bitwarden | Resource Center

Every second counts: 9 days to fix at-risk credentials is too long

Two thirds of IT admins say credential management is crucial. So why do so many lack the tools to do it? Find out in the latest Bitwarden Business Insights report.

View the full interactive version at:

https://bitwarden.com/resources/bitwarden-business-insights-report/

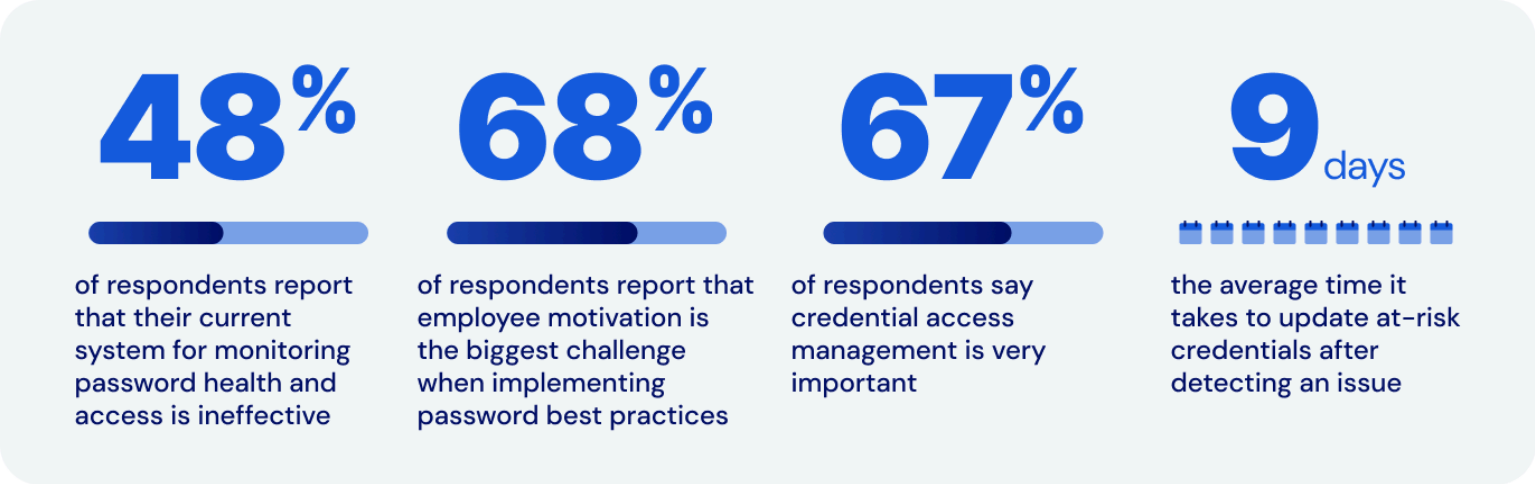
Executive summary

Weak or compromised passwords are easy to crack or purchase on dark web marketplaces. These flimsy credentials are the digital equivalent of a front door with a key left in the lock: It's trivial for attackers to use them to gain illicit entry into an organization.

Yet updating these passwords is a constant challenge. IT admins often lack visibility into which passwords are weak, reused, or compromised. Even when they can identify at-risk passwords, it can be challenging for them to convince users to update their credentials or replace them with stronger ones. Poor password monitoring can also lead to uncontrolled access to sensitive, high-privilege systems, opening the organization up even more security risks.

To understand this landscape, Bitwarden conducted a survey of IT managers to understand their pain points concerning password health visibility and remediation. These findings were compiled in the following Bitwarden Business Insights 2025 report.

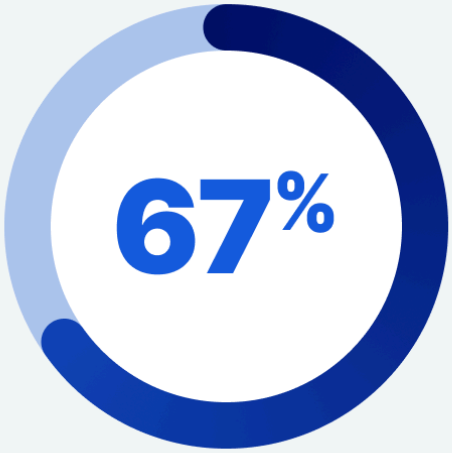
Key findings



A closer look: Credential monitoring is needed, but often absent or lacking in the current toolset

Two-thirds of respondents (67%) say credential access management is very important for their organizations. However, almost half (48%) report that their current system for monitoring password health and access is ineffective.

