Productiv™

The State of SaaS Sprawl in 2021

CHALLENGES OF A DISTRIBUTED WORKFORCE AND LARGE APP PORTFOLIO

SaaS sprawl is a big deal

‘SaaS sprawl’ — you’ve heard the phrase a dozen times by now, but it doesn’t seem significant in the context of your critical IT priorities. You know what your cloud technology stack looks like (for the most part). You feel fairly confident about your level of visibility into governance and application usage. That’s good enough, right?

The truth is many businesses have a much larger blind spot than they realize when it comes to SaaS apps. More and more business units are independently purchasing app subscriptions or downloading freemium tools. That’s great for employee productivity in the short term, but it can create new challenges for the IT teams tasked with managing the SaaS portfolio and ensuring governance.

Every SaaS purchase outside of IT has the potential to expand your security risk surface and create fragmentation that prevents your employees from doing their best work. More tools means greater opportunity for users to work in silos without a clear view of interdependencies. SaaS sprawl also drastically impacts your business spend, whether you see the bill or not. Having many team-owned tools can lead to unregulated SaaS budgets and an increased cost of ownership due to situations like missed renewals.

To understand the current state of SaaS sprawl, we looked at an anonymized subset of Productiv data across hundreds of instances and tens of thousands of SaaS apps. The results offer a clear picture of how decentralized SaaS management is affecting businesses both large and small across app visibility, employee productivity, and risk governance.

The truth is many businesses have a much larger blind spot than they realize when it comes to SaaS apps.

HIGHLIGHTS

Key takeaways

Shadow IT is growing across the board, but most prevalent among high-growth businesses.

The number of apps not owned or managed by IT grew by 4 percentage points (from 52% to 56%) on average in the last year. Small organizations have the highest percentage of Shadow IT, likely due to having younger and fast-evolving SaaS portfolios.

Most departments now have 40-60 tools each, with 200+ apps at the company level.

Departments related to Security, IT, and product development had the highest average number of tools. In addition, analysis of app categories revealed significant overlap across critical functions such as messaging and file storage that often leads to fragmentation and collaboration breakdowns.

Average percentage of engaged users across all apps is 45%.

We measured how employees are engaging with apps at the feature level (which is more accurate than using login data), and found average engagement to be low. This implies companies are having trouble aligning licensing to how employees are using tools. Apps purchased outside of IT have a higher engagement rate, suggesting employees are finding more value in the tools they select for themselves.

The majority of apps have 3 or fewer security certifications, and Shadow IT is typically less compliant.

Our analysis found 83% of tools were compliant with less than half of the 7 most common certifications. Shadow IT had fewer certifications on average compared to apps managed by IT, reinforcing the need for IT to be made aware of all tools in the company's SaaS portfolio.

Nearly 70% of apps managed by IT are behind SSO.

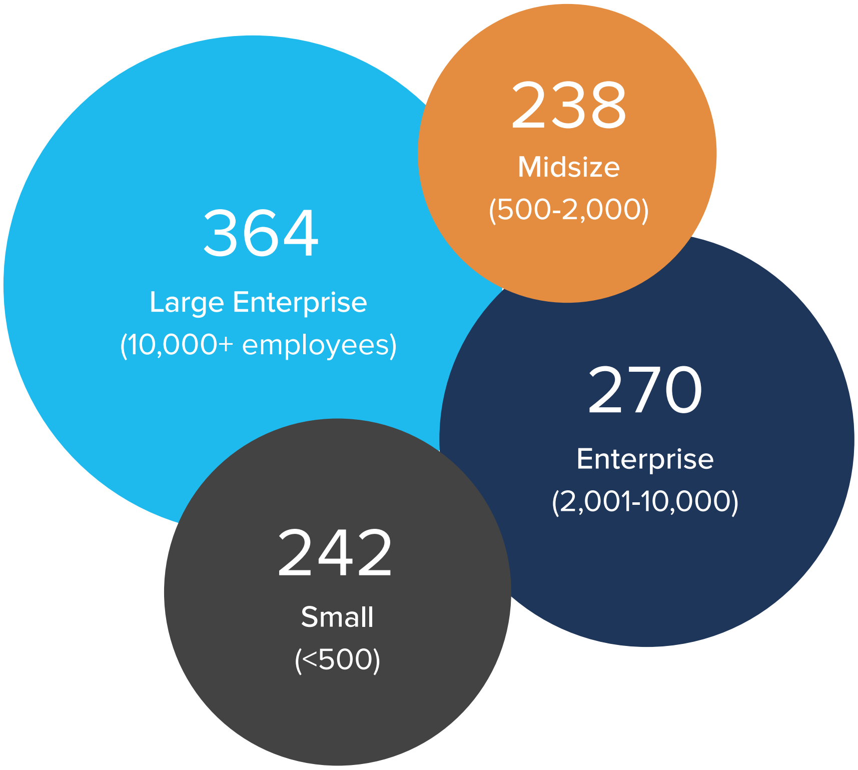
SSO is a key tool organizations are using to provide governance and access control, and more than half of all IT-managed apps are behind SSO. Enterprises have the highest SSO coverage across their apps, which may be the result of more robust security protocols.

