WHITE PAPER

REINING IN SAAS SPRAWL TO REDUCE COST AND MINIMIZE RISK

Flexera

Inform IT. Transform IT.™

Reining in SaaS Sprawl to Reduce Cost and Minimize Risk

Summary

Countless thousands of SaaS apps are readily available to everyone in a company across departments and business units. This can result in wasted spend as well as security and compliance risks. Manual app management methods can't keep SaaS sprawl under control. Automation is the answer.

Déjà vu all over again

Iconic New York Yankees catcher Yogi Berra, known for his amusing yogi-isms, once remarked, "It's like déjà vu all over again." His often-repeated phrase aptly describes what's happening today in information technology.

Not long ago, virtual servers burst onto the scene. They were so easy to access and began popping up all over the enterprise. Before long, IT struggled to rein in server sprawl. Manual management methods—such as tracking thousands of servers on a spreadsheet—came up short. Ultimately, server sprawl was stopped in its tracks by automated server management.

IT professionals are confronting a similar sprawl problem today with software as a service (SaaS). Thousands of SaaS apps are readily available. Individual employees, departments and business units can buy them with a corporate credit card or submit the charges on an expense report. A large percentage of these purchases happen outside the purview of central IT, a phenomenon often referred to as shadow IT. In fact, the Flexera 2020 State of Tech Spend Report indicates business units control more than one-quarter of IT spend—much of it on SaaS.

IT departments are now scrambling to bring SaaS sprawl under control. Not doing so could result in hundreds of thousands of dollars in wasted IT spend. What's worse, shadow SaaS apps can introduce security and compliance risks. Manual app management processes can't get SaaS sprawl under control.

So once again, automation is the answer. And Flexera, a recognized industry leader in software asset and cloud management, comes through with Flexera SaaS Manager. This industry-leading solution brings order to SaaS chaos, keeping costs in check and minimizing business risk.

SaaS: a double-edged sword

There's no doubt organizations are flocking to SaaS. Gartner predicts SaaS apps will account for 45 percent of overall software spend by 2021.[1] Gartner also predicts SaaS revenue to grow to more than $113 billion by 2021.[2] Like all disruptive technologies, SaaS has pluses and minuses.

The positive edge

SaaS apps are quick and easy to implement because there's no hardware to procure, install and maintain. The subscription model makes them easy to budget for and purchase. There are no upfront capital expenditures. And there are no management headaches because the vendor maintains the infrastructure and takes care of software updates and patches. Consequently, SaaS eliminates spending on implementation, management and maintenance and allows the IT staff to focus on innovation and value creation.

SaaS apps also give department and business unit managers greater agility in adapting to rapidly changing market demands. SaaS apps also enable them to get the software that most closely matches their specific needs.

The negative edge

The many benefits of SaaS are not without disadvantages. In too many organizations, there are hundreds of SaaS apps running outside central IT's visibility and governance framework. The actual number of these shadow SaaS apps is significantly higher than most organizations realize. A study by Symantec[3] found that most chief information officers (CIOs) believe their companies use only 30 to 40 SaaS apps. The average, however, is actually 928.

The implications for IT spend, security and governance are serious.

[1] *Forecast Analysis Public Cloud Services, Worldwide, 2Q18 update*
[2] *Forecast Analysis Public Cloud Services, Worldwide, 4Q17 update*
[3] *Symantec Internet Security Threat Report, Volume 22*

