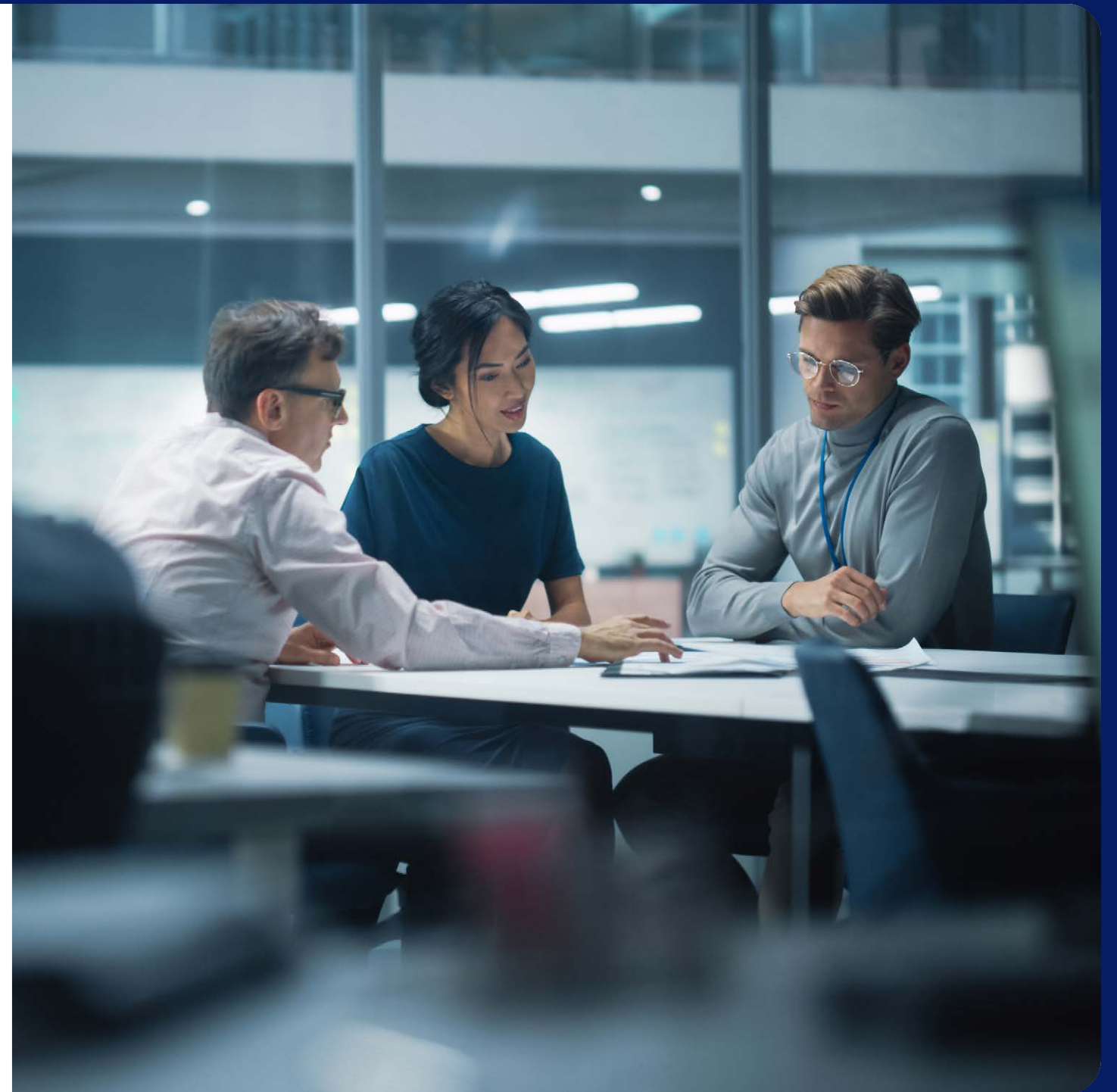

Why Workforce Password Management Is Nonnegotiable



Contents

Taken by Convenience: When Speed Beats Security	4
Taken by Phishing: The High Cost of a Compromise	5
Taken by Blind Spots: A Lack of Consumer Protections	6
Enterprise Authentication Protection with Idira Workforce Password Management	7
Built for the Enterprise	7
Frustrate Attackers.....	8
Take Control and Secure Your Passwords with Idira	9
About Palo Alto Networks	10



