

Zero-Stress Cybersecurity

Secure Access
Applications & Devices

Table Of Contents

About SelectHub	3
Introduction	5
Key Takeaways	6
How Does a Password Management Tool Work?	7
Deployment Methods	8
Primary Benefits	9
Implementation Goals	12
Basic Features & Functionality	13
Advanced Features & Functionality	14
Current & Upcoming Trends	15
Software Comparison Strategy	17
Popular Password Management Software	19
Questions To Ask	32
Next Steps	34
1Password Feature	35
Enterprise Software Selection Assistance	36
Password Management Software Help	37

About SelectHub

SelectHub is a combination of a software selection platform and research firm providing the methodology and expertise that makes selecting enterprise software streamlined, agile, collaborative, and free of bias.

SelectHub supports everything from initial research to vendor selection and price negotiation. Driven by data from detailed analysis and research, and validated across thousands of diverse selection projects, SelectHub shortcuts the selection process, ensuring more informed, accurate purchase decisions.

SelectHub has helped 125,000+ companies select the right software



Top 10 Endpoint Security Software Comparison

WEBROOT®
an **opentext™** company

CARBON
BLACK
ARM YOUR ENDPOINTS


Microsoft®
System Center


CISCO

eset®

 **TREND**
MICRO™

 **BlackBerry®**

 **McAfee™**

 **SOPHOS**
ENDPOINT

 **Symantec™**

Free Report



Introduction

Keeping your business secure shouldn't feel chaotic. But if you're trying to manage dozens of apps, devices and passwords, it probably does. You're not alone, and you're definitely not doing anything wrong.

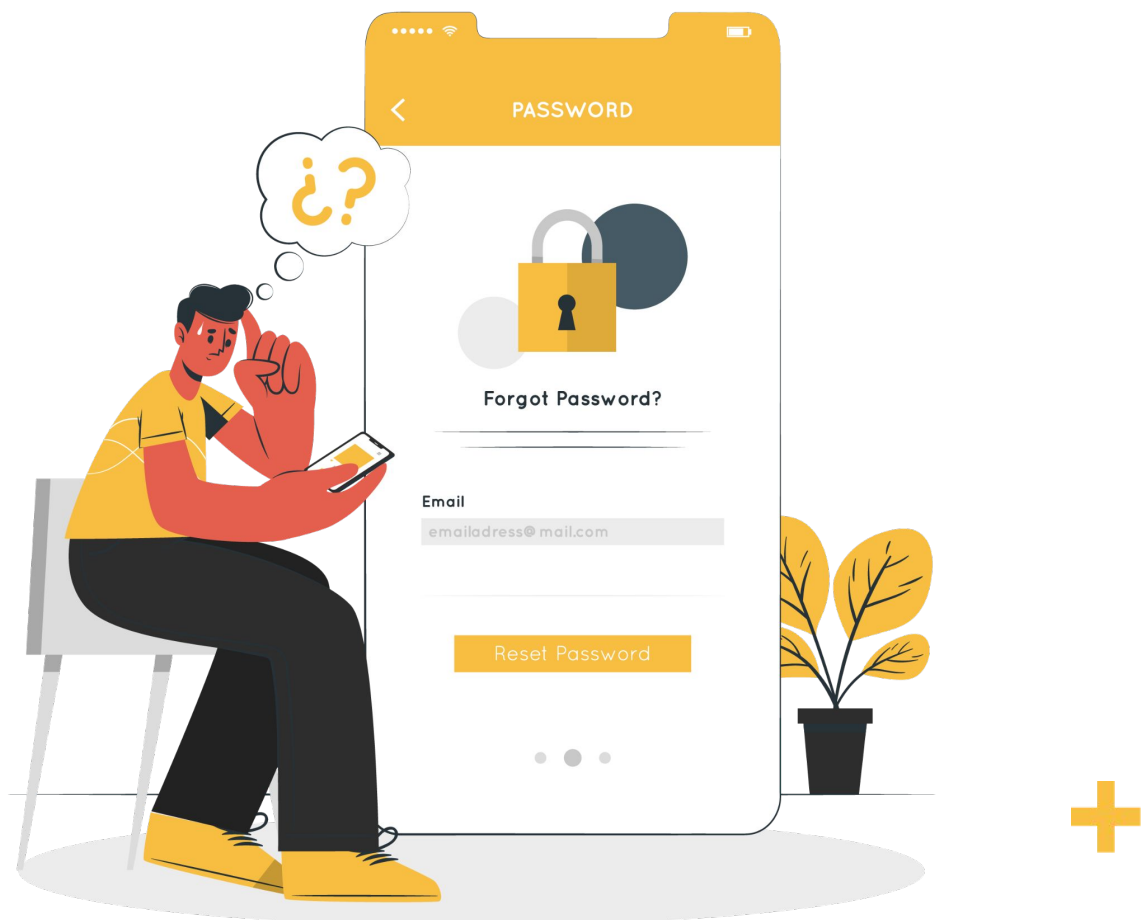
The good news? You don't need to overhaul your entire tech stack to take control. One of the easiest first steps is using a password manager — a simple tool that stores your login info securely, saves your team from password headaches, and gives your IT folks one less thing to worry about.

It's a small change that removes a big risk and gives you a fast win on the path to smarter, safer operations. Let's walk through what it does, why it matters, and how it's the perfect starting point for zero-stress cybersecurity.



Key Takeaways

- ★ Password managers help companies improve data security, promote productivity and reduce the risk of data breaches.
- ★ System admins and security officials can monitor threats and breaches, enforce security policies, gain visibility into password health, manage access and compliance, and improve ROI.
- ★ Core capabilities include password generation, password management, proactive security insights, single sign-on integration and zero-knowledge encryption.
- ★ The platform enhances the user experience by safely storing passwords and digital assets in encrypted formats, relieving employees from the need to remember numerous passwords.
- ★ When choosing a password manager, take the time to research vendors and ask some probing questions.





How Does a Password Management Tool Work?

A password manager acts as a digital brain for all your logins — only smarter, more secure, and way less forgetful than you (or anyone on your team). Instead of managing dozens of passwords across your laptop, phone, work apps and email accounts, you only need to remember one: your master password.

