1PASSWORD® EXTENDED ACCESS MANAGEMENT

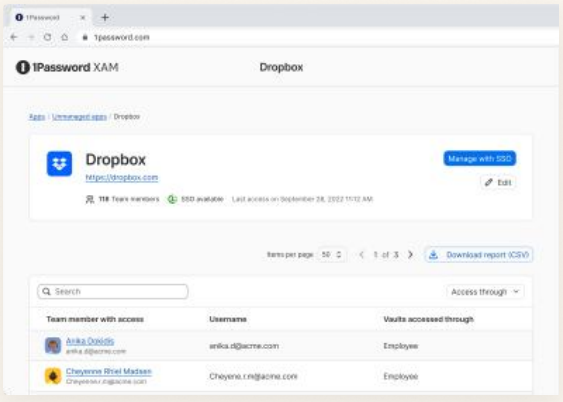
1Password

Secure every sign-in for every app on every device

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

Employees are trying to boost their productivity while embracing the flexibility of modern work – and they're turning to applications and devices not secured by (or even visible to) IT and security teams to do it. With remote work, bring-your-own device, and shadow IT becoming commonplace, businesses are stuck relying on traditional identity and access management (IAM) solutions – which were built for a way of work that no longer exists – to secure this new way of work.

Beyond IAM: Extended Access Management (XAM)



Extended Access Management is a new category of security software that fills critical gaps between IAM and mobile device management (MDM) to secure the unmanaged devices and applications that today's tools cannot see. By closing this Access Trust Gap, organizations can experience significant productivity gains and cost savings, and can empower employees to be proactive about compliance and remediation.

Modern IT and Security teams need Extended Access Management

1Password Extended Access Management is the only solution that secures access to all the places sensitive business data goes, giving companies the ability to manage:

- Unsanctioned and unmanaged apps and websites (shadow IT) not secured behind single sign-on (SSO)
- Unmanaged devices unprotected by mobile device management (MDM) or outside its scope altogether (BYOD)

Why 1Password Extended Access Management?

- **Comprehensive visibility**
  Combine visibility and management of identity, applications, and device security into a single pane of glass.
- **Accelerate security remediation**
  Enforce identity safeguards and make sure only trusted users on secure devices can gain access to business data.
- **Simplify access**
  Manage access for both admins and end users for all types of applications and devices.

Key capabilities of 1Password Extended Access Management

- **Secure every sign-in.** Ensure end user authentication methods are secure, whether they access managed or unmanaged apps through single sign-on (SSO), passwords, multi-factor authentication (MFA), or passkeys.
- **Mitigate Shadow IT risks.** Gain visibility into both managed and unsanctioned SaaS apps employees are using. Analyze application usage data across corporate and bring-your-own devices.
- **Ensure device health.** Monitor device health and security in real-time to mitigate security risks by addressing device compliance before access occurs.
- **Implement contextual access management.** Block access to apps until end-users have completed important security tasks such as addressing a Watchtower alert, updating their browser, and fixing serious device compliance issues. 1Password XAM assists end-users in accomplishing self-serve remediation tasks without ITs help.

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

1Password