IMAGINE ACTOR LIAM NEESON, from the movie "Taken," leaning into the glow of a computer screen with his jaw set, his eyes steely. Then, in his deep, gravelly voice, he says, "I don't know who you are. I don't know what defenses you have. But if you use passwords, I will look for you, I will find you, and I will breach you."

While Neeson wouldn't make such a threat, other threat actors are out there who would, eyeing your network with similar determination and a will that's stronger than your passwords.

Password security isn't the frontline protection that it once was. In 2025, **88%** of breaches involved stealing credentials, with stolen credentials reportedly used in **31%** of breach incidents.¹ In 2024 alone, over **2.8 billion** passwords were posted as free or for sale on the dark web.² These numbers will continue to climb if organizations don't diversify beyond password-centric models.

Security collapses begin with mundane human decisions, including weak passwords, poor password habits, inefficient tools, and a lack of oversight. Organizations that don't diversify beyond password-centric models can't survive today's identity threats. To avoid credential vulnerabilities, organizations need to manage them invisibly, monitor them continuously, and never allow users to handle them alone.

Attackers exploit everyday password risks because common defenses fall short. By diversifying defenses beyond credential-centric models, your organization can evolve from having outdated illusions of security to taking control of workforce password security.

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

2. Verizon, *2025 Data Breach Investigations*.

Credentials don't have to be a vulnerability if they're managed invisibly, monitored continuously, and never left to the user to handle alone. Organizations must diversify beyond password-centric models if they want to survive today's identity threats.

Taken by Convenience: When Speed Beats Security

When faced with juggling multiple logins, deadlines, and meetings, often the straightest, easiest path wins. Millions of employees change only a few characters in an old password to create a new password, demonstrating the finding that only 3% of unique passwords analyzed in breaches meet traditional complexity requirements.³

Employees Have Come Clean on Password and Credential Use⁴

65% of employees knowingly violate cybersecurity protocols to get their work done, often choosing speed over security.

49% admit to using the same login credentials for multiple work-related applications.

27% knowingly reuse the same password across multiple platforms simply for convenience.

36% report reusing passwords across both personal and workplace accounts.

Even when companies issue password guidelines, without active enforcement, they become little more than friendly reminders.

³. Verizon, 2025 Data Breach Investigations.

⁴. 2024 CyberArk Employee Risk Survey, CyberArk, December 2024.

Taken by Phishing: The High Cost of a Compromise

More than half of organizations' workforce users have access to sensitive corporate data through the applications employees use for their jobs. Having access to this information might be one small mistake away from getting into the wrong hands.

51%+

of organizations reported falling victim to phishing or vishing attacks multiple times.⁵

75%+

of organizations experienced successful phishing attacks, many driven by increasingly sophisticated AI-based techniques.⁶

25%

of employees have reported losing a device used for work.⁷

All it takes is for an employee to reuse one password across multiple tools—stored in a browser or phished from a distracted employee—for an attacker to gain entry. In cases leading up to ransomware attacks, 54% of victims had their credentials exposed by infostealers, or password-stealing malware designed to harvest stored credentials, cookies, and sensitive information directly from users' devices.⁸

