1Password

How to choose a password manager for your business

Introduction

Identity is at the core of every organization's security strategy, but credentials remain its weakest link; 1Password's 2025 Annual Report found that half of the CISOs who had experienced a breach within the past three years identified compromised credentials as a root cause. In the same report, two-thirds of employees admitted to unsafe credential practices, like reusing passwords across work and personal accounts, or sharing plaintext passwords via email or messaging apps.

Password managers are a foundational identity security control. A modern enterprise password manager provides oversight and management of these vulnerabilities by enforcing the use of strong and unique credentials and extending identity protection across all systems and devices.

Still, different password managers offer varying security and features. Here are critical differentiators to consider when finding the password manager that will best reduce breach risk, simplify audits, protect business continuity, and enable secure, efficient work across your organization.

What to look for in a modern password manager

Many users are familiar with password managers through first-party solutions like Apple's Passwords app and Google Password Manager. However, these often lack critical security features that are necessary for business security and compliance. Google Password Manager, for instance, doesn't default to on-device encryption, meaning that passwords may be left vulnerable.

For enterprise password management, third-party password managers provide stronger security and better cross-platform support. In this space, there are many options, and comparing their features requires going beyond checking compliance boxes. A password manager may have the right security, but implement it in a way that adds too much friction to employees' daily workflows. Other solutions may have varying security depending on the company using them, like only offering SSO provisioning on their highest-tier Enterprise plans.

When evaluating solutions, teams should begin by prioritizing the one that strengthens both security and operational efficiency. The right enterprise password manager should complement your existing identity, device, and security stack, so that all of your employees can stay productive and secure.

1.

A security model you can defend

The average cost to recover from a ransomware incident, excluding the ransom payment itself, exceeds $2.7M – not including downtime or reputational damage. Your password manager needs to have critical security features to protect against attacks.:

- **High end-to-end encryption standards** protecting credentials, URLs, item titles, and vault metadata, with decryption that happens locally on user devices.
- **Zero-knowledge architecture,** ensuring that only your organization can decrypt vault contents.
- **Locally generated secrets (such as a Secret Key)** that prevent server-side decryption, even if account credentials are compromised.

2.

Integration with your identity ecosystem

Password managers should extend and complement your company's chosen identity provider.

- **SSO unlock** so employees authenticate with existing credentials (Okta, Microsoft Entra ID, Google Workspace, and more).
- **SCIM provisioning** to automate joiner–mover–leaver workflows.
- **Granular policy controls** to enforce password standards, sharing rules, and MFA requirements.

3.

Visibility and governance for non-SSO authentication

1Password's 2025 Annual Report found that 34% of apps, on average, are not protected by SSO. Password managers need to bridge the gap and provide insight and control over these non-SSO tools.

- **Password health dashboards** identify weak, reused, or exposed credentials across your organization.
- **Centralized reporting** consolidates security health, usage, and sharing data – exportable for audits or SIEM ingestion.
- **Breach monitoring** notifies admins when corporate credentials appear in breach datasets.

4.

Policy, provisioning, and scale

Over one-third of employees have successfully accessed a prior employer's account, data, or applications after leaving the company. Teams should prioritize tools with automated and secure provisioning and deprovisioning processes to make sure that only the right people have access to the right applications.

- **Automated provisioning via SCIM** syncs user management with your IdP, eliminating manual onboarding and offboarding.
- **Fine-grained access controls** through vaults and group permissions enforce least privilege for shared accounts and sensitive systems outside SSO.
- **Audit-ready logs and Events APIs** streamline evidence collection for SOC 2, ISO, and internal reviews.

5. User experience and adoption

The user-experience is paramount to the success of any security tool. After all, even the most secure control fails without adoption.

- **Intuitive apps** for macOS, Windows, Linux, iOS, and Android, plus browser extensions that make secure login effortless.
- **Reliable autofill** that works consistently across platforms and environments.
- **Onboarding and training resources** that drive behavior change and reduce help-desk volume.
- **Free family accounts** that help employees practice good security habits at home, leading to higher engagement and long-term risk reduction at work.

6. Developer & IT workflows

Modern password managers should secure infrastructure secrets, not just user credentials – applying the same zero-knowledge encryption to every asset:

- **Secrets management** for API tokens, app keys, and SSH credentials, with autofill and CLI integrations that eliminate hard-coded secrets.
- **Travel Mode** to temporarily remove vaults from devices when crossing borders or entering high-risk regions, without disrupting admin operations.

7.

Support for passwordless authentication

89% of security and IT professionals say their company is encouraging employees to shift logins to passkeys. Still, passwords aren’t likely to be fully deprecated any time soon. Choose a solution that bridges current credential needs with emerging standards:

- **Passkey support** that integrates cleanly with existing MFA and device-trust policies.
- **Flexible access policies** to manage both password-based and passwordless authentication during rollout.

8.

Support that scales with your business

Security tools are only as strong as the teams behind them. Choose a partner with the scale, expertise, and accountability to support mission-critical operations.