From there, your password manager jumps in to help wherever you need it:

- **Logging into your apps on any device?** It autofills your credentials, whether you're opening Slack on your laptop or checking email on your phone. It typically uses end-to-end encryption and advanced methods like 256-bit AES encryption to protect your online identity and reduce the risk of cyber threats.
- **Using a browser to access tools like Google Workspace, Salesforce or Zoom?** Your login info pops in automatically — no typing, no digging through sticky notes or spreadsheets.
- **Working remotely or on the go?** You can access all your credentials securely from any device, with end-to-end encryption keeping things locked down.

And there's more! It can flag weak or reused passwords, suggest stronger ones, and even let you securely share logins with teammates without ever emailing a password. Overall, it takes the stress out of managing passwords across the tools and devices your business runs on every day.





Deployment Methods

Bringing in a new tool can shake things up, for better or worse. The way you roll it out can either make things smoother or slow down your workflow.

That's why it helps to understand your deployment options upfront.

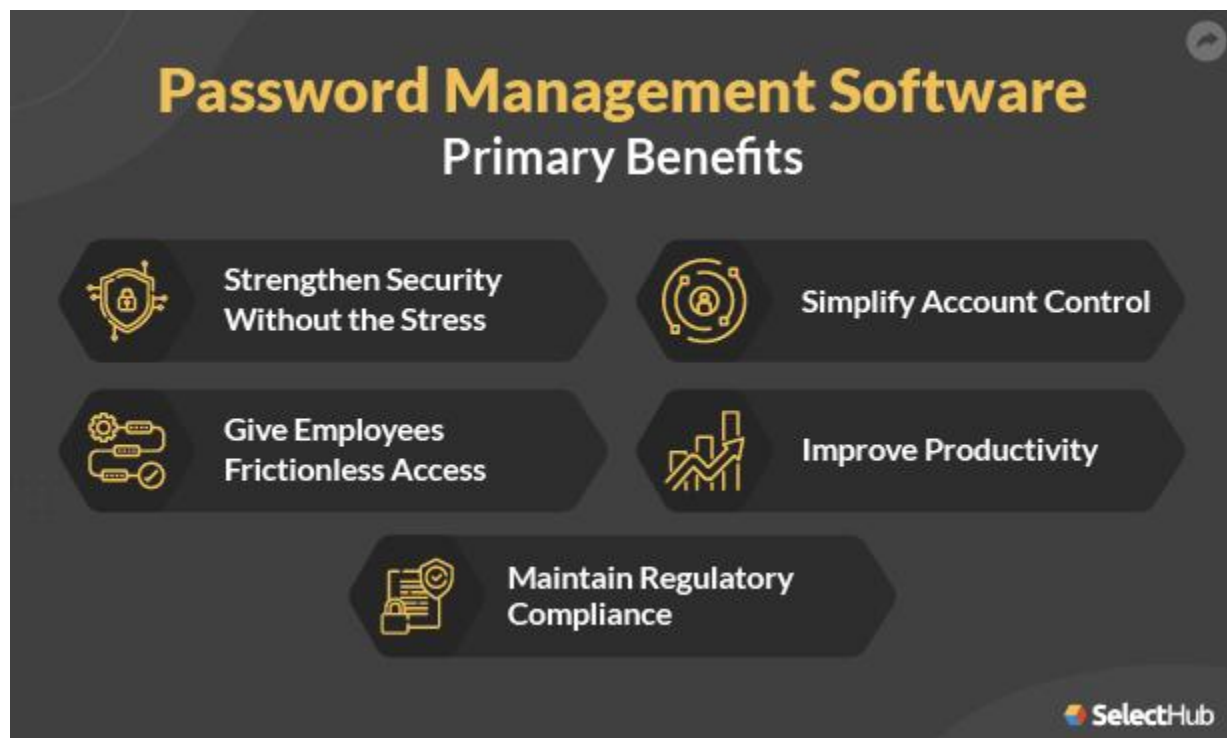
Here's a quick breakdown to make your transition as stress-free as possible:

Deployment Type	Best For
On-Premises: Installed and operated from the organization's in-house servers and computing infrastructure.	Large enterprises with dedicated IT teams, stringent security requirements and the need for control over data storage due to compliance requirements.
Cloud-Based (SaaS): Hosted and maintained by a third-party provider on the cloud. Users access the software through a web browser or a cloud-connected desktop or mobile application.	Small to medium businesses or any organization looking for lower upfront cost, rapid deployment and scalability without needing extensive IT resources.
Hybrid: Combines elements of on-premises and cloud-based deployment. Certain components may be hosted in the cloud, while others are managed on-site.	Organizations that want the flexibility to keep sensitive data on-premises while leveraging cloud scalability and accessibility.





Primary Benefits



Strengthen Security Without the Stress

Enterprise-grade password managers use AES-256 encryption to store credentials safely, but their real strength lies in everyday protection. By generating unique, complex passwords for each account and auto-filling them only on verified websites, they help prevent phishing attempts before they ever become a problem.

Some platforms, like 1Password, go even further with automatic updates, ensuring your software is always running with the latest security patches. Admins can also set up custom roles and access groups, giving teams the access they need without overexposing sensitive data.

Give Employees Frictionless Access

Let's face it — most people reuse passwords. In fact, 61% of employees admit to it, according to the 1Password State of Enterprise Security Report. This creates a serious risk: one compromised password could unlock five more apps.

With a password manager, your team only needs to remember one master password. From there, the software auto-fills credentials across work apps — from email and file sharing to CRMs and project management tools. Less password fatigue means faster logins, fewer mistakes, and a lower chance of risky workarounds.

Simplify Account Control

Managing user access across dozens of tools can get messy, fast. Password managers give IT teams a single dashboard to handle onboarding, offboarding and access changes without hunting through individual apps.

Features like secure password sharing, access logs and custom permissions help you stay in control of who can access what and when. No more emailing passwords or manually updating every platform when someone changes roles.



Improve Productivity

Forgotten passwords waste time and IT resources. With a password manager, employees don't need to reset credentials or wait for help from tech support. Everything is securely stored and ready to go, so they can focus on what actually matters: their work.

Even better, password managers integrate with browsers and mobile devices to autofill logins instantly, whether users are in the office or working remotely.

Maintain Regulatory Compliance

If your business needs to meet standards like SOC 2, HIPAA or GDPR, password managers help you check key boxes. They enforce password policies, enable secure sharing and generate audit logs to track access activity, giving your team the documentation needed for audits or assessments.

Features like multi-factor authentication (MFA) and role-based access control help demonstrate that you take data security seriously, without making compliance feel like a chore.



