1Password

1Password Secrets Management Tools

In today's cloud environments, workloads (including applications and containers) rely heavily on secrets such as API keys, SSH keys, passwords, OAuth tokens, .env files, and certificates. When secrets go unmanaged, organizations become easy targets for cyberattacks that go straight to the heart of an organization's most sensitive resources. 1Password helps ensure that secrets are protected and managed.

Core features

Securely store, manage, automate, and share secrets for applications and infrastructure in 1Password's password manager.

SECURE AND CENTRALIZE SECRETS

- Centralize secret storage (passwords, passkeys, SSH keys, and API keys) in encrypted vaults
- Manage secrets across different environments with centralized visibility, including secrets syncing with AWS

INTEGRATE WITH EXISTING DEVOPS WORKFLOWS

- Increase security while maintaining employee productivity by integrating and syncing with other DevOps services, including 1Password's Command Line Interface, 1Password's CI/CD integrations, and 1Password's IDE integrations

PROVE COMPLIANCE, SIMPLIFY AUDITS

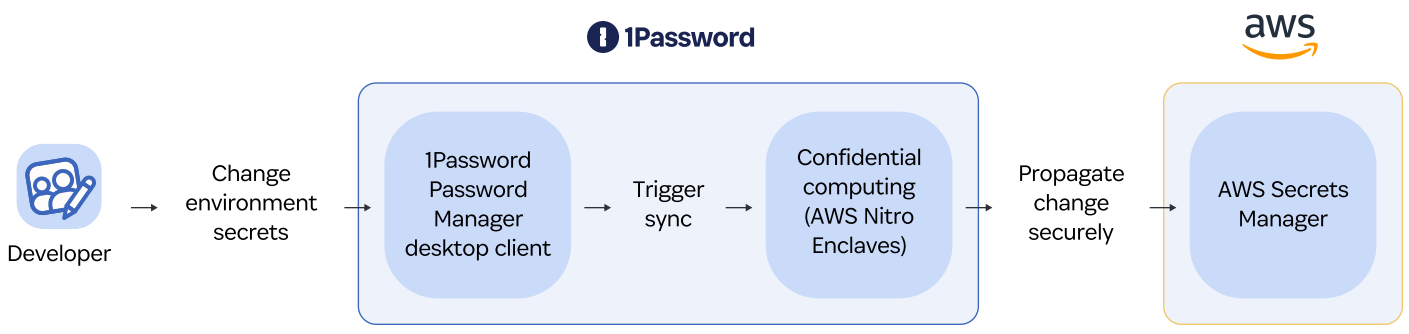
- Get full audit trails and logging to meet regulatory and compliance requirements

1Password secrets syncing integration with AWS Secrets Manager

Securely and automatically sync developer secrets and environment variables from 1Password into AWS.

- **Centralized management**: Use 1Password to manage secrets and environment variables across environments
- **Easy to use:** Simplify secrets management and reduce management overhead with automatic syncing to AWS
- **Audit-ready**: Full visibility into how secrets are created and synced

How 1Password's secrets syncing integration with AWS works



How it works

1. IT admins and developers store passwords, passkeys, SSH keys, API keys, and more in 1Password's password manager.

2. IT admins and developers authenticate and sign commits with their SSH keys stored in 1Password's password manager using the 1Password SSH agent, without having to open the 1Password desktop client. This ensures technical employees can keep productivity up while being secure.

3. IT admins and developers store secrets and environment variables inside 1Password environments, which is an easy-to-use section in the 1Password desktop client to group secrets and environment variables. IT admins and developers can then set up AWS Secrets Manager as a destination, with 1Password using confidential computing, backed by AWS Nitro Enclaves, to securely sync secrets and variables from 1Password to AWS Secrets Manager.

4. IT admins and developers customize with 1Password SDKs – production-ready, open source libraries for Typescript/ JavaScript, Python, and Go — to support full programmatic access to 1Password items including creating, reading, updating, deleting, listing, and sharing information stored in vaults.

Solutions

CREDENTIAL RISK MANAGEMENT

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

PASSWORDLESS

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

DEVICE SECURITY

- Eliminate secret sprawl by discovering unencrypted SSH keys on devices and securing them in 1Password.

AGENTIC AI SECURITY

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

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.

About 1Password

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.

For more information about 1Password Secrets Management Tools visit