With more organizations working remotely, SaaS sprawl has surged

The mass shift to remote and hybrid work in 2020 led many organizations further down the path of building or enhancing their cloud tech stack. Today, we see businesses of all sizes are relying on hundreds of SaaS apps to conduct operations. Large enterprises average 364 tools, while small businesses average a portfolio of 242 apps.

254 apps Average SaaS Portfolio

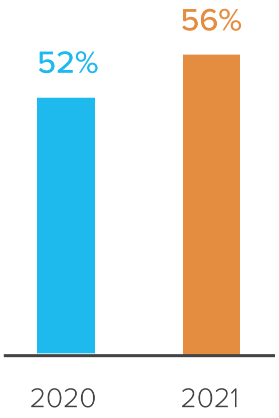
Average app portfolio size



Shadow IT rose by 8% overall, but larger organizations have fewer unmanaged apps on average

The combination of a distributed workforce and employees with unfettered access to hundreds of thousands of apps had a predictable outcome: businesses experienced a rise in tools not managed or owned by the IT department (AKA Shadow IT). Between 2020 and 2021, our data shows Shadow IT increased by nearly 8%.

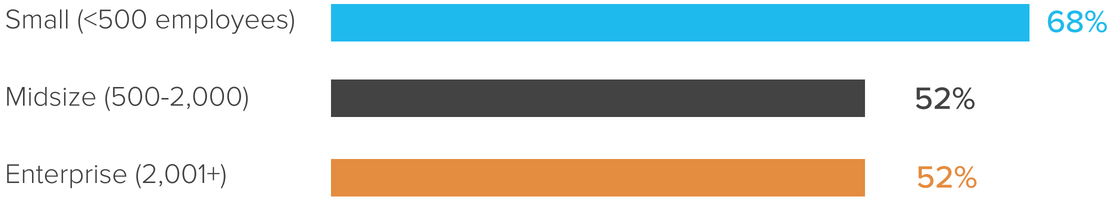
Prior to the pandemic, organizations were already seeing growth in Shadow IT. The transition to remote work exacerbated the challenge, as individual business units problem-solved app needs on their own by directly purchasing or signing up for tools. Today, more than half of portfolio apps are Shadow IT on average.



Shadow IT increased by an average of 4 percentage points

The magnitude of Shadow IT also correlated to business size. Midsize and large companies, which tend to have more mature app portfolios, showed a lower percentage of Shadow IT apps compared to small businesses.

