

A Softchoice guidebook

A Softchoice guide for advancing your SaaS maturity

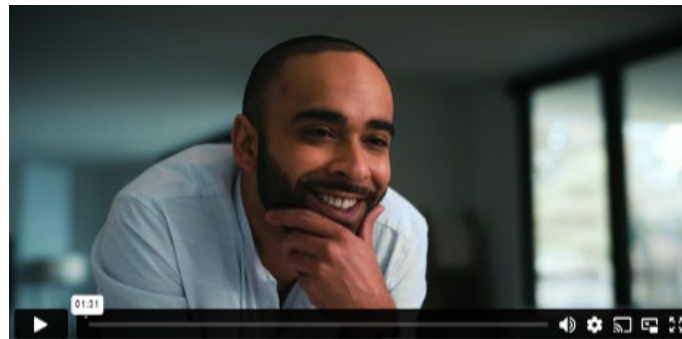


About Softchoice

Softchoice is a software-focused IT solutions provider that equips organizations to be agile and innovative, and their people to be engaged, connected, and creative at work.

We do this by delivering secure, AI-powered cloud and digital workplace solutions supported by our advanced licensing methodology and capabilities.

At the core of our business is Softchoice SAM+, our subscription-focused software asset management practice that helps reduce risks and costs while unlocking long-term value.



\$1B+

in software spend under management



30+

years of licensing and software expertise



3000+

software publishers supported



Softchoice SAM+

“With a business strategy and model rooted in licensing, software is in our DNA. Our progressive SAM+ methodology empowers you to navigate your software entitlements, save money, and free up resources. Operating as an extension of in-house IT teams, we shift manual tasks to our proficient licensing experts and empower your people to focus on the work that moves the business forward and builds careers.”

Raksha Matthias,
Director of Software Asset Management

Software as a service (SaaS) is the new normal, and it's leaving some businesses struggling to keep pace. The number of SaaS solutions keeps growing, but most IT teams aren't growing along with them.

Without the proper resources, many organizations resort to shortcuts that have long-term business impacts. Whether it's delegating tasks to non-IT teams, adopting a reactive approach to renewals, or overlooking shadow IT, these half-measures quickly spin budgets out of control and expose your organization to risks.

But here's the good news: There's a way to turn things around. A strategic asset management approach backed by expert guidance, data, and visibility is all you need.

This guide will provide you with all the information you need to help your business reach SaaS maturity.

You'll learn how to:



Eliminate manual and error-prone discovery and management processes



Identify and eliminate redundant applications



Strengthen your IT governance to avoid shadow IT



Understand the usage of accounts and apply security policies



Cut costs by rightsizing resources and optimizing your procurement strategy



Adopt a proactive and programmatic approach to renewals management



In 2024, SaaS spending is projected to reach (Gartner)

\$243.9B¹



Listen to our latest podcast on SaaS sprawl

[Podcast] [The Catalyst: Untangling SaaS sprawl: strategies for efficient and secure software management | Softchoice](#)

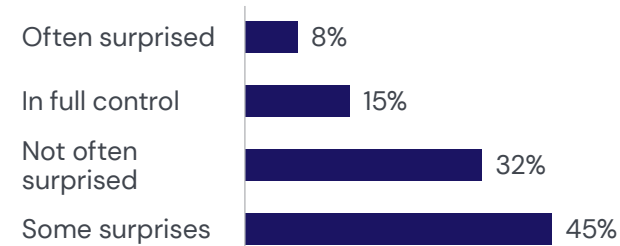
Eliminate manual and error-prone discovery and management processes

The first step to regaining control over your SaaS estate? Centralized and granular visibility.

Our data revealed that 45%² of organizations have encountered some surprises due to insufficient visibility and control over their software licenses and entitlements. These surprises—including unexpected invoices, data breaches, and compliance failures—can disrupt your business’s reputation and financial stability.

The common culprit behind these surprises? Error-prone and manual tracking processes that lead to fragmented visibility and siloed data.

Surprises arising from insufficient software visibility and control



The solution is simple: Ditch the spreadsheets and legacy tools



Manual spreadsheets

- Scatter information
- Prone to error
- Fall short in keeping data current
- Offer incomplete snapshots of the environment



Legacy tools

- Built for on-premises applications
- Lack integration capabilities with SaaS applications
- Typically operate on outdated software

3 keys to managing your SaaS estate:



Adopt a SaaS management platform or schedule periodic assessments from software experts to gain single pane of glass visibility, data-driven insights, and actionable recommendations for improvement.



