BetterCloud WHITEPAPER

Fixing IT's Blind Spots

8 Critical Security and Management Policies to Implement in Your SaaS Environment

Table of Contents

Industry best practices: the 8 categories of policies you need to implement

Introduction

Software-as-a-Service (SaaS) is transforming the modern workplace as we know it.

But as SaaS adoption continues to skyrocket, control is increasingly shifting to end users—not IT. End users can control file sharing settings, create their own groups, install third-party apps by themselves, and so forth. All too often this results in headline-worthy data breaches.

Unfortunately, native admin tools are not powerful, granular, or sophisticated enough for IT to manage their SaaS environments properly. IT cannot easily track where corporate data is flowing or who has access to it. The bring-your-own-device (BYOD) trend exacerbates this problem. Additionally, IT can't keep up with the breakneck pace as employees are hired and fired, contractors come and go, and users switch teams and offices. IT is being asked to do more and more, but their teams aren't scaling accordingly. Furthermore, data is stored in siloed systems and sprawled across dozens of apps, creating an ever-growing web of accounts, users, files, assets, etc. It is impossible to determine who (or what) is not in compliance. Alerts are excessive, irrelevant, and not actionable, resulting in alert fatigue. Management interfaces are inadequate and not purpose-built for IT.

So how can IT wrangle this SaaS chaos, mitigate security threats, and regain control of their environment?

The answer: Create and implement policies.

Policies are essential for monitoring and protecting corporate data. For example, IT may not realize that sensitive data is exposed or sent outside the company, or that the wrong people have access to confidential data until it's too late (or ever). Policies bring visibility to these blind spots and cure them.

In this whitepaper, we'll:

- Explain which policies you must implement at the bare minimum, and why
- Provide industry best practices
- Identify the biggest blind spots IT has, and how to solve them
- Discuss the business value of policies and dispel common myths
- Describe how to develop robust policies and how you should be thinking about them

What is a policy?

Let's start with the dictionary definition:

A policy is "a definite course or method of action selected from among alternatives and in light of given conditions to guide and determine present and future decisions."

This definition is true in an IT context as well. Simply put, policies are guidelines that you don't want people to violate. They outline what correct behavior looks like.

They're your rules—your official stance on specific processes. They describe what people can or can't do. If policies are violated, then you must remediate them somehow (either manually or automatically).

You can have policies on just about anything. In SaaS environments, they can run the gamut from file sharing to offboarding to email forwarding and beyond. They can be broad or very, very specific (more on this later).

Let's take file sharing as an example. What's your policy on sharing files? Can users share files with external domains, or can they only share files internally? If someone violates this policy, how will it be remediated? Who should be notified of violations (if anyone)?

There is no perfect "one-size-fits-all" policy, so you'll need to sit down and decide what guidelines best fit your organization's needs. Later in this whitepaper, we'll dive into the process for developing robust policies, what the most critical policies are, why they're important, and how you can implement them in your organization with BetterCloud.

Policy enforcement adds significant value to the business

In a Dark Reading article called "Security Worries? Let Policies Automate the Right Thing," author John De Santis writes:

"In fact, most security breaches and system failures are the result of people not operating systems correctly. They forget to do something or give themselves permission to do an action, then leave that permission open so that bad actors can take advantage of it. **These missteps could be avoided by a security approach that automatically directs, guides, or encourages system operators to do the right thing or blocks them from doing bad things.** It is an enlightened security leader who prioritizes and budgets for this kind of security policy enforcement; **without active and automated enforcement of policy, the breaches keep coming, costs keep rising, and heads keep rolling**."

This excerpt captures exactly why organizations need to implement policies today. And if you can create and enforce policies successfully, this is a win for the IT department that you can take all the way up to C-level executives.

Business leaders are most concerned with how organizational risk is identified and managed. Fittingly, the whole point of policy enforcement is to identify and manage risk on an ongoing basis. Specifically, this risk comes from blind spots—areas IT has no visibility into. Policies identify and fix common blind spots, improving security for the entire organization.

Like any other component of IT security/risk management, policies are like car brakes. As the saying goes, they're not there to slow you down; they're there to allow you to go faster, more safely. They are strategic investments in reducing corporate risk. They protect the business and foster innovation at the same time. They also free up resources, enabling IT to focus on strategic, revenue-generating projects rather than just "keeping the lights on."

Policies can also help the C-suite understand the business value that IT brings to the table.

