

BUYER'S GUIDE

# How to choose a SaaS management platform



## CHAPTER 1

# Introduction

---

SaaS management is how teams discover, govern, and optimize the SaaS applications employees use every day. For IT teams, a SaaS Management Platform (SMP) provides a system of record for SaaS inventory, access, usage, spend, and ownership so you can scale SaaS without scaling risk or manual work.

Most organizations already use hundreds of SaaS applications and must work to continuously manage and optimize access. However, spreadsheets, ticket queues, and periodic audits were never designed to keep up with constant SaaS change. As a result, IT teams struggle with incomplete visibility, inconsistent access control, and ongoing license waste.

This guide outlines the requirements of modern SaaS management and how to evaluate these platforms in today's reality.



# The role of SaaS management in a modern organization

---

SaaS management sits at the intersection of IT operations, security, and finance. The goal is to:

- Maintain an accurate inventory of SaaS applications
- Ensure users have the right access at the right time
- Reduce unnecessary spending
- Support audits with defensible access evidence

Unfortunately, the new reality is that shadow IT isn't a fringe behavior anymore; it's the default, and organizations can't afford to wait or look the other way when employees and business units sign up for SaaS on their own. These unmanaged applications quickly become part of how work gets done, often handling sensitive data, storing credentials, or integrating with other tools. IT is faced with a fragmented ecosystem where they're expected to manage access, control costs, and meet compliance requirements of tools they cannot consistently see or govern.

These unmanaged apps create blind spots in access control, complicate offboarding, inflate spend, and make audits harder to defend. The challenge isn't preventing this, but getting visibility and applying governance without breaking workflows. Effective SaaS management keeps teams moving while IT maintains control of access and spend.

# Why IdPs, SSOs, identity governance, or finance tools can't meet SaaS management needs

---

Most organizations already have tools that cover part of the SaaS story. But none of them were built to reconcile it into a single, continuously accurate system of record.

- **IdPs and SSO** only reflect apps that are integrated with SSO. While many vendors don't support SSO or require enterprise-tier licensing, the challenge for larger organizations is not budget or technical capability; it's scale. Even with resources and in-house expertise, the number of applications that require integration far exceeds what IT can implement, especially as new SaaS tools are adopted at an accelerating pace. The backlog of apps to integrate grows faster than teams can address it.
- **IGA** tools can enforce processes, but they typically don't solve SaaS discovery, ongoing inventory, and license management. They often depend on clean application integrations and structured entitlement models, which are hard to maintain across hundreds of fast-changing SaaS apps. They also do not inherently link usage context to decisions like deprovisioning or license right-sizing.
- **Procurement and finance systems** show what you pay for, not what's actually used or who still needs access. They can be strong sources for renewals and vendor spend, but they don't link spend to actual adoption, who is accessing them, or whether licenses need to be reclaimed when people change roles or leave.
- **Ticketing systems** document intent, not outcomes. A closed ticket does not prove that access was removed everywhere, that orphaned accounts were eliminated, or that licenses were recovered across apps outside of SSO.

“ Even with resources and in-house expertise, the number of applications that require integration far exceeds what IT can implement, especially as new SaaS tools are adopted at an accelerating pace. ”

| Existing tools                                 | Coverage and Gaps                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Identity Provider / Single Sign On (IdP / SSO) | <p><b>Good at:</b> authentication and SSO-managed apps</p> <p><b>Where it stops:</b> apps not integrated with SSO, local accounts, shared credentials, and ongoing usage context</p> <p><b>What's missing:</b> complete discovery, lifecycle control across non-SSO apps, and spend/usage correlation</p>                                |
| Identity Governance and Administration (IGA)   | <p><b>Good at:</b> formal workflows and access review processes for a subset of well-modeled apps</p> <p><b>Where it stops:</b> broad SaaS discovery, fast-changing entitlements, license usage/optimization, and long-tail app coverage</p> <p><b>What's missing:</b> continuous SaaS inventory + usage-informed decisions at scale</p> |
| Procurement and finance systems                | <p><b>Good at:</b> invoices, renewals, vendor data, and spend tracking</p> <p><b>Where it stops:</b> who actually uses the app, who should own it, whether licenses are active, and whether access was removed</p> <p><b>What's missing:</b> linkage between spend, access, and real adoption</p>                                        |
| Ticketing systems                              | <p><b>Good at:</b> documenting intent and routing requests</p> <p><b>Where it stops:</b> verification that access was actually provisioned/removed across every SaaS app</p> <p><b>What's missing:</b> outcomes, automated remediation, and audit-ready proof</p>                                                                        |

