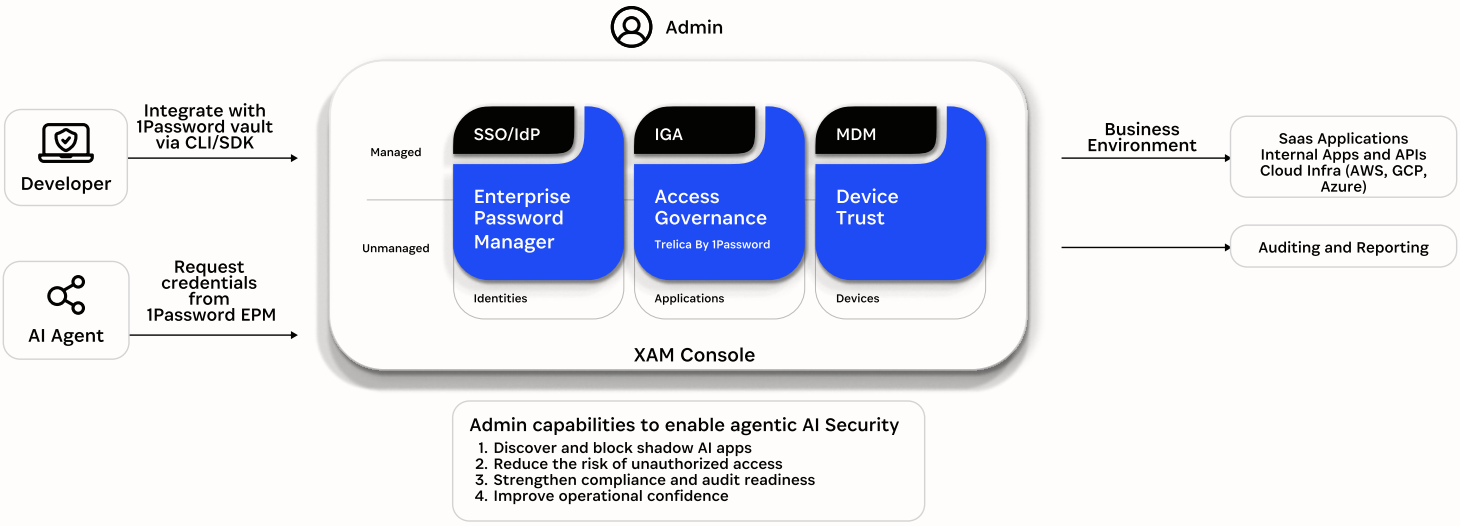
1Password

Secure access for AI agents

AI agents are transforming how work gets done. From streamlining internal workflows to scaling customer support, autonomous agents are driving unprecedented gains in productivity and efficiency. The pace of innovation is accelerating, and companies are moving fast to integrate AI into their everyday operations.

In order to accomplish complex, sophisticated tasks, AI agents need access to internal systems, tools, and data – and managing that access securely is now mission-critical. **1Password Extended Access Management** makes it easy to securely manage and govern access for AI agents, ensuring that agents have the appropriate level of access while maintaining security and human oversight.

1Password Extended Access Management enables agentic AI Security



Admin capabilities to enable agentic AI Security

1. Discover and block shadow AI apps
2. Reduce the risk of unauthorized access
3. Strengthen compliance and audit readiness
4. Improve operational confidence

Why it matters

AI agents behave like users but don't follow the same rules. Most AI agents aren't tracked, verified, or scoped for least privilege access. Developers may inadvertently hardcode secrets, agents act on static permissions, and IT has no visibility into what's happening in the background. That's a recipe for data loss, compliance failures, and unauthorized access.

These invisible risks contribute to the growing Access-Trust Gap, which refers to the security risks posed by unfederated identities, unmanaged devices, applications, and AI agents accessing company data without proper governance controls.

- 80% of unauthorized AI transactions stem from internal misuse or misconfiguration, not outside attacks. (Gartner Market Guide for AI Trust, Risk, and Security Management, February 2025)
- AI agents often use human credentials, making it challenging to audit actions or revoke access when needed.
- It's now taking 292 days on average to detect breaches involving compromised credentials. (Cost of a Data Breach Report, IBM, 2024)

By addressing agentic AI security with 1Password, you can:

- Discover shadow AI, monitor credential use, and audit their access events
- Govern and apply access policies, enforce least privilege, and rotate secrets
- Separate identities so AI agents no longer share or mimic human accounts

1Password Extended Access Management and AI agent security:

- **Enable non-persistent authentication for agentic AI:** Authenticate AI agents securely using encrypted credentials (AES-256) that are retrieved programmatically at runtime via the 1Password SDK—eliminating hardcoded secrets, static API keys, and the need to disable MFA.
- **Ensure AI agents authenticate without bypassing MFA:** Enable AI agents to use TOTP-based MFA (AES-256 encrypted) at runtime as part of authentication, eliminating the need to disable security protections for automation.
- **Prevent identity sprawl for AI agents:** Avoid over-permissioned AI agents and identity sprawl by dynamically retrieving only the credentials and private context needed for each task. Replace .env files or static secrets, with centrally managed, time-bound access.
- **Audit and report on AI agent actions:** Maintain full visibility into how AI agents authenticate, what they access, and when. Use audit logs to enforce internal policies and meet compliance standards.

How 1Password products and capabilities to enable agentic AI security

1Password	How it contributes
1Password Enterprise Password Manager	Securely stores secrets and context in AI agent dedicated vaults so AI agents access only the credentials they need. Meet compliance needs with detailed audit logs that help track and manage non-human identities.
1Password SDK	Provides developers with an SDK to programmatically create, read, update, delete, list, share, rotate, and archive 1P item fields and types for AI agents. This makes it easier to automate workflows, improve security operations, and support business-critical integrations.
1Password Service Accounts	Enables IT admins and developers to create API keys to enable their AI agents to retrieve secrets from vaults without exposing human credentials.
1Password Device Trust	Gain visibility into unauthorized AI tools found on employee devices and block access until security policies are met.

Get in touch with us. Experience 1Password Extended Access Management by requesting a demo today.