

# Reimagine Workforce Access: A Security Leader's Guide to the Future of Passwords

A Roadmap to Stronger Security and  
Better User Experiences

## Authentication Dilemma: Modernizing Without Disruption

Workforce authentication is at a crossroads. Passwords remain the most widely used authentication method. Yet, they are also a leading cause of security breaches, contributing to at least 87% of attacks perpetrated by external threat actors.<sup>1</sup> This weak link can—and does—fail often, whether passwords are stolen, brute forced, or obtained through phishing and other methods of compromise.

Security stakeholders are well aware of these limitations. Driven by advances in biometrics, the ready availability of passkeys, and the widespread adoption of FIDO2 standards, passwordless authentication is becoming more widely deployed. Offering a secure, user-friendly alternative to passwords that also promises to reduce administrative burden, passwordless is the future of authentication.

But getting rid of passwords entirely can be difficult for a variety of reasons. Many organizations are now operating in a hybrid state, balancing legacy systems that still require passwords with modern authentication solutions that are passwordless-compatible. Security leaders need a strategic roadmap to guide them during this transition, ensuring security and usability throughout the process. By taking a phased approach in which workforce password management (WPM) is deployed to set the foundation for passwordless authentication, organizations can mitigate present-day password risks while preparing to eliminate them in the months and years to come.

**87%** of data breaches involve some form of credential theft or compromise.<sup>2</sup>

**#1** stolen credentials and phishing are the most common attack vectors.<sup>3</sup>

**9 out of 10** organizations have experienced an identity-related breach in the past year.<sup>4</sup>

Layering on additional identity assurance controls, such as dynamic risk assessment during sessions and AI-driven anomaly detection, can further protect your organization's most valuable digital assets, no matter where you are on the road to passwordless authentication.

## Understanding Evolving Threats

Identities have long been among attackers' top targets. Even as enterprise security teams race to harness the power of AI to shore up defenses, these attacks continue to succeed at an alarming rate. Over 90% of organizations have experienced an identity-related breach in the past year.<sup>5</sup> Even in the age of multifactor authentication (MFA), a single stolen password offers attackers multiple pathways to your organization's most sensitive resources.

Identities are targeted throughout the digital journey—before login with phishing and malware, during authentication via brute force or MFA fatigue, and after login through token theft or session hijacking. A compromise at any one of these points opens the opportunity for lateral movement to other accounts and resources.

Now, threat actors are using AI to level up these attacks. As large language models (LLMs) become increasingly accessible, attackers are scaling up the volume and the variety of phishing attempts. With AI in their toolkit, they're able to personalize malicious email messages to make them nearly indistinguishable from legitimate communications. This poses problems for employees being targeted and for the email security solutions designed to filter out spam and messages from fraudsters.

1. *2025 Data Breach Investigations Report*, Verizon, May 2025.

2. Verizon, *2025 Data Breach Investigations*.

3. *2024 Trends in Securing Digital Identities*, Identity Defined Security Alliance, January 2024.

4. *2025 Identity Security Landscape*, CyberArk, April 2025.

5. CyberArk, *2025 Identity Security Landscape*.

Bad actors are also leveraging generative AI tools to create malicious code, such as shape-shifting polymorphic malware, that can evade detection by traditional security solutions while it works to bypass authentication mechanisms. AI-augmented reconnaissance tools can quickly find vulnerabilities and ways to gain elevated privileges in an environment. AI can also be used to harvest long-lasting session cookies, which can then be exploited or offered up for sale on the dark web.<sup>6</sup>

AI-driven threats and identity attacks aren't going away. And static security checkpoints are no longer enough. To stay secure, organizations must modernize their authentication approach by:

- Securing existing passwords.
- Taking steps to move beyond passwords.
- Adopting continuous identity assurance using AI-powered analytics and privilege controls.

## Why Passwords Remain, Despite Their Shortcomings

Passwords are still the most common access control, even though most CISOs are ready to move beyond their use. More than two-thirds of IT and security leaders report that adopting passwordless authentication is a priority for their organizations.<sup>7</sup> Going from aspiration to action, however, is challenging. Deploying passwordless solutions isn't easy because often people, processes, and technologies aren't ready to make the switch.

### Lack of Support for Modern Authentication Standards

Legacy systems remain prevalent in modern organizations. Developed prior to the advent of today's authentication standards, they don't speak with modern protocols, like FIDO2, making it difficult to integrate them with passwordless authentication solutions. Achieving this can require major redevelopment effort or the use of middleware.

### Inconsistent Platform Readiness

The result of gradual technology addition is a complex mix of on-premises servers and cloud infrastructure, modern containerized apps, and outdated software. Many of these systems don't support passwordless authentication. Some, like devices with local administrative passwords, require the use of passwords by default. This fragmentation makes it impossible to implement passwordless authentication consistently across all platforms.

### Workforce Resistance to Change

Employees are creatures of habit. They might worry about being unable to access important digital resources during the transition phase, or fret about whether the new biometric system will function with the protective attire they wear at work. Or they might be uncomfortable sharing biometric data for privacy reasons. Without education and a well-thought-out change management plan, resistance can slow, stall, or thwart deployment success.

