1Password

1PASSWORD® EXTENDED ACCESS MANAGEMENT

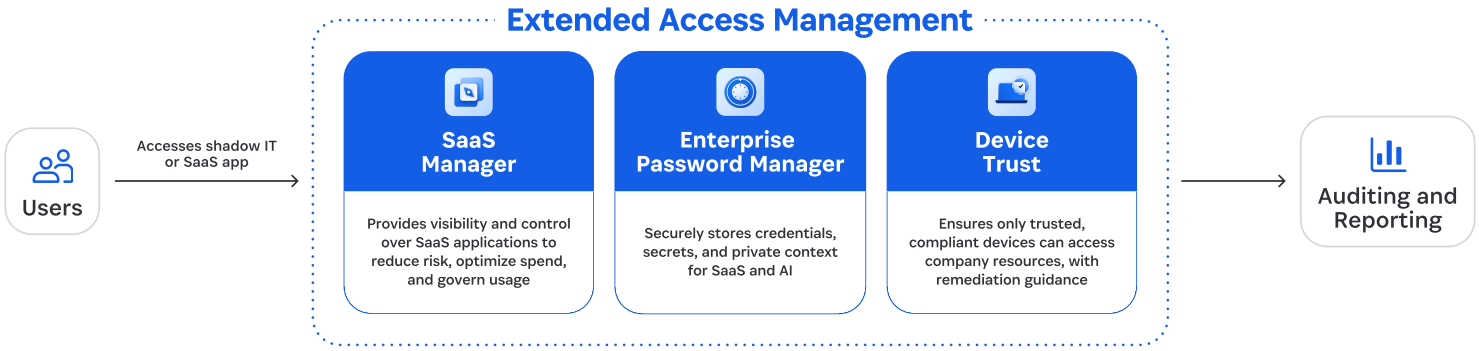
Secure every sign-in, to every app, from every device

Productivity and security are at odds. They don't have to be.

Today's companies have a sprawl problem: SaaS sprawl, device sprawl, identity sprawl. The combination of decentralized SaaS access and a more tech-savvy workforce has given employees the confidence to identify and procure the right tools for their job, rather than only using the tools and devices provided by the company.

As organizations strive to empower employees and maximize productivity, they face increased risk from the **"Access-Trust Gap"**. This gap represents the security risks posed by unfederated identities, unmanaged devices, applications, and AI-powered tools accessing company data without proper governance controls. Without coordinated and contextual visibility and safeguards across these areas, businesses face growing security and compliance risks.

Beyond IAM and MDM: Extended Access Management



Admin capabilities

1. Discover and identify SaaS apps and shadow AI
2. Enable workflows to take action on discovered applications
3. Meet compliance requirements and log SaaS access

Extended Access Management (XAM) secures the devices, applications, and AI agents that cannot be managed by existing solutions for identity and access management (IAM), single-sign on, and mobile device management (MDM). It helps organizations close the Access-Trust Gap, so they can **reduce security and compliance risks**, experience significant **productivity gains and cost savings**, and **empower employees to be proactive** about compliance and remediation.

Modern IT and Security teams need Extended Access Management

1Password Extended Access Management is a platform composed of 1Password Enterprise Password Manager, 1Password Device Trust, and 1Password SaaS Manager. 1Password Extended Access Management secures access to sensitive business data by giving companies the ability to manage:

- **Unsanctioned and unmanaged apps (shadow IT)** not secured behind single sign-on (SSO)
- **Unmanaged devices** that are unprotected by MDM
- **AI agents** with access to multiple systems and the ability to autonomously perform tasks

Why 1Password Extended Access Management?

- **Achieve comprehensive visibility**
  Combine identity, application, and device management and security into a single pane of glass.
- **Accelerate security remediation**
  Enforce identity safeguards and ensure only trusted users on secure devices can access business data.
- **Simplify access**
  Manage access for admins, end-users, and AI agents for all types of applications.

Key Capabilities of 1Password XAM

- **Secure every sign-in**
  Ensure end-user and AI agent authentication methods are secure, whether they access managed or unmanaged apps via SSO, passwords, MFA, or passkeys.
- **Mitigate Shadow IT risks**
  Discover and secure employees' access to all apps, whether company-managed or unmanaged. Gain insights into SaaS usage, optimize SaaS spend, and streamline access management workflows.
- **Ensure device health**
  Monitor device health and security in real-time to prevent access from unknown and unhealthy devices. Assist end-users in completing self-serve remediation tasks without IT's help.
- **Implement contextual access management**
  Block app access until users complete critical security tasks—e.g., addressing a Watchtower alert, updating a browser, or resolving device compliance issues.

Ready to learn more about 1Password Extended Access Management?
Visit **https://1password.com/xam/extended-access-management**

1Password