

# 2020 State of SaaS Ops

## The Impact and Implications of the SaaS Revolution



Our *2020 State of SaaS Ops* survey reveals that as more companies scale up their SaaS environments, IT organizations are dealing with significant SaaS challenges around cost, complexity, and risk. The study also confirms that IT organizations are turning to SaaS Ops to deal with these challenges in a sustainable and cost-effective manner.

SaaS Ops provides IT with a disciplined approach to discovering, managing, and securing SaaS at scale, based on the use of centralized, automated tool sets. The results of the study indicate that as more companies adjust to the realities of managing SaaS at scale, SaaS Ops has the potential to evolve into a core IT discipline—influencing strategic priorities, technology investments, and even job titles.



# Table of Contents

- Letter from Our CEO ..... 3
- Demographics ..... 7
- Key Findings ..... 9
- SaaS Steps into the IT Spotlight ..... 11
- SaaS Adoption and Business Growth ..... 13
- Combating COVID-19: SaaS Innovation  
and Inspiration Win the Day ..... 15
- Understanding the Attraction of SaaS ..... 18
- The Trouble with SaaS: Taking Stock of Visibility,  
Automation, and Security Challenges ..... 21
- SaaS Visibility: Missed Opportunities and Missing Insights ..... 23
- Manual Tasks: Making SaaS Harder Than It Needs to Be ..... 25
- SaaS Data Security: Learning to Balance Risk and Productivity ..... 27
- SaaS Ops: Keeping SaaS Apps on the Path to Value ..... 34
- The SaaS Ops Framework: Processes and Priorities ..... 36
- 5 Things to Know About Working with SaaS Ops ..... 37
- SaaS Ops Gives SaaS the Future It Deserves ..... 43
- Methodology ..... 44





LETTER FROM OUR CEO

# SaaS Ops: Preparing IT for a new world of technology challenges



When you look back at why 2020 was such a remarkable and challenging year, software as a service (SaaS) probably isn't the first thing that comes to mind. That's true because of the world-changing events that seemed to unfold on a daily basis, but it's also true because SaaS is literally everywhere today, creating the experiences that define how we work, play, shop, learn, and socialize. SaaS is invisible because it's ubiquitous.

But it's worth taking a moment to understand why 2020 wasn't just about business as usual for the adoption and usage of SaaS. Someday, we'll look back and realize this was actually a pivotal year for understanding the true power of the SaaS model—and for giving IT organizations the tools they need to help SaaS live up to its remarkable potential.

## SaaS applications save the day

In the early part of the year, we watched SaaS power a historic workforce transformation. In just a matter of weeks, businesses around the world leveraged SaaS platforms to shift employees out of traditional offices and into distributed, mostly home-based work environments.

This was a tour de force for the SaaS model, which supplied the tools needed to keep workers connected, engaged, and productive, and ensured these tools were affordable, even for the smallest businesses. In the process, SaaS apps helped to keep millions of people employed and productive during very uncertain and challenging times.

But there's a flip side to this story. While it's less visible outside the IT space, it's important to anyone who wants SaaS to continue living up to its full potential. It's the story of SaaS Ops.



## SaaS Ops: Setting up SaaS for success at scale

Today, we're seeing businesses adopt SaaS apps at an astounding pace. Since 2015, the number of IT-sanctioned SaaS apps has increased tenfold, and there's much more to come: It's expected that by 2025, 85% of business apps will be SaaS-based. And as businesses bet their futures on SaaS, there's a lot riding on an IT organization's ability to manage, integrate, and secure SaaS environments that may include dozens or even hundreds of apps.

This growing complexity is turning the path to success with SaaS into a bumpy and unpredictable ride. IT organizations in particular are discovering that managing and securing SaaS environments at scale can be a very difficult and time-consuming process. Ad hoc approaches to SaaS management tasks are breaking down; concerns over cost, security, and lack of control are on the rise. Such challenges may feel like growing pains today, but they'll eventually create real barriers to managing SaaS cost and risk.

IT organizations are discovering that managing and securing SaaS environments at scale can be a very difficult and time-consuming process.





## Shining a light on SaaS Ops practices

The good news is that IT organizations are uniting behind a proven solution to their SaaS challenges: **SaaS Ops, a discipline that offers a proven framework for discovering, managing, and securing SaaS environments through centralized and automated operations, is helping to reduce friction, improve collaboration, and create better employee experiences.** But there's still a burning need for data-driven insights into how and why IT organizations are leveraging SaaS Ops tools and methods.

We think the *2020 State of SaaS Ops* report will go a long way toward closing this information gap. This year's report is based on a truly exceptional body of research: More than 650 IT leaders and practitioners, representing a wide range of company sizes and industries, contributed insights and opinions based on their own SaaS Ops experiences.



This is the largest body of data ever assembled on how modern IT organizations deal with the challenges of managing SaaS at scale. It's also the culmination of more than a decade of experience collecting, analyzing, and publishing research, and educating the market on these topics—with our research appearing on CIO.com, Forbes, The Wall Street Journal, Business Insider, CNBC, ZDNet, and countless other media outlets.

 [SaaS Ops pushes] traditional IT to be more proactive, more oriented towards business goals, and even more mindful of how to use technology to empower the end user. 

—IT Manager, transportation company with 400 employees



## Preparing for your future with SaaS Ops

We designed the *2020 State of SaaS Ops* report to give IT organizations the insights and practical tips they need to understand this issue and take informed action. The report confirms that IT leaders and practitioners see SaaS Ops as a necessity given the challenges of managing SaaS at scale. It also shows that automation—a key capability for a SaaS Ops platform—has a game-changing impact on how IT manages SaaS environments.

The *2020 State of SaaS Ops* report confirms that IT leaders and practitioners see SaaS Ops as a necessity given the challenges of managing SaaS at scale.

TWEET THIS 

Finally, our research establishes that SaaSops has evolved into a core IT discipline and career priority: 30% of practitioners have already integrated the term into their job titles or plan to do so. These individuals believe that SaaSops is truly the future of IT, and they’re putting themselves on the cutting edge of SaaSops adoption.

We have no doubts that we’ll look back at 2020 and recognize it as the point when SaaS truly took its place as the future of IT. Thanks to SaaSops, 2020 will also be the year when IT gave SaaS a secure and sustainable future. We hope the *2020 State of SaaSops* report shows you why SaaSops is such an essential part of this story and that it helps you prepare your IT organization for success with it.

### David Politis

CEO and Founder, BetterCloud

“Enablement of SaaSops in our environment is critical to the overall success of our company.”

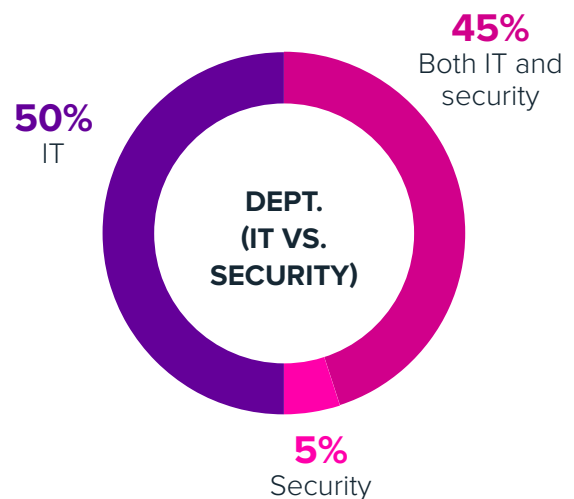
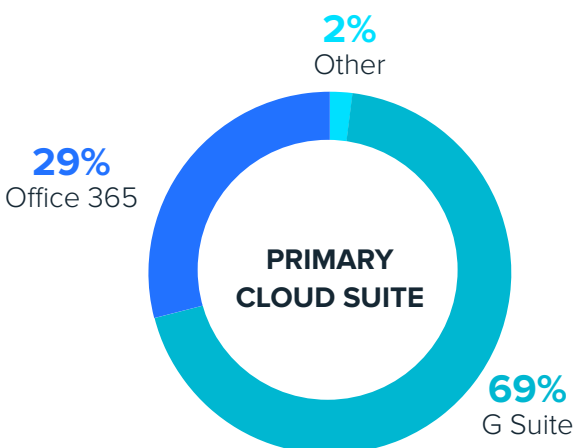
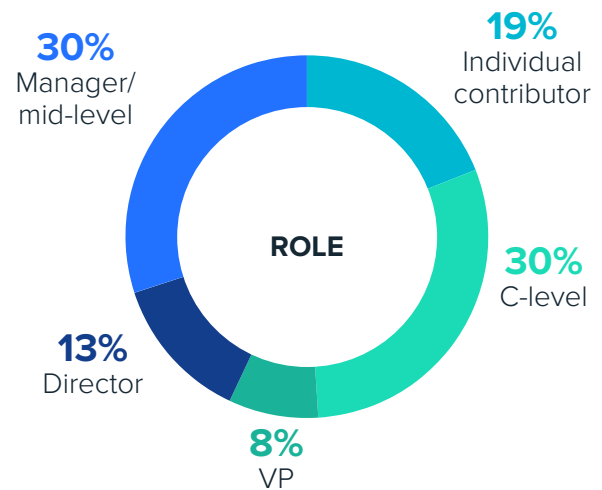
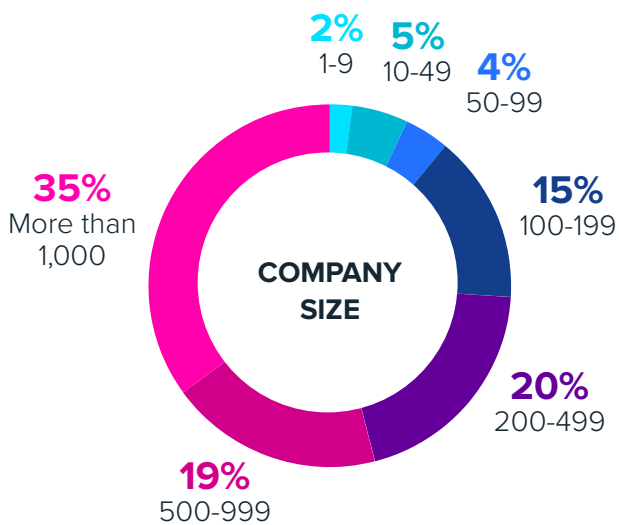
— IT Director, healthcare company with 950 employees





## Demographics

During April to May 2020, BetterCloud surveyed 676 IT and security professionals. These individuals ranged in seniority from C-level executives to front-line practitioners and included both IT and security department roles. The respondents' companies represented a wide range of company sizes and industries; most of these were established businesses with significant experience using SaaS apps. Almost all of those surveyed use either G Suite or Office 365 as their primary cloud productivity suite.

