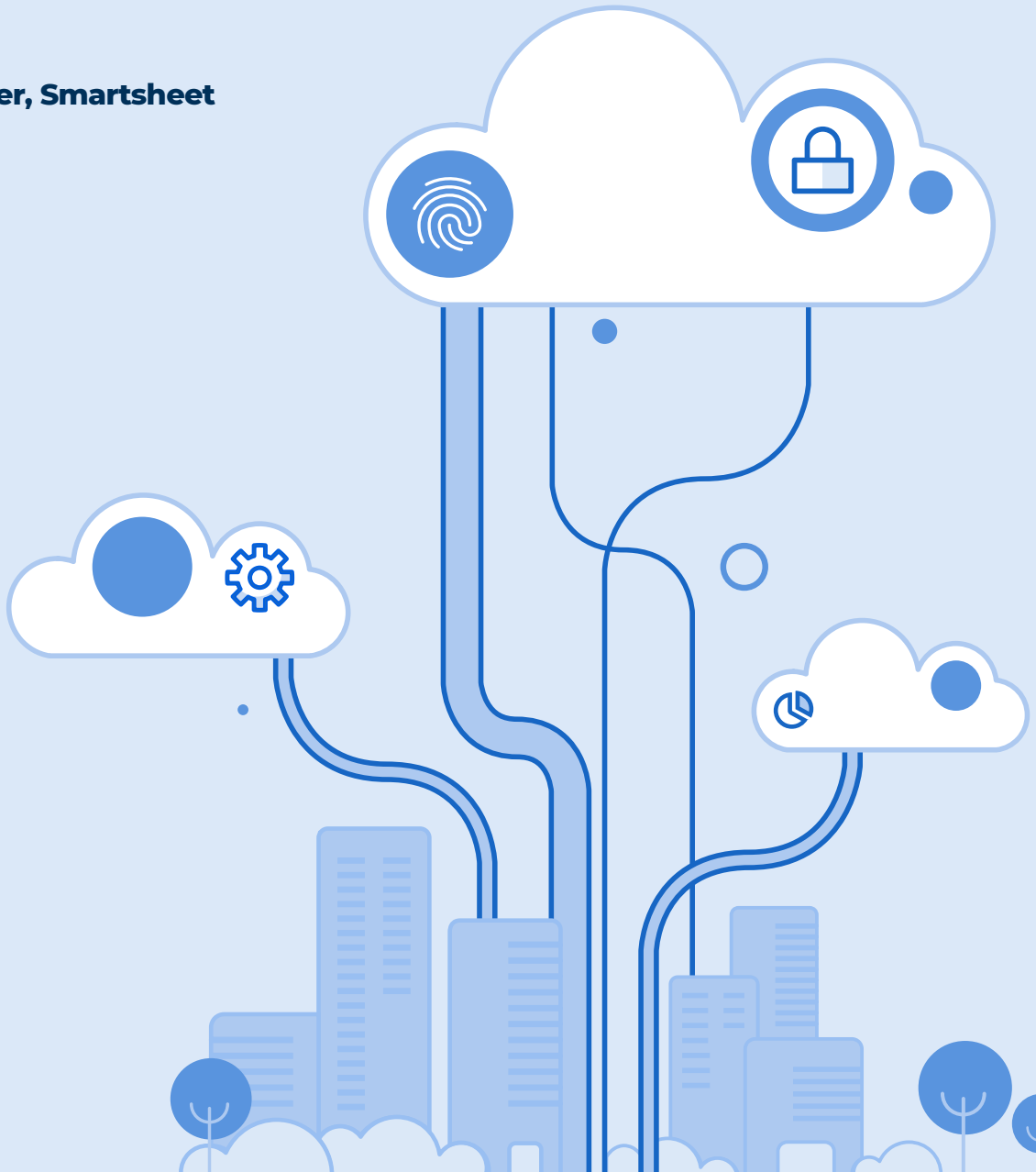
smartsheet

A Smartsheet Report:

The Hidden Costs of SaaS Sprawl

By Praerit Garg
Chief Technology Officer, Smartsheet



As far back as 30 years ago, companies were automating key business functions like finance and HR, and a growing ecosystem of vendors was innovating—writing new applications with functionality to extend or fill in the gaps left by those larger ERP systems. Companies, seeking an edge and each with its own unique processes and business models, began piecing together point solutions and platforms to create the perfect blend for their operations.

But with so many traditional processes being transformed by new software, it wasn't long before many of those companies found themselves with too many applications. Struggling with integration issues and siloed information pools, they began to focus on reining in this burgeoning application sprawl.

