1Password

1Password Enterprise Password Manager

SECURE EVERY CREDENTIAL. STRENGTHEN EVERY SIGN-IN.

Credential-based attacks are the #1 way cybercriminals breach organizations. Weak, reused, and stolen passwords expose companies to risk, compliance gaps, and operational inefficiencies.

1Password Enterprise Password Manager reduces those risks by securing every login and empowering employees to follow strong security practices. Built-in visibility, policy controls, and phishing-resistant authentication give IT and security teams the oversight they need without disrupting workflows.

More than 165,000 businesses trust 1Password to keep their teams and data secure.

Core features

CREDENTIAL MANAGEMENT

Secure every sign-in across every device.

- Autofill across desktop, mobile, and browser
- Store passwords, OTPs, credit cards, and passkeys
- Organize with private and shared vaults
- Cross-platform access on iOS, Android, Windows, macOS, and Linux
- Strengthen security hygiene with Watchtower alerts

COLLABORATION & SHARING

Collaborate securely with role-based permissions.

- Role-based vaults for teams and groups
- Set granular vault access permissions
- Share logins, SSH keys, and sensitive data
- Organize team members and manage vault access
- Securely share items with external parties

SECURITY & INTEGRATIONS

Ensure strong security and compliance.

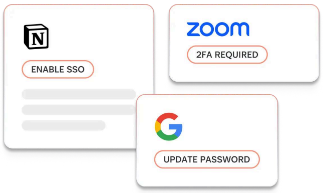
- Apply MFA, password, and sharing policies
- Audit logs for SOC2, ISO 27001, and HIPAA
- SIEM support (Datadog, Splunk, Sentinel, etc.)
- Device compliance with 1Password Device Trust integration
- IDP integration via SSO or SCIM

SECRETS MANAGEMENT TOOLS

Secure credentials for humans and machines.

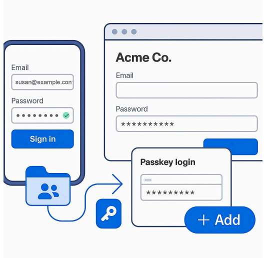
- Store and share SSH keys, API tokens, and secrets
- SDK for managing credentials used by AI agents
- Service accounts for programmatic access
- Prevent plaintext secrets in config files
- Integrate with developer tools securely

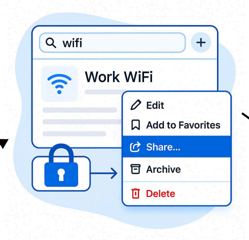
How 1Password Enterprise Password Manager works



Establish strong security compliance policies to reduce risk and meet regulatory standards. Granular vault permissions ensure employees only access what they need without slowing teams down.

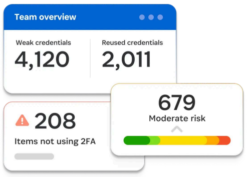
Manage credentials across every device, storing everything from passwords and passkeys to SSH keys and credit cards in fully encrypted vaults.





Collaborate securely using role-based vaults and granular permissions. Set view, edit, or manage access so everyone gets what they need and nothing they don't.

Identify risk early with real-time insights to take action before threats become incidents.



Unmatched capabilities of 1Password Enterprise Password Manager

INDUSTRY-LEADING ENCRYPTION ARCHITECTURE THAT KEEPS YOUR DATA PRIVATE.

ZERO-KNOWLEDGE ARCHITECTURE WITH DUAL-KEY ENCRYPTION

1Password uses a unique Two-Secret Key Derivation (2SKD) model that combines a user's account password with a 128-bit device-generated Secret Key. This ensures end-to-end encryption, and as a result, even if someone steals or guesses your 1Password account password, they still can't access your account.

SECURE ACCESS FOR AI AGENTS AND NON-HUMAN IDENTITIES

Secure access beyond workforce credentials—extend your access strategy to AI agents, scripts, and automated workflows. Store secrets like SSH keys, API tokens, and environment variables in encrypted vaults with fine-grained access controls. Service accounts give bots and scripts the access they need—without the risk of plaintext credentials or hardcoded secrets. You get complete visibility, auditable access, and policy-driven control over every non-human identity in your environment.

ON-DEVICE DECRYPTION, EVEN WITH SSO

Unlike other solutions that weaken encryption for convenience, 1Password keeps your data private—even when using SSO. Our Unlock with SSO feature uses a trusted device model and device-generated encryption keys to ensure decryption happens locally. Your identity provider never has access to your encryption keys, and 1Password never sees or stores your secrets—preserving our Zero-Knowledge architecture at every step.

Solutions

SHADOW IT DISCOVERY

- Discover, manage, and secure shadow IT and every SaaS application. Enforce credential policies that secure access to these applications.

PASSWORDLESS

- Get on a path to passwordless by identifying passkey-enabled services and guiding your team through the transition with easy-to-use insights and policy enforcement.

DEVICE SECURITY

- Securely access non-SSO applications with strong, unique passwords while ensuring only compliant devices can sign in—reducing the risk of compromised credentials and unauthorized access.

CREDENTIAL RISK MANAGEMENT

- Proactively reduce risks from weak, reused, or compromised credentials.

COMPLIANCE & CYBER INSURANCE

- Meet the requirements for compliance and cyber insurance. Support SOC2, ISO 27001, HIPAA, and NIST compliance with customizable policies and detailed audit trails.

AGENTIC AI SECURITY

- Provide AI agents with identity-aware, device-trusted, and secrets-managed access to critical applications, APIs, and SaaS services.

About 1Password Extended Access Management

1Password pioneered Extended Access Management, a new cybersecurity category built for the way people and AI agents work today. Our mission is to unleash productivity without compromising security. The 1Password Extended Access Management platform secures every sign-in to every app from every device, including the unmanaged ones that legacy IAM, SSO, and MDM tools can't reach. Over 165,0000 leading companies rely on 1Password to close the Access-Trust Gap: the growing risk created when unmanaged apps, devices, and AI agents access sensitive company data and resources without proper governance controls. Learn more at 1Password.com.

Get in touch with us

Ready for a demo? Visit https://1password.com/contact-sales