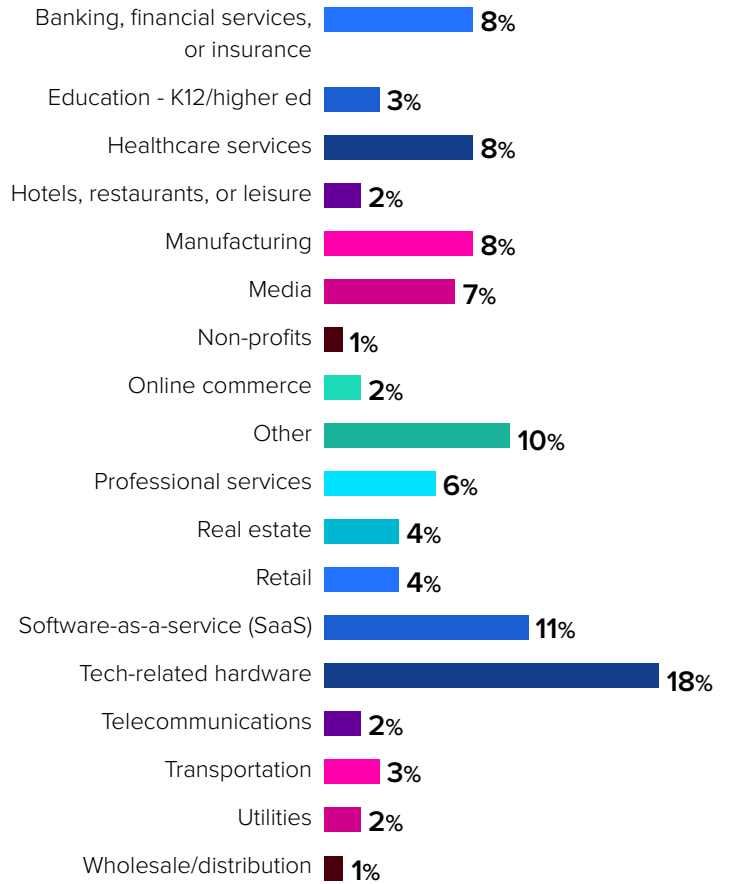




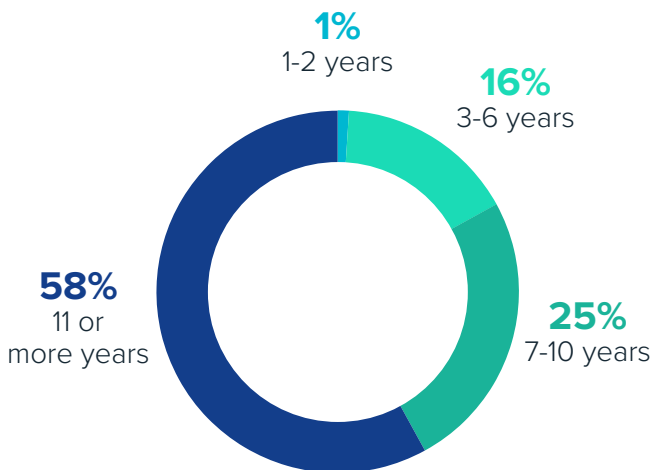
### GROWTH STATUS IN 2019



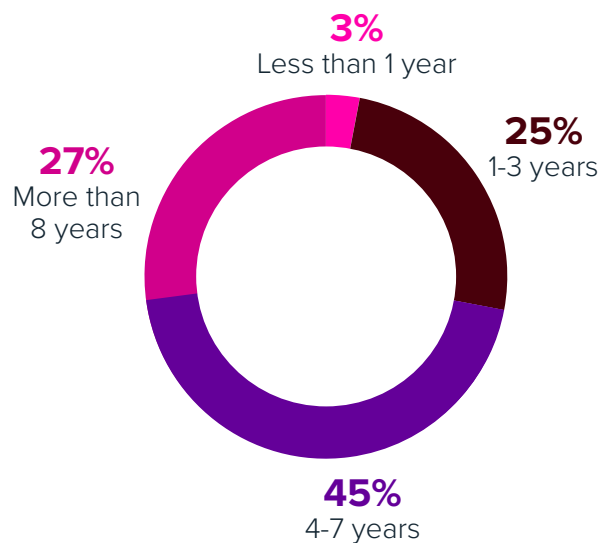
### INDUSTRY



### COMPANY AGE



### LENGTH OF TIME USING SAAS







## Key Findings

### TOP INSIGHTS



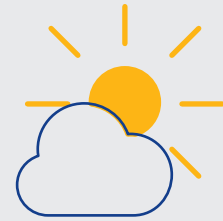
**SaaS Ops as a market has clearly emerged.**

Its necessity is driven by scale, and the line between IT and security is blurring.

**2x**

**more total SaaS, custom SaaS, and IT-owned apps**

The number of total apps used by companies with SaaS Ops platforms as compared to non-SaaS Ops platform users



**SaaS Ops is the future of technology.**

IT professionals strongly believe SaaS Ops will continue to grow in importance and size.

## SAAS USAGE

### Top 2 Motivators for Using More SaaS Apps

**80**

Average number of SaaS apps used

[TWEET THIS](#)



Increase productivity

**21**

Average number of custom\* SaaS apps used

*\*(e.g. an app developed internally, but hosted in AWS in a SaaS model for internal users)*



Reduce costs

Companies estimate that **70% of the business apps they use today are SaaS-based.**

**By 2025, they expect 85%** of the business apps they use will be SaaS-based.

[TWEET THIS](#)



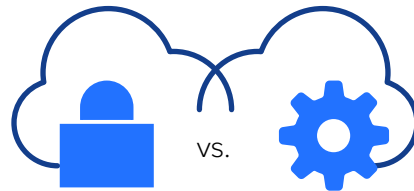
## Key Findings

# IT CHALLENGES AND CONCERNS

# 1:89

Average ratio of

**1 IT person : 89 employees**



### Balancing security vs. productivity

Respondents rated themselves in the middle, skewing *slightly more* toward productivity.

### TOP 5 Places where sensitive data lives

1. Files stored in cloud storage
2. Email
3. Devices
4. Chat apps
5. Password managers

TWEET THIS

### TOP 3 Most crucial challenges to solve

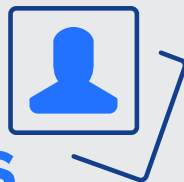
1. Manually onboarding and offboarding users
2. Securing sensitive data/files
3. Managing all SaaS apps in use

### TOP 2 Security concerns for IT teams

1. Sensitive files shared publicly
2. Former employees retaining data access

## EMPLOYEE ISSUES

# 7.12 hours



Average time to offboard a user across SaaS apps

### Almost everyone (92%)

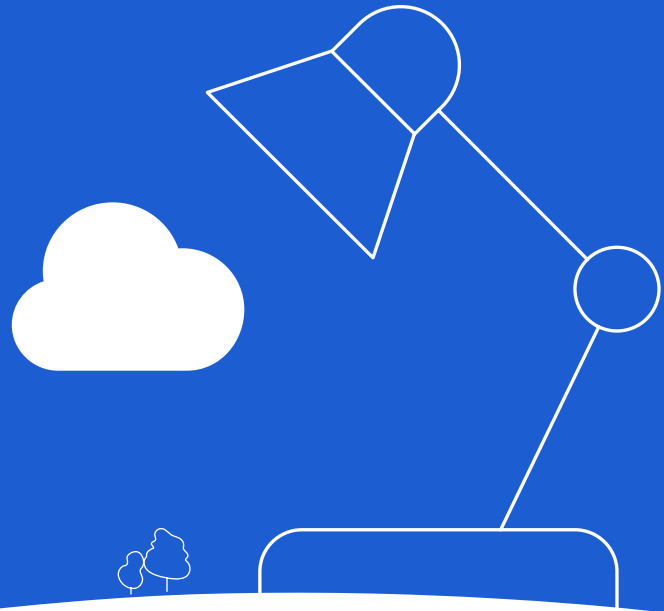
gives new employees access to devices on their first day.

### Entitlements & app

training (~40%) are much less common on day one.



# SaaS Steps into the IT Spotlight



2020 was a pivotal year for the SaaS market. Most companies already recognized how SaaS apps could make them more efficient and help them benefit from the pace of technology innovation. But nobody could have predicted that SaaS apps would also provide a critical lifeline for businesses caught in the fallout from a global pandemic.

That was especially true for companies forced to move from office-based to virtual teams. In this scenario, and in many others, SaaS apps and services played a critical role in keeping businesses operating and workers employed during the pandemic.

