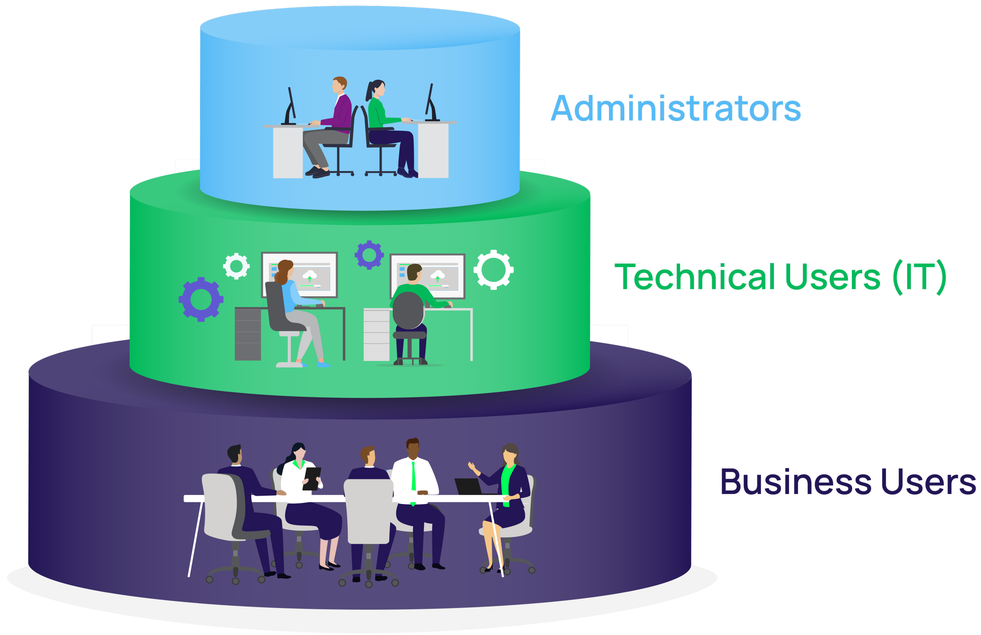
Delinea

The Hidden Risk:

Why workforce credentials need protection

How to incorporate business user passwords in your identity security strategy



Mitigates risk from business users and seamlessly enforces secure credential access for every identity from any browser and any device.

These days, most organizations carefully manage privileged accounts and passwords for a small group of domain administrators and IT staff.

Meanwhile, another attack vector is typically left unguarded: business user passwords.

Non-technical users, such as HR, commercial teams or finance and accounting departments, regularly access confidential, sensitive, and protected personal information (PPI) via business applications.

They are common targets for credential theft.

Business users are notoriously poor at protecting passwords. But it's not fair to blame your workforce for being the "weakest link" in password security.

Most people want to do the right thing.

It's time to stop treating these folks as a lost cause or afterthought. They need the same password security and oversight as your IT team.

See how you can empower your workforce with an enterprise-grade password management solution that offers a consumer-grade experience.

Chances are, each of these scenarios is occurring inside your business

Susan is part of the marketing team and needs to log into social media accounts, data analysis tools, and the Customer Relationship Management (CRM) system. To make it easier to remember, she uses the same password for each of these systems. She also makes occasional purchases with the company credit card, which she stores in her desk drawer.

