BetterCloud REPORT

# State of Insider Threats in the Digital Workplace

2019

# Introduction

While cybercriminals, hacktivists, and ransomware often make a big splash in the news headlines, the reality is that the biggest security threat is often right in front of you.

Insiders–people already in your organization–pose a pervasive security risk, whether their behavior is malicious or accidental.

In fact, according to the 2016 U.S. State of Cybercrime report by *CSO Magazine*, insiders were the source (or cause) of the following:

- 50% of incidents where private or sensitive information was unintentionally exposed
- 40% of incidents where employee records were compromised or stolen
- 33% of incidents where customer records were compromised or stolen
- 32% of incidents where confidential records (i.e., trade secrets or intellectual property) were compromised or stolen

And with the rise of SaaS applications, it's easier than ever to expose private or sensitive data, whether it's intentional or not.

New attack vectors and data leakage points are emerging in SaaS apps. As a result, a new type of insider threat is taking shape.

New attack vectors and data leakage points are emerging in SaaS apps. As a result, a new type of insider threat is taking shape.

**What makes this new breed of insider threats especially insidious? It stems primarily from the well-meaning but negligent end user**. In the age of SaaS, where end users interact with and share data freely, it can spell trouble.

Featuring survey data from 500 IT professionals, proprietary product data from 2,000+ BetterCloud customers, and commentary based on BetterCloud's 7+ years of industry experience, this is the most comprehensive insider threats report to date.

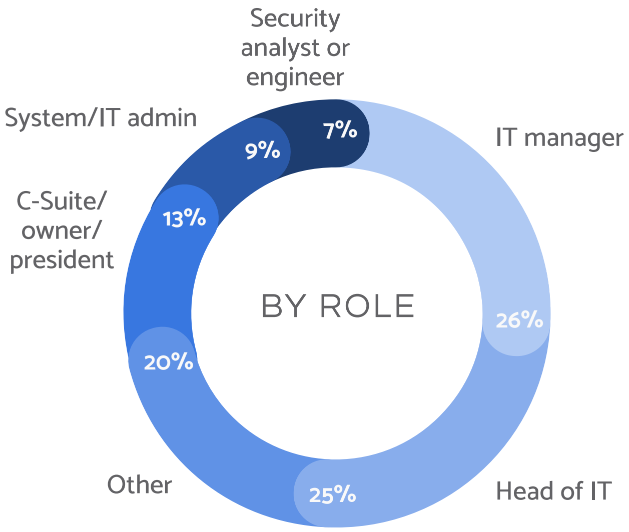
The data provides insight into a nascent generation of risks, shedding new light on where IT and security professionals feel the most vulnerable, what they feel most vulnerable to, and how they're mitigating insider threats.

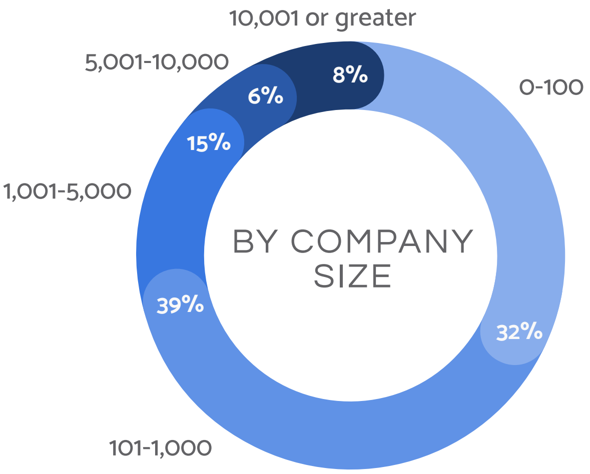
How are we defining *insider threats*? We took the definition from the CERT Guide to Insider Threats and modified it slightly. In the context of this report, an insider threat is defined as a current or former employee, contractor, or business partner who has access to an organization's network, systems, or data and is either:

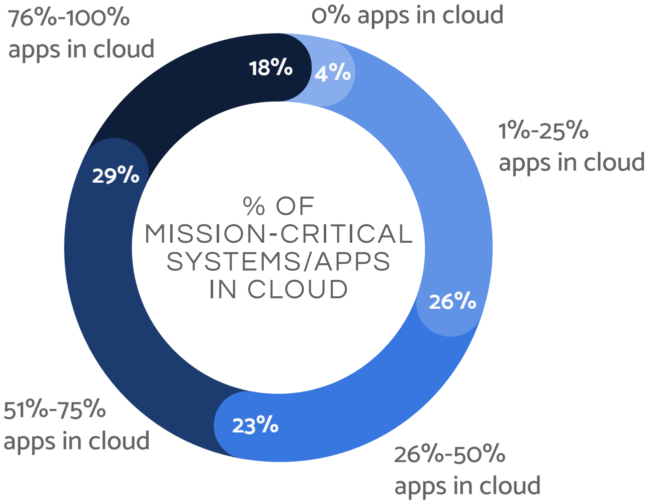
- Compromised *(exploited by outsiders through compromised credentials)*
- Malicious *(intentionally causes harm, either for personal or financial gain)*
- Negligent *(well-meaning, but accidentally exposes sensitive information)*

# Demographics

We surveyed **491 IT and security professionals** in October 2018. The respondents range from C-level executives to IT admins to security engineers, representing organizations of varying sizes (less than 100 employees to 10,000+) across all industries. These organizations are also at various stages in their cloud journey.

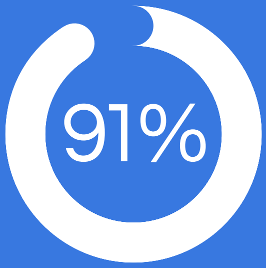






# Key Findings

BetterCloud

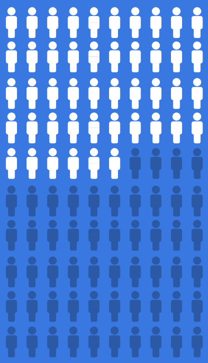


feel vulnerable to insider threats.

**62%** of respondents believe the biggest security threat comes from **well-meaning but negligent end users.**

**75%** believe the biggest security challenge lies in **cloud storage/file sharing and email.**

of people using a CASB still feel vulnerable to insider threats.



**46%** of IT leaders (heads of IT and above) believe that the rise of SaaS applications makes them the most vulnerable to insider threats.

**74%** of C-level executives don't think they've invested enough to mitigate the risk of insider threats.

## What companies feel the most vulnerable to

**40%** Exposure of confidential business information
*Financial information, customer lists, transaction histories*

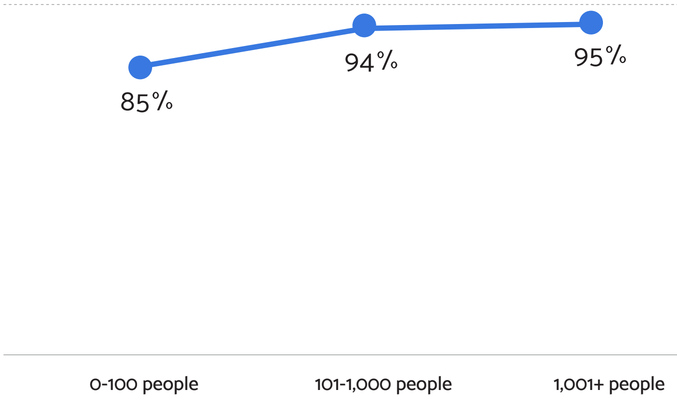
**30%** Exposure of customer data

**13%** Exposure of employee data

**17%** Exposure of IP
*Trade secrets, research, confidential roadmaps*

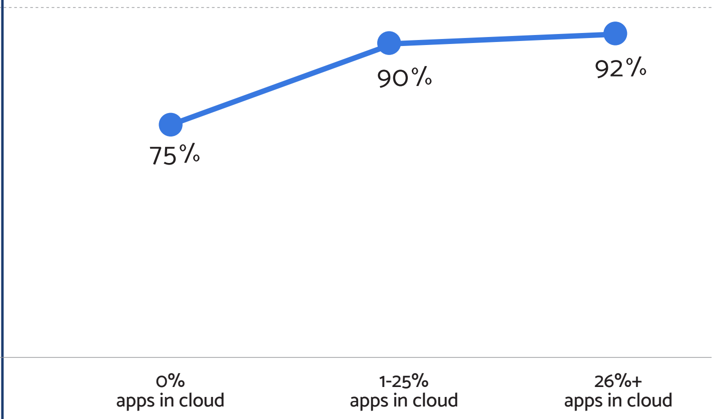
## Percentage of companies that feel vulnerable to insider threats

### BY COMPANY SIZE



As companies grow in size, they feel increasingly vulnerable to insider threats.