Use policies to present compelling metrics to executives (examples: the number of thwarted security threats, the speed of identifying and remediating security policy violations, the number of critical exposures, or total cost savings for unused app licenses). With this data, IT's work now becomes much more relevant and interesting to executives. They will understand that IT is proactively mitigating security risk and reducing costs. In other words, they will see how IT and the business align, and how IT brings value to the table.

The four steps of policy enforcement

We recommend four steps for enforcing your policies.

1. **Define**
2. **Investigate**
3. **Remediate**
4. **Automate**

Important note: You may not need (or want) to complete all four of these steps. A common misconception about policies is that they must be fully automated in order to be valuable. This is not true. We want to dispel that myth upfront.

Keep in mind that each step is highly valuable on its own; you may not have to progress to the next step. It depends on your organization's needs. Some companies may only need to define policies, and that degree of enforcement is sufficient for their organization. They may never reach the point where they can automate their policies, and that's okay. For example, policy automation may never be a reality for very large organizations.

Here are the four steps described in depth:

Define - The first step is to define exactly what your policy is. What behavior is permitted and not permitted? What are the rules around onboarding/offboarding, file sharing, compliance, etc? Define what your official stance is, as well as what violations and resolutions would look like. Spend time with your security, executive, and HR teams to figure out what policies your organization needs to implement. For many companies, this is the most difficult step to complete.

Documenting the rules and requirements for individuals who access your organization's sensitive applications and data is your first line of defense against security threats and data breaches. By defining the actions you want to mandate or prohibit, IT and security teams can enforce the same standards across all applications and data.

It is important to create policies that support productivity and innovation and also include exceptions for special use cases.

Investigate - Next, explore your environment and investigate. Dig deeper and figure out what's in compliance and what's not.

Remediate - If there are policy violations, the next step is to fix them. It's important to note that remediation can mean different things to different people. For some, remediation may mean notifying people of the violation (e.g., IT, end users, executives, security, or HR personnel). That notification may be enough to remediate the issue.

Other companies may need to manually remediate the problem and take action to fix the violation. At this point, it's very common for teams to circle back to Step #1 (Define) to modify their policy definitions and get more specific. For example, they may need to tweak their policies and blacklist/whitelist specific apps.

Automate - Some companies will automatically remediate policy violations and therefore automatically enforce their policies from start to finish. This creates a "self-healing" environment. Again, not all companies may need (or want) to do this step.

In circumstances where automation makes sense, we recommend it. In a recent CSO.com article on New Year's resolutions for CISOs, one of the resolutions listed is: "Make a commitment to automate and orchestrate manual processes. In cybersecurity, whatever can be automated

> should be automated. This includes gathering data, analyzing suspicious files, and applying simple remediation rules to block malicious activities."

Policies can be highly broad or highly specific

Policies can be very broad or specific, depending on the type of data at hand, company type, industry, company size, etc.

Here's an example of a broad (coarse) policy:

Employees cannot share any files publicly.

This policy is fairly sweeping. It doesn't specify what kind of files or which employees in particular. It applies to every employee and all types of files. Broad policies like this are general and non-specific. Typically, organizations that are subject to very strict security and regulatory requirements will implement broad policies. For example, some government agencies only allow their users to share files with certain domains, like a .gov or a .mil.

Keep in mind, however, that if the policy is too broad or strict, it may stymie collaboration and ultimately defeat the whole purpose of adopting a productivity and collaboration platform.

Here's an example of a specific (granular) policy:

When a finance spreadsheet containing credit card numbers is shared publicly, automatically revert its sharing settings.

On the other end of the spectrum are highly specific policies like the one above. They outline exact specifications, such as the file type, business unit, and file content. They typically reference high-risk business units (e.g., finance, HR, executives) or high-risk data (e.g., credit card numbers, social security numbers, or keywords like "Confidential" or "Attorney Client Privilege").

Because granular policies are so specific, they often contain conditional elements (e.g., when this happens, if this is true, then take this action).