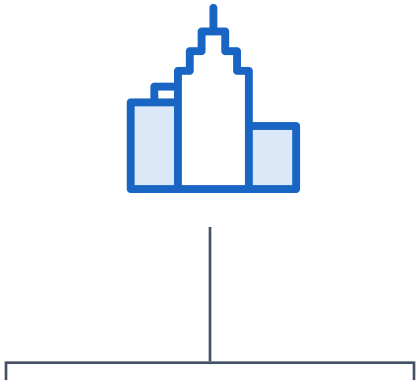
Out of that period came the integrated software suites we know today, and an emphasis on application portfolio consolidation and optimization across the enterprise. The discipline of IT, at least, learned to be strategic and methodical when it comes to bringing in new apps.

Today we're in a similar situation. Technology has been democratized, and we live in a world where applications flow like water. After a decade of innovating in the cloud, apps power everything from factory floors to traffic signals. The number of devices has also exploded. Nearly everyone has two, three, or even more screens, each one loaded with apps. On a daily basis, any number of phones, laptops, smart watches, and other devices make their way into and out of any organization.

And these are issues that will only continue to grow in scope, with more devices and more SaaS apps coming every year. According to a recent Forrester report, as all of the major cloud providers continue to grow in 2019, the market for business services and SaaS applications will top $200 billion, up more than 20%.[1]

Part of what's fueling that growth is simply the ease with which cloud-based apps can be acquired and implemented. Anyone with a smartphone can download an app in a few minutes. On an organizational level, business units can dial up a SaaS subscription with a credit card. A 2017 report from McAfee found that the average enterprise had 1,427 distinct cloud services and the typical employee used 36 different applications during their workday.[2]

In this environment, most companies do not know the extent of their entire application portfolio. They can't say where every single app is running, what it does, or who it serves. Just like those earlier days of IT, they are suffering from application sprawl.



A 2017 report from McAfee found that the average enterprise had 1,427 distinct cloud services and the typical employee used 36 different applications during their workday.[2]

1. Forrester, Nov. 2018. Predictions 2019: "Cloud Computing Comes of Age as the Foundation for Enterprise Digital Transformation."
2. McAfee, 2017. "Cloud Usage is Now More Than 90%, but IT is Struggling to Keep Up. Are You?"

Chances are good that your organization is one of those affected, and you may not even know. But what are the hidden costs of having so many apps across the organization? And what can be done to tame SaaS sprawl and restore sanity to your application portfolio?

Cost No. 1:

The security snowball

Tension between IT and business units goes through cycles, and SaaS is the newest iteration. Back in the 1990s, users would go and buy their own file servers and keep them outside of the purview of IT. The impetus behind these servers-in-a-closet was often the feeling that IT wasn't responsive to the needs of the business, so those business units took matters into their own hands. In doing so, however, they also created risk for the organization and ultimately more work for those already overburdened IT departments.

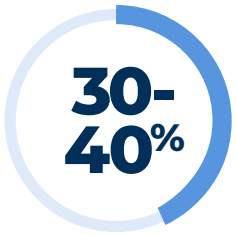
In the cloud world, end-user empowerment is at another level. Employees don't need to buy software or hide physical servers under their desks. They can go to a site, enter a credit card number, and start consuming a service as if they were consuming cable television. Computing has been democratized, increasing the complexity of an organization's overall IT picture—and drastically widening the attack surface.

Computing has been democratized, increasing the complexity of an organization's overall IT picture—and drastically widening the attack surface.

Just looking at the human element can put this issue into perspective. If a company has 500 SaaS vendors, and each of those vendors employs 100 people, that represents at least 50,000 more laptops, phones, email accounts, and other potential targets for an attack that could eventually wind its way back to the organization and its critical data resources. With shadow IT, you don't get the service level agreements and other requirements designed to mitigate that risk and protect the organization as you would with a proper IT implementation.

And that's not even considering the apps themselves. Just like those rogue file servers in the 90s, SaaS apps don't always have the security, manageability, and control needed in a modern enterprise. With the flexibility and ease afforded by the cloud, business units adopt and deploy solutions without ever conducting a risk assessment or building a security strategy for the solution. This is leading some IT teams to adopt "zero trust" security models, trusting no one by default—even those inside the network perimeter.

According to Gartner, shadow IT now represents 30% to 40% of IT spending in large enterprises, and by 2020, those same shadow IT resources will be the targets for a third of successful attacks.[3] And yet increasingly cloud-based spending in organizations bypasses the CIO, as lines of business make those decisions. In this sense, SaaS sprawl represents a critical risk and a security imperative for the organization.



