BetterCloud

State of SaaSOps

2021

BetterCloud

TABLE OF CONTENTS

Welcome to the 2021 State of SaaSOps

Since 2012, we've been surveying IT professionals and publishing research to better understand what the shift to SaaS means for IT, end users, and the broader organization. Every year we explore IT's biggest challenges and concerns, trends in SaaS adoption, and what the future holds—making this the industry's largest and longest running research of its kind.

This year's survey of 523 IT and security professionals reveals the latest challenges of managing SaaS at scale, particularly as digital transformation catapulted forward in 2021—and IT kept the momentum going. It also sheds new light on SaaS file security, the state of SaaSOps automation, the workplace of the future, and more.

We're excited to share the results here. We hope these insights help you evolve your SaaSOps practice and thrive through change.

BetterCloud

Here's a look at the key findings that stood out.

SaaS adoption continues to explode.

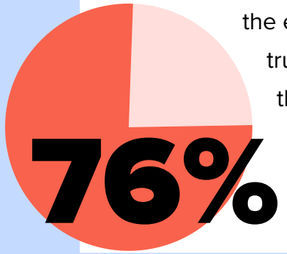
In a year like none other, organizations have embraced SaaS faster than ever before. Up from an average of 80 apps last year, this year organizations use **110**, for a **38%** increase. This is nearly a **7x** increase in SaaS app usage since 2017, and almost a **14x** increase since 2015.

2020
80 APPS

2021
110 APPS

In response to the past year, IT's role is becoming more strategic.

This past year, IT's role shifted from functional to strategic. They're solving challenges with SaaS, transforming the employee experience, and becoming trusted business partners—ultimately leading the way to tomorrow's workplace.



76% **of respondents report being more or much more strategic over the last 12 months.**

More SaaS brings more challenges.

More than half (55%) of respondents say the most crucial challenge to solve is

lack of visibility

into user activity and data. The next two biggest challenges? Knowing all SaaS apps in use and consistently managing app configurations.

The well-meaning but negligent employee poses the biggest data loss threat—by far.

72% **of organizations say it's the well-meaning employee**

When it comes to data loss, the biggest threat is not from hackers or saboteurs. Instead, **72%** of organizations say it's the everyday employee who has good intentions and is just trying to do their job, but may inadvertently expose sensitive information along the way.

Levels of SaaSOps automation will nearly double in the next 3 years.

SaaS-Powered Workplaces report that

45% **of their SaaS operations is already automated**

and estimate it will rise to nearly

80% **within the next three years.**

The SaaSOps role is here to stay.

60% of respondents already use the term "SaaSOps" in their job title/description or plan to include it in the future—**a 100% increase from last year.**

SaaS creates new security concerns for IT.

Lack of visibility is a pervasive challenge: 55% of respondents say their biggest security concern is not knowing where sensitive data exists.

69% of IT professionals are concerned about unsanctioned SaaS apps creating security issues. Additionally, **46%** say they have difficulties securing user activities within SaaS apps. This year SaaS file security violations have spiked **134%**, and the number of files containing PII has grown **1944%** year over year.

The future of SaaSOps is now.

When asked about the future of SaaSOps, more than **40%** of respondents wrote that it's "mission critical" or "essential in IT."

1

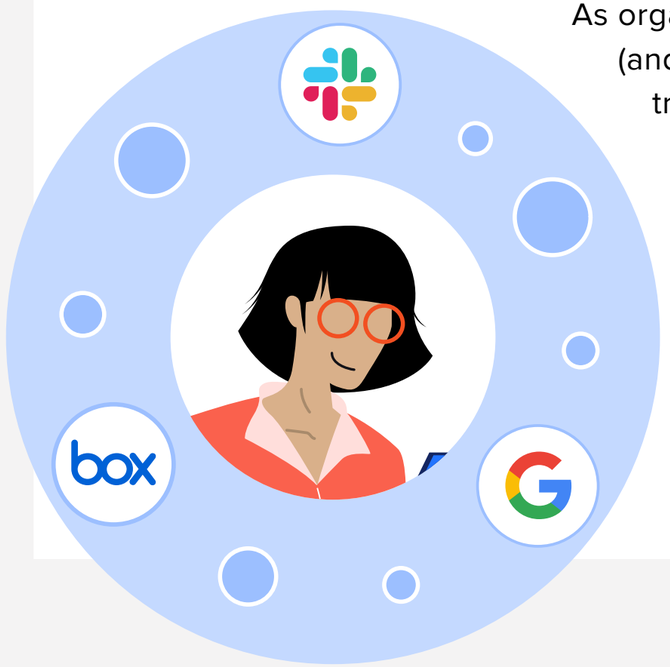
SaaS in the Workplace

SaaS adoption continues unabated, as organizations use an average of 110 SaaS apps in 2021

38%
Growth in number of SaaS apps since last year

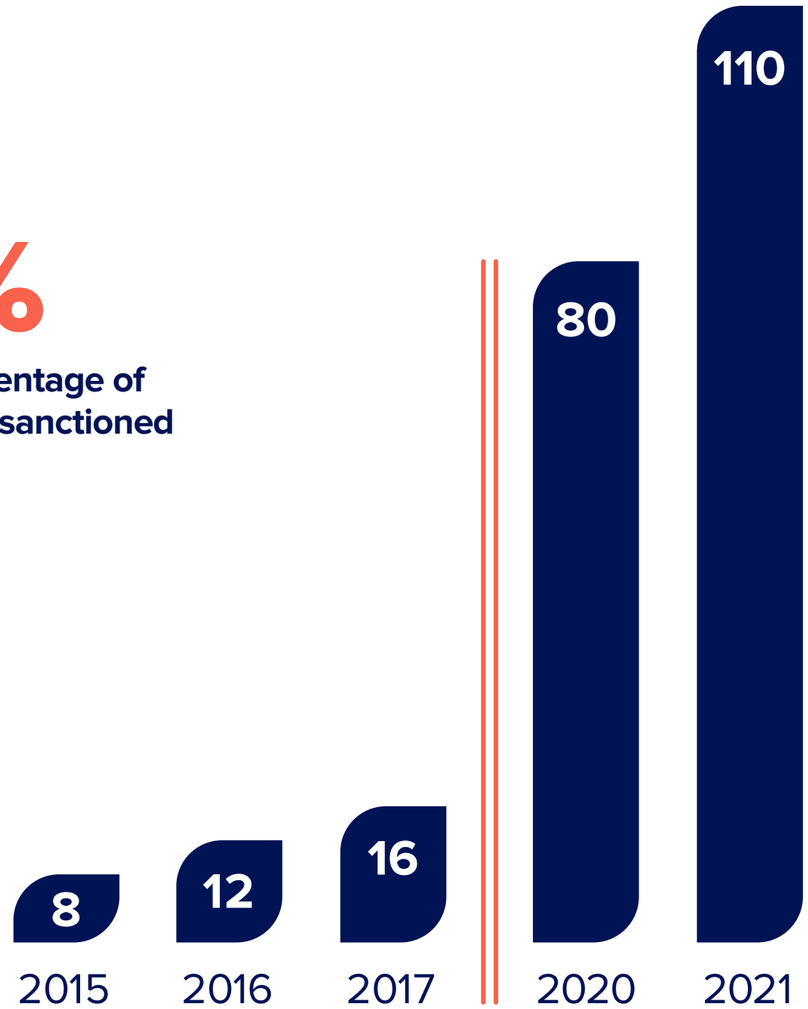
1275%
Growth in number of SaaS apps since 2015

53%
Average percentage of apps that are sanctioned



As organizations continue to embrace (and accelerate) their digital transformation journeys, SaaS adoption remains unabated. Up from an average of 80 apps last year, **this year organizations use 110 apps, for a 38% increase**. This is nearly a **7x** increase in SaaS app usage since 2017, and almost a **14x** increase since 2015.

Number of SaaS apps used per organization

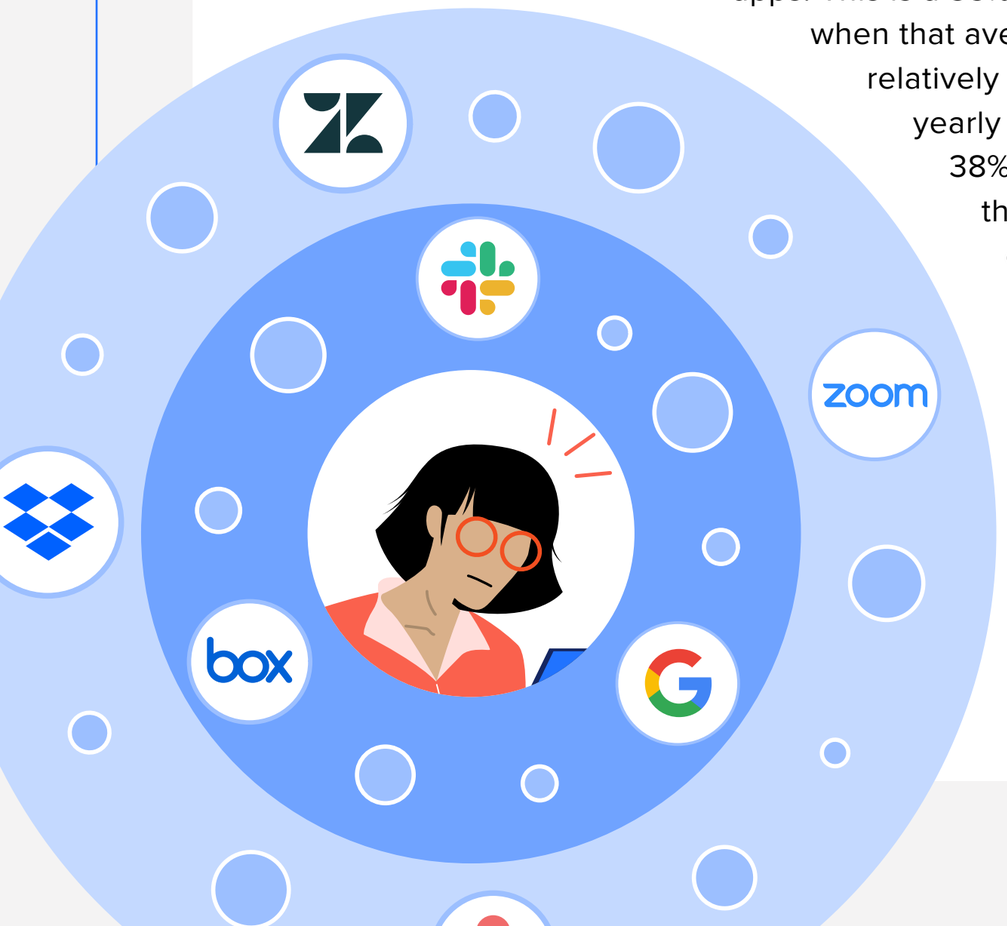


Large enterprises use an average of 447 SaaS apps

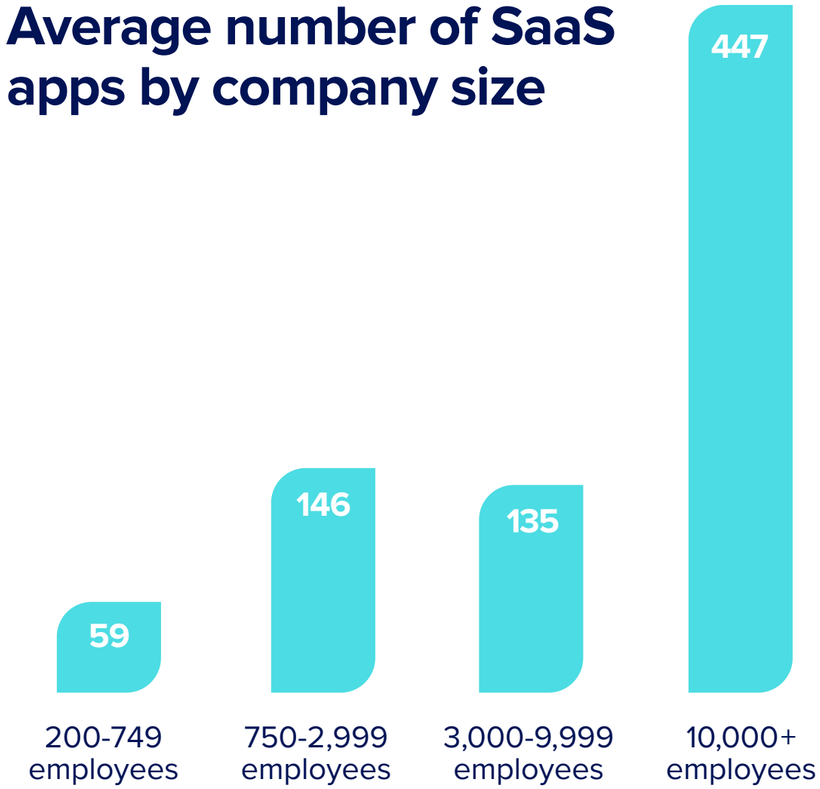
Predictably, the average number of SaaS apps an enterprise uses varies by company size.

In 2021, enterprises with less than 750 employees use about 60 different SaaS apps, while mid-sized organizations use about 140.

Meanwhile, large enterprises use nearly 450 SaaS apps. This is a 35% increase since last year, when that average was 332, and it's relatively in line with the overall yearly SaaS growth rate of 38%. However, considering the usual slower pace of large enterprises, it suggests SaaS adoption is accelerating in that segment.



Average number of SaaS apps by company size



"SaaSOps will continue growing within organizations as SaaS becomes the standard, replacing legacy and traditional on-prem applications."