Shadow IT breakdown by business size



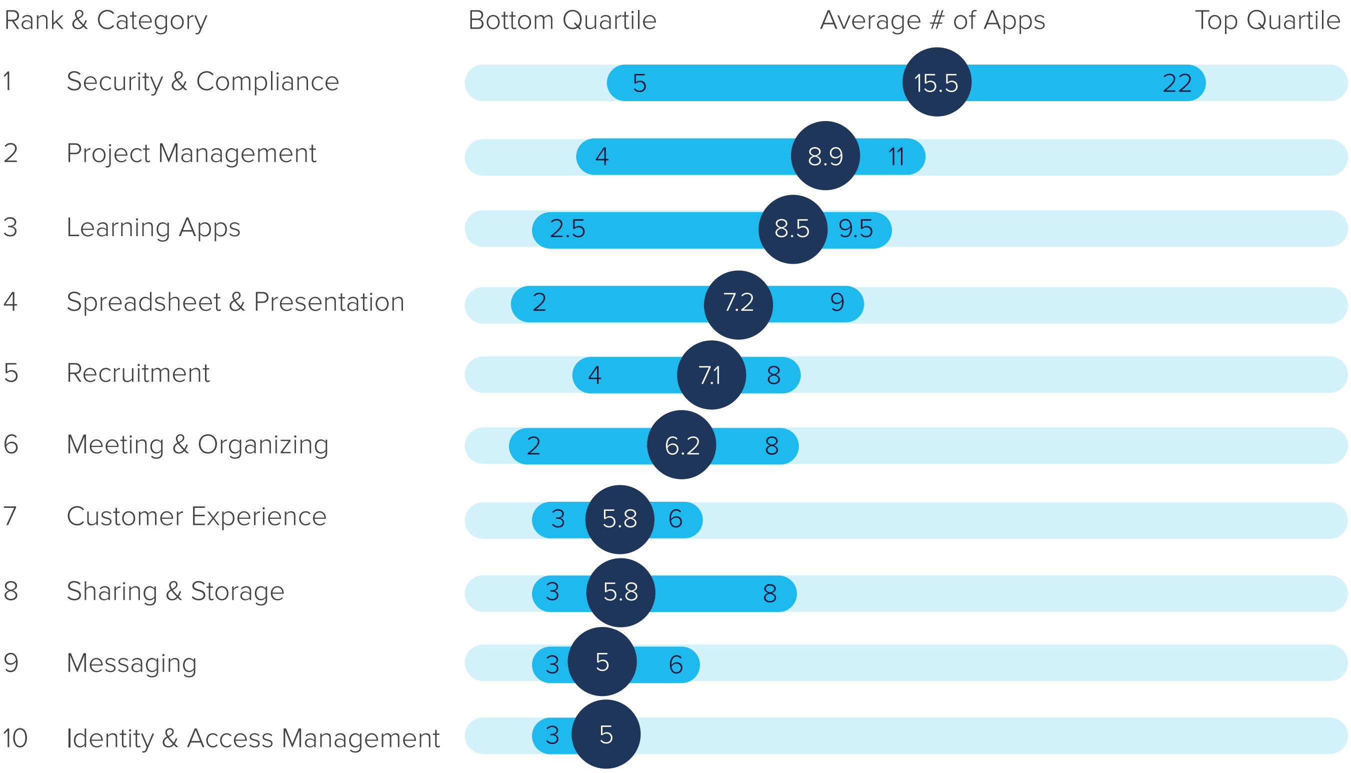
APP CATEGORIES

Having too many apps may hinder productivity

SaaS sprawl is not confined to specific types of apps, either — it's occurring across the organization. We analyzed 107 categories of apps and found that organizations typically had 17 categories with 5 or more tools.

Our data shows on average businesses have 5 or more apps in critical categories like project management, sharing & storage, and messaging. These numbers are concerning, as having too many apps with similar functionality can create fragmentation and be detrimental to employee productivity. For example, the average number of project management tools is 8.9. As a result, project oversight efforts may be too scattered for those apps to deliver on their potential value. Furthermore, this trend is likely to keep rising as business units and individuals purchase more apps independent of IT.

Top 10 categories with the highest average number of apps



APP ENGAGEMENT

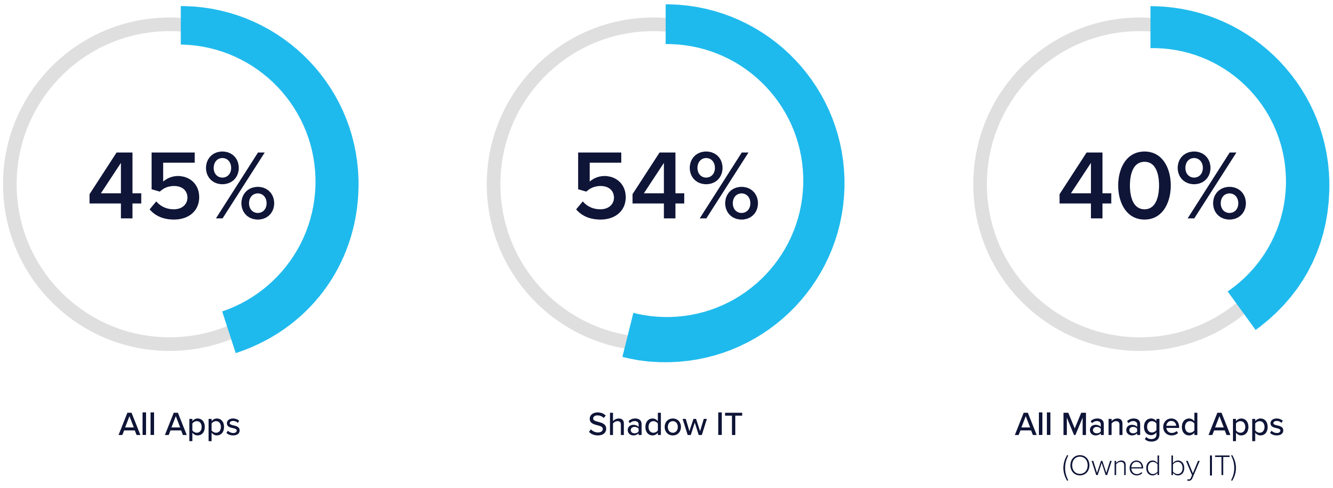
Despite growing app portfolios, engagement remains low

But are employees actually leveraging all of the tools at their fingertips? The data tells us otherwise. We measured how employees were engaging with apps by evaluating feature-level usage on a monthly basis (across all tools, for every employee with a license).

