World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

Breaking free from passwords: The secure shift for modern organizations

Rajiv Dewan [1,*], Nirupam Samanta [1] and Devdas Gupta [2]

[1] *Cybersecurity IAM Professional.*
[2] *Software Development and Engineering Lead.*

World Journal of Advanced Engineering Technology and Sciences, 2025, 15(03), 049–052

Publication history: Received on 21 April 2025; revised on 29 May 2025; accepted on 01 June 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.15.3.0890

Abstract

The transition from traditional password-based authentication to passwordless systems is gaining momentum across organizations. This shift is driven by the increasing need for better security, improved user experience, and cost reduction. However, the journey to passwordless authentication is complex and full of challenges, including technical limitations, resistance from users, integration issues with legacy systems and applications, and regulatory concerns. This paper explores the concept of going passwordless, highlight common challenges faced by organizations, and potential solutions to those challenges that can help achieve a successful outcome. The findings are based on a review of industry reports, and case studies, offering practical insights for IT and security professionals.

Keywords: Passwordless Authentication; Cybersecurity; Identity Management; Biometric Authentication; MFA; User Experience; IT Security; Organizational Change

1. Introduction

Passwords have been the most common method for user authentication for decades. Despite their popularity, passwords are considered weak, reused, and vulnerable to attacks like phishing, brute force, and credential stuffing. According to Verizon's 2023 Data Breach Investigations Report, over 80% of hacking-related breaches involve weak or stolen passwords (Verizon, 2023). Such security breaches have encouraged organizations to explore passwordless authentication methods to enhance security and streamline their access related processes.

Passwordless authentication replaces traditional passwords with more secure and user-friendly options, such as biometrics, security keys (YubiKeys Google Titan Keys etc.), hardware token, Windows Hello, or others device-based authentication. Although the benefits are clear, organizations face several challenges in implementing passwordless solutions. This article discusses these challenges and provides potential solutions to overcome them.

2. Research methods

This study uses a qualitative research approach based expert opinions, and case studies. Sources include academic journals, cybersecurity reports, white papers, and real-world implementations by organizations like Microsoft, Google, and Okta.

* Corresponding author: Rajiv Dewan; E-mail: dewanrajiv2010@gmail.com

3. Challenges in Going Passwordless

3.1. Legacy Infrastructure

Many organizations still use many legacy systems or applications that are not compatible with modern authentication methods and have huge dependencies on passwords. These systems often lack support for standards like SAML 2.0, OIDC, WebAuthn or FIDO2, making it difficult to deploy passwordless solutions.

3.2. User Resistance

Users are habitual to use passwords. Any major change in login behavior may face resistance, especially from employees who are not tech-savvy. A successful transition must consider change management and user education.

3.3. Cost of Implementation

Implementing passwordless authentication can involve significant upfront costs. This includes purchasing new hardware (e.g., biometric devices or security keys), upgrading systems, and training staff.

3.4. Integration Complexity

Organizations often use a wide range of applications, platforms, and identity providers. Integrating passwordless solutions across all systems can be time-consuming and technically challenging.

3.5. Regulatory Compliance

Different industries are subject to regulations such as HIPAA, GDPR, and PCI-DSS etc. Ensuring that passwordless systems meet compliance standards adds another layer of complexity to the solution and becomes challenging to implement.

3.6. Device Dependence

Many passwordless solutions rely on personal or corporate devices. This raises concerns about device loss, theft, or unauthorized access, which must be addressed in the design of the system. This also requires implementation of an appropriate MDS solution for organizations before passwordless solution can be implemented.

3.7. Scalability and Maintenance

As organizations grow, maintaining a secure and scalable passwordless system requires careful planning and resource allocation.

4. Solutions to Achieve Passwordless Authentication

4.1. Implementing Multi-Factor Authentication (MFA) as a Step

Before going completely passwordless, organizations can introduce MFA, combining passwords with another factor like biometrics or a mobile authenticator app. This approach improves security while gradually moving toward full passwordless authentication.

4.2. Using FIDO2 and WebAuthn Standards

The Fast Identity Online (FIDO2) standard enables secure, passwordless login using biometric data or security keys. WebAuthn, a part of the FIDO2 standard, is supported by major browsers and platforms, making it ideal for cross-platform implementations.

4.3. Leveraging Biometric Authentication

Biometric systems use fingerprints, facial recognition, or voice patterns for user authentication. These are hard to replicate and provide a high level of security. Windows Hello and Apple Face ID are common examples used in corporate environments.

4.4. Security Keys and Smart Cards

Hardware tokens like YubiKeys provide a simple and secure passwordless experience. These keys generate unique cryptographic responses, reducing the risk of phishing and password theft.

4.5. Single Sign-On (SSO) Integration

Integrating passwordless authentication with SSO platforms allows users to log in once and access multiple systems. This improves user experience while maintaining security.

4.6. Identity and Access Management (IAM) Solutions

Modern IAM platforms such as Okta, Azure AD, and Ping Identity support passwordless features and help manage users, devices, and access policies.

4.7. Zero Trust Architecture

A Zero Trust model assumes no user or device is trusted by default. Integrating passwordless authentication into a Zero Trust strategy enhances security by verifying every access request dynamically.

4.8. User Training and Awareness Programs

A successful passwordless transition requires educating users about new methods, benefits, and how to use them safely. Training reduces resistance and increases adoption.

5. Case Studies

5.1. Microsoft

Microsoft introduced passwordless authentication options for Azure Active Directory using Windows Hello, Microsoft Authenticator, and FIDO2 security keys. According to Microsoft (2022), over 150 million users now use passwordless login methods, significantly reducing account takeover risks.

5.2. Google

Google implemented security keys across its workforce and reported zero successful phishing attacks since the adoption. Employees are required to use Titan Security Keys for authentication (Google, 2023).

5.3. Dropbox

Dropbox transitioned to WebAuthn-based login options, offering passwordless access to users. The change improved both security and user experience, especially for enterprise customers (Dropbox, 2023).

6. Conclusion

The journey to passwordless authentication is not without hurdles. Organizations must navigate technical, cultural, and financial challenges to achieve a secure, seamless login experience. However, the benefits, reduced breaches, improved user satisfaction, and compliance readiness, far outweigh the costs. By leveraging standards like FIDO2, using biometrics, adopting hardware keys, and educating users, organizations can move confidently toward a passwordless future.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Dropbox. (2023). Enabling Passwordless Authentication with WebAuthn. Retrieved from https://www.dropbox.com

[2] Google. (2023). Security Keys: Advanced Protection for Google Employees. Retrieved from https://security.googleblog.com

[3] Microsoft. (2022). The Passwordless Future Starts Now. Retrieved from https://www.microsoft.com

[4] Verizon. (2023). Data Breach Investigations Report. Retrieved from https://www.verizon.com/business/resources/reports/dbir/

[5] FIDO Alliance. (2023). FIDO2: Moving the World Beyond Passwords. Retrieved from https://fidoalliance.org/fido2/

[6] Okta. (2024). The State of Passwordless Security. Retrieved from https://www.okta.com/resources