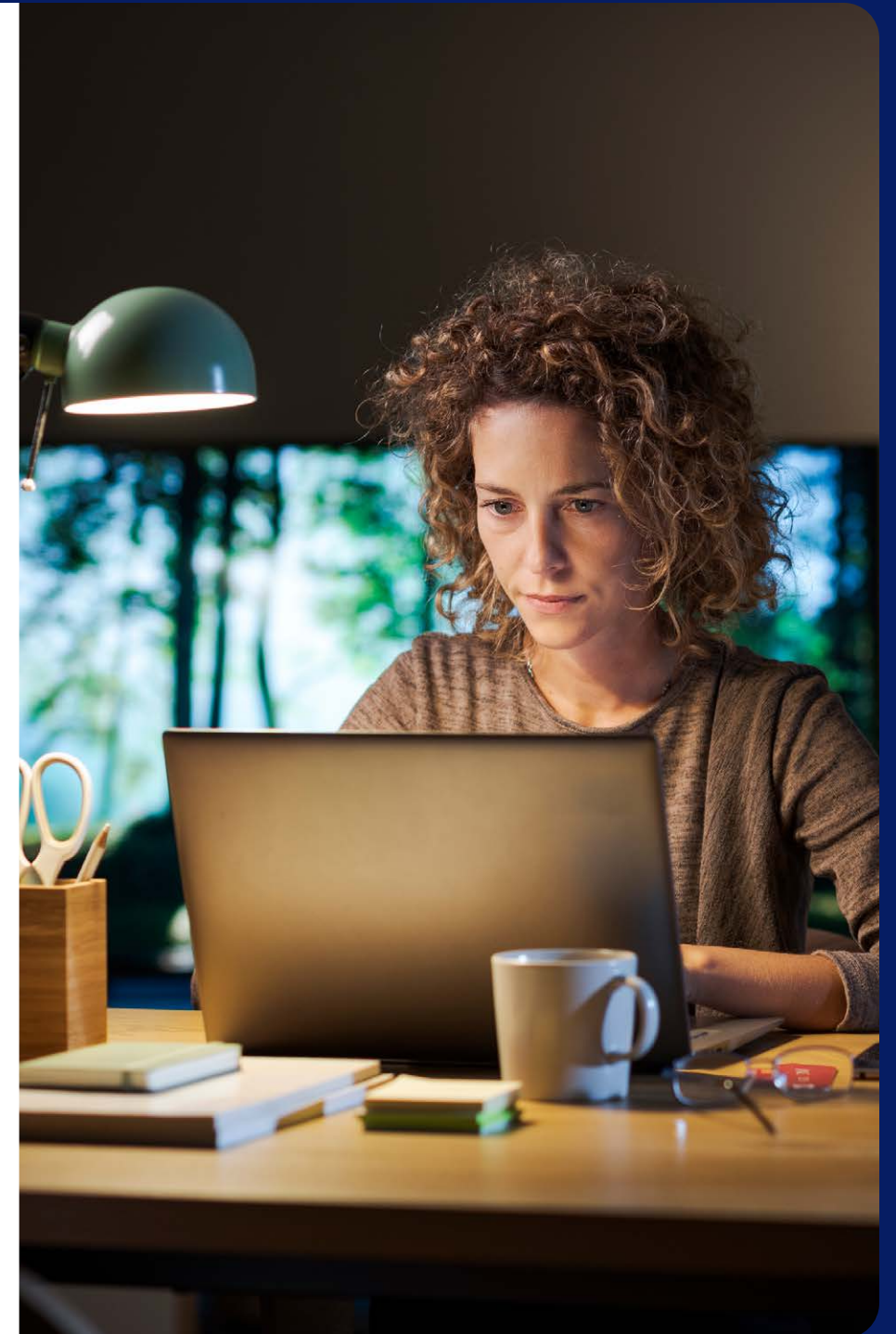
These attacks typically begin with a phishing email, a malicious download, or a compromised website. Once the malware is inside, it can scan local files and insecure password managers, quietly extracting everything it can. The stolen credentials are then sold on the dark web for pennies, shared in private groups, or reused for further account takeovers.

5. 2025 Identity Security Landscape, CyberArk, May 2025.

