

LastPass...|

Finding a Password Management Solution for Your Enterprise

A guide to evaluating and comparing options.



Introduction

The challenge to secure every login grows. With the rise of a remote workforce and the rapid adoption of cloud applications, businesses need to ensure security while enabling their employees to work from anywhere.

But it's not just about security. Passwords are a source of frustration, decreased efficiency, and lost productivity for employees, too.

Although many organizations believe that securing logins with two-factor or multifactor authentication or deploying single sign-on (SSO) alone will protect an organization, a password management solution for every employee is an essential complement to lock down **all** access points.



45% of organizations have deployed an enterprise password management solution to address these challenges¹.

Password management provides a simplified workflow that employees crave without sacrificing security or control. It is a foundational tool to protect your company from data breaches.



Breach opportunities continue to widen as digital lives expand.

70%

Spent more time online².

50%

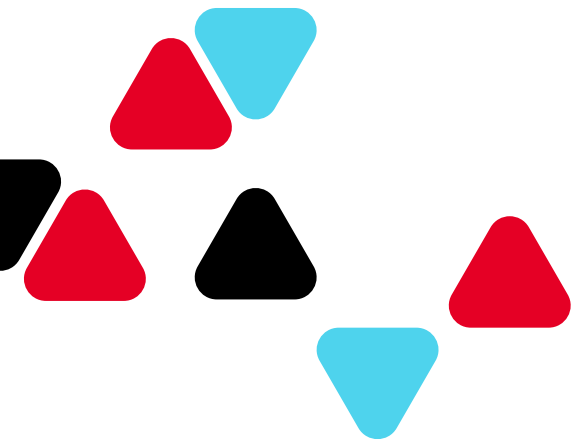
Created more accounts than last year².

¹ IDC InfoBrief, commissioned by LastPass, Enabling the Future of Work with EPM, Identity and Access Controls, #EUR148370521, February 23, 2022

² 2021 Psychology of Passwords

In this guide, we'll explore:

- What an enterprise password manager (EPM) is
- Why your business needs a solution
- How a password manager works with SSO or MFA
- A comprehensive set of criteria for evaluating enterprise password management solutions
- Best practices for implementing an enterprise password manager
- Common password-related challenges, and how an enterprise password manager solves them
- Organization-wide deployment of an enterprise password management solution



Password management: what it is and why it matters.

At its most basic, an enterprise password manager does what it says: It's a software tool that helps a user store, manage, and protect their passwords. Users only have to remember one (ideally very strong) master password that grants access to their password vault.



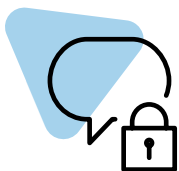
Passwords and other sensitive data stored in the password manager are usually encrypted, ensuring that only the user can access their logins.

Built-in password generators create randomized passwords for every online account. Additional features help users improve their online security and protect their personal information.



Reporting features give IT administrators both global and granular insight into password strength and login activity.

By gaining visibility into the everyday password habits of employees, businesses can ensure that every credential is as effective as possible, while ensuring employee collaboration by appropriately granting and managing permissions.



Securely managing, sharing, and using passwords significantly reduces the threat of hackers stealing or guessing passwords.

All too often, hackers leverage stolen credentials to remotely access a company's networks, servers, and on-premise or cloud applications to steal valuable data or defraud the business.



Why use an enterprise password manager?

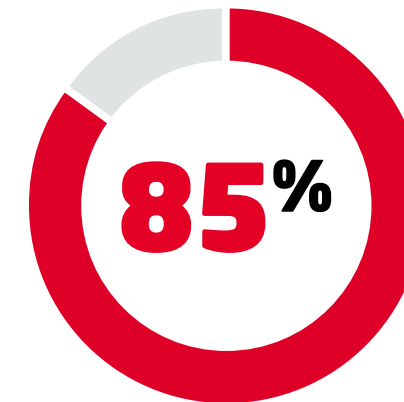
People have too many passwords to remember and manage in the workplace – and at home. As a result, creating memorable passwords or writing them down somewhere insecure is often the default.

.....

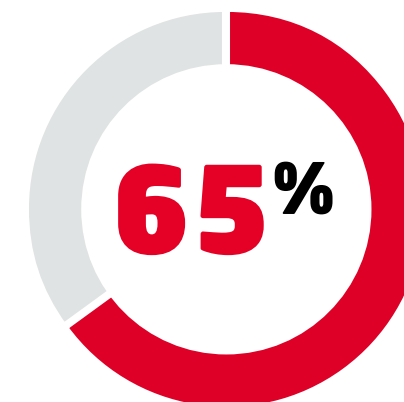
36% In fact, “too many passwords” is a key challenge for 36% of large organizations⁵.

.....

