eBOOK

5 INSIGHTS FOR EFFECTIVE SAAS MANAGEMENT

Contents

©2019 Flexera

Welcome to our eBook:

5 Insights for Effective SaaS Management

The SaaS industry is perhaps one of the fastest growing industries out there, particularly in cloud services, and trying to grab hold of it is like trying to catch the tail of a comet. According to **IDC**, the public cloud services market grew nearly 30 percent in 2017, and the SaaS segment holds nearly 69 percent of the overall public cloud market share. How is SaaS evolving and how do companies manage its rapid expansion across the enterprise?

From the overall SaaS industry perspective, 2017 was all about expansion without much consolidation. We continue to see many new companies entering the SaaS market with specializations. There are SaaS applications for virtually every task and function across all business segments, making it easy for SaaS spend and all its related data to get out of control quickly. We hear about it every day.

From a management perspective, 2017 was the beginning of the bell curve of awareness that SaaS is something that must be managed collectively as opposed to letting individual buyers manage their own instances. Major public security breaches forced IT to assess their exposure and what they may not be managing, such as shadow IT.

Beyond security, Gartner, Forrester, ITAM Review and other analyst groups started to beat the drum of SaaS spend management. They are bringing awareness into the amount of financial waste due to unused SaaS licenses and SaaS redundancy, compelling companies to manage SaaS for security, compliance and financial reasons.

We hope you enjoy a few of our most popular blog posts and will continue to keep you up-to-date on all SaaS management-related topics.

Paul Pieske, Flexera Product Marketing
linkedin.com/in/paulpieske

©2019 Flexera

The #1 biggest risk to CIOs

What keeps CIOs up at night

CIOs have plenty to think about these days. Shrinking budgets and too much work for too few resources are just the beginning. Security brings in a much more emergent threat. Cloud apps aren't just the newest blip on the radar, they can quickly become DEFCON 1. What is the biggest risk to CIOs?

Lack of visibility

When the IT landscape consisted of on-premise software, tracking investments in and usage of these technologies was relatively simple. The cloud changed all of that for most companies. It became more challenging to control cloud application procurements because they are so easy to find and use – often without anyone in IT every knowing. **Symantec believes that CIOs may underestimate the number of apps being used across their organizations by as much as 900.**

With every SaaS application that joins the software ecosystem, there is risk. With every risk, there is a single denominator – CIOs simply don't have enough visibility into what's really going on across their organizations. If you can't see it, it doesn't mean it isn't there. In fact, there's a good chance it's the most dangerous type of risk because it hides until it causes enough damage to make itself known.

> *"At the end of 2016, the average enterprise organization was using 928 cloud apps, up from 841 earlier this year. However, most CIOs think their organization only uses around 30 or 40 cloud apps."*
>
> **—SYMANTEC**

The 3 most common risks of cloud app blindness

If you have a single cloud app in your IT infrastructure, you have risk. Add in a cloud app here and a cloud app there and your risk increases exponentially. Yet it's not that simple. Different cloud apps bring different threats. What are the most common? We'll give you three.

1. Attack vectors

Every account with every vendor is an attack vector. An attack vector is the route by which a hacker finds its way into your network. If you have any system vulnerabilities, you can bet there's a hacker out there who will find it.

To make things worse, every employee becomes his or her own attack vector. They may not intentionally present risk, but either through negligence or misuse, they still add vulnerabilities. The **U.S. Department of Health and Human Services Offices for Civil Rights** reported the top breach in 2017 was theft, loss, improper disposal and unauthorized email access or disclosure – all from employees, not hackers half a world away.

Yet it's not all bad news. Companies can dramatically decrease their risk of attack when they have visibility into those attack vectors. Turn a blind eye and good luck. According to **Trend Micro**, many companies are turning to vulnerability research in order to identify vulnerabilities within software before they are exploited. Investing in security engineers who focus less on how systems work and more on how systems fail is an investment well spent.