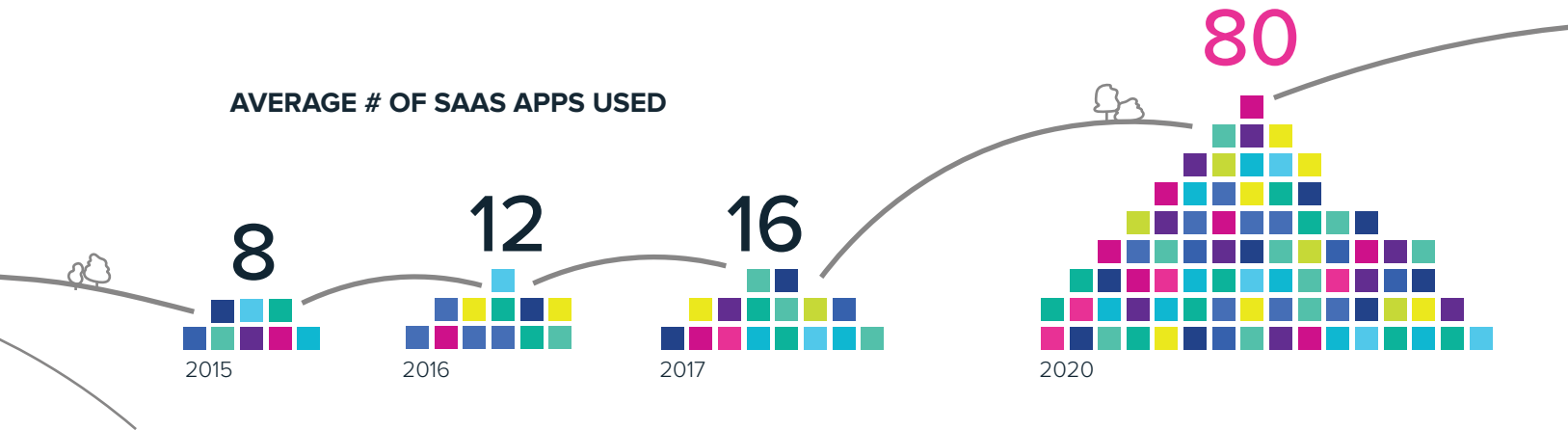


“[SaaS Ops] will be critical as more and more companies move to SaaS offerings and potentially more companies remain remote.”

— CTO, media company with 200 employees



While SaaS continues to save the day for many businesses, even more organizations are ready to migrate entirely to SaaS applications—or to get as close as possible to this goal. According to our research, companies today say they’re using five times as many SaaS apps than they were in 2017, and 10 times as many compared to 2015. These companies also tell us that SaaS applications now account for 70% of their total software usage, and that just 15% of their software will be non-SaaS products by 2025.



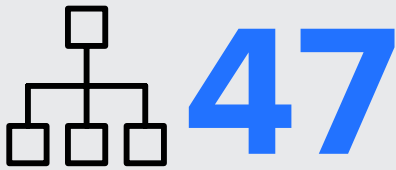
The use of unsanctioned SaaS apps, otherwise known as “shadow IT,” is one of the most daunting challenges for any IT administrator. Employees adopt unsanctioned SaaS apps for a wide range of reasons, but most people do so because they believe an unsanctioned app will improve their job performance—and that IT can’t or won’t support this goal. This makes shadow IT a key sign of a disconnect between IT and its customers within the business, and of changes in the business-IT relationship.

Progressive IT organizations understand that shadow IT isn’t a problem—it’s a symptom of a broken IT-business relationship.

 **SAASOPS INSIGHT**

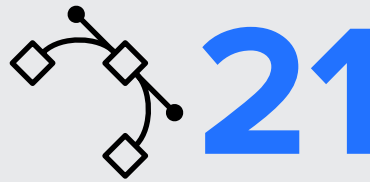
The best cure is to rebuild employee trust by partnering with shadow IT users to bring their apps into the light—securing them, managing them, and offering benefits such as integrations and upgrades.





47

Average # of  
**IT-owned apps**  
in 2020



21

Average # of  
**custom SaaS apps**  
used in 2020

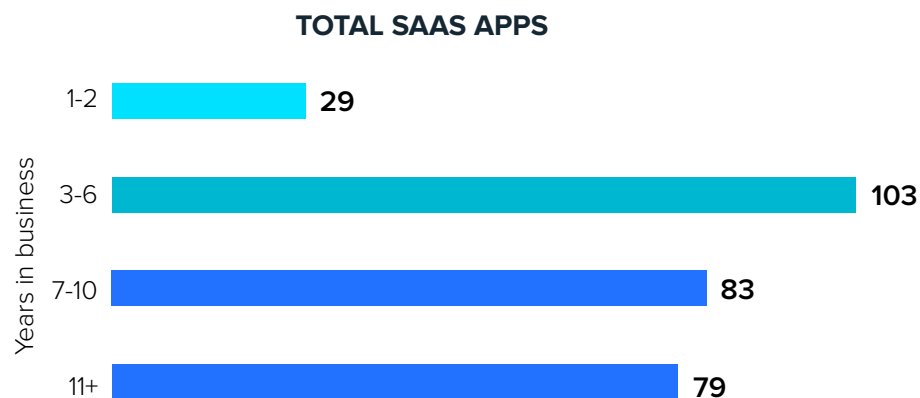


Survey respondents reported an average of 47 SaaS apps under direct IT ownership this year, compared to just 17 apps in 2017 and eight in 2015. This is a trend where positive momentum can be self-sustaining: As IT takes advantage of opportunities to deliver value through integration, shadow app owners feel more incentivized to come forward with similar requests.

## SaaS Adoption and Business Growth

People have a knack for accumulating things over time. Our research shows that companies have the same habit, especially when it comes to software. While younger companies typically start out with a few dozen apps, it doesn't take long for a growing organization to end up with 100 or more apps running within its walls.

Young companies (one to two years old) start out with 29 apps on average. **By the time they're three to six years old, that number spikes to 103.** The number comes down after that, likely because of consolidation.





Of course, with age comes maturity. We also discovered that companies approaching their second decade in business get serious about consolidating applications. Not surprisingly, large companies still use many more SaaS apps than smaller companies. Larger organizations also tend to add their own custom apps to the mix.

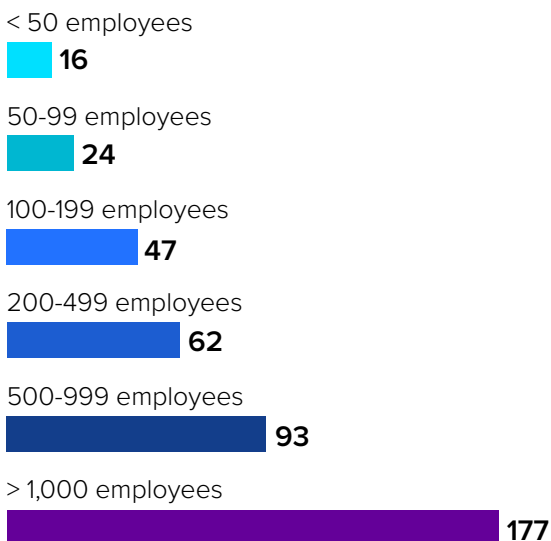
“I think that traditional systems administration is slowly merging with SaaS Ops and will continue to do so as more and more products and productivity suites move to SaaS-only models.”

– IT Director and Information Security Officer, advertising company with 600 employees

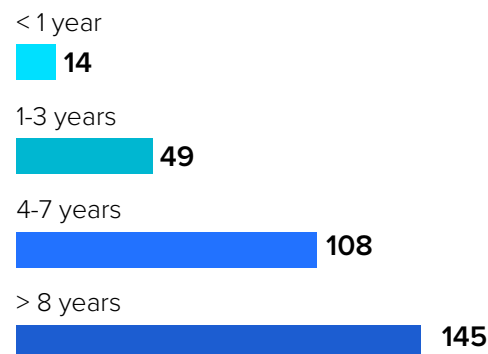


How many more total apps are used by companies that have SaaS Ops platforms as compared to those that don't

Not surprisingly, large companies use many more SaaS apps and custom apps than SMBs do.



The longer that companies use SaaS, the more SaaS and custom apps they use.





# Combating COVID-19: SaaS Innovation and IT Inspiration Win the Day



As the COVID-19 pandemic gained momentum in the spring of 2020, most U.S. businesses closed their offices and other non-essential facilities. Many businesses weathered the shutdown and avoided mass layoffs by shifting from more traditional workplace settings to work-from-home arrangements, distributed teams, and virtual workplaces.

☞ SaaS Ops will be the heart and soul of IT...Covid-19 has forced companies to adopt SaaS-based tools, and now they must continue to change and adapt or they will not survive.☞

– VP of Global IT, advertising company with 2,000 employees



Over the past decade, a number of infrastructure and software advances have combined to give businesses and employees everything they needed to more easily carry out this shift. SaaS apps played a critical role in this process, giving employees instant access to high-quality, low-cost productivity suites, collaboration tools, data- and document-sharing services, and other key applications, as well as by keeping them informed, engaged, and productive in home-office settings.



Pivoting an entire organization, even a smaller one, from a physical to a fully virtual work environment in a matter of weeks is an impressive feat. Our research shows many IT organizations faced changing organizational priorities even as they worked to prepare businesses for virtual arrangements:

### NEW PRIORITIES SINCE COVID

Upgrade VPNs to improve performance



Adopt new SaaS apps



Use more video conferencing



Make IT budget cuts



Better secure remote workplaces



Reduce IT staff



Reduce non-IT staff



Make IT's role within the business more prominent



Consolidate SaaS app functionality into fewer subscriptions



Make IT decisions that directly impact profitability



No changes



### TOP 3 new priorities



Use more video conferencing



Better secure remote workplaces



Make IT decisions that directly impact profitability





The type of rapid digital transformation that took place in the spring of 2020 couldn't have happened without the support of a versatile, responsive, highly innovative SaaS app ecosystem. In fact, these tools worked so well that many survey respondents are considering whether to turn these temporary arrangements into a more strategic (and usually more limited) shift towards distributed workplaces. Companies we surveyed also believe that long-term public health concerns will require businesses to keep their virtual workplace capabilities on standby, ready to play a bigger role when needed or perhaps supporting a permanent embrace of lower-density work environments.

“ Covid-19 has shown that we need to be more flexible in providing access to company data while making sure we keep our security protocols in place.”

– Director of IT, restaurant company with 1,200 employees



The modern, distributed workforce is here to stay—and, as a result, so is the need to manage, deploy, monitor, and secure SaaS environments on an unprecedented scale.

TWEET THIS A small white Twitter bird icon.