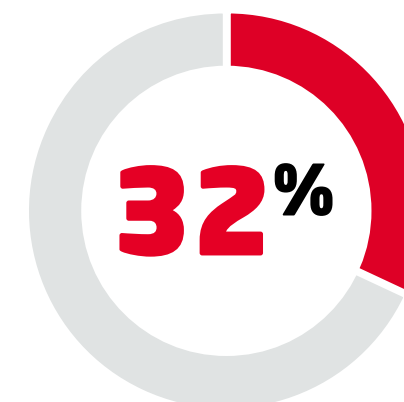
Key statistics:



Breaches involve a human element, like phishing, stolen credentials, and human error³.



Use the same password or a variation, so it's not a matter of if but when an employee credential is compromised⁴.



Create strong passwords for work accounts⁴.

³ Verizon DBIR, 2021

⁴ 2021 Psychology of Passwords

⁵ IDC InfoBrief, Enabling the Future of Work with EPM, Identity and Access Controls, 2022

An enterprise password management solution enables you to centrally manage all passwords, so you can:



Address the gap
left by the apps and
web services that can't
support SSO.



**Help IT enforce
security controls**
for employee-introduced
apps and web services.



**Facilitate secure
password sharing**
throughout the
organization.



Solve for co-management
of work and personal
credentials.

Every single login is a potential entryway for a hacker - and needs to be secured accordingly.

For employees, password management automates tedious password-related tasks, like creating, managing, filling, updating, assigning, sharing, and revoking passwords.

The IT department frees up time spent resetting passwords for more value-add projects.

The business overall can increase confidence in mitigating password-related attacks and preventing data breaches.

How does a password manager work with single sign-on (SSO)?

Rather than submitting a form-based login with a username and password specific to every app, SSO requires that an employee only authenticate once (to the SSO provider) and then uses a protocol like Security Assertion Markup Language (SAML) or Lightweight Directory Access Protocol (LDAP) to authenticate the user in the background with the same secure session.

While SSO protects logins for some traditional business applications, employees experience friction when it comes to secondary applications or those not covered by SSO, like social media accounts, demo accounts, IT credentials, services, and more. These inefficiencies force employees to create workarounds or revert to poor password practices.



75%

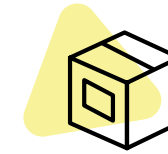
Say SSO is not universal for all the apps they use, so they also need password management⁶.



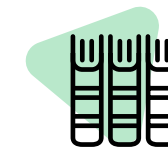
IT maintains a holistic view, including every single app, password, and user.

If an application or website is not compatible with SAML or LDAP, a password manager provides a method to securely store and share that credential. By layering password management with SSO, your IT team will have full control and visibility over which applications your employees access.

What to look for in an SSO solution:



Out-of-the-box setup for admins.



An extensive SSO catalog with a broad range of pre-integrated apps.



One portal where both SSO apps and standard credentials are stored.



One central IT dashboard to manage consistent policies across passwords, SSO apps, and MFA.

How does a password manager work with multi-factor authentication (MFA)?

MFA verifies a user's identity using two or more "factors" during the authentication process. These extra proof points stop would-be attackers from gaining access, even when they have stolen a valid password.

MFA should be layered on to key access points, like workstations and highly confidential logins, but adding MFA to every single log in will create extreme employee friction - imaging having to unlock every password through your authenticator app, text/email/call, every time - the friction alone will deter employees. Enter EPM, for every login, then layer MFA strategically.

**Together is always better:
EPM combined with SSO and MFA.**

91% Say EPM provides a usability convenience that employees appreciate for frequently visited external websites⁷.

77% Say the more layers of controls and safeguards they have, the better⁷.



Common challenges an enterprise password manager should solve.

Any password manager you select should solve these common password challenges:

- 1 Encrypt all passwords.** Passwords need to be kept somewhere safe and hidden from view, where security best practices protect them, and only authorized parties have access to them.
- 2 Take back employee passwords when they leave.** The moment an employee or external client leaves or changes roles, you need to prevent passwords from going with them. Auditing and user management functionality allows IT admins to change permissions and rotate passwords at any time.
- 3 Reduce password reuse.** IT admins need visibility into the overall password habits of the organization. Highlight employees with inadequate password hygiene and encourage or mandate employees take appropriate preventative actions.
- 4 Share access to accounts without sharing passwords.** Facilitate secure password sharing, where credentials are encrypted. Maintain accountability and oversight, whether sharing internally or working with external partners, agencies, or clients.
- 5 Keep everyone up to date with changes.** A changed password shouldn't disrupt the team's workday. Facilitate silent, secure updates whenever credentials need rotating.
- 6 Gain visibility into Shadow IT.** Capture all credentials in the organization and gain visibility into hidden apps used by employees. Truly measure the impact of Shadow IT on the organization, so you can embrace its potential while minimizing its risks.
- 7 Maintain accountability with passwords.** Leverage detailed event logs as an auditing tool to build compliance organization-wide. Even with shared items, tie specific actions to specific users to maintain accountability.
- 8 Alert users if a credential is at risk.** Dark web monitoring continuously keeps track of your email addresses within a database of breached credentials and immediately alerts you if they have been compromised.