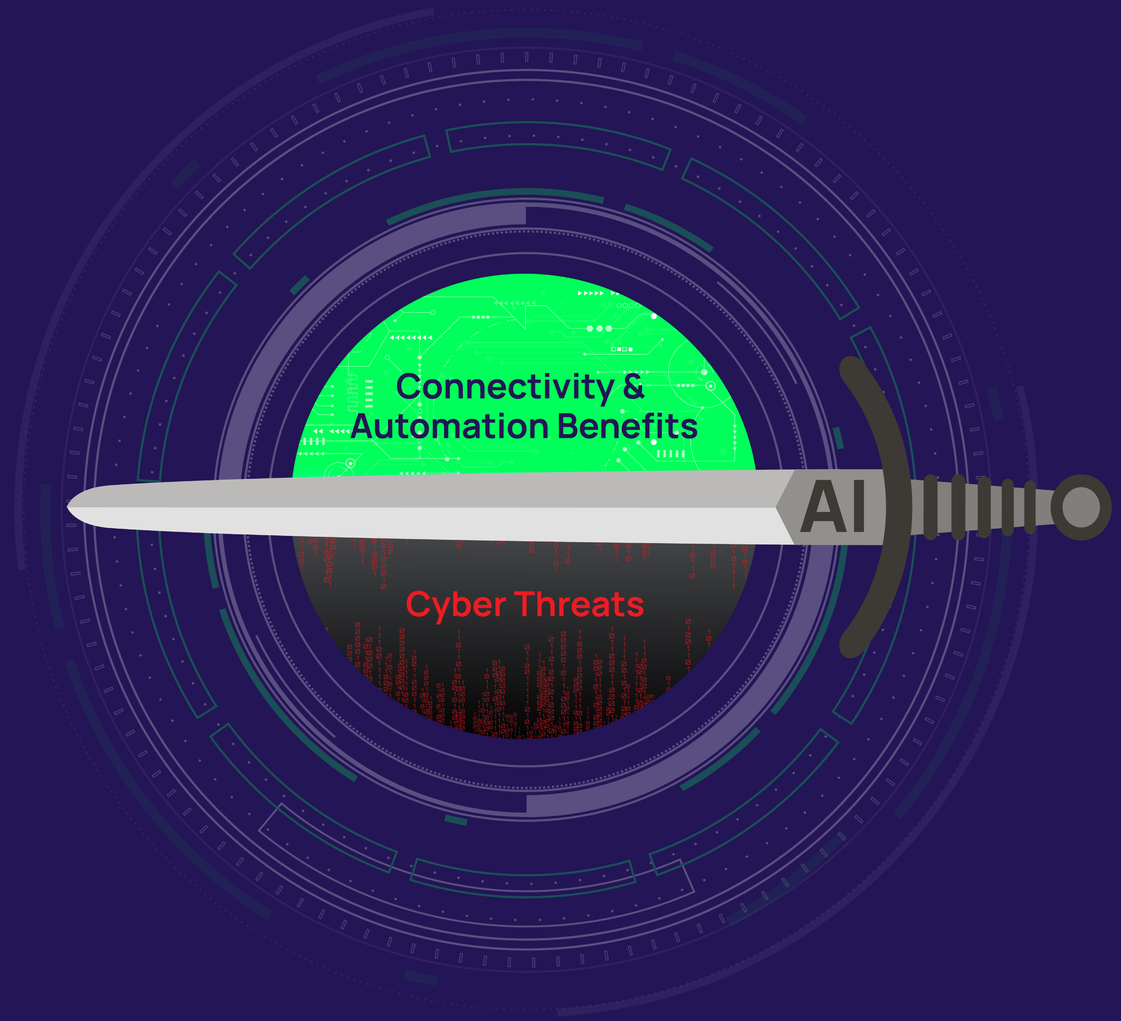
Andrea is a finance manager who frequently accesses the company's ERP system from her browser. She keeps her ERP password in her personal password manager, the same one she uses to store her private passwords, such as Netflix and Amazon. Each month, she needs to share the ERP password with her team members to close out the books. She intends to create a new password to give them each month, but sometimes, she forgets.

John is an IT associate. Even though he is a technical user, he is not an admin, so he is not covered by the organization's PAM policies and workflows. John responds to help desk tickets that often require him to access sensitive company accounts, like AWS. Rather than ask for access every time he needed to make a quick fix, John has memorized a password given to him by his boss. Next week, John is leaving the organization.

These workforce users are prime targets for password-based attacks.

Duplicate passwords, shared accounts, and static access increase your risk. Yet, all these scenarios lack the visibility and oversight of IT. You may not discover the risk before it's too late.

Likelihood of password-based attacks



Compromised credentials are the number one attack method, according to the Verizon Data Breach Investigations Report. The primary vector for these attacks is web applications.[1]

The rise of AI-powered password cracking strategies, including phishing, vibe hacking, credential stuffing, and Infostealer malware, is increasing attack frequency and making attacks more difficult to detect.