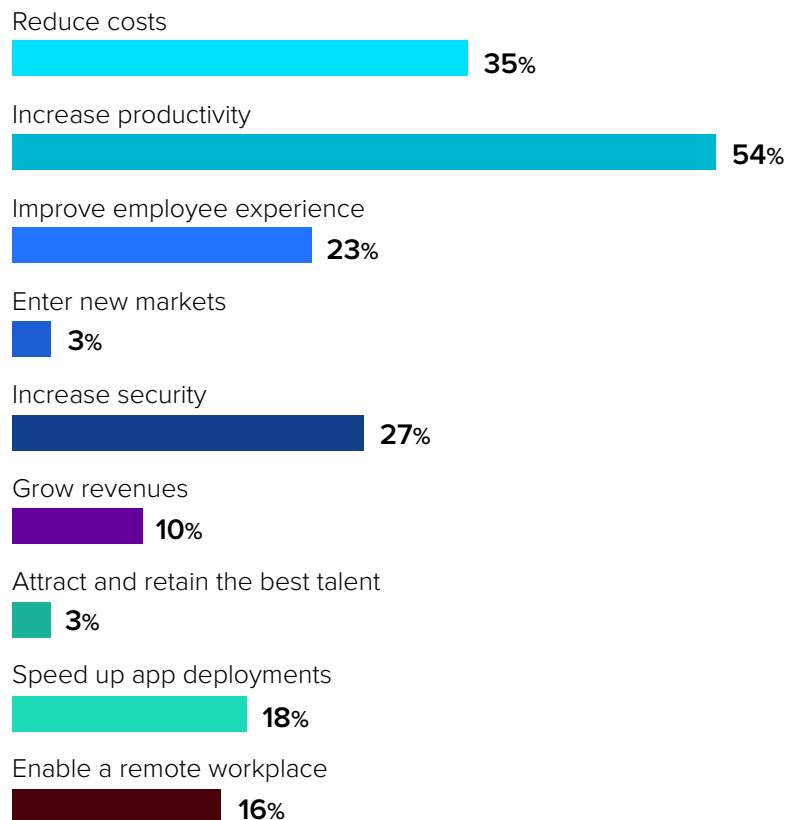


# Understanding the Attraction of SaaS

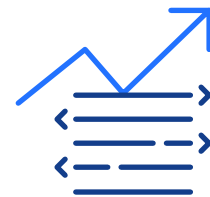


The promise of SaaS is that it offers organizations higher productivity and more collaboration, and can help create more engaged employees. In this “nirvana state,” employees can work securely, stay productive and motivated, and help drive organizational success.

## MOTIVATIONS TO USE MORE SAAS



## TOP 2 Motivators for Using More SaaS Apps



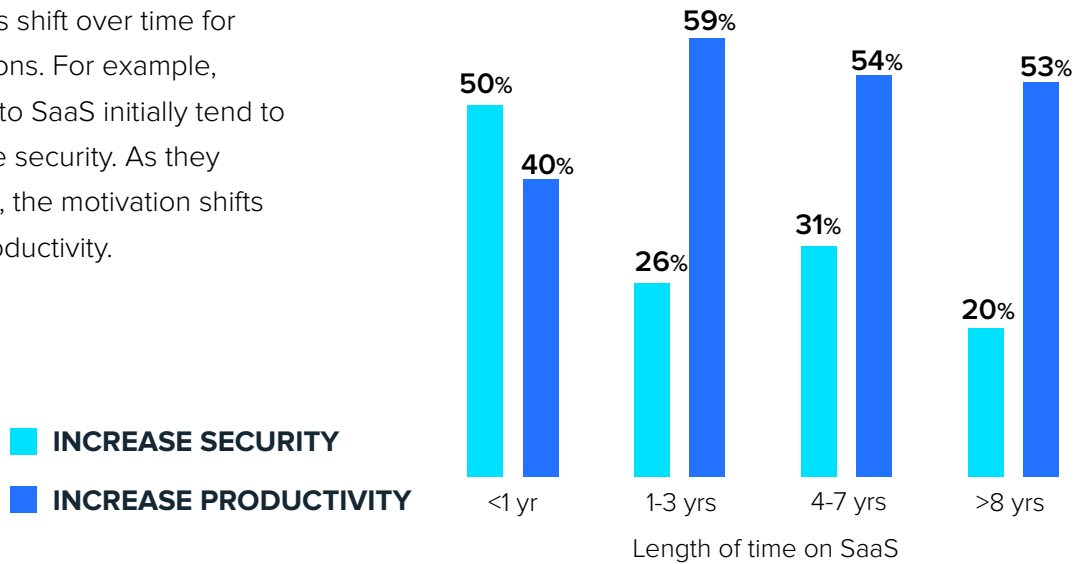
Increase productivity



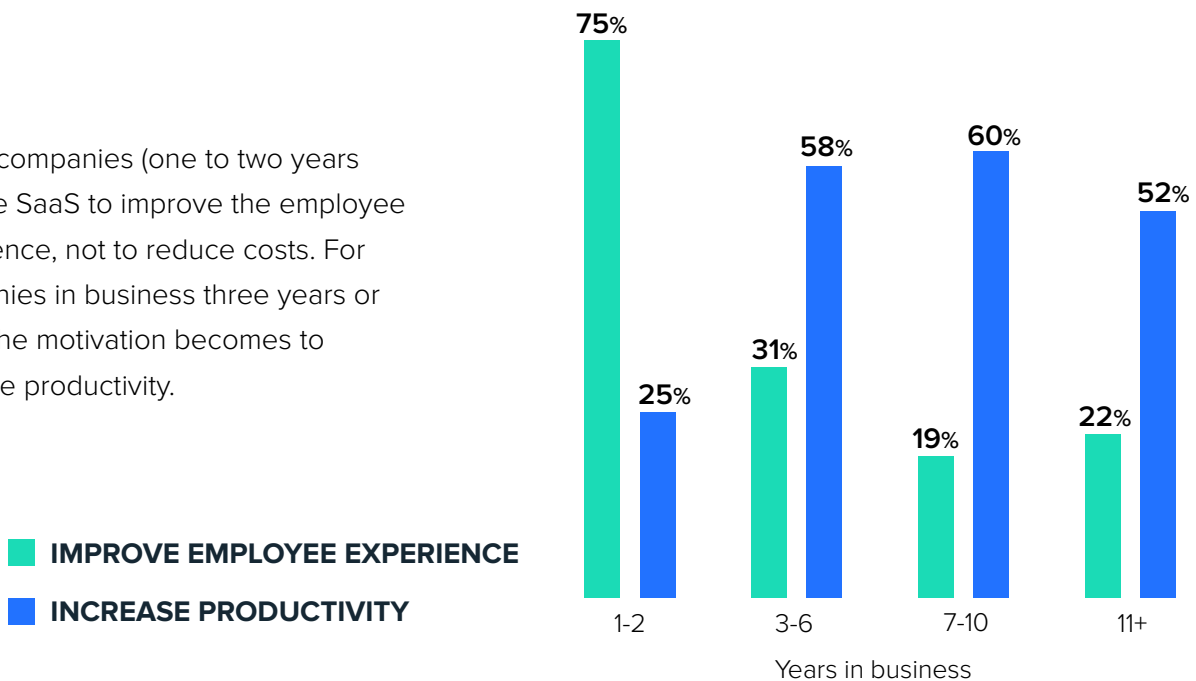
Reduce costs



Those motivators shift over time for some organizations. For example, companies new to SaaS initially tend to use it to increase security. As they continue using it, the motivation shifts to increasing productivity.



Young companies (one to two years old) use SaaS to improve the employee experience, not to reduce costs. For companies in business three years or more, the motivation becomes to increase productivity.



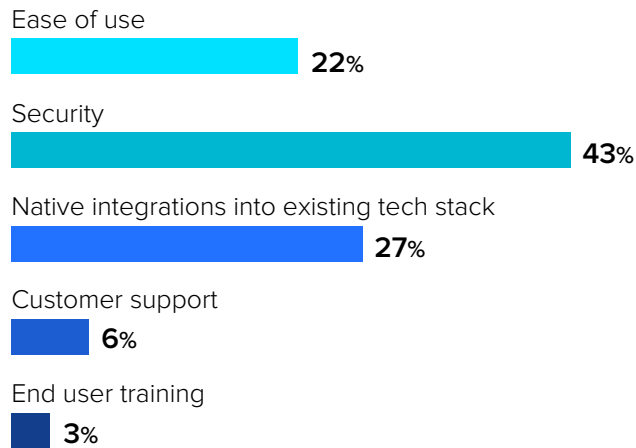


Assuming a new SaaS app meets cost and feature/function requirements, the top three criteria that respondents care most about are:

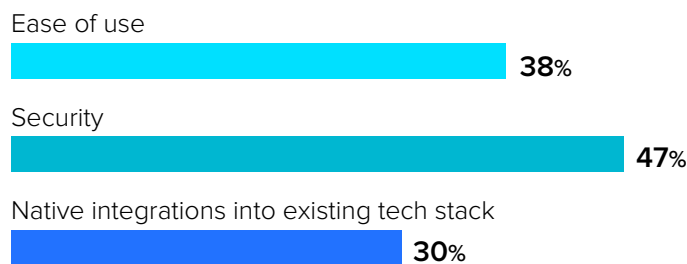


### WHAT ORGANIZATIONS CARE ABOUT MOST

#### 2020 FINDINGS

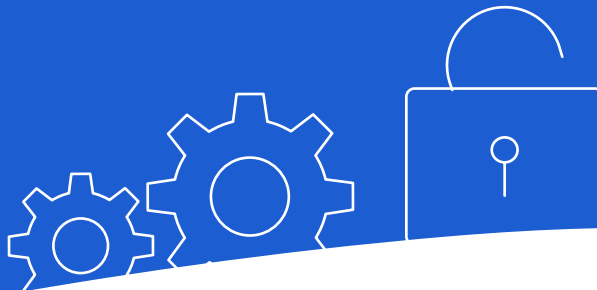


#### 2017 TOP 3 FINDINGS





# The Trouble with SaaS: Taking Stock of Visibility, Automation, and Security Challenges



One of the defining traits of the SaaS model is its ability to tear down traditional barriers to adopting and using software. This is why businesses were able to rely on employees to set up their own home offices virtually overnight, at little or no cost to the business or its IT resources. But it's also why SaaS presents significant challenges to IT organizations charged with managing and securing a company's SaaS app environment.