Implementation Goals

Like a train needs a destination, you need clear goals to work toward, ensuring your chosen software holds up its end of the bargain. Here are a few standard implementation goals to keep on your radar:

Goal 1 Enhance Security and Compliance	Password policies and encryption methods help protect sensitive information. This will ensure your company stays compliant with industry regulations and mitigates the risk of data breaches.
Goal 2 Optimize User Experience	Integrated single sign-on (SSO) and password autofill create a smoother and more efficient workflow, minimizing disruptions and improving overall productivity.
Goal 3 Centralize Management and Monitoring	You can manage and monitor password usage using a centralized platform. Allow IT administrators to enforce policies, track access and swiftly respond to potential security threats.



Basic Features & Functionality

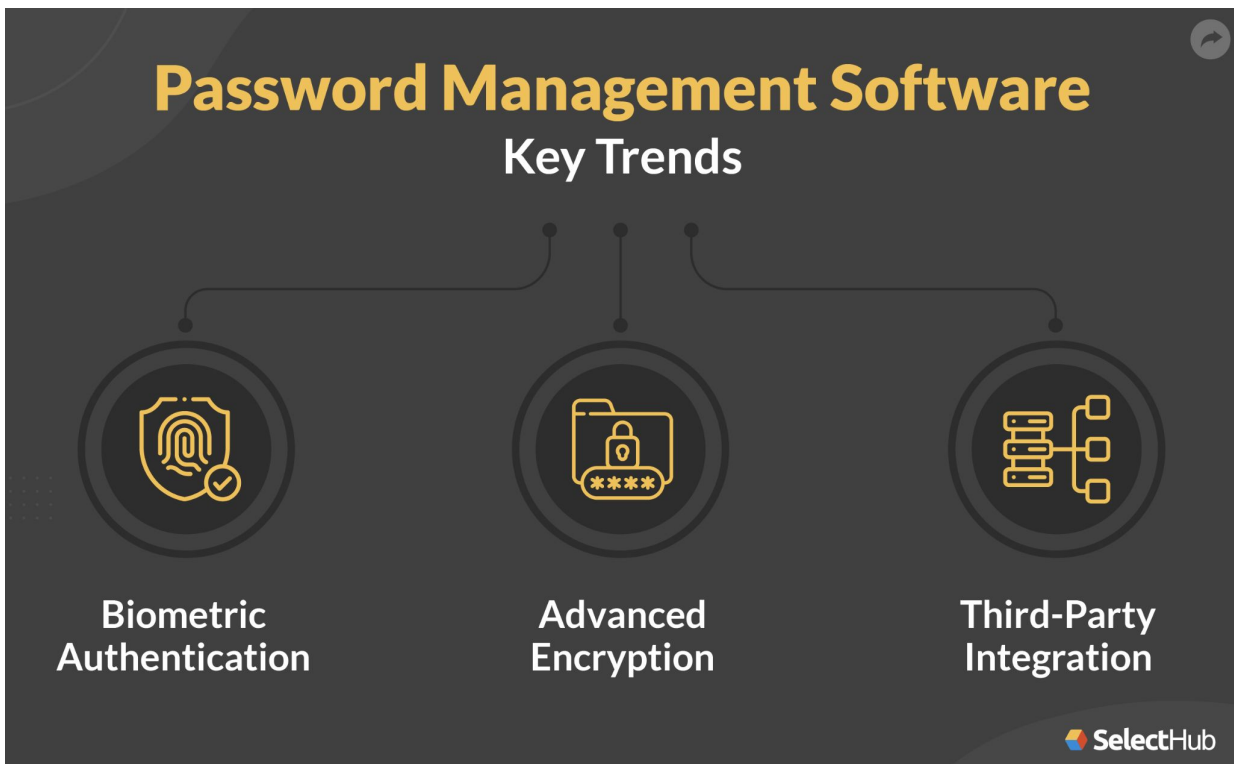
Multi-Factor Authentication (MFA)	MFA uses various authentication methods, including hardware tokens, software tokens, one-time passwords (OTP) and mobile push, significantly enhancing security compared to passwords alone. The only downside is that its increased complexity may lead to some employee frustration.
User Reports and Activity Logs	Generate reports and logs on activities such as file access and application usage. You can also filter or customize these reports to narrow the scope and focus on specific details. This functionality helps administrators monitor important events in the account, like when team members set up new devices, ensuring comprehensive oversight of account activities.
Password Generator	Creating unique, robust and random passwords is key to protection from hacking attempts. Password manager systems automatically create passwords that can withstand such attempts.
Password Management	You can store and auto-fill unique passwords securely. This feature eliminates the need to write down or store passwords in insecure locations. It also relieves users from the burden of managing multiple passwords.
Zero-Knowledge Encryption	This feature ensures that only you, as the owner, can access your data or passwords, not even the password management software vendor. It safeguards your data and reduces the risk of security threats.

Advanced Features & Functionality

Single Sign-On Integration	An integrated single sign-on interface provides access to all managed applications. Log in once, and you'll be signed into all the modules you need, enhancing both user experience and security.
Automated Provisioning and Deprovisioning	Onboarding new employees or changing job roles can be a nightmare for IT teams. It's difficult to manually handle permission approvals, account setups and endless forms. When integrated with your company's SSO provider, some password managers can automate provisioning by instantly granting access based on the employee's role. However, the extent of this automation may vary. When someone leaves, deprovisioning automatically revokes their access to ensure security and save you time.
SIEM Integration	Gain comprehensive visibility and control over authentication activities. You can collect, analyze and correlate data from password management solutions to identify suspicious behavior and potential security threats in real time.



Current & Upcoming Trends



Biometric Authentication

Who wants to type in a master password every time? Increasingly, password managers are supporting biometric authentication, like fingerprints or facial recognition, to make logging in feel as easy as unlocking your phone. Biometrics add both convenience and security, removing the need to remember (or mistype) a complex password. It's fast, intuitive and helps reduce the risk of weak or reused credentials.



Advanced Encryption

More password managers are adopting zero-knowledge security models, which means even the service provider can't see your data. Your credentials are encrypted before they ever leave your device, and only you hold the key.

This approach, along with end-to-end encryption and modern cryptographic algorithms, ensures that even in the unlikely event of a breach, your data remains unreadable and secure. It's peace of mind, built into the tech.

