Finding a Password Manager for Your Business

A guide to evaluating and comparing solutions.

LastPass

Security starts with the basics.

Solving the password security disconnect between IT and employees demands the right solution. From external threats to managing Shadow IT, protecting your company, employees, and customers is a complex job. Staying on top of all possible threats can be overwhelming. What you need is a solution that gives you the right security, in a way that is effortless for employees.

81% of confirmed data breaches involved weak, default, or stolen credentials.

— Verizon 2017 Data Breach Investigations Report (DBIR)

The average data breach now costs $4 million US.[1]

37% of people forget a password at least once a week.[2]

55% reuse passwords despite understanding the risks.[3]

60% of hacked SMBs are out of business 6 months later.[4]

61% of people use the same or similar password for all accounts.[5]

[1] IBM's 2016 Ponemon Cost of Data Breach Study

[2] Intel Security Poll 2016: buzzfeed.com/josephbernstein/survey-says-people-have-way-too-many-passwords-to-remember?utm_term=.dud82LVQa#.ee4Bv0pXE

[3] LastPass Psychology of the Password Report 2016: prod.cdata.app.sprinklr.com/DAM/434/LastPass_ExecutiveSummary_fina-88e8a5a2-00cb-4a09-b363-e01a45f829d6-1389898992.pdf

[4] US National Cyber Security Alliance

[5] LastPass Pscyhology of the Password Report 2016: prod.cdata.app.sprinklr.com/DAM/434/LastPass_ExecutiveSummary_fina-88e8a5a2-00cb-4a09-b363-e01a45f829d6-1389898992.pdf

Password management: What it is and why it matters

A definition of password management

A password manager is a software solution that helps a user store, manage, and protect their passwords. Users only have to remember one master password that grants access to their password store.

Consumer vs. business solutions

Consumer password management focuses on the needs of an individual by safeguarding and auto-filling passwords for personal accounts, sharing passwords with friends and family, and generating strong passwords.

Business password managers typically offer the same end user experience, but the best solutions add comprehensive admin features that provide organization-wide oversight, user management, and security controls.

But it's not just about security. For both the consumer and business professional, passwords are a source of frustration, decreased efficiency, and loss of productivity. Password management provides a simplified experience without sacrificing security or control.

In this guide, we'll focus on password management in the workplace and explore:

- Password manager types and solutions
- A comprehensive set of criteria for evaluating solutions
- Comparing password managers to other identity and access management (IAM) solutions
- Best practices for implementing a password manager

We'd love to hear more about your business needs, so please reach out to us when you're ready to take a closer look: **lastpass.com/contact-sales**

Why a password manager?

Despite all the talk of the "death of the password," we don't yet live in a post-password world. We have too many passwords to remember and manage. As a result, the security of your business suffers from:

- Inaccurate password tracking
- Haphazard password solutions
- Weak, reused passwords
- Lack of oversight for shared passwords
- Lockouts and productivity loss

Protecting the data of employees, customers, and partners requires that passwords are handled appropriately.

Achieving best practices means:

- Randomizing every password for every account.
- Rotating passwords when appropriate.
- Applying role-based permissions to passwords.
- Proper oversight and accountability for shared credentials.
- Only sharing passwords in an encrypted format.
- Adding protection with multifactor authentication wherever possible.
- Decommissioning employee credentials after they leave or change roles.

Password management is the simplest, most effective way to make strong password security the default across the entire organization.

Your password manager should:

1.Encrypt all passwords.
Store passwords somewhere safe, and restrict access to authorized parties.

2. Rescind employee access when they leave.
Equip IT to audit user access, change permissions, and rotate passwords instantly.

3. Reduce password reuse.
Gain visibility into poor password hygiene, and measure improvements.

4. Share access to accounts, without sharing passwords.
Maintain accountability and oversight of shared accounts, internally and externally.

5. Keep everyone up-to-date with changes.
Facilitate silent, secure updates to passwords, without disrupting anyone.

6. Gain visibility into Shadow IT.
Capture all credentials in use, and reduce the risks of Shadow IT.

7. Maintain accountability with passwords.
Leverage detailed event logs to build compliance organization-wide.

To cloud or not to cloud

Password managers come in two flavors: cloud-based and on-premise. Cloud-based solutions offer several advantages and have gained in popularity over the last 10 years as more businesses adopt cloud-based solutions to address a wide range of needs.