Our analysis puts average app engagement at 45%. In other words, less than half of the app licenses in an organization’s portfolio are being utilized on a regular basis. This means many companies are facing issues around license forecasting or tool adoption.

What’s particularly interesting is that tools purchased outside of IT have a higher average percentage of engagement, at 54%. The data indicates employees are finding more value in tools purchased by their business unit compared to apps managed and provisioned by IT.

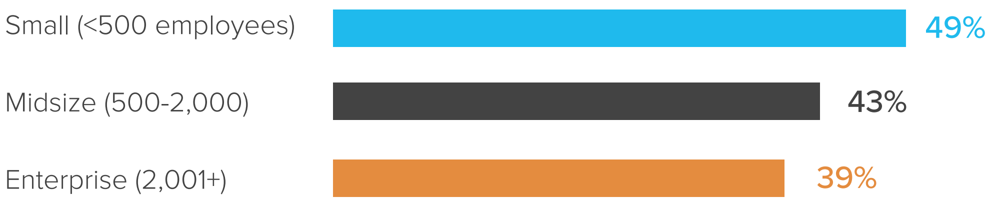
App engagement: Managed vs Shadow IT



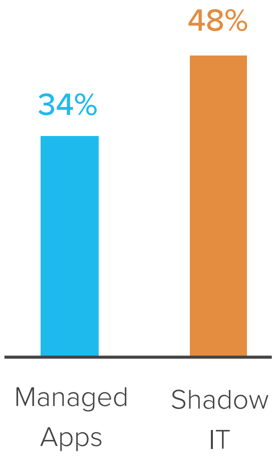
Larger businesses have lower app engagement on average

Looking at app engagement by business size, we discovered that larger organizations typically have lower app usage compared to midsize and small organizations. As we saw earlier, small businesses tend to have lighter SaaS portfolios and a higher percentage of Shadow IT. These factors help explain why small organizations have a higher average engagement rate.

App engagement by business size



However, a more detailed look at app engagement among enterprises shows an interesting contrast between Managed Apps and Shadow IT. Through this lens, we again find that Shadow IT apps have a significantly higher engagement rate on average compared to tools owned and managed by IT. Use of Shadow IT apps is 14 percentage points higher than those of Managed Apps.



Enterprise app engagement 14 percentage points higher among Shadow IT

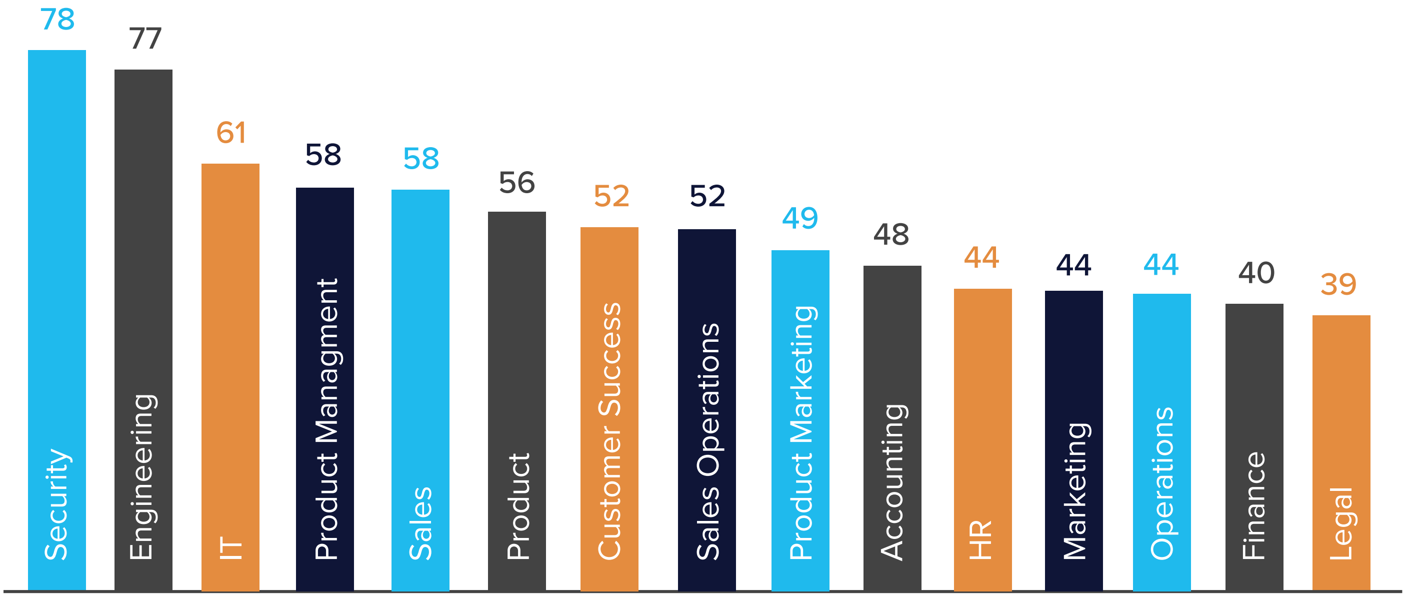
Teams are using dozens of apps on average

How is SaaS sprawl distributed across different departments? Our findings show that the majority of teams have between 40 and 60 apps, with a few outliers.