### BY % MISSION-CRITICAL APPS IN CLOUD



As companies adopt more SaaS applications, they feel increasingly vulnerable to insider threats.

INTRODUCTION

# The Evolving Security Landscape

In today's digital workplace, traditional security tools are protecting the wrong things.

"The tools and technologies used to protect organizations from hacks and attacks weren't designed for today's challenging business and IT environments," writes SecurityRoundtable.org. "Firewalls, intrusion-detection systems, malware protection, and simple whitelists and blacklists worked relatively well when organizations had few entry points for user access–and limited data to manage."

But today, employees use multiple endpoints (desktops, laptops, tablets, smartphones, Chromebooks, etc.) to work from any place, at any time. Each endpoint connects to the corporate network and represents a potential point of ingress for attackers. The amount of data to manage is also staggering. SaaS is creating a massive information sprawl, the likes of which IT has never seen before.

> So where does your data live today? It's not on your endpoints. It's in your SaaS apps.

SecurityRoundtable.org goes on to say: "The perimeter has disappeared. It's no longer about protecting boundaries, it's about protecting data."

So where does your data live today? It's not on your endpoints. It's in your SaaS apps.

In 2017, companies used 16 SaaS apps on average, up 33% from the previous year. In fact, 73% of organizations say nearly all (80%+) of their apps will be SaaS by 2020. Your confidential business data, your trade secrets and intellectual property, your employee data, your customer data–all of this lives in your SaaS apps because SaaS is the system of record now.

With the rise of SaaS comes a whole new type of insider threat.

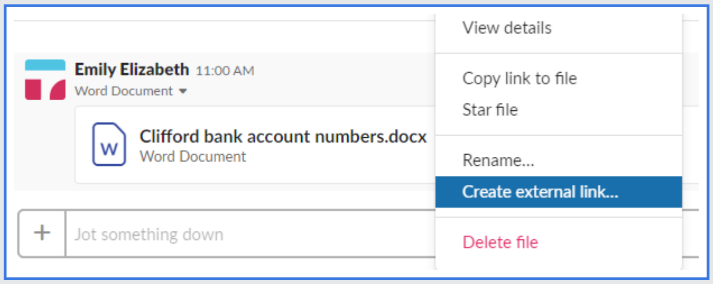
INTRODUCTION

# New Security Risks

SaaS is creating a new generation of insider threats for three reasons:

1. **End users have a *lot* of freedom and power when using SaaS apps (and as a result, IT and security teams are losing control)**

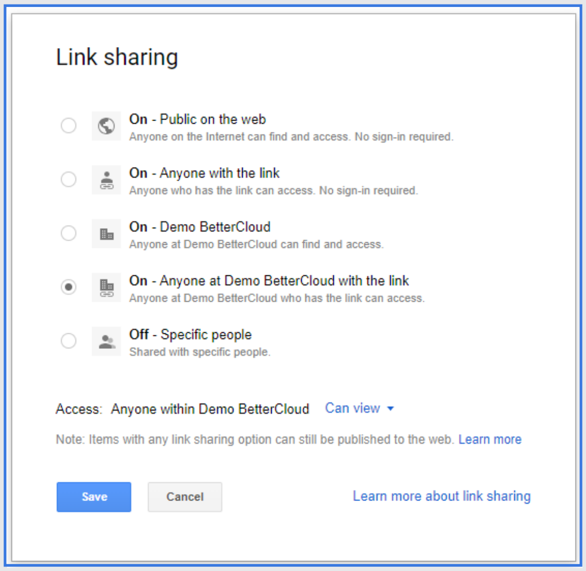
More than ever before, end users are empowered with countless ways to collaborate and interact with data and other users. With SaaS apps, users can share files freely with just about anyone inside or outside the org: colleagues, partners, customers, contractors, even competitors. They can share documents, calendars, spreadsheets, and presentations publicly on the web, meaning anyone on the Internet can find and access them, since these files are scraped and indexed by search engines. They can create public links to files in seconds. They can add themselves to distribution lists and groups. They can adjust permissions and sharing settings on their own.



Emily Elizabeth 11:00 AM
Word Document ▾

Clifford bank account numbers.docx
Word Document

SLACK



Link sharing

○ On - Public on the web
Anyone on the Internet can find and access. No sign-in required.

○ On - Anyone with the link
Anyone who has the link can access. No sign-in required.

○ On - Demo BetterCloud
Anyone at Demo BetterCloud can find and access.

● On - Anyone at Demo BetterCloud with the link
Anyone at Demo BetterCloud who has the link can access.

○ Off - Specific people
Shared with specific people.

Access: Anyone within Demo BetterCloud Can view ▾

Note: Items with any link sharing option can still be published to the web. Learn more

G SUITE BUSINESS

Of course, all of this freedom is by design. It's what makes SaaS such a boon to productivity. But it's also exactly why it is *very* easy to expose data through these interactions, either intentionally or unintentionally.

2. **SaaS creates dangerous blind spots– hidden security threats that many IT and security professionals don't even know exist**

Because SaaS is so new, everyone's sort of "figuring things out as they go." Not enough time has passed for official certifications or industry best practices to exist.

In fact, 78% of IT professionals are just getting started managing SaaS apps or teaching themselves.

As a result, IT and security teams are unaware of emerging security threats (aka blind spots) that accompany SaaS applications. Specifically, these blind spots refer to new avenues for data exposure and leakage.

On a recent webinar poll, we found that 86% of IT professionals think (or aren't sure if) they have confidential/sensitive data exposed, and 76% of IT professionals believe that former employees still have access to their organization's data.

### 3. File sharing permissions and configurations are complex

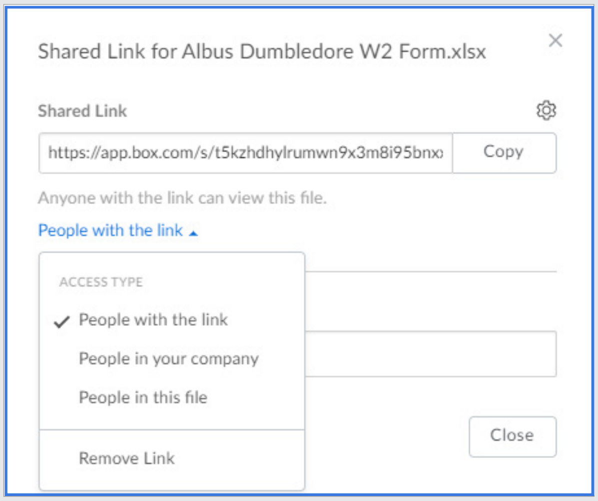
In 2018, the Kenna Security research team discovered a widespread misconfiguration in Google Groups that exposed sensitive information. Three thousand organizations, including Fortune 500 companies, hospitals, universities, television stations, and US government agencies, were leaking "some form of sensitive email."