Credential access management is a top priority for two-thirds



of organizations say credential access management is very important for their organizations.

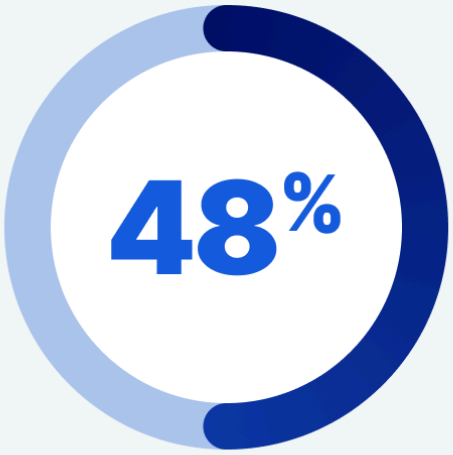
This lack of effective password health monitoring and visibility directly contributes to unmet security goals and slow resolution.

For example, 53% of IT managers want to tackle credential-related security proactively, but only 33% say they are currently doing so. About 60% of IT managers say their current strategy for updating at-risk credentials in a timely manner is only somewhat effective or completely ineffective.

Usually (90% of the time), respondents ask employees to update their own credentials, and they most often do this through an email (42%) or one-on-one conversations (36%).

Unfortunately, over half of IT managers (51%) report that their employees don't take cybersecurity measures seriously at all or only somewhat seriously.

Organizations struggle with ineffective password monitoring



of organizations say their system for monitoring password health for critical applications is only somewhat effective or totally ineffective

As a result, employees take an average of 9 days to update their at-risk credentials after detection, leaving these credentials as open vulnerabilities for malicious actors to exploit. One organization reported that employees take a whole year to update at-risk credentials!

Delayed credential updates leave organizations vulnerable to attacks

9 days
the average time it takes to **update at-risk credentials** after detecting an issue

Motivation and prioritization: The keys to improvement

The biggest challenge in changing this widespread credential management problem and implementing password best practices is finding a way to motivate employees to change their habits, as reported by 68% of respondents.

Employees themselves may not have the tools or information they need. Among IT admins, 44% say that employee confusion about how to make password changes is a challenge, and 36% complain of difficulty tracking employee progress toward more secure practices.

The top strategy for more effective cybersecurity, cited by half of IT managers (51%), is to prioritize critical security actions more clearly. Additionally, almost half would like to see more intuitive workflows for nontechnical people (46%) and more regular security training (45%). Forty percent would like to have visibility into who hasn't completed crucial security tasks.

Combining effective prioritization, workflows, and training would help these managers better demonstrate to employees the value of having secure credentials — and would enable them to focus on the credentials and privileged users that are most at risk. That, in turn, would help motivate employees and reduce the time to update weak or compromised passwords. Implementing these strategies will help organizations better protect their business applications, infrastructure, and accounts from malicious actors.

Monitor password health and manage access across the organization with Bitwarden

Bitwarden empowers IT teams with the tools they need to securely manage their organization's credentials with security solutions for least privileged access, passwords, secrets, and passkey management. Trusted by tens of thousands of businesses and millions of users worldwide, Bitwarden makes it easy for employees to adopt strong password best practices and for administrators to manage organization vaults.

For organizations that struggle with identifying password health, Bitwarden offers vault health reports, which enable IT admins to detect at-risk credentials — including exposed, reused, and weak passwords — associated with their organization. This is the first step towards strengthening credential-related security posture.

Once at-risk credentials have been identified and employees are notified, the built-in Bitwarden password generator enables end-users to quickly replace an offending credential with a strong, unique password and securely save it to their company vault.

Give these security features a test run with a free 7-day Bitwarden business trial!

Methodology

Bitwarden survey targeted IT admins and owners at companies with more than $1M in revenue. Responses were collected during late 2024 and early 2025, receiving 108 responses in total.