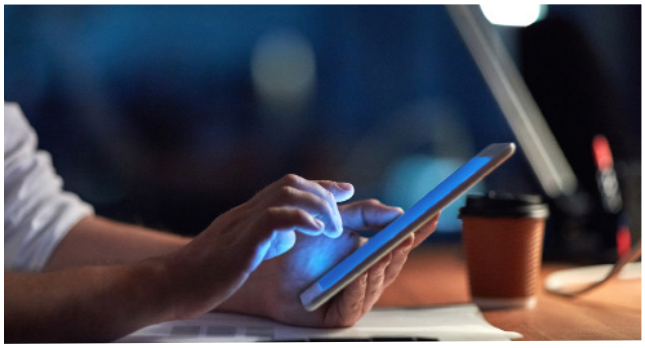
2. Single sign on

What do you think about SSO? If you're like most CIOs and employees, you don't like it. It's expensive and it's a bad process. While it may be convenient for employees to use one set of login credentials to access multiple applications, it makes it just as convenient for those with bad intentions to gain the same easy access to every application.

Companies must establish solid policies and governance around SSO without forgetting about the many accounts that may not be connected to SSO. As employees are free to use any app they find, these apps aren't always included under the SSO umbrella. They can bring the most threats because they aren't being tracked.

Strong SaaS management using the right tools, however, can shine a light on both SSO applications and non-SSO applications – who is logging in and when. Alerts can be set up to notify IT of any potential issues before they become crises.

©2019 Flexera



3. Unauthorized access

Who has access to what is a big question mark for many organizations. Does everyone who logs into a cloud app have the right clearance and permissions? Do former employees still have access, perhaps via a personal mobile device?

Without visibility into every cloud app across the enterprise, it's nearly impossible to know if the proper modifications have been made to each of them when an employee is offboarded. Sure, you may have denied access to DropBox, but what about all of the lesser used apps?

Tracking both cloud apps and the employees who use them is critical to reducing vulnerabilities and risk. Companies can leverage **SaaS management software** to combine all of this data into one location so tracking is simplified and access is automatically monitored.

X-ray vision

CIOs and their teams don't need glasses to better see their cloud platform; they need x-ray vision. They must be able to see between the lines, inside the shadows, and under the covers. Cloud applications, with all of their benefits, are challenging. You can't live without them these days, but their risks make it hard to live with them.

Cloud applications aren't going anywhere, leaving companies no choice but to adjust. They can begin by setting and enforcing standardized policies, choosing the right tool to automate the tracking of cloud apps and their utilization across the enterprise, and continually measuring their effectiveness. It isn't easy, but no one got into IT because it was easy. Keep your eyes wide open and boost your SaaS management strategy. You'll reduce your risk, lower costs and gain greater control over your cloud application environment.

CIOs and their teams don't need glasses to better see their cloud platform; they need x-ray vision. They must be able to see between the lines, inside the shadows, and under the covers.

©2019 Flexera

Why single sign on (SSO) isn't ideal for SaaS management

What are you betting your SaaS on?

So you've invested in single sign on (SSO) capabilities to give your employees a convenient way to log into the most used company apps. Great job. Now, you'll finally be able to see who is logging into those apps so you can understand what apps are really being used. In theory, this would be helpful information to drive better SaaS management and save costs.

In theory.

The problem is, as much as SSO can benefit the organization, it provides only the most basic data on your SaaS usage. Here's why:

Shadow IT isn't monitored

SSO is helpful to show you who has logged into the apps under IT management, but it ignores any SaaS apps IT doesn't know about, which are often many. If you don't think anyone in your organization is using a cloud app without telling IT, you're in for a surprise. If you're in IT, you may be sighing with recognition.

In a **Symantec poll**, 37 percent of respondents believe users or business units at their organizations are frequently or occasionally deploying cloud applications or putting data in the cloud without consulting IT. Based on my experience and other reports I have read, this may be a highly conservative number, particularly for organizations without a strong (or any) governance policies in place. The Symantec poll found 31 percent of organizations lack even the most fundamental cloud security policies, procedures or tools.