Third-Party Integration

The best password managers aren't standalone tools anymore. They're part of your wider security ecosystem. Many now integrate with your existing IT systems for real-time threat monitoring, especially when connected to SIEM platforms (Security Information and Event Management). They also work hand-in-hand with SSO (Single Sign-On) solutions, so employees can access multiple business apps with just one secure login.



Software Comparison Strategy

With so many password management tools out there, selecting the right one can be tricky. The first step is to create a checklist to ensure the software meets all your basic and advanced needs. Consider factors like:

- **Feature Set:** Ensure the software meets your organization's specific identity and access management needs, including support for compliance with relevant regulations.
- **Integration Capabilities:** Check compatibility with your existing infrastructure and apps. The more seamlessly a password management solution can integrate, the better its performance and utility will be.
- **Scalability:** Consider whether the password management solution can scale as your organization grows and if it can manage the increasing number and types of users and services.
- **Vendor Reputation and Support:** Assess the vendor's reputation, industry track record and quality of customer support. This can be crucial for resolving potential issues swiftly and effectively.
- **Security:** Evaluate the robustness of the security features provided, including how the system manages updates and patches to address new vulnerabilities.
- **Total Cost of Ownership (TCO):** Consider the initial purchase cost and any ongoing expenses. Account for training, support, maintenance and potential upgrades and compare the TCO of shortlisted software options.



- **Support and Maintenance:** Ask about the vendor's support and maintenance services. Understand the service level agreements (SLAs) and whether ongoing support comes with the original subscription.
- **Data Security and Compliance:** Consider security features and compliance certifications. Ensuring that the software complies with data protection regulations is crucial, and any additional security measures may impact the total cost.



Popular Password Management Software

With plenty of options to choose from, we've curated a list of popular password management systems to kickstart your search.

Product	User Satisfaction	Company Size	Starting Price
1Password	Excellent (94%)	S, M, L	\$19.95/mo (up to 10 users)
LastPass	Great (89%)	S, M, L	\$4.25/user/mo
NordPass	Excellent (90%)	S, M, L	\$1.79/user/mo
Sticky Password	Great (88%)	S, M	\$29.99/user/year
Enpass	Great (89%)	S, M, L	\$9.99/mo (up to 10 users)
Password Manager Pro	Great (84%)	M, L	\$595/year (2 admins, unrestricted users)

Editor's Note: Starting prices are for teams or business plans (whichever is cheaper), not personal or family plans.

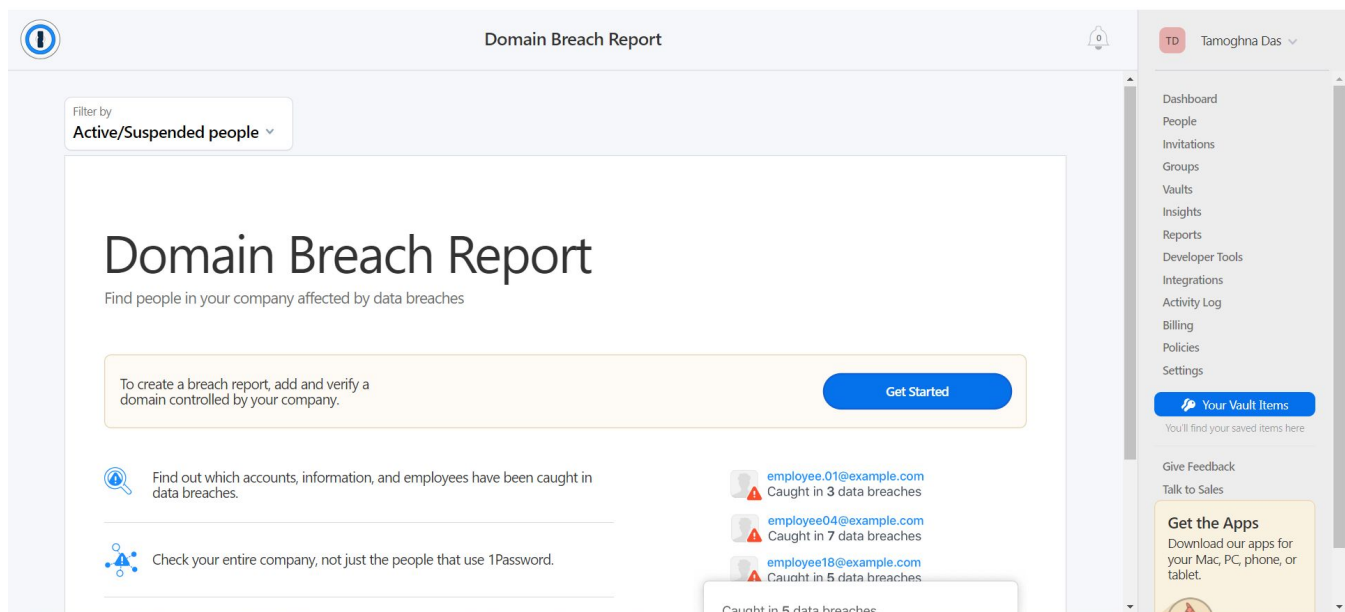


[Pricing](#)

1Password is built for people who want strong security without constantly worrying about it. AES-GCM-256 encryption and a unique Secret Key lock down your logins, notes and credit card info in a clean interface. Everything lives in a secure web vault; only you (not even 1Password) can access it.

What makes 1Password different is that it simplifies your day-to-day. It auto-generates strong, unique passwords, fills them in with a single click and syncs them across devices so you're not digging through notebooks or repeating the same weak password.

Security extras like Travel Mode let you remove sensitive data from your devices when you're on the move. Admins can set granular policies for apps, firewall access and even developer tools, so your team stays secure without feeling micromanaged.



Get a domain breach report on 1Password.

Its browser extension works smoothly across Chrome, Edge, Firefox and Safari, allowing you to autofill logins, save credentials and even manage passkeys. You can organize, move and securely share passkeys just like you would a saved password.

Designed for individuals, families and companies alike, 1Password offers scalable plans that grow with your needs, starting at \$2.99 per month. A 14-day free trial lets you test it out risk-free.

With a user sentiment score of 94% in our analysis, users love how it removes friction from daily login chaos, without sacrificing enterprise-level protection.

Best For: Security With Zero Stress

1Password is ideal for distributed or hybrid teams that rely on collaboration without compromising on control. For instance, a remote startup scaling rapidly across time zones can use 1Password's shared vaults to manage access to project tools, client accounts and sensitive documents, all while keeping everything secure and easy to organize.