Look For:

- A private encryption key, so only the user can unlock the vault.
- A reliable service utilizing world-class data centers with full redundancy and an "offline mode."
- BYOD-friendly, automated sync so employees can safely work anywhere.
- Automatic, behind-the-scenes updates with the latest improvements and bug fixes to reduce IT burden.
- Secure password sharing for internal staff as well as contractors, partners, agencies, and others.

Completing the IAM stack

If your business has already invested in single sign-on (SSO) or privileged access management (PAM) solutions, you may be wondering what value a password manager adds.

Each solution addresses a unique set of needs:

- SSO manages users' identities beyond your directory of choice for a core set of enterprise-ready apps. However, this does not cover all services in use in the workplace.
- PAM is an IT-centric solution that leverages Active Directory to restrict access to privileged accounts and facilitate secure password rotation, as well as manage non-web tools like servers and routers.
- Password management complements these other solutions by providing oversight of all web-based accounts across the business. This gives IT visibility into the apps and sites people are using as well as the strength of passwords in use.

Together, these solutions address all areas of identity and access management, at all levels of the organization, ensuring a more efficient workforce and greater protection against data breach.

Criteria for evaluating solutions

So you've decided your business could benefit from a password manager. Now what? Finding the right solution means understanding your needs as well as what you expect a password manager to do for you, and then finding the product that best delivers on those needs and expectations.

Key areas when comparing solutions:

- **Business-grade controls:** Are admins given the right amount of oversight and visibility?
- **An effortless experience:** How easy is it to use, and does it address the password challenges employees are facing?
- **An appropriate cost of ownership:** What budget does the solution require upfront, and what are the costs (monetary or otherwise) in the longer-term?
- **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 the solution, and how does it simplify management of ongoing tasks?

Business-grade controls

It's not enough to collect passwords in one place and give access to others. The true power lies in capturing data about password security and facilitating appropriate action.

✓ Look for:

- At-a-glance insights into users, their stored sites, and their password behavior
- Credential sharing that tracks actions to individuals
- Organization-wide measurements on password security
- Detailed reporting logs for auditing and compliance
- Revoking passwords or secure account recovery when employees leave

? Questions to ask:

- Is there an audit trail, and what details do the reports capture?
- How is password hygiene measured, at the global and individual level?
- How do you terminate or reclaim a user's account when they leave?
- What can reporting tools tell us about Shadow IT within the organization?

! Action items:

- **Review reporting logs.** Take note of what actions and events are recorded for both users and admins, how granular the logs are, and how long they are available.
- **Ask questions about a range of scenarios.** You want to see actionable overviews of your security profile that will help you proactively protect against threats.

An effortless experience

Password management is only effective if employees actually use it. No matter how much IT loves the solution, it's not worth implementing if employees won't use it.

Look for:

- Little set up work required of the user
- Auto-capture and auto-fill of passwords
- Simple, up-to-date password sharing
- Automatic sync for access across devices
- Support for all web-based logins

Questions to ask:

- How easy is it to get started and use?
- Does it automate tedious tasks for the user?
- How does password sharing work?
- Are passwords auto-captured for the user?

Action items:

- **Try it 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 just starting out.
- **Inventory devices in use.** Ensure that any solution you adopt is compatible with those devices and use cases.
- **Find customer experiences.** Case studies, customer testimonials, app store ratings, and reviews from technology publications are all good indications of adoption and satisfaction.

An appropriate cost of ownership

Cost is important, but like any other software purchasing decision, it shouldn't be the sole driving factor. Find a solution that is within your budget but that provides the critical functionality required to successfully address password challenges.

✓ Look for:

- Budget-friendly, without sacrificing functionality or security
- Minimal to no add-on costs for core functionality
- Resources that admins can leverage for internal training
- Little to no professional services required for installation and deployment

? Questions to ask:

- What is the per-user cost?
- Are there add-on costs for additional functionality or services?
- Can licenses be purchased and/or renewed online or is it managed by a sales representative?
- What is the cost in time and resources, of deploying and maintaining the solution?

! Action items:

- **Confirm your budget.** Understand the total allocated budget and whether your first choice solution fits within it.
- **Determine the resources you require.** If your business requires extensive support or training needs, understand what options are available and the added cost.
- **Walk through implementation scenarios.** Ask about how routine tasks are performed – like adding or removing users, sharing credentials, adjusting policies, and rotating passwords.

