Finding A Password Management Solution For Your Business

A guide to evaluating and comparing options.

We know that solving the security disconnect between IT and employees demands the right solution. When 85% of breaches involve a human element (phishing, stolen credential, human error), employee password practices remain the weakest point in a company's security and put sensitive data at risk.[1]

With the rise of a remote workforce, 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.

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

In this guide, we will explore:

- What a password manager is
- Why your business needs a solution
- A comprehensive set of criteria for evaluating solutions
- Best practices for implementing a password manager
- Common password-related challenges and how a password manager solves them
- Complementing a password manager with single sign-on (SSO) and multi-factor authentication (MFA)

1 2021 Verizon DBIR

Password Management: What It Is and Why It Matters

At its most basic, a 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 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 A Password Manager?

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

Key statistics:

- **66% of people use the same password everywhere, so it's not a matter of if but when an employee credential is compromised.**[2]
- **More than half of the data compromised in breaches in small (52%) and large (64%) businesses was credentials.**[3]
- **With 15 billion stolen logins circulating on the dark web, IT must ensure employees' credentials remain secure.**[4]
- **85% of breaches involve a human element, which encompasses any attack that involves a social action such as phishing, stolen credentials or human error.**[5]

Password management automates tedious password-related tasks, like creating, managing, filling, updating, assigning, sharing, and revoking passwords. Remembering and creating countless passwords is no longer a burden for employees. 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.

2 Psychology of Passwords, 2020
3 2020 Verizon DBIR
4 Digital Shadows, "From Exposure to Takeover," 2020
5 2021 Verizon DBIR

Common Challenges a Password Manager Should Solve

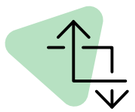
Any password manager you select should solve these common password challenges.

Challenge 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.

Challenge 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.

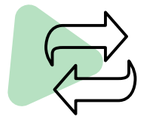


Challenge 3: Reduce password reuse.

IT admins need visibility into the overall password habits of the organization. Highlight employees with inadequate password hygiene and encourage or mandate employees to take appropriate preventative actions.

Challenge 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.



Challenge 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.

Challenge 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.

Challenge 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.

Challenge 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 Password Management Solutions

So, you've decided your business could benefit from a 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.

Explore these key areas when comparing solutions:

- **A frictionless employee experience:** How easy is it to use, and does it address the password challenges employees face?
- **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 for gaps by taking action?
- **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?

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
- 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?
- 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?
- 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?

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 are 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.

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
- Multi-factor authentication integration for additional account security
- Experience addressing vulnerabilities or security incidents, with a track record of responsiveness and transparency
- Dark web monitoring to monitor, alert, and protect accounts

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 multi-factor authentication options are available, and is there an added cost?

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.

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:

- Designate admins with special privileges for managing and securing the deployment
- Directory services that can sync and virtualize the identity information already in use
- Particularly for small to medium businesses, a self-service solution that doesn't require extensive time or internal resources
- Automated updates to the service that require little to no involvement of IT
- Ability to add licenses throughout the year as the team grows and advances your strategy by adding enhanced security solutions
- 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
- 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?
- How many admins are supported, and what privileges do they have?

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.

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?

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.

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, 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 in order to access one or the other?

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 a 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.

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 bring your own device (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.

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.

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.
- 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 Thorough Product Training For Both Admins And Employees

Whether you offer training sessions or open office hours for employees, providing 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.
- 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.

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 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.

How Does A Password Manager Fit With Other Security Solutions?

A business password manager offers a strong foundation for securing your business. There's no doubt that more robust password security significantly reduces cyber risks while eliminating genuine frustrations for employees.

That said, complementary technologies like multi-factor authentication (MFA) can add even more security to access points. Plus, security solutions like single sign-on (SSO) can also move your company in the direction of a passwordless authentication experience.

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.

Today's best MFA solutions leverage what users always have – their smartphones – along with contextual and biometric data to deliver superior security. The user can prove they are who they say they are with biometric factors like fingerprint or face ID, while the device can establish the user's identity with behind-the-scenes data like phone location or IP address. This adaptive MFA can ensure the correct users access the appropriate data at the right time by adapting requirements to the risk of any given login event. But most importantly, adaptive MFA adds critical layers of security while offering a seamless authentication experience for employees.

WHAT TO LOOK FOR:

- **Option to use personal smartphones for end-user convenience**
- **Use of "hidden factors" like geolocation, device ID, and IP address**
- **Support for "human factors" like fingerprint scans and face ID**
- **Security by design that encrypts biometric data at the device level**
- **Combination of methods in use, such as push notification, biometrics, and adaptive authentication**
- **Support for cloud and legacy apps, VPNs, workstations, identity providers, and more**
- **Direct integration with password manager for centralized administration and streamlined user experience**

Single Sign-On (SSO)

SSO goes a few steps further than a password manager by replacing the authentication protocols used to log employees into services. 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 SAML 2.0 to authenticate the user in the background with the same secure session.

In other words, SSO reduces the number of end-user passwords by providing secure cloud access to multiple applications with only one set of credentials. Combining SSO with a password manager allows IT to "see" and manage all access points across the business, whether an IT-managed app or an employee's website login saved to the portal.

WHAT TO LOOK FOR:

- **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**

Checking The Boxes With Lastpass Business

For more than 70,000 businesses, 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.

In addition to password management, LastPass Business offers additional security features, such as single sign-on (SSO) with simplified access to up to three cloud applications and multi-factor authentication (MFA) that secures the LastPass vault and those single sign-on applications.

Features include:

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

Additional Add-Ons:

LastPass Advanced Single Sign-On

LastPass Advanced Single Sign-On 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 single sign-on 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.

LastPass •••|

Security, simplified for your business.

Learn More