— VP of IT at manufacturing company with 1,250 employees

Every organization will eventually become a SaaS-Powered Workplace

As SaaS adoption continues to reach dizzying heights, a new type of workplace has clearly emerged: the SaaS-Powered Workplace. These are organizations that are running almost entirely on SaaS. But of course, not every organization is as reliant on SaaS yet. Three segments stood out in our study, all with varying levels of SaaS maturity, which illustrate how the digital workplace is evolving:

SaaS-Powered Workplaces

Top 15% of study

212
Average number of SaaS apps

93%
of their apps are SaaS-based

Workplaces in Transition

Middle 70% of study

79
Average number of SaaS apps

55%
of their apps are SaaS-based

Traditional Workplaces

Bottom 15% of study

39
Average number of SaaS apps

8%
of their apps are SaaS-based

Many organizations are still in the early stages of their SaaS adoption journey. But the data clearly reveals that they too are trending in the same direction as SaaS-first workplaces. **SaaS has crossed the chasm—and at some point, every organization will become a SaaS-Powered Workplace.**

In the process of embracing SaaS apps, SaaS-Powered Workplaces are paving new SaaSOps ground. They provide a glimpse into the future, revealing the challenges that come with managing SaaS at scale. Thanks to their pioneering ways, other organizations can see around the corner and learn how to successfully navigate future challenges.

SaaS-Powered Workplaces are committed to creating a productive digital workplace through SaaS operations (SaaSOps)

So there's one conclusion we can already make: SaaS is integral to how IT empowers the business.

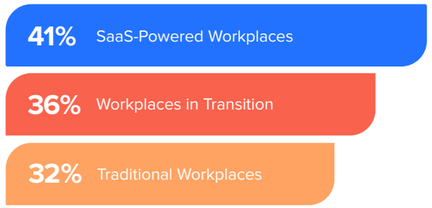
In fact, more than **80%** of SaaS-Powered Workplaces agree or strongly agree that they create a modern digital workplace to **improve end user productivity**. In today's era of remote work, frictionless employee experience matters now more than ever. Employees want to feel productive and empowered to use the SaaS tools they need to best do their jobs. SaaS-Powered Workplaces are keenly aware of this expectation. They aim to enable collaboration and productivity, removing friction from the business.

SaaS-Powered Workplaces are also more apt to trust end users to be responsible with company data than Traditional Workplaces.

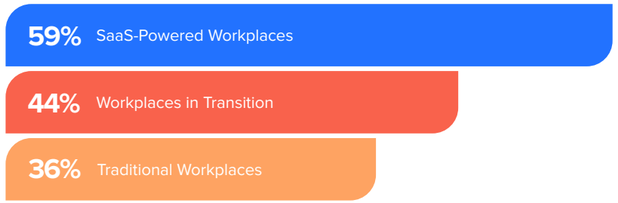
And SaaS-Powered Workplaces are likelier than Traditional Workplaces to back up their commitment with IT budget dollars. While only 36% of Traditional Workplaces agree that they spend enough on SaaS operations (SaaSOps), nearly **60%** of SaaS-Powered Workplaces agree they do. As organizations start to rely more on SaaS, there is a clear shift in priorities, budgets, and end user trust.

> *"For us, the future of SaaSOps is to keep securing [our environment] as best as we can, while trying to ensure the end user doesn't have to jump through hoops for simple tasks."*
>
> **— Senior director of IT at advertising company with 250+ employees**

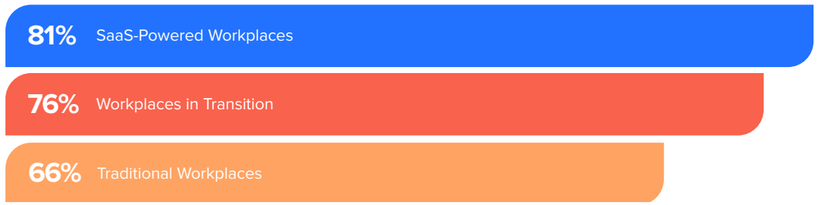
Trusts end users to responsibly share and store company data
% agree/strongly agree



Allocates enough budget to SaaS operations
% agree/strongly agree



Creates a modern digital workplace to improve end user productivity
% agree/strongly agree



LEGEND

SaaS-Powered Workplaces
Workplaces that are almost entirely running on SaaS today. Comprised of the top 15% of our study, these orgs are 93% SaaS-based today.

Workplaces in Transition
Workplaces that are using a mix of SaaS and on-prem tools. Comprised of the middle 70% of our study, these orgs are 55% SaaS-based today.

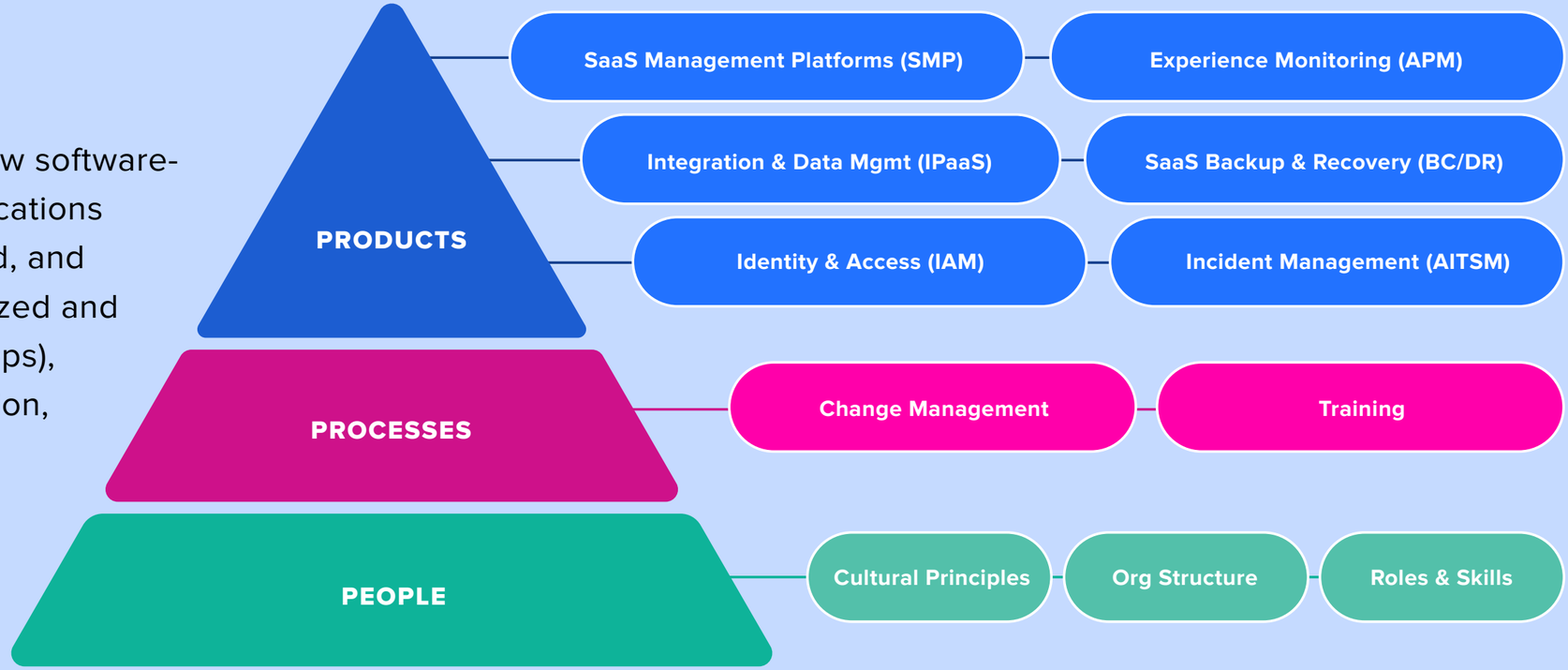
Traditional Workplaces
Workplaces that are primarily using on-premise tools. Comprised of the bottom 15% of our study, these orgs are 8% SaaS-based today.

SaaSOps includes people, processes, and technologies

SaaSOps is a practice area for IT professionals that aligns products, people, and processes to effectively support a “best-in-breed” software strategy and drive broader organizational transformation.

SaaSOps *noun*

a practice referring to how software-as-a-service (SaaS) applications are discovered, managed, and secured through centralized and automated operations (Ops), resulting in reduced friction, improved collaboration, and better employee experience



SaaSOps successfully enables remote work: Most SaaS-Powered Workplaces are still majority remote

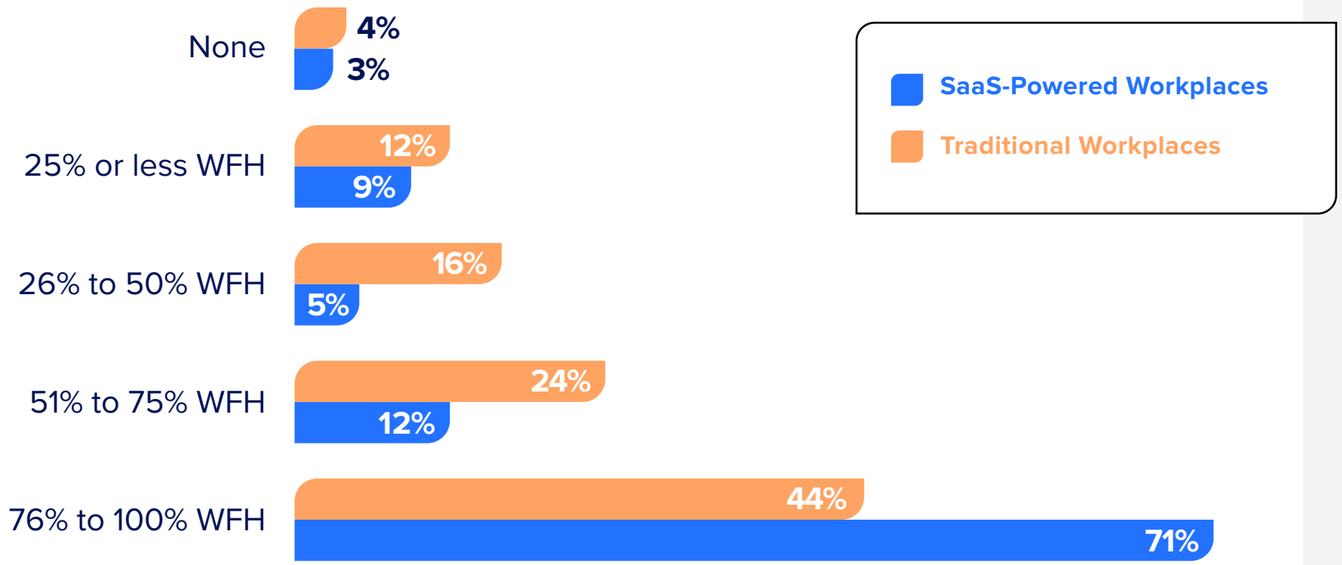
In 2020, most organizations went home and went online.

Overall, in 2021, **half of all organizations** said that three-quarters to all employees are still working from home (WFH).

But when you compare SaaS-Powered Workplaces to Traditional Workplaces, there's a dramatic difference. More than **70%** of SaaS-Powered Workplaces are majority remote compared to only 44% of Traditional Workplaces. With their heavy SaaS usage, many SaaS-Powered Workplaces already have the tools employees need to be productive, even when working remotely. And as organizations contemplate long-term remote and hybrid plans, SaaSOps takes on a heightened importance.

> *"The pandemic has pushed companies to work in dispersed, remote, and hybrid models, which impacts all phases of the employee lifecycle—from pre-hire to offboarding. This will make SaaSOps a bigger need than before."*
>
> — **Director of IT systems at e-commerce company with 1,800 employees**

Percentage of employees that work from home



But more SaaS brings more challenges—and the most crucial one to solve?

Lack of visibility

The number one challenge according to our respondents is **lack of visibility into all user activity and data files/folders.**

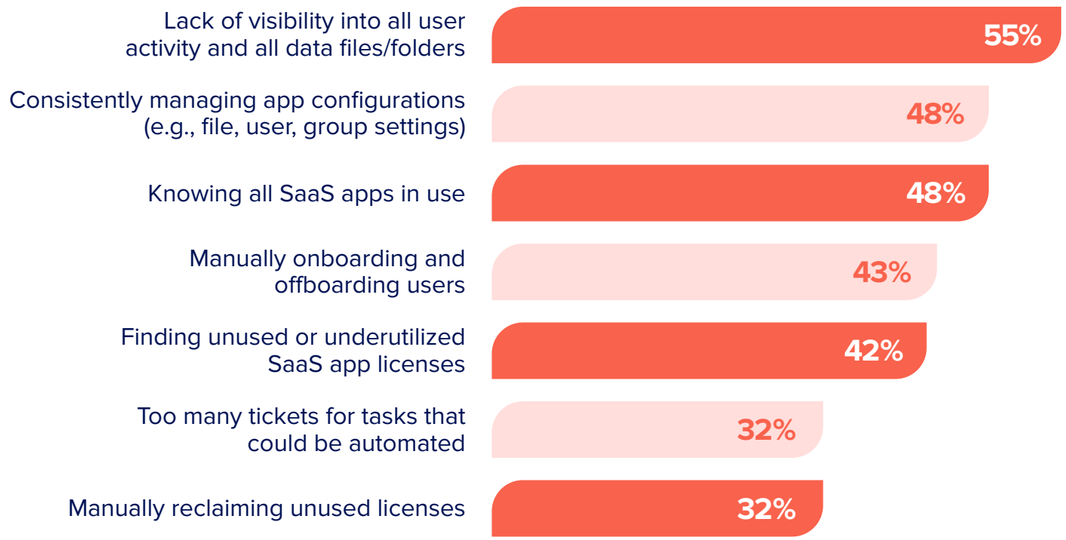
What data are users downloading, sharing, exporting, and forwarding? Where does sensitive data live? What apps are employees using?

