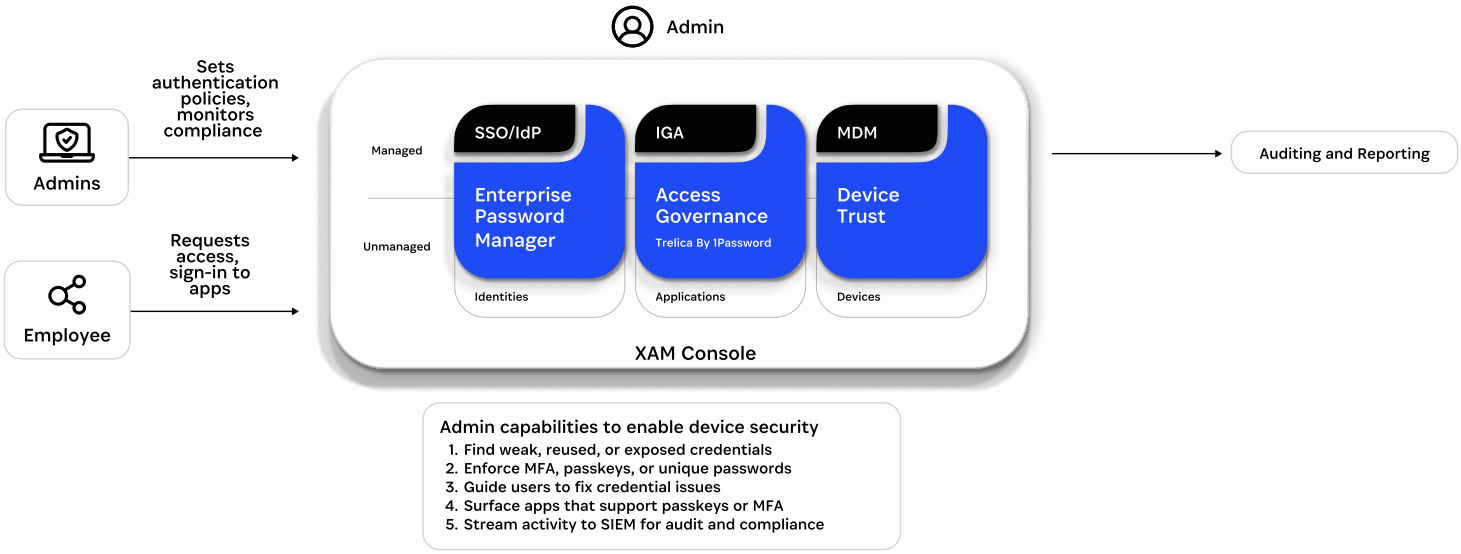
1Password

Reduce credential risk & accelerate your path to passwordless

Passwords are one of the biggest security risks in your organization. Weak, reused, or unmanaged credentials open the door to reduced IT productivity, breaches, and compliance failures. Free password managers that are browser or OS-based were not built for today's decentralized workplace and cannot support the variety of devices, browsers, and applications that employees use.

1Password Extended Access Management helps organizations reduce credential risk while accelerating their transition to passwordless authentication. You gain insights into where credentials put your organization at risk, help guide users to stronger sign-in methods like passkeys and MFA, and enforce policies that make passwordless adoption seamless and scalable.

1Password Extended Access Management enables your journey to passwordless



Why it matters

Stolen and weak credentials are a key part of the Access-Trust Gap, the security risks posed by unfederated identities, unmanaged devices, applications, and AI-powered tools accessing company data without proper governance controls.

- 61% of employees have poor password habits, like reusing or never changing passwords. (Balancing Act: Security and Productivity in the Age of AI, 1Password, April 2024)
- It takes an average of 292 days to identify and contain a breach caused by stolen credentials. (Cost of a Data Breach Report, IBM, 2024)
- 68% of all breaches involve a human element—often due to credential theft or phishing. (Verizon 2024 Data Breach Investigations Report, Verizon, May 2024)

By addressing credential risks with 1Password, you can:

- Dramatically reduce breach risk by eliminating weak and reused credentials.
- Build momentum toward passwordless sign-in without disrupting employee workflows.
- Uncover hidden risks from unmanaged apps and credentials.
- Meet compliance and audit requirements with less manual work.
- Reduce help desk tickets and IT overhead related to password resets.

1Password Extended Access Management

1Password Extended Access Management helps you eliminate password risk, accelerate passwordless adoption, and secure sign-ins across every app, device, and user.

- **Find risky credentials fast:** Automatically discover weak, reused, or exposed credentials across managed and unmanaged apps, including those outside SSO.
- **Accelerate passwordless adoption:** Guide employees to use passkeys, add MFA, or store strong, unique passwords securely, with no IT tickets required.
- **Block access from risky devices:** Ensure that weak or unsecured credentials can't be used on compromised or untrusted devices.
- **Meet Zero Trust and compliance requirements:** Tie credential health to device posture and access policies to enforce least-privilege, risk-aware authentication.
- **Gain full visibility into credential usage:** See which credential vaults are in use, where they're stored, and who is accessing them—with built-in audit trails for compliance.

How 1Password products enable passwordless

1Password	How it contributes
1Password Enterprise Password Manager	Finds weak, reused, or exposed credentials and recommends remediations.
1Password Device Trust	Enforces contextual access policies based on device compliance mandates you set.
Activity Logging with Events API	Monitors credential usage and provides detailed usage logs for auditing and compliance.
Passage Passkey Flex	Enables passwordless access for your customer-facing apps with fast, flexible integrations.

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