1Password

The business case for a **password manager**

An outcome-driven guide to align secure access with strategic business priorities.

Chances are, you already understand that a password manager is essential for protecting your business, but you may need to convince your leadership team that it's a worthwhile purchase. They may be resistant to adopting and rolling out a new security tool, or assume existing measures like SSO or MFA are sufficient.

The key to securing executive buy-in is demonstrating how secure vaulting and credential management directly drive top-level organizational goals: mitigating security risks, enabling efficiency, and optimizing budget.

This isn't just an IT discussion, it's a business one. According to 1Password's 2025 Annual Report, 66% of employees engage in unsafe password practices, like reusing credentials across multiple accounts. These bad habits have real business impact; year after year, compromised credentials remain the most common vector for costly data breaches. Likewise, poorly managed credentials complicate onboarding and offboarding and cost hours of IT time fielding password reset requests.

Purchasing an enterprise-grade password manager is one of the simplest, most impactful choices you can make to improve your company's security and efficiency.

In this guide, we'll show you how to convince your leadership team to make it a priority.

Table of Contents

Let’s begin by describing what an enterprise password manager is and does, using 1Password as the example.

1Password Enterprise Password Manager is an **encrypted vault that protects every credential your business relies on,** including passwords, API keys, tokens, and machine secrets.

It secures and governs credentials across SaaS, cloud, and AI environments, giving IT and Security confidence that every secret is protected and auditable.

Value gained when you secure credentials with 1Password

To gain buy-in for a new tool, you must first prove its value and overcome initial objections around budget constraints, implementation fatigue, and compliance concerns.

Executives think in terms of revenue protection, operational efficiency, risk mitigation, and competitive advantage. To gain traction with stakeholders, you can connect credential management directly to those priorities.

1Password Enterprise Password Manager secures credentials for humans, systems, and AI agents across SaaS, cloud, and DevOps environments. This isn't just about protecting employee logins; it's about governing the secrets that enable operations.

When you position it this way, the conversation shifts from "another security tool" to "foundational credential infrastructure."

1. Reduce risk and improve visibility

Passwords are an acknowledged problem for businesses; 44% of CISOs cite weak or compromised passwords as their top security challenges. While SSO helps to secure authentication and centralize access management, 70% of IT leaders acknowledge that it isn't a complete solution, and with an average of 34% of apps sitting outside SSO, many logins go unprotected.

Security and IT teams often lack visibility into credential health, not just for passwords, but for API keys, tokens, and machine secrets that teams and systems rely on.

You don't know where passwords are weak, reused, or compromised, nor can you easily track who has access to what, or identify shadow IT. The problem has intensified with the rapid adoption of AI tools.

Shadow AI is now the second-most prevalent form of shadow IT, with 27% of employees using AI applications that their employers haven't approved. Combined with the 52% of employees who download apps without IT approval, this creates significant blind spots in your application ecosystem.

A password manager provides a single source of truth, where you can enforce policies consistently and make informed security decisions. 1Password Enterprise Password Manager serves as a centralized solution for managing, accessing, and sharing critical company data, with role-based access controls that ensure users adhere to company security policies. This visibility is foundational for security, demonstrates audit readiness, and helps you maintain control as you scale.

2. Boost operational efficiency

Password resets are frustrating and time-consuming for end users and IT alike. When employees store and autofill credentials seamlessly, incidents of forgotten passwords drop dramatically.

1Password customers have reported a 66% reduction in IT time spent on password reset requests. That's time your team can reinvest in projects that move the business forward.

Access requests, manual provisioning, and delayed onboarding/offboarding waste hours across teams. 1Password reduces the burden on overstretched teams by cutting support tickets, automating provisioning via shared vaults or SCIM integration, and enabling self-service access with seamless credential sharing. This reduces IT workload and prevents costly lapses.