The reason for the misconfiguration?

"Due to complexity in terminology and organization-wide vs. group-specific permissions, it's possible for list administrators to inadvertently expose email list contents," Kenna Security wrote. "In practice, this affects a significant number of organizations."

The terminology and permissions in collaboration software are confusing, no doubt.

There are dozens of privacy and access settings for both end users and admins alike:



Shared Link for Albus Dumbledore W2 Form.xlsx

Shared Link

https://app.box.com/s/t5kzhdhylrumwn9x3m8i95bnxo

Anyone with the link can view this file.

People with the link ▴

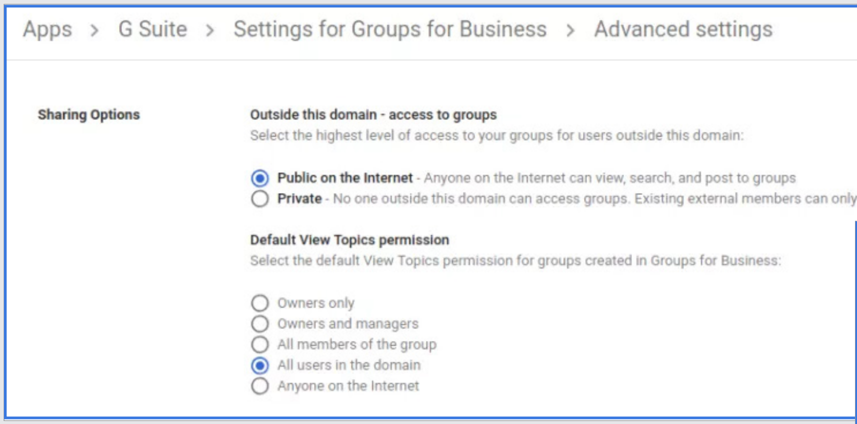
ACCESS TYPE

✓ People with the link

People in your company

People in this file

BOX (BUSINESS)



Apps > G Suite > Settings for Groups for Business > Advanced settings

**Sharing Options**

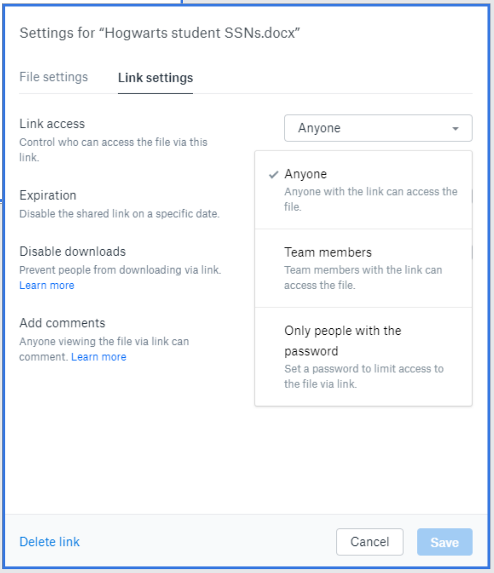
**Outside this domain - access to groups**
Select the highest level of access to your groups for users outside this domain:

● **Public on the Internet** - Anyone on the Internet can view, search, and post to groups
○ **Private** - No one outside this domain can access groups. Existing external members can only send email to groups.

**Default View Topics permission**
Select the default View Topics permission for groups created in Groups for Business:

○ Owners only
○ Owners and managers
○ All members of the group
● All users in the domain
○ Anyone on the Internet

G SUITE BUSINESS



Settings for "Hogwarts student SSNs.docx"

File settings | **Link settings**

Link access
Control who can access the file via this link.

Anyone ▾

✓ Anyone
Anyone with the link can access the file.

Team members
Team members with the link can access the file.

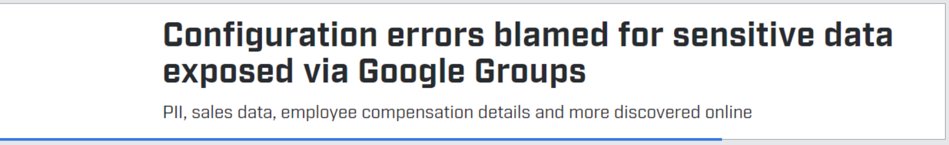
Only people with the password
Set a password to limit access to the file via link.

Expiration
Disable the shared link on a specific date.

Disable downloads
Prevent people from downloading via link. Learn more

Add comments
Anyone viewing the file via link can comment. Learn more

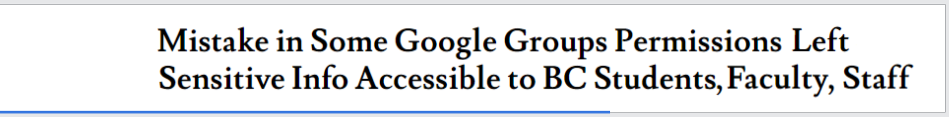
DROPBOX BUSINESS (STANDARD)



**Configuration errors blamed for sensitive data exposed via Google Groups**

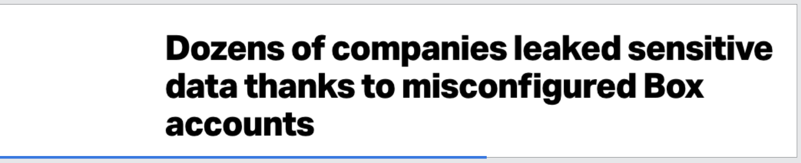
PII, sales data, employee compensation details and more discovered online

CSO | JULY 2017



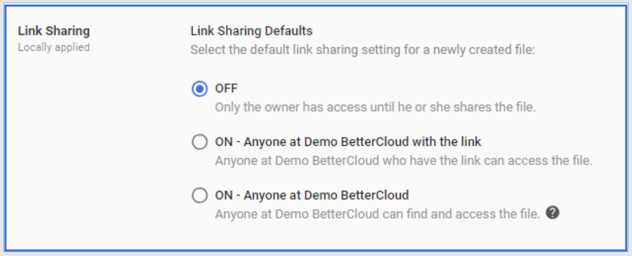
**Mistake in Some Google Groups Permissions Left Sensitive Info Accessible to BC Students, Faculty, Staff**

THE HEIGHTS | APRIL 2018



**Dozens of companies leaked sensitive data thanks to misconfigured Box accounts**

TechCrunch | MARCH 2019



**Link Sharing**
Locally applied

**Link Sharing Defaults**
Select the default link sharing setting for a newly created file:

● **OFF**
Only the owner has access until he or she shares the file.

○ **ON - Anyone at Demo BetterCloud with the link**
Anyone at Demo BetterCloud who have the link can access the file.

○ **ON - Anyone at Demo BetterCloud**
Anyone at Demo BetterCloud can find and access the file.

G SUITE BUSINESS

One mistake–one simple misconfiguration–can easily expose data.

That's exactly what RedLock researchers stumbled upon in 2017. They discovered hundreds of companies exposing PII and private emails through a simple misconfiguration error in Google Groups. (The groups were created with the "Public on the Internet" sharing setting rather than "Private.") Employee salary compensation, sales pipeline data, and customer passwords were exposed, among other data.

How can your average end user (or admin) be expected to understand and navigate all of these complex permissions securely?

INTRODUCTION

# A New Breed of Insider Threats

All of these factors today are creating a new breed of insider threats that is emerging via SaaS apps.

To be clear, these insider threats still fall into the same traditional categories: malicious (e.g., IP theft, corporate espionage, financial gain) or unintentional (e.g., poor judgment, human error). But data exfiltration is occurring in ways beyond phishing, malware, poor password hygiene, unlocked devices, or data transfers to USB drives.