Criteria for evaluating enterprise password management solutions.

So, you've decided your business could benefit from an enterprise password manager. Now what?

The right solution requires understanding your needs and what you expect a password manager to do for you. Then, you must find the product that best delivers on those needs and expectations.

Key areas when comparing solutions:

A frictionless employee experience.

How easy is it to use, and does it address the password challenges employees face? Can employees collaborate and share with both external and internal teams?

A focus on security.

Is the solution safe and reliable, and does it help you achieve your security goals?

A centralized admin experience.

What does it take to deploy, and how does it simplify management of ongoing tasks?

Custom, granular, and action-oriented controls.

Are admins given the right amount of oversight and visibility and can they easily solve gaps by taking action?

Integrations that meet your needs.

Simplify IT management and the end user experience through integrations with leading identity providers to connect with existing security practices like SSO and MFA, sync directories, and federate users.

A personal account to promote holistic protection.

With personal and professional lives merging like never before, can employees use a password manager to protect all aspects of their digital life?

Let's explore.



1 A frictionless employee experience.

Password management is only effective if employees use it. When evaluating solutions for the entire company, it doesn't matter how much the IT team loves the admin features and back-end functionality. If employees won't use it, the solution is not worth implementing.

What to look for:

- Little setup work required of the user
- Autofill of passwords in the browser
- Auto-capture of credentials (new and existing) as the user browses
- Secure, streamlined sharing with internal and external parties
- Automatic sync for access across devices
- Automatic updates to shared credentials
- Support for all web-based logins (not just a subset of cloud apps)
- Credentials and other sensitive data are encrypted and stored securely
- Security across personal and business accounts
- A robust support site for users to self-serve

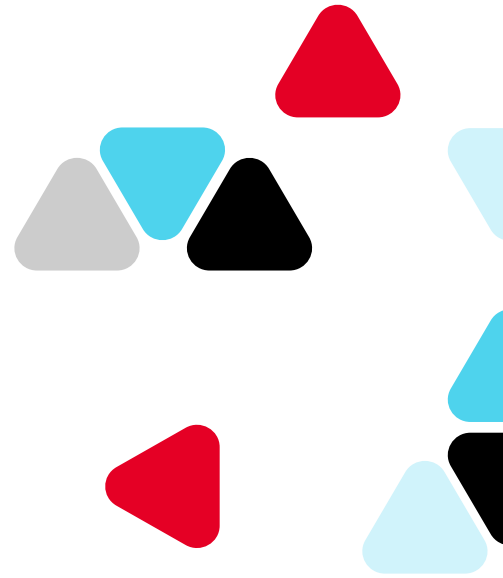
Questions to ask:

- How easy and intuitive is it to use?
- Can everyone use it, what are the accessibility requirements?
- Will employees adopt the product?
- Does it do tedious tasks on behalf of the user?
- Can employees share passwords, and is the password always visible?
- Who can employees share passwords with and how frequently? How is access granted/revoked?
- What steps are required of the user to share a credential and manage those shared items?
- Will it capture all the passwords and data employees use?

1 A frictionless employee experience. (cont.)

Action items:

- ☐ **Try it yourself.** Most password management solutions offer free trials that small groups of people can test. The best way to see how it works is to just jump in yourself. A proof of concept with a group of users will give you insight into how the product works and how intuitive it is when starting.
- ☐ **Inventory devices in use.** If you don't know what devices your staff is using and whether they're using personal or work devices, now is the time to do an inventory. Once you have a complete list, you can ensure that any password solution you adopt is compatible with those devices.
- ☐ **Find customer experiences.** The proof is in the numbers — of happy customers, that is. Dig into case studies, customer testimonials, app store ratings, and reviews from technology publications. All are a good indication that the product meets customer needs.



2 A focus on security.

When evaluating the security implications of adopting a password manager, there are two things to consider: 1) Whether the service itself is safe and reliable, and 2) whether the service helps you achieve your security goals. The goal of a password manager is to reduce the risk of a data breach and safeguard your business. You want to ensure that any solution you adopt adequately secures and gives you the right tools to enforce better policies in your organization.