Without a dedicated SaaS management platform that correlates identity, finance, usage, and ownership signals, teams are left to manually reconcile across systems. In practice, that means:

- Many SaaS apps and shadow IT remain invisible
- Onboarding and offboarding remain manual and incomplete, especially outside of SSO
- License optimization happens too late to influence renewals
- Access reviews and audits require manual reconciliation and evidence gathering

Modern SaaS environments demand a purpose-built approach that delivers continuous inventory accuracy, lifecycle control beyond SSO, usage-informed spend governance, and audit-ready access logs.

## CHAPTER 2

# Key requirements for SaaS management platforms

---

The needs of SaaS management have evolved. As organizations adopt more SaaS, IT teams must continuously manage access, spend, and risk, not just quarterly or annually. Modern SaaS management must:

- Account for apps adopted outside of IT control
- Support frequent access requests and offboarding apps outside of SSO
- Optimize spend by removing redundant applications and unused/orphaned licenses, and improving contract renewals
- Provide ongoing visibility, not snapshots in time
- Provide access and usage reports for compliance purposes
- Automate manual IT workflows
- Fit into existing IT workflows without slowing teams down

# Overview: SaaS Management requirements

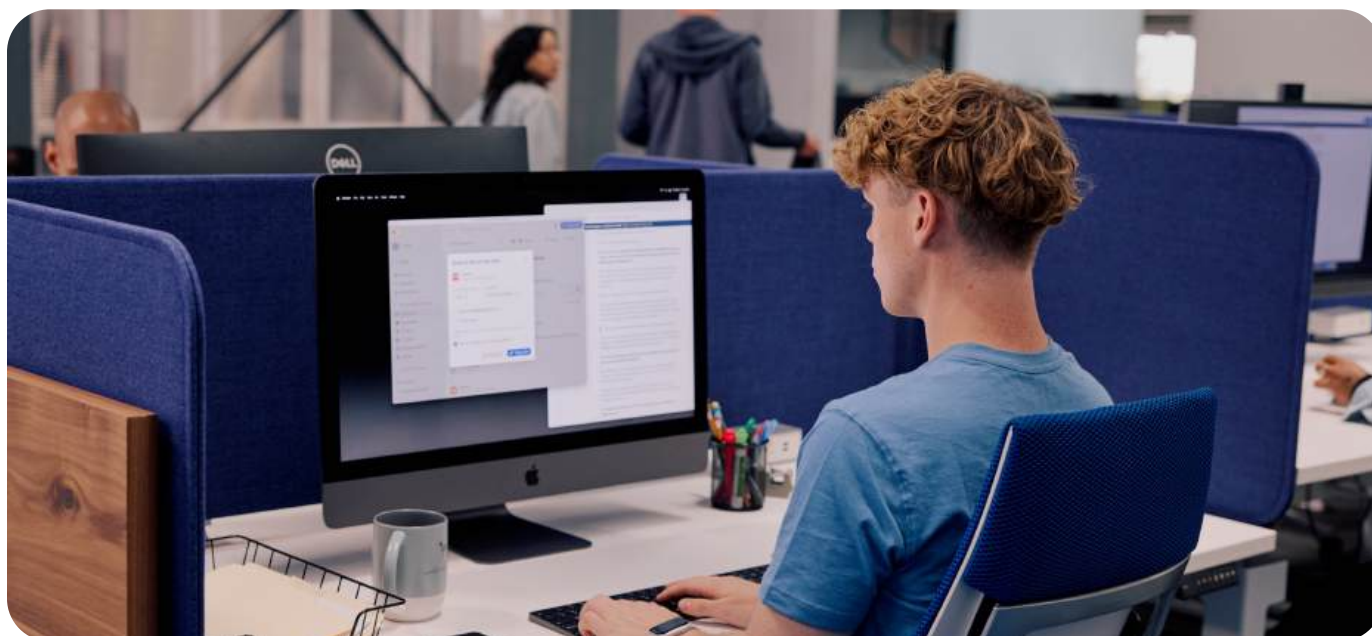
Each requirement can be broken down into specific capabilities to evaluate when evaluating solutions.