6. CyberArk, 2025 Identity Security Landscape.

7. CyberArk, 2024 Employee Risk Survey.

8. Verizon, 2025 Data Breach Investigations.



Taken by Blind Spots: A Lack of Consumer Protections

Today's IT teams are dealing with a mind-boggling threat landscape that extends beyond weak credentials. It also includes unsanctioned apps, personal tools, user tracking, and vendors who can become third-party breach vectors. This situation contributes to a shadow infrastructure that security teams don't have the tools to monitor or control.

35%

of employees store workplace-related data in personal storage services like Dropbox or Google Drive.⁹

46%

of compromised systems with corporate login data were on nonmanaged devices, such as BYOD laptops.¹⁰

In addition, the common solutions we rely on are showing limitations. Users often rely on personal, consumer-grade password managers to store business-critical passwords. These managers, however, often prioritize convenience, freemium models, and marketing analytics over strict, enterprise-grade security standards.

Single sign-on (SSO) is a powerful tool, but plenty of high-value apps—like collaboration tools, banking platforms, shipping services—still insist on standalone usernames and passwords. Without secure management for these credentials, organizations leave blind spots scattered across their environment, offering attackers an easy way in. While passwordless authentication solutions promise to reduce password dependency, they don't integrate with legacy applications that still require username-password combinations.

The absence of comprehensive backward compatibility limits adoption, leaving organizations reliant on less secure, password-based authentication for a significant portion of their application landscape. Traditional password storage and fully passwordless solutions are no match for today's advanced identity threats.

Organizations must recognize that using password-centric models as their primary defense is not a strategy, but rather blind hope.

A secure, practical workforce password management solution can:

- Enable stronger workforce access controls.
- Prevent credential leakage to unmanaged applications.
- Deliver enterprise-grade security with consumer-grade simplicity.
- Enterprise-grade security features like integration with adaptive multifactor authentication (MFA).

CASE STUDY

LastPass, one of the better-known password manager entities, made headlines in 2022 with a breach stemming from a compromised developer account.¹¹ A postmortem on the attack revealed that the LastPass Android app had transmitted user behavioral data to third parties for analytics and marketing. There's no such thing as "just analytics" anymore because having more vendors means having a larger attack surface and a greater risk of compromise.

9. CyberArk, 2024 Employee Risk Survey.

10. Verizon, 2025 Data Breach Investigations.

11. Karim Toubba, "03-01-2023: Security Incident Update and Recommended Actions," LastPass, March 01, 2023.

Enterprise Authentication Protection with Idira Workforce Password Management

Palo Alto Networks Idira™ Workforce Password Management delivers end-to-end password protection. It securely stores, manages, and shares workforce credentials in an enterprise-grade vault—providing strong security, simplified access, and full visibility. This solution integrates directly with your organization's identity security framework to deliver a consumer-grade experience that doesn't compromise on protection.

