RESOURCE CENTER

Password Management Maturity Model

from Bitwarden

Get the full interactive view at https://bitwarden.com/nl-nl/resources/password-management-maturity-model/

bitwarden

Password Management Maturity Model

Success Factors	LEVEL 1 Open	LEVEL 2 Launch	LEVEL 3 Evolve	LEVEL 4 Proactive	LEVEL 5 Leader
Password Manager Deployment	Password free-for-all	Decentralized password management	Limited password management	Rising employee adoption	Complete organizational adoption
Security Culture	Minimal security awareness	Building on the basics	Security culture emerging	Actionable employee awareness	Employees leading security improvements
Technical Maturity	Land of do-it-yourself	Isolated solutions	Coverage underway	Connected into IT workflows	Comprehensive coverage and reporting

bitwarden

Organizations that wish to strengthen security by deploying an enterprise-wide password manager can ensure better resilience by assessing key areas for improvement through the following password management maturity model. This framework helps organizations understand their password manager maturity level — based on their current operations — and identify what steps are necessary to improve their existing classification.

Level 1: Open opportunity

The wild west of weak passwords, reused passwords, and potentially compromised passwords

LEVEL 1
Open

Password Manager Deployment	Security Culture	Technical Maturity
Password free-for-all No password manager processes in place	**Minimal security awareness** No emphasis on security best practices	**Land of do-it-yourself** Sensitive information often shared unencrypted

Level 1 organizations are starting from the ground up with plenty of opportunities for quick improvements through simple actions that can provide an immediate security boost.

Organizations in the Level 1 category have not deployed an enterprise-wide password manager. The lack of a centralized password management system increases the risk of compromised passwords, as employees may use weak or reused passwords without proper oversight. Instead, employees take a siloed, ad-hoc approach to securing company passwords. This may involve using browser-based password managers, Excel spreadsheets, sharing passwords via Slack, or writing them down on paper and sticky notes. This environment is unlikely to foster a robust security culture or emphasize security best practices. Company-wide training is infrequent or non-existent. When it comes to overall technical maturity, there is a strong likelihood that sensitive or critical data, when shared, is unencrypted and at risk.

- **Password Manager Deployment**: A Level 1 organization has no password manager processes in place, leaving employees to their individual habits.
- **Security Culture**: A Level 1 organization does not emphasize security best practices and has minimal security awareness.
- **Technical Maturity**: A Level 1 organization shares sensitive information insecurely, often unencrypted.

Level 1 organizations are starting from the ground up with plenty of opportunities for quick improvements through simple actions that can provide an immediate security boost. The priority next step for a company to improve security is to require one team to use a password manager, typically IT, and then make a plan for a wide-scale rollout.

Level 2: Launch

Wading into the world of

Level 2 companies place a slightly larger emphasis on data security, but overall practices remain decentralized.

Level 2 indicates a slightly more mature, but still growing, approach towards strong password security and management. Organizations at this stage are not using an enterprise-wide password manager, and password security practices are decentralized, with employees relying on a combination of browser-based password managers and other built-in password management tools. Some organizations might start with a free password manager before moving to a more centralized solution. Security best practices are a cursory focus during employee onboarding but are not a consistent focus for the organization. Technical maturity at this level is characterized by a mix of encryption practices - some information is encrypted, some isn't - and two-factor authentication is used sparingly for enhanced identity verification. Organizations seeking to progress from Level 2 to Level 3 should focus on increased awareness and education to establish fundamental credential security practices some of the time.

- **Password Manager Deployment**: Level 2 companies feature decentralized password management or ad hoc use of built-in password managers, such as Apple keychain or those built into browsers.
- **Security Culture**: Level 2 companies place limited emphasis on password security best practices.
- **Technical Maturity**: Level 2 companies contain inconsistent approaches to sharing encrypted information and using multifactor authentication (2FA).

Level 2 companies place a slightly larger emphasis on data security, but overall practices remain decentralized. The immediate next step to improve security is to select a centralized,

cross-platform password manager that works across all employee devices and begin a phased rollout.

Level 3: Evolve

Exploration of other password managers and the start of protecting sensitive data

Moving from Level 2 to Level 3 represents a significant step toward securing your business. Limited teams within the organization rely on a stand-alone password manager, but overall deployment remains minimal. Security training is more frequent and consistent, and employees experience more frequent alerts when engaging in obvious and potentially risky security practices. From a technical maturity standpoint, employees who collectively utilize a password management solution have coverage across all company-issued devices and are able to share passwords and other sensitive information securely. Using an encrypted password vault can significantly enhance security by securely storing sensitive information. The ability to securely share data between colleagues marks a departure from Level 2.

Level 3 companies are moving in a more centralized, albeit spotty, direction toward prioritizing data security.

- **Password Manager Deployment**: Level 3 companies have some measure of centralized password management, with one or two teams utilizing stand-alone password managers in favor of built-in tools.
- **Security Culture**: Level 3 companies place an increased emphasis on security culture but don't have tools or systems in place for concrete accountability.
- **Technical Maturity**: Level 3 teams using a centralized password manager benefit from cross-platform coverage across devices and secure sharing between employees.