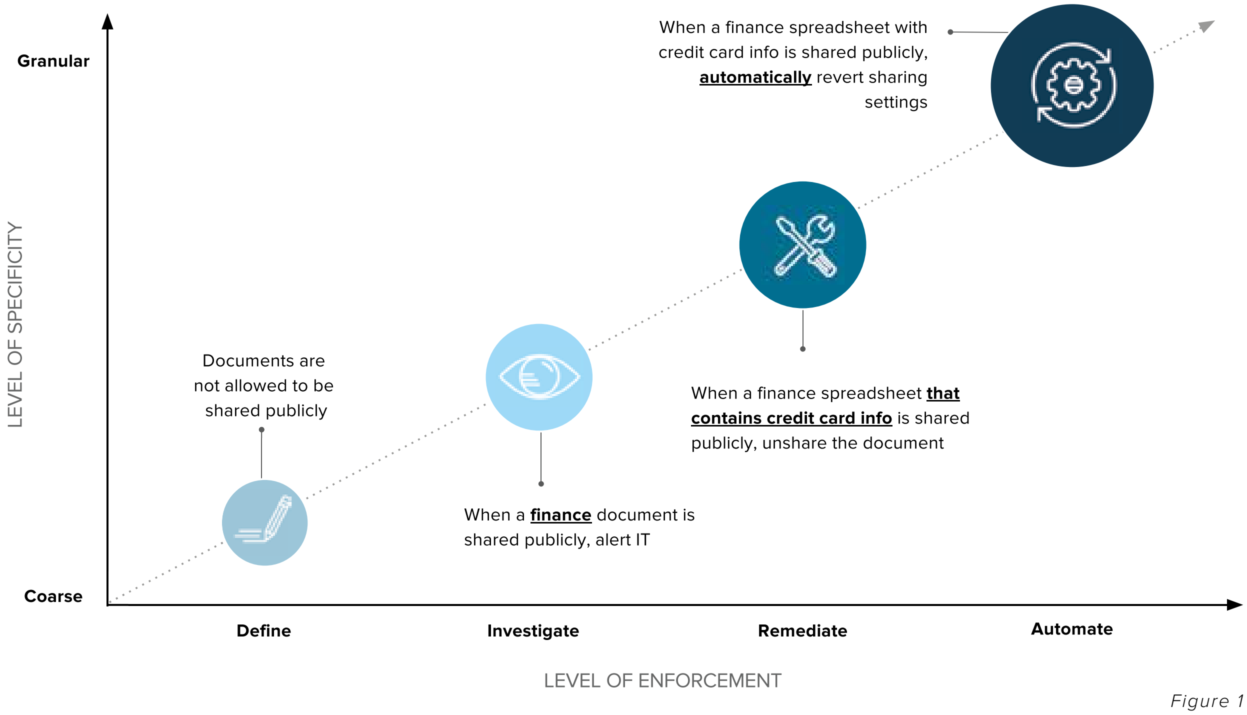


Figure 1

Policy enforcement vs. granularity

Figure 1 illustrates how you should think about the relationship between policy enforcement and granularity.

For very coarse policies, you would likely only reach the first step of policy enforcement (Define). Because these policies are so broad, they'd end up hampering productivity if you were to automate them. For instance, if you implemented and automated a sweeping, general policy like "Documents may not be shared publicly," this would probably frustrate users who are trying to collaborate on work.

As policies get more granular, you can move on to the next steps of policy enforcement, like Investigate or Notify. For example, you probably wouldn't want to be notified every time a document was shared publicly (a coarse policy), but you would want to be notified if a **finance spreadsheet** was shared publicly (a more granular policy).

Extremely granular policies, such as "When a finance spreadsheet with credit card info is shared publicly, **automatically** revert sharing settings" can be automated *because* they are precise and hyper-relevant. You can be confident that the automation will remedy only that specific scenario; it will not block productivity for the entire company or needlessly affect other areas of your environment. This granular policy example identifies the exact type of file you want to protect and outlines the exact remediation action. With this type of granularity, it makes more sense to enforce them more actively.

Industry best practices: the 8 categories of policies you need to implement

Regardless of your industry or level of SaaS adoption, every organization should document and enforce these eight categories of policies across all SaaS applications.

Of course, some companies may have additional types of policies. But we recommend setting up these eight categories at a bare minimum in order to run a high-functioning, efficient, and secure SaaS environment. These are the baseline policies needed to protect your organization from security breaches and limit the potential exposure of sensitive data.

We selected these categories based on hearing direct feedback—as well as analyzing product usage data—from thousands of BetterCloud customers. These are the policies that customers tell us are most critical for their day-to-day SaaS management and security. We consider these industry best practices.

If you're new to BetterCloud and would like to learn more about implementing policies, please visit https://www.bettercloud.com/demo-policywp/. If you're a current BetterCloud customer, please email success@bettercloud.com.

CATEGORY #1

User Lifecycle Management

Why you should care about user lifecycle management

Today, user lifecycle management (ULM) is a flawed operation.