Data exfiltration is also happening through SaaS applications. SaaS is the new threat vector.

Why? Because in today's digital workplace, it's extraordinarily easy to expose data in SaaS apps. It's easy to accidentally share a confidential file publicly. It's also easy to purposely share a confidential file with a competitor.

The very beauty of SaaS–the ability to collaborate, the ease of sharing data–is also its ugliest and most dangerous security risk.

**This new insider threat stems from the user and all their interactions with data.**

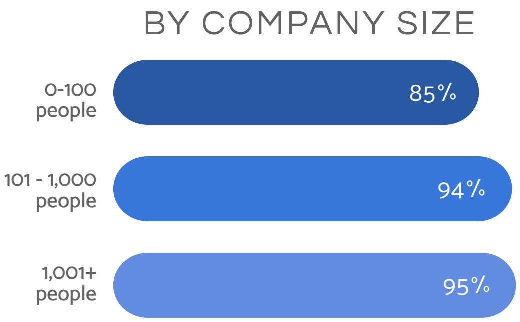
> The very beauty of SaaS—the ability to collaborate, the ease of sharing data—is also its ugliest and most dangerous security risk.
>
> This new insider threat stems from the user and all their interactions with data.

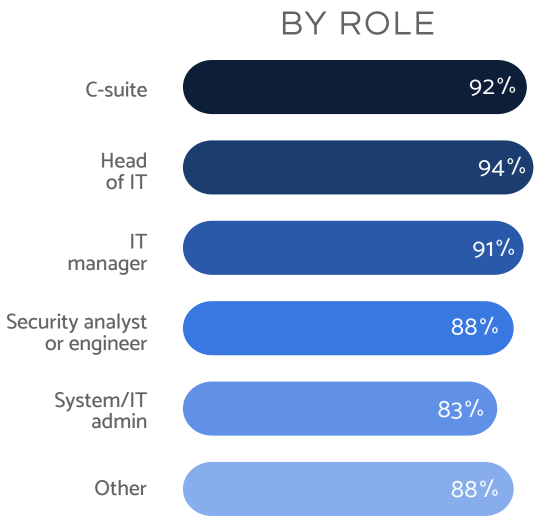
Similarly, the data below suggests that many IT and security professionals regard SaaS apps and users as a significant security risk.

# A Universal Concern

Just about everyone feels vulnerable to insider threats. **Ninety-one percent of our respondents said they felt vulnerable.**

WHO FEELS VULNERABLE?



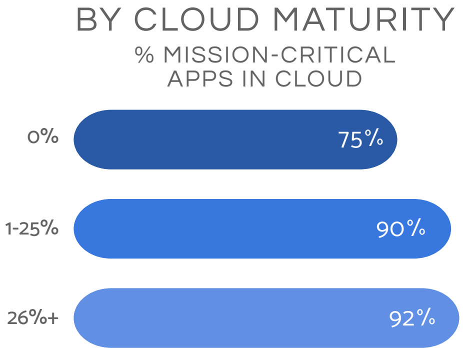


What's interesting here when we break it down by role is that 92% of C-level executives feel vulnerable to insider threats, vs. 83% of system/IT admins. Usually, we'd expect to see the higher percentage from admins.

Because they're in the trenches every day, admins typically feel the pain of security vulnerabilities more keenly than execs. Often there is a disconnect between these two groups.

This data suggests that the disconnect may be lessening. Perhaps insider threats, which are growing year over year, are now more top of mind for executives.

Insider threats have a business-wide impact. As the C-suite assumes greater responsibility for cybersecurity and takes a more active role in shaping their companies' security strategies, they may have a better understanding of this impact.



As companies adopt more SaaS applications and progress along their cloud journey, they feel increasingly vulnerable to insider threats. When the usage of SaaS becomes widespread and companies store more of their business-critical data in the cloud, more sensitive data is potentially at risk.

### Where would you rank insider threats on your list of security concerns?

More than half (59%) of C-level executives who have any cloud adoption say insider threats are a **top five** concern of theirs.

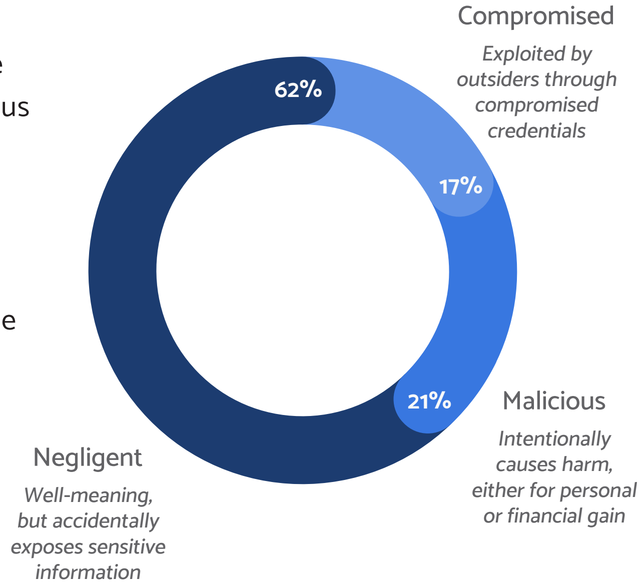
# What Type of Insider Poses the Biggest Security Risk?

## Which type of actor poses the biggest threat?

**By far, the most dangerous type of actor is the negligent end user.**

When you think of insider threats, you might think of memorable stories you've seen in the news. Many times, these incidents are malicious and/or intentional. They may be motivated by financial gain. They may aim to sabotage, perhaps in retaliation for a missed promotion (see: Tesla). They may be for whistle-blowing purposes (see: Edward Snowden). They may be for a career benefit, like taking valuable IP to a competitor (see: Uber vs. Waymo).

But these cases, while high profile, don't necessarily reflect who IT and security professionals actually view as the most dangerous type of insider.



Only 21% of our respondents thought malicious actors (intentionally causing harm, either for personal or financial gain) posed the biggest threat. Even fewer (17%) thought compromised users (exploited by outsiders through compromised credentials) posed the biggest threat.

The reality is more mundane than that. The biggest threat is not from flashy saboteurs.

Overwhelmingly, it's the negligent end user whom IT and security professionals view as the biggest threat. These are your ordinary employees.

Overwhelmingly, it's the negligent end user whom IT and security professionals view as the biggest threat. These are your ordinary employees. They mean well, but they can be careless and unintentionally expose sensitive information. They are particularly dangerous because they have access to critical assets, but lack the training or knowledge to keep sensitive information safe as they do their jobs.

And for companies that are powered by SaaS apps, the negligent end user has even more freedom to unintentionally expose sensitive information. This statistic illustrates the extent of human error and the importance of end user training.