Pros

- Seamless multi-platform integration
- Military-grade encryption and zero-knowledge architecture
- Easy-to-use admin dashboard and policy controls
- Travel Mode and secure vault sharing

Cons

- Premium pricing may not suit small teams
- Mobile app UX can feel less refined than desktop
- Occasional browser extension glitches

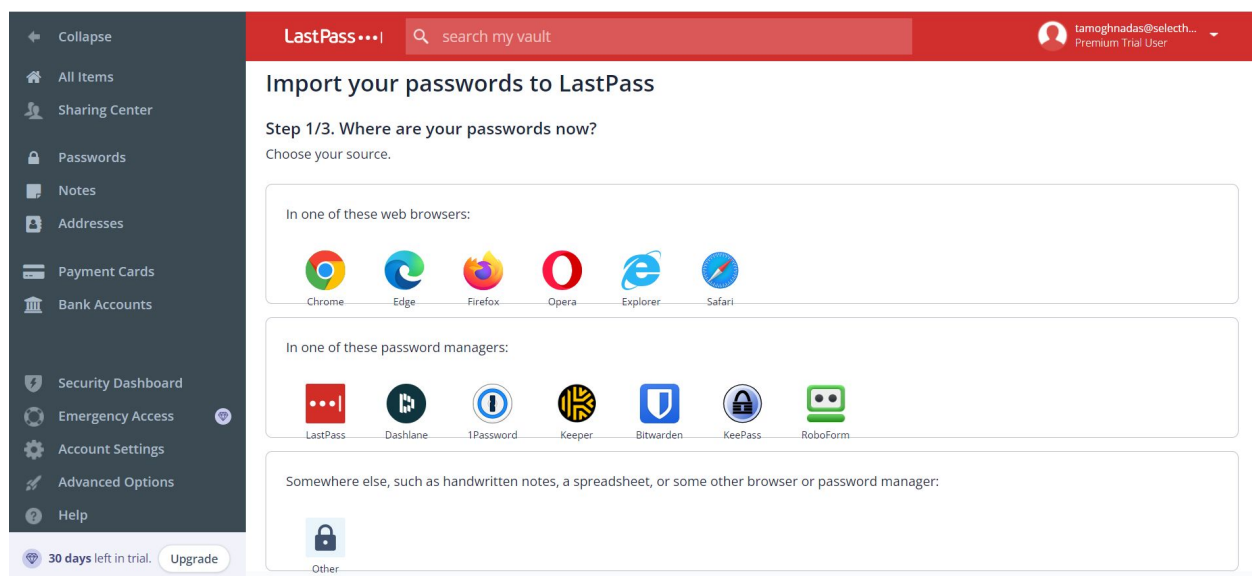




Pricing

LastPass helps you keep all your passwords in one place, securely encrypted, easily accessible and available wherever you are. It works across devices and browsers, auto-fills credentials, and even generates strong passwords to help you break the “123456” habit for good. LastPass encrypts password data using AES-256-bit encryption and locks everything down before your data hits the cloud.

It doesn't stop at convenience. LastPass offers a built-in security dashboard that flags reused or compromised credentials so you can fix problems before they become threats. You'll also get features like emergency access (so trusted people can recover your account), secure sharing and multi-factor authentication, which adds a second layer of protection beyond your master password.



Access various import options through LastPass.

Its free plan gives solo users a decent starting point, but you'll want a paid tier to unlock key features like unlimited device syncing, 1 GB of secure storage, advanced MFA options and priority support. For families and businesses, shared folders and admin controls make it easy to manage accounts across teams or households.

LastPass offers team plans starting at \$4.25 per user monthly, including a 14-day free trial.

With a user sentiment score of 89% in our analysis, LastPass is valued for its wide feature set and flexibility, even though some users keep an eye on its security history.

Best For: Different Device Preferences

LastPass is useful for teams that need multi-device access, secure password sharing and a built-in security dashboard, with a balance of ease and control. It's great for organizations where IT may not be hands-on with day-to-day operations.

Pros

- Centralized admin panel and policy enforcement
- Strong MFA, SSO and passwordless login options
- Useful security dashboard for real-time threat visibility
- Scalable pricing with team-focused features

Cons

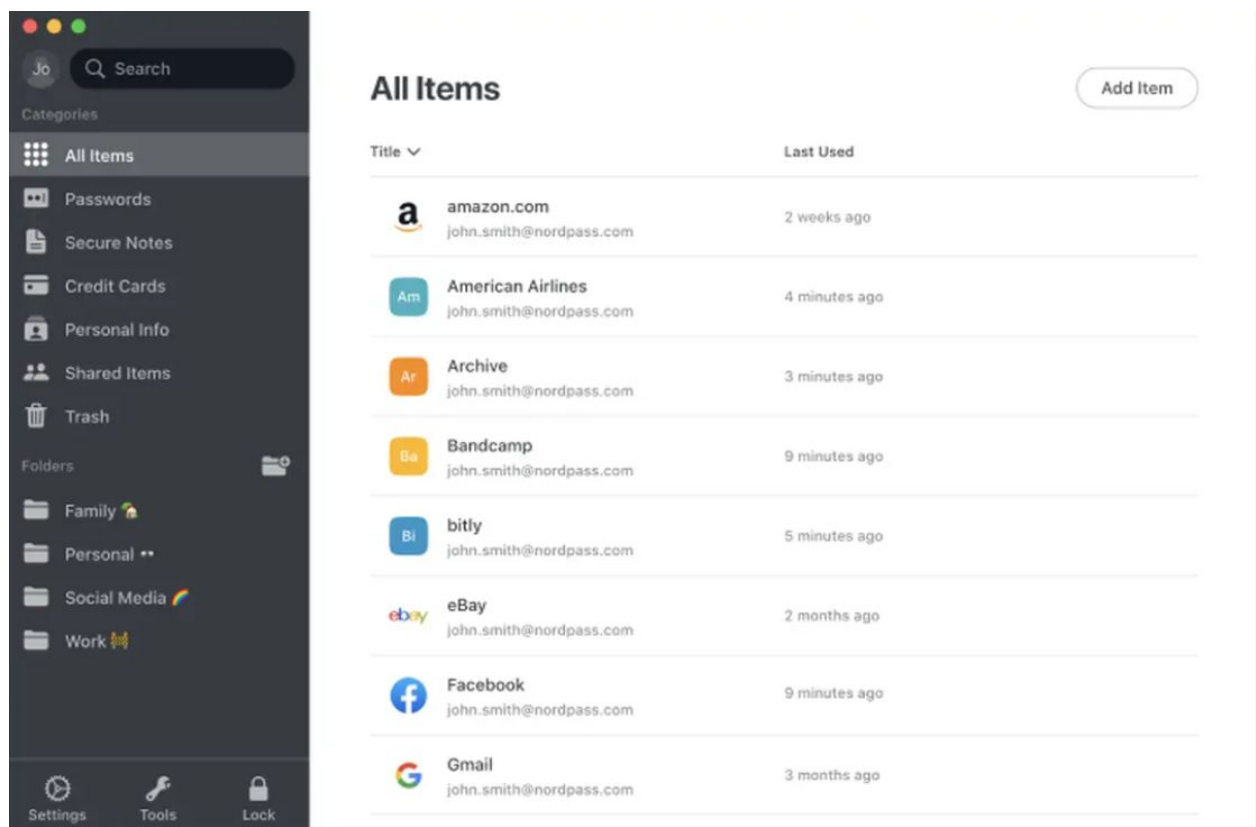
- History of breaches may concern risk-averse teams
- Limited features on the free tier
- Browser extension issues reported