The top three departments with the highest number of tools were 1) Security, 2) Engineering, and 3) IT. In the case of Security and IT, these departments often have a high number of lower-touch tools that run in the background. Organizations of all sizes are prioritizing data protection and minimizing security risks, and many tools in this category are built for a very specific purpose.

Departments like HR and Marketing tend to use software suites with multiple modules such as Workday and Marketo. Therefore, it makes sense to see those teams at the lower end of the spectrum. The low averages for Finance and Legal departments may be due to smaller department sizes. Alternatively, that type of work is sometimes subcontracted out to a third party, which could also explain their position in the ranking.

Average Number of Apps



FUNCTION-SPECIFIC APPS

Key cross-functional apps dominate

Although most teams now have access to dozens of apps, a few tools stand out as the most popular cross-functional apps. Unsurprisingly, these include the two largest general business suites with email clients (Microsoft Office 365 and Google Workspace) as well as leading collaboration tools Slack and Zoom. The presence of Salesforce and Okta suggests those tools have also become top-tier choices in their respective markets.

MOST POPULAR CROSS-FUNCTIONAL APPS

slack
salesforce
Google Workspace
zoom
okta
Office 365

What's interesting is the breakdown of top function-specific apps across individual departments. We looked at 15 departments and saw the same tools being used in multiple teams. For example, Zendesk appeared as a top app for 4 departments: Security, Engineering, IT, and Customer Success.

The data shows us that teams are purchasing more tools than ever before, and yet the list of most popular function-specific apps shows significant overlap. These tools are likely essential for cross-department collaboration. If departments used different tools in these instances, organizations would experience greater fragmentation and employees would be less productive.

FUNCTION-SPECIFIC APPS

DEPARTMENT	KEY FUNCTION-SPECIFIC APPS
Security	ATLASSIAN Envoy zendesk GitHub CROWDSTRIKE
Engineering	ATLASSIAN PagerDuty zendesk aws Lucidchart Figma
IT	ATLASSIAN PagerDuty zendesk aws jamf
Product Mgmt	ATLASSIAN Lucidchart smartsheet
Sales	ATLASSIAN Lucidchart zoominfo Outreach DocuSign
Product	ATLASSIAN Lucidchart Figma tableau
Customer Success	ATLASSIAN zendesk GONG
Sales Operations	ATLASSIAN tableau asana
Product Mktg	ATLASSIAN Lucidchart asana box
Accounting	ATLASSIAN smartsheet Concur NETSUITE Adobe DocuSign
HR	workday. DocuSign greenhouse
Marketing	asana Figma Dropbox Marketo™
Operations	ATLASSIAN asana Lucidchart DocuSign
Finance	Expensify NETSUITE Adobe DocuSign
Legal	Expensify Envoy box DocuSign

Differences in compliance rates reveal mixed app security frameworks

So you likely have hundreds of apps in your portfolio, and Shadow IT is flourishing. How does that affect your security risk surface? To find out, we analyzed compliance across 7 certifications:

- CCPA
- FedRAMP
- FISMA
- GDPR
- ISO27001
- SOC2
- Swiss-US Privacy Shield

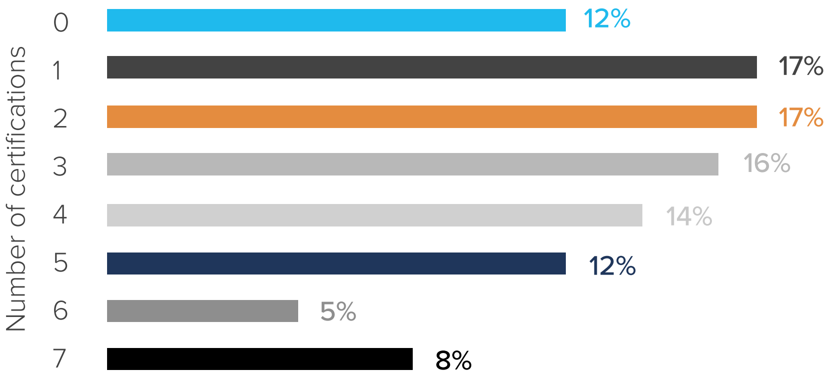
83% of apps 3 or fewer certifications

Of the apps we looked at, 83% had 3 or fewer security and compliance certificates. IT leaders may be making security and compliance a key priority as data grows more distributed, but our analysis reveals that many apps still may not meet industry compliance standards.

