

However, it's surprising that 10% made no changes, indicating a potential vulnerability for future breaches. Organizations should urgently address these shortcomings by adding multiple layers of authentication and making sure the password layer is secure. It's also vital to boost user awareness about cyber threats while embracing regular audits and vulnerability assessments as part of a holistic cybersecurity strategy.

► **If your organization experienced any of the mentioned authentication-related cyberattacks, what changes were made to strengthen your authentication security measures?** Multiple answers allowed



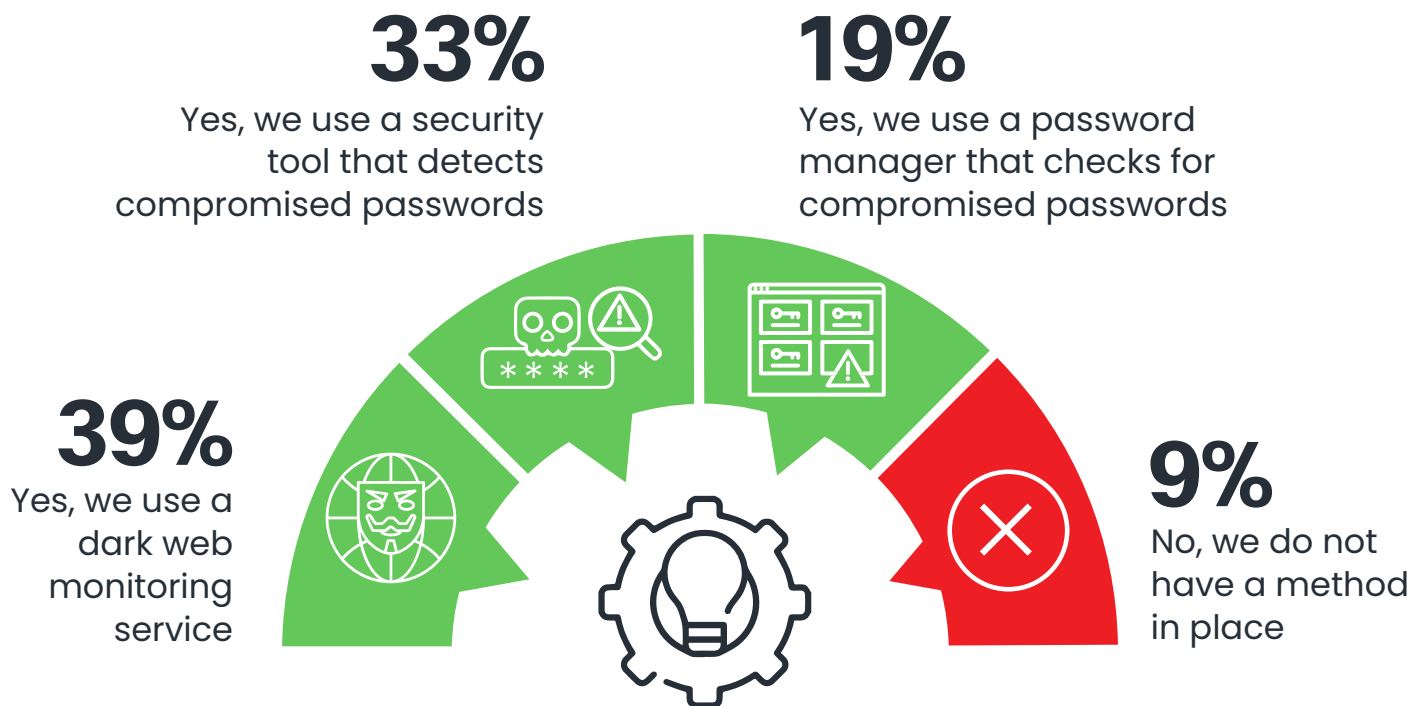
Implemented encryption and secure communication protocols 22% | Enhanced access controls and user privilege management 20% | Implemented detection and remediation of compromised credentials 18% | Adopted passwordless authentication methods 12% | No changes were made 10%

Identifying Compromised Passwords

Detecting compromised passwords promptly is critical in preventing unauthorized access and protecting sensitive data. A variety of tools and methods are available to assist organizations in achieving this. Interestingly, the majority of respondents use various methods to detect compromised passwords - dark web monitoring services (39%), password managers (19%), and specific security tools (33%). Still, 8% do not have a method in place to determine compromised passwords, revealing a notable blind spot in their security measures.