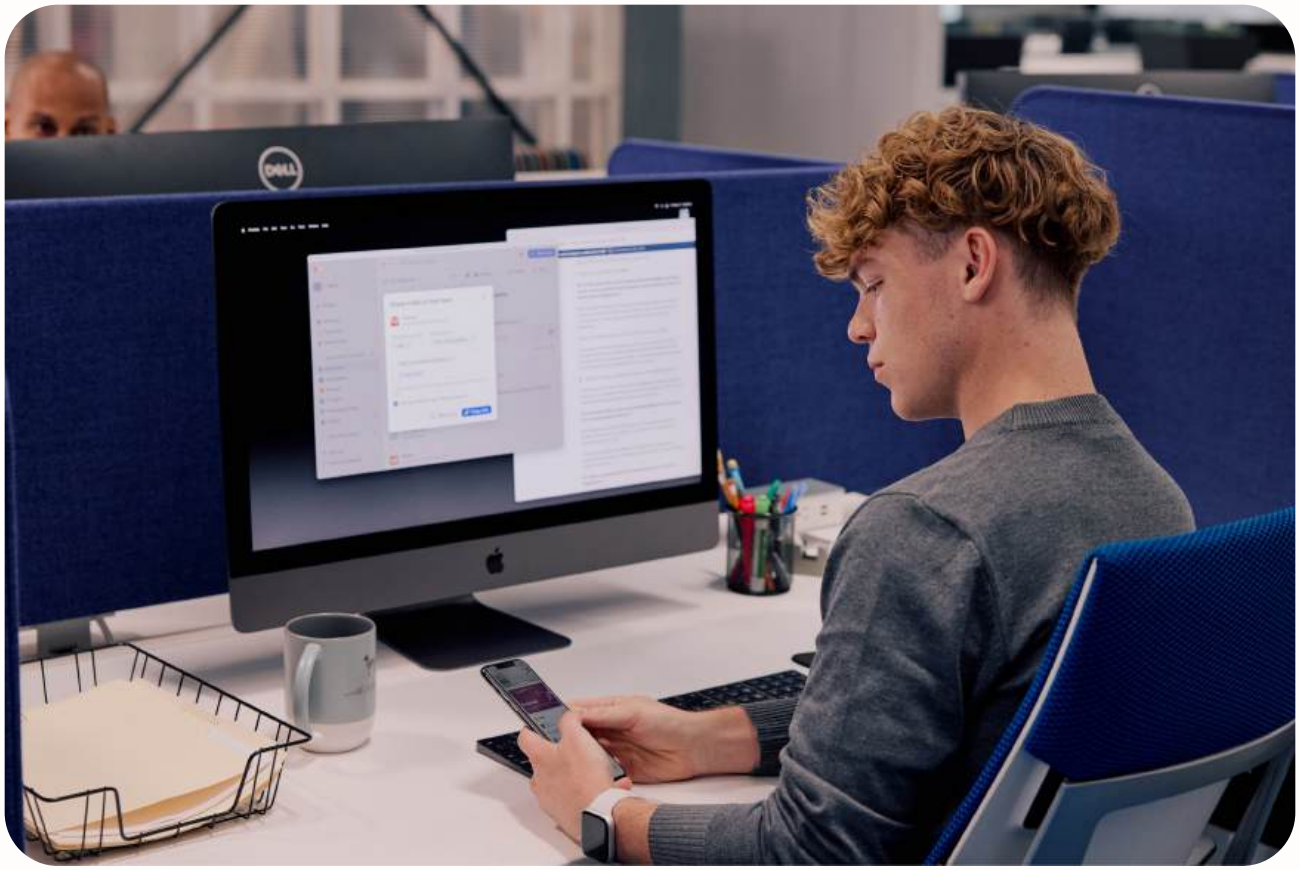
3. Enhance developer productivity and secrets management

For technology leaders, 1Password's value shows up in developer productivity. Developers need fast, secure access to secrets, API keys, SSH credentials, and environment variables.

Enterprise credential management simplifies the generation and use of strong, unique credentials, from passwords to API keys and developer secrets.

For development teams, it eliminates secrets sprawl by centralizing access to tokens, SSH keys, and environment variables, preventing hard-coded credentials from becoming security liabilities. For instance, 1Password's software development kits (SDKs) are production-ready, open-source libraries for TypeScript/JavaScript, Python, and Go that support secure access to secrets and items stored in 1Password.

1Password Enterprise Password Manager offers CLI support, CI/CD integrations, and secrets management that removes friction, prevents hard-coded secrets and secrets sprawl, and ensures credentials don't become technical debt. It's the encrypted vault for every credential your development teams rely on.



4. Demonstrate compliance, resilience, and business continuity

Compliance depends on continuous monitoring and record-keeping. Demonstrating compliance is easier with centralized audit logs, domain breach alerts, and password health reporting. With 1Password, you get the documentation and oversight needed to close gaps and demonstrate continuous compliance without manual reviews, simplifying evidence gathering for frameworks like SOC 2, ISO 27001, and NIST.

It's proof that your organization follows best practices for access control, credential hygiene, and data protection. It also supports Zero Trust by enabling least-privilege access, since admins can issue and revoke credentials based on team membership, seniority, or project participation.

As your business grows, whether adding team members, onboarding contractors, or acquiring companies, 1Password scales with you so security doesn't become a bottleneck.

When a contractor needs temporary access to an application, provisioning them via 1Password takes minutes. When vendors change login processes, your team doesn't scramble. You maintain resilience through centralized credential ownership that’s compatible with any device, without complex integrations.

Human and machine identities are provisioned quickly, access is segmented by role, and consistent standards are maintained across all types of credentials your organization depends on.

5. Drive measurable ROI

A password manager costs dollars per user per year, but the potential savings are exponential. Beyond avoiding the millions lost in a credential-related breach, 1Password customers see tangible reductions in IT support costs, fewer wasted hours on credential problems, and faster onboarding.

A password manager is more than just a security solution – it’s a business enabler. When you frame the conversation this way, you're not asking for budget approval. You're inviting leadership to make a strategic decision that advances the entire organization.