What to look for:

- Local-only encryption (meaning the service provider never receives the master password and encryption key)
- Leading encryption algorithms
- Best practices for securing data in transit and at rest
- A large portfolio of policies and advanced controls at the admin level
- Accessibility of data in a range of scenarios, both online and off
- Compatible multi-factor authentication and SSO integrations
- Experience addressing vulnerabilities or security incidents, with a track record of responsiveness and transparency
- Dark web monitoring to monitor, alert, and protect accounts
- Compliance standards: SOC2, SOC3, C5, ISO27001, GDPR

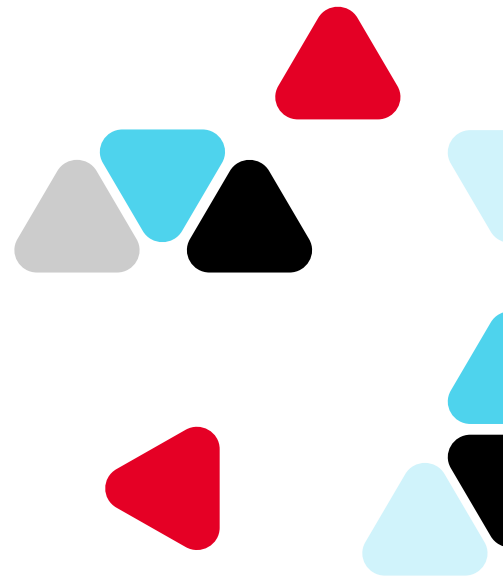
Questions to ask:

- Which encryption algorithms does the service use?
- How is data secured locally and server-side?
- In what circumstances, if any, are the master password or encryption key sent to the service provider?
- What policies and security settings are available?
- Can policies be applied on a global, group, and per-user basis?
- What compliance standards does the product meet?

2 A focus on security. (cont.)

Action items:

- ☐ **Review internal security policies.** The password manager you select should align with the guidelines you have in place. If compliance regulations require that you store data like passwords in an encrypted format or in a specific region, ensure that the product offers the encryption and storage standards you need.
- ☐ **Read the technical whitepaper.** Note how data is secured and how the encryption key is protected (ideally, the service provider never receives it). Ensure redundancy is built-in to protect against downtime.
- ☐ **Evaluate the complete list of policies and controls.** Some password managers only offer a dozen or so policies, while others provide over 100. It's not just about how many are available but also what you can accomplish. Look for a granular level of control, allowing you to set custom requirements around account access, password hygiene, feature usage, and more.



3 A centralized admin experience.

To scale password management for your organization, you need robust admin controls that automate key processes. Admins need a centralized, streamlined way to deploy the service and manage and maintain it going forward. Admins also need to be empowered to report back to key stakeholders on the program's impact and progress in strengthening password security across the business.

What to look for:

- Designated admins with special privileges for managing and securing the deployment
- Directory services that can sync and virtualize the identity information already in use
- Automated updates to the service that require little to no involvement of IT
- A solution that covers your entire organization, not just individuals or departments – every login should be secured
- Provisioning tools that facilitate the lifecycle of an employee's digital identity across creation, propagation, management, and termination
- A comprehensive view into your entire account with a Customer Success Manager to guide you along the way
- A fast time-to-deployment

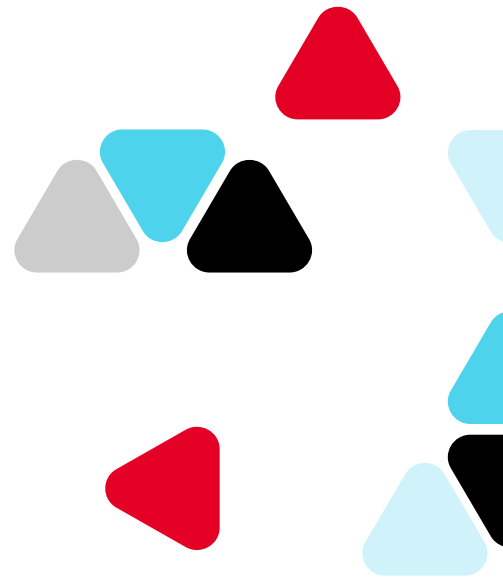
Questions to ask:

- What roles are available, and at a high level, what are the privileges given to admins?
- Are any advanced skills or knowledge required to deploy the solution? Is that knowledge available internally, or will it need to be found externally?
- How can Active Directory or other existing systems be leveraged to automate user management?
- Are there education resources admins can send to end users to help with adoption?
- Will there be a designated point of contact or customer success manager to help with deployment, what level of support is included?

3 A centralized admin experience. (cont.)

Action items:

- ☐ **Explore the admin dashboard.** As you trial solutions and create a proof of concept with a test group, thoroughly evaluate the admin dashboard. Keep an eye out for critical features like reporting that depicts actionable insights, user and group management, shared credential management, policies, security scores, and custom integrations.
- ☐ **Leverage Active Directory sync.** If your business already uses Active Directory to manage processes and services, be sure to compare options for integrating with a password manager. Some allow you to sync with your directory to automate user management, assign shared credentials, and apply policies.
- ☐ **Ask for Support.** While you want to select a solution that is easy to deploy, let's be honest- questions arise. You should feel comfortable seeking support and know of any community groups, support sites, or direct point of contacts so your questions or issues are resolved within a timely manner, giving you peace of mind.



