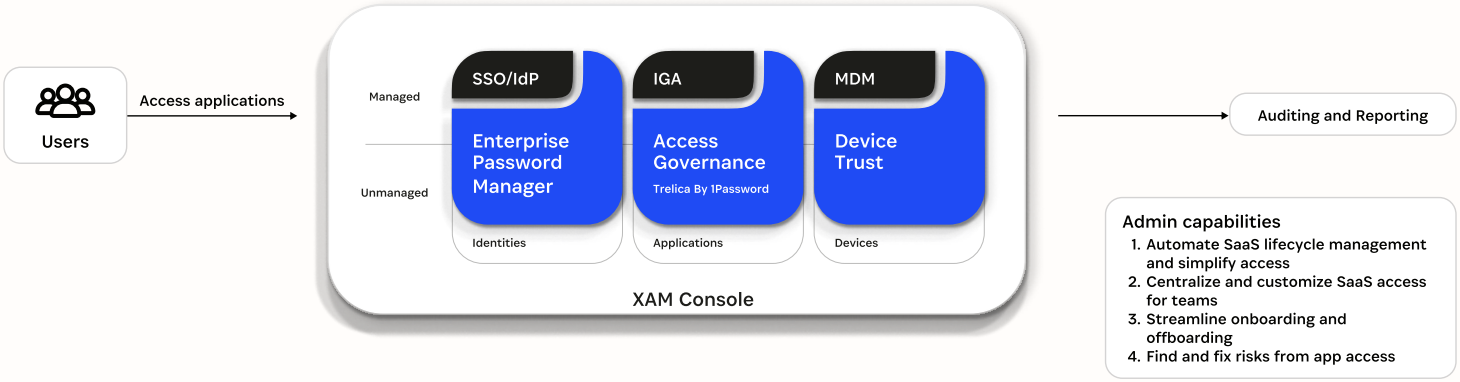
1Password

SaaS access governance

SaaS apps are everywhere – and IT isn't able to control all of them. From productivity apps to AI tools, employees are adopting tools on their own, creating massive SaaS sprawl and shadow IT. Without proper governance and lifecycle management, companies face security gaps, compliance failures, and wasted spend.

1Password Extended Access Management enables organizations to take control of their SaaS environments, mitigate access risks from onboarding and offboarding, and empower security and IT teams to optimize SaaS investments while focusing on strategic initiatives.

1Password Extended Access Management enables SaaS access governance



Why it matters

When IT and security teams can't see what apps are in use or who has access to them, everything from risk to cost spirals out of control. Shadow IT, over-permissioned users, and manual access workflows open the door to breaches, compliance gaps, and operational drag.

- 65% of all SaaS applications are not approved by IT, posing significant security and compliance challenges. (Trelica, Shadow SaaS: Why You Can't Ignore Shadow IT Risks, 2024)
- 77% of US technology decision-makers report moderate to extensive levels of technology sprawl. This sprawl can result in unsustainable costs, slower IT delivery, reduced operational resilience, and increased security risks. (Forrester, Q2 2024 Tech Pulse Survey, 2024)
- Through 2027, orgs that don't manage SaaS lifecycles will be 5x more likely to experience a breach or data loss. (Gartner, Magic Quadrant for SaaS Management Platforms, July 2024)

By solving for SaaS access governance with 1Password, you can:

- Gain visibility into every app used, whether managed, unmanaged, or AI-powered
- Eliminate risky access and over-permissioned users
- Reduce SaaS spend by uncovering unused or duplicative licenses

1Password Extended Access Management and SaaS access governance

1Password Extended Access Management helps organizations discover every app in use, manage and govern access securely, and eliminate SaaS-related blind spots.

- **Discover every SaaS app:** Get a full inventory of all apps being used, whether IT approved them or not. That includes shadow IT and shadow AI.
- **Monitor access and usage:** See who has access to what and how often they use it. Identify stale accounts, risky access, and over-permissioned users.
- **Automate onboarding and offboarding:** Provision and deprovision access automatically when employees join, move roles, or leave – reducing risk and manual work.
- **Customize access by team or role:** Give every employee a catalog of apps based on their team or responsibilities, so they get what they need without unnecessary access.
- **Block or restrict risky apps:** Prevent access to unsanctioned apps – like unapproved GenAI tools – that pose security or compliance risks.
- **Strengthen compliance posture:** Maintain access records and audit trails across all apps, supporting SOC 2, ISO 27001, and GDPR requirements.
- **Reduce SaaS spend:** Identify unused licenses, duplicated subscriptions, and shadow tools that drive up costs – then cut what's unnecessary.

How 1Password products enable SaaS access governance

1Password product	How it contributes
Trelica by 1Password	Identify shadow IT and SaaS usage by monitoring credential usage; get detailed usage logs for auditing and compliance.
1Password Device Trust	Enforce contextual access policies on SaaS apps based on the policies you set.
1Password Enterprise Password Manage	Secure credentials for every SaaS app, SSO-managed and unfederated applications.

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