Overcome common objections

To gain buy-in for a new tool, you must first prove its value and overcome initial objectionWhen proposing any new security tool, you can anticipate some resistance. Use these responses to help field common questions and concerns from your leadership team, whether they come from Finance, Operations, or elsewhere. No matter the objection, you'll be ready to demonstrate how 1Password Enterprise Password Manager strengthens your security posture, saves time, and delivers measurable ROI.s around budget constraints, implementation fatigue, and compliance concerns.

Leader Type	Potential Objections	Counter Arguments
Financial	A password manager costs too much.	The average cost of a data breach is $4.44 million. 1Password Enterprise Password Manager is the best way to protect your organization against credential-based attacks.
Financial	We already have cybersecurity tools, why add another?	1Password Enterprise Password Manager secures credentials, which are the number one cause of breaches. It manages access for apps outside SSO and protects developer secrets.
Financial	We'll invest when the business grows larger.	Smaller businesses are prime targets for attackers because they often lack strong credential management. Investing early prevents costly security gaps and protects your business growth trajectory.
Operational	It'll take too long to implement a password manager.	Customers like Synex have implemented 1Password in just four days.
Operational	I'm not sure 1Password will fit into the tools we already use.	1Password is designed to fit into your existing stack, not to replace it. It supports identity security, plugs into SecOps and DevOps workflows, and works across the browsers, devices, and applications your team already uses.
Operational	Valuable time will need to be spent helping people learn how to use a password manager.	1Password's intuitive design makes it easy for anyone to use. And, with resources like 1Password Community and a best-in-class support team, 1Password is easy to onboard.
Technical	We already have a single sign-on (SSO) solution.	SSO reduces the number of passwords that every team member needs to manage and remember. But many accounts aren't covered by SSO, all of which need to be protected by strong passwords.
Technical	We already use multi-factor authentication (MFA), isn't that enough?	1Password can act as an authenticator for sites that support MFA, streamlining the login process for everyone on your team.
Technical	Don't we already have password management built into our browsers?	Browser-based managers are convenient for individuals, but they're not built for businesses and don't offer the centralized controls, visibility, security, or IT oversight that companies need.
Security	Keeping all our passwords in one place makes us vulnerable.	The information you store in 1Password is encrypted, and only you hold the keys to decrypt it.
Security	Isn't it risky for 1Password to have access to all that information?	1Password can't see your 1Password data, so they can't use it, share it, or sell it.

How businesses are **using 1Password**

More than **180,000 businesses trust 1Password** to secure their business and protect their data. Here's what our clients have to say about us.

"We looked at other tools. At the end of the day, we chose 1Password because of its supportability and usability."

– Reddit

"We constantly have new engineers joining our company as we go through a period of strong growth. We use 1Password as a way to securely provide access to passwords during the onboarding process. Having a way to provide access to those that require it quickly has helped us keep our data safe and secure."

– CareClinic

"Security can be a pain point or come across as a burden to employees, but 1Password is helping to eliminate the friction between security and business operations."

– Under Armour

"The internet is changing more and more. Many of the services our employees want to use don't support OpenID Connect (OIDC), SSO, or other enterprise tools. You need a tool like 1Password to provide secure, trusted access to those accounts."

– BuzzFeed

G2 REVIEWS

★★★★★ **September 17, 2025**

"A solid password manager that saves me hours and tons of headaches."

What do you like best?

I think the best thing about 1Password is how effortlessly it works across all my devices, especially with the browser extension. The auto-fill feature is brilliant and saves me a ton of time every single day. On top of that, the secret key option gives me peace of mind that my data is safe.

★★★★★ **July 31, 2025**

"Secure, seamless, and essential for modern work."

What do you like best?

1Password makes password and credential management incredibly seamless across devices and browsers. I love how intuitive the interface is, autofill works consistently well, and shared vaults make it easy for teams to collaborate securely without ever needing to exchange passwords manually.

Is your decision-maker a racing fan? Share that 1Password is the Official Cybersecurity Partner of Oracle Red Bull Racing to show you're on track for excellence.

1Password

Trusted by over 180,000 businesses, millions of consumers, and 1 million developers, 1Password is redefining identity security for the way people and AI agents work today. Our mission is to unleash productivity without compromising security. The 1Password Extended Access Management product suite delivers zero trust security that protects, manages, and governs access to all SaaS applications, whether managed by IT or not. Built on 1Password's Enterprise Password Manager, which secures more than 1.3 billion credentials, 1Password's Agentic AI capabilities extend identity security to AI agents and other non-human identities. Leading companies such as Asana, Associated Press, Browserbase, Canva, Cresta, Golden State Warriors, Hugging Face, MongoDB, Octopus Energy, Salesforce, SandboxAQ, Slack, Stripe, and Under Armour trust 1Password to provide the right person or AI agent the right access to the right app from a trusted device.

Learn more at 1Password.com.