4 Custom, granular and action-oriented controls.

When comparing solutions, consider the visibility and control available to admins. It's not enough to collect passwords in one place and give access to others – even a password-protected Excel file can do that, albeit clumsily. The true power of a password manager is how it captures and reports on password security and facilitates actions to address any deficiencies both across the organization and at the individual level.

What to look for:

- At-a-glance insights into users, their stored sites, and their password behavior
- Actionable reports detailing how users are performing and where to make improvements
- Security reports to show a clear impact on reducing password reuse
- Policies and settings applied globally, per group, and per user
- Credential sharing that tracks actions to individuals
- Organization-wide measurements on password security
- Detailed reporting logs for auditing and compliance
- A kill switch to revoke passwords when employees leave
- Secure account recovery when a user leaves or forgets their master password
- Visibility into Shadow IT

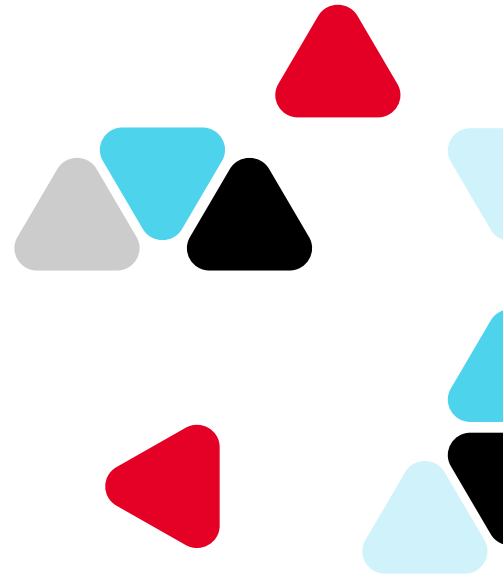
Questions to ask:

- Can access be restricted on a user, group, or global level?
- How is password reuse and other markers of security measured across the organization?
- What roles are available, and what are their privileges?
- Is there an audit trail, and what details do the reports capture?
- How is password hygiene measured at the global and individual level?
- How are user accounts terminated or reclaimed when someone leaves?
- How can an account be recovered in the case of a forgotten master password?
- Can reporting tools highlight Shadow IT within the organization?

4 Custom, granular and action-oriented controls. (cont.)

Action items:

- ☐ **Review reporting logs.** Once you've started a trial and have tested the product yourself, review any reporting logs available to admins. Which actions and events do the reports record for both users and admins? Note the granularity of the logs and how long they are available.
- ☐ **Ask questions about a range of scenarios.** Ask the provider about user-level insights into password behaviors and access patterns. An advanced password management solution should give you visibility into failed login attempts and actions taken by users and admins. You also want to see actionable overviews of your security profile that will help you proactively protect against threats.



5 A personal account to promote holistic protection.

With professional and personal lives merging at an unprecedented rate, it is crucial that your employees' value secure data storage across all accounts – especially if they're accessing your business data, like corporate email or communication apps, from their personal devices. Their personal password behavior can impact professional password behavior.

What to look for:

- A password manager that has a consumer product available for employees – even better, a consumer product that expands to their family as an added benefit
- A personal password manager that has similar business features, such as:
 - The ability to generate, store, and manage credentials
 - Sharing capabilities, like unlimited shared folders
 - Password generator to create strong, unique passwords
 - Security dashboard that indicates overall strength of passwords
 - Dark web monitoring that notifies users of compromised accounts

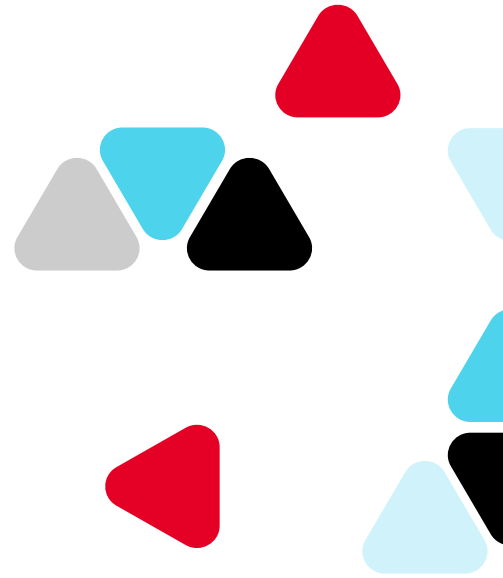
Questions to ask:

- Does the password manager have both business and consumer products?
- Is the consumer password manager as robust as the business offering?
- Can employees utilize this just for themselves, or extend to their families as well?
- Does the password manager allow for use across unlimited devices?
- Is there an additional cost for adding personal accounts to business accounts?
- Do employees have to link their personal accounts to access one or the other?

