bitwarden | Resource Center

Bitwarden Security Impact Report

Mandates, communication, and leadership combine to streamline password management adoption

View the full interactive version at:

https://bitwarden.com/resources/bitwarden-security-impact-report/

2025 Report: Mandates, communication, and leadership combine to streamline password management adoption

Executive Summary

Bitwarden, the most trusted password manager, is used by millions of individuals and organizations to securely store their sensitive information and enhance their security posture. IT leaders praise Bitwarden for “smooth” and "easy” implementations to their organization.

But how do you get employees actually using and enjoying the benefits of password management? In 2025, Bitwarden surveyed IT managers and enterprise users to find out.

> **The bottom line? Leadership is critical to adoption success. Company-wide password management mandate more than doubles regular usage.**

However, it’s not enough to simply lay down the law: Communicating the “why” of the deployment, providing training materials, using technical enforcement methods like preventing users from storing passwords in their browsers, and ensuring buy-in from leadership are all crucial for ensuring regular usage.

By the numbers

- 99% of Bitwarden enterprise customers reported that Bitwarden has improved their company’s security posture
- 35% say the biggest challenge to password management was user resistance
- 2.4x more employees use Bitwarden regularly when it is mandated company-wide, compared to organizations without a mandate
- 43% reported that technical enforcement is one of the most effective techniques for encouraging usage
- 38% reported that executive announcements (via email or company-wide meetings) were the most effective communications strategy

Bitwarden improves your security posture

Much like last year’s Security Impact report, nearly all respondents said that Bitwarden has improved their company’s security posture, once it’s been deployed and is in place long enough to determine an effect.

- 99% of customers that have fully rolled out Bitwarden said that their company's security posture had improved.
- 68% attributed their security posture improvements to eliminating at-risk, weak, or reused passwords.
- 55% reported that they have increased awareness amongst employees of the importance of using strong, unique passwords across accounts.

"When we first adopted Bitwarden, we had some users with over 200 passwords that were reused. It is much better now," said one respondent.

Another survey respondent noted, "It's a no-brainer. Do it. This is such an easy win for your security posture. It's easy and effective. Your overall security posture will be significantly higher once this is completely rolled out."

Company-wide mandates help drive adoption

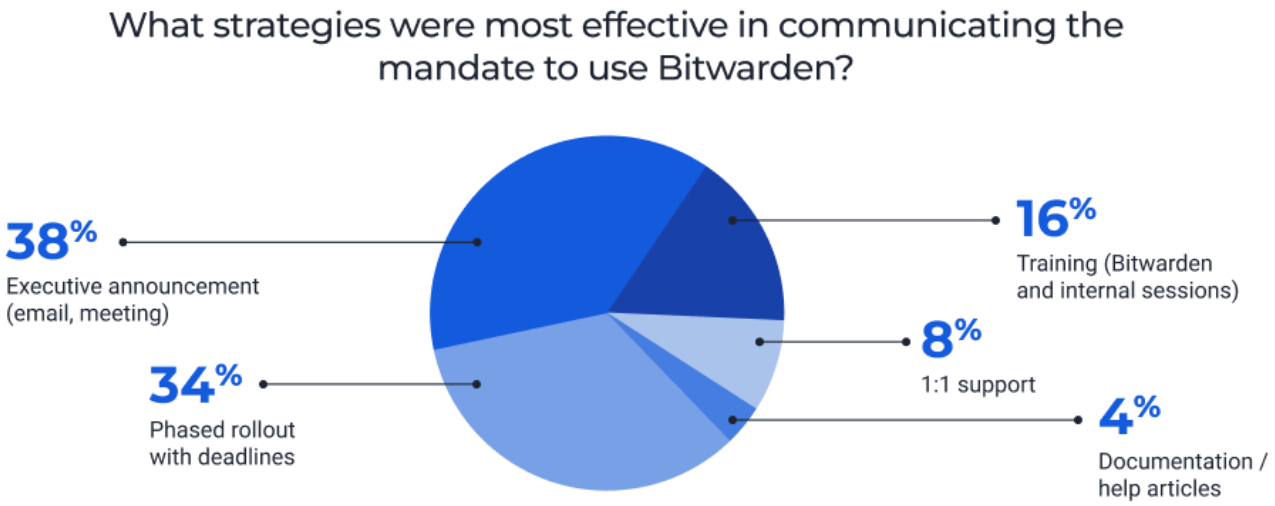
When deploying a new password manager, the biggest challenge is getting users onboard with the new way of managing passwords and logging in to the services they use every day.