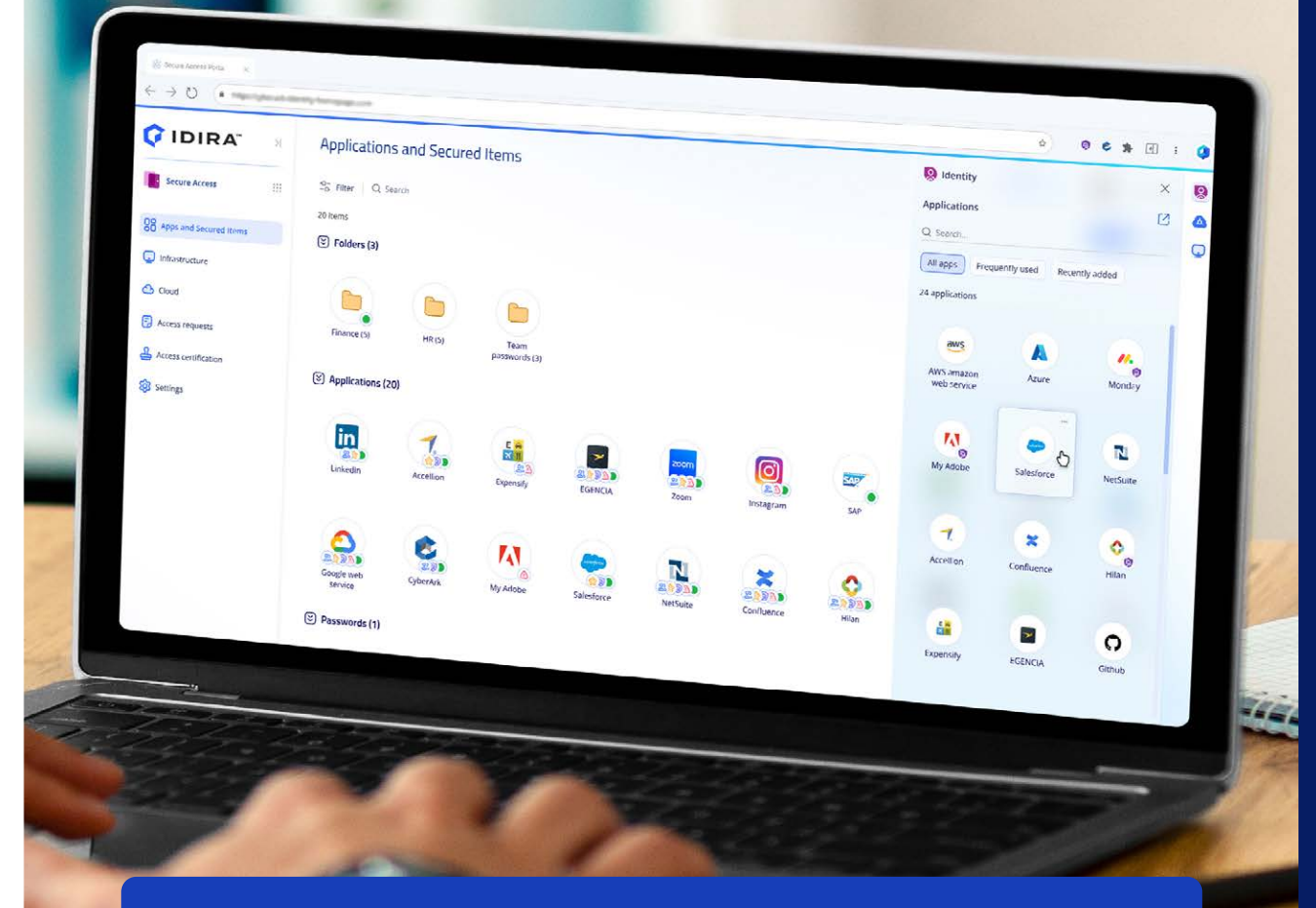
Built for the Enterprise

Repurposed tools and weak defenses leave organizations open to attacks and exploitation. True protection demands a purpose-built solution for enterprise authentication.

Unlike consumer tools, Idira Workforce Password Management avoids master passwords, integrates with identity providers like Entra ID and Okta, is certified for FedRAMP High authorization, and delivers **99.99%** uptime without third-party tracking.

Idira Workforce Password Management avoids caching credentials on the local device and, instead, integrates adaptive MFA for step-up and continuous authentication. With adaptive MFA, organizations get another layer of intelligence so they can dynamically adjust authentication requirements based on user behavior and risk level, keeping sensitive credentials and sensitive sessions out of attackers' reach.

This solution stores credentials in a centralized, secure cloud or self-hosted PAM vault, with the option for on-premises storage, if required, to meet compliance or data residency needs. Admins can enforce IP restrictions, certificate-based authentication, and tightly control which credentials are stored, shared, or blocked at the enterprise level. With Idira, they can also detect and block compromised credentials that were previously involved in a data breach.



Idira Workforce Password Management gives users a single access point for all their resources and applications.

Frustrate Attackers

Designed for productivity, Idira Workforce Password Management delivers enterprise-grade security with a consumer-grade experience. It eliminates password fatigue with features like autofill, land and catch for new credentials, strong password generation, and breach detection. Plus, it detects when users create new accounts, saving credentials securely and enabling effortless enterprise app access.