12% of apps have no certifications, and FISMA has the lowest compliance of all certifications

In addition to discovering the vast majority of apps had a maximum of 3 certifications, we were also surprised to find that 12% of tools had zero compliance certifications published. The most common number of certifications was 1 or 2, with 17% of apps compliant with those quantities of certifications.

Percentage of compliance certifications

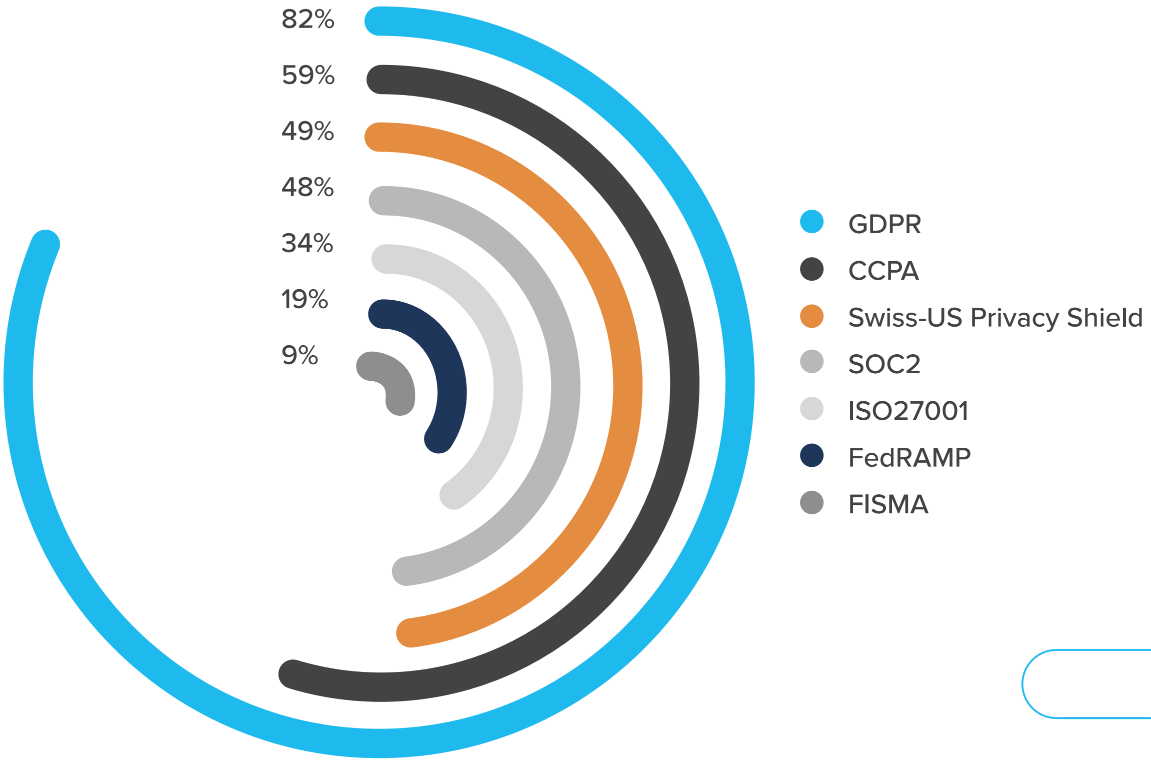


COMPLIANCE

We also found large variations in compliance rates across the specific certifications. GDPR had the highest compliance rate, with 82% of the apps we analyzed meeting that certification. On the flip side, FISMA had the lowest compliance rate at 9%.

FISMA is a less common US regulation that applies to federal agencies and private businesses who conduct work with federal agencies, which may explain why compliance was so low.

Average percent of compliance certifications



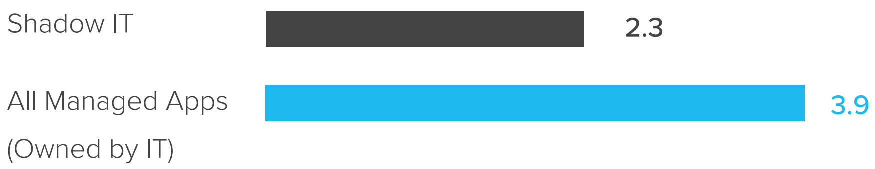
Shadow IT apps pose more risk with fewer compliance certifications

How does the picture of app compliance change when you zoom in on Shadow IT? Per our analysis, Shadow IT tools have 2.3 compliance certificates on average. Conversely, Managed Apps have an average of 3.9 certificates. Simply put, tools owned outside of IT may pose a greater risk to your data security.