Organizations should implement a robust and reliable method for identifying compromised passwords to ensure immediate notification and action when a password is compromised.

▶ **Do you have a method in place to determine when existing passwords have been compromised?**





Future of Authentication Security

An abstract graphic consisting of several concentric, semi-transparent circular arcs of varying shades of gray, centered in the lower half of the page.

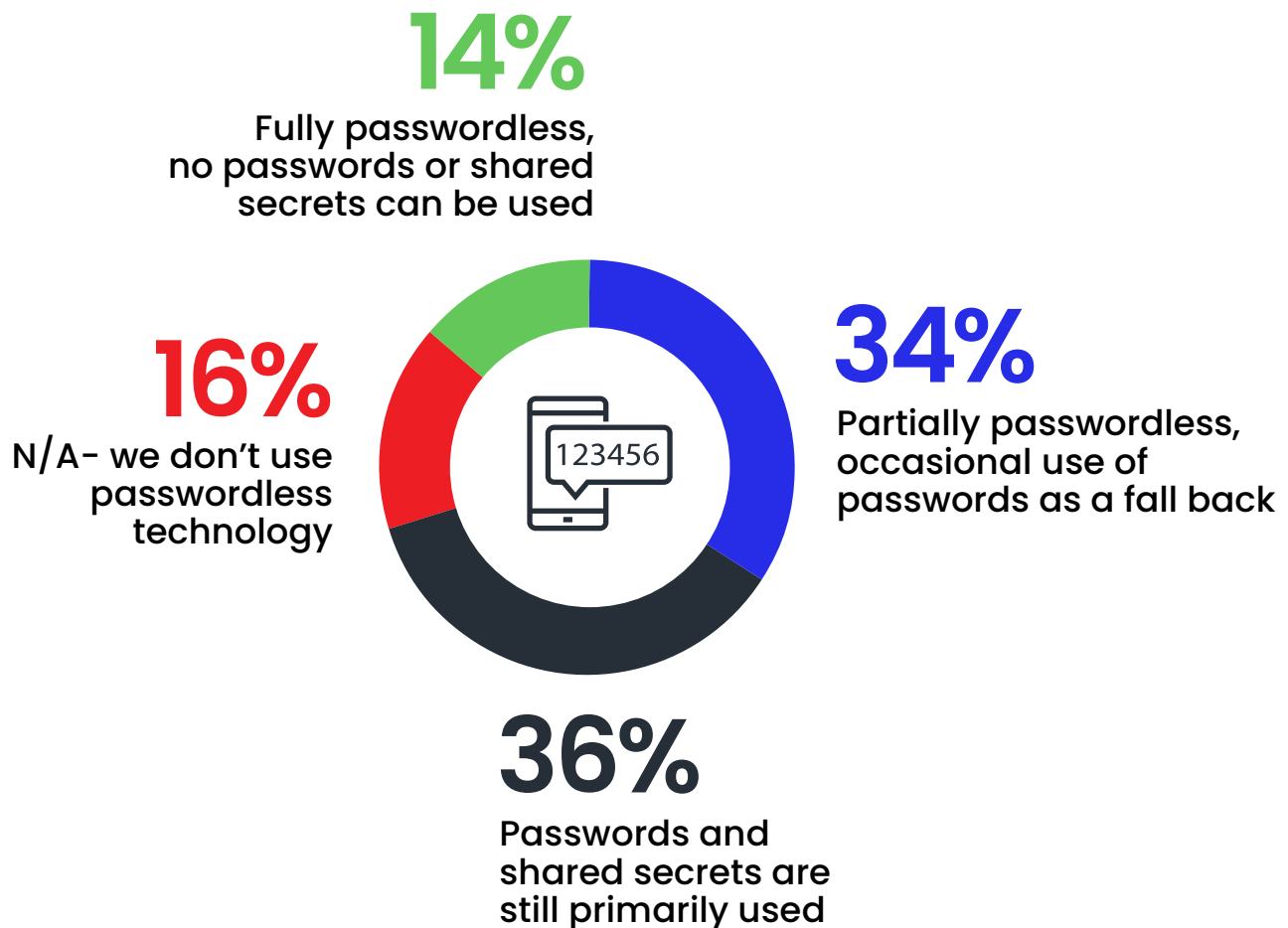
MFA Dependence on Passwords

Passwordless multi-factor authentication (MFA) presents an alternative approach for secure access. However, a decrease in the risks related to weak or stolen passwords can only be achieved if passwords are completely omitted from the authentication process, even as a backup option. Those planning a transition to passwordless methods should be aware of views from organizations such as NIST, which refers to biometric options as ‘probabilistic in nature,’ indicating sporadic unreliability, and recommends offering backup authentication methods.

The majority of surveyed organizations (36%) indicate that passwords and shared secrets are still primarily used as part of their “passwordless” MFA solution. Another third (34%) uses partially passwordless MFA with occasional password use as a fallback. However, only 14% reported being fully passwordless.