Analyze existing SaaS management tools to ensure they are up-to-date, properly integrate data, offer full visibility, and deliver on intended objectives.



Encourage collaboration between cross-functional departments to eliminate silos and align on a unified approach to SaaS management.

Identify and eliminate redundant applications

Leverage insights gained from your improved SaaS visibility to optimize your environment and begin realizing cost and time efficiencies.

A crucial step in optimization is simply getting rid of redundant applications and tools.

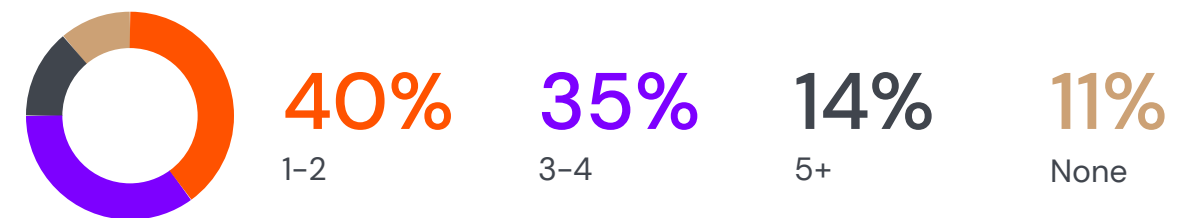
Many applications are critical for business operations and productivity. Some are not. It’s time to separate the best from the rest.

Our data shows that 40%² of organizations have 1-2 redundant software tools. This may not sound like much, but the associated costs can be significant for enterprise-grade solutions. Plus, the maintenance and updates required for each can strain resources.

3 in 5

organizations use over 50 SaaS applications³ (Auvik)

Percent of organizations with redundant software tools



A redundancy isn’t simply a duplicate application. It could be a different app with overlapping features or functionalities.

Here are some examples:

Redundancy type	Example
Like-for-like redundancy: Various departments using different applications for the same purpose.	Your marketing teams use Asana for project management, while your IT team uses Jira.
Bundle redundancy: Software bundles that have applications with overlapping functionalities.	You have multiple productivity suites (like Microsoft 365 and Google Workspace) with overlapping tools for document creation, communication, and email.
Feature redundancy: Features introduced over time that overlap with those of other tools you use.	You bought two project management tools: one for tracking tasks and the other for collaboration. However, the task-tracking tool has since added direct messaging and collaboration features.



Pinpoint and eliminate shadow IT

You can't manage what you can't see. End unauthorized—and risky—procurement by understanding and addressing user needs.

One of the top blind spots for IT teams is unapproved SaaS spend. The ease of buying SaaS apps with a credit card has inevitably increased unauthorized purchases by non-IT teams.

Here's a common example of shadow IT: An employee, frustrated by the limitations of the organization's internal messaging platform, installs an unauthorized application to communicate with clients. She's just looking for a way to solve business problems but ends up unwittingly increasing risk and overhead.

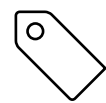
Employee is frustrated:

Marie is frustrated by the file-sharing capabilities of the organization's internal messaging platform.



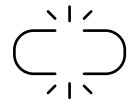
of IT professionals have limited visibility into shadow IT adoption³ (Auvik)

So, how does this impact your business?



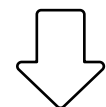
Increased costs and renewal complexity:

Different departments may be purchasing and paying for the same applications through separate contracts.



Fragmented and siloed data:

Integrating data across redundant applications often calls for costly middleware and custom solutions.



Reduced productivity:

Employees need to navigate between various platforms and be trained in multiple applications, taking valuable time away from core tasks.

3 best practices for avoiding redundancies:

1

Establish a complete inventory of your organization's software assets to assess and classify deployed applications and tools.

2

Standardize and consolidate your SaaS application stack by bundling licenses with similar functionalities under a single product suite or vendor.

3

Conduct a regular analysis to identify usage patterns and pinpoint underutilized or redundant licenses.

Here's a breakdown of the potential business impacts caused by unsanctioned SaaS products:



Cost

Without central oversight, organizations might face hefty expenses to address the risks posed by unauthorized software.



Risk

Non-IT teams often don't have the skills needed to properly configure, deploy, and secure applications.



Complexity

Different departments using disparate systems and tools complicates IT management and increases operational overhead.



Understand the usage of accounts and apply security policies

It's not enough to simply procure and deploy SaaS products. Monitoring their usage and security is vital.