The growth of Shadow IT and the certification trends of those tools reinforces the need for complete visibility. It's just as important to keep an eye on your Shadow IT apps as it is to audit your Managed Apps. Being able to effectively monitor and mitigate security risks today extends beyond the apps that IT owns.

Tools owned outside of IT may pose a greater risk to data security.

Average compliance certifications:
Managed vs Shadow IT

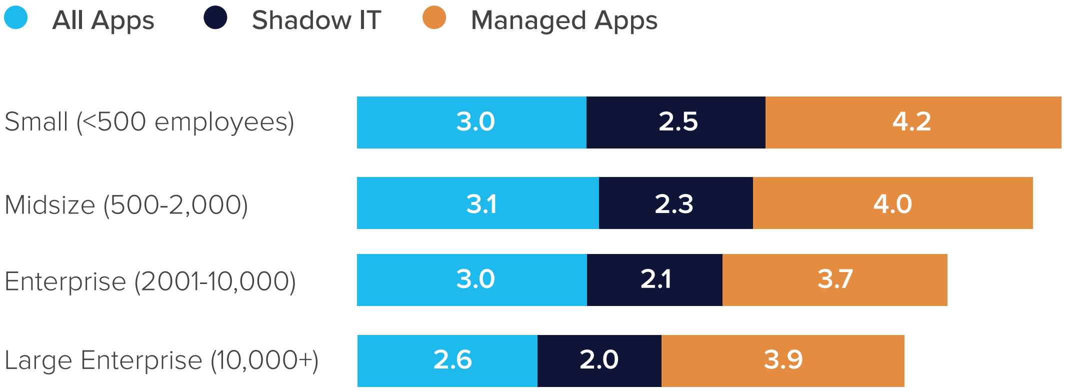


Small business tools are more compliant on average

Despite typically using more Shadow IT, smaller organizations have a higher average of compliance certifications across Shadow IT and Managed Apps. Small businesses may be leveraging younger, forward-thinking tools with higher numbers of certifications, whereas large companies may have more established app suites that can be slower to adopt industry trends.

However, overall the difference in number of certifications is relatively minimal across businesses of all sizes. Across both Shadow IT and Managed Apps, tools used by small businesses have 3 compliance certifications on average compared to 2.6 certifications among large enterprises.

Average compliance certifications by company size



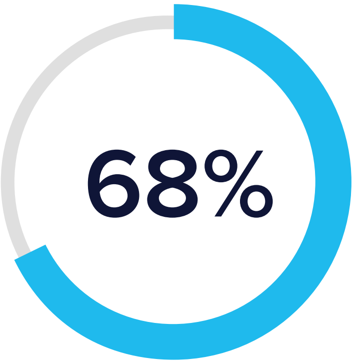
SSO use more prevalent among enterprises

Compliance certifications are one indicator for evaluating security and compliance risks in your SaaS portfolio, but we wanted a more comprehensive view. To get there, we also looked at how companies use SSO across their apps. SSO allows IT teams to better secure and control who has access to critical business apps.

The caveat here is that companies tend to use SSO for Managed Apps, or tools that IT owns and manages. (Since IT doesn't generally own or manage Shadow IT apps, that makes it difficult to identify such tools as candidates to put behind SSO.) For the purposes of this analysis, we only examined data pertaining to Managed Apps.

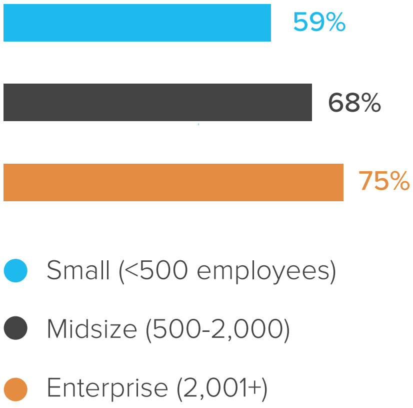
Although SSO has grown increasingly popular, we found that almost one-third of Managed Apps were not behind SSO. Many organizations appear to have integrated SSO throughout the majority of their Managed Apps but may face logistical or financial challenges with the remaining ungated Managed Apps.

SSO use also varies significantly by business size. Enterprise organizations have the highest usage, with 75% of Managed Apps behind SSO on average. Smaller businesses are lagging behind with less than 60% of Managed Apps currently behind SSO. The lower percentage for small companies may be in part due to resource constraints and more lax security policies.



Managed Apps behind SSO

% of Managed Apps behind SSO by company size



CONCLUSION

How can you apply these findings to your organization?

As our report reveals, businesses are shifting further away from centralized management of their SaaS apps. The reality of remote work and Shadow IT makes it all the more difficult for you to achieve complete visibility of your entire app portfolio. We recommend taking the following actions to improve oversight of your SaaS tools:

1. **Take inventory of all SaaS apps currently in use**

   Conduct regular audits of your SaaS tools. That can involve monitoring your network for unknown apps, surveying employees, partnering with Finance to identify expensed app purchases, and more. Or you can use Productiv, which automates many of these actions to give you complete real-time visibility of your SaaS app portfolio — no manual audit necessary.