Despite adopting “passwordless” strategies, 70% of organizations continue to rely on passwords either as a primary or fallback authentication method. Consequently, these organizations remain vulnerable to compromised credentials, underlining the limited effectiveness of nominally “passwordless” solutions that still depend on password-based paths for convenience. These findings highlight the urgent need to protect the password layer present in these solutions.

- ▶ To what extent does your organization’s “passwordless” multi-factor authentication (MFA) solution rely on passwords or shared secrets (e.g., one-time password (OTP), SMS code)?



Challenges With MFA

Although multi-factor authentication (MFA) is often touted as a compensating control that enhances the security of systems, applications, and data, it might not be the ultimate solution. The usability and compatibility of MFA solutions are crucial, as difficulties in these areas can significantly affect adoption and effectiveness. The survey reveals that a significant majority of organizations have encountered issues with MFA (56%), including challenges with usability or compatibility.

To ensure the successful implementation and usability of MFA, organizations should invest in comprehensive user training, seamless integration, and user-friendly solutions that enhance the security of authentication without adding undue complexity. Importantly, MFA is designed as a supplementary control and is not intended to replace the necessity for strong passwords. It's also crucial to ensure the compatibility of the MFA solution with existing systems to avoid delays in deployment or operational disruptions.

- ▶ **Have you ever encountered any issues with multi-factor authentication, such as difficulty using it or issues with compatibility?**