5 A personal account to promote holistic protection. (cont.)

Action items:

- ☐ **Evaluate your policies.** If you have a bring your own device (BYOD) or bring your own application (BYOA) policy at your organization, it is important that employees are implementing proper password hygiene across personal devices and applications.
- ☐ **Ensure a seamless process for employees.** Ask the provider if adding a personal password manager requires extensive setup. Extending the same value of a password manager should enhance your employee's experience and be seen as an added benefit, not add complexity.



A checklist for ensuring a successful implementation.

Once you've chosen an enterprise password management solution, you will want to ensure that it is widely adopted and used to its full potential by both employees and IT admins. Using the previous evaluation criteria to select the best password manager for your business, you will lay the groundwork for a successful implementation.

However, several steps are vital to getting the password manager into the hands of your staff and making sure it becomes a key asset in their toolbox.



1 Define the project and goals.

Tackling password management is a tremendous opportunity for improving security and giving employees a boost in daily productivity. Before you dive in, you need to develop a solid deployment strategy.

Action items:

- ☐ Set clear objectives for implementing a password manager.
- ☐ Understand where a password manager fits in your larger security strategy.
- ☐ Assign ownership of the project, including evaluating, comparing, selecting, and implementing a password solution.
- ☐ Inventory the technology in use. Are you in a BYOD work environment? What cloud apps have you adopted company-wide? What other identity and access management (IAM) technologies are you using in the workplace? How do you want them to integrate, if at all, with your password manager?
- ☐ Confirm management buy-in and align leadership with the security goals the organization is working to achieve. Communicate how a password manager will help accomplish those goals.
- ☐ Confirm how you will show successful adoption and ROI for the implementation. Some providers even have an ROI calculator you can use in advance of purchase.

2 Review and turn on appropriate policies and security controls.

Default options are in place to provide standard levels of security, but your business may have unique requirements. Whether it's restricting when and where employees can access their password vault, disabling certain features, or requiring the use of specific security settings, it's essential to familiarize yourself with available security options. Review and enable permissions and restrictions before employees start using the service.

Action items:

- ☐ Define your security level and what you need to protect.
- ☐ Review all available security policies and settings in the password manager.
- ☐ Decide which controls should apply globally to the whole business.
- ☐ Decide which rules should apply granularly to specific groups or individuals.
- ☐ Enable the policies and settings that are appropriate for your security model.
- ☐ Use additional security measures like multi-factor authentication.

3 Get the password manager in the hands of users.

The actual value lies in user adoption. To achieve a successful deployment, use available features to streamline the onboarding process and plan for users who fail to sign up or start using the product.

Action items:

- ☐ Evaluate options for onboarding employees and choose the one that best suits your environment.
- ☐ Sync with existing directories to automate onboarding.
- ☐ Prepare employees by sending pre-invites and raising awareness around their new password manager.
- ☐ Invite all employees to join and complete the setup of their accounts.
- ☐ Point employees to self-serve educational tutorials on how to use the product until formal training is established.
- ☐ Communicate policies and best practices to all employees, particularly around password reuse, password strength, password sharing, and password expiration.
- ☐ Schedule follow-up reminders for those who fail to sign up or with subpar product usage.