### What actor poses the biggest threat?

**People who are either *planning to leave* or *have already left* are also dangerous insiders.**

More than half (53%) of respondents felt that either:

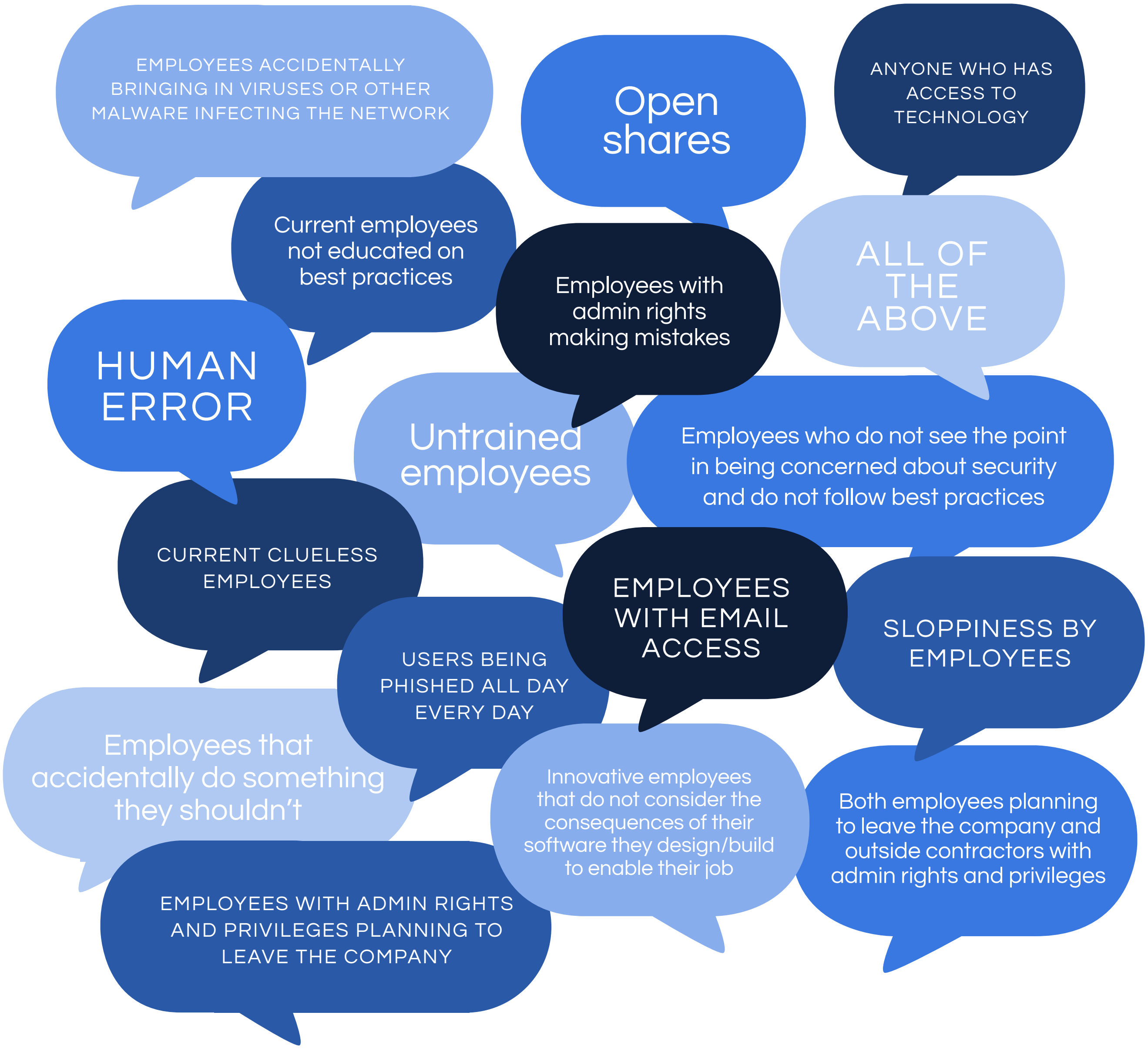
- Employees who have left the company,
- Employees planning to leave the company, or
- Contractors whose contracts have ended

posed the biggest threat to their organization. Namely, users with access directly pre- or post-termination are the biggest threat. Because offboarding processes are often unorganized and slapdash, exiting employees or contractors can fall through the cracks and retain access. Employees planning to leave, if they are disgruntled, may also be inclined to steal data before their access is revoked.

*Data from BetterCloud Customers*

On average, our customers have 59 Single-Channel guests and 66 Multi-Channel guests in Slack. These roles are meant for users who only need limited access (e.g., contractors, interns, or clients). However, if they are not properly offboarded when their contracts expire, they can retain access to corporate data long past their contract end date, which poses a security risk.

Thirteen percent of respondents chose "Other" and wrote in their answers. Here are a few of the responses we received:



EMPLOYEES ACCIDENTALLY BRINGING IN VIRUSES OR OTHER MALWARE INFECTING THE NETWORK

Open shares

ANYONE WHO HAS ACCESS TO TECHNOLOGY

Current employees not educated on best practices

Employees with admin rights making mistakes

ALL OF THE ABOVE

HUMAN ERROR

Untrained employees

Employees who do not see the point in being concerned about security and do not follow best practices

CURRENT CLUELESS EMPLOYEES

EMPLOYEES WITH EMAIL ACCESS

SLOPPINESS BY EMPLOYEES

USERS BEING PHISHED ALL DAY EVERY DAY

Employees that accidentally do something they shouldn't

Innovative employees that do not consider the consequences of their software they design/build to enable their job

Both employees planning to leave the company and outside contractors with admin rights and privileges

EMPLOYEES WITH ADMIN RIGHTS AND PRIVILEGES PLANNING TO LEAVE THE COMPANY

Many of these responses shared a common theme: current employees who are either "untrained," "sloppy," or "clueless." A few mentioned admin rights and privileges, highlighting the importance of the principle of least privilege.

Employees with admin rights can be dangerous because they are granted the keys to the kingdom. As Infosecurity Magazine puts it, this "leaves them with enormous power and destruction. It means more holes in your organization and more paths for an attack to spread."

# What Type of Technology Poses the Biggest Security Risk?

Forty-one percent of respondents believe that too many endpoints (e.g., user devices, computers, networks, etc.) make them the most vulnerable to insider threats.

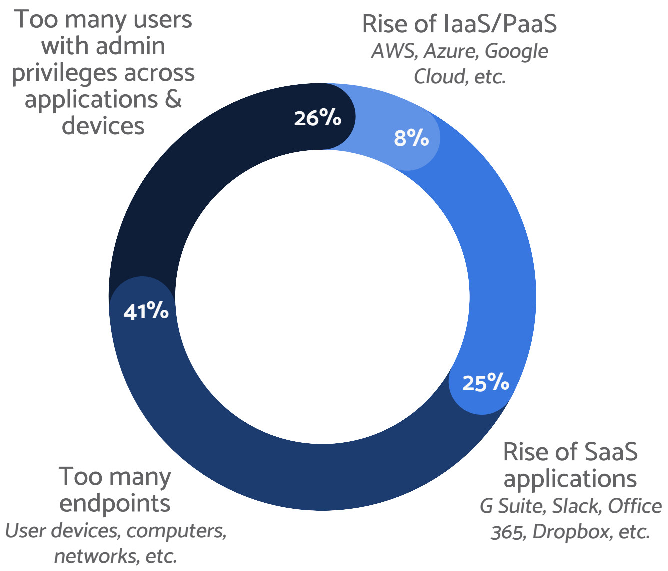
The next two factors were too many users with admin privileges across applications and devices, and the rise of SaaS applications, at 26% and 25% respectively.

The confluence of these factors has created an environment ripe for security threats.

IT and security teams must now grapple with securing devices (e.g., mobile device management, policy management, device access and tracking). The rise of SaaS means that they must also control and secure users' connections (i.e., authentications) to all of their SaaS apps.

On top of that, they must also control and secure users' interactions across their SaaS apps (e.g., entitlements/admin privileges, file sharing, groups, calendars, email forwarding, file downloads, etc.). These factors create a complex IT environment that presents numerous security challenges.

## WHICH FACTOR HAS MADE YOU THE MOST VULNERABLE TO INSIDER THREATS?



*Data from BetterCloud Customers*

On average, our customers have:

7 admins in Okta

13 admins in Zendesk

7 Global Administrators in Microsoft Azure

7 super admins in G Suite

8 admins in Box

9 team admins in Dropbox

**Forty-six percent of IT leaders believe that the rise of SaaS applications makes them the most vulnerable to insider threats.**

When looking at IT leaders only (heads of IT and above), almost half (46%) say that the rise of SaaS applications makes them the most vulnerable to insider threats.