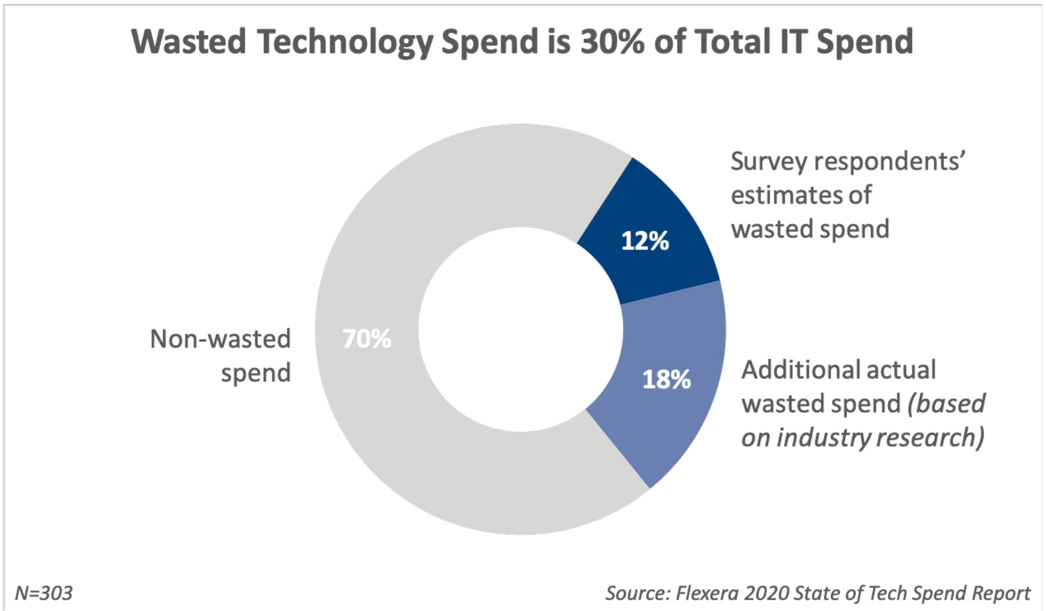


Figure 1. Wasted technology spend

IT spend

Because many SaaS apps are invisible to central IT, the IT staff can't get a handle on what the organization is spending on them, let alone optimize that spend. Lack of visibility into usage means IT can't answer key questions about SaaS apps. Who uses them? How often? Which features are being used? Without these answers, the organization may be overbuying licenses and paying for unused features.

Without visibility into license terms and conditions related to usage, the organization is exposed to risk—for example, the risk of financial penalties at audit true-up time due to underbuying of licenses and features. Additionally, lack of visibility into subscription lifecycles means apps no longer used may be automatically renewing.

Furthermore, employees may purchase unnecessary SaaS licenses or purchase licenses at higher prices than available under vendor enterprise contracts. For example, an employee may purchase a one-off license for an app not knowing the app falls under a vendor enterprise contract. Or an employee may purchase an app not knowing the organization has an app with similar functionality that is under a vendor enterprise contract.

All this adds up to wasted IT spend. As Figure 1 shows, respondents to the State of Tech Spend survey estimate their organizations waste about 12 percent of total IT spend. Research by Flexera and other industry experts, however, puts that amount at 30 percent, and perhaps higher. Considering the millions organizations spend on IT, waste is a huge cost and presents a major opportunity for savings.

Security risk

Perhaps even more alarming, lack of visibility introduces security risks. SaaS apps may include unsanctioned software the security team doesn't know about and has not vetted. Unsanctioned software may introduce software vulnerabilities that open doors to hackers and may expose proprietary data to unauthorized access. In addition, lack of visibility into who is using SaaS apps may result in employees retaining access to sensitive apps and data after they leave the organization.