> **Key insight:** Your biggest security threat could be your own employees. 1 in 3 companies say the biggest challenge faced was getting employees to use a password manager.
>
> In companies with a company-wide mandate, 79% of users were actively using Bitwarden. That's more than twice the adoption rate of companies with department-level mandates.

"Before Bitwarden, people had all kinds of logins to websites stored in the browser. We stopped that," said Tony Manzo, IT Manager at MDI Hospital. "We mandated no more password storage in browsers. If you do want to store passwords, use a password manager. 75% to 80% of our employees now take advantage of that function."

Mandates alone are not enough. Communicating the "why" for moving to Bitwarden and providing training sessions and documentation will all help overcome resistance.

"I'd advise clear communication of the policy's purpose to gain buy-in, choosing a user-friendly tool like Bitwarden to ease adoption, and providing thorough training to address usability challenges," said one survey respondent. "Ensure IT support is ready for setup issues and emphasize security benefits to motivate compliance."



How to stop password resistance now

Technical enforcement and department-by-department rollouts are also effective tools for driving adoption.

Say 'No' to browser-based password managers

Remove access to browser-based password storage and other password managers. If users want to store a password, they need to use Bitwarden. This approach was rated "very effective" at driving adoption by 43% of respondents.

Stop 'hand-delivering' passwords

When employees ask for passwords or credentials, make them go through Bitwarden instead.

"Every time someone would want a password shared, IT would send it through Bitwarden. That's how we helped a lot of the users that didn't implement it at first," said Kyle Morrison, IT Specialist at Securly. "Bitwarden was the only way they could have this shared password, in the collection with all your other teammates. That's where everything's stored and that's where everything's going to be stored for the future."

Win department by department

Customers recommend conquering one department, then expanding. The phased rollout approach, department by department, was rated "very effective" by 35% of respondents.

"One of the best ways that we addressed any kind of employee resistance to using a password manager was phased rollouts based on departments," said Michael Young, IT Support Specialist at Point North Insurance Group. "We started with our accounting team and then they were basically the pilot group for it. Then we just rolled it out to everyone."

Use every communication tool available to support rollout

Successful teams didn't just send one email – they used every communication tool available to communicate the why, how, and when surrounding Bitwarden rollout. Cover your employees with support from every channel.

Fun fact! The most popular knowledge management tool was Confluence, cited by 40% of people taking the survey. The most common form of communicating a Bitwarden rollout was email, cited by 75% of respondents.

Multiple strategies advised

When asked what advice they would give to other companies considering a top-down mandate for their password management strategy, Bitwarden customers gave a variety of recommendations, with the majority of respondents suggesting a mandate and dedicated training.

IT champions Bitwarden, but execs provide leadership

In 81% of the cases reported in our survey, IT or security teams are the champions of Bitwarden deployment, but winning executive buy-in is also necessary.

Key insight: 38% of customers say that executive announcements, either in company meetings or emails, were the most effective communications strategy for getting everyone aligned.

"The C-suite was on board right from the start. Bitwarden was optional but the CEO, CFO and the CTO said, 'Hey, you need to get on Bitwarden.' That helped from an employee's perspective," said Kyle Morrison, IT Specialist at Securly.

But it's not enough for execs to communicate: They also need to demonstrate leadership, not just management. In other words, they need to model and inspire the organization to make the change.

"Once we showed management how easy it was to autocomplete their credentials, they were all in at that point. Bitwarden wasn't a hard sale at all," said one respondent.

Methodology

Bitwarden surveyed enterprise customers, including end users and IT admins from May 12th to June 10th 2025 and received 111 responses, including 81 IT administrators, 14 department heads, 4 executive leaders, and 7 end users. Follow-up questions were sent to selected IT admins to ask them more specific questions about how they're using Bitwarden.

To find out more about how Bitwarden can improve your organization's security posture and password management adoption, start a free 7-day business trial today.

2024 Report: Enterprise Password management leads to better security

> Download the summary presentation here.

Executive summary

Bitwarden offers the easiest and safest way for enterprises, teams, and individuals to store and share login credentials and sensitive information from any device. Trusted by millions of users, Bitwarden protects online information with end-to-end encryption and a trusted open-source architecture. Bitwarden also supports global accessibility for more than 50 languages.