Level 3 companies are moving in a more centralized, albeit spotty, direction toward prioritizing data security. The next step to improve security is to broaden password management coverage from a phased rollout into a company-wide rollout.

Level 4: Proactive

Getting serious about all your passwords and ensuring employees use an encrypted vault

Level 4 companies have taken a much more uniform, concrete approach to data

security, with a focus on ensuring universal coverage.

Level 4 is marked by the universal adoption of an enterprise-wide password manager, with a deployment initiated across the organization. It is crucial to create a strong master password to secure the password manager. All employees are urged to use the company password manager to create, store, and share passwords with other team members. Additionally, security training is normalized and accepted by the entire organization, with management tracking and incentivizing participation through detailed training modules. Level 4 technical maturity indicates enterprise-wide password management with directory services integration and single sign-on. Integration with directory services (which may include Active Directory/Entra, Google Workspace, or OneLogin) syncs users and groups from an external directory to the password manager. Integration with single sign-on enables organizations to leverage their existing identity provider to authenticate users with their enterprise password manager.

- **Password Manager Deployment**: Level 4 companies have deployed a stand-alone password manager across the organization, with teams heavily encouraged to completely eschew built-in tools and ad-hoc practices.
- **Security Culture**: Level 4 companies offer regular security training and incentivize attendance with participation metrics.
- **Technical Maturity**: Level 4 companies have integrated password managers with IT workflows, including directory services and single sign-on (SSO).

Level 4 companies have taken a much more uniform, concrete approach to data security, with a focus on ensuring universal coverage. The next step to improve security is to mandate enterprise-wide password management across the organization. Once that is in progress, enable passwordless authentication and require multifactor authentication (2FA) for all teams.

Level 5: Leader

A password-managing powerhouse using a strong master password, unique passwords, and

At this stage, an organization has undergone full-scale adoption of an enterprise-wide password manager

passwordless authentication

integrated into organizational workflows.

	Password Manager Deployment	Security Culture	Technical Maturity
LEVEL 5 Leader	**Complete organizational adoption** Company-wide stand-alone password manager rollout complete Adoption enablement with mandatory use Offer family plans as employee benefit	**Employees leading security improvements** Security training programs required for the entire company Clear channels where employees are encouraged to report suspicious activity	**Comprehensive coverage and reporting** Enables passwordless options from biometrics to passkeys Using APIs with automated scripting for integration with other tools, such as SIEM Mandatory 2FA

At this stage, an organization has undergone full-scale adoption of an enterprise-wide password manager integrated into organizational workflows. This password vault is used for securely storing and managing sensitive information, including passwords, credit card details, and personal data. Company-wide password management adoption is mandated, with restrictions on alternative password storage methods. Enterprises at this stage offer employees password management family plans to cultivate a 360° security culture, emphasizing personal and professional password management habits. Security training is required for the entire organization, and employees are encouraged to report suspicious cybersecurity activities. Technical maturity is characterized by comprehensive coverage and reporting. The enterprise-wide password manager enables passwordless options from biometrics to passkeys, while developers use APIs for integration with other tools, such as SIEM, in order to ensure an effective security stack. Automated scripting with APIs is utilized to enhance administrative control and simplify complex workflows.

- **Password Manager Deployment**: Level 5 companies require all employees to use a stand-alone password manager.
- **Security Culture**: Level 5 companies have instituted mandatory security training, with employees taking the initiative to flag suspicious activity to the IT department.
- **Technical Maturity**: Level 5 companies have embraced an enterprise-wide password manager that offers passwordless authentication, requires multifactor authentication (2FA), and encourages developers to utilize APIs for integration with other tools.

Level 5 companies have a comprehensive, sophisticated, enterprise-wide password management system in place. Companies interested in progressing beyond this point should explore secrets management tools that secure infrastructure and machine secrets.

Password Management Maturity Model

Success Factors	LEVEL 1 Open	LEVEL 2 Launch	LEVEL 3 Evolve	LEVEL 4 Proactive	LEVEL 5 Leader
Password Manager Deployment	**Password free-for-all** No password manager processes in place	**Decentralized password management** Ad hoc use of browser and other built-in password managers	**Limited password management** Stand-alone password manager rollout to one team	**Rising employee adoption** Company-wide stand-alone password manager rollout initiated	**Complete organizational adoption** Company-wide stand-alone password manager rollout complete Adoption enablement with mandatory use Offer family plans as employee benefit
Security Culture	**Minimal security awareness** No emphasis on security best practices	**Building on the basics** Limited emphasis on security best practices	**Security culture emerging** Some security training available with limited accountability	**Actionable employee awareness** Security training program offered to the entire company with participation metrics	**Employees leading security improvements** Security training programs required for the entire company Clear channels where employees are encouraged to report suspicious activity
Technical Maturity	**Land of do-it-yourself** Sensitive information often shared unencrypted	**Isolated solutions** Inconsistent approach to encrypted information Ad hoc use of 2FA	**Coverage underway** Cross-platform coverage across all devices Enables management of organizations and secure sharing between colleagues	**Connected into IT workflows** Directory Services integration Integrates with SSO	**Comprehensive coverage and reporting** Enables passwordless options from biometrics to passkeys Using APIs with automated scripting for integration with other tools, such as SIEM Mandatory 2FA

bitwarden