1. https://www.verizon.com/business/resources/reports/dbir/

Credentials on the Dark Web

In its *State of the Underground Report*, the Bitsight TRACE Security Research team has suggested that the amount of breach data, including compromised passwords and credit cards, skyrocketed by 43% in the past year.[2]

Recent reports reveal that at least 19 billion compromised passwords have been published online to criminal forums. The vast majority of these are repeated common passwords.[3]

In addition, there are at least 14.5 million credit card numbers listed on underground criminal forums, up 20% over the previous year.[4]

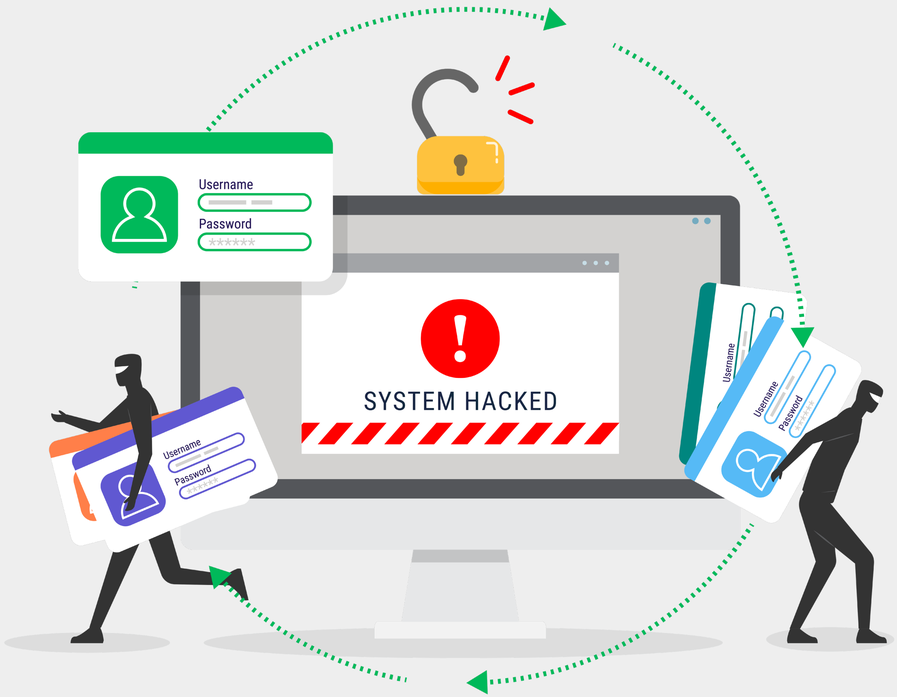
2. https://www.bitsight.com/report/state-of-the-underground-2025
3. https://www.forbes.com/sites/daveywinder/2025/05/06/new-warning--19-billion-compromised-passwords-create-hacking-arsenal/
4. https://www.forbes.com/sites/daveywinder/2025/05/11/dark-web-alert--29-billion-passwords-14-million-credit-cards-stolen/

Common user behaviors expose passwords

Consumer password behavior is notoriously poor. Despite years of password education, “123456” and “password” still top the list of most common passwords.[5] Half of password users apply the same password to more than one account.[6]

Consumer password behavior can infect your workplace. A high percentage of employees admit to reusing passwords between their personal and work accounts, despite knowing the risks. A study from April 2025 found that 46% of employees were reusing passwords exposed in breaches.[7]

Forced password resets are an ineffective tactic to improve password security. Nearly half (49%) of employees simply change or add a digit or character to their password when updating their company password every 90 days.[8]



46% of employees were reusing passwords exposed in breaches

5. https://www.codemotion.com/magazine/cybersecurity/the-most-common-passwords-of-2024-weve-all-used-them-at-least-on-cecybersecurity/
6. https://www.forbes.com/sites/daveywinder/2025/03/14/password-warning-50-of-internet-users-open-to-reuse-attack/
7. https://cybernews.com/security/american-companies-employees-reuse-passwords/
8. https://www.hypr.com/resources/infographic-password-usage

Browser-stored passwords aren’t safe from attack

87 the average number of passwords used for business-related accounts

So they don’t have to memorize passwords, many business users save their login credentials for web applications in their browser. This practice is extremely risky for several reasons:

- Brower-stored passwords can be exposed to attackers by accessing the browser’s memory in plain text or exploiting security flaws in the browser or operating system.
- Malware can access the local files where browsers store passwords.
- Anyone with physical access to a device can potentially access stored passwords.
- Synchronization across devices can be a target for cybercriminals.