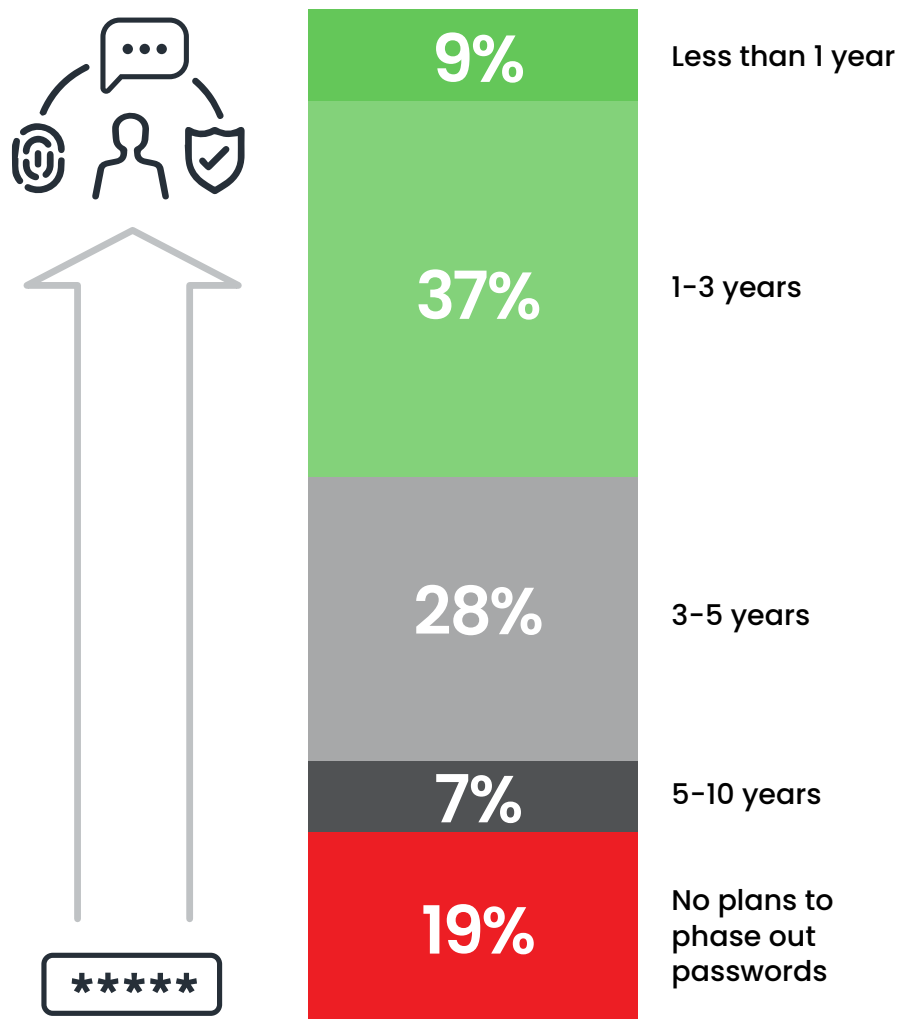
Passwords are Here to Stay

Despite the hype around passwordless solutions, it appears that traditional passwords aren't going anywhere soon. Organizations face a myriad of challenges, from cost, technical capabilities, and business disruptions, that make transitioning away from passwords less feasible.

The survey indicates that about half of organizations are planning to phase out passwords within the next 3 years (46%), and a considerable portion plan to follow suit within 3-5 years (28%). However, a notable 19% have no plans to phase out passwords, pointing to the enduring role that passwords will have for the foreseeable future.

These statistics underline the fact that passwords will remain a crucial part of our digital lives for some time to come. Rather than chasing the latest passwordless alternatives, which may or may not be suitable for every organization, the focus should be on securing existing password-based systems. This approach acknowledges that the promised shift towards alternative authentication methods is neither as attainable nor as universally applicable as some proponents would have us believe.

► What is your estimated timeframe for phasing out passwords in your environment?



NIST Password Guidance Awareness

Staying updated with recommendations from esteemed institutions such as NIST is paramount for organizations aiming to uphold rigorous cybersecurity standards. NIST, in its forward-thinking approach, suggests a shift from the age-old password complexity rules. Instead, it recommends monitoring for compromised passwords, aiming for a more effective and targeted approach to password security.