*Data from BetterCloud Customers*

On average, our customers have 14 public Google Calendars (visible to the public including via Google search).

**Sixty percent of retail companies believe that the rise of SaaS applications makes them the most vulnerable to insider threats.**

When looking at the data by industry, more than half (60%) of retail companies believe that the rise of SaaS applications makes them the most vulnerable to insider threats. Retailers may be particularly susceptible to insider threats, more so than other industries, due to a few factors. With the hiring of temporary workers, plus high turnover rates and seasonality, employees may slip through the cracks when it comes to onboarding, offboarding, and user training.

*Data from BetterCloud Customers*

On average, our customers have found:

- 403 G Suite files shared publicly
- 14,256 G Suite files with public sharing links
- 2,123 G Suite folders with public sharing links
- 5,728 Dropbox files with public sharing links
- 1,421 Dropbox folders with public sharing links
- 2,138 Box files with public sharing links
- 1,041 Box folders with public sharing links
- 16 Slack files shared publicly

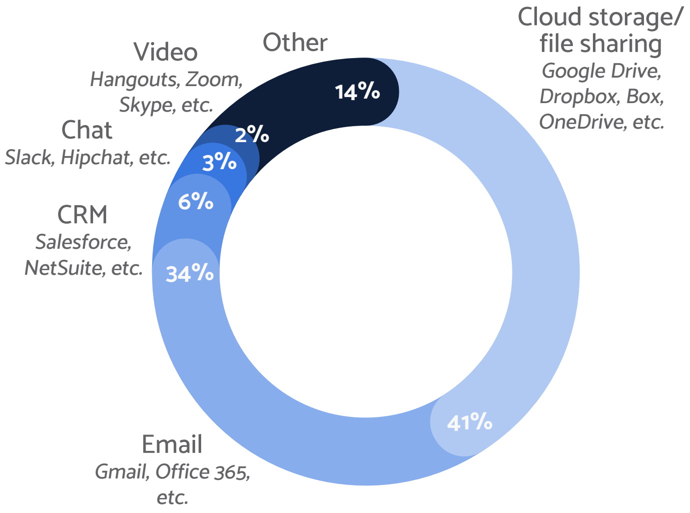
## Which technology within your SaaS environment poses the biggest security challenge?

**Seventy-five percent of respondents believe that cloud storage/file sharing and email pose the biggest security challenge.**

Nearly half (41%) of respondents believe that cloud storage/file sharing (Google Drive, Dropbox, Box, OneDrive, etc.) pose the biggest security challenge.

This is not surprising, given that organizations likely store their most sensitive and valuable data here. These apps also provide the most freedom and flexibility for collaboration. File sharing and openness make these apps beneficial, and by the same token, they also create security risks.

WHICH TECHNOLOGY WITHIN YOUR SAAS ENVIRONMENT POSES THE BIGGEST SECURITY CHALLENGE?



Email (Gmail, Office 365, etc.) was next, with 34% of respondents saying that this technology was the biggest security challenge.

Other SaaS collaboration tools were far behind. CRM (Salesforce, NetSuite, etc.), chat programs (Slack, Hipchat, etc.), and video (Hangouts, Zoom, Skype, etc.) represented the biggest

*Data from BetterCloud Customers*

The highest number of people we found automatically forwarding their corporate email to their personal email accounts was 2,496 users at one company. Email forwarding can violate compliance laws (e.g., HIPAA) and increase the risk of sensitive data exposure.

security challenge for only 6%, 3%, and 2% of our respondents, respectively.

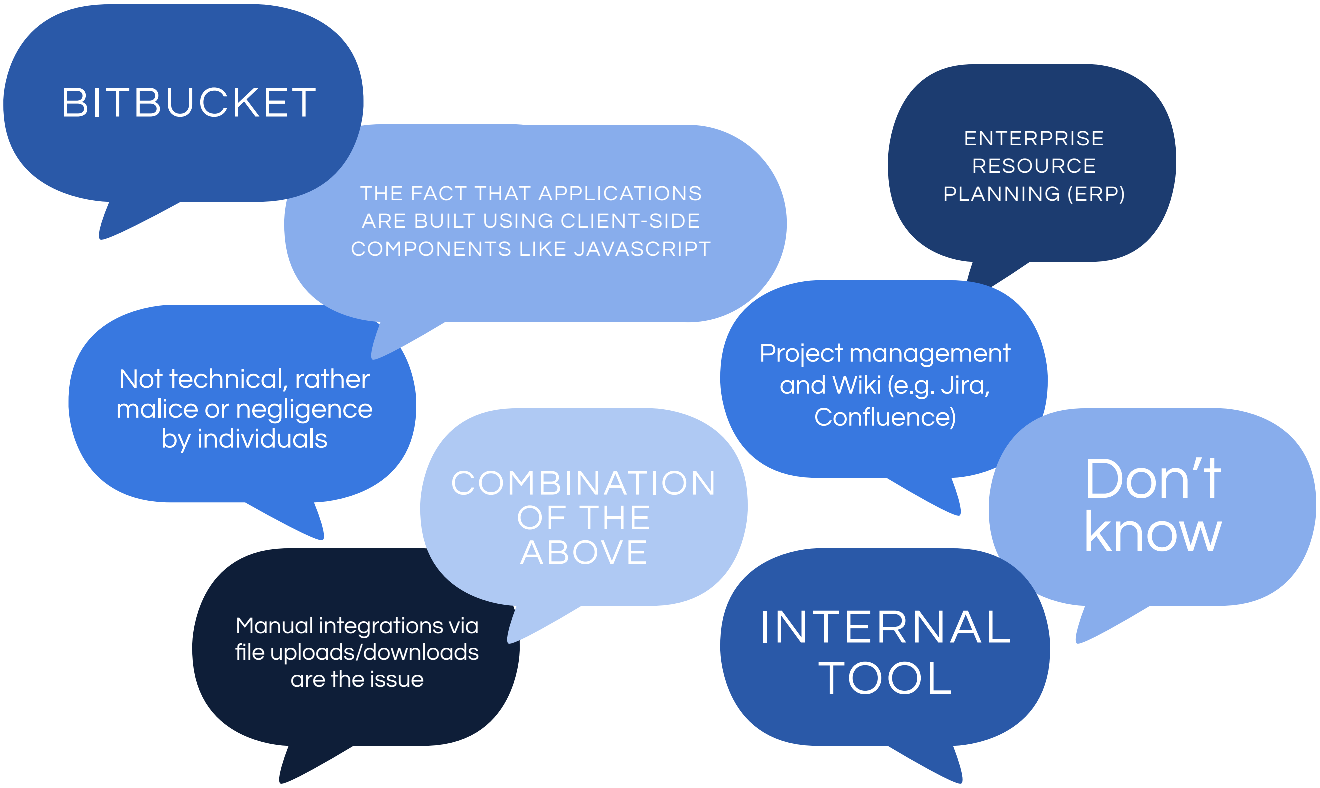
Of course, your response to this question will depend on where your most sensitive data is stored and what type of business you are. Nonetheless, the reality is that your business data is stored in some type of SaaS app today.