The SaaS model's ability to tear down traditional barriers to adopting and using software has been both a blessing and a curse for IT organizations.



 **SAASOPS INSIGHT**

As IT organizations scale their SaaS environments to manage more apps across bigger groups of users, they'll encounter new SaaS management challenges—and significant new sources of cost, complexity, and risk.

While some of these challenges deal entirely with technology questions, others are a function of the relationship—good or bad—between an IT organization and its business customers. All of these challenges tend to get more costly and complex, and much harder to solve, as organizations scale up their SaaS environments to manage more apps for more users.

Our research identified three issues that exemplify the challenges IT organizations face when administering SaaS apps vs. managing and securing SaaS apps, especially as they scale up their SaaS environments:

**1**

Disagreements over the true extent and nature of unsanctioned app usage, often combined with missed opportunities to gain better insights into these issues

**2**

An overreliance on tedious, labor-intensive tasks, many of which could be automated relatively easily

**3**

Pervasive, and potentially dangerous, data security issues

Let's look more closely at what the *2020 State of SaaS Ops* report uncovered about these challenges and their IT impacts.

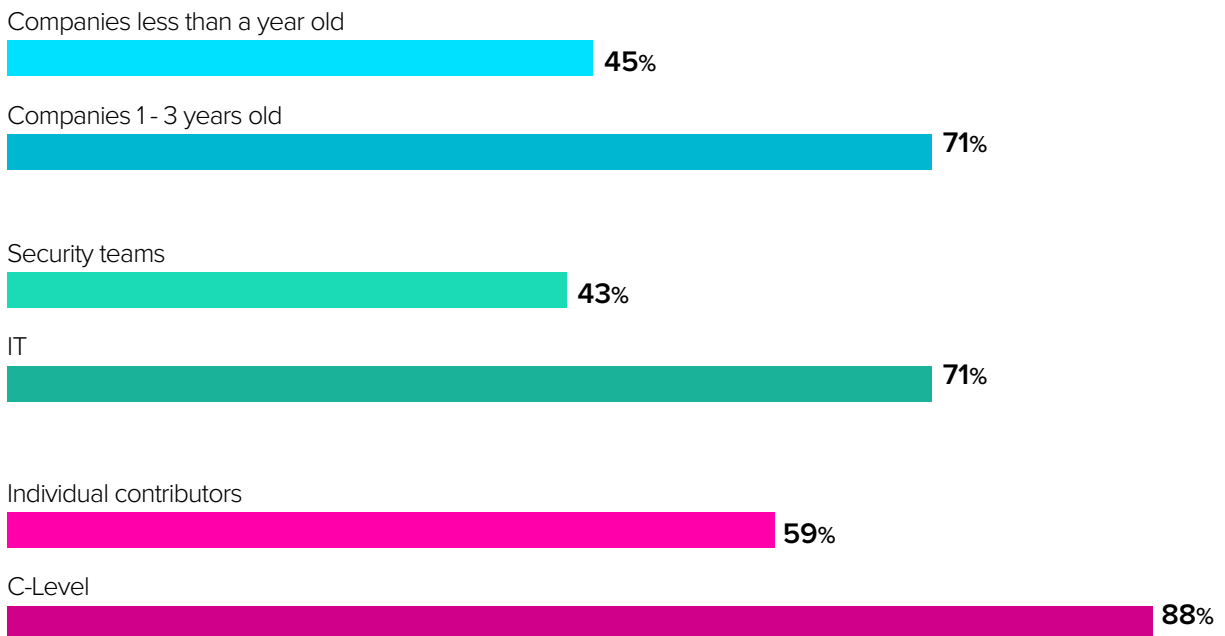


## SaaS Visibility: Missed Opportunities and Missing Insights

The first step any IT group can take toward effective SaaS management is getting an accurate app count. Overall, 72% of the professionals we surveyed said they were “very certain” of the total number of SaaS apps in use at their organizations.

Some stakeholders, however, are more confident in their app counts than others. Among the security professionals surveyed, for example, only 43% were very confident in their organizations’ SaaS discovery capabilities, as compared to 71% of IT professionals. And while 88% of C-level executives said they were “very certain” on this point, that number fell to just 59% for individual contributors.

### % OF PEOPLE OR COMPANIES “VERY CERTAIN” OF THE TOTAL NUMBER OF SAAS APPS IN THEIR ORGANIZATION





One in three companies surveyed aren't searching their networks for unsanctioned end user app subscriptions.

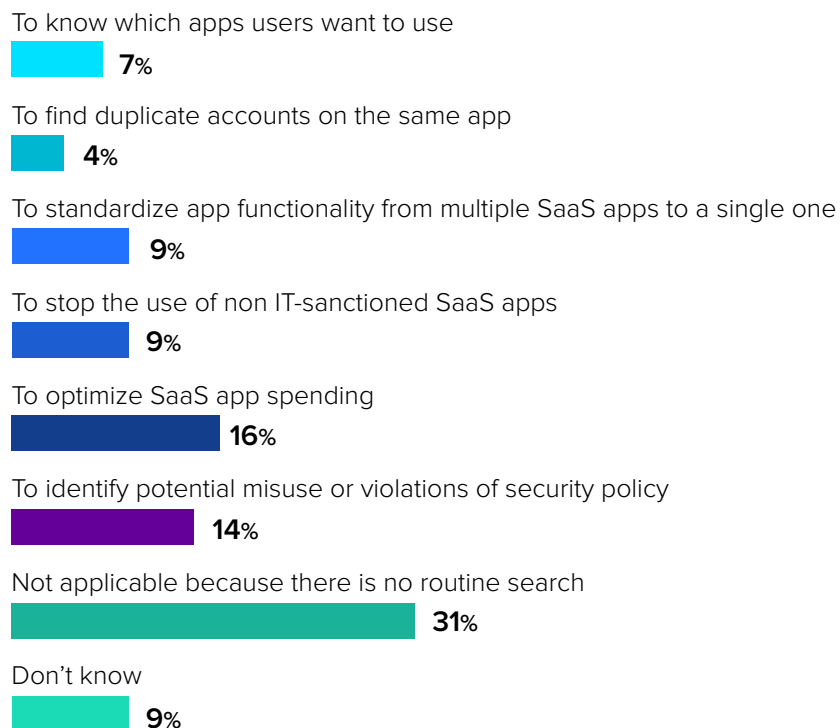
### SAASOPS INSIGHT

Monitoring SaaS app usage and tracking end user app subscriptions isn't about hunting down and penalizing employees who use shadow IT. It's simply a basic SaaS security and management task, and an essential IT activity.

It's noteworthy that nearly one-third of the companies we surveyed aren't searching regularly for end user app subscriptions on their organizations' networks. That's a significant number of businesses that aren't performing a basic SaaS security and management task.

On the other hand, it's also clear that only a few IT teams (9%) are treating unsanctioned app usage purely as a policy violation, which would do nothing to improve the underlying relationship between IT and business users. Instead, IT's motivations are more procedural:

#### WHY COMPANIES ROUTINELY SEARCHED THEIR NETWORK TO FIND NEW END USER APP SUBSCRIPTIONS



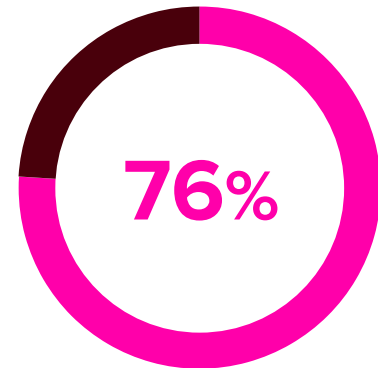




Additionally, we asked respondents how actively they're tracking usage of unauthorized applications—and many of them aren't tracking this activity at all. When asked to respond to the statement “We identify employees who use unauthorized apps,” 51% of respondents either disagreed with that statement or felt neutral.

Company size (# of employees)	# of third-party apps with read/ write access to Google Drive
0 to 199	35
200-499	69
500+	214

*Anonymized BetterCloud customer data*



of people are concerned about non IT-sanctioned apps creating security issues.

## Manual Tasks: Making SaaS Harder Than It Needs to Be

This year has been full of reminders that modern IT organizations are an extremely valuable and strategic business resource. However, 34% of the technology pros we surveyed spend half a week or more performing SaaS management tasks manually. Automation is hardly a radical new concept for IT management tasks, and if it's missing here, it's unlikely to show up for more difficult and time-consuming tasks, either.



“ [SaaS Ops is about] automation, automation, automation, and security.”

– CIO, manufacturing company with 500 employees



User offboarding is a great example of a task where automation pays off in a big way. Today, offboarding without the benefit of a SaaS Ops platform requires an average of 7.12 hours per user—and in some cases, offboarding a single employee can consume 16 hours or more of an IT practitioner’s time.



# 7.12 hours

Average time to offboard  
a user across SaaS apps



**SAASOPS INSIGHT**

Offboarding is a task that every IT organization can and should automate. Those that adopt a SaaS Ops platform can expect to discover additional opportunities to automate labor-intensive SaaS management tasks.

It’s a very different story for IT organizations that reported using SaaS Ops platforms to automate the offboarding process, which ultimately helps them recover precious hours for team members to spend on more rewarding and strategic tasks. One thing to note: The larger the company, the more complex it is to integrate all apps that every user touches. Because larger companies have hundreds of applications, the process to get them discovered and integrated into a SaaS Ops platform is still very much a work in progress.