To safeguard critical business data, you must analyze accounts used within your organization to identify potential attack surfaces and entry points across applications. Take an inventory of accounts, then examine shared and personal account usage, as they can both expose your organization to unnecessary risk.

96%

of employees said they are dissatisfied with the tools provided to them to manage work⁴ (Slingshot)

Dissatisfied employees are the primary reason shadow IT is on the rise.

Simply blocking shadow IT doesn't address the core issue, which is that employees either lack clarity in the capabilities and functionality of approved SaaS products, or that those products aren't meeting the demands of their jobs. The key to solving this problem lies in understanding user needs and involving them in the decision-making process.

4 steps to eradicate shadow IT:

1. Empower employees to use sanctioned tools by identifying needs within each business unit and researching tools that will do the job for everyone.
2. Adopt a proactive approach to monitoring the network for signs of unauthorized software usage.
3. Establish a central procurement team and implement approval workflows.
4. Set up a regular feedback system to understand how employees use tools and identify any perceived gaps to avoid unnecessary spending and poor user adoption.



Shared accounts

- Introduce new attack vectors for cybersecurity actors
- Make it harder to track down exposed individuals
- Increase difficulty off-boarding employees
- Pose a greater risk of violating vendor's terms of services



Personal accounts

- Increase risk of data breaches as information can be synced and saved
- Lead to loss of visibility into how organization data is used by the application
- Disrupt access to critical applications and data if the individual is unavailable

Another key factor that increases vulnerability? The absence of single sign-on (SSO). The numbers are hard to ignore.

123456

Most common password⁵

87

Average number of passwords per person in the workplace⁶

\$4.45M

Global average cost of a data breach⁷



Cut costs by rightsizing resources and optimizing your procurement strategy

Achieve the full value of your SaaS products by regularly monitoring usage against entitlements and procuring software through marketplaces.

The flexibility of SaaS licenses is a double-edged sword: It can lead to big savings or quickly spiral budgets out of control. Ensuring favorable outcomes is dependent on you making smart, informed decisions.

Our data shows 55%² of organizations estimate that only 50–75% of their software entitlements are being used. That means up to half of their licenses are shelfware—paid for but not benefiting the business.

58%

of IT professionals said they either have limited or zero visibility of SSO usage in SaaS applications³ (Auvik)

Employees facing the burden of managing dozens of passwords often resort to reusing them, increasing the risk of data breaches and cyberthreats.

That’s where SSO can help. It eliminates the need for individual passwords and allows users to access all their applications with just one set of credentials. SSO doesn’t just simplify user experiences; it plays a critical role in streamlining user access management, ensuring compliance with vendor terms, securing sensitive information, and effectively off-boarding employees.

3 rules for managing accounts:

1. Enforce policies that prevent employees from accessing applications once they leave the organization, using personal logins for critical business resources, and saving passwords using browser methods.
2. Establish monitoring, reporting, and alerting processes for shared accounts.
3. Conduct regular trainings that help employees understand the risks that shared and personal accounts pose to the organization.

The industry agrees that SaaS overspend is rampant.

~20%

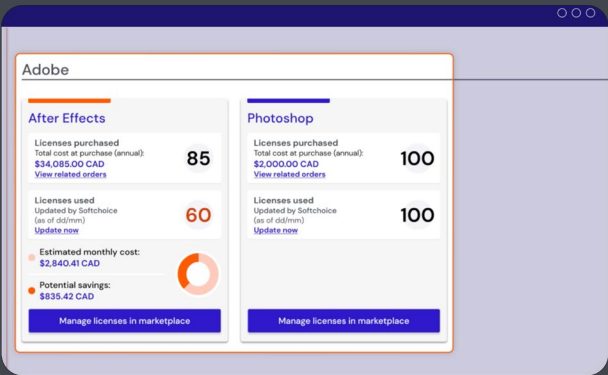
Even advanced ITAM practitioners self-estimate ~20% wasted spend on SaaS software⁸ (Flexera)

\$135,000

The average company wastes more than \$135,000 in unused licenses⁹ (BetterCloud)

You may be surprised by your budget surplus once you identify wasted SaaS spend. So, how do you capture those savings?

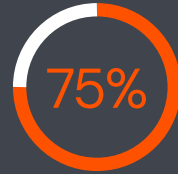
The key is regularly assessing your actual usage and comparing it to your entitlements to uncover rightsizing opportunities.



