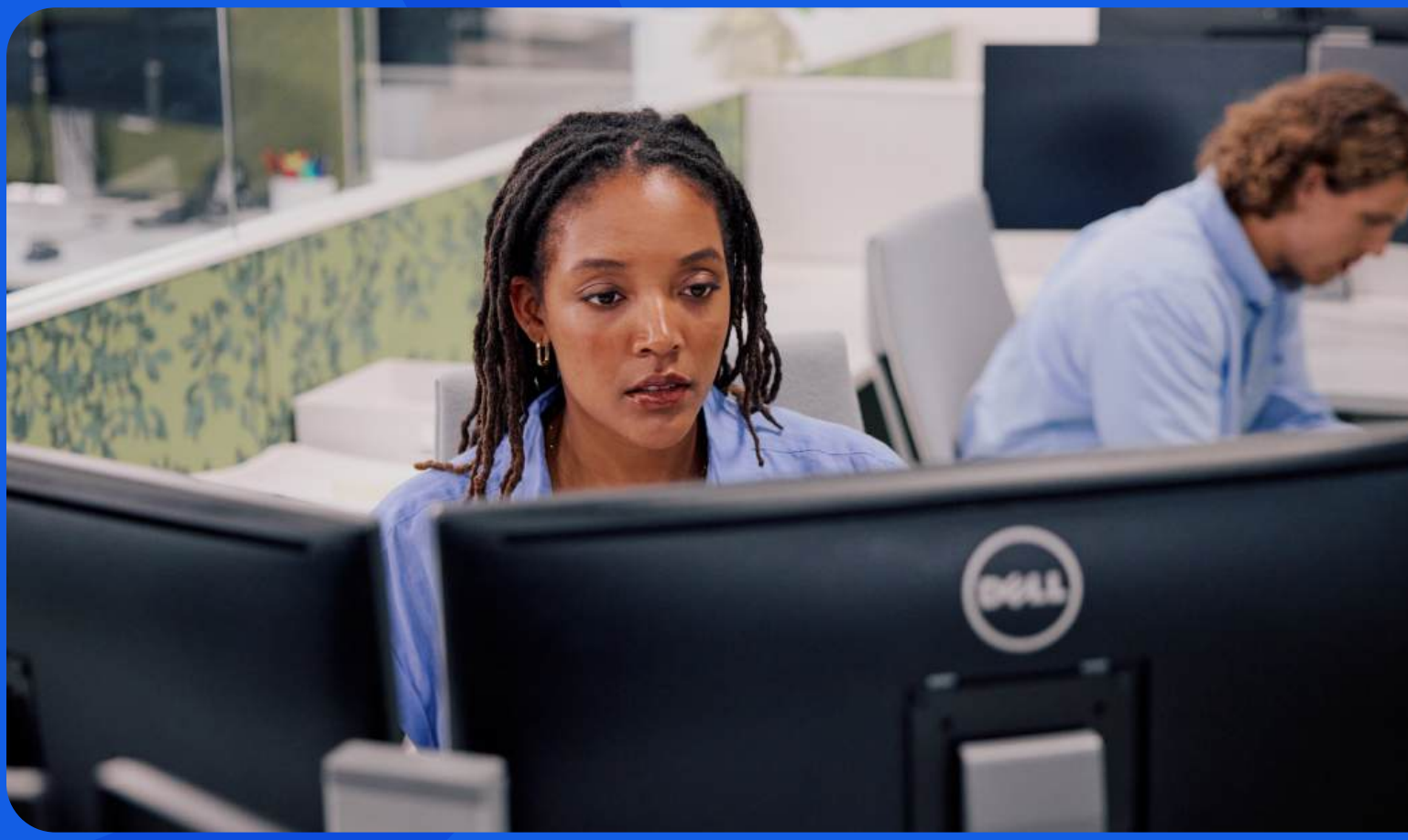
1Password

How to solve SaaS chaos with 1Password SaaS Manager



SaaS is Everywhere. Control Isn't.

Today's employees expect flexibility – flexibility to work from anywhere, from any device, and to use any tool or application that makes them most productive. They aren't waiting for IT tickets to clear or single-sign-on (SSO) integrations to go live. They're adopting their own applications often without anyone's approval. In many cases, applications are being adopted by teams or business units (think "marketing needs Figma licenses"). Either way, you end up with a proliferation of unmanaged applications.

This is software-as-a-service (SaaS) sprawl. SaaS tools have become so easy to sign up for, use, and purchase that employees are increasingly skipping traditional methods of procurement, such as going through IT, and instead acquiring their own tools. While it can help these teams move faster, it creates massive visibility gaps and risk for IT and security teams, including:

- Gaps in visibility into applications in use by the organization
- Potential loss of control of sensitive data
- Inability to fully offboard employees, meaning their access to company data continues long after they depart
- Increased cost and risk from duplicative shadow IT and unsanctioned shadow AI
- Uncontrolled proliferation of digital identities (identity sprawl) across multiple shadow applications

Today's popular IGA, IAM, and SSO tools weren't built for an earlier time, and this world of SaaS apps and AI doesn't fit the legacy model that they perfected. They can't see every application or use of AI. They can't see every login. They can't use context to empower employees to address risk without a helpdesk ticket. They can't keep up with AI agents acting independently. And that's the problem: the disconnect between the tools provided by the organization and the apps and tools people use creates risk. It's called the Access-Trust Gap.

What is the Access-Trust Gap?

The Access-Trust Gap is the outcome of an empowered and technically-savvy employee base circumventing traditional cybersecurity measures in order to increase their productivity.

As a result of the Access-Trust Gap, security risks are posed by unfederated identities, untrusted devices and applications, and AI-powered tools accessing company data without proper governance controls.