Bitwarden Password Manager empowers administrators to securely grant credential access and sharing across their workforce, monitor and manage credential usage and vulnerabilities via Bitwarden vault health reports, and securely store and sync all login credentials – including passwords, passkeys or passphrases – in the cloud.

> In 2024, Bitwarden surveyed enterprise end users and IT admins about the impact Bitwarden Password Manager has had on their lives and organizations.
>
> **Key findings:**
>
> 96% of all respondents say Bitwarden **has improved their security posture**
>
> 88% of admins using Bitwarden are rolling out **regular password security training**
>
> 81% of all customers have **reduced reused passwords since using Bitwarden**

> 45% say they've eliminated **more than 15 reused passwords**

Overall, respondents said that Bitwarden helps them:

- Mitigate security risks
- Improve overall security culture
- Identify and fix exposed and reused passwords

Bitwarden Security Impact — Bitwarden plays a critical role in improving enterprise security

Bitwarden mitigates security risks

Key finding: 96% of all respondents say Bitwarden has improved their security posture

For IT administrators and end-users alike, passwords remain one of the biggest security risks. If an attacker can discover a user's password, it could give them access to everything the user can do on their computer — and the company's network. That, in turn, could lead to a host of threats, ranging from data theft to ransomware.

Attackers can use several avenues of attack. Passwords that are weak (too short or too easy to guess) are subject to brute-force attacks, where the hackers simply try many different common passwords in quick succession until something works.

Reused passwords introduce another layer of weakness. If a user has the same password for multiple services — which is common, because people find it hard to memorize many different passwords — then an attacker has only to get one password and they suddenly have access to many resources.

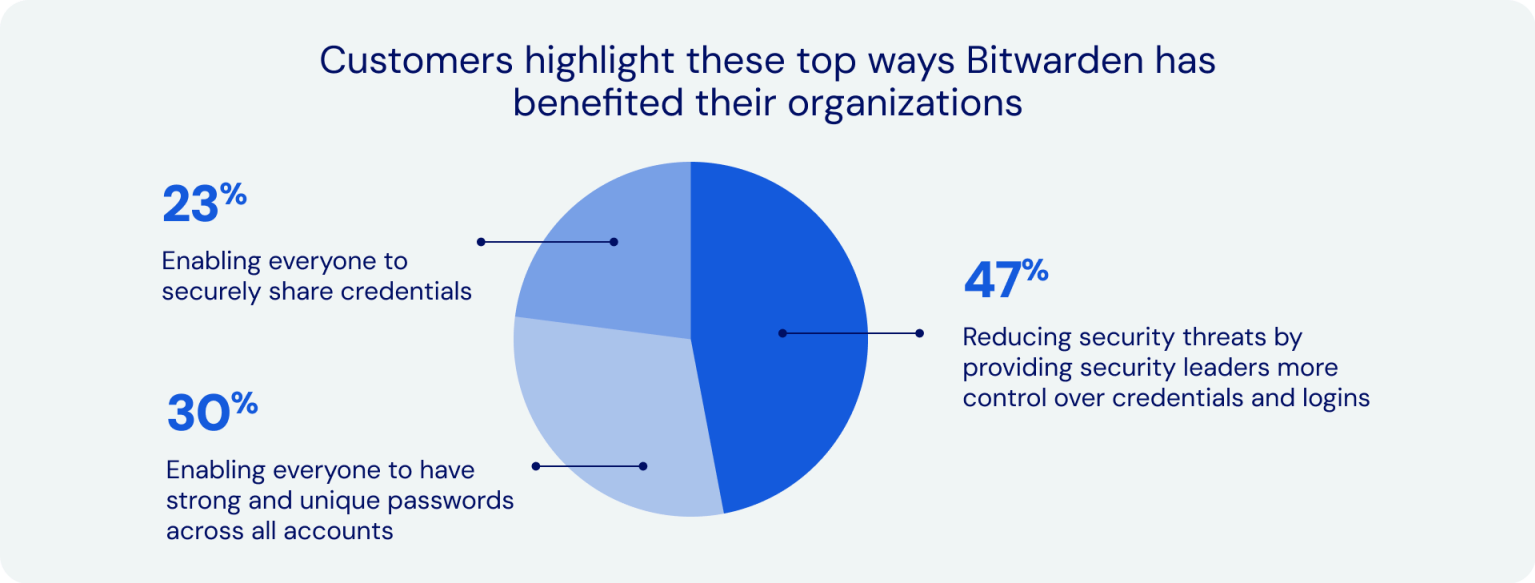
Finally, if a password has been cracked or stolen, it may wind up on a list of known passwords shared with other hackers. Unless the user changes the password, these compromised passwords allow any number of hackers access to the user's account.