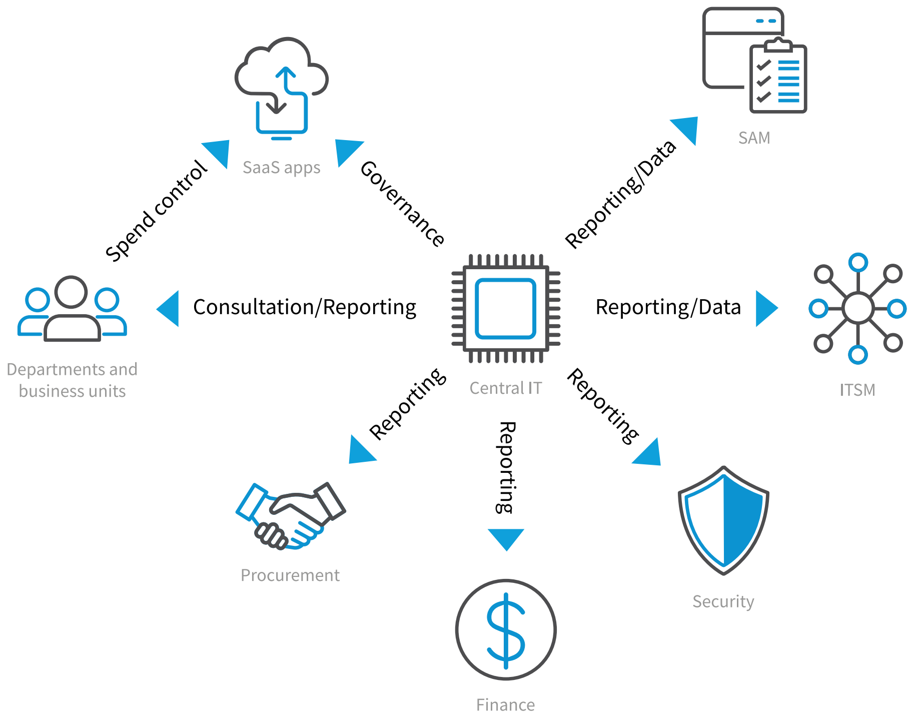


Figure 2. Collaboration among all stakeholders

Lack of proper governance

Because many SaaS apps are outside the IT governance framework, IT cannot ensure that SaaS investments are supporting the organization's business objectives. Consequently, the organization is probably not getting maximum value from its SaaS investments. Moreover, without proper governance, IT can't mitigate the risk these apps introduce.

Collaboration is key

SaaS apps must be brought under the IT governance umbrella, considering the potentially negative impact on cost, security and governance. This doesn't mean IT must wrestle control of IT spend away from departments, functional areas and business units. Instead, IT should pursue a strategy based on cooperation and collaboration with all stakeholders as illustrated in Figure 2.

The business units maintain budgetary control of their SaaS spend, so they can choose the apps that align with their unique needs. Central IT brings the apps into the organization's governance framework and provides the departments and business units with consultation and reporting. Central IT also provides other stakeholders with appropriate reports and data.

Collaboration with departments and business units

To gain cooperation, IT must position itself as a consultant and trusted partner. This can be done by demonstrating to the departments and business units that bringing the SaaS apps into the IT governance framework delivers significant benefits not only to them, but also to the enterprise.

Lower cost

IT can help departments and business units identify and eliminate waste. For example, IT can help better align cost with usage and eliminate automatic renewal of subscriptions for apps no longer used.

With greater visibility into contracts, pricing models, license implications and renewal specifics, IT can better manage vendor contracts. For example, IT can incorporate many independently acquired SaaS apps into enterprise vendor contracts for higher discounts.

A department or business unit may be running several apps with overlapping functionality resulting in portfolio creep. IT can help reduce these redundancies by working with departments and business units to standardize on a smaller number of apps that deliver the needed functionality.

Lower risk

IT can uncover unsanctioned apps that jeopardize security or compliance with industry standards or government regulations. They can work with departments and business units to replace unsanctioned apps with sanctioned ones that have equal or superior functionality.

IT can also ensure compliance with license terms and conditions to avoid financial penalties. In addition, future requirements can be predicted more accurately based on historical usage data to ensure that money is available when needed.

Collaboration with security

The security team also needs to be engaged by IT. Most organizations are aware of the need for strong security to help offset risk. Respondents in the State of Tech Spend survey cite cybersecurity as one of their organizations' top three priorities. Consequently, many organizations are increasing spend on security.

SaaS management must be included in the organization's security strategy. As with the departments and business units, IT must persuade the security team to collaborate by citing the benefits. For example, IT can help lower security risk by making the security team aware of risky SaaS apps and working with the team to either mitigate the risk or remove the offending apps from the software portfolio.

It's also advisable to include identity management and access management in the security strategy. For example, when an employee leaves the organization, IT can use the employee's identity information to determine the SaaS apps the employee accessed and immediately terminate that access.