©2019 Flexera

Logins ≠ Utilization

The nature of SSO means employees are automatically logged into a series of corporate apps with one username and password, whether these employees actually use every app or not. This means your reports aren't really showing utilization, only logins.

To confuse matters more, login statistics may be redundant. IT may frequently set timeout rules when implementing SSO, making employees log in each time or once every several of hours. Obviously, this will skew any metrics and are not an actual reflection of cloud app utilization.

How apps are being used is ignored

SSO does not tell you what users are actually doing in each app, which features are being utilized and which are a waste of money. SSO only gives you marginal data on who logged in (intentionally or by default), but it can't tell you what your users did once they got into the apps.

SaaS contracts are often tiered, with companies paying higher costs for more features and additional users. If you don't know what features are being used and who is really using them (not simply logging in), how can you negotiate the best contracts and fees? Exactly. You can't.

Companies who really want to understand SaaS utilization so they can right-size their contracts, waste less money, reduce risk with improved security, and gain control over their SaaS landscape MUST do more than simply track misleading logins from SSO software. They absolutely have to gain visibility into the entire IT landscape, identifying all cloud apps in their ecosystem, including those rogue apps of which IT wasn't informed. Anything less is a half-assed, or should I say, "half-SaaSed" approach to management.

Integrate, Integrate, Integrate.

SSO attracts users because of the promise of integrations. SSO vendors survive based on their pre-built connections to thousands of on-premise and cloud vendors. While these integrations are a critical link, SSO only passes along login credentials to those apps with which IT is familiar. What about the dozens, even hundreds, of shadow cloud apps that aren't a part of the big, happy family? What's integrating to those and measuring their logins, users, utilization and fees?

Fortunately, there is hope for stressed out IT leaders. You can get the enterprise transparency you want and need for effective SaaS management. There is one caveat, however. You aren't going to get it from SSO alone.

True SaaS management demands integrations with cloud vendors and SSO vendors alike. Here's how it should work:

First, in order to find all cloud software being used, you must be able to analyze expenses and financial records along with SSO. This isn't as difficult as it may sound. Flexera works with SSO vendors while also continually expanding our own database of cloud vendors. This ensures we can easily pair up SSO data with charges for subscriptions to apps and quickly identify shadow IT.

The result? Users have real-time access to an interactive catalog of every SaaS vendor in their IT ecosystem, based not only on what employees admit using but on what may be hidden in "miscellaneous items" on expense reports. SSO doesn't come close to this level of detail.

Second, once each SaaS vendor has been identified, it's all about reporting to give you the information you really need to make the best decisions. Flexera SaaS Manager integrates with your SSO and each of your cloud vendors for more detailed, accurate user login information, including how the products are being used.

Why does this matter? Because with this data, you can easily identify where you are overspending on licenses and features. You can leverage volume discounts, scale back on underutilized features, eliminate redundant subscriptions, and right-size every contract. With SSO, you only get unreliable login data.

Is SSO even needed?

SSO is a powerful backend function that provides a seamless front-end experience for employees. It reduces login time as well as the costs and time associated with employees calling a help desk for password resets. It is enjoyed by many for the time it saves. It also gives companies some sense of control over the apps authorized by IT. Is that enough? Resoundingly, no.

Partial control is really no control at all. Use SSO to make it easier for employees to get their day started with one username and password to remember. They and your IT help desk will appreciate it, I am sure. However, if you are using it to reduce all costs associated with SaaS apps and improve security, you're using the wrong tool.

SSO doesn't go far enough by missing all of the shadow IT and it doesn't go deep enough by not providing the required level of detail leaders need to make better decisions. SSO is really meant for one thing: convenience. It does this well and for that reason, it's worth consideration.