With Bitwarden, users have multiple options they can use to eliminate at-risk passwords, including the Bitwarden password and passphrase generator for strong and unique passwords for every website, or by creating passkeys for sites where they are supported.

Fortunately, the vast majority (96%) of all respondents — end-users and IT admins alike — say Bitwarden has been able to improve their security posture, reducing the number of weak, reused, and compromised passwords.

More than three-fifths of IT admins reported that their organization has mitigated security risks and that they have been able to prevent breaches using Bitwarden. In addition, many have been able to reduce known security threats.

> **"Bitwarden has become an invaluable tool in our corporate security infrastructure. And it's intuitive, easy to use, deploy and manage." — IT admin at CoreTec Pro**



Bitwarden Security Impact — Enterprise customers highlight these top ways Bitwarden has improved their overall security

Bitwarden improves security culture

Key finding: 88% of admins using Bitwarden are rolling out regular password security training

Password security training is essential for maintaining a strong security posture. Without training, employees will choose passwords that are too easy to guess, like simple sequences of numbers, the word "password," or their own birthdates.

As the U.S. Cybersecurity and Infrastructure Security Agency (CISA) says, choosing a simplistic password that is easy for attackers to guess is "like locking the door but leaving the key in the lock."

Passwords need to be:

- Long enough that they're difficult to crack (16 characters is great)
- Comprised of a random string of numbers or a passphrase made out of random words
- Unique (not used for more than one account)

Regular employee training is key for helping employees understand the importance of good passwords and the criteria that they need to use when choosing a password.

Because it's difficult to think of and remember good passwords for the vast number of accounts people have today, a password manager like Bitwarden is crucial.

Many IT admins have found that deploying Bitwarden facilitates training and reinforcement of good password policies. Since rolling out Bitwarden, 88% of IT admins surveyed say they have already incorporated regular password security training in their organizations, or plan to do so soon.

> **"Storing credentials using Bitwarden has been a godsend. It's made it very easy to find what we need and also makes for easy password changes, tightening our security posture. By storing credentials, we were able to do a complete credential refresh across the business, which removed multiple repeatedly used passwords." — IT admin at thechange.co.uk**

Bitwarden reduces exposed and reused passwords

Key finding: 81% of respondents have reduced the number of reused passwords in their organization

Compromised passwords are among the greatest security threats facing any organization. These are passwords obtained by attackers, either through brute-force attacks, guessing, hacking, or other means.

According to the 2024 Verizon Data Breach Investigations Report, 98% of all web application attacks in 2023 happened because of weak or stolen passwords (77% via stolen credentials and 21% via brute force attacks, which usually leverage easily guessable passwords).

Once stolen, passwords often appear in online marketplaces — the Verizon report authors found thousands of users' passwords offered for sale per day, for about $10 each, often appearing within a day of when they were stolen.