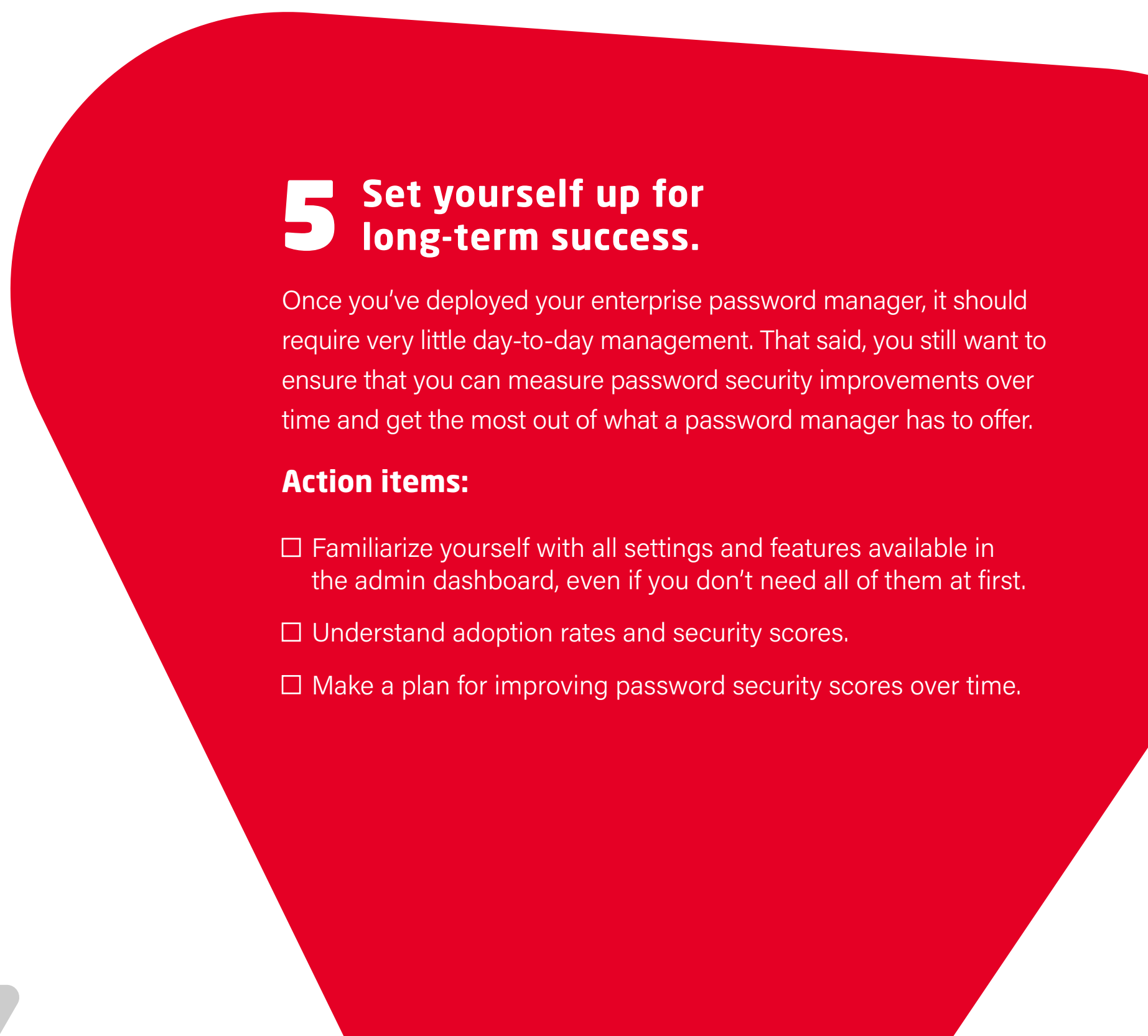


4 Organize thorough product training for both admins and employees.

Whether you offer training sessions or open office hours for employees, providing some training for both admins and users will help raise awareness and drive interest in the password manager.

Action items:

- ☐ Schedule employee training to cover core password management features.
- ☐ Create internal onboarding “toolkits” such as handouts, presentations, or webinars – be sure to use any of the resources that come with your product.
- ☐ Facilitate Q&A sessions with staff, either during training or in separate office hours.
- ☐ Add training for password management to new employee onboarding processes, so anyone new to the team is automatically trained to use the service.
- ☐ Have clear guidelines for submitting questions and seeking support with problems.



5 Set yourself up for long-term success.

Once you’ve deployed your enterprise password manager, it should require very little day-to-day management. That said, you still want to ensure that you can measure password security improvements over time and get the most out of what a password manager has to offer.

Action items:

- ☐ Familiarize yourself with all settings and features available in the admin dashboard, even if you don’t need all of them at first.
 - ☐ Understand adoption rates and security scores.
 - ☐ Make a plan for improving password security scores over time.
- 

Checking the boxes with LastPass Business for Enterprises.

LastPass Business reduces friction for employees while increasing control and visibility with a password management solution that is easy to manage and effortless to use. LastPass Business empowers employees to generate, secure, and share credentials seamlessly while ensuring protection through LastPass's zero-knowledge security infrastructure.

Features include:

- Central admin console
- Adoption Dashboard
- Universal password management
- User directory and federation integrations
- 100+ security policies
- Detailed security reports
- Secure internal and external password sharing
- Dark web monitoring
- Basic single sign-on
- Basic multi-factor authentication
- Integrations with all major IDPs
- A free Families account for employees

Additional add-ons:

- LastPass Advanced Single Sign-On
- LastPass Advanced Multi-Factor Authentication



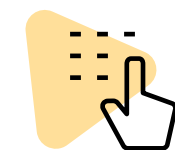
Don't have a Single Sign-On or Multi-factor Authentication solution yet?



LastPass Advanced Single Sign-On

LastPass Advanced Single Sign-On (SSO) simplifies employee access to an unlimited number of cloud applications, while streamlining provisioning cloud applications for IT– all in the same application they trust to store their passwords.

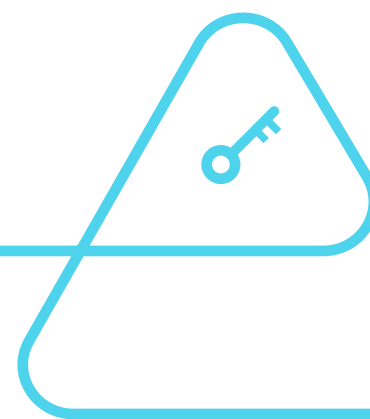
With SSO for top priority apps and password management to capture and secure everything else, LastPass protects every access point and conveniently connects employees to their work.