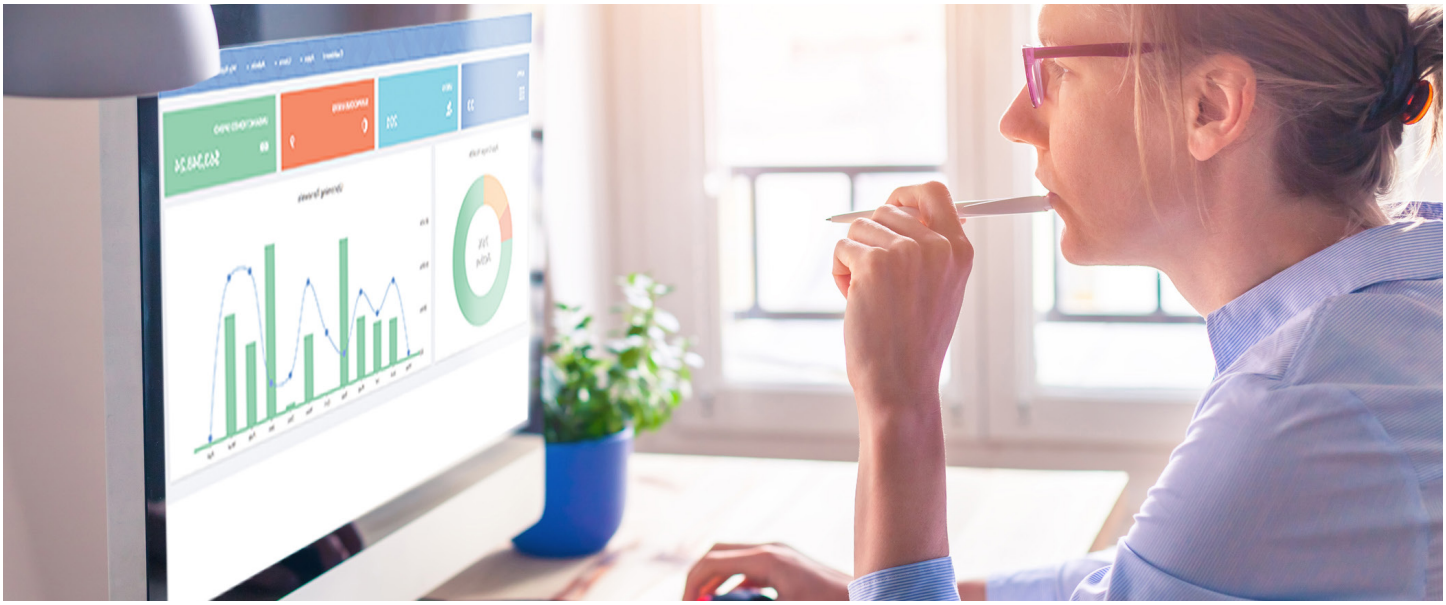
SaaS management = Visibility

True SaaS management, which should be on every company's priority list, is all about transparency. If you can't see it, you can't monitor it, protect it or manage it.

With more software moving to the cloud, the demand for better, more comprehensive SaaS management will continue to grow. Are you ready? Do you have a 360-degree view of your enterprise applications? Are your SaaS vendor contracts right-sized for your current needs or are you paying for future needs that may or may not ever evolve? Are the right people accessing the right cloud apps?

If you're only relying on SSO, you likely answered no to those questions, or worse, have no idea. It's okay. You aren't alone. This is new territory for many and wrangling it all into a manageable view hasn't been easy until now. The cloud has transformed our software and how we work. Thankfully, modern tools are available to make sense of it all. Use the right ones and this SaaS management thing won't be so hard.

©2019 Flexera



What is usage? Step one in calculating SaaS ROI

For many big-ticket items, business purchases usually make a notable impact on an organization – from management and IT to the watercooler – and sometimes even get communicated out to the client ("we're about to bring on X which will cut our response time down to verifiably proactive!!").