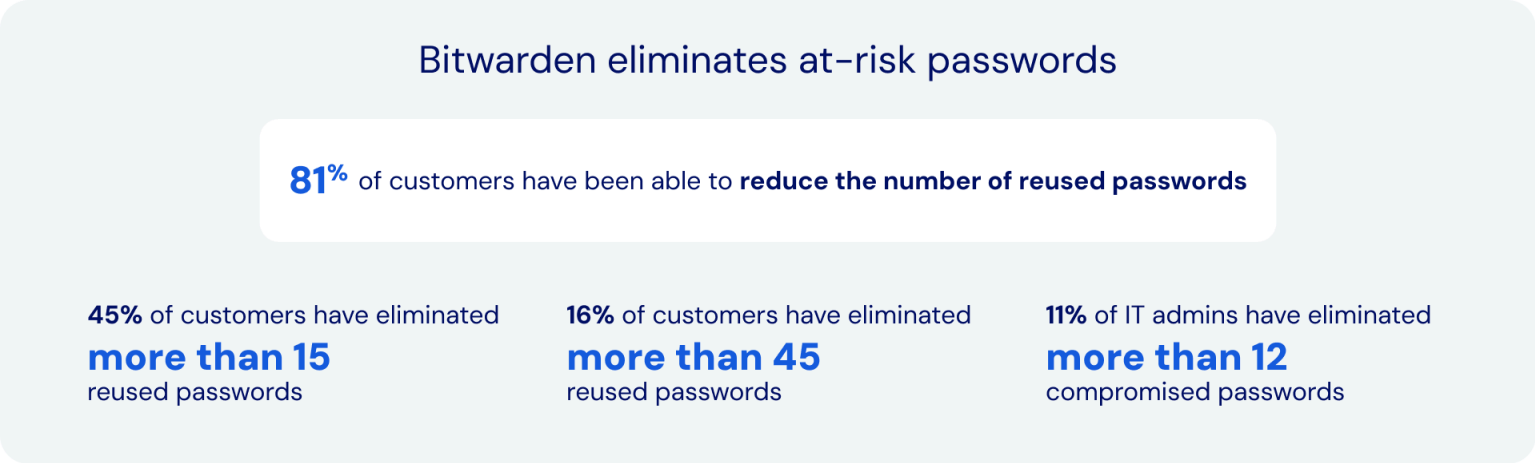
People who reuse their passwords multiply the problem. Once a password is stolen, it then renders all of the accounts where it's used vulnerable.

While some big tech companies, such as Google and Apple, now offer warnings if they detect a password that has appeared in one of these marketplaces, organizations need a more comprehensive solution. That's where Bitwarden comes in. Through comprehensive password management, IT admins and end users can discover which of their passwords might have been exposed in a data breach — and which are being reused.

As a result, more than four-fifths (81%) of Bitwarden customers have been able to reduce the number of reused passwords. Almost half (45%) say they've eliminated more than 15 reused passwords, and 16.5% say they've been able to eliminate more than 45. What's more, 11% of IT admins say they've been able to identify and eliminate more than 12 compromised passwords. That's a big impact!

> **"It was eye-opening and alarming for users to see how many times they used the same password. After we implemented Bitwarden, we updated the frequency and complexity of our domain accounts. We also required the use of stronger and unique**

> passwords and increased the frequency of password rotation." — IT team at RiverStreet Networks



Bitwarden impact — Bitwarden helps enterprises eliminate at-risk passwords that can lead to serious data breaches

Take control of your security

Bitwarden has a large, positive impact on both end-users and the organizations that use it. Respondents to our survey noted that it helps them mitigate security risks, improve their overall security culture, and identify and fix passwords that have been compromised or that are being reused.

IT admins appreciated the way that Bitwarden improves their organization's security posture, facilitates user education, and gives them more control.

For IT admins, here are the top benefits they cited:

- Reducing security threats by giving me more control over my credentials and logins
- Enabling me to have strong and unique passwords across all my accounts

End-users also appreciate the security and control Bitwarden gives them. The top benefits cited by end users are the same, although in a different order:

- Enabling me to have strong and unique passwords across all my accounts
- Reducing security threats by giving me more control over my credentials and logins

In short, Bitwarden has a demonstrably positive effect on improving companies' security posture and security culture. And both end-users and IT admins alike are enthusiastic about how it enables them to have greater control and reduce security threats.

For enterprises that are exploring passwordless authentication, Bitwarden also offers passkey management for all users, and passkey APIs and developer toolkits for developers to easily deploy passkey authentication.

To find out more about how Bitwarden can improve your organization's security posture and culture by reducing password reuse, start a free 7-day business trial today.

Bitwarden impact — With Bitwarden, both IT admins and end users take control over password security

About Bitwarden vault health reports

Bitwarden vault health reports leverage dark web monitoring, data breach monitoring, and other services to keep individuals and organizations secure. These reports flag exposed, compromised, reused, or weak passwords, alerting end-users and admins to the need to correct these security vulnerabilities. They also help identify any unsecured websites, sites where multifactor authentication is available but is not being used, and any data breaches associated with vault websites.

Methodology

Bitwarden surveyed enterprise customers, including end users and IT admins from June to September 2024 and received 116 responses, including 87 IT administrators and 29 end users. Follow-up questions were sent to select IT admins to ask them more specific questions about how they're using Bitwarden.