Collaboration with finance and procurement

IT can provide the financial team with SaaS spend information to give the team a more accurate picture of enterprise IT spend. Plus, IT can provide SaaS usage information to the procurement team so they're positioned to negotiate favorable contracts with vendors.

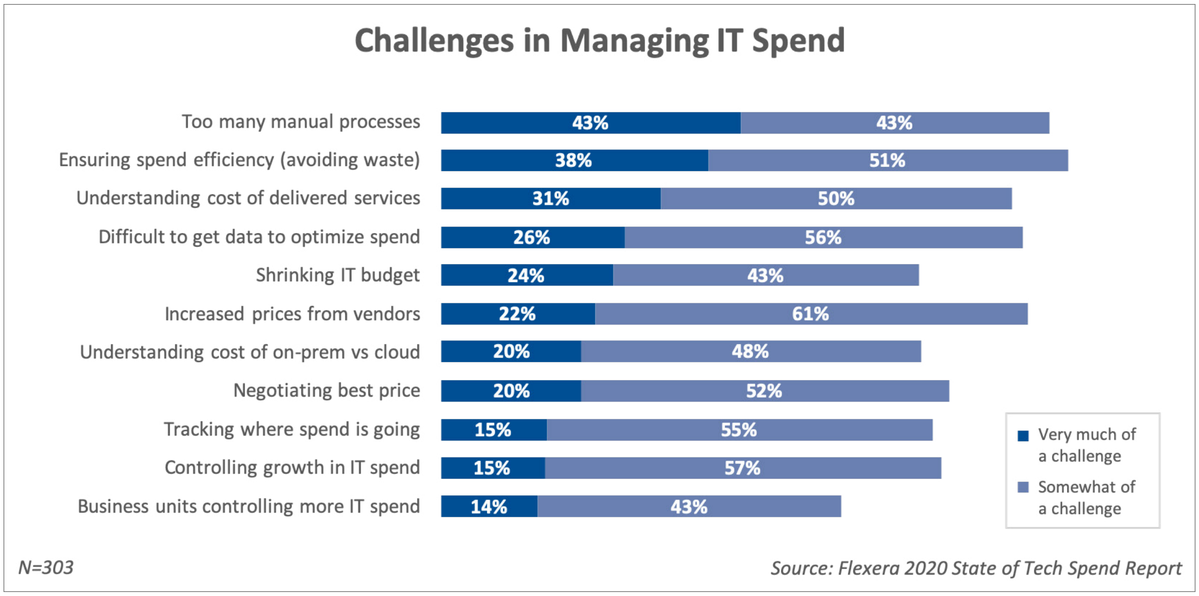
Collaboration with SAM and ITSM

Within IT, the SaaS management team can provide reports and data to the software asset management (SAM) and IT service management (ITSM) teams so they can more efficiently and effectively manage software assets.

SaaS management technology is essential

Gaining broad and deep visibility of SaaS apps across the organization and then leveraging that visibility to effectively govern the apps is not easy. There are typically hundreds of different apps and thousands of app users. Many apps are highly complex and involve multiple services from different vendors. Furthermore, the SaaS environment is highly dynamic.

Many organizations are using manual processes to track applications. This approach is impractical in the world of SaaS. The problem is that different departments and business units may be managing their SaaS apps without oversight from IT. Consequently, app data is fragmented and scattered across the organization and is often inaccurate and incomplete.



Source: Flexera 2020 State of Tech Spend Report

Figure 3. Top challenges in managing IT spend

What's more, because IT has to spend an inordinate amount of time manually gathering the data and rationalizing it across business units and functional areas, much of the information may be outdated by the time data collection is completed.

As Figure 3 shows, State of Tech Spend survey respondents indicated the most vexing spend management challenge is too many manual processes.

To tackle the challenge, IT needs a SaaS management technology solution that automates much of the process of monitoring and managing SaaS apps. That solution must meet a number of stringent requirements.

Gather detailed SaaS app data

The SaaS management technology solution must discover and identify all SaaS apps deployed across the enterprise. That's difficult because thousands of different SaaS apps are available.