Also during those big launches there is a lot of visibility into the nature of the changes – there are consultants, and trainers, and hotlines for support – and management gets their first glimpses into reports, and although some promises inevitably get deferred, some dreams do come true. You'll see smiling managers asking how folks like the new functionality, and a few employees quietly griping about the way things used to be so much more obvious (they weren't, btw).

Sometimes even the smallest and least expensive of new tech can have a profound effect in the company culture – those of us who have done more than a cursory trial of Slack or Trello wonder how we got along before them (whiteboards and centralized offices, mostly).

And these big changes usually provide ample anecdotal evidence of usage, right? You're getting everything that you paid for because you remember the pain of bringing it on board. And everyone was in on the decision, so totally worth the effort, right?

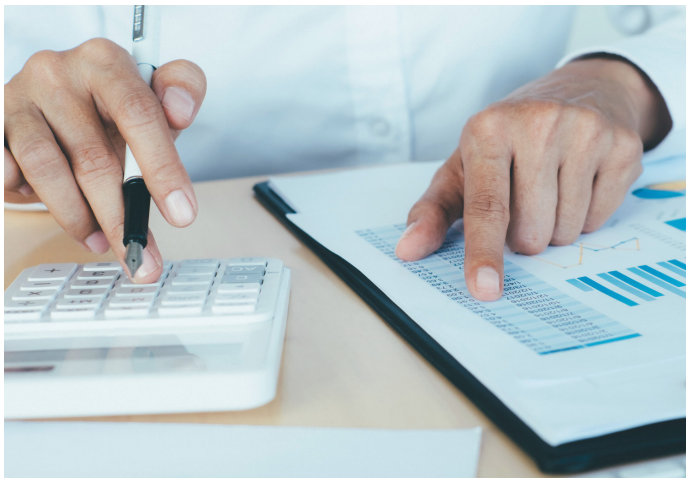
For every big-ticket item (Salesforce, Workday, Concur, Marketo), there's a handful of smaller-ticket items that have very real costs--integration, training and opportunity costs, to name a few--and the potential loss of value represented by potentially leaking or outright siloed and hidden IP.

So how do we make a case for the actual ROI of all these solutions that are potentially draining bits of time, money, and IP from your bottom line?

©2019 Flexera

As you might predict, determining ROI for your SaaS investment is not going to be a one and done campaign – you'll need to build a continuous process that allows for changes in your own organization, and new technology that will come online in the future.

Our first step will be to determine what constitutes usage of a SaaS product.



Determining SaaS usage

Let's start with an examination of the ways that usage gets billed, and we can use those methods as a proxy for further discussion of calculating SaaS ROI. There are three buckets of current ongoing billing practices (and remember even if the service is free or a one-time purchase, there is still the ongoing opportunity cost).

Per user billing

This is probably the most familiar method. Often described as seats, this is accounted for by having specific users with specific functions, access, permissions, and privileges within the solution. In some cases, the functions may be billed at different rates. These do tend to be specialized solutions – like Salesforce for example, or Adobe Creative Cloud. There may be bundle pricing at various numbers of seats – $X per user up to 10, $.8X for 10-50, etc. – that allow some economy of scale.

We might measure a proxy of usage of these solutions by checking logins – these people logged in a lot, but these people did not, so why are we paying for these seats, or what do we need to do to encourage the non-logins to harness the value that the solution offers.

Per account billing

Also very common, and usually priced with a bundle scheme per size of company, the most obvious example in my mind would be expensing software like Concur which needs to be potentially available to everyone in the company, but is likely to really be hammered by managers, directors and sales folks.

Again, we might use logins as a proxy for usage, but we might get a closer ROI calculation if we look at the number of transactions that take place in the system and compare savings to previous benchmarks.

Per transaction billing

I work in marketing so don't directly encounter too many products that get billed in this way, but what does get billed per transaction by some solution vendors is support or consultation. There are many automation solutions that bill per transaction, and we're all familiar with the potential pitfalls of transactional billing because of the text message portion of our cell-phone plans.