| Use case                                    | Requirement                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Continuous discovery and app library</b> | <p>Support multiple discovery sources (IdP, SSO, finance, browser extension, device agents, credential vaults) with ongoing sync and reconciliation</p> <p>Usage context and access method per app (SSO, local accounts, shared credentials) plus basic activity signals</p> <p>Clear ownership assignment for every app (with reassignment support)</p> |
| <b>Onboarding / offboarding</b>             | <p>Centralized user access visibility across SaaS, including apps not behind SSO</p> <p>Automated provisioning and deprovisioning workflows (HRIS or directory triggered) with audit logging</p> <p>Integration with identity providers (works with IdP, but doesn't rely on IdP alone)</p>                                                              |
| <b>Access requests</b>                      | <p>Centralized access request intake for SSO and non-SSO apps</p> <p>Policy-based approval workflows (role, department, risk, app owner)</p> <p>Auditable request and approval history (who, what, when)</p>                                                                                                                                             |
| <b>License utilization and optimization</b> | <p>Granular visibility into license usage with clear definitions for active versus inactive users</p> <p>Automated workflows that communicate with employees and reclaim orphaned accounts or downgrade licenses</p> <p>Actionable recommendations (for example- reclaim, downgrade), not static reports</p>                                             |
| <b>Contract management and renewals</b>     | <p>Centralized contract and renewal tracking (dates, owners, key terms)</p> <p>Usage-informed renewal decisions (adoption, redundancy, cost per active user)</p> <p>Clear ownership and cross-functional visibility for IT, finance, and procurement</p>                                                                                                 |

| Use case                      | Requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Access reviews</b>         | <p>Centralized access to data for reviews, including apps not integrated with SSO, where possible</p> <p>Structured access review workflows (assign reviewers, track completion, capture attestations)</p> <p>Exportable audit evidence (decisions, timestamps, access state at time of review)</p>                                                                                                                                                                                                                                                                                                                                                      |
| <b>Workflow orchestration</b> | <p>No-code workflows with pre-built steps, templates, and app-specific actions that handle the nuances of each system (no custom scripting)</p> <p>Communicate with employees using Slack, Teams, and email inside workflows to collect approvals, request info, and share next steps</p> <p>Fast time to value (initial insights and first automated outcomes without months of configuration)</p> <p>Trigger from real signals like HR systems, identity providers, app discovery events, or usage patterns</p> <p>Optimize SaaS spend using automation by reclaiming unused licenses, send contract renewal reminders, and discover new app usage</p> |

*Overview of the needs and requirements of SaaS management platforms.*

The following sections define each requirement and list vendor questions for evaluating SaaS management platforms.



## CHAPTER 3

# SaaS Management Platforms: evaluation criteria

---

The evaluation criteria below are designed to help IT leaders meet the operational, security, and financial requirements of a modern SaaS environment. When used in the buying process, these criteria help ensure you evaluate the most important capabilities required for an effective SaaS management platform.

## 1. Continuous SaaS discovery and inventory

Maintaining accurate visibility into SaaS usage is foundational to SaaS management. Without it, IT teams are forced to operate reactively, responding to incidents, renewals, and audits after the fact. The challenge is that SaaS is introduced into the organization through multiple pathways, often outside IT oversight. As a result, traditional discovery methods frequently leave gaps. Modern SaaS management requires continuous, multi-source discovery that reflects how SaaS is actually adopted and used.

- **Multiple discovery sources (IdP, SSO, finance, device agents, credential vaults, browser extensions):** Relying on a single discovery signal, such as SSO, inevitably results in blind spots. Not all apps are connected to identity providers, and many are adopted with corporate cards before IT is aware of them. A SaaS management platform must correlate discovery data from identity systems, financial records, and directories to build a more complete and accurate SaaS inventory.
- **Always up-to-date inventory of apps used across the organization:** Connect your IdP, SSO, finance systems, device agents, and use the SaaS management platform's browser extension to continuously uncover and manage apps.
- **App catalog with app category, security certifications, etc:** Give employees a central library of all company-approved SaaS tools. Employees can browse available apps, see which are pre-approved for their team, and request access in just a few clicks. Behind the scenes, IT defines access policies and approval chains so access requests are routed automatically.