Without visibility and actionable insights into their SaaS environment, IT is flying blind. And as SaaS adoption continues to massively climb, these challenges only compound.

Most notably, the SaaS-Powered Workplaces had a different challenge land at the top of their list. When you consider their average of 212 SaaS apps, it's not surprising that over half (52%) of them said **manually onboarding and offboarding users** was their most crucial challenge to solve.

In the next sections of our report, we'll dive into some of the biggest challenges in more detail.

Challenges most crucial to solve in SaaS environment



**Respondents were asked to select their top three challenges*

2

Understanding the Challenge of SaaS Visibility

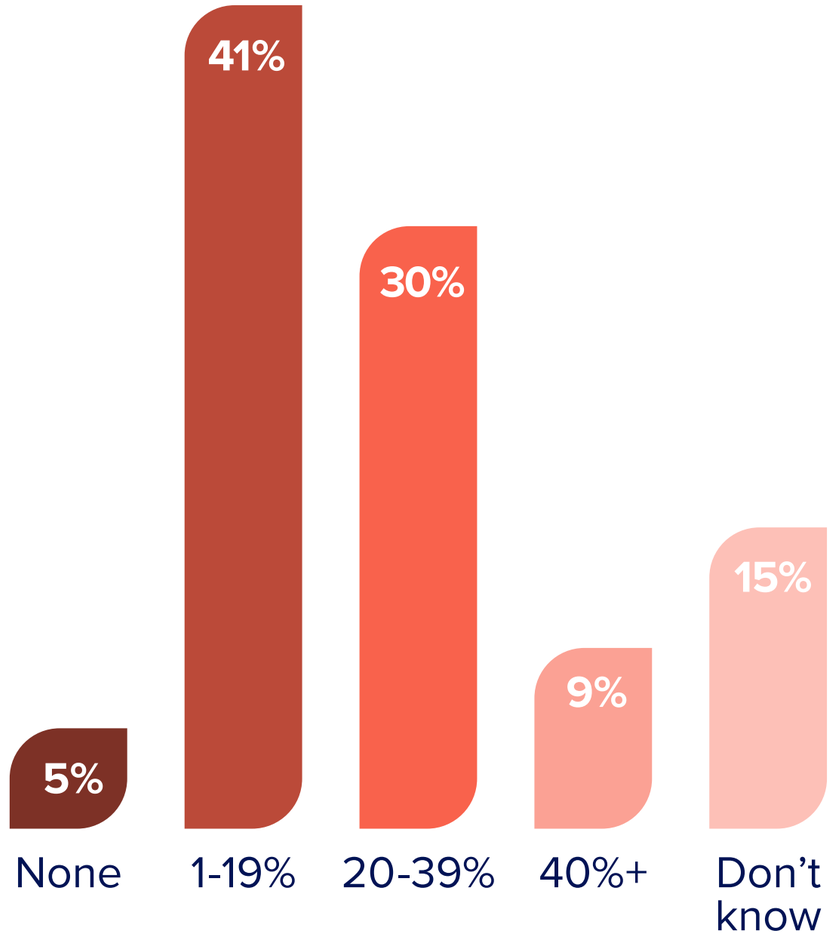
Lack of visibility results in wasted SaaS spend

Lack of visibility, as we just learned, was the most cited challenge across respondents. But it's also related to other challenges on the list, like **finding unused or underutilized SaaS app licenses** (*finding* being the operative word here). 42% of respondents said this was one of their most crucial challenges to solve. And indeed, **80%** of respondents concede that some percentage of their SaaS spend *is* being wasted.

License waste comes in many flavors. It could be the apps that go unloved and unused. It could be similar apps solving the same use case, like having six different project management apps across the business. It could be different departments using the exact same app, only with different accounts. In all of these cases, there are massive untapped opportunities to cut costs and properly allocate licenses. **But without visibility, it's incredibly difficult to identify these opportunities.**

So how much of total SaaS spend is wasted on unused or underutilized SaaS licenses? **Nearly a third said between 20-39%**—which can mean thousands (or even millions) of dollars, depending on your SaaS spend. Additionally, 41% said it's somewhere less than 20%.

Percent of total SaaS spend that is wasted on unused or underutilized licenses



To recoup costs, more than 60% of SaaS-Powered Workplaces get busy consolidating redundant SaaS apps

To combat license waste and recoup costs, more than 60% of SaaS-Powered Workplaces actively consolidate apps with redundant use cases. Only 20% of Traditional Workplaces do the same. Since they're still in the early stages of their SaaS adoption journeys, Traditional Workplaces likely don't have many redundant apps yet—but will reach that point eventually as SaaS proliferates.

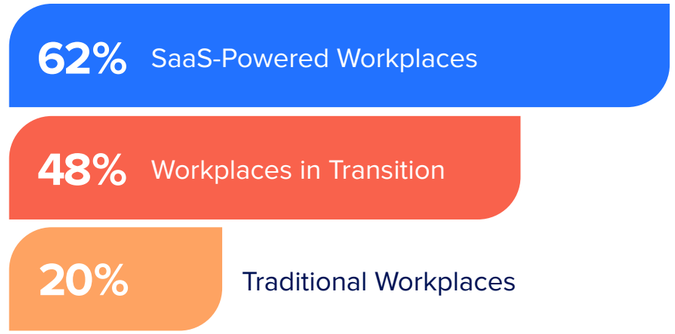
Similarly, only 12% of Traditional Workplaces actively work to remove unsanctioned SaaS apps, whereas 33% of SaaS-Powered Workplaces do. These apps, which are being used without IT's approval or knowledge, can pose a security risk. But while SaaS-Powered Workplaces might be removing more unsanctioned apps, in many cases they are learning more about how they're used—and working together with users to identify a better or more secure option.

As SaaS adoption accelerates, unwieldy SaaS sprawl becomes an inevitable challenge for every organization. This data illustrates the types of activities that the most SaaS-forward organizations are undertaking to rein in SaaS sprawl and save on costs. After all, since SaaS is easy to buy and hard to manage, consolidating redundant apps saves both money and time. Furthermore, getting rid of unsanctioned apps is key to a strong security posture.

In the next section of the report, we'll explore the latest trends in SaaS security, particularly around file security.

> *"SaaSOps will only continue to grow, especially if cost savings become more easily defined."*
>
> — **Director of IT at consulting company with 520 employees**

Consolidate redundant SaaS apps



Remove unsanctioned SaaS apps

3

Trends in SaaS File Security

Organizations say they learned the hard way: 45% recently experienced security policy violations

In the past year, IT has experienced its fair share of security incidents.

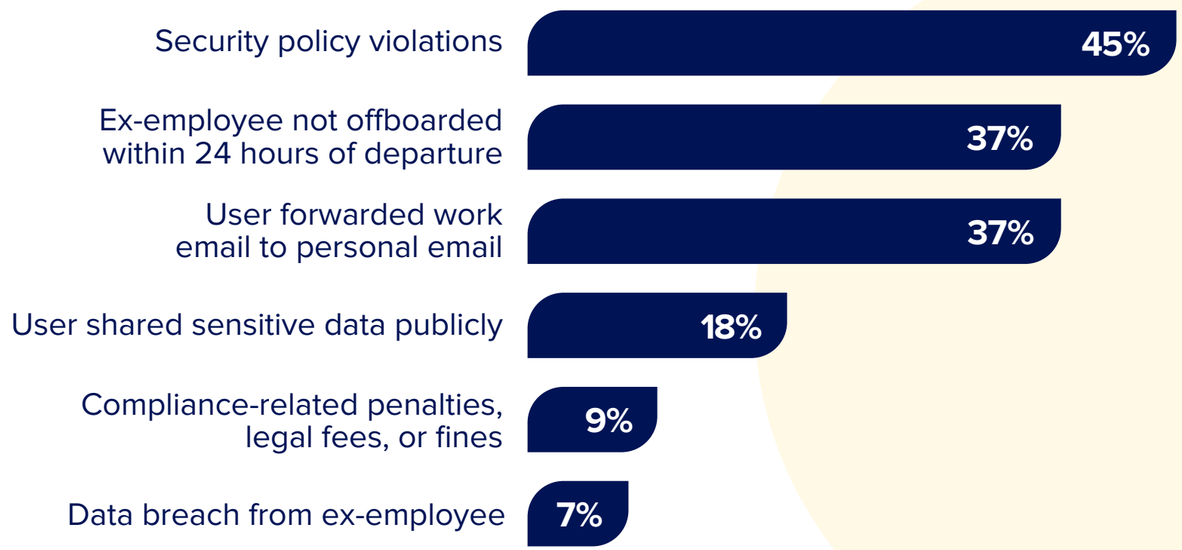
Nearly half of respondents (45%) reported security policy violations in the past 12 months.

Violations can occur for a number of reasons. Employees may flout rules for the sake of convenience, or they simply may not be aware of security policies in place.

For more than a third **(37%)** of respondents, prompt offboarding was a challenge. **37%** also reported instances of users forwarding work emails to their personal email addresses. Both of these can put your company at risk of compliance violations, data loss, and data exposure. For example, if exiting employees are not offboarded in a timely manner, they can leak, alter, or destroy sensitive data, or take it to their new employer. And while email forwarding might seem innocuous at first blush, if an email contains sensitive information like PHI, it can result in compliance violations and sensitive data exposure.

And yet another **18%** said users shared sensitive data publicly. It all gives rise to the importance of knowing how—and where—to protect sensitive SaaS data.

Security-related experiences within last 12 months



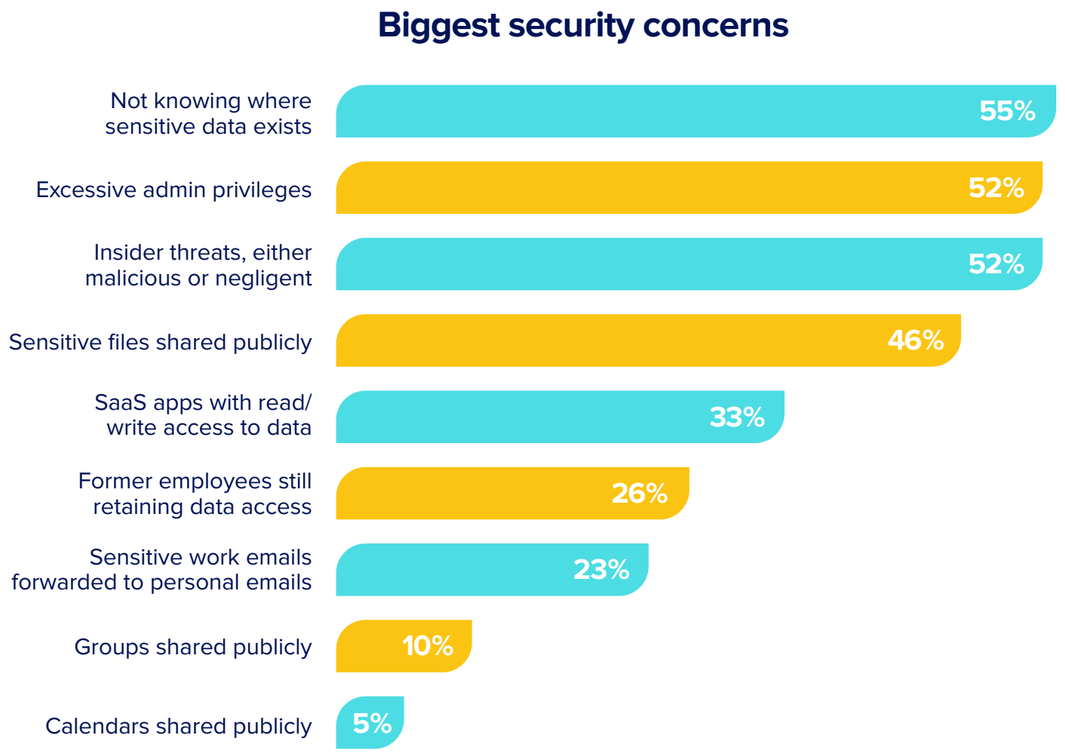
The biggest security challenge: not knowing where sensitive data exists

Earlier in the report, we learned that visibility was a major challenge for IT teams. So it's not surprising, then, that the biggest security challenge plaguing IT when it comes to SaaS is **not knowing where sensitive data exists**. If you don't know where your data resides, you can't protect it.

Additionally, information lives in multiple places. You can share Drive and Dropbox files in Slack. You can install connected apps (like Chrome extensions, Slack bots, or marketplace apps) with a click of a button. Many SaaS apps work together in some way.

Other security concerns keeping IT up at night: excessive admin privileges (52%), insider threats (52%), and sensitive files shared publicly (46%).

SaaS cuts both ways. While SaaS is a gamechanger for productivity, it also gives employees new levels of control over critical company assets. And with this new control comes new risks related to app misconfigurations, excessive permissions, and uncontrolled file sharing.



**Respondents were asked to select their top three concerns*

"I think the future of SaaSOps is transitioning from basic automations into a more security-focused practice. We saw this with DevOps and the 'shift left' movement, and it makes sense for SaaSOps too. Once we've tackled many of the repetitive or complicated tasks, security is next on the list." **— VP of IT at advertising company with 550 employees**

Unsanctioned apps add to SaaS security woes

It's never been easier for end users to procure and deploy SaaS by themselves. These unsanctioned apps have emerged as a top concern for IT.

Nearly three-quarters (69%) of our respondents worry about unsanctioned SaaS apps.

Unknown, unsanctioned apps can introduce risk since they're not secured or monitored by IT. Although SaaS has never been more powerful and easy to use, IT teams need to understand how each application interacts with data across the organization. Additionally, IT needs to ensure that each SaaS provider follows the highest security standards.