### SAASOPS AUTOMATION OFFBOARDS

**34%**  
**FASTER**

<200

**136%**  
**FASTER**

200-499

**151%**  
**FASTER**

500-999

**49%**  
**FASTER**

>1,000

Total number of employees


Similar gains applied to companies that automate their SaaS-related help desk and support functions, such as account management, provisioning, and security. At companies with more than 1,000 employees and above-average SaaS use, SaaS Ops automation reduced the mean number of help desk tickets from 74 per week to less than 43. This is a remarkable workload reduction.



# SaaS Data Security: Learning to Balance Risk and Productivity

Everybody in IT today understands why data security is a very serious business with very little room for error. But the traditional security “lockdown” mindset is increasingly at odds with a business culture that relies on collaboration, sharing, and the agility to compete and innovate.

 The future is now.

Organizations need to begin finding ways to balance the ease of use and productivity that many SaaS apps allow for with the additional security concerns they impose. 

— Information Security Analyst, manufacturing company with 250 employees



In fact, SaaS applications demand a more flexible approach to data security. Typically, IT assumes that sensitive data is more likely to be found in a handful of commonly used SaaS apps, such as email and cloud storage services.

Businesses with less experience using SaaS are more likely to focus on five types of SaaS app they believe to be the top data security risks:

## TOP 5 Data security risks



Cloud storage files



Email



Devices



Chat apps

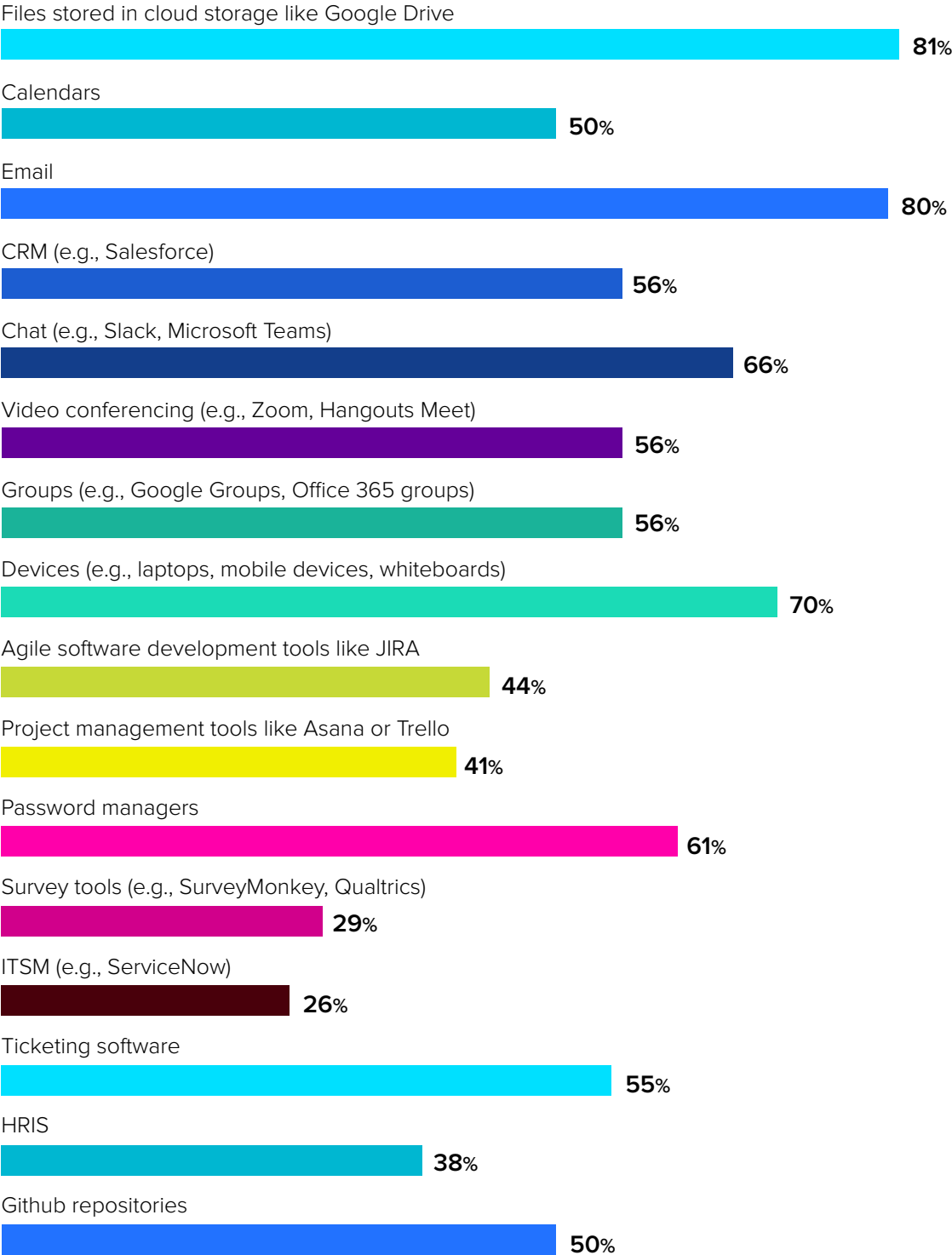


Password managers



Experienced SaaS users, however, are more likely to recognize the truth: Sensitive data can live anywhere and everywhere in a SaaS environment. This is why we gave respondents no less than 16 options for naming their top data security hot spots—and why every last one of these options got a significant number of responses!

### WHERE SENSITIVE DATA LIVES





Sensitive data lives everywhere in a SaaS environment—and a SaaS data security strategy must be comprehensive if it's going to be effective.

Data can live everywhere these days. SaaS apps have become systems of record for companies of all sizes. Inevitably, each application you add will become a source for sensitive data. The breadth and sprawl of the apps you use is limitless, and many apps live outside of IT's direct purview. While sensitive data has always lived within SaaS apps, many people are only beginning to understand the extent of it.

Organizations that focus their security efforts on certain SaaS apps at the expense of others are practicing what amounts to “security by coincidence.” Maybe an attacker will choose the “right” place to attack, maybe they won't. This was never a prudent data security stance, but it's especially risky as attackers get more resourceful and the threat landscape becomes increasingly diverse and dynamic.

## SaaS security priorities: automation and education

The nature of SaaS data security makes a lockdown mentality impractical and ineffective. A worthwhile solution should balance security and user productivity, while also accounting for the diverse and far-flung nature of potential security risks.

Automated discovery and monitoring tools  
are a good starting point for a realistic approach  
to SaaS data security.



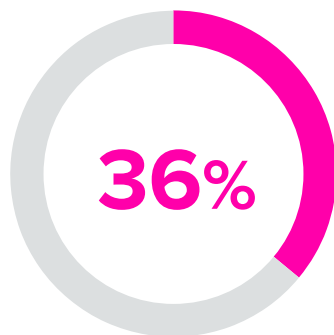


Automated tools for discovering potential security issues and for monitoring compliance with security best practices, such as those found in a modern SaaS Ops platform, are a good starting point for a realistic data security stance. Automated discovery and monitoring can alert IT to high-risk resource sharing practices (such as those identified below) and guide efforts to educate users on security policies and best practices.

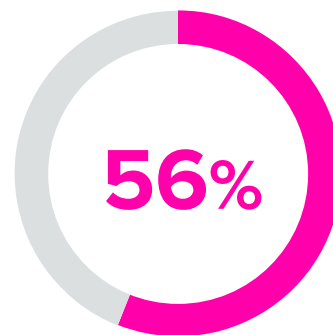
Company size (number of employees)	Average # of alerts for public email distribution lists	Average # of alerts for public calendars	Average # of alerts for forwarding work email to personal emails
0 to 199	115	5	45
200-499	314	10	96
500-4,999	1,376	38	340
5,000+	3,551	153	594

## Reducing exposure to SaaS management mistakes

As SaaS app environments become more complex, routine IT management tasks are more vulnerable to mistakes and oversights that create security risks. Many respondents point to employee offboarding—the process of revoking a departing employee’s access to systems and data stores—as an especially problematic SaaS management task:



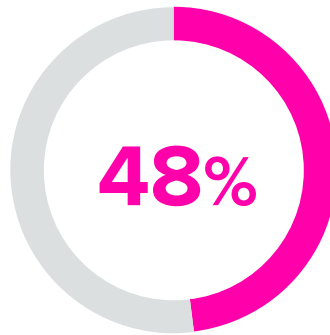
of respondents were less than fully confident that ex-employees were always locked out of file sharing and storage apps.



of respondents voiced similar concerns about access to department-specific applications.



Once again, automation and monitoring tools are significant pieces of the security puzzle here. But too many IT organizations clearly lack necessary capabilities in this area:



say they rarely/never or only sometimes monitor to prevent data exposure.

IT organizations often reveal a gap between what they think they know about their SaaS environments and what they actually know.



It's also important for IT organizations to invest in tools for discovering and understanding the SaaS environments under their management. More than once, respondents put themselves on the wrong side of a gap between what they think they know about their SaaS environments and what they actually know based on insights from BetterCloud user metrics.



“SaaS Ops will continue to grow its footprint in organizations, prompting a more sophisticated monitoring and management of SaaS apps.”