According to Gartner, shadow IT now represents 30% to 40% of IT spending in large enterprises, and by 2020, those same shadow IT resources will be the targets for a third of successful attacks.[3]

Cost No. 2:

Productivity lost in silos

Too often, SaaS tools are used in isolation without any integration of processes or data. One business unit rolls out an app across the team, and just down the hall, another business unit rolls out a completely different app.

In many organizations today, this results in app overload for users. Workers can be using multiple chat-based collaboration tools, dozens of different file shares, and productivity tools from different vendors and platforms.

In this environment, finding a particular file or workstream can often boil down to finding the right person who simply knows where it lives. Even then, the same file may reside in multiple locations, each with its own set of updates. This means that departments across the company could be working with incomplete or inconsistent data. There is no single source of truth.

Another contributing factor involves working with third parties—partners, customers, agencies, and vendors. Efforts to integrate and streamline processes with these outside entities can lead to the incorporation of even more tools, even more file shares, compounding the complexity that workers must unravel.

Think of all the possible permutations of applications, storage, files, passwords, naming conventions, versions, workstreams, and roles and responsibilities created by the ad hoc addition of dozens or even hundreds of applications to an organization's IT. McKinsey's landmark 2012 study looked at the effects of this issue on productivity and found that knowledge workers at that time were spending 1.8 hours per day searching for information—almost 20 percent of their day.[4] Even with today's better search capabilities, locating information can be a huge productivity drain.

3. CIO, April 2017, "How to Eliminate Enterprise Shadow IT."
4. McKinsey Global Institute, July 2012. "The Social Economy: Unlocking Value and Productivity Through Social Technologies."

When applications spring up organically across an organization, silos are the inevitable result, and silos impede productivity, communication, and organizational effectiveness. All of those applications were brought in to solve business challenges, but taken as a whole, the problem of application sprawl poses a hurdle for the organization.

Cost No. 3:

Bloated budgets

From the perspective of the IT department, it is far too easy to license and deploy a SaaS application. Business units and even individual users can and will bring in new applications any time they see a gap in the functionality they need to do their jobs, and the IT department itself is under pressure to keep up and give users the tools they need.

But at a certain point you have to ask, how many applications are we going to bring in? What are they all doing—and where do they overlap? And how much is all of this investment costing the company?

SaaS sprawl poses a tough challenge for security and productivity, and it's also hard on the organization's wallet. The easy availability of apps and a lack of transparency and communication across business units and operational departments can easily lead to redundant applications, multiple subscriptions to the same service, or subscriptions for software that, in fact, is not being used at all.

This is a problem shared by both software sanctioned by the IT department, as well as that growing shadow IT portfolio so many companies struggle with today. Lacking a centralized way to track and manage all of the apps in use by the organization, companies are hard-pressed to manage the overall spend on their app portfolios. Shadow IT makes this essentially impossible, too, because you can't track spending for licenses you don't even know about.

In addition, without that clear view across the application ecosystem, pruning the budget and weeding out unneeded apps becomes much more difficult. When it comes time to pare down, you want to make sure you're cutting the right things.

This is a problem that can't be solved overnight. To really clear up application sprawl, companies need a methodical process that involves both the technologies themselves, and the people across the organization who use them.

Cost No. 4:

Less effective IT

The great irony in all of this is that the fundamental cause of SaaS sprawl and shadow IT is the business units and users who are demanding more functionality, faster. Many organizations will cite the IT department as not being responsive enough to the needs of the business when making the case for a new application, either formally or informally.

Yet at the same time, the proliferation of apps is overwhelming the resources and capacity of the IT department to manage them, let alone to serve the business in a more agile fashion. Risk exposure is increased, necessitating more resources to address security and compliance. And the ROI of approved IT investments is impacted as well, as the user base spreads out to other applications and processes. Not to mention the time and effort involved in tracking down, evaluating, and integrating new apps as they are requested, or in the case of unsanctioned apps, discovered.

Ultimately the job of IT is to empower the organization to transform digitally so it can run at the speed of business, while minimizing and mitigating the risk involved. By stretching those resources, SaaS sprawl draws focus away from the prime objective of IT and can slow the department's ability to respond to new business needs. This, in turn, can lead to even more sprawl and more shadow IT as business units and users follow the now decades-old practice of skirting formal IT processes and implementing rogue technologies on their own.

A way forward

This sprawl of application usage is a direct result of democratization of information technology—from mainframes to servers to PCs to mobile devices and app stores—combined with the growth of the internet and cloud services. It is important to recognize that fighting this will not make any central IT organization succeed. IT's mission is to make employees more effective, and if users believe that this growing suite of applications makes them productive, saying "no" is not going to work.

Align IT's thinking with the business

The role of IT has evolved to where IT leaders are business leaders. Instead of dictating IT policies from the top down, IT organizations should seek to create a culture of partnership with the broader organization, with a focus on empowering the business.