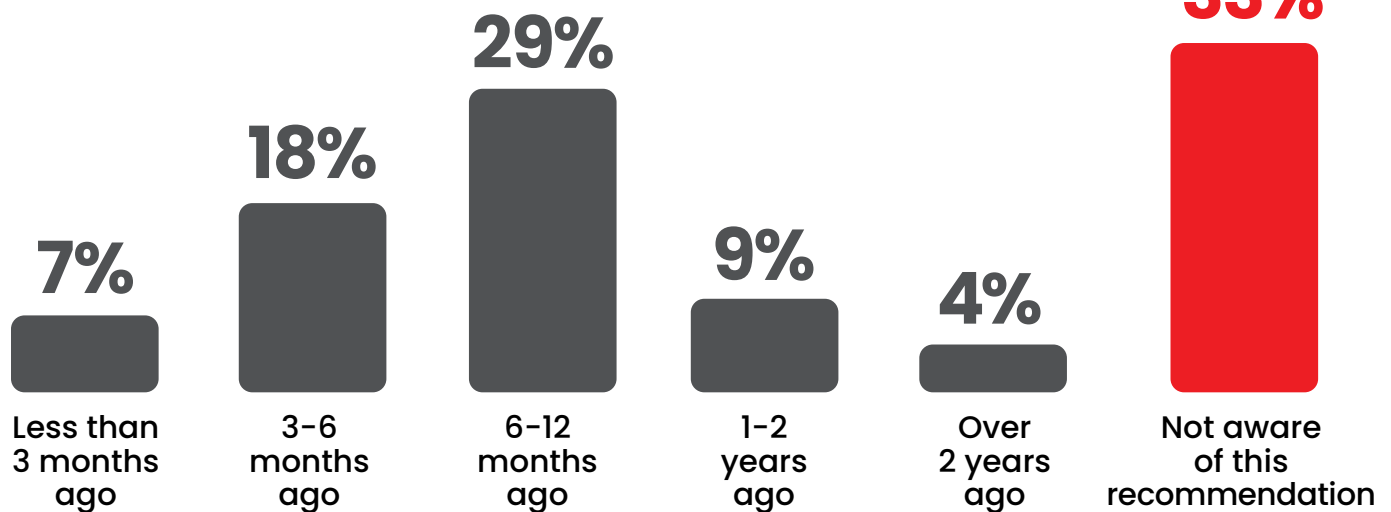
A majority (54%) only learned about the NIST password guidance within the last 12 months, even though the NIST password recommendations were first released in 2017. However, it's alarming that 33% of respondents are not aware of this recommendation at all. This lack of awareness and resulting delay in adopting crucial guidance may result in weaker password security measures.

To enhance cybersecurity, organizations should regularly implement recommendations from cybersecurity standard bodies like NIST and utilize authentication platforms that automatically enforce robust password policies, without adding complexity for users.

► When did you first learn about NIST's recommendation to replace traditional password complexity rules with a blacklist-based approach?

54%

learned about the NIST password guidance within the last 12 months



Best Practices for Effective Authentication Security

Ensuring robust authentication security has never been more critical. Here are some best practices that can help your organization achieve more secure authentication and reduce vulnerability to cyberattacks.



Embrace Multi-Factor Authentication (MFA): MFA adds an extra layer of protection by requiring users to provide two or more verification factors to gain access to resources. This can be a compensating control to limit unauthorized access if a password is compromised.



Secure What you Have Today: Organizations should not delay strengthening their existing password security with the hopes of pursuing uncertain passwordless benefits in the future; instead, they should focus on improving current password-based protection. This pragmatic approach acknowledges that passwords remain a critical and proven part of our cybersecurity infrastructure, and emphasizes the need to secure them properly.



Regular Security Audits: Conduct regular security audits and vulnerability assessments to identify and address potential weaknesses in your authentication process. This proactive approach allows you to stay ahead of cyber threats.



Continuous User Education: Regularly train your users about the importance of secure authentication practices. It helps to build a cybersecurity-conscious culture within the organization and can be a strong defense against social engineering and phishing attacks.



Implement Screening of New Passwords: Implement a policy that blocks known compromised and common dictionary passwords. This helps prevent attackers from accessing accounts by exploiting commonly used or previously compromised passwords.



Deploy Monitoring and Detection Tools: Implement tools to detect suspicious login attempts or compromised credentials. Early detection can allow you to respond promptly to potential security incidents, minimizing potential damage.



Leverage Dark Web Monitoring Services: Regularly check if your organization's credentials have been compromised and are available on the dark web. Early detection of such breaches can help to mitigate risks promptly.



Abandon Algorithmic Complexity: Abstain from enforcing arbitrary password complexity requirements such as mixtures of uppercase letters, symbols, and numbers. Experience and research suggest that these restrictions often lead to weaker passwords, consequently diminishing your security posture rather than enhancing it. This is why organizations like NIST have removed all password complexity requirements from their guidelines.