- **Dedicated onboarding and resources** that accelerate deployment.
- **Support via chat, email, and phone** for confident scaling.
- **Comprehensive documentation and admin guides** for efficient troubleshooting.

Questions to ask potential vendors

1. How does your encryption model prevent unauthorized access to data outside of our organization?
2. Do you encrypt vault metadata (URLs, item titles) in addition to credentials? What about data in transit?
3. Can employees unlock your solution using our existing SSO?
4. Does your SCIM integration offer full automation for onboarding and offboarding?
5. What visibility and reporting tools are available to identify weak or compromised credentials?
6. How do you support passkeys and other passwordless standards?
7. What options exist for exporting logs or integrating with our SIEM?
8. What customer success and support resources are included with the subscription?

These questions separate basic tools from true enterprise-grade solutions built for security, scale, and compliance.

What do you need to do before getting started?

Identify your key stakeholders and understand their requirements

Effective password management requires alignment across security, IT, and operations. Here are considerations to keep in mind to get buy-in from key stakeholders throughout the process of considering and rolling out a password manager.

IT and Operations require integration with existing providers, ticket volume reduction, and onboarding/offboarding automation.

Questions to ask:

- How many password reset tickets do we handle monthly? What's the cost and time spent per ticket?
- How many applications sit outside of our SSO? Which applications are they? How do we secure those today?
- What's our current process for revoking access when someone leaves? How long does it take to do so?
- Do we have visibility into shared credentials or accounts accessed by contractors?

Security is concerned with zero-trust architecture, audit logging, SIEM integration, and incident response capabilities.

Questions to ask:

- Where are our biggest credential-related blind spots today?
- How quickly can we detect and respond to a compromised credential?
- What percentage of applications enforce MFA? What about phishing-resistant MFA?
- Do we have audit-ready logs for access reviews and compliance reporting?

Compliance teams require verifiable controls and reporting to meet regulatory requirements and compliance frameworks like SOC 2, ISO 27001, HIPAA, and GDPR.

Questions to ask:

- What's our process for preparing audit reports today? How much manual effort is involved?
- Are access controls clearly mapped to compliance requirements?
- Where do we have unmanaged identities or SaaS apps creating compliance gaps?
- How do we document password policies and enforce them across the organization?

Executives and finance both require clear ROI, reduced risk exposure, and faster audit cycles.

Questions to ask:

- Do we have visibility into SaaS license utilization across tools?
- Are we experiencing SaaS sprawl or redundant tooling?
- What's the cost of our current identity and access management stack?
- Can we consolidate vendors to reduce overhead and improve ROI?

When these groups are aligned, password management becomes more than a security initiative; it becomes a measurable business control that enables team workflows, saves time for employees, and scales with your organization.

How 1Password helps organizations stay secure and agile

1Password is trusted by over 180,000 businesses to protect credentials and secrets across every device, team, and environment. Our platform combines human-centric design with uncompromising security to deliver protection that teams actually use.

Measurable business impact:

Forrester's Total Economic Impact study of 1Password Business found:

- 206% ROI over three years
- $286,000 saved through reduced IT support costs, and 70% reduction in password reset tickets
- An increase of 4,310 hours per year in total employee efficiency

Security architecture built for zero-trust:

- **Zero-knowledge, end-to-end encryption** means only you can access your data – by using AES-256-GCM encryption for vaults, TLS 1.3 for all connections, and metadata encryption to prevent inference attacks.
- **Dual-key protection** adds an additional layer of encryption through a locally generated Secret Key unique to each account.

Identity ecosystem integration:

- **SSO and SCIM integrations** extend your identity provider, automate provisioning and onboarding/offboarding, and maintain policy alignment.

Effortless adoption:

- **Cross-platform apps and browser extensions** make secure login effortless anywhere your team works.
- **Dedicated onboarding and 24/7 support** with global customer success and documentation to ensure quick adoption and operational continuity.

Continuous monitoring and visibility:

- **Watchtower** continuously monitors for weak, reused, or breached credentials across your domains.
- **Audit logging, insights reporting, and Events APIs** give admins real-time visibility and integration with SIEM tools for audit logs and compliance.

Developer and infrastructure security:

- **Secrets Management** for secure storage and distribution across the DevOps lifecycle using 1Password Developer Tools (CLI, SDKs, Environments).

Modern authentication support:

- **Passkey support** provides governance and storage for passwordless authentication methods.

The result: 1Password provides companies with stronger security posture, measurable risk reduction, and simplified audit readiness – all without slowing your teams down.

Choosing with confidence

The right password manager doesn't just protect logins; it enforces policies, centralizes visibility, and closes the identity gaps every attacker looks for.

1Password combines uncompromising security architecture with the usability that drives real adoption from admins and end-users alike. It's a control you can defend to your leaders, and one your teams will actually use.

Our team will work with you to understand your unique business needs. Head to 1Password.com/business to start a 14-day free trial, or contact the 1Password Sales team to explore whether 1Password is the right fit for your organization.

Need help building the business case? Learn how to convince your leadership team with our free guide: How to Make the Case for a Password Manager, and download the Forrester TEI report to assess the financial impact.

Ready to evaluate 1Password?