## Balancing Security and User Experience

Security and usability have long been thought of as natural enemies, but passwordless authentication brings them together. When you implement a modern passwordless access solution, there's no need to choose one or the other.

### Security Team Benefits

- Reduced credential-related risk.
- Increased visibility and control.
- Lower operational overhead.

### End-User Benefits

- Faster, frictionless access.
- Fewer password resets.
- Consistent login experiences across applications and devices.

6. "Analyzing 3 Offensive AI Attack Scenarios," CyberArk, August 6, 2023.

7. *The State of Passwordless Authentication: Security and Convenience Drive the Change*, a Dark Reading report commissioned by OpenText, December 2023.

## Regulatory Frameworks Assume Controls Are Password-Based

Even though passwordless authentication offers more robust security, some regulatory frameworks still stipulate that password-based controls be used to protect customer data or other digital assets. The Payment Card Industry Data Security Standard (PCI DSS) 4.0, for example, encourages the use of MFA but requires passwords and so does SOC 2. Many of these requirements persist because legacy systems remain prevalent in regulated industries.

Because of these roadblocks, most organizations cannot simply go passwordless. The implementation process can be lengthy, and it's common for password-based and passwordless systems to operate side by side for an extended period during the transition.

In the meantime, organizations can apply the following password management best practices to reduce exposure and support long-term progress:

- **Enforce strong password policies:** Requires complexity, length, and regular updates, and monitor for weak or compromised credentials.
- **Use a secure password vault:** Protects access to critical systems with centralized password storage, especially for privileged accounts.
- **Integrate password controls with broader identity tools:** Combines SSO, MFA, PAM, and secure browsing for layered protection.
- **Implement session monitoring and auditing:** Detects threats in real time and creates audit trails to support investigation and response.
- **Avoid storing passwords and access tokens on local devices:** Uses secure password management solutions and enterprise browsers to prevent compromise of credentials on the endpoint.

## Overcoming Passwordless Adoption Roadblocks

We recommend a phased implementation strategy, starting where the change is least likely to cause disruption to business-critical workflows or where it is most likely to deliver a quick win by reducing major risks. Today, passwordless authentication is not feasible for every application and device. Taking a multilayered approach to authentication modernization makes it possible to improve security everywhere by enforcing consistent policies and controls. You can achieve this for passwords by implementing a WPM solution to support the phased adoption of passwordless authentication.

## Using Workforce Password Management as a Bridge

Idira™ Workforce Password Management, by Palo Alto Networks, provides secure credential storage, management, and sharing. Passwords are protected with robust encryption, the organization achieves granular visibility and control, and end users enjoy simple, easy login experiences. This solution helps to solve many of the common challenges that passwords present by providing:

- **Enterprise-grade security:** Secures storage of business credentials, files, or notes, with password policy enforcement to comply with organizational requirements or frameworks like NIST 800-63B.
- **Effortless employee access:** Automatically saves and autofills credentials, with easy one-click access to apps, including on mobile devices.

## 5 Signs Your Organization Is Ready to Go Passwordless

1. **You've deployed MFA, but identity-based attacks still occur.** Attackers now use techniques, like MFA fatigue and social engineering, to bypass protections.
2. **Your help desk is overwhelmed with password reset requests.** Rising support tickets are a clear signal that password management is draining resources.
3. **Your workforce is largely remote or hybrid.** Remote employees are frequent targets for phishing and device-based credential theft.
4. **You're modernizing or replacing legacy applications.** Moving away from systems that don't support modern identity protocols clears the path to passwordless.
5. **You've adopted zero trust or an identity-first model.** Passwordless solutions align with the principles of continuous authentication and device trust.

- **Enterprise visibility and control:** Includes customizable access policies, proactive alerting on weak or compromised credentials, continuous risk intelligence and monitoring, and granular visibility so admins can address risks in real time.
- **The ability to measure and track risk posture:** Provides detailed insights and reports that make it easy for admins to assess and address risks.

Idira Workforce Password Management seamlessly integrates with the organization's existing identity ecosystem, including Microsoft Active Directory and SSO platforms, to ensure consistent policy enforcement and user lifecycle management. It also integrates with adaptive MFA for logins and should support step-up or continuous authentication for sensitive or high-risk apps. These integrations—with a full identity stack that's passwordless-ready—provide an important foundation for passwordless adoption.

Idira Workforce Password Management seamlessly integrates with Idira Identity Security Platform to support continuous authentication, risk-based access, and real-time threat detection. These are the key pillars in an end-to-end passwordless strategy. This solution also supports modern and passwordless authentication methods like passkeys and FIDO2-compliant credentials. This way, the organization can deploy passwordless authentication alongside existing password-based workflows.

Idira Workforce Password Management simplifies the login experience for end users, supporting one-click application access. Once this streamlined process becomes familiar, employees will feel more comfortable with simple, one-touch login methods, greatly reducing the culture shock that passwordless adoption can otherwise bring.