[Pricing](#)

NordPass is a modern password manager built by the cybersecurity experts behind NordVPN. It's designed for people and businesses who want airtight protection that doesn't get in the way. Using the XChaCha20 encryption algorithm, NordPass secures everything from logins to credit card details, even notes, while keeping things fast and user-friendly.

Its autosave and autofill features work across major browsers, including Chrome, Firefox, Safari, Edge and Opera. You can sync your data across all devices, desktop, mobile and tablet, without worrying about version mismatches or missed updates.



Securely store passwords and other sensitive information with NordPass.

One standout feature is NordPass's web vault. It encrypts all your data locally (on your device) before uploading it, so even if someone breaches the cloud, your info stays unreadable. It also supports passkeys, keeping you ahead of the curve as more platforms move toward passwordless logins.

NordPass also makes pricing approachable. Personal and family plans include a 30-day free premium trial, while its business tier starts at just \$1.79/user/month (for a 10-user pack). This pricing makes it one of the most affordable options for small teams just getting serious about security.

With a user sentiment score of 90% in our research, users consistently highlight how easy it is to get started and how quickly it makes password stress a thing of the past.

Best For: Small Teams

NordPass is a good match for startups or lean teams that need strong encryption, simple UI and budget-friendly plans. The XChaCha20 encryption standard, smooth browser extension performance and passkey support make it a future-ready choice, without complexity or steep learning curves.

Pros

- Strong encryption with zero-knowledge architecture
- Passkey and biometric support
- Affordable business pricing and family plans
- User-friendly web vault and mobile apps

Cons

- The free version is limited to one device at a time
- No VPN bundling like some competitors
- Credential sharing and attachments are not available in the free plan



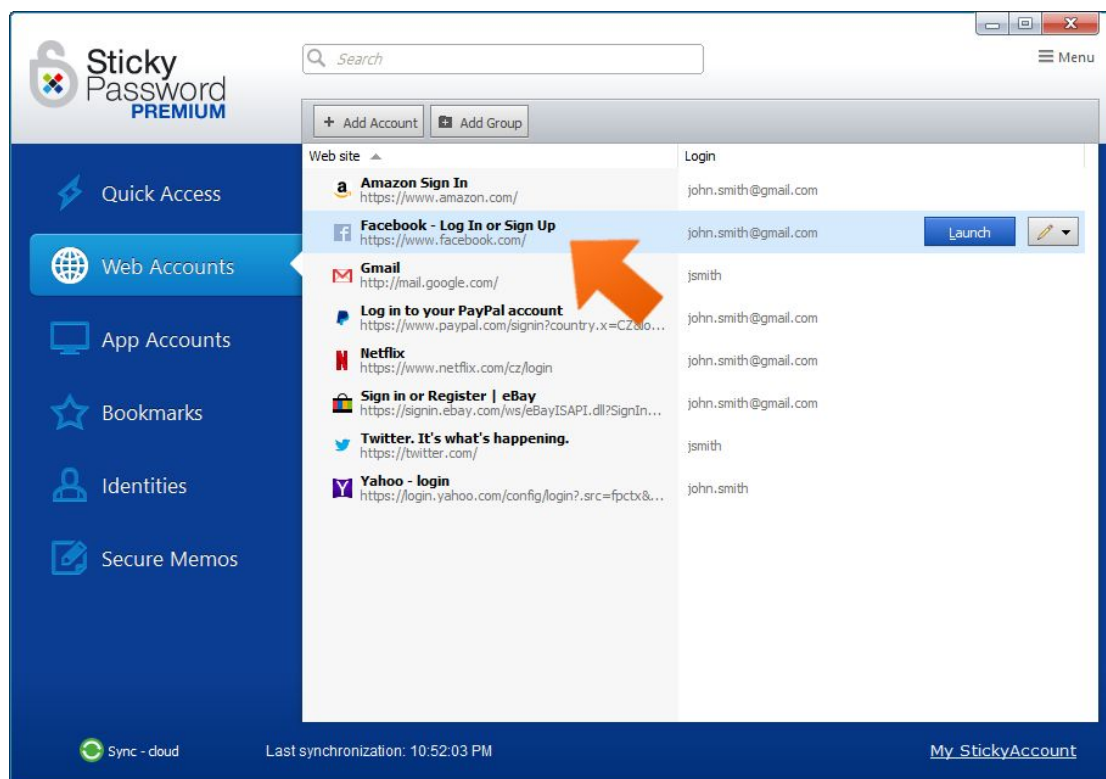


Pricing

Sticky Password is a security-first password manager for teams and individuals who want full control over how and where their data is stored. While most password tools default to cloud syncing, Sticky Password gives you a rare option: local Wi-Fi sync. That means your data never has to touch the cloud — ideal for privacy-conscious users or offline work environments.

It uses AES-256 encryption and allows secure sharing, biometric logins and automatic form filling across devices. Sticky Password is compatible with all major operating systems and browsers and offers a one-time purchase option, making it attractive for teams who want strong protection without recurring fees.