Employees join companies. They get promoted, move office locations, switch teams, go on vacation, need password resets. They leave companies. Contractors join for projects, then leave. It is up to IT to manage all of these lifecycle changes: onboarding, offboarding, group memberships, email delegation, calendar management, user management, and more.

These tasks are notoriously repetitive, manual, and time-consuming. This is because native admin consoles are clunky and inefficient; they weren’t purpose-built for IT. **And unfortunately, the status quo for ULM is holding businesses back. It kills productivity. It slows IT down. It prevents them from innovating or adding value to the business.**

A recent survey of 150 mid-market IT decision makers showed that “much of an IT pro’s day is spent bogged down by routine maintenance requests, ticket documentation, and troubleshooting.”

The report goes on to say that routine requests "often limit time spent innovating, strategizing, and modernizing technologies—tasks that IT pros love. According to the Spiceworks research, IT pros estimate only 11 percent of their time is spent on IT planning and strategy, and only 13 percent of their time is centered around what they want to do most: modernizing technology."

Another report found that over 40% of information workers surveyed spend at least a quarter of their work week on manual, repetitive tasks. Nearly 70% of workers say the biggest opportunity of automation lies in reducing time wasted on repetitive work. Nearly 60% estimate they could save six or more hours a week—almost a full workday—if these repetitive aspects of their jobs were automated.

While you may never reach the point of automating your ULM policies, just defining your policies (and not using native admin consoles) can provide huge value to the business.

A BetterCloud customer, a large retailer in the UK with thousands of customers, has already seen massive cost and time savings when it comes to streamlining repetitive admin tasks. (For privacy purposes, we are not naming this customer.) This retailer is using BetterCloud for ULM admin tasks related to group membership, email delegation, user management, calendar management, deprovisioning, and others. In the first six months of purchasing BetterCloud, this customer had already saved 1,926 hours of tedious admin work by using BetterCloud instead of the native G Suite admin console. This equaled £120,000 or $163,000 USD in cost savings for them. In fact, they calculated that they would have needed 1.09 full-time employees to perform the same amount of work. This customer story illustrates how native admin consoles are significant obstacles to productivity when it comes to ULM.

Below are two critical ULM policies that every IT team should implement. These policies can lead to substantial cost savings, time savings, productivity gains, and reduction in ticket volume.

USER LIFECYCLE MANAGEMENT POLICY #1

Onboarding

What is onboarding?

Onboarding is the process that equips new hires with the proper tools, access, and resources they need to do their jobs. This includes steps such as provisioning new accounts, giving users access to shared files and folders, adding them to the right groups, applying email signatures, etc. All new employees need to be onboarded when they first join a company. This ensures that they have the right systems access as soon as possible. However, onboarding tasks are usually very manual and time consuming.

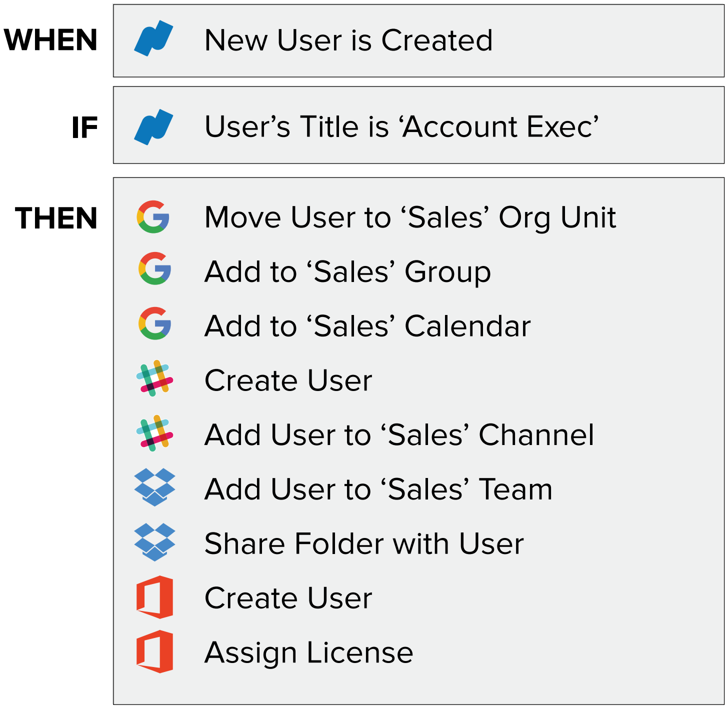
What's the business value of an onboarding policy?