## 2. Control access across the lifecycle

User access constantly changes as employees join, change roles, and leave. Manual lifecycle processes don't scale and often fail at the most critical moments, especially during offboarding. Effective SaaS management requires centralized, automated lifecycle control.

- **Onboarding/offboarding:** Manual processes introduce delays and inconsistencies. Automation ensures that users receive appropriate access when needed and that access is removed promptly when roles change or employment ends. This reduces both security risk and operational overhead. Critically, these workflows must include offboarding for shadow IT.
- **Integrations with HRIS, identity providers, and 350+ business applications:** Lifecycle automation must align with identity systems. Integration with identity providers allows SaaS management platforms to act on authoritative user data and reduce duplication of effort across tools.
- **Access Requests:** Manage every stage of the access request process, from the initial request through approval and provisioning, all while integrating with your existing ITSM workflows.

### 3. Optimize licenses and spend

SaaS spend grows quietly. Unused licenses, duplicate tools, and missed renewal windows add up over time. Without usage context, optimization efforts are reactive and often too late to influence renewals.

- **Reclaim unused licenses:** Knowing how many licenses you own is not the same as knowing how they're used. SaaS management platforms must surface actual usage data so IT teams can identify underutilized or unused licenses with confidence.
- **Manage contract renewals:** Renewals should never come as a surprise. Clear renewal dates and assigned owners allow IT to review usage, validate business needs, and engage stakeholders before contracts auto-renew.
- **Consolidate redundant applications:** Spot duplicate or overlapping tools and consolidate contracts to reduce costs.

### 4. Support audits and access reviews

Access reviews and audits are recurring realities for many organizations. When access data is scattered across systems, reviews become time-consuming and error-prone. SaaS management should simplify, not complicate, this process.

- **Simplify access reviews:** Ensure they are repeatable and auditable. Structured workflows help ensure reviews are completed consistently and on time, reducing last-minute audit pressure.
- **Remove access directly in access reviews:** Access reviews should do more than validate access, they should be the point of action. IT teams should remove access or licenses directly within the review workflow so risks are addressed immediately, follow-up work is eliminated, and every decision is captured in a clear, auditable trail.
- **Exportable audit evidence:** Auditors expect evidence. SaaS management platforms should provide clear, exportable records that demonstrate who had access, who reviewed it, and when decisions were made.

“ Knowing how many licenses you own is not the same as knowing how they're used. SaaS management platforms must surface actual usage data so IT teams can identify underutilized or unused licenses with confidence. ”

## 5. Alignment between IT, Security and Finance

SaaS management is a cross-functional problem. It requires shared visibility into apps, access, and spend, plus workflows that make it easy for every team to take action and stay aligned over time.

- **Broad integration coverage:** Prebuilt integrations bring identity, HR, ITSM, and finance signals together so every team is working from the same inventory and the same access context.
- **Automated workflows for IT Ops and Fin Ops:** Guided workflows with clear owners and audit history help teams complete access and spend actions consistently, without custom scripting or constant upkeep.
- **Fast time to value:** Early, credible insights build trust across teams and create momentum for shared processes like access reviews, offboarding, and budgeting decisions.



## CHAPTER 4

# Questions to ask vendors

---

Based on the defined evaluation criteria, a variety of questions are critical to answer when evaluating SaaS management platforms. Each vendor included in the evaluation process should answer these questions and provide a detailed response explaining how their platform addresses each use case.