By design, SaaS provides a lot of freedom. To get work done, users can share files publicly, assign elevated admin privileges, upload sensitive data, create public groups, and more. But without full visibility into their SaaS stack, organizations of all sizes also struggle to secure user activities within SaaS apps. As a result, it's not surprising that nearly half (**46%**) of respondents say they **have difficulties securing user activities**.

46%

Have difficulties securing users' activities within SaaS apps

69%

Concerned about unsanctioned apps creating security issues

The greatest risk to data loss is the well-meaning but negligent employee

According to our respondents, the greatest risk to data loss isn't the hoodie-wearing hacker or disgruntled employee. Overall, a whopping **72%** of organizations feel that the greatest risk to data loss is the **well-meaning employee who unwittingly shares sensitive information**. These employees have good intentions and are just trying to do their jobs, but often lack the training or knowledge to keep sensitive information safe. Because they have access to confidential data and systems, it's critical to implement thoughtful and thorough security training and develop a healthy security culture as well.

> *"SaaSOps has a permanent future."*
>
> **— Senior security engineer at SaaS company, 800 employees**

SaaS-Powered Workplaces are even more acutely aware of these risks, with **83%** of them feeling this way. Because SaaS was designed to foster productivity, users have full control over how they share data and with whom. Employees who are merely trying to get work done or circumvent friction may share data publicly across the organization (or even publicly on the internet) without realizing the implications of their actions. Default sharing settings can also be broad—for some organizations, too broad. The nuances of sharing settings can also be confusing, as they vary from app to app. As a result, it can be easy for well-meaning employees to unintentionally expose data.

Actor posing greatest threat to data loss

FILE SECURITY RISK REALITY CHECK

File security violations lurk throughout the average organization

Average number of public files	Small (200-749)	Medium (750-2,999)	Large (3,000-9,999)	Very Large (10,000+)
In your cloud storage apps	88,952	269,928	148,543	17,708
In your cloud productivity suite	71,987	51,894	122,022	2,142,814

Average number of files with sensitive data	Small (200-749)	Medium (750-2,999)	Large (3,000-9,999)	Very Large (10,000+)
With U.S. Social Security numbers, credit card numbers, or passwords	102,685	52,304	191,564	464,163
With general personally identifiable information	49,978	29,659	98,388	128,368

The top 5 most common types of sensitive data stored in cloud apps:

5. U.S. passport numbers
4. Social Security numbers
3. U.S. driver's license numbers
2. Security codes
1. Login keywords

1944%

Year-over-year growth in files containing PII

Organizations today trust SaaS vendors to house their most mission-critical, sensitive data, so it's not surprising that file security is top of mind. With SaaS, it's all too easy to share data publicly across the domain, or even publicly on the internet.

If you're wondering just how common file exposures are, this table shows the average number of violations that occur for organizations like yours.

Source: Internal BetterCloud data, June 2021

Only 18% of IT organizations consistently monitor their SaaS environment to ensure that confidential data isn't shared publicly

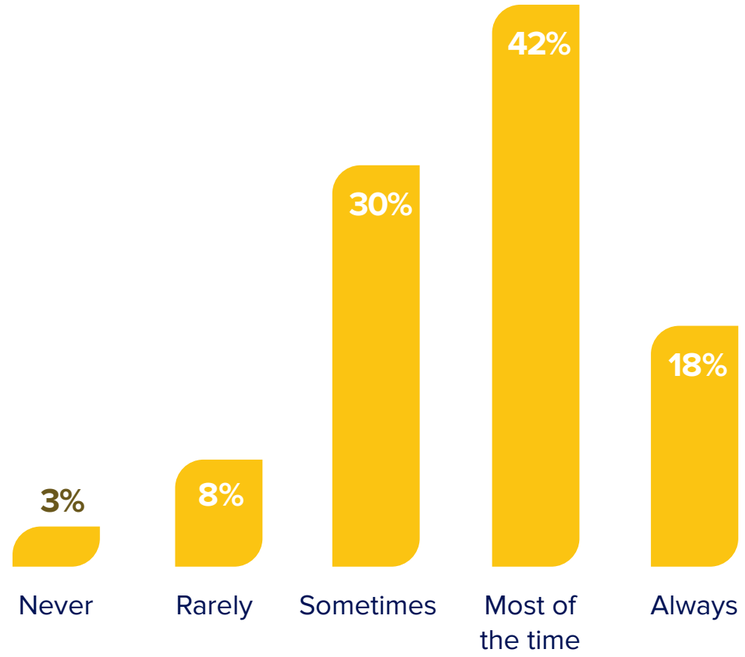
SaaS-Powered Workplaces do slightly better, with 23% of them saying they always monitor for confidential data exposure. That number drops to 12% for Traditional Workplaces.

Overall, 42% of respondents say they monitor *most of the time*, and 30% say *sometimes*.

At any given moment, users are creating sensitive data data, editing it, and/or sharing it both within and outside the organization. IT is tasked with knowing where the most sensitive data exists and securing it. With every day that goes by without regular and automated SaaS file scans, organizations run the risk of data exposure and potentially costly compliance violations.

> *"SaaSOps is an essential area of growth within our company."*
>
> **— Director of information systems at real estate company with 850 employees**

How often IT monitors to prevent confidential data from being shared publicly

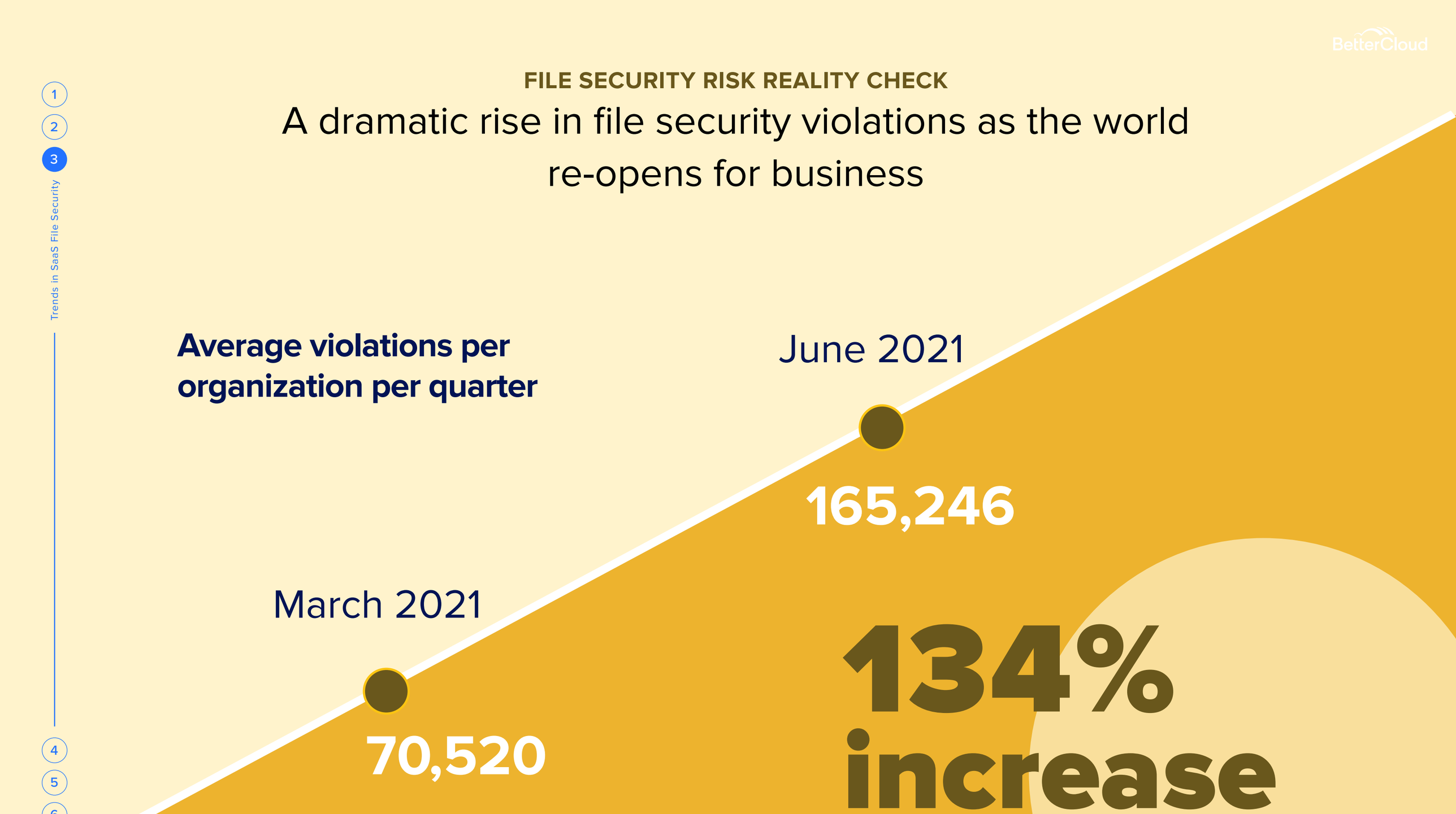


Always monitors to prevent public sharing of confidential data

FILE SECURITY RISK REALITY CHECK

A dramatic rise in file security violations as the world re-opens for business

Average violations per organization per quarter



Source: Internal BetterCloud data, June 2021

FILE SECURITY RISK REALITY CHECK

File sharing settings vary by industry

Industry	% of Internal Files	% of External Files	% of Public Files
Banking, financial services, or insurance	90%	9%	1%
Consumer services	79%	20%	2%
Education - K12/higher ed	78%	15%	6%
Healthcare services	90%	8%	3%
Hotels, restaurants, or leisure	82%	14%	4%
Manufacturing	95%	5%	0.3%
Media	92%	8%	1%
Professional services	89%	9%	2%
Real estate	95%	4%	1%
Retail	91%	7%	2%
Software-as-a-Service (SaaS)	92%	6%	1%
Transportation	88%	7%	5%
Utilities	80%	17%	3%
Overall	**87%**	**11%**	**2%**

Every industry and company has different competitive imperatives for balancing security with collaboration, user empowerment, and productivity. They also have different security, privacy, and compliance requirements.

Therefore, the degree of public file sharing is driven by this mix.

Education, an industry that serves the public, has the highest percentage of public files. Contrast this with manufacturing, SaaS, and media with their intellectual property protection needs. And then with banking and real estate with their security requirements.

How does your organization compare?

Source: Internal BetterCloud data, June 2021

Less than half say they invest enough to protect data within SaaS apps

Less than half (48%) of respondents say they invest enough to protect data within their SaaS apps. Clearly, many organizations feel that there's more work to be done when it comes to securing their SaaS data.

In addition to new tools, investment should include training on file sharing best practices. It should describe individual sharing permissions in detail (e.g., viewer, editor, commenter) and what public link sharing options mean.

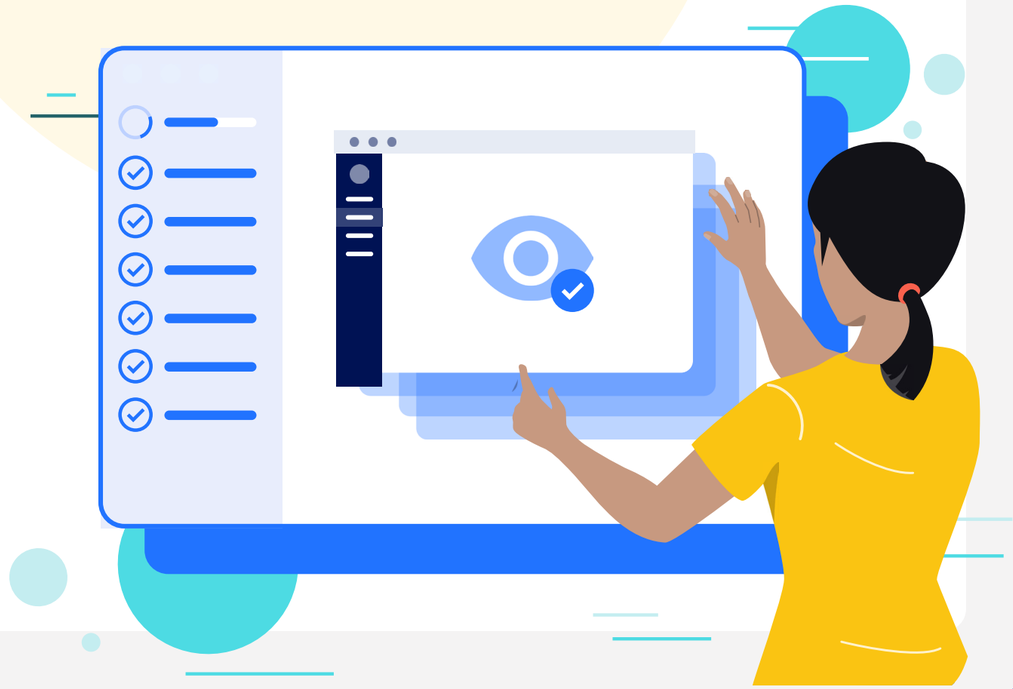
Training should also review restrictions to be enabled on the end user side. This includes providing temporary access or preventing people from re-sharing or downloading certain files.

This way users know exactly what happens when they're choosing sharing settings—and why they're important—thereby reducing risks of accidental data exposure.

In the next sections, we'll dive into the biggest challenges around managing SaaS operations—and the tools and processes organizations are using to solve them.

48%

Invest enough to protect data within their SaaS apps



4

Building Efficient SaaS Operations

More than half of organizations find SaaS sprawl challenging to manage

As SaaS adoption grows, so does the amount of data living in those SaaS applications. Think of all the users, files, folders, groups, records, contacts, calendars, third-party apps, permissions, logs, etc. associated with those apps. What results is an enormous, decentralized information sprawl. Where SaaS data exists, who has access to it, how it's shared, where it's exposed, what apps are actually being used–it all becomes nebulous and difficult to control.