See Everything Before Attackers Can

Idira Workforce Password Management empowers administrators with strong control over credential use, enabling organizations to:

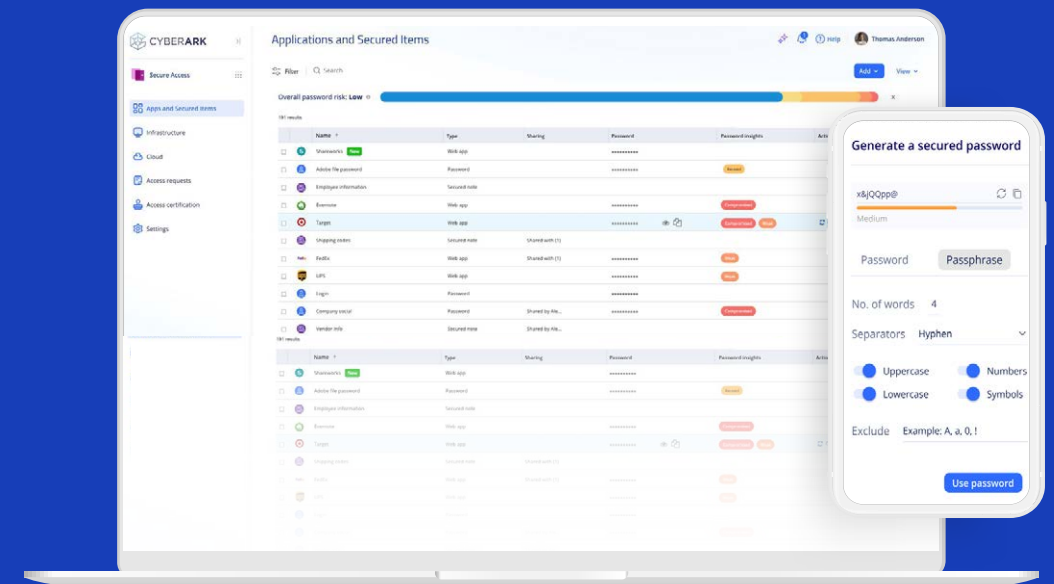
- Set NIST-aligned password policies.
- Block saving credentials for certain domains.
- Instantly revoke access when employees leave.
- Restrict password sharing to managed users only.
- Enforce adaptive MFA that protects users without slowing them down.

With these controls, organizations get the oversight they need to enforce security policies, reduce risk, and maintain control over every credential—before, during, and after access is granted.

Admins can take advantage of dark web monitoring, along with other alerts and reports, to detect risks from aged or weak passwords, boosting your overall security posture.

Idira Workforce Password Management lets employees access shared business accounts—like social media or finance platforms—without seeing or copying the actual password. Credentials are securely autofilled into login fields, preventing unauthorized reuse or leakage. Admins control who can access shared accounts, block password visibility, and instantly revoke access if needed. If an employee leaves, credential ownership can be automatically transferred to another user, maintaining business continuity without password resets or disruptions.

Idira Workforce Password Management supports secure, controlled, and seamless shared access—even as teams change.



Take Control and Secure Your Passwords with Idira

Because attackers always seem to find the gaps, you need to be ready. One weak password may be all that stands between your sensitive data and attackers.

Attackers might have a particular set of skills, but Idira Workforce Password Management makes sure your teams do, too. Organizations worldwide trust Palo Alto Networks to protect their most sensitive credentials. We've built Idira Workforce Password Management on that same security-first, enterprise-grade foundation.

Learn more about how Idira Workforce Password Management improves security hygiene, eliminates frustration for end users, and gives security teams the upper hand. To explore all the ways Idira can secure the identities across your organization, visit [<linked page name>](#).



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.



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

© 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_eb_why-workforcepassword-management-is-non-negotiable_041426