One of its most stress-saving features is its simple interface. You won't find complex dashboards or confusing settings here. Just straightforward functionality that gets the job done.



Access your logins quickly using Sticky Password.

Sticky Password provides a 30-day free trial, and its annual subscription starts at \$29.99.

According to our research, Sticky Password earned a user sentiment score of 88%, with users appreciating its low-friction setup and privacy-forward features.

Best For: Privacy Without Cloud

With local Wi-Fi syncing, Sticky Password is perfect for teams working in offline or secure environments. For example, a legal team operating on-premises in a data-sensitive industry can sync passwords locally across devices via Wi-Fi. No cloud exposure, no client risk.

Pros

- Strong encryption and biometric logins
- Easy form filling and cross-platform support
- One-time purchase available (lifetime license)

Cons

- Outdated UI and limited collaboration features
- No dark web monitoring or SSO
- Premium plan needed for cross-device sync

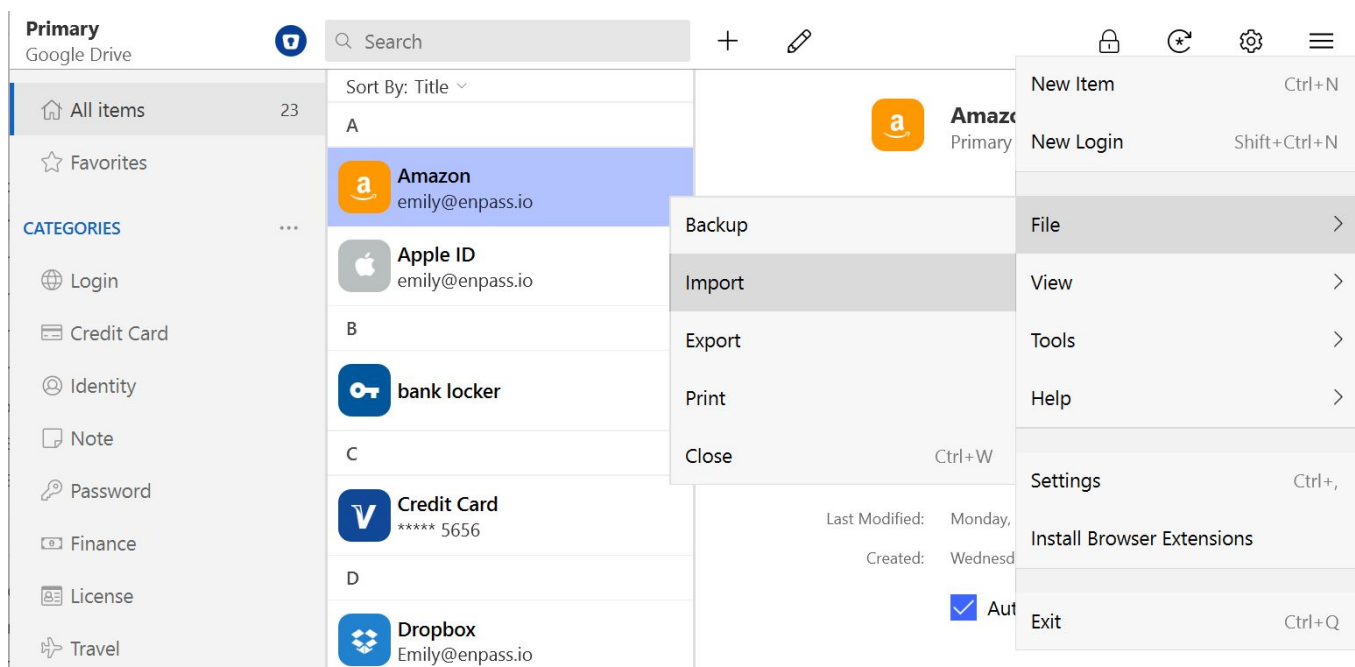


[Pricing](#)

Enpass flips the script on typical password managers by giving you total ownership of your data — no vendor cloud, no behind-the-scenes syncing. Everything is stored locally or synced through a third-party cloud provider of your choice (Google Drive, Dropbox, iCloud, etc.). That means you decide where your data lives and who touches it.

It supports unlimited passwords on desktop (even on the free plan), works offline and uses industry-standard AES-256 encryption to protect credentials, credit card data and secure notes. You can set up biometric login, autofill forms and access your vault across platforms, including Windows, macOS, Linux, iOS and Android.

Enpass offers a 14-day free trial for its business plan, and its Starter Plan costs \$9.99 monthly, billed annually.



Securely import your passwords and data into Enpass.

For compliance-heavy environments or teams managing sensitive client data, Enpass removes a huge amount of stress. There's no pressure to trust external cloud servers and no hidden sync policies to worry about. Its user sentiment score of 89% in our analysis reflects this trust, with many users citing Enpass as their go-to for local-first security.

Best For: Strict Compliance

Enpass is a smart choice for compliance-driven companies. For instance, a financial planning firm that needs strict control over customer data can store all passwords locally, disable cloud sync, and ensure everything remains compliant with internal and regulatory data retention rules.

Pros

- Local data storage with optional cloud sync
- Works offline with no vendor lock-in
- Free unlimited desktop storage
- Budget-friendly lifetime license

Cons

- The free mobile version is limited to 25 passwords
- No built-in sharing or advanced integrations
- Manual setup for some security features