LastPass Advanced Multi-Factor Authentication

LastPass Advanced Multi-Factor Authentication secures every access point to your business. From cloud and legacy apps to VPN and workstations, LastPass Advanced MFA adds a layer of security on top of your endpoints to maximize protection.

By adding LastPass Advanced MFA, your business can secure all web logins while adding endpoint verification – all with one easy-to-use mobile app.



Organization-wide deployment of an enterprise password management solution.

Password management must be a priority throughout your entire cybersecurity strategy, not just implemented in pockets of your organization. Every credential is a key to the doors of your business. Eliminate poor password behavior and reduce risk by providing every employee with a password manager professionally.

An organization-wide deployment of LastPass offers a LastPass account for every employee in your organization at a flat fee versus a seat-based rate. This option offers you the flexibility to scale LastPass as your company grows, without any additional costs. You'll be able to secure your entire organization while saving up to 25% on each license.

In addition to flexibility and functionality, LastPass customers can receive a Customer Success Manager (CSM) who will be available as you roll out LastPass.

High adoption, fast results.

Employees are onboarded quickly, without the need for extra technology services, overhead, and time – meaning deployment is simple, which leads to better adoption.

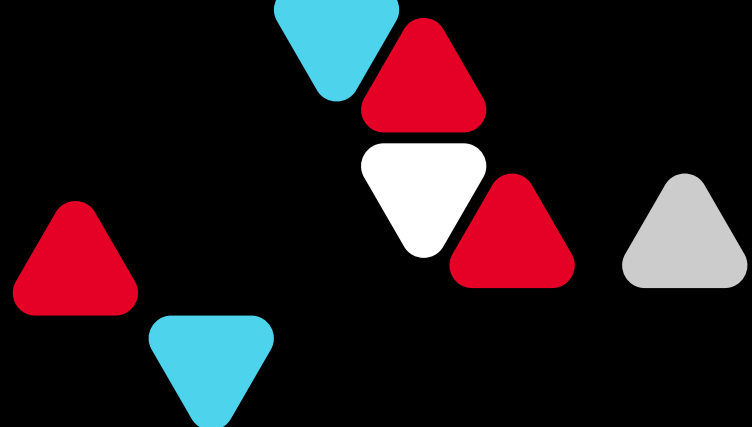
Ease of use.

Employees can seamlessly generate, autofill, save and safely share (internally and externally) passwords from their vault. Access can be granted and revoked in real-time to ensure company data stays within company walls.

Comprehensive security.

An organization-wide deployment of LastPass is critical. Employees are also provided with a free, personal LastPass Families account to ensure holistic protection, wherever they are, both on and off the clock.

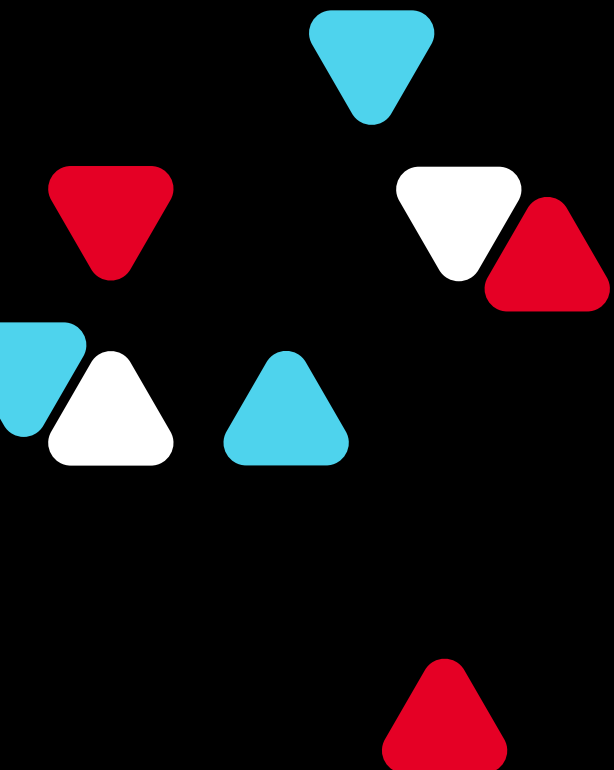


A cluster of several triangles in red, cyan, white, and grey colors, arranged in a loose, abstract pattern in the top right corner of the slide.

LastPass...|

Trusted the most by the most.
With over 1B sites secured, 30M users, and
85,000 Business customers, LastPass makes
online security simple and approaching by
eliminating barriers presented by passwords.

LastPass. The best password management
solution for businesses.

A cluster of several triangles in red, cyan, and white colors, arranged in a loose, abstract pattern in the bottom left corner of the slide.