For each app, IT must aggregate detailed information:

- How much the app costs
- Who's using it, how often and which features
- User details such as role, organization and location
- Up-to-date vendor contract information, including pricing model (is it based on feature consumption?), license information (what are the usage entitlements?) and renewal information (is renewal automatic and what is the renewal lifecycle?)

Integrate with other enterprise systems

Gathering the needed information requires the SaaS management solution integrate with other enterprise systems. For example, integration with financial systems such as NetSuite and expense management systems such as Concur provides information on items that employees charge to corporate and personal credit cards or submit on expense reports. This can uncover which SaaS apps were purchased, by whom and at what cost.

Integration with HR systems such as Workday and identity provider systems such as Okta provides information on users, including department, job title, location and more. IT can use this information when they need to contact a specific user, department or business unit.

Facilitate information sharing

To foster collaboration, the solution must facilitate sharing of information with stakeholders by generating meaningful reports and exporting relevant data. This enables IT to:

- Disseminate information to the departments and business units so they can make better informed decisions about IT spend
- Provide information to security teams so they have a complete picture of the threat environment
- Report cost and historical usage data to financial teams so they can more accurately forecast future requirements and budget accordingly
- Provide information to procurement teams for better-informed negotiations with SaaS vendors
- Deliver SaaS app information to SAM and ITSM teams—for example, exporting SaaS app data to the organization's configuration management database (CMDB) to provide a single source of truth for all IT assets

Partner with a leader

With the rapid proliferation of SaaS apps and their implications on spend and security, IT needs to partner with Flexera, an industry leader, to govern them effectively. Flexera was named by Gartner as a 2019 Magic Quadrant Leader in both the Software Asset Management Tools and Cloud Management Platforms categories. It's the only company in the top tier of both categories.

Flexera SaaS Manager is a leading solution for managing SaaS applications and it meets the requirements just discussed. This advanced solution delivers industry-leading features:

- Discovers more than 32,000 different SaaS applications
- Maintains detailed, up-to-date information on more than 6,200 SaaS vendor licenses and contracts
- Integrates with hundreds of systems containing data on SaaS app costs, SaaS app usage and user identities
- Analyzes and presents information via displays and reports that are meaningful to IT, departments and business units, procurement and finance

Flexera SaaS Manager can help you get your arms around SaaS and deliver benefits to all parts of the organization.

Increase security

Flexera SaaS Manager helps you strengthen security by:

- Bringing unsanctioned SaaS apps to light and reporting them to the security team
- Identifying owners of unsanctioned apps and working with them to replace these apps with sanctioned apps that have similar functionality
- Identifying apps that were used by employees who have left the organization and terminating their access

Manage SaaS vendors

Flexera SaaS Manager helps you optimize SaaS vendor management by:

- Enabling the procurement team to participate in vendor meetings with full knowledge of vendor contracts
- Leveraging price model and usage information to ensure the enterprise takes full advantage of every license and subscription
- Renewing, modifying or cancelling subscriptions on time so people have the apps they need and the enterprise doesn't pay for apps no longer in use

With the right strategy and SaaS management solution, you can bring SaaS apps out of the shadows and into the full visibility of IT. The rewards are substantial. You'll reduce wasted IT spend across the enterprise to drive down costs. At the same time, you'll strengthen security and compliance. Plus, the departments and business units in your organization will retain the SaaS budgetary independence they need to stay agile.

NEXT STEPS

Find out more about how SaaS Manager can help you

CONTACT US

ABOUT FLEXERA

Flexera helps executives succeed at what once seemed impossible: getting clarity into, and full control of, their company's technology "black hole." From on-premises to the cloud, Flexera helps business leaders turn IT insight into action. With a portfolio of integrated solutions that deliver unparalleled technology insights, spend optimization and agility, Flexera helps enterprises optimize their technology footprint and realize IT's full potential to accelerate their business. For over 30 years, our 1300+ team members worldwide have been passionate about helping our more than 50,000 customers fuel business success. To learn more, visit **flexera.com**

1-800-374-4353 | FLEXERA.COM

Flexera

Inform IT. Transform IT.™