In fact, cybercriminals have developed numerous techniques to steal stored browser passwords. These include physical access, synchronization hacks, and targeted malware attacks like RedLine Stealer and XLoader, which are specifically designed to extract stored credentials.

What is IT security to do?

The IT industry is moving away from being the gatekeeper to delegating authority to users.

Instead of having IT manage all security decisions, like password management, delegated authority means giving teams the ability to manage their own requirements, with IT providing guardrails rather than being the bottleneck.

That said, IT is on the hook for risk. If employee passwords are compromised, IT has to clean up the mess. It's a classic case of accountability without control.

So, if you want to balance these competing interests, what are your options?

Placing the onus on employees won't work.

Should you cross your fingers and trust that they'll do the right thing? The data we've just reviewed demonstrates that choice isn't working out too well.

Providing the workforce with a consumer-grade password manager isn't sufficient.

Consumer password managers require that individual users set up, maintain, and always use the app. The user assumes all responsibility for keeping the technology up to date and functioning properly. They must do the heavy lifting of setting up, password rotation, and, most importantly, making sure the password vault is used all the time.

Plus, in this scenario, IT has no visibility, oversight, or control, even if they do set it up. You can't report on password management or demonstrate compliance to regulators, auditors, or cyber insurance companies.

A workforce credential vault is the way forward

The best option is an enterprise-grade password vault without the complexity or management overhead of fully featured Privileged Access Management (PAM).

This type of password vault provides a consumer experience and enterprise-level security.

The IT team assumes responsibility for the tech behind corporate password security. They do the work of getting it started and keeping it going. All the user does is enjoy it.

With a consumer-grade experience, users are more likely to adopt the vault

- Users can create, store, share, and access credentials when they need them
- In one click, they can autofill credentials in a web app, using any browser or mobile device
- It doesn't interrupt their workflow, so they stay productive
- They could even store data business users need to keep private and secure, such as credit cards, bank account information, and alarm codes

With enterprise-grade controls, IT security teams have oversight for compliance

With ALL passwords in a central vault, IT can enforce best practices, such as creating complex, unique passwords that meet compliance requirements and rotating them automatically to avoid reuse.

IT teams or app administrators can distribute necessary access to vaulted credentials to business users and be confident that strong credential hygiene and controls are in place across the organization.

If you don't already have a fully featured PAM vault, consider vaults that provide both sides of PAM: enterprise-grade controls for administrators and easy-to-use workflows for business users and IT admins.

You don't want to manage two systems, one for your account admins and one for the rest of your workforce. So, any vault you provide your workforce should be fully synchronized with all password policies and central reporting to ensure oversight and compliance.

Learn about Delinea Credential Manager

Delinea provides a simplified vault experience that enables business users to access essential credentials seamlessly from anywhere in any browser, while leveraging the power and flexibility of enterprise-grade controls. This gives IT admins full visibility into user activity and consistent oversight across the organization.

See for yourself how Delinea Credential Manager ensures seamless credential access across web and mobile, reduces risk with granular controls, and enhances administrator visibility into credential hygiene and usage across all identities.

Delinea

WATCH THE DEMO

Delinea Credential Manager: Simple and secure access for your entire workforce

Delinea

Stop unauthorized access

Delinea is the identity security control plane enterprises trust to secure human, machine, and AI identities across on-premises, multi-cloud, and dynamic environments. Built for the AI era, Delinea continuously discovers identities, analyzes risk, and enforces least-privilege through just-in-time, policy-based authorization. By supporting both credential-based and ephemeral access models, Delinea enables organizations to reduce risk, simplify governance, and move toward Zero Standing Privilege at their own pace. Easy to deploy and built to scale, Delinea delivers value in weeks, not months, with up to 90% fewer resources required and 99.995% uptime. Learn more at **delinea.com**.