| Criteria Category                              | Vendor Evaluation Question                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Continuous SaaS discovery and inventory</b> | <ol style="list-style-type: none"> <li>1. How do you build a complete, continuously updated inventory of all SaaS apps across our company?</li> <li>2. What sources do you use to discover SaaS acquired outside IT (for example, corporate cards, browser activity, or vaulted credentials), and what coverage should we expect?</li> <li>3. Can your platform show how each app is accessed (SSO, local accounts, shared credentials), and how do you detect each?</li> <li>4. How quickly does your inventory reflect a new app, user, or a meaningful change in usage?</li> <li>5. How do you assign and track owners, and what happens when ownership changes?</li> </ol>                                                              |
| <b>Lifecycle control and access requests</b>   | <ol style="list-style-type: none"> <li>1. How do you onboard/offboard users across SSO and non-SSO apps, and how do you verify completion?</li> <li>2. What parts of onboarding and offboarding are automated end-to-end and what is manual</li> <li>3. How do access requests flow from intake to approvals, provisioning, verification, and audit logging?</li> </ol>                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Optimize licenses and spend</b>             | <ol style="list-style-type: none"> <li>1. How do you measure active/inactive license usage, and what signals do you use?</li> <li>2. What optimization actions can the platform execute to reclaim and right-size licenses, and remove orphaned accounts? How is employee communication handled?</li> <li>3. How do you track renewal dates, contract owners, entitlements, and key terms in one place, and how is that data kept up-to-date?</li> <li>4. How do you identify redundant or overlapping tools across teams, and what evidence do you provide to support consolidation decisions?</li> <li>5. How do IT, finance, and procurement collaborate in the platform on renewal decisions using the same underlying data?</li> </ol> |
| <b>Implementation and success</b>              | <ol style="list-style-type: none"> <li>1. What integrations are out of the box (IdP, HRIS, ITSM, finance), and what is the typical implementation effort?</li> <li>2. What does measurable value can we expect in the first 30/60/90 days, and which dashboards do different stakeholders use to track that?</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                     |

| Criteria Category                            | Vendor Evaluation Question                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Support audits and access reviews            | <ol style="list-style-type: none"> <li>1. How do you run access reviews in your platform, and what is automated versus manual for reviewers and admins?</li> <li>2. What evidence can you provide to prove who had access to what, who approved it, and when, in an auditor friendly format?</li> <li>3. What is the typical time to complete an access review cycle using your platform, and what reduces that time the most?</li> <li>4. How do you handle auditor questions about completeness, accuracy, and evidence integrity?</li> <li>5. Can you include apps that are not integrated with SSO in access reviews, and how do you collect the access data for those apps?</li> </ol>                                                             |
| Alignment between IT, security,, and Finance | <ol style="list-style-type: none"> <li>1. How do you provide a shared source of truth for SaaS access and spend that IT, Security, and Finance can all trust?</li> <li>2. How do different teams get the data they need without exporting spreadsheets or reconciling multiple systems?</li> <li>3. Which existing systems do you integrate with out of the box (IdP, HRIS, ITSM, finance), and what implementation effort is typically required?</li> <li>4. How quickly can we expect to see value after deployment, and what does “value” look like in the first 30 to 90 days?</li> <li>5. Which stakeholders typically need to see measurable outcomes for long term success, and what dashboards or reporting do you provide for each?</li> </ol> |



## CHAPTER 5

# SaaS Management: How 1Password helps

---

1Password SaaS Manager is built to help IT teams discover, govern, and optimize SaaS usage without relying on manual processes. With 1Password SaaS Manager, teams can:

- **Discovery & inventory:** Maintain a continuously updated inventory and make SaaS use visible, including apps outside SSO
- **Automate employee lifecycle management:** Automate onboarding/offboarding workflows, including shadow IT
- **Optimization & renewals:** Identify unused licenses and upcoming renewals using usage data to support right-sizing and renewal decisions
- **Access reviews & audits:** Run structured access reviews using live data
- **Scale & speed:** Integrate with existing IT workflows and scale as your organization grows

By focusing on operational clarity and ease of use, 1Password SaaS Manager helps IT teams regain control of SaaS without slowing the business down.

# Conclusion

---

## 1Password

Managing SaaS has become a defining challenge for modern IT teams. As SaaS and AI adoption accelerate, access, spend, and risk change continuously. While traditional tools like identity providers, finance systems, and ticketing workflows still play an important role, they weren't designed to manage SaaS end-to-end. A purpose-built SaaS Management Platform, helps team maintain control with continuous visibility, consistent access control, and ongoing license management.

Want to see how 1Password can support your SaaS management needs? Contact your account rep or [register for a demo today](#).