– VP of SaaS Ops, software company with 200 employees



For example, when looking at the enforcement of least-privileged access policies, IT practitioners consistently underestimated the number of users with SaaS app super admin privileges:

Company size (number of employees)	Estimated # of super admins per app by non-SaaS Ops users, according to survey	Average # of super admins, according to anonymized BetterCloud customer data
0 to 199	80% think they have 3 or less	5
200-499	65% think they have 3 or less	7
500+	48% think they have 3 or less	11

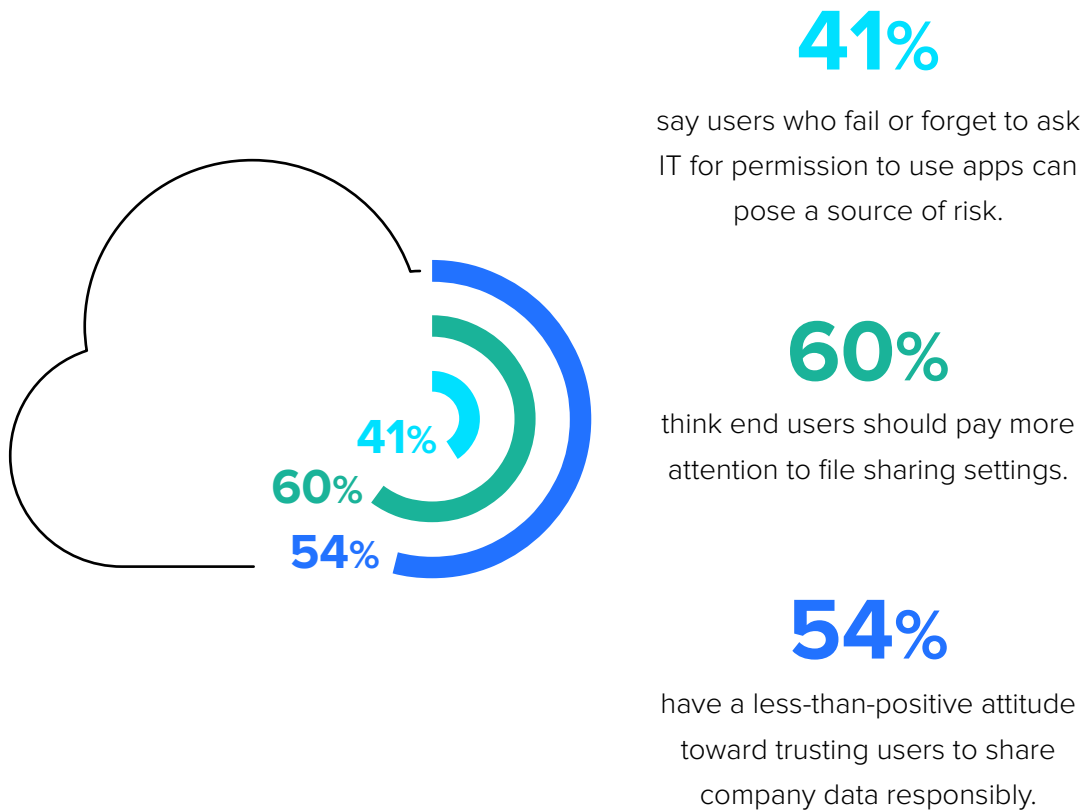
A similar disconnect emerges around perception vs. reality for the number of files with potentially sensitive data that are accessible to the public:

Company size (number of employees)	Estimated # of confidential/PII files shared publicly, per week, according to survey	# of alerts for confidential files with SSNs or credit card numbers shared publicly, per week, according to anonymized BetterCloud customer data
0 to 199	98	923
200-499	10	1,399
500+	128	12,454





Finally, respondents identified end users as the source for a number of key security risks. While there's a sense that users don't focus on security as much as they should—and a hesitation to trust users that share company data—most end user security lapses involve honest mistakes as opposed to gross negligence or malicious intent.

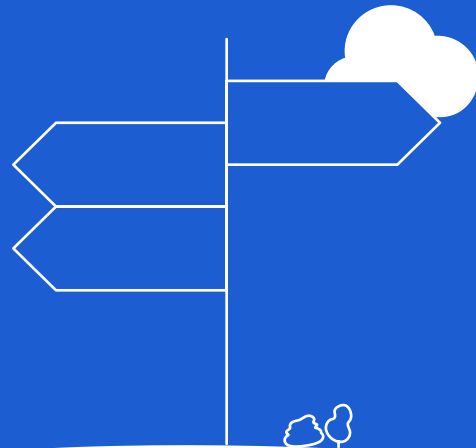


On a related note, the line between IT and security appears to be blurring: 45% of respondents say their department does *both* IT and security. And while security didn't always fall on the IT organization, the nature of SaaS has created a new set of security responsibilities for IT that didn't exist before, including defending against insider threats, securing data, and enforcing least-privileged access policies.





# SaaS Ops: Keeping SaaS Apps on the Path to Value



One of the goals of the *2020 State of SaaS Ops* report was to understand the true size and complexity of the challenges IT organizations face managing and securing SaaS app environments. It's especially important to recognize issues with cost, complexity, and risk that are getting more difficult to handle as businesses scale their SaaS environments—and that could, if left unchecked, eventually force businesses to rethink their commitment to SaaS.

In fact, many of the challenges we've discussed here do seem to be tied to the emergence of bigger and more complex SaaS environments. A number of IT organizations still lack the tools and methods needed to deliver solutions, and there's a definite risk that adopting SaaS at scale will make things much worse before they get better.

## SAASOPS INSIGHT

SaaS Ops gives IT organizations a comprehensive discipline for discovering, managing, and securing SaaS apps at scale, using centralized and automated tools.

TWEET THIS 





But IT organizations are taking a proactive approach to solving the challenges that come with managing and securing SaaS at scale. Specifically, these organizations are adopting SaaS Ops: a discipline for discovering, managing, and securing SaaS apps, using centralized and automated tools and a standard framework for applying these tools.

☞☞ SaaS Ops and IT will be synonymous. There's no separating the two already in most modern/young companies.☞☞

— IT Manager, insurance company with 270 employees



SaaS Ops is proving its value for managing SaaS environments at scale, and IT organizations are responding with a groundswell of support for SaaS Ops tools, methods, and problem-solving approaches. In fact, SaaS Ops appears to be taking a significant step in 2020: establishing itself as a core IT discipline and shaping how IT practitioners think about their skill sets, careers, and even job titles.

All of this shows that SaaS Ops is making a difference where it matters: in real-world situations where IT practitioners need proven and practical tools for managing SaaS at scale. These changes will help prepare IT for a future where SaaS shapes and dominates the technology landscape.

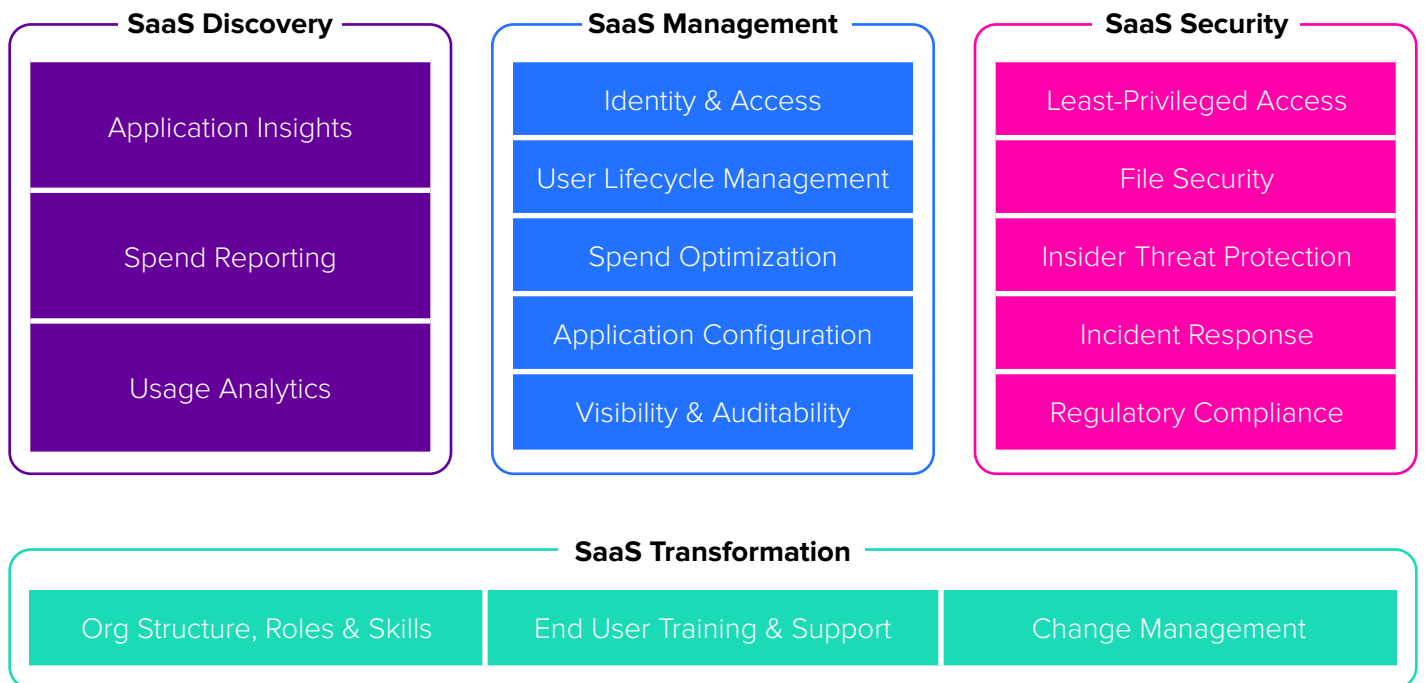
 **SAAS OPS INSIGHT**

Just as SaaS is driving a revolution in how businesses deploy and use software, SaaS Ops is driving a fundamental shift in how IT organizations—and even individual IT practitioners—approach SaaS management and security issues.



## The SaaS Ops Framework: Processes and Priorities

The SaaS Ops Framework is the key to understanding SaaS Ops as a living, breathing highly adaptable IT discipline. It aligns with each of the three SaaS Ops functional pillars—discovery, management, and security—to help IT assess and implement SaaS Ops tools. It also ties in key processes that organizations can use to transform and elevate their SaaS performance.

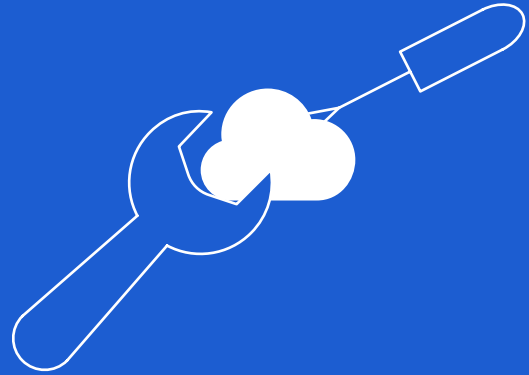


The real question, of course, is exactly how IT organizations apply the SaaS Ops Framework and other resources to solve their SaaS challenges and to make SaaS management simpler and less expensive. Based on research and conversations with practitioners, five key trends are shaping SaaS Ops use and adoption in the field.