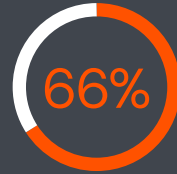
Check out the [Softchoice SAM+ Hub](#), where you can see a snapshot of licenses used vs purchased and calculate the possible savings of rightsizing usage at the product level within seconds— all at zero cost.

Another way to drive savings is optimizing your procurement strategy with cloud marketplaces

Here's why businesses are turning to marketplaces and how you can benefit: According to Forrester's 2022 Total Economic Impact Study, AWS Marketplace customers saw on average:



Reduction in onboarding effort for new vendors



Time saved due to procurement efficiencies



Reduction in licensing costs

Tailor contracts and cut costs: Use credits and funding from cloud providers to reduce purchase price and customize payments to align with budget cycles

Streamline procurement: Minimize the number of purchase order requests and simplify procurement and billing.

Draw down on cloud commits: Retire cloud consumption commitments with budgeted spend using marketplace transactions

\$85B

by 2028, enterprise software sales via hyperscaler cloud marketplaces are expected to hit \$85 billion by 2028¹⁰ (Canalys)

Pro tips for maintaining a cost-efficient SaaS stack:

- Use self-serve subscription software management tools to quickly track usage against entitlements and right-size your subscriptions.
- Reclaim unused licenses and downgrade users who don't need access to premium features.
- Regularly negotiate with publishers to secure better pricing aligned with actual usage and take advantage of available discounts and offers.
- Review historical usage patterns for better forecasting when considering volume license agreements.



Adopt a proactive and programmatic approach to renewals management

An ad-hoc approach to managing SaaS renewals is a surefire way to overpay and break budgets.

Juggling hundreds of renewals annually—each with unique pricing, terms, and licensing models—can quickly become cumbersome. But neglecting them leaves you with unnecessary procurement, lost negotiation opportunities, and missed cost savings.

Reflect on your SaaS renewal process. You're likely spending countless hours and over 50% of your SaaS budget on renewals.

How many SaaS apps do you renew each year?

What percentage of your SaaS budget is allocated towards renewals?

How long does it take to complete each SaaS renewal?

Getting the renewals process right is critical and means steering clear of these common pitfalls:

Limited visibility: Without a full view of your subscriptions and current usage, you'll be left with purchasing licenses and features you don't need.

Poor budget planning: The absence of a carefully planned budget backed by accurate forecasting and contingency plans for unexpected changes quickly spirals costs out of control.

Unfavorable negotiations: An inadequate strategy or understanding of various pricing structures and discounts can result in unfavorable terms and overpaying for your SaaS products.

Missed renewals: Ineffective and decentralized renewal tracking methods increase the risks of overlooked renewals, leading to lock-ins, service interruptions, and missed opportunities to create business value.

Compliance issues: Mismanaged software inventories and non-compliance with licensing agreements lead to hefty fines that prevent business growth.

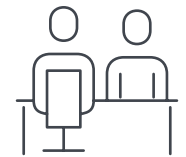


Conclusion

Don't be daunted by SaaS management. With a strategic and proactive approach, you'll reduce complexity and effectively use your SaaS solutions to advance business priorities.

Getting the full value of your SaaS investments isn't always easy, but you don't have to do it alone. We're here to help with Softchoice SAM+, our subscription-focused software asset management solution.

Our comprehensive service portfolio is built to support you at every stage of the SaaS journey. Whether you need help assessing your current SaaS stack, creating action plans for improvement, or looking for long-term deployment and management support, we'll meet you where you are.



Book a free consultation with a SAM Specialist.

Renewal preparation and negotiation tips:



Establish a renewal calendar and checklist 3-6 months in advance.



Evaluate the total cost of ownership and consider discounts offered through multi-year agreements.



Compare alternative software publishers, including differences in terms, pricing structures, and features.



Negotiate favorable terms based on your actual usage and prevent price hikes on future renewals.



Align the expiration dates of multiple software licenses so that they fall on the same date for buying power.