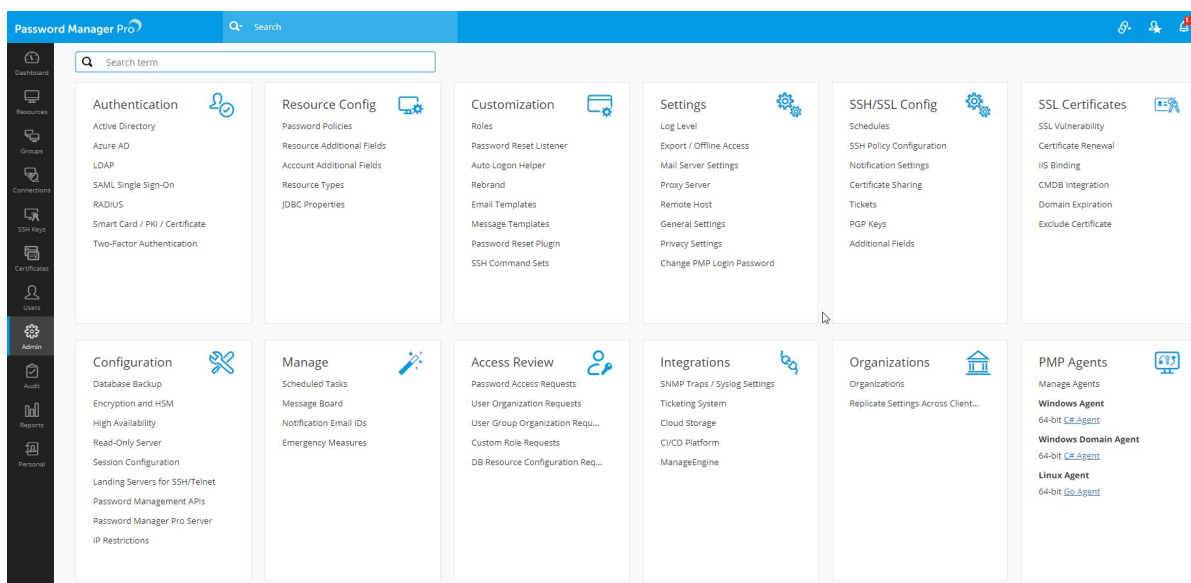
ManageEngine Password Manager Pro

Pricing

Password Manager Pro, developed by ManageEngine, is a powerful solution built for IT teams and large enterprises that need airtight credential management at scale. It isn't just about storing passwords — it's about enforcing least-privilege access, logging every action and integrating directly with your IT stack.

The platform uses AES-256 encryption, role-based access and multi-factor authentication to protect privileged credentials, service accounts and remote system logins. It integrates with SIEM tools, Active Directory and ITSM platforms. Also, it supports password rotation, auto-login and centralized vaulting for all accounts, no matter how complex your infrastructure.

What sets Password Manager Pro apart is its full audit trail. You can trace every access request, login attempt or credential update back to a user and timestamp, helping meet regulatory requirements and avoid internal mishaps.



Securely control authentication and resource access using Password Manager Pro.

Users can experience Password Manager Pro through its 30-day free trial, after which pricing starts at \$595.

With a user sentiment score of 84% in our research, it's well regarded for its feature depth, though users note it's best suited for environments with dedicated IT resources.

Best For: Enterprises With Complex Infrastructure

Password Manager Pro is built for IT administrators who need granular control and privileged account management. It's best suited for regulated industries, large IT teams or organizations with heavy infrastructure footprints.

A hospital IT department can use Password Manager Pro to restrict access to clinical software, log every login attempt and ensure that every action is traceable, supporting both security and compliance. It takes some setup but delivers industrial-strength control.

Pros

- Granular role-based access and password vaulting
- SIEM integration and advanced audit logs
- Auto-login and password rotation for service accounts
- Built for regulated and high-security industries

Cons

- Steep learning curve and complex UI
- High cost for enterprise features
- Limited mobile access usability
- Support responsiveness can vary



Questions To Ask Yourself

Before you pick a password manager, it helps to ask your team a few questions first. It'll save you from frustrations later and make sure you get your money's worth. Start with these:

- Why is a password manager important for managing our employee access?
- Can we define user permissions based on specific roles, resources and actions?
- What are our must-have features? What are our specific password management needs, and how will the new software effectively address them?
- What level of customer support and training do we need?
- How many employees will use the software?
- How scalable do we need the system to be? What's our desired deployment method?
- How easily does the password manager integrate with our existing IT systems and apps?
- What training resources and documentation are available for our IT teams?
- How quickly can we expect to see a return on investment?



Questions To Ask Vendors

Before you lock in a vendor, take a moment to research a little deeper. Asking smart, targeted questions helps you quickly zero in on solutions that actually fit.

About the Software

- What core features does the software offer?
- How intuitive is the user interface?
- How often is the software updated?
- Is it accessible on mobile devices, and does it offer a consistent user experience across platforms?
- What mobile-specific features are available?
- What analytics and reporting tools does the software offer?
- What automation and customization are available?
- Can you provide a pricing breakdown based on the user number or specific features?
- Does your software meet relevant industry standards and compliance regulations?

About the Vendor

- Can you share testimonials or success stories from satisfied clients?
- What measures are in place to ensure data privacy and security?
- What customer support do you provide? What contact methods are available, and what are the support hours?
- What recovery and data loss prevention methods are in place?
- Can you clarify contract terms, including termination clauses and renewal processes?
- How much notice do you require for termination, and what happens to our data upon termination?

Next Steps

You don't need to solve cybersecurity overnight. Choosing a password manager is just one step, but it's a meaningful one. The right tool should simplify your team's day-to-day, making it easier for employees to log in securely, and giving system admins more visibility and control without constant firefighting.

Start by narrowing your focus: What's most important — price, features, integrations or support? Pick the one that ticks your top boxes and confidently move forward. Because at the end of the day, security shouldn't be stressful. It should be one less thing to worry about.

See the following pages for additional help and resources from SelectHub.



Featured: 1Password Review

1Password has a lot to offer, including password generation, management and access control. Take a closer look at what 1Password does, who it's ideal for, and what its top use cases are.



Sponsored by 1Password

Part one of SelectHub's video series on 1Password. Also available: [1Password Key Differentiators](#), [1Password In-depth Review](#)

**Learn more about 1Password
for Password Management Software**

View All



Enterprise Software Selection Assistance

SelectHub's bite-sized approach is easy to follow and provides the best results.

Technology Selection & Sourcing Process

Source: SelectHub

	PROJECT STAKEHOLDER INVOLVEMENT		
	END USERS	IT DEPARTMENT	SOURCING & PROCUREMENT
➤ Requirements Gathering			
➤ Preliminary Research			
➤ Vendor Shortlisting			
➤ Informal Enquiries			
➤ Request for Demos			
➤ Tech Eval Scorecards			
➤ RFIs and RFPs			
➤ Business Case Review			
➤ Vendor Viability & Reference Checks			
➤ Contract Negotiation & Close			

SelectHub's Technology Selection Management (TSM) platform enables relevant stakeholders to come together and follow bite-sized process steps to achieve an objective, informed and consensus-driven purchasing decision. The specific process steps can be based on criteria such as project budget size, scope and sponsorship or even broader aspects such as organizational policies and compliance needs.

Evaluation & Selection

Assistance



Password Management Software Selection



Free assistance: Call 855-850-3850