# 5 Things to Know About Working with SaaS Ops



## 1. IT organizations have defined a “SaaS Ops tech stack” for managing and securing a SaaS environment.

IT organizations occupy a wide range of positions on an emerging SaaS Ops tech maturity curve.

Most have implemented native admin consoles.



Most have implemented scripts.



Nearly half have implemented Identity as a Service (IDaaS) tools for their SaaS environment.



About one in five are using Cloud Access Security Brokers (CASBs).



A quarter are either using integrated SaaS Ops solutions or plan to adopt one.



Across the spectrum, the most effective SaaS Ops stacks appear to be those that move proactively to acquire and implement a complete set of tools rather than those that make piecemeal acquisitions only as pain points emerge.



**SAASOPS INSIGHT**

Organizations expect a modern SaaS Ops platform to give them the best of both worlds: first-class data security tools plus a no-compromises approach to innovation and productivity.

## 2. Automation is a core SaaS Ops function, but only a handful of IT organizations have completed this journey.

Most respondents (75%) are still automating operational processes, compared to just 9% that say they're done. Organizations with a longer history of using SaaS also have longer and more complex automation priorities to address. By comparison, SaaS Ops users tend to have a higher level of automation maturity across the board.

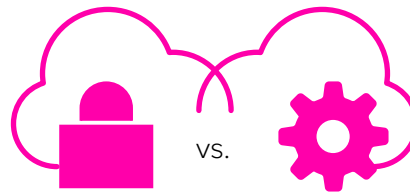
Company size (number of employees)	Time needed to offboard one user without automation	Average amount of time a company with a SaaS Ops platform was required to execute automated offboarding workflows
0 to 199	3 hours	<b>12 minutes</b>
200-499	7 hours, 30 minutes	<b>1 hour, 10 minutes</b>
500+	5 hours, 20 minutes	<b>38 minutes</b>





### 3. SaaS Ops challenges IT organizations to think carefully about the balance between security and productivity, though the latter is gradually coming out on top.

To some extent, how IT strikes the balance between security and productivity depends on its industry sector, but there's a gradual trend in favor of productivity. We believe that by this time next year, SaaS Ops will support an even more pronounced tilt towards productivity.



#### **Balancing security vs. productivity**

Respondents rated themselves in the middle, skewing *slightly more* toward productivity.

This doesn't mean IT is ready to discount security as a top priority; it simply reflects the role that SaaS plays in supporting employee productivity, collaboration, and engagement. Security will always be imperative, but productivity gets to the reason why most companies implement SaaS apps in the first place.



Security is essential, but productivity is the motivating factor behind why most companies turn to SaaS apps in the first place.

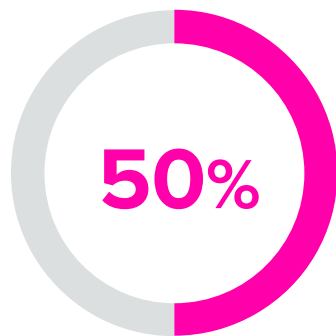




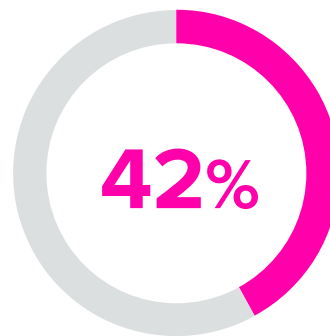
## 4. How IT implements SaaS Ops is consistent with a team's own pursuit of modern priorities and practices.

As we pointed out earlier, very few IT groups are pressing a traditional agenda focused on order-taking, maintenance, and gatekeeping duty. Instead, 62% of respondents said their IT groups are focused on innovation, revenue growth, and creating superior user experiences.

### WHEN AN IT ORGANIZATION ADOPTS A SAASOPS PLATFORM:



are more likely to emphasize user experience as a priority.

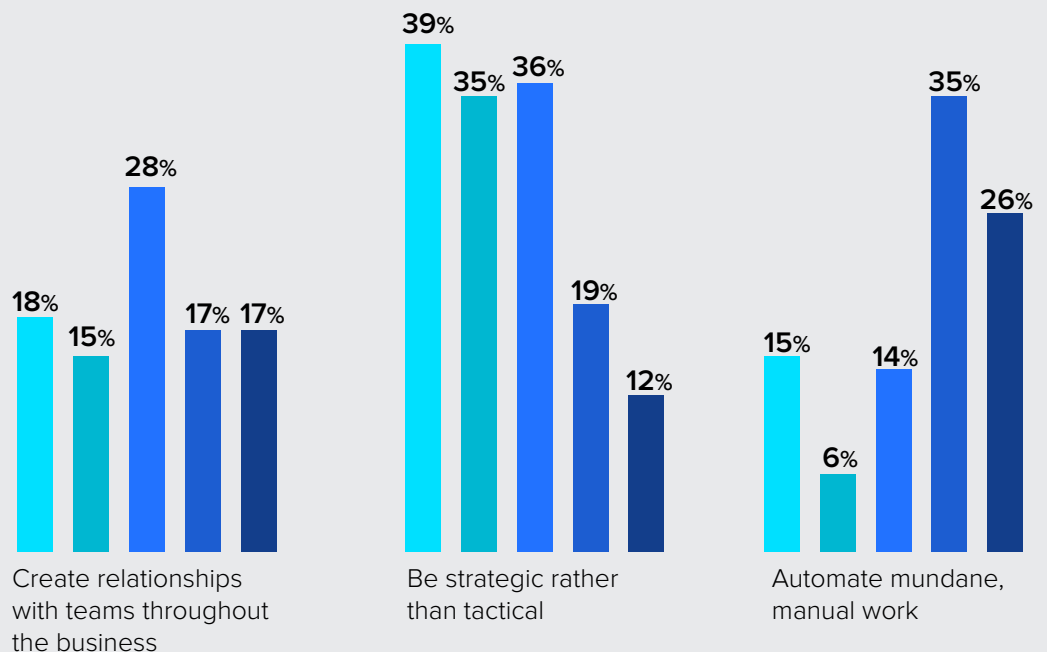


are less likely to cite tech repair and maintenance as primary tasks.

On an individual basis, respondents tend to select priority tasks based on their job role, but these are generally consistent with a self-image now anchored firmly on their strategic importance and impact.

### TOP THREE CAREER GOALS FOR INDIVIDUALS

- C-level
- VP
- Director
- Manager/mid-level
- Individual contributor







## 5. SaaS Ops gives IT an important set of tools for delivering on the promise of SaaS and creating a modern digital workplace.

From onboarding and training to enhancing productivity, SaaS Ops platforms appear to generate value from SaaS applications faster while ensuring that value translates directly into strategic business outcomes. Nearly three out of four SaaS Ops platform users, for example, agree with the idea that they're using SaaS to create a modern digital workplace for users and, in the process, improving end user productivity.

### SAAS OPS INSIGHT

SaaS Ops platforms don't just benefit IT organizations. By maximizing SaaS performance and productivity, a SaaS Ops platform can also improve employee productivity and engagement, and move the needle on a company's profitability and performance.

#### WHEN IT GIVES NEW EMPLOYEES ACCESS TO SAAS APPS

**40%**  
before first day



**45%**  
by EOD, day 1



## ON DAY ONE, WHAT RESOURCES DOES AN EMPLOYEE GET ACCESS TO FOR SAAS APPS VS. NON SAAS APPS?

Corporate-owned devices (e.g., laptop)



SaaS apps



Entitlements



Group membership



Calendars



SaaS apps training



Does not use a SaaS Ops platform

Uses a SaaS Ops platform

SaaS Ops accelerates the process of getting value from SaaS and ensures that value translates into strategic business outcomes.





# SaaS Ops Gives SaaS the Future It Deserves



## If there's one word that describes the state of SaaS Ops, it's momentum.

SaaS has already reshaped almost every aspect of the technology industry, from how teams build software to how consumers use it. And now, at a critical stage in the evolution and impact of SaaS, SaaS Ops has earned increased loyalty, support, and budgets from a sizable and growing set of IT organizations. SaaS Ops is even influencing the evolution of IT job titles: **30% of the respondents to our survey already have SaaS Ops in their job title or plan to include it soon.**

The momentum around SaaS Ops isn't being driven by hype or hot air. SaaS Ops is gaining ground because it's necessary; it offers practical and highly effective solutions to increasingly urgent IT challenges. As SaaS environments struggle with the impacts of app sprawl, surging adoption, and business growth, SaaS Ops gives IT a single framework for solving all of these problems. From management and discovery to automation and security, SaaS Ops was designed to take the pain out of working with SaaS at scale. It also gives IT an effective set of tools for managing SaaS without sacrificing its new emphasis as a strategic business function.

In every way that matters, SaaS Ops offers tangible IT value to teams, individual practitioners, and other business technology stakeholders. And by solving the challenges that come with adopting SaaS at scale, SaaS Ops is quite literally securing the future for software as a service.

SaaS Ops is quite literally securing the future  
for software as a service.





## Methodology

This survey was conducted online from April 15, 2020 to May 15, 2020. 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.

To report product data, we analyzed and anonymized data from thousands of BetterCloud customers across a variety of company sizes and industries. The product data represents customer activity from January 1, 2020 to July 3, 2020.

## About BetterCloud

BetterCloud is the leading SaaS Ops platform that enables IT professionals to discover, manage, and secure the growing stack of SaaS applications in the digital workplace. With an expanding ecosystem of SaaS integrations, thousands of forward-thinking organizations like Zoom, Walmart, and Square now rely on BetterCloud to automate processes and policies across their cloud application portfolio.

For more information, please visit [www.bettercloud.com](http://www.bettercloud.com).

For a demo of the leading SaaS Ops platform, please visit [www.bettercloud.com/request-a-demo](http://www.bettercloud.com/request-a-demo).