Anatomy of SaaS sprawl: how did we get here?

SaaS sprawl has been driven by the rapid, decentralized growth of SaaS applications. While it begins innocently, with employees adopting the tools they need to do their jobs, it quickly evolves into an unmanageable environment for IT and security professionals:

- 34% of employees use unsanctioned apps. (Source: 1Password, Balancing Act: Security and Productivity in the Age of AI, 2024)
- IT is typically aware of only a third of the applications used due to decentralized ownership and sourcing. Gartner estimates that as many as 25%, and vendors report that up to 50% of licenses are not regularly used. (Source: Gartner, SaaS Sprawl: How To Turn Shadow IT into Democratized Delivery, 2025)
- 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. (Source: Forrester, Q2 2024 Tech Pulse Survey, 2024)

The challenges of SaaS extend beyond visibility. Companies also expose themselves to risk across finance, compliance, and security, often without being aware of it.

- Through 2027, organizations that fail to centrally manage SaaS life cycles will remain five times more susceptible to a cyber incident or data loss due to incomplete visibility into SaaS usage and configuration. (Source: Gartner, Magic Quadrant for SaaS Management Platforms, July 2024)
- Growing financial, security and operational risks are posed by IT's inability to discover, govern and enable SaaS, automate management tasks, optimize costs and licenses, and protect data and identity. (Source: Gartner, Market Guide for SaaS Management Platforms, December 2022)
- 59% of security pros say they don't control whether employees follow software (SaaS) downloading policies. (Source: 1Password, Balancing Act: Security and Productivity in the Age of AI, 2024)

Why organizations are flying blind

When it comes to SaaS sprawl, IT and security teams face a unique challenge: how do you secure and control the applications that you do now know are being used? This is why legacy IAM and device management tools fall short of meeting the challenges posed by the Access-Trust Gap. They were built for a time when applications were fully managed and procured by IT and security.

Traditional cybersecurity tools simply fail to meet the needs of modern technology stacks:

- SSO tools only secure the applications that sit behind and integrate with the SSO.
- Traditional IAM tools are focused on securing applications that are already managed by IT and security.
- Consumer-grade password managers can only secure credentials. They don't provide the oversight or tools needed by IT and security to reduce business risk.
- Identity governance and administration tools are either focused explicitly on lifecycle management or on addressing hybrid environments. Most do not offer SaaS discovery or spend management.

So, how do you secure these SaaS apps? That's where SaaS governance comes in.

The role of SaaS governance

As organizations adopt more cloud-based tools, SaaS governance has become essential for managing risk, cost, and complexity. SaaS governance is a strategy for identifying, managing, and optimizing SaaS usage across your organization. This includes providing visibility into applications that are currently unmanaged by IT, like shadow IT and shadow AI. Critically, SaaS governance is different from traditional IGA tools in that it provides continuous SaaS discovery and automated lifecycle management.

Discover applications

- Automatically identify sanctioned and unsanctioned (shadow IT and shadow AI) applications
- Surface usage patterns, renewal dates, and spend across departments
- Evaluate risks and security posture to inform decisions

Bring applications under control

- Enforce security and compliance policies
- Automate app approval and access workflows
- Enforce OAuth hygiene by detecting and revoking risky third-party tokens
- Align access with company policies using criteria like role, department, and device health
- Flag risky permissions and remove leaver access automatically

Optimize SaaS usage and spend

- Detect and consolidate duplicate tools across teams
- Reclaim unused licenses and eliminate shelfware
- Use real-time utilization metrics to inform renewals and reduce unnecessary spend

Critically, SaaS governance is different from traditional IGA tools in that it provides continuous SaaS discovery and automated lifecycle management.

Reducing SaaS sprawl with 1Password SaaS Manager

SaaS sprawl can be managed with the right strategy and tooling. 1Password SaaS Manager empowers IT and security teams to regain oversight of sprawling SaaS environments without compromising the employee experience. With SaaS discovery, organizations can also uncover unknown SaaS and AI applications while cutting spend.

1Password SaaS Manager enables you to get control over SaaS sprawl:

- Gain complete visibility over SaaS apps
- Easy-to-use workflows
- Streamline onboarding and offboarding of app access
- Automate policies for SaaS
- Identify app usage and reduce IT spend
- Block risky applications, like unapproved GenAI
- Meet and stay compliant
- 350+ direct integrations across identity providers, HRIS, MDMs, and business applications

By bringing unmanaged applications under control and managing SaaS sprawl, you can effectively minimize the Access-Trust Gap as it relates to applications.

Next Steps

SaaS sprawl is a systemic issue. Without tools to uncover and govern the apps in use across your organization, the Access-Trust Gap and its related risks will only grow.

With 1Password SaaS Manager, IT and security teams can finally gain the visibility, control, and efficiency needed to secure modern work.

Request a Live Demo
Explore the guided 1Password SaaS Manager Demo

1Password

Trusted by over 180,000 businesses and millions of consumers, 1Password pioneered Extended Access Management, a new cybersecurity category built for the way people and AI agents work today. Our mission is to unleash productivity without compromising security. The 1Password Extended Access Management platform secures every sign-in, to every app, from every device, including the managed and unmanaged ones that legacy IAM, IGA, and MDM tools can't reach. Leading companies such as Asana, Associated Press, Aldo Group, Canva, IBM, MongoDB, MediaComm Communications, Octopus Energy, Slack, Salesforce, Stripe, Under Armour, and Wish rely on 1Password to close the Access-Trust Gap: the security risks posed by unfederated identities, unmanaged apps, devices, and AI agents accessing sensitive company data without proper governance controls.

Learn more about 1Password.