These might be the easiest to begin calculating ROI, particularly if you have a sense for the benchmarks of work those transactions are replacing. [I, personally, am waging a war on ctrl-c ctrl-v work – it seems like any work that involves repetitive copy paste in my line of work needs to be botted, so I can have more time to think a little about alliteration, or ponder puns, or whatnot. To me those are the transactions with real value. That is ultimately intangible of course. I'm not getting paid per pun or littered with awards for alliteration. Alas.]

©2019 Flexera

Determining SaaS ROI – The first step

Having walked through these common billing methods, it seems that the transactional basis might be the ideal starting place as a proxy for determining usage. Again, this isn't a one and done process. Your business is complex and every solution is chosen for perceived value. So as you work through your list (if you need some help in compiling a list of your SaaS portfolio, our post **How to create a SaaS governance policy** offers some tips), try to establish a cost per transaction, and if that doesn't work you can fall back to cost per user or account.

This would be a good time to think through the value of those transactions. Three adjacent columns I would suggest are:

- **Result** – what do the primary transactions accomplish – more sales? less confusion? Better use of available cash? A reduction in SaaS spend?
- **Replaces** – what processes does the solution replace – human time? a different system? bad cash handling procedures?
- **Risk** – what is at risk if we lose these transactions – does it warrant inclusion in disaster recovery plans? How many man hours would we lose if we had to attend to these transactions manually – even temporarily? how much IP is embedded in the transactions?

Figuring out your SaaS ROI is not a simple process. The best starting place, after starting a list of all the solutions, is to get a handle on what sort of usage metrics are most appropriate for judging the impact of the solution. For your own best time management, while you are collecting that usage information, you should also gather some key info about why you are investing in the solution – results, what it replaces, and what is at risk.

As you might predict, determining ROI for your SaaS investment is not going to be a one and done campaign – you'll need to build a continuous process that allows for changes in your own organization, and new technology that will come online in the future.

©2019 Flexera

SaaS management: shifting from compliance to cost containment

SaaS spending continues to increase

In a report **published by Gartner** earlier this year, the issue of SaaS management was brought front and center. Today's organizations are increasingly foregoing on-premise software for cloud- and subscription-based software. Gartner estimates SaaS spending will grow by nearly 20 percent to $76 million by 2020.

The reasons and benefits are obvious: no maintenance fees, little IT support, zero footprint, and simple upgrades, to name a few. While SaaS is quickly becoming the new norm for purchasing and IT, SaaS software management and SaaS vendor management is proving to be a bit more challenging. Much of this is unchartered territory.

The issue of SaaS management doesn't rear its ugly head until an organization begins to use multiple SaaS applications, particularly when it's across divisions and geographies. Because much of this software is easily accessible and often comes with a free trial period, unless there are enforced protocols, governance, and oversight in place, virtually anyone in the organization is free to download whichever SaaS application they think is cool or useful. Purchasing and finance often have no idea just how many applications are being purchased after that trial period. There is no order. Just chaos.

RELATED: What exactly Is shadow IT and how do I stop it?

Sure, the explosion of SaaS applications gives us a dizzying array of options promising everything from increased productivity to unprecedented accessibility. The problem, however, is complicated. First of all, these free trials expire. Secondly, every department has their favorite SaaS apps and can justify (or not) their absolute necessity. An organization is left with escalating costs and no real grasp on how many of these applications are being used, who is using them, and how much these one-off apps are costing the company.

Where are costs coming from?

Most companies don't really care if their employees have found an app that helps them to their job better or faster. It's the cost of those apps that moves the needle. While SaaS applications may seem less expensive and surely less cumbersome than on-premise software, companies can spend thousands, even millions, for software licenses. Tragically, many of these licenses are a waste of money – not because the software isn't useful, but because they aren't being fully utilized.

When a company purchases licenses, it is assuming the software is both useful and will be used by those for whom they are purchasing it. But, when employees are free to download their own SaaS applications, they often do so in conjunction with halting their use of the replaced software. That license is still being paid for and renewed when that employee is no longer using it. Same thing occurs when an employee leaves the company or shifts roles and no longer uses that same software. If the license isn't being monitored for utilization on a per-employee basis, the company continues to pay for the license when it's no longer necessary.

