RESOURCE CENTER

9 steps to a successful top-down approach with your password manager

Get the full interactive view at https://bitwarden.com/resources/successful-top-down-approach-with-your-password-manager/

bitwarden

Mandate security from the top. Exec leadership drives stronger adoption and resilience

When implementing a password manager, some companies opt to make using the new tool optional rather than required for employees. Companies that go this route often face hurdles around adoption of their password manager, and they see fewer employees develop the habit of using a password manager to secure all their sensitive information.

Meanwhile, other companies elect to require the password manager company-wide, **approaching the roll-out as a top-down initiative with a C-suite level mandate**. This requires thoughtful change management, and when successful, the key goal of improved cyber security is met with the global implementation of a company-wide password manager. "Change management" means managing the change—this is something that happens when new policies or processes are mandated across an employee base.

Bitwarden data and surveys of customers have shown that companies that take this approach have higher adoption rates for their password manager—and are thus more secure. They are able to ease the burden of employee provisioning & deprovisioning, create and enforce company-wide credential policies, and reduce risk with the use of shared credentials—to name just a few of the benefits of requiring adoption of a password manager company-wide.

Here are seven proven principles to follow when implementing a password manager across the entire organization:

Companies that take a top-down approach to password manager implementation have higher adoption rates—and are thus more secure.

#1: Announce company-wide, through multiple channels

Take advantage of these pre-written email templates that will help you announce the roll-out of Bitwarden Password Manager to your end-users and IT team. It's also important for employees to see high-level executives talk about security on all-hands or town hall calls and presentations to help jump-start buy-in.

#2: Consider a practical approach to making password management a workplace requirement

Implementing any requirements across an organization requires flexibility, clear communication, and consistency. Instituting password management is a common path for enterprises that are taking security seriously. Those setting the requirements need to clearly document and communicate these policies; employees need a way to understand and acknowledge what's expected of them. Consider Why bring Bitwarden to your entire business – it might convince you to do so.

#3: Create a documented rollout plan

Use our detailed roll-out guides to help make Bitwarden a success at your organization. Read through Rolling out the Bitwarden Password Manager to your Organization and use the Bitwarden Enterprise Password Manager Implementation Guide to help you structure and schedule the key phases of your rollout.

#4: Enact company-wide training

Have your IT department set up training sessions across the company in order to support all employees learning how to use the new password manager. These can be organized by departments or teams, and they can be virtual training sessions available to everyone.

#5: Place critical passwords within Bitwarden

Companies can add an element of hands-on learning by storing passwords that employees need for their daily work in the new password manager and asking them to access the password manager in order to get the login credentials. This ensures that they will follow through on logging into Bitwarden and is a fun way to help employees learn how to use their new password manager.

#6: Move your team away from browser-based password managers

There are many reasons to discourage, or even prohibit, employees from using browser-based password managers: lack of cross-browser support, limited device compatibility and secure sharing. Probably the most important issue is that of security. Browser-based password managers simply lack critical security features such as advanced multifactor encryption and authentication to protect your credentials. Also, keep in mind that browsers are built to give you access to websites and not to protect your credentials with end-to-end encryption. Learn more about why companies are looking beyond browser-based password managers here.

Additional resources

Instructions on how to deactivate browser password managers using device management

Instructions on how to automate deployment of Bitwarden browser extensions to users with an endpoint management platform or group policy

#7: Install Bitwarden on managed devices

Make your password manager part of the default software suite given to all employees on their professional computers. This reduces the friction of users needing to install the software themselves and sends the message that cyber security is a core priority at your company. Here's a useful guide on how to deploy the Bitwarden browser extension company-wide.

#8: Build a security culture

Prioritize building a cybersecurity culture in the workplace by implementing key strategies, such as ensuring credential security best practices and regular cyber awareness training. Cybersecurity and strong password management practices is not a set-it-and-forget-it thing—it requires regular training, reminders, check-ins, and educational opportunities.

#9: Turn your leaders into champions

Organizations that want to promote a robust, top-down cybersecurity culture should ensure that the reasoning for the need for a password manager is understood by C-level executives, and that VPs, directors, and other people leaders share this information with and encourage their own reports to use Bitwarden. Provide them special training in Bitwarden geared toward leaders, such as how to manage a team collection, and use this as an opportunity to practice change management skills.

Wide adoption for high ROI

Some organizations may worry about the cost of implementing a password manager company-wide, but history shows that data breaches are far more expensive. According to IBM's Cost of a Data Breach Report 2024, the average cost of a breach in 2024 is $4.88M USD - a 10% increase over last year and the highest total ever.

What's more, a relaxed, inconsistent approach to cybersecurity on the part of an organization can lead to the exposure of highly sensitive information—nearly 10 billion passwords were publicly uploaded and exposed in the rockyou2024.txt file. Organizations that make their password manager rollout a top-down initiative with a C-suite level mandate are poised to potentially save millions, while protecting their company's most sensitive information and optimizing their employees' time.

The average cost of a data breach in 2024 is $4.88M USD, a 10% increase over last year and the highest total ever.