It's no surprise, then, that **54%** of respondents agree or strongly agree that their SaaS sprawl is challenging to manage.

On average, offboarding takes 7 hours per user

Similarly, the more SaaS you adopt, the more tedious and complex offboarding gets. Deprovisioning, data transfer, security cleanup, data backup, license removal—all these steps multiply by leaps and bounds across SaaS apps. And IT teams are still grappling with slow, manual offboarding processes.

This year, respondents told us that on average, offboarding takes them **7 hours** per user.

SaaS-Powered Workplaces and Traditional Workplaces do have markedly different offboarding times. Since they're more likely to use SaaS management platforms and IDaaS tools to automate IT processes, SaaS-Powered Workplaces take an average of 2 hours and 49 minutes, while Traditional Workplaces take an average of 7 hours and 14 minutes.

The engineering department is most difficult to on- and offboard

Both Traditional Workplaces and SaaS-Powered Workplaces agree:

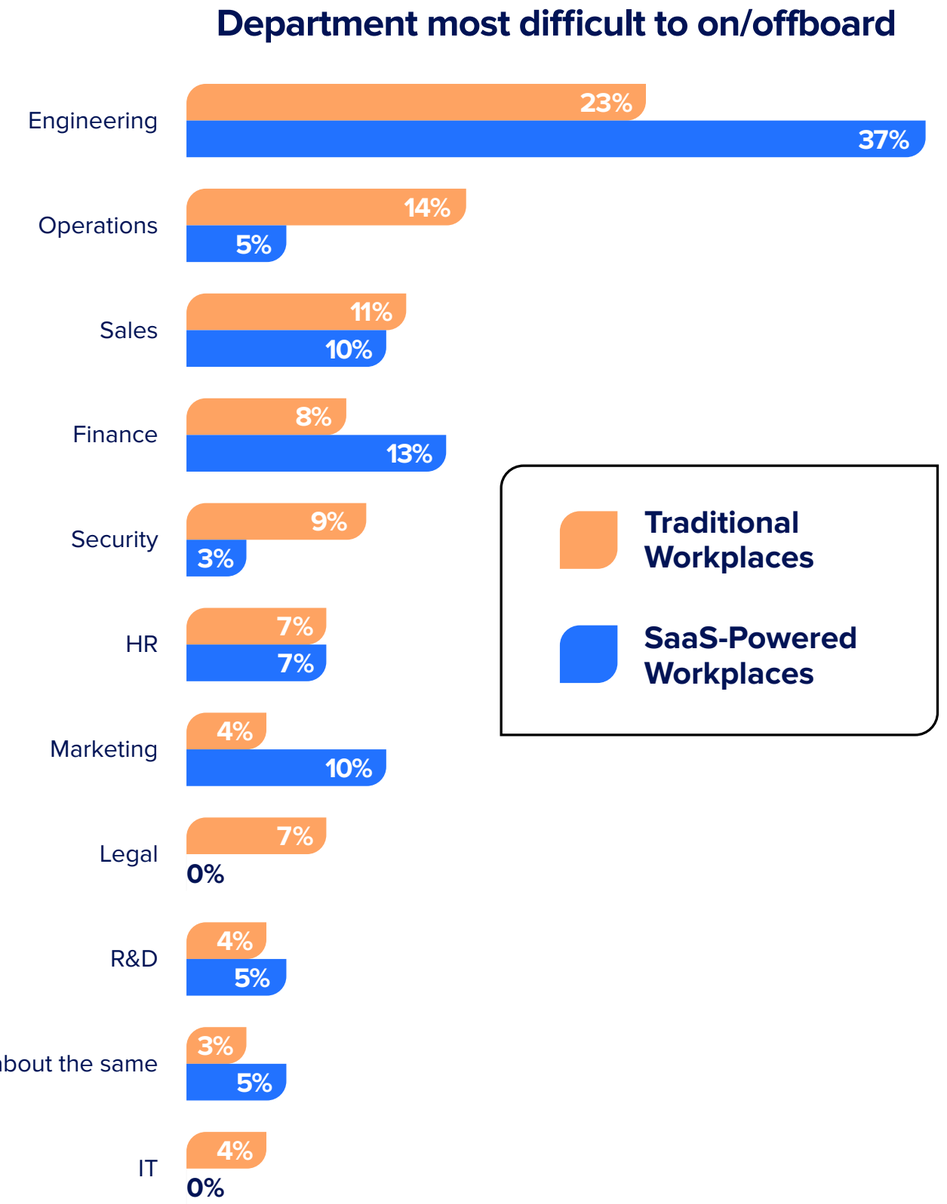
The engineering department is the most difficult to on- and offboard.

Given the sensitive nature of their content, some engineering tools are owned by non-IT teams. As a result, this complicates offboarding since IT must rely on other teams to complete the process.

The second most difficult to on- and offboard? For SaaS-Powered Workplaces it's the finance department, and for Traditional Workplaces, it's the operations department.

Offboarding in general is challenging. **It's more than just revoking access**. There are many more steps than people often realize—steps that are critical for data security, compliance efforts, and business continuity.

Tools like SaaS management platforms (SMPs) enable IT to create automated workflows that simplify ULM tasks. Offboarding processes that once took hours can be reduced to minutes and sometimes even seconds.



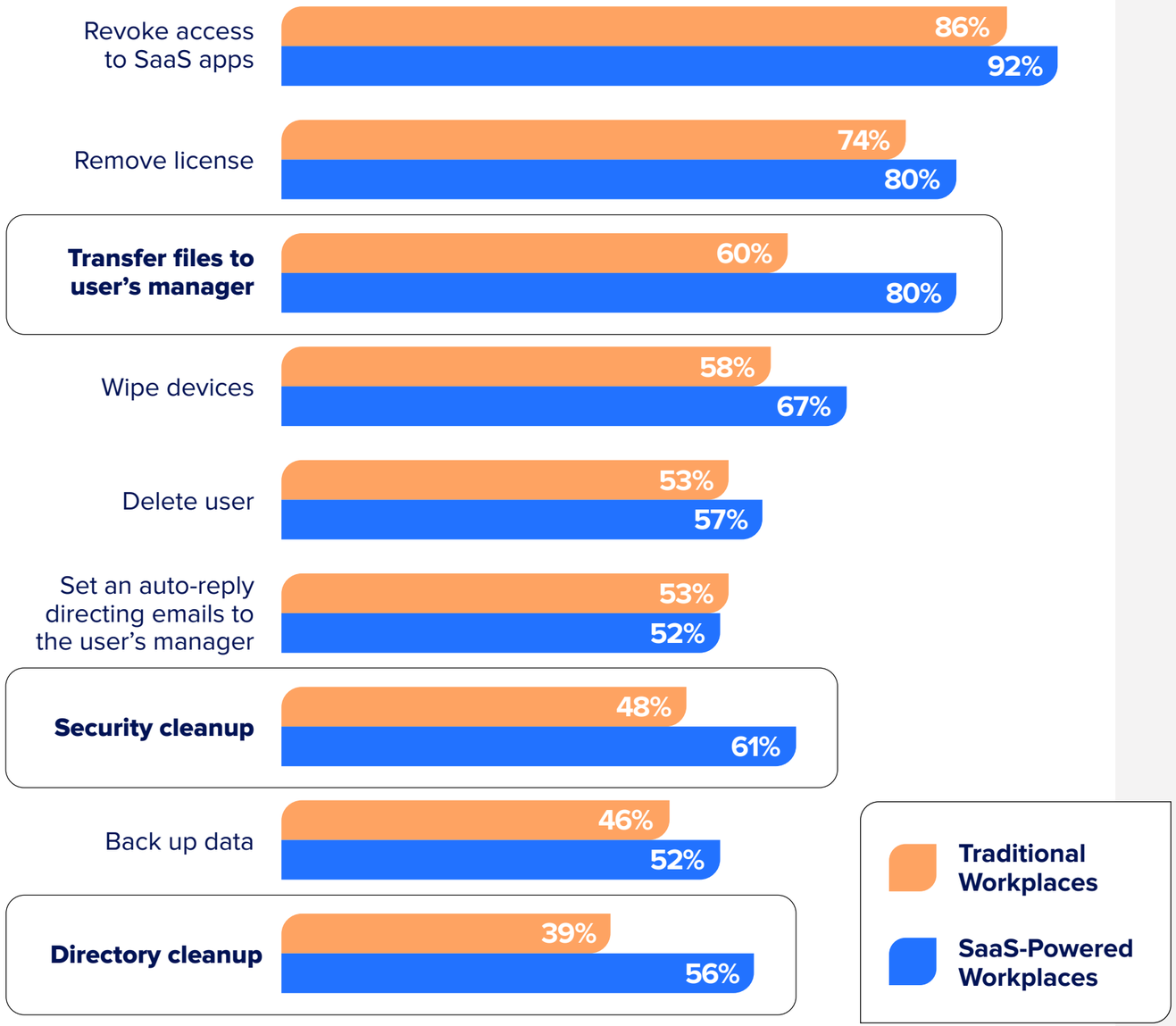
SaaS-Powered Workplaces generally perform more complete offboarding

While every organization has different offboarding checklists, requirements, and processes, there are several best practices to ensure thorough and complete offboarding.

SaaS-Powered Workplaces generally perform more complete offboarding.

The majority (**80%**) of them will transfer a departing employee's files to their manager. Only 60% of Traditional Workplaces complete that step. This step is critical because it preserves data for compliance reasons, and it ensures that other team members can continue working without any disruption.

Additionally, **61%** of SaaS-Powered Workplaces complete security cleanup tasks, such as revoking third-party apps. Less than half (48%) of Traditional Workplaces do them. Traditional Workplaces are also less likely to perform any directory cleanup. Only 39% of them complete it, compared to 56% of SaaS-Powered Workplaces.



The value of automation is well understood...

Given how time consuming it is to manage manual work, wrangle SaaS sprawl, and secure data, IT teams are increasingly turning to automation. The top benefit that IT teams expect from automating SaaS management? **Improved operational efficiency.** By eliminating manual tasks, you quickly create more capacity. This in turn allows you to dedicate more time on automation, which compounds. It's one of the most powerful ways IT can do more with less. Automation is also a key way to free up the resourcing required to be a strategic department, as well as shift to a proactive mode of operation.

The second most important benefit—at 44%—is **reduced human error**.

Manual mistakes can jeopardize an organization's security posture. However, automation makes sure all steps are performed according to documented processes. In addition, it strengthens security and compliance because it eliminates the possibility of overlooked steps, misconfigured apps and systems, and more.

Expected benefits from automating SaaS management

More than half (56%) of organizations agree or strongly agree that they prioritize IT automation

**Respondents were asked to select their top two choices*

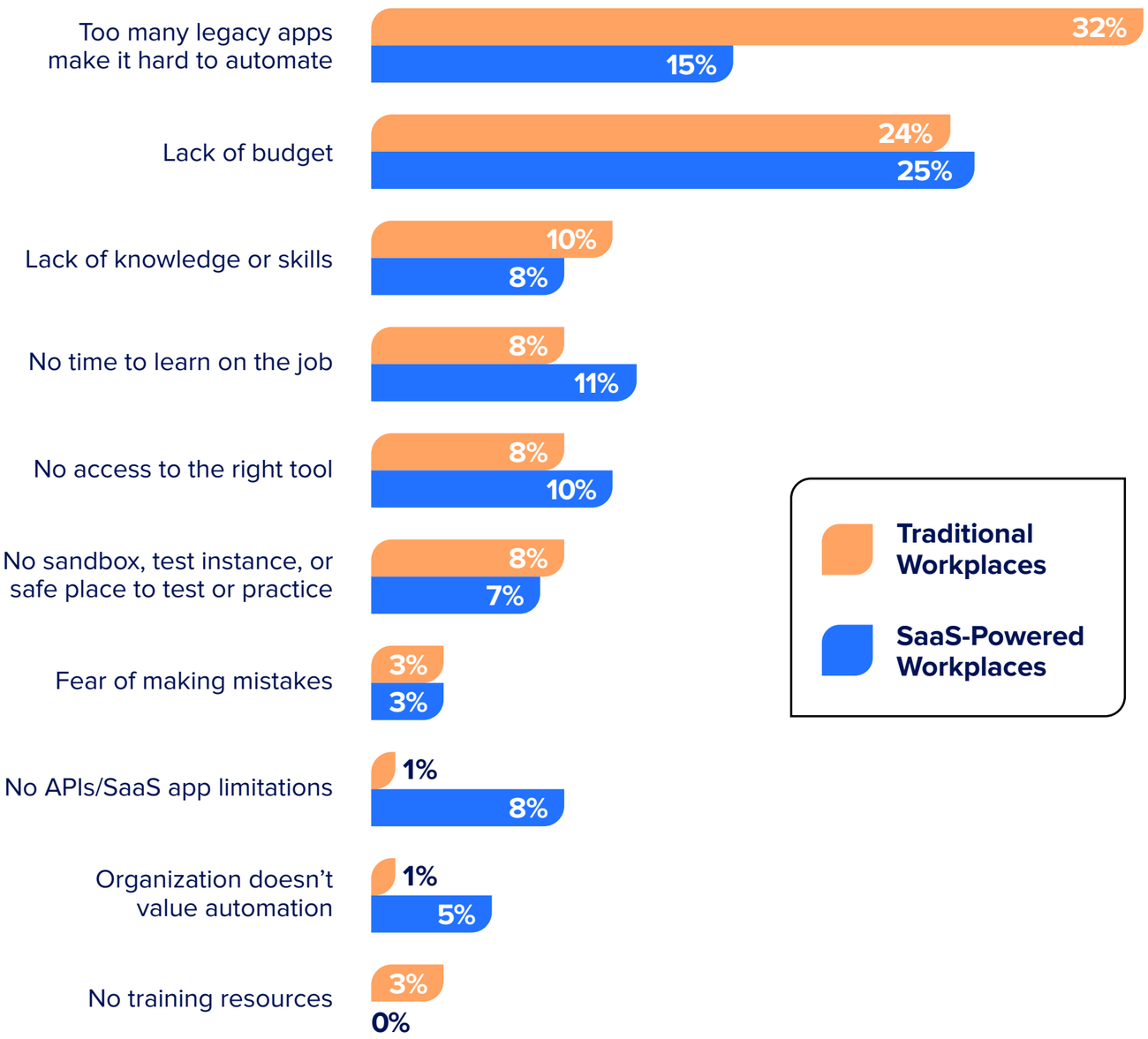
...but there are unique challenges preventing IT from automating even more

While there are many powerful benefits to IT automation, organizations have discovered several unique challenges while trying to do *more* of it.