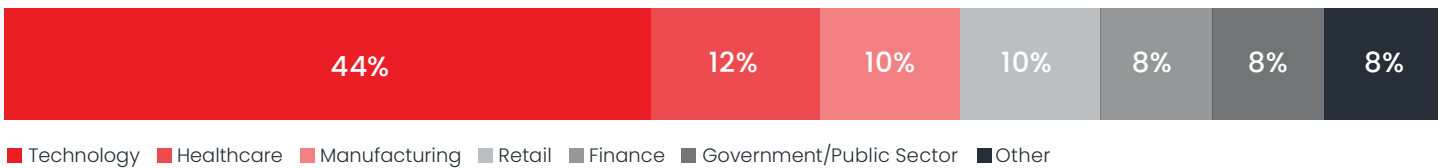
Methodology and Demographics

The 2023 State of Authentication Security Report is based on a comprehensive survey of 483 people to explore the state of passwordless authentication, the key drivers and barriers to adoption, and organizations' technology preferences. The respondents range from technical executives to IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

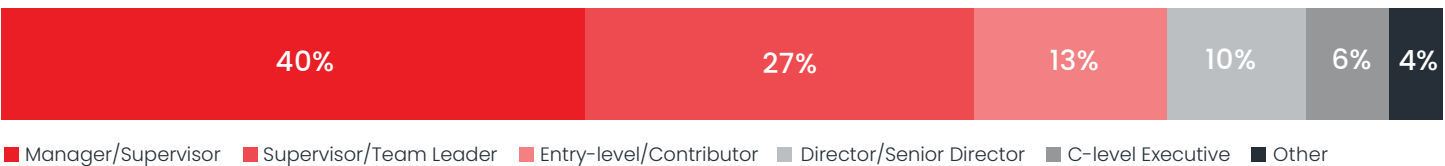
Company size



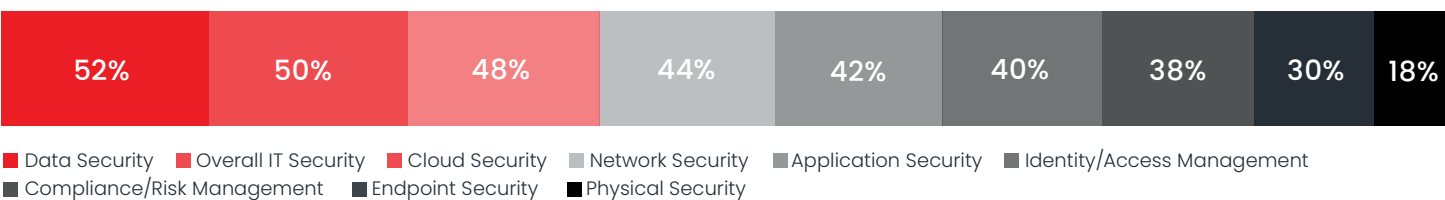
Primary industry



Job position



Security focus areas





Enzoic is an enterprise-focused cybersecurity company committed to preventing account takeover and fraud through actionable Dark Web research. What sets Enzoic apart is the unique proactive approach to solving the problems that compromised passwords and credentials cause. By combining human intelligence with automated proprietary monitoring, Enzoic delivers the most current and complete threat research data.

Organizations can use Enzoic solutions to screen customer and employee accounts for exposed username and password combinations to identify at-risk accounts and mitigate unauthorized access. Enzoic's comprehensive approach to compromised password detection and its tailored solutions, like Enzoic for Active Directory, represent our company's unwavering commitment to protecting customer environments. Enzoic is a profitable, privately held company in Boulder, Colorado.

Email us at info@enzoic.com or visit enzoic.com

Cybersecurity

I N S I D E R S

Cybersecurity Insiders brings together 600,000+ IT security professionals and world-class technology vendors to facilitate smart problem-solving and collaboration in tackling today's most critical cybersecurity challenges.

Our approach focuses on creating and curating unique content that educates and informs cybersecurity professionals about the latest cybersecurity trends, solutions, and best practices. From comprehensive research studies and unbiased product reviews to practical e-guides, engaging webinars, and educational articles - we are committed to providing resources that provide evidence-based answers to today's complex cybersecurity challenges.

Contact us today to learn how Cybersecurity Insiders can help you stand out in a crowded market and boost demand, brand visibility, and thought leadership presence.

Email us at info@cybersecurity-insiders.com or visit [cybersecurity-insiders.com](https://www.cybersecurity-insiders.com)