1Password

# Securing your business starts with 1Password

## Enterprise Password Management

1Password gives you more visibility into your security posture, and the passwords and other secrets that impact it. Because you can't protect what you can't see.

You also get simple, centralized, granular controls to manage it all – and robust integrations to adapt 1Password to your needs. And it's all backed up with uncompromising security and usability to reduce your risk of non-compliance and breaches.

Forrester Consulting's Total Impact™ reports an organization using 1Password can experience 206% return on investment, reduce helpdesk tickets by 70%, and save 12,310 employess hours to increase productivity.

# When we say zero knowledge, we mean it

Protecting your data from breaches is only one aspect of enterprise security, but 1Password goes further to ensure that your secrets will remain safe – even in the unlikely event of a breach.

---

## Data protection and encryption

1Password encrypts your vault data in a fundamentally different way than most other password managers. Your information isn't just protected by an account password, but also by your unique Secret Key: a 128-bit, machine-generated code that's mathematically infeasible to crack. Dual-key encryption ensures that a breach would pose no threat to sensitive information stored in your vaults. Neither of these keys are stored on 1Password's servers, so even we can't access them.

1Password also takes the extra step of encrypting vaults, vault and item names, and website URLs. Attackers wouldn't know if they were trying to crack a vault with credit cards or cookie recipes.

- End-to-end encryption.
- 256-bit AES encryption.
- Secure Remote Password (SRP).
- PBKDF2 key strengthening.
- Two-key derivation (account password + Secret Key).
- Trusted device model.

### Details matter: Securing sign-in with SRP

Most websites use a traditional authentication process, sending your password to a server when you sign in. In addition to TLS encryption, 1Password uses a custom protocol known as Secure Remote Password (SRP) to ensure your password is never sent over the network, where an attacker could intercept it.

## Transparency

1Password wasn't built in a vacuum. It was developed on top of open standards that anyone can investigate, implement, and improve. We've documented our entire security model for experts to review – and they do, often.

- Open data formats.
- Trusted encryption algorithms.
- Principled privacy policy.
- Straightforward import and export tools.
- Public assessment and customer trust profile.

## Compliance certifications and audits

1Password meets and exceeds some of the most broadly recognized security standards and offers solutions to help you address your compliance requirements. We work with third-party security experts to audit 1Password, and we offer the largest bug bounty program in the industry so our security model stays one step ahead of ever-evolving threats.



**SOC2 Type 2 compliant.**



**GDPR, CCPA compliant.**

### Unlock 1Password with Okta, Azure, Duo, OneLogin, JumpCloud, and more

Single sign-on (SSO) protects logins for apps that you specifically add to your SSO provider. 1Password protects virtually everything else. Unlock with SSO is built the 1Password way, with a trusted device model to maintain zero knowledge and end-to-end encryption. Decryption happens on-device and, as always, **we don't store or have access to the keys needed to decrypt your data.**

# Easy to use, easy to manage

For more than a decade, 1Password has offered a best-in-class user experience so anyone – no matter how tech-savvy they are – can protect their sensitive information. That simple, intuitive experience extends to enterprise end users and admins, eliminating the friction between security and convenience.

---

## Simple workforce security

1Password secures your workforce by making the secure thing to do the easy thing to do, from generating and autofilling strong passwords to secure sharing and collaboration.

- **Create vaults to organize your items and share them with others.**
  - Manage individual access to each vault.
  - Set default vault permissions.
  - Manage permissions for a group or a user.
  - Use collections to create a custom group of vaults.
  - Choose which apps can be used to access a vault.
- **Autofill credentials and identity information.**
- **Access 1Password on Mac, iOS, Windows, Android, Linux, and in the browser.**
- **Use Travel Mode to remove vaults from your devices when you travel.**
- **Secure item sharing.**
  - Create secure links to share copies of items with anyone.
  - Manage who your team can share items with externally.
  - Manage how long an item can be shared.
  - Manage document and item attachment sharing.
  - View item history for audit logs of sharing activity.
  - Stop sharing an item at any time.

## Scalable admin controls and visibility

Admins use 1Password to enforce stronger, integrated security policies at scale. Centralized, granular controls and intuitive dashboards make it easy to reduce risk and take action when necessary.

- **Simple account recovery.**
- **Granular vault permissions and role-based access controls.**
- **Policy management.**
  - Account password policy.
  - Modern app requirements.
  - Two-factor authentication.
  - Default session duration.
  - File storage.
  - Firewall rules.
- **Robust reporting.**
  - Unified admin dashboard.
  - Security issue reports.
  - Account activity reports.
  - Team insight reports.
  - Events API and SIEM integration.

## Don’t forget infrastructure secrets

Developer workflows are an often-overlooked aspect of secrets management. They shouldn’t be. 1Password Developer Tools streamlines and secures SSH keys, API tokens, and other infrastructure secrets throughout the entire software development life cycle.

- **1Password CLI.**
- **Shell Plugins.**
- **SSH Commit Signing.**
- **Service Accounts.**
- **CI/CD integration.**

> “Our use of 1Password is always increasing because it’s easy to access. I feel better knowing that everything is stored securely, and that if there’s a compromise we won’t suffer from an attack.”
>
> **Mike Parent**
>
> Security Engineering Manager at Drift

# Strengthen your existing security infrastructure

1Password integrates with your existing tools, including your Identity and Access Management (IAM) solution, to enhance and extend your security infrastructure.

- OIDC-based single sign-on (SSO).
- User and group provisioning via SCIM.
- Two-factor authentication.
- SIEM integration and Events API.
- Developer Tools – CI/CD integration, 1Password Connect.

| SSO and Provisioning | SIEM | Developer Tools | 2FA and Other |
|---|---|---|---|
| Microsoft | splunk> | GitHub | DUO |
| okta | elastic | GitLab | yubico |
| Google Workspace | panther | Gitpod | slack |
| onelogin by ONE IDENTITY | sumo logic | aws | ramp |
| jumpcloud | DATADOG | circleci | Brex |