For SaaS-Powered Workplaces, IT automation is most limited by lack of budget **(25%)**, an unseemly number of legacy apps **(15%)**, and lack of time to learn on the job **(11%).**

Traditional Workpaces are slightly different. Their biggest IT automation challenges are legacy apps **(32%)**, lack of budget **(24%)**, and lack of skills **(10%)**.

But another interesting limitation surfaced as a write-in response. 8% of SaaS-Powered Workplaces reported that SaaS applications themselves can have limitations. Some don't have APIs or don't easily integrate with a SaaSOps tool.



SaaS-Powered Workplaces lead the way in automation

Although they're not immune to the challenges of IT automation, SaaS-Powered Workplaces automate a much greater percentage of their operations than Traditional Workplaces.

This year, **a typical SaaS-Powered Workplace automates nearly half (45%) of its IT operations**. The typical Traditional Workplace automates 25% of its IT operations. While this still accounts for a significant amount of their routine SaaS operations, it also means that SaaS-Powered Workplaces automate **80%** more of their routine tasks than Traditional Workplaces.

What's clear is that automation is the path forward, as IT teams everywhere are bogged down with repetitive tasks.

82% of respondents said they spend at least 20% of their work week (i.e., an entire day) working on repetitive tasks.

Without prioritizing automation, IT teams will long be stuck in reactive mode, toiling on manual, time-consuming tasks.

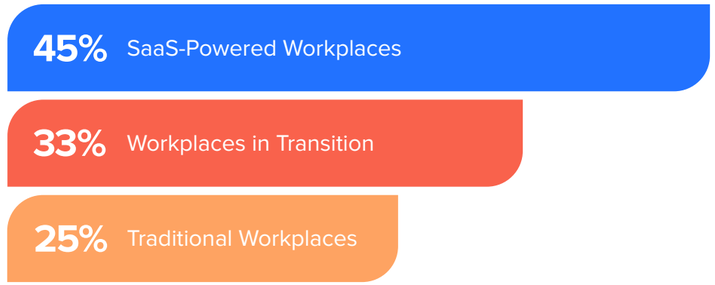
LEGEND

SaaS-Powered Workplaces
Workplaces that are almost entirely running on SaaS today. Comprised of the top 15% of our study, these orgs are 93% SaaS-based today.

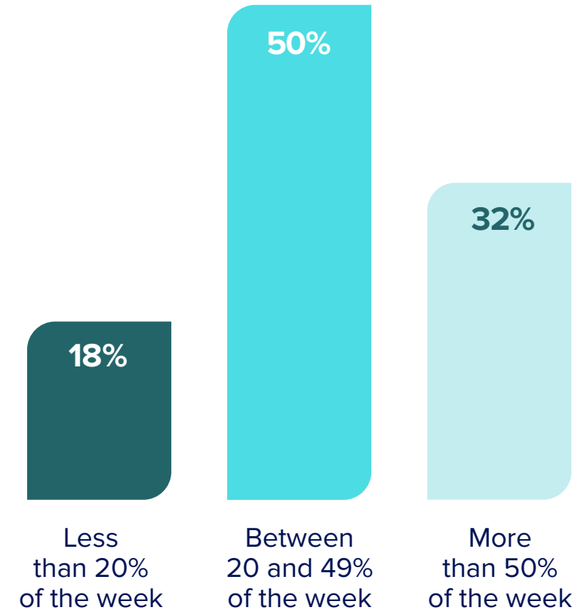
Workplaces in Transition
Workplaces that are using a mix of SaaS and on-prem tools. Comprised of the middle 70% of our study, these orgs are 55% SaaS-based today.

Traditional Workplaces
Workplaces that are primarily using on-premise tools. Comprised of the bottom 15% of our study, these orgs are 8% SaaS-based today.

Percentage of routine SaaS operations automated today



Percentage of IT's work week doing repetitive tasks



"Automation is going to be a cornerstone of SaaSOps."

— VP of IT at real estate company with 750 employees

Automation frees up IT teams to work on meaningful, higher-value initiatives.

Here's what respondents told us they're working on with that extra time:

Automating even more

- Implementing true zero-touch deployment
- No-code business automations
- Machine learning
- Looking for more business workflows that haven't yet been automated!

Improving the employee experience

- Creating new in-house IT services that improve users' business efficiency
- Being proactive about user issues
- Automate company processes and controls to give a better user experience
- Enabled a more nimble workforce
- Additional training for the team

Security & compliance

- SOX preparedness
- Becoming a 100% Zero Trust network operation
- Improving proactive audits for compliance and security
- Designing a SOC
- DevSecOps
- More automation, alerting, and intelligence-based anomaly detection
- Threat hunting
- Patch management
- Mobile device security
- Data loss prevention, scanning sensitive applications
- MFA, privilege management
- Endpoint protection
- Expanding scope of MFA outside of SaaS, including end user computers, servers (SSH/RDP/console), special networks, etc.
- Improve resilience and recovery processes

Consolidation & integration

- Consolidating data centers and multiple SaaS instances
- Consolidating and eliminating tools that will no longer be needed
- Cost reduction initiatives
- Integrating new technologies
- Optimize SaaS tech stacks
- Fully integrating Salesforce add-ons

Being a strategic business partner

- Being more involved in strategic planning
- Projects that align with the business strategic roadmap
- The "fun" stuff. Things that utilize critical thinking/come up with creative solutions
- Customer experience
- More time on analytics and supporting the business as a strategic partner
- Interfacing with departments to help them solve challenges with SaaS

Migration & modernization

- Migrating legacy workloads to cloud systems
- Overhauling old systems and teams with new IT automation
- Server refresh, network redesign, storage upgrade
- Service management improvements
- Increased virtualization

R&D

- Implementing and researching new SaaS technologies
- Invest in new office productivity tools
- Developing more bespoke solutions
- Innovation

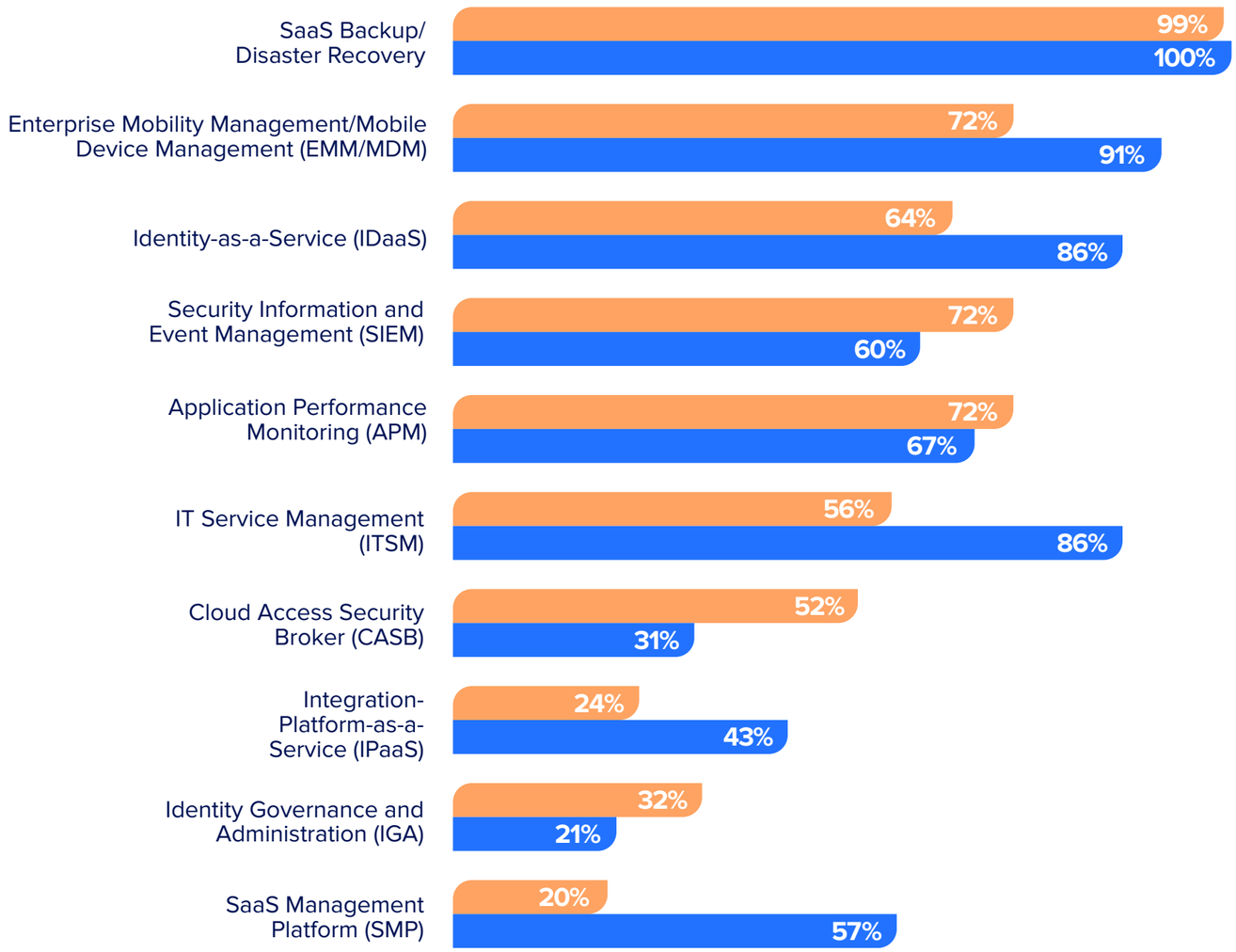
Professional development

- Pursuing industry certifications in cloud architecture

When it comes to solving SaaSOps challenges, different organizations are more likely to use some tools than others

While SaaS-Powered Workplaces are *more* likely to use EMM/MDM, IDaaS, SMP, iPaaS, and ITSM tools, Traditional Workplaces are more likely to use IGA, SIEM, and CASB tools. Nearly 60% of SaaS-Powered Workplaces, about twice that of Traditional Workplaces, use an SMP.

SaaSOps tech stack comparison



Better together: Who uses an IGA, SMP, and IDaaS together?

18% of those surveyed use all three of these technologies together—and all are key to security, governance, and compliance.

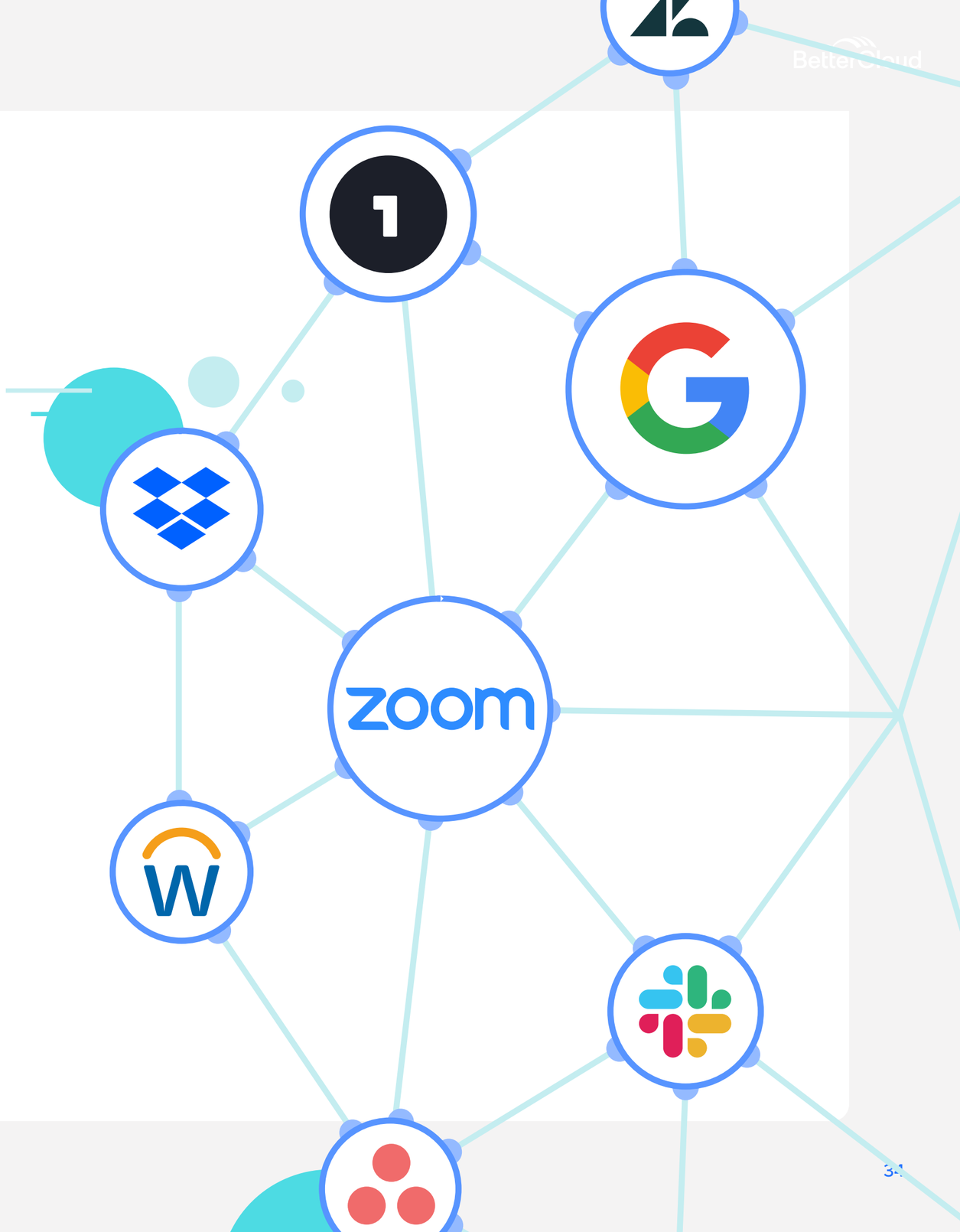
As you might expect, this set of users is more likely to be in banking, SaaS companies, professional services, and manufacturing.