Another issue, brought up by Gartner, is that when employees sign up for these SaaS applications themselves, they lose the bargaining power afforded by a mass license purchase. Prices continue to escalate as the contract renews, yet the company often has no idea the costs are getting out of control until the balance sheets begin to tip.

The SaaS model indeed has its benefits, but companies must take a proactive approach in managing the contracts, vendors, and costs. It's no longer an issue of compliance, that is, adherence to the terms and conditions of usage in the licensing contract, but of reducing costs associated with SaaS applications.

RELATED: 3 reasons to prioritize SaaS spend management

Gartner's take

Gartner clearly recognizes the challenges organizations are facing when it comes to SaaS management. They offer three recommendations for business leaders tasked with managing software licensing:

- **Demand self-service and granular active usage reporting from the SaaS provider or SAM tool vendor before committing to any contract to provide the data necessary for effective cost management and containment.**
- **Prioritize their organization's SAM capability to focus on metering SaaS application usage to eliminate unnecessary tools, and ensure that any SAM tools in place, or being acquired, can deliver cloud service metering.**
- **Implement and drive adherence to software requests, allocation and harvesting of unused software processes, to eliminate unnecessary or costly provisioning of SaaS services.**

©2019 Flexera

It may not be as simple as relying on the SaaS vendor to produce detailed reports of application usage per employee. Depending on the vendor, the reports content and timing will vary. All of those reports will still need to be aggregated, compared, and managed. Organizations end up with is disjointed reporting with little integrated perspective. Instead, Gartner suggests companies should "augment their SAM investments and demand SaaS-capable solutions and services from internal or third party providers."

A third party is likely better suited to aggregate the many bits of information from the various SaaS solution providers to offer a unified view of the overall SaaS spend, utilization, and contracts.

What companies can do now to contain costs

Companies can do much more to contain costs when it comes to SaaS applications and they can begin today.

- Establish corporate policies on SaaS application acquisitions and spend of any kind
- Invest in a tool to unify SaaS management
- Budget SaaS spend like any IT spend
- Select software options and license quantities in advance
- Measure utilization per employee and establish thresholds for retainment

Companies should easily be able to quantify the value of the SaaS applications as they measure not only how many employees use each app but how frequently they use it. It's one thing to know 150 employees have logged into a CRM application, for example. It's quite another to understand that only 50 of them are using the application on a regular basis.

Keep in mind that many of these applications have single sign on and automatic login. **If you are relying on a utilization report that only gauges usage based on logins, you are making decisions based on false data. Logins do not equate usage.** Are you paying license fees for employees who are only automatically logged into an app they never or only rarely use?

How many former employees are you still paying license fees for specific software? How much SaaS overlap is there between departments? How many separate software contracts are being negotiated for the same software without the knowledge of those who are doing the negotiating? How much is the company forking over for SaaS application features that aren't being used? How many automatic renewals are missed because there is no centralized calendar?

Control over the chaos

Every one of these scenarios is happening on a regular basis in companies without an intentional solution to manage SaaS applications and vendors. With every added application, there comes contracts, licenses, renewals, fees, users, and owners. It forms an entangled web of solutions that can add up to exorbitant and mushrooming costs.

Companies must gain control over SaaS management and it shouldn't involve spreadsheets or email. These desktop tools are no match for this complicated ecosystem that continually evolves. It's time to invest in a unifying **SaaS management tool** that can provide the much-needed insight into this complex world.

The bottom line? As companies opt for SaaS applications over on-premise software purchases, the need to monitor costs and usage data is critical. Costs can quickly escalate unnecessarily when left unchecked. It is essential for companies to get as much value from their subscriptions as possible to justify the costs.