2. **Understand how employees are using the tools available to them**

   Take steps to find out what users are doing beyond whether they're logging in: which features are they using, who are they collaborating with, which devices are they accessing from, and more. Request user reports from your SaaS vendors or ask for feedback from employees. This information can help you determine whether you're getting value out of the apps you're paying for — and if not, help you take action to increase user engagement.

3. **Look for opportunities to consolidate duplicate apps**

   You likely have multiple apps with overlapping functionality, such as different project management tools for different teams. Duplicate apps can cost you more money, create data silos, increase your security risk surface, and cause fragmentation among your workforce. You can categorize apps to pinpoint where you might have multiple tools serving the same purpose.

4. **Track app compliance and leverage SSO**

   To track compliance, we recommend you start by focusing on your critical business apps and reviewing their websites for compliance certifications. If you have an SSO provider, look at which tools aren't behind SSO yet and figure out what obstacles are preventing that from happening. If you don't use SSO, you may want to consider a provider like Okta.

You can also leverage Productiv's SaaS Intelligence Platform to simplify and easily manage your complex SaaS portfolio. We do it all — help you track all of your apps, tell you how employees are using them, enable you to compare tools with similar functionality, and monitor app compliance.

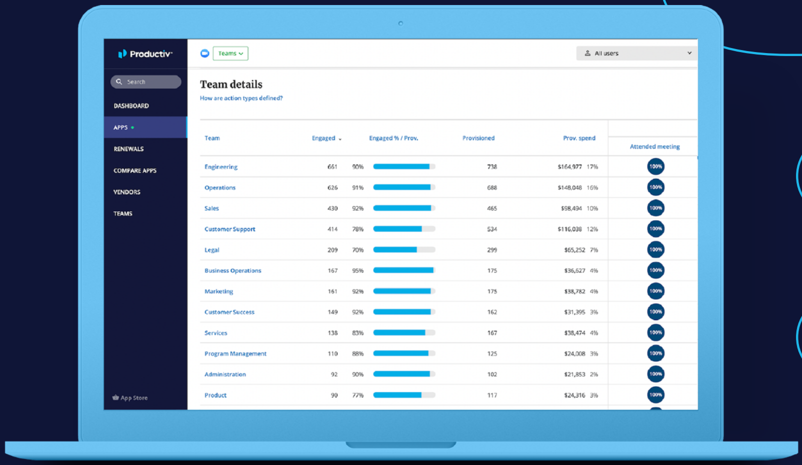
METHODOLOGY

About the report

The findings in this report are based on analysis of anonymized data from businesses using Productiv. We looked at hundreds of active instances of the Productiv platform, which included data on more than 30,000 applications.

Productiv tracks Shadow IT, or what we refer to within our platform as Discovered Apps, by aggregating data from HR systems, finance and expense management software, contract management tools and files, and SSO and CASB providers. For the purposes of this report, we categorized apps as Shadow IT based on non-managed applications with a data source from 1) an expense or finance system, 2) network monitoring tools, or 3) Google single sign-on (SSO).

The Productiv SaaS Intelligence Platform uses proprietary app integrations that provide rich insights into feature-level usage. Our integrations go beyond login data to standardize the measurement of user engagement across all apps. For this report, we based all engagement data on a 60-day period of usage and calculated engagement using the number of purchased licenses for each app across every instance.



Team details

How are action types defined?

Team	Engaged	Engaged % / Prov.	Provisioned	Prov. spend	Attended meeting
Engineering	661	90%	738	$164,977 17%	100%
Operations	626	91%	688	$148,048 16%	100%
Sales	430	92%	465	$98,494 10%	100%
Customer Support	414	78%	534	$116,038 12%	100%
Legal	209	70%	299	$65,252 7%	100%
Business Operations	167	95%	175	$36,627 4%	100%
Marketing	161	92%	175	$38,782 4%	100%
Customer Success	149	92%	162	$31,395 3%	100%
Services	138	83%	167	$38,474 4%	100%
Program Management	110	88%	125	$24,008 3%	100%
Administration	92	90%	102	$21,853 2%	100%
Product	90	77%	117	$24,316 3%	100%

Productiv™

Productiv is the comprehensive SaaS Intelligence Platform that automates critical workflows, increases visibility and security of your SaaS portfolio, and helps you understand exactly how employees use your apps. We help leading enterprise organizations like Uber, Zoom, and Square solve their complex SaaS challenges.

Want to see why we're the trusted provider of SaaS management for enterprises?

Schedule your demo.