And they're big. They have an average of 17,036 employees.

71% use Microsoft for cloud productivity and 40% have been using SaaS for less than three years.

Putting it all together, it suggests that these companies are likely to be publicly traded, and compliance requirements drive their need to use these three important technologies together.

Next up, we'll look forward and provide a glimpse into what the future of SaaSOps holds.



5

A Glimpse into the Future of SaaSOps

In 2021, IT's role (finally) shifted from functional to strategic—and will continue growing in importance

In 2021, enterprise IT continues its transformation to the complete digital workplace. Amid the accelerating pace of technology and explosion of SaaS adoption, IT is helping organizations address new challenges and evolving its role from ticket taker to tech enabler.

To continue driving momentum and enabling their modern workforces, **IT changed to think strategically—as 76% told us**.

In the past year, they've become less reactive, more proactive. They're participating in strategic planning, driving customer outcomes, and becoming trusted strategic partners to the business—ultimately leading the way to tomorrow's workplace.

What respondents say they're working on:

"Being more involved in strategic planning"

"Innovation"

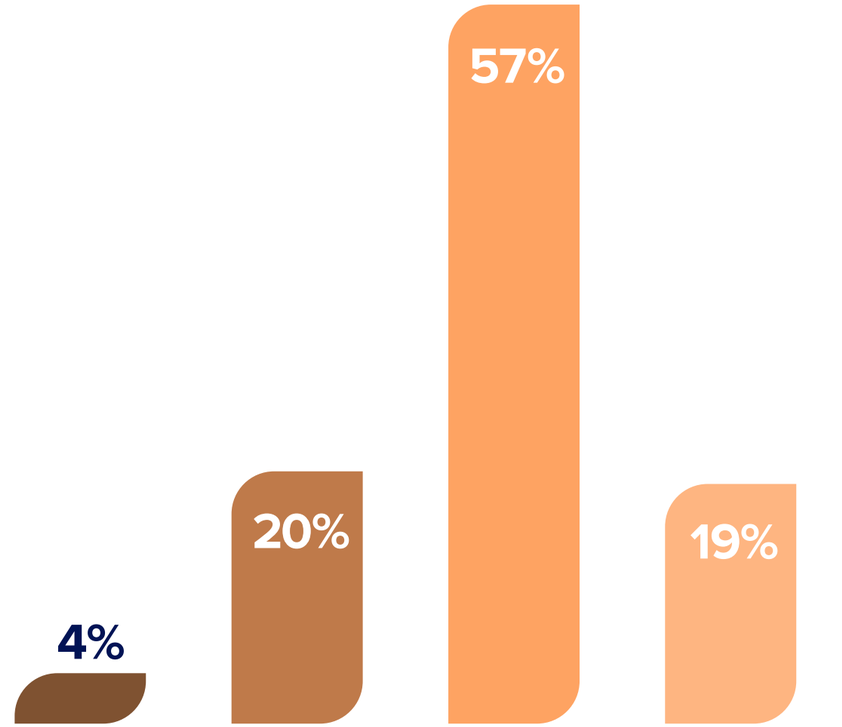
"Being proactive about user issues"

"More time on analytics and supporting the business as a strategic partner"

"Projects that align with the business strategic roadmap"

"Interfacing with departments to help them solve challenges with SaaS"

How IT's role changed in past year



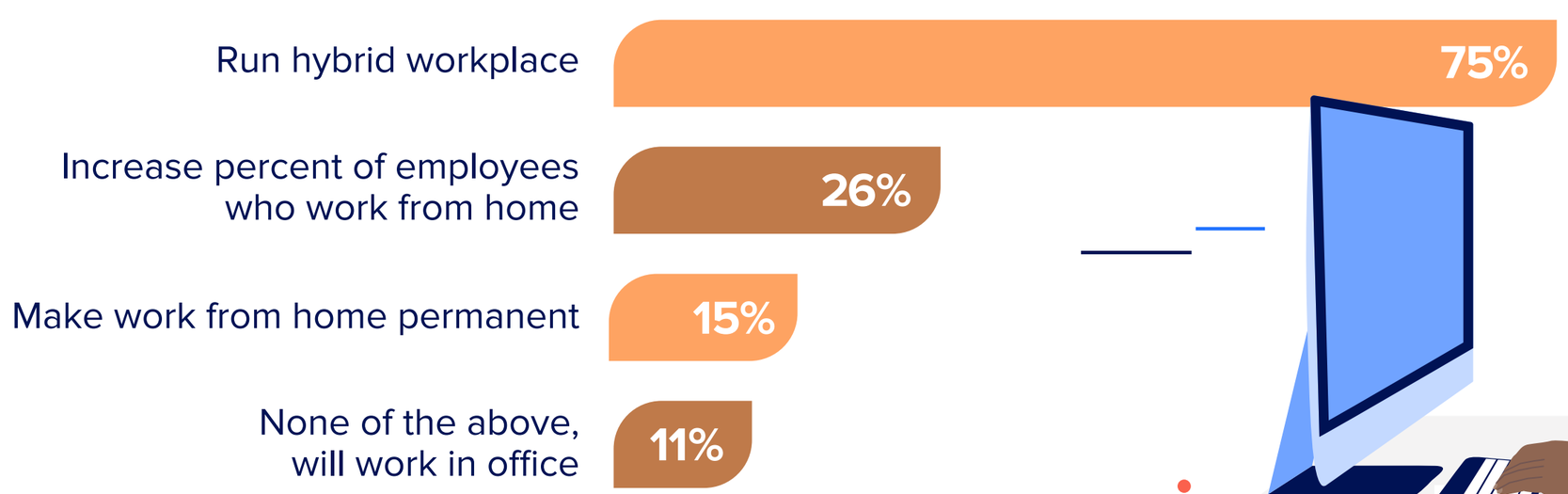
Enabled by SaaS and SaaSOps, hybrid workplaces are here to stay

When you look at the next 12 months, they'll look a lot like the last 12 months. Even as some organizations plan office reopenings, WFH is here to stay in some way, shape, or form.

In fact, **75% of organizations plan to operate a hybrid workplace for the next year.** Companies are recognizing the benefits of hybrid work, especially when it comes to employee experience—and IT plays a critical role in optimizing that employee experience. **SaaSOps equips organizations with the tools, processes, and skillsets to successfully transition to a hybrid future.**

At this point in time, only 11% of organizations plan to resume normal office operations.

Workplace plans for next 12 months



Fast forward to 2025: Rapid SaaS adoption will continue, and everyone will eventually become a SaaS-powered workplace

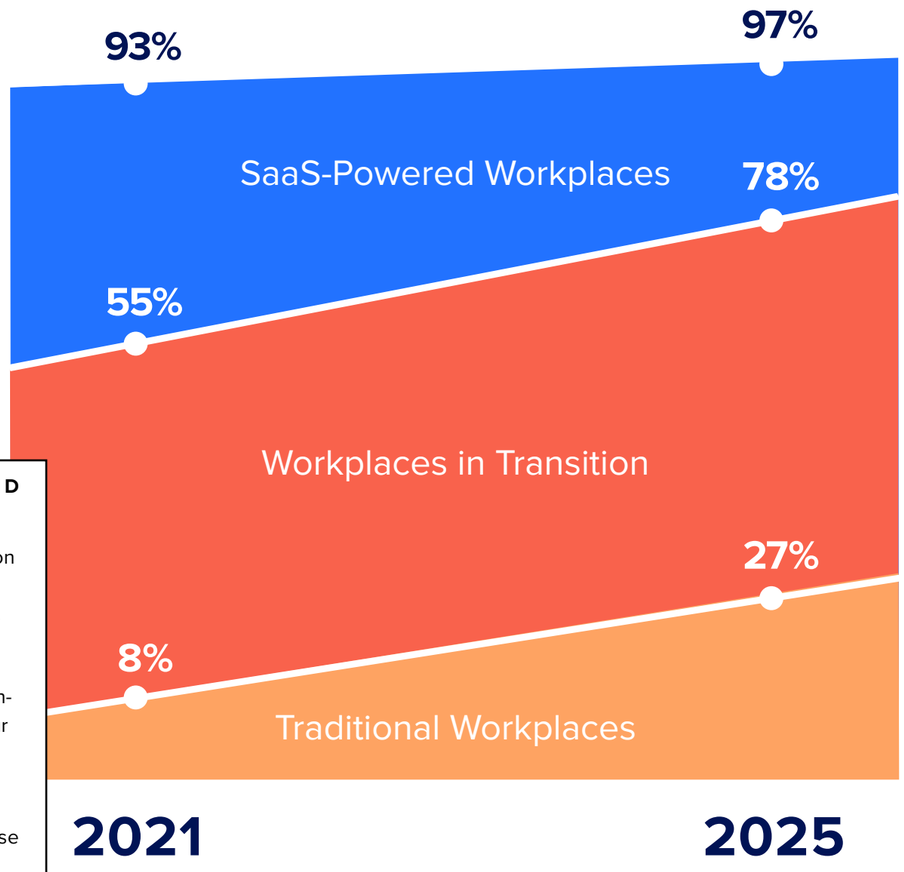
The next certainty is that every organization will eventually become a SaaS-powered workplace.

SaaS is clearly part of every organization's digital transformation strategy, and even the most established, legacy infrastructure-bound organizations are moving toward it.

SaaS-Powered Workplaces are, well, almost 100% SaaS powered. As a result, by 2025, their percentage of SaaS-based enterprise apps won't increase dramatically. However, we believe the number of apps used will still continue to rise as more use case-specific apps emerge on the market.

And when it comes to Workplaces in Transition, they expect to go from 55% to 78% SaaS-powered over the next four years. Similarly, the fact that even Traditional Workplaces plan to go from 8% to 27% SaaS-powered (a 238% increase) is indicative that the tipping point is here. Every organization is trending in this direction, and there's no going back to the legacy ways of working now.

Percentage of enterprise apps that will be SaaS by 2025



LEGEND

SaaS-Powered Workplaces
Workplaces that are almost entirely running on SaaS today. Comprised of the top 15% of our study, these orgs are 93% SaaS-based today.

Workplaces in Transition
Workplaces that are using a mix of SaaS and on-prem tools. Comprised of the middle 70% of our study, these orgs are 55% SaaS-based today.

Traditional Workplaces
Workplaces that are primarily using on-premise tools. Comprised of the bottom 15% of our study, these orgs are 8% SaaS-based today.

Levels of SaaSOps automation will nearly double in the next 3 years

The next prediction isn't terribly surprising, either. Automation is the path forward, and automating routine SaaS operations is an imperative. But its pace looks to accelerate.

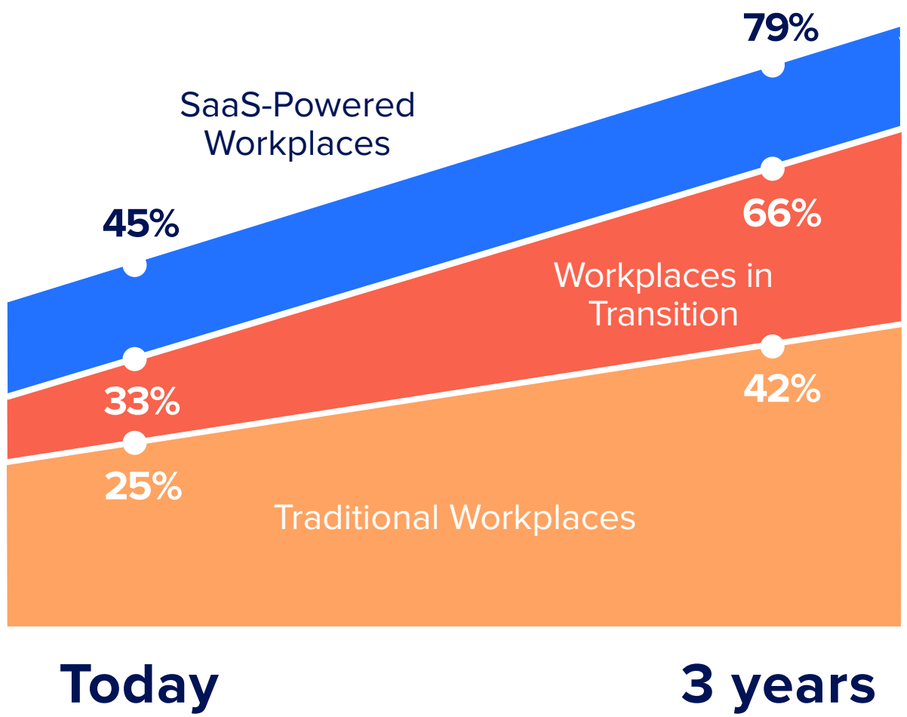
IT automation will make big gains over the next few years. SaaS-Powered Workplaces report that today 45% of their routine SaaS operations is already automated and estimate it will rise to nearly 80% in three years.