*Data from BetterCloud Customers*

On average, our customers have found:

- 73 Google Groups that allow external members
- 23 Google Groups that anyone can join
- 322 Google Groups that anyone can post in
- 32 Google Groups that anyone can view

Fourteen percent of respondents chose “Other” and wrote in their answers. Here are a few of the responses we received:

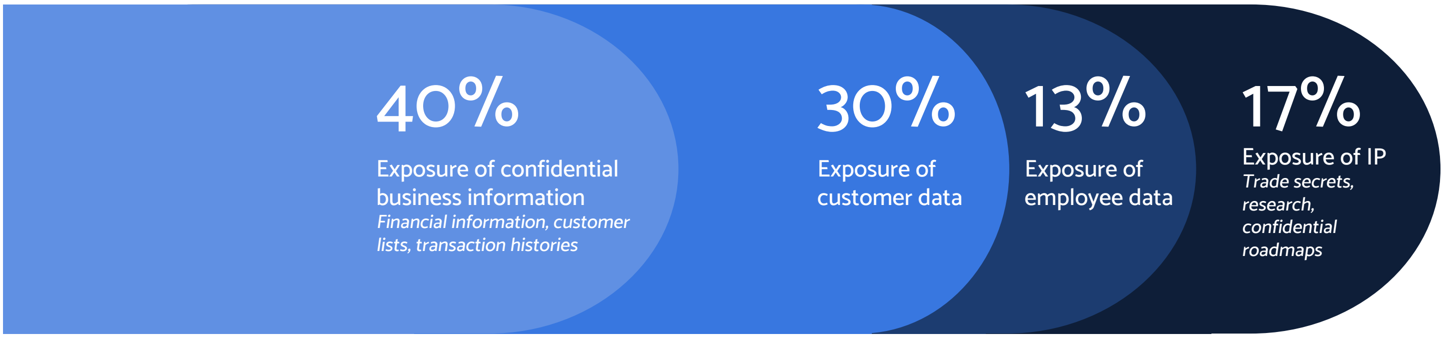

BITBUCKET
THE FACT THAT APPLICATIONS ARE BUILT USING CLIENT-SIDE COMPONENTS LIKE JAVASCRIPT
ENTERPRISE RESOURCE PLANNING (ERP)
Not technical, rather malice or negligence by individuals
Project management and Wiki (e.g. Jira, Confluence)
COMBINATION OF THE ABOVE
Don’t know
Manual integrations via file uploads/downloads are the issue
INTERNAL TOOL

# What Are Organizations Most Vulnerable To?

While exposing any sensitive data is undesirable, respondents felt more vulnerable to certain kinds of data exposure than others.

Forty percent of respondents felt they were most vulnerable to exposure of confidential business information (e.g., financial information or customer lists). Exposure of customer data came in second, with 30% of respondents weighing in.

Respondents felt least vulnerable to exposure of employee data (13%) and IP (e.g., trade secrets or research) (17%).



# Mitigating Insider Threats

## INVESTMENT

### Do you believe your organization has invested enough to mitigate the risk of insider threats?

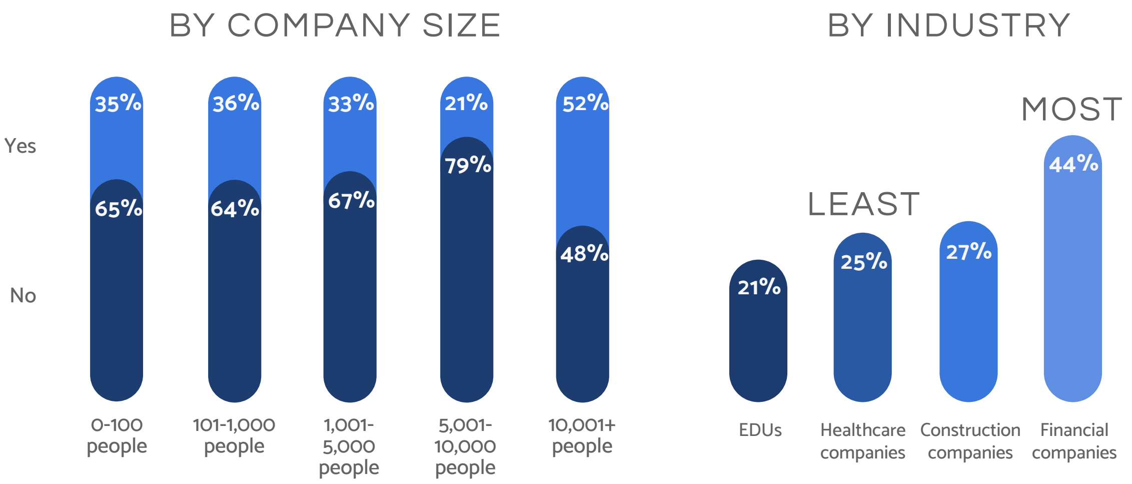
Executives feel less sure that they've invested enough. **Only 26% of C-level executives believe they have invested enough, vs. 44% of IT managers.**

When we look at the data by percentage of mission-critical apps in the cloud, 53% of companies with no cloud apps believe they've invested enough. Meanwhile, only 32% of companies entirely in the cloud feel the same way. This suggests that companies are less confident about their risk mitigation investments by the end of their cloud journeys than when they started.

This makes sense. As companies adopt more SaaS applications, the volume and value of data in the cloud increases. Additionally, more of their employees are using SaaS applications. It's not surprising that they may feel increasingly concerned about mitigation measures as they make this journey.

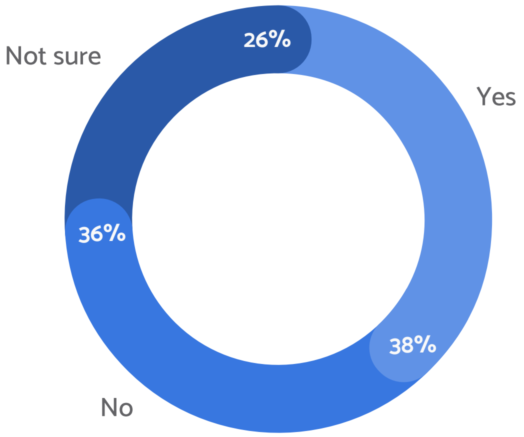
When we look at the data by company size, only 21% of large companies (5,001-10,000 people) believe they've invested enough to mitigate the risk of insider threats.

WHO FEELS THEY'VE INVESTED ENOUGH?



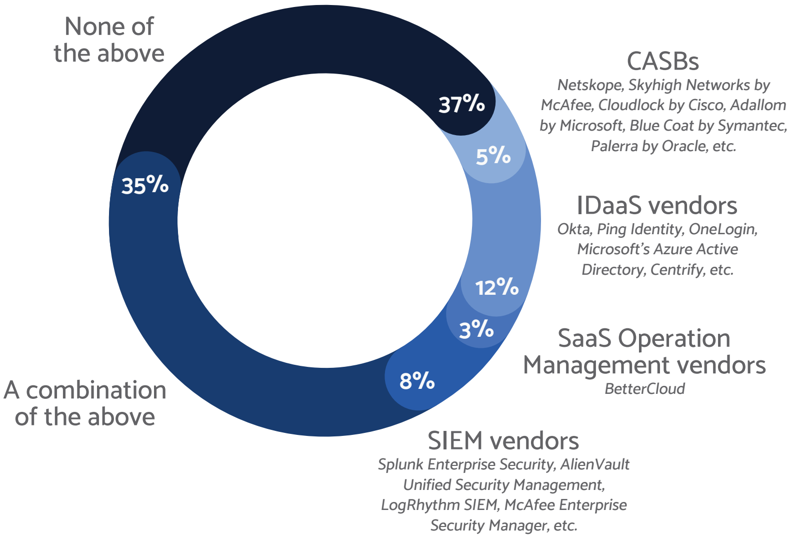
## MITIGATION PROGRAMS

DO YOU HAVE A PROGRAM OR MEASURES FOR MITIGATING INSIDER THREATS?