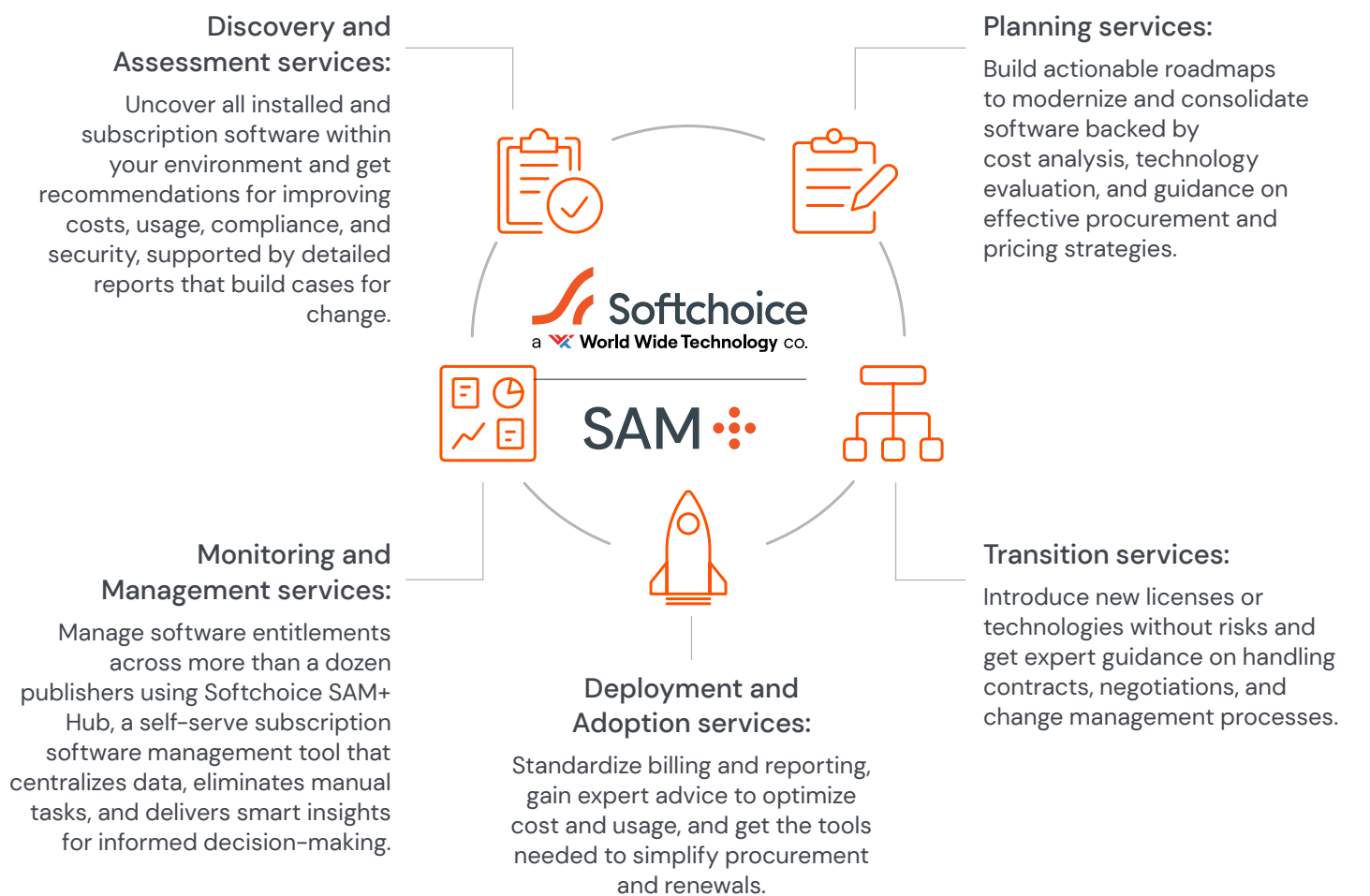


Schedule expert-led quarterly reviews covering renewals, compliance, usage, and key insights, including end-of-support dates, publisher changes, and new benefit programs.

Sample renewal checklist

60 - 120 days

- Identify upcoming renewals and contract end dates
- Analyze usage and assess if products are meeting business needs
- Evaluate costs and plan your budgets
- Develop your negotiation and discount strategy





Footnotes

1. Gartner: Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach \$679 Billion in 2024
2. 2023 Softchoice-led campaign that surveyed 374 organizations
3. Auvik IT Trends 2024: industry report
4. Slingshot: Managing Work in 2023
5. NordPass: Top 200 Most Common Passwords 2023
6. NordPass: 2024 NordPass Password Survey
7. IBM: 2023 Cost of a Data Breach
8. Flexera: 2024 State of ITAM Report
9. BetterCloud: 2024 State of SaaS Ops
10. Canlys: Now and next for hyperscaler marketplaces 2024



SAM