### Pro Tip

If you have already adopted Idira Workforce Password Management, this work is already done for you, because centralizing credentials is part of the implementation process. Idira Workforce Password Management has robust reporting capabilities that provide immediate, effortless visibility into all passwords in use within your enterprise.

## Phased Implementation Strategy for Passwordless Success

- **Inventory your existing environment** to identify all endpoints, applications, and user accounts that rely on passwords.
- **Categorize each part of your inventory** according to its importance to the business, the severity of risks they pose, regulatory constraints, and the ease (or difficulty) of integrating them with passwordless authentication solutions.
- **Determine which applications to begin with.** Newer cloud-native applications and SaaS solutions are the least likely to cause disruption. Others will deploy passwordless for systems that pose the greatest risks first.
- **Implement certificate-based and device fingerprint-based authentication** where supported while rolling out FIDO2-compliant passkeys, biometrics, or hardware tokens.
- **Secure remote and hybrid workforces** before legacy systems, and privileged accounts before third-party partners and vendors.

## Beyond Authentication: Modernizing Workforce Identity Security

Modernizing authentication is a critical part of cybersecurity, but on its own, it's no longer enough. MFA bypass techniques are increasingly common and are used to give threat actors access to sessions postlogin. Your authentication approach needs to be part of a broader workforce identity security strategy that combines multiple layers of protection across the identity ecosystem.

Idira Workforce Password Management and passwordless authentication are natural partners. It can secure credentials for apps that can't easily support passwordless, while integrating with your passwordless solution to unify credential security across your enterprise. Integrating these time-of-login protections with continuous identity assurance and threat detection is vital. They extend visibility and risk-based protections everywhere, from the endpoint to ongoing application access beyond login.

This kind of workforce strategy requires:

- **Risk-adaptive controls** that evaluate context, behavior, and device trust before authorizing each connection.
- **Endpoint-to-application protection** that ensures sessions are secure from start to finish.
- **Just-in-time access and intelligent session controls** for every workforce user, including those with elevated privileges.

In addition, to fight against credential-based attacks, organizations need to embed AI-driven insights and continuous risk analysis across every phase of the employee journey—from device login through secure web sessions and SSO.

Palo Alto Networks is an industry leader in identity and access management (IAM), identity governance and administration (IGA), and privileged access management (PAM), with Idira solutions that extend granular controls across your entire workforce.

The Idira Identity Security Platform approach includes:

- PAM, IAM, and IGA.
- Endpoint identity security, credential protection, and passwordless authentication.
- Intelligent threat detection from login until end of session.
- Lifecycle controls for all identities.

## Key Competitive Differentiators

- **Unified, privilege-centric solution:** Discovery, context, adaptive privilege controls, policy automation, and lifecycle governance for all identities (human, machine, and AI agents) through a single pane of glass.
- **Deep zero trust foundation:** Built-in session isolation, continuous threat monitoring, and endpoint identity security that extends least privilege enforcement beyond the initial login.
- **AI-powered threat detection:** Powered by proprietary AI technology, the platform continuously discovers identities, analyzes behavior patterns, and delivers remediation guidance in real time.

## The Path Forward

The future of workforce access is both passwordless and password-smart. Modernizing authentication workflows depends on your ability to recognize where passwords can be retired and where they can still be used in ways that are secure and intelligent.

With secure, flexible, efficient identity protection, Idira Workforce Password Management empowers security leaders to modernize workforce access at scale.

To explore all the ways Idira can secure the identities across your organization, visit

[www.paloaltonetworks.com/idora](http://www.paloaltonetworks.com/idora).

## Beyond Login: Securing the Full Identity Lifecycle

Modern workforce identity strategies must stop credential misuse from endpoint to application. Idira supports this with passwordless login, passkeys, secure web sessions, and workforce password management.

By balancing strong security with a smooth user experience, organizations see faster adoption and fewer help desk calls. Privilege controls and real-time identity threat visibility give security teams the power to detect and stop active attacks.

---

## About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to cybersecurity, information technology, artificial intelligence and operational technology. Each of our 38 media properties provides education, research, and news that is specifically tailored to key vertical sectors including banking, healthcare, and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment, OT security, AI, and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

## About Palo Alto Networks

Palo Alto Networks (NASDAQ: PANW), the global AI cybersecurity leader, protects our digital way of life with a comprehensive portfolio of cybersecurity solutions and platforms across Network, Cloud, Security Operations, AI, and Identity. Trusted by more than 70,000 customers and powered by Unit 42® threat intelligence, our AI-driven platforms eliminate complexity, empowering enterprises to modernize with confidence and securing the speed of innovation. Explore the future of security at [www.paloaltonetworks.com](http://www.paloaltonetworks.com).



3000 Tannery Way  
Santa Clara, CA 95054

Main: +1.408.753.4000  
Sales: +1.866.320.4788  
Support: +1.866.898.9087

[www.paloaltonetworks.com](http://www.paloaltonetworks.com)

© 2026 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.  
idira\_wp\_security-leaders-guide-to-the-future-of-passwords\_042826