## MITIGATION TOOLS

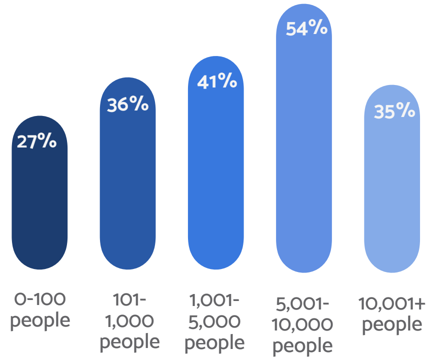
WHAT TOOLS ARE YOU DEPLOYING TO MITIGATE INSIDER THREATS?



Thirty-five percent of respondents said they are using a combination of CASBs, IDaaS, SOM, and/or SIEM tools. **However, 95% of people using CASBs still feel vulnerable to insider threats.** Thirty-seven percent said they are not using any of these tools.

Fifty-four percent of large companies (5,001 - 10,000 people) said they used a combination of tools, whereas only 27% of small companies (0-100 people) said they used a combination. More than half of small companies (0-100 people) said they don't use any of the above.

PERCENTAGE OF COMPANIES USING A COMBINATION OF TOOLS



BY SIZE

Smaller organizations tend to use one or no tools to address insider threats—perhaps due to budget constraints or lack of security awareness. As companies grow in size, they start to adopt a combination of tools as their infrastructure, tech stack, and business needs grow more complex.

# Solutions

Of course, there is no panacea for insider threats. To help minimize the risk from insider threats, IT and security professionals can take a few steps:

1. **Invest in security awareness training**

### Instill a culture of security that makes employees feel personal ownership

As we saw earlier, the majority of respondents felt that the biggest insider threat risk came from negligent end users. As a result, part of your mitigation strategy should focus on educating users. It all starts with instilling a culture of security. Employee training should reinforce the message that everyone in the company has a duty to protect corporate data.

“Success looks like employees who feel personal ownership—the ones who involve Security before making an architectural or purchasing decision with security implications, or the ones who lock their computer workstation before walking away,” says Austin Whipple, senior security architect at BetterCloud.

“Success looks like employees who feel personal ownership–the ones who involve Security before making an architectural or purchasing decision with security implications, or the ones who lock their computer workstation before walking away,” says Austin Whipple, senior security architect at BetterCloud.

To instill a culture of security, Whipple has rolled out a successful laptop bounty program, phished his own employees, and more. (Read more about his programs here: What Does a Successful Security Program Look Like?)

"By having good security programs, gamifying education and security tasks, and convincing everyone we are all on the same team, I get lots of trust from other employees, and employees self-reporting security events (policy violations, vulnerabilities, etc.)," he says.

### Frame things in a "what's in it for me?" context

Framing things in a "what's in it for me?" context is also helpful.

Teresa Banks, manager for information security and compliance programs at the University of Arizona, uses this tactic when creating security awareness for the students and employees on campus.

> She doesn't just explain what a phishing email looks like; she illustrates the disastrous consequences of a successful phishing scam.

She doesn't just explain what a phishing email looks like; she illustrates the disastrous consequences of a successful phishing scam. "It's showing them: 'Now I can get into your employee record, I can find your Social Security number, your date of birth, and I can steal your identity right there. Oh, you have direct deposit. I can change the routing number and the account number and I can reroute your paycheck to me now.' Once you visually walk people through scenarios that relate to their lives, they get it."

### Use pop culture examples to make the concepts resonate more with users

As an example, her first security awareness campaign was James Bond themed. "We called it 'The Spy Who Hacked Me.' Every presentation's name was a twist on a James Bond movie. We've done pirate themes too. It's memorable, it's relatable, and it makes it fun," she says. "What better way to relate to people talking about bad guys than pirates and spies?”

(For pop culture examples you can use in training sessions, check out this article: Information Security and Pop Culture: How Real-Life Social Engineering Techniques Are Used in Movies and Television.)

Training should describe individual sharing permissions in detail (e.g., viewer, editor, commenter) and link sharing options.

### Focus training on SaaS sharing permissions

When it comes to insider threats and SaaS apps, comprehensive user training can be an effective mitigation strategy. Training should describe individual sharing permissions in detail (e.g., viewer, editor, commenter) and link sharing options. The curriculum should also include a review of restrictions that can be enabled on the end user side, such as the ability to prevent editors from changing access, or the option to prevent viewers from being able to download certain files. This ensures that users know exactly what happens when they choose sharing settings, thereby reducing the risk of accidental data exposure.

Additional security resources:

- A Top G Suite Expert Shares His 31 Best Modern Security Tips
- If You’re Not Phishing Your Employees, You Should Be: Here’s How
- 3 Real Phishing Attacks Your C-Suite Needs to See

2. **Get visibility into user interactions (e.g., suspicious user behavior or data exposure due to settings misconfigurations) in SaaS apps**

Another way to mitigate risk is to get clear visibility into what your users are doing within SaaS apps. A SaaS Operations Management (SOM) platform listens for any changes in application configurations, document settings, and privileged access, and immediately reverts potential threats with automation sequences. It also listens for suspicious user behavior such as mass file downloads, access to unauthorized applications, or multiple failed logins, and creates policies to automate IT and Security's response when these events occur.

3. **Be aware of key data points and behaviors that may indicate an imminent insider threat**

   According to Carlos Batista, BetterCloud's CISO, some potential data points and behaviors that, in combination, may indicate suspicious behavior include:

   - Data dumps from key applications
   - Attempts to connect or download data to removable devices
   - Suddenly working very odd hours
   - HR data: employees performing poorly, disgruntled employees who are passed over for promotions or about to be laid off
   - Visiting job sites, updating LinkedIn

4. **Have the right tools in your insider threats toolkit**

   Some potential tooling that can help enable data collection needed for successful insider threat programs include:

   - Traditional DLP tools (email, endpoint, web)
   - Web proxy logs
   - Privileged access management (PAM)
   - HR/people data
   - SIEM tools
   - UEBA tools
   - SaaS Operation Management (SOM) tools
   - CASBs
   - Building security logs

*For tips and guidance on how to implement a robust insider threats program, check out our webinar recording Two Cybersecurity Experts Share Their Secrets to an Effective Insider Threats Program.*

# Conclusion

The digital workplace presents a new generation of insider threats.

IT and security teams must tighten security where business-critical data is most exposed. Today, that's in your SaaS applications. Data lives there now, not on your endpoints. As employees collaborate freely through SaaS applications–from any place, at any time–SaaS is turning into a new threat vector. This is because:

1. SaaS creates new and easy ways for users to expose data, whether it's intentional or not.
2. Many IT and security professionals are unaware of these blind spots–i.e., how and when data is exposed in SaaS applications.
3. File sharing permissions and configurations are complex.

This "perfect storm" creates a new breed of insider threats. Such data exposures are difficult to detect at scale. As a result, these insider threats are hidden in plain sight.

SaaS has exponentially expanded the scope and difficulty of managing insider threats. As more companies continue to adopt SaaS, this difficulty will only increase.

Understanding the various leakage points in SaaS is essential in creating safeguards. With the right tools for visibility and remediation, it's possible to mitigate some of these risks in the digital workplace.

BetterCloud

## ABOUT BETTERCLOUD

BetterCloud fundamentally changes the way you manage and secure mission-critical SaaS applications. As a pioneer in the SaaS Operations Management space, BetterCloud empowers companies to secure user interactions across the digital workplace.

By centralizing mission-critical SaaS applications, BetterCloud is able to enrich the data from SaaS providers to present a complete view of your users, data, and applications across your environment. Using a custom alerts interface, BetterCloud listens for the events that signal a potential security threat or policy violation, such as settings changes, administrators added, or suspicious user behavior. When an alert is triggered, BetterCloud automates a sequence of administrator actions in the native application to remediate the policy violation, notify relevant teams and users, and secure your environment before anything can happen.

**To learn more about how BetterCloud can secure user interactions in your digital workplace, request a demo.**