Even the Workplaces in Transition and Traditional Workplaces will make enormous strides. On average, while Workplaces in Transition automate a third (33%) of their SaaS operations today, they expect that to double to 66% in three years. The same trend applies to Traditional Workplaces too. Though only 25% of their routine SaaS operations is automated today, that figure will also nearly double, rising to 42%.

Any organization adopting SaaS will eventually face the same operational challenges that come with discovering, managing, and securing SaaS apps, users, and files at scale. As SaaS apps proliferate, IT is beset with more and more manual tasks. **And as SaaS-Powered Workplaces have learned, automating SaaSOps is the only way to scale and create more capacity.**

> *"SaaSOps is critical to our success."*
>
> **— Senior director of IT, consumer electronics company, 1,000 employees**

Percentage of routine SaaS operations that will be automated in 3 years



The SaaSOps role will be critical to every IT team

Additionally, SaaSOps is increasingly influencing the evolution of job titles. All told, **60%** of IT professionals already have “SaaSOps” in their job titles/descriptions or plan to add it in the future—a whopping **100%** increase from last year. For many respondents, SaaSOps is where they’ll realign their career goals, if they haven’t started to already.

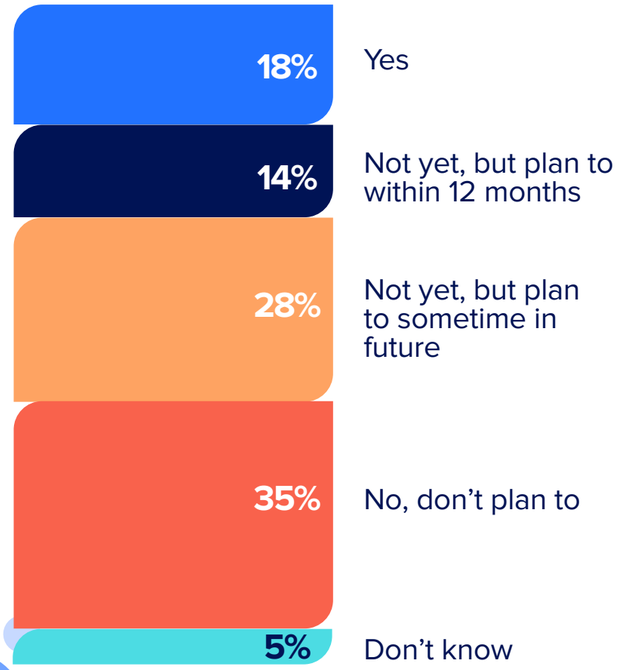
It’s no surprise that SaaS-Powered Workplaces are more likely to embrace SaaSOps in their job titles and job descriptions. Nearly a third (**32%**) of them currently do. But what’s interesting is that Workplaces in Transition and Traditional Workplaces, too, are aware of this shift to SaaSOps and plan to evolve job titles and/or roles as well.

While only **13%** of Workplaces in Transition have a SaaSOps team member right now, an impressive **49%** expect to add this role in the future. Traditional Workplaces follow a similar trend. Only **12%** have a SaaSOps role now, but another **36%** will add it in the future.

Workplaces in Transition and Traditional Workplaces are more established organizations with legacy infrastructure—and they, too, recognize the need to hire for SaaSOps roles and skills.

IT organizations of all types increasingly understand that SaaSOps is key to smooth SaaS operations. Teams who know how to automate and optimize SaaS apps, secure data without compromising productivity, and unlock the value of apps are at a bigger advantage because they can successfully drive organizational transformation.

Have SaaS operations (SaaSOps) in job title and/or description



“SaaSOps is table stakes for the IT department.”

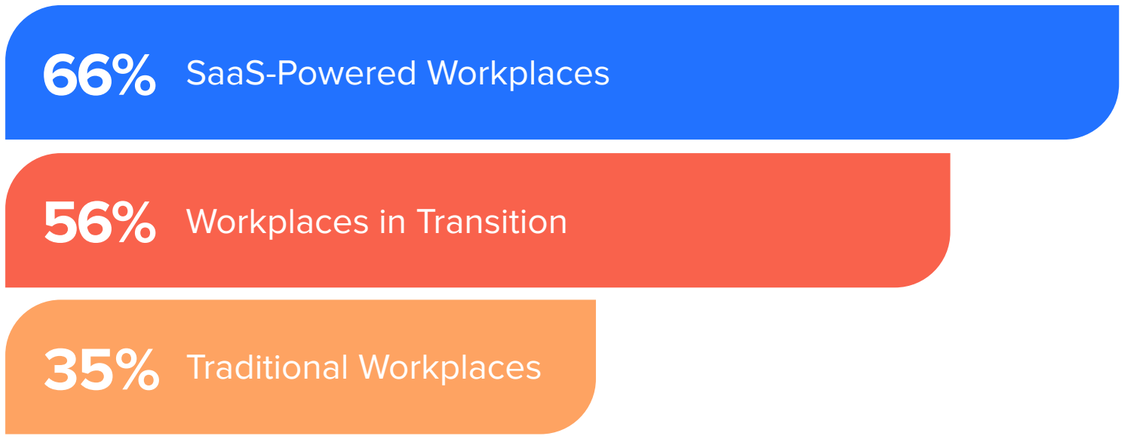
— CIO at software company with 650 employees

More than half of organizations will use a SaaS management platform (SMP) in the next year

In SaaSOps, the right skills and processes are half the battle. The other half is the right set of tools.

Overall, over half (57%) of organizations plan on using a SaaS management (SMP) in the next 12 months.

Likeliness to subscribe to a SaaS management platform (SMP) in the next 12 months



The likeliness to subscribe to an SMP, not surprisingly, varies based on SaaS usage. With their heavy reliance on SaaS, SaaS-Powered Workplaces are the *most* likely to use one; 66% of them say they will. Meanwhile, 56% of Workplaces in Transition and 35% of Traditional Workplaces say they're planning on using one in the next year.

As SaaS adoption increases, the need for a scalable approach to SaaS management increases in tandem. Managing SaaS in browser tabs—across disparate admin consoles—mires IT in manual work and is not sustainable. It also weakens IT's ability to establish a consistent security posture across their cloud portfolio. One way to manage SaaS at scale is by automating policies and processes with an SMP.

So as we wrap up this year's State of SaaSOps, the undeniable conclusion is that the state of SaaSOps is strong. **With each new tool adopted and automation built, SaaSOps becomes the standard way to support a best-of-breed strategy—enabling an empowered, productive, and secure organization.**

The final words on the 2021 state of SaaSOps: mission critical

For the second year in a row, we closed our survey by asking respondents to share what they think the future of SaaSOps is.

This year, even stronger consensus emerged.

41% of respondents wrote that the future of SaaSOps is “mission critical,” “very important,” or “essential in IT”

30% wrote that the SaaSOps future is “bright,” “growing,” and “evolving”

So as we aim towards 2022 and beyond, we can’t say it better than our survey respondents:

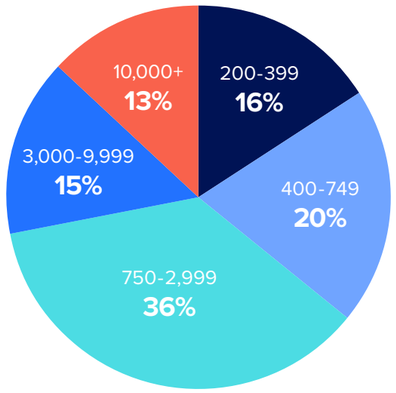
SaaSOps is mission critical for every IT department in every organization.

6

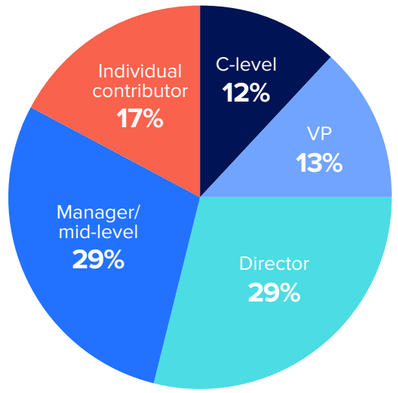
Demographics and Methodology

Demographics

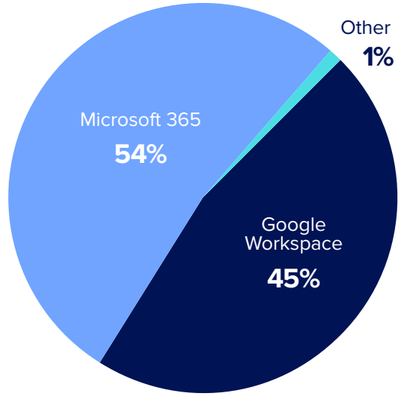
Company size



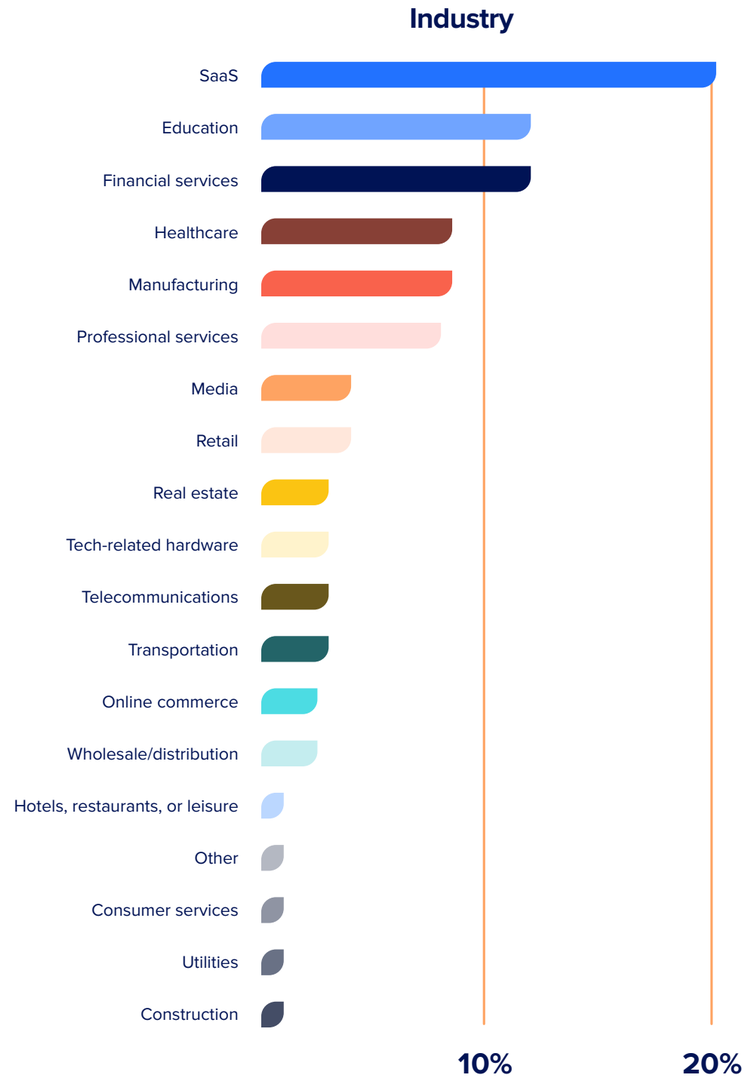
Job level



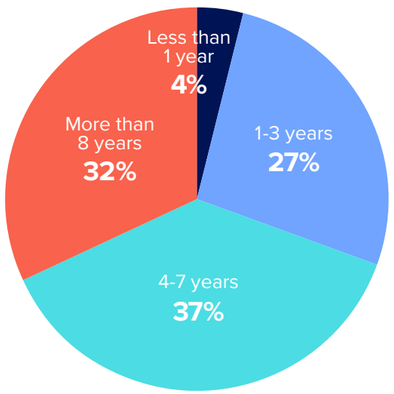
Primary cloud suite



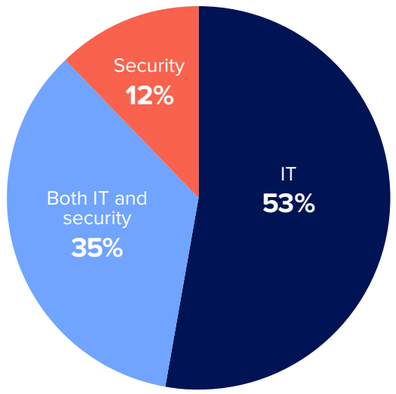
Industry



Length of time using SaaS



Department (IT vs. security)



Methodology

This survey was conducted online from May 3, 2021 to May 31, 2021. We collected data from IT and security professionals who were personally involved in one or more of the following activities related to SaaS apps: approving or making final buying decisions; researching and recommending apps; determining requirements for new apps; supporting end users; managing, deploying, or securing apps; or handling vendor relationships and/or procurement. Respondents consisted of members of our IT community (including our Slack community and daily newsletter subscribers), BetterCloud customers, and non-customers.

In addition, we analyzed file security violations across BetterCloud users. This analysis includes data from nearly 2,000 organizations with more than 200 users covering millions of users and files across hundreds of SaaS apps. The data comes from BetterCloud's automated scanning with 90+ pre-built data identifiers to find the most common sensitive data types for 25+ different countries. This includes personally identifiable information (PII) like U.S. Social Security numbers and financial information.