©2019 Flexera

7 steps to successfully managing a SaaS subscription renewal

Managing any type of vendor contracts requires careful attention to detail, and SaaS contracts are no exception. If you're tasked with handling the upcoming renewal for a SaaS contract, it might seem natural to wait until the renewal window comes up to start the process.

Waiting until go time is like running a marathon with no previous training. Your body hasn't built up the necessary endurance and reserves. The stakes are different here: a fumbled renewal could mean higher costs for your business or intermittent loss of access to the SaaS platform.

Giving yourself a head start on the renewal process is critical – but that's not all. Here's a handy checklist to help you successfully negotiate a SaaS renewal contract:

- **Before you do anything, check (and double-check) the renewal window in the contract.** This window is the amount of time you have to handle the contract renewal. Looking for the renewal window in the contract is a start, but to take it one step further, reach out to your SaaS account rep to confirm the window. The last thing you want is to be operating off an incorrect time period. If you need a refresher, review our recent post on the **nuts and bolts of contracts.**

- **Scour the contract for an auto-renewal clause.** Knowing the renewal window gives you one important input, but you might also have an auto-renewal clause. This clause states that if the client doesn't notify the SaaS vendor by a certain date, the contract auto-renews for a set amount of time. The auto-renew clause can take effect during or at the end of the renewal window. It's also a good idea to confirm the terms of the auto-renewal clause with the SaaS vendor.

- **Give yourself 90 days to do some homework before the renewal window starts.** If you have the luxury of time, use it. Gathering a wealth of data allows you to better understand your business's relationship with the SaaS vendor, and how you can improve it during the renewal process. If you walk into a current renewal, so be it, but do yourself a favor and pad your calendar wherever possible.

©2019 Flexera

- **Contact departmental owners for context and history on the SaaS platform.** The leaders and employees at your company can provide great insight in the renewal process. How did employees find the SaaS tool? Who negotiated the initial contract? How did the negotiation go? How has the SaaS tool performed since the launch? What do managers and employees wish they could change about it? This is just a handful of questions to ask to give yourself a broader picture – before renewal discussions begin.

- **Evaluate SaaS usage against what you're currently paying.** Dig into the reports for the SaaS platform and look for usage patterns. Are 80% of your users only using about 20% of available functionality? Are there ways you could cut costs by dropping down to a lower usage level? Alternatively, are the majority of users frequently going over usage limits and costing you overage fees? **Evaluating usage** will give you another important data point that may provide leverage during the renewal.

- **Understand changes to the SaaS tool since the contract started.** This data might come from multiple sources, including employees who use the tool AND your SaaS account rep. Survey employees internally to find out what new features of the SaaS platform they use that weren't available initially. If you come up short, check in with your SaaS account rep – not to start renewal discussions, but to ask for any enhancements they've built. You'll have a better understanding of any additional value your employees might derive from the SaaS platform.

- **Contact your SaaS account rep when you've filled in all the blanks.** With all the information you've gathered, you're ready to reach out and begin the renewal conversation. Even if you're on a short timeframe, try to wait until you feel prepared. There will almost always be surprises you can't anticipate. The best thing you can do is equip yourself with all available inputs to make the most informed decision.

RELATED: Take control of your SaaS spending: know your contracts

©2019 Flexera

2018 and beyond

As a leader in SaaS management, Flexera will continue educating companies about their SaaS risk and spend, and developing products that solve real problems. We listen to our customers and we know they need SaaS management tools that empower them to take control of their expanding SaaS environment.

Throughout 2018 and beyond, we will continue to roll out new features and functionality that give customers the necessary visibility into their data, with actionable insights to improve their overall SaaS management spend, security posture, and compliance readiness.

NEXT STEPS

To learn more about effective SaaS management, visit us online

LEARN MORE

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**

1-800-809-5659 | +44 870-871-1111 | FLEXERA.COM

© 2019 Flexera Software LLC. All other brand and product names mentioned herein may be the trademarks and registered trademarks of their respective owners.

Flexera

Inform IT. Transform IT.