A focus on security

When adopting a password manager, there are two things to consider:

1) Whether the service itself is safe and reliable.

2) Whether the service helps achieve your security goals, and enforce better policies.

✓ Look for:

- Local-only encryption that keeps the master password private
- Best practices for securing data in transit and at rest
- Advanced policies and controls
- Multifactor authentication
- A track record of responsiveness and transparency

? Questions to ask:

- How is data secured locally, and server-side?
- What policies and security settings are available?
- What options are available on a global, group, and per-user basis?
- What multifactor authentication options are available?

! Action items:

- **Review internal security policies.** Ensure the password manager aligns with and reinforces the policies you have in place and compliance you need to meet.
- **Read the technical whitepaper.** Take note of how data is secured, and how the encryption key is protected (ideally, it's never shared with the service provider).
- **Evaluate the full list of policies and controls.** Look for a granular level of control, allowing custom requirements around account access, password hygiene, and feature usage.

A centralized admin experience

To scale password management, admins need a centralized way to deploy, manage, and maintain the service as well as report on password security across the business.

✓ Look for:

- Admin privileges for managing and securing the deployment
- Directory services that can sync identity information already in use
- A self-service solution
- Provisioning tools that facilitate the lifecycle of an employee's digital identity
- Single Sign-On capabilities to launch federated cloud applications

? Questions to ask:

- What roles and privileges are offered?
- What skills or knowledge are required for deployment?
- Can Active Directory or other systems automate user management?
- Are Single Sign-On capabilities supported?

! Action items:

- **Explore the admin dashboard.** Look for key features like reporting, user and group management, shared credential management, policies, and security scores.
- **Leverage Active Directory sync.** Automate user management, assign shared credentials, and apply policies.

Ensuring successful implementation

Define the project and goals

By using the previous evaluation criteria to select the best password manager for your business, you have laid the groundwork for a successful implementation. However, several steps are key to getting it into the hands of your employees and ensuring it becomes a key asset:

- Set clear objectives for implementing a password manager.
- Understand where it fits in the larger security strategy.
- Assign ownership of the project, including evaluating, comparing, selecting, and implementing a password solution.
- Inventory the technology in use. Are you a BYOD work environment? What apps have you adopted company-wide? What other identity and access management (IAM) solutions are used? How do you want them to integrate with your password manager?
- Ensure alignment on security goals and how a password manager will help.
- Confirm how you will show successful adoption and ROI for the implementation.

Review and turn on policies and security controls

Default options provide standard security, but your business may have unique requirements. Whether it's restricting employees access, disabling features, or requiring security settings, it's important to familiarize yourself with available options. Ensure appropriate permissions and restrictions are in place before employees use the service.

- Define your security level. Is your business locked down or lax?
- Review all available security policies and settings in the password manager.
- Decide which controls should apply globally, to groups, or individually.
- Enable the policies and settings that are appropriate for your security model.
- Use additional means of authentication like multifactor authentication.

Get the password manager in the hands of users

The true value lies in user adoption. To achieve a successful deployment, streamline the onboarding process and plan for users who fail to sign up.

- Evaluate onboarding options and choose the one that best suits your environment.
- Sync with existing directories to automate onboarding.
- Prepare employees by raising awareness around their new password manager.
- 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.

Organize training for admins and employees

Whether you offer brown bag training sessions over lunch or open office hours, training for both admins and users will drive interest in the password manager.

- Schedule employee training to cover core password management features.
- Leverage internal onboarding "toolkits" such as handouts, presentations or webinars.
- 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 is automatically trained to use the service.

Set yourself up for long-term success

Once you've deployed your 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.

- Familiarize yourself with all settings and features 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 solutions.

LastPass offers effortless security. LastPass combines an experience users love with powerful admin features that help businesses strengthen their password security and provide a frictionless login experience.

Whether your team just needs to share passwords, or you’re worried about a data breach, LastPass scales to fit the needs of your business. With so many employees struggling with password fatigue, your business needs a smart solution that users will readily adopt.

LastPass provides:

- An experience users and admins love.
- Automation of key password processes, like saving, filling, creating, sharing, updating, and reporting.
- A strong, proven security model.
- Centralized, flexible admin controls with the right amount of visibility.
- Affordable packages, built for businesses of all types.

Learn more: lastpass.com/business