While application sprawl is a technology issue, it is also at its core a human issue, and in the workplace it is driven by business needs. Therefore, any assessment of technologies has to begin with the need or challenge it was meant to address.

Business groups generally have good reasons for wanting to adopt SaaS cloud services. They are trying to work more effectively. The job of IT today is to understand that rationale and the requirements and objectives of achieving the business' goals. IT can then combine that understanding with their expertise in finding and integrating the right solutions that support the business while mitigating risk.

Assess your application ecosystem

It's important to get a holistic view of the entire application portfolio. Managing apps with more rigor is becoming a new differentiator, because the organization can then begin to assess how successful those investments are, in addition to resolving the challenges we've been talking about above.

With IT and business units working in partnership, the organization should be able to report on every app in their ecosystem, whether it powers a multi-million dollar production facility or a minor process. At a high level, the organization needs to know what the app is, what impact it is driving, who is using it, how it's being used, where it's running, and whether it's secure. And this rigor should be applied not just to existing applications and investments but to new ones as well.

Identify risks

Not all apps are created equal, and the risks that some apps pose to the organization are too great to ignore. File sharing apps commonly come under scrutiny here, but vulnerabilities can be found not just in the apps themselves, but in how and where they are hosted and a multitude of other factors, such as who has access and what permissions they have. For any application that the organization wants to keep and run, a risk assessment plan should be conducted, and any mitigating controls implemented.

A critical area of risk is how users authenticate to the application. The ability to integrate the app with the corporate directory so that single-sign-on works is key. This reduces the risk of credentials being leaked and also ties the access to each user's corporate identity, which can ensure that the access is bound by the user's employment. It also enables easy auditing of what the user is doing.

Educate the organization

Addressing SaaS sprawl and its consequences is an ongoing mission for IT, and end-user education plays an important role. If you identify high-risk applications and ask users to switch to alternatives, you need to educate them on why. This is another reason it's key to start from a partnership point of view and acknowledge the business need that drove the app's adoption—now presenting an alternative becomes easier.

Break learning into micro sessions so you don't overwhelm employees. Lunch and learns or fireside chats that happen over time and are a regular part of your culture can be very effective. You can also use messaging throughout your organization that keeps information at the forefront.

As the organization evolves, the level of risk it can absorb will evolve, too. Create a sustainable model and culture around ongoing employee education.

Take action

Once you've taken stock of your applications and educated the organization, you can use your own IT to understand where any gaps may be and stay apprised of changes, monitoring the network, watching traffic and endpoints, and using a variety of tools to enable even more control.

Once more, this isn't about being a gatekeeper; instead, it's about enabling the process of inventory, risk assessment, and user education as an ongoing concern. Simply shutting down a team's access could ultimately backfire, leading to new work-arounds that create even more risk and erode the business communications you've been working to build.

Make sure you can explain clearly why a particular tool won't work for the organization, and before you shut down an app, identify an alternative that meets both the user's needs and the company's security and risk assessment profile.

Manage cloud with cloud

In the age of SaaS, it's also important that the tools and policies you implement include cloud-native components so you can see, manage, and respond to events continually in both your on-premises and cloud-based systems. Strong access controls can provide visibility into any systems or processes that interact with cloud infrastructures, and third-party vendors such as cloud access security brokers can go even deeper, including the ability to help you uncover shadow IT in the organization.

Adopt a DevOps mindset for IT

Once these processes are in place, they should become a continual process. People join and leave companies all the time. Tools and functionality are continually evolving. The needs of the business constantly change. The goal of IT is to stay ahead of all of these factors to empower the business to succeed.

About the author

Praerit Garg is Smartsheet's chief technology officer and executive vice president of engineering. He has more than 23 years' experience building large-scale distributed systems and internet services, and is the former general manager for identity, access, and directory services at AWS. At Microsoft, he was part of the original team that built Active Directory, and led the design and implementation of many of the user identity, access, and encryption features in Windows. He is also co-inventor on more than 25 patents.

About Smartsheet

Smartsheet (NYSE:SMAR) is a leading cloud-based platform for enterprise achievement, enabling teams and organizations to plan, capture, manage, automate, and report on work at scale, resulting in more effective processes and better business outcomes. Smartsheet is committed to continuously delivering a secure and extensible platform that meets the complex needs of today's largest enterprises. More than 75% of the companies in the Fortune 500 rely on Smartsheet to implement, manage, and automate processes across a broad array of departments and use cases. To learn more about Smartsheet, visit www.smartsheet.com, or reach out to us at smartsheet.com/contact and we'll help you get started today.