Effective onboarding means productivity gains for the business. New hires can hit the ground running on day one and start contributing right away. All too often, new employees wait days or weeks to get access to the information they need, resulting in expensive productivity losses. Research shows that organizations with a strong onboarding process improve new hire retention by 82% and productivity by over 70%.

What does an onboarding policy look like?

A good onboarding policy will provision new accounts across SaaS providers and grant access to all necessary groups, calendars, files, assets, etc. Because onboarding is not a one-size-fits-all process, the level of access a person receives will depend on their business unit, department, role, title, location, etc.

Figure 2 is an example of a BetterCloud onboarding workflow that is triggered when a new user is created in a HRIS like Namely.



WHEN New User is Created

IF User's Title is 'Account Exec'

THEN
Move User to 'Sales' Org Unit
Add to 'Sales' Group
Add to 'Sales' Calendar
Create User
Add User to 'Sales' Channel
Add User to 'Sales' Team
Share Folder with User
Create User
Assign License

Figure 2

Note: This is just a sample policy meant to illustrate the wide range of onboarding actions you can take in BetterCloud. Your onboarding policy may not require all of these steps.

What kind of steps should I be including in my onboarding policy?

We analyzed product usage data to see which onboarding actions customers are taking most often in BetterCloud. We discovered that there was a set of core onboarding steps that remained consistent across all size segments and industries. These included basic yet essential steps like "Add to Group/Channel," "Share Calendar," "Set User's Profile," and "Move User to Org Unit." "Add to Group" was by far the most popular action, appearing in 87% of all our customers' onboarding policies.

REAL-LIFE BETTERCLOUD CASE STUDY

Story #1: How a media company used policies to reinvent the way HR and IT work together to onboard, reducing IT tickets by 90%

Fullscreen Media, which connects brands to content creators, uses BetterCloud to build automated onboarding policies. When HR makes a new employee active in Namely, BetterCloud automatically does the following:

- Sends an email to the Fullscreen IT team alerting them of the new hire
- Automatically creates a Gmail account for the user
- Gives the new hire a generic password that must be changed the moment they log in
- Provisions Slack for the new hire
- Provisions the new hire a Dropbox login, if they are in a particular group

This onboarding policy in BetterCloud shaves off one-third the total time it takes to onboard a single user. What's more, internal ticket volume is way down too. "We reduced our IT tickets by 90%," says Shira Harrison, IT Director. Before BetterCloud, the IT team was constantly inundated with tickets from users asking for access to certain applications. "We don't get asked those questions anymore," she says. Now, instead of answering tickets, Harrison and her team are working on more important long-term projects.

Story #2: How IDaaS solution Ping Identity uses BetterCloud as a complementary onboarding solution

Even IDaaS providers like Ping Identity are using BetterCloud to build automated onboarding policies for their core SaaS applications.

Ping was facing a whirlwind pace of growth—one new business hire per day in the first half of 2017. The onboarding process for each new hire was "at least 60 manual steps long and requires 15-20 windows open at a time," said Woody Grover, Ping's IT Manager.

Grover's team uses Ping to auto-provision applications that are widely used by the company and can be turned on with the flip of a switch. One example is WebEx. "The first time on your first day that you hit our PingOne portal, your WebEx account is provisioned automatically. We don't have to touch that," he says.

But these aren't the applications adding tedious steps to his onboarding checklist and limiting his team's efficiency. Rather, he estimates that per week, one of his team members spends half of their time simply making new accounts in their core applications like G Suite, Zendesk, Slack, Salesforce, and Atlassian.

As a result, Ping recently upgraded to BetterCloud Core to take advantage of the integrations with core SaaS apps—a move he called "a no-brainer."

"BetterCloud builds on what Ping already does, providing a similar automated process for Google, Zendesk, and Atlassian apps. Ping doesn't have auto-provisioning for those services, so BetterCloud interlocks with how our current Ping tools provision users," he says.

Across G Suite, Slack, Salesforce, Zendesk, and Atlassian, Grover hopes to not only cut down his onboarding checklist dramatically but eventually automate it completely.

“I predict that with BetterCloud, we’ll create an automated workflow for a sales exec, for example, that will place them in the right Slack channels and Google Groups that they need to be in.

“The pie in the sky dream is to have a workflow fire automatically when a new hire is created in our HRIS, and we don’t ever have to see that person until they show up in our office,” he says.

Story #3: How a K-12 school used policies to reduce their onboarding time by 94%

Another BetterCloud customer, a K-12 school, used policies to reduce their time spent onboarding people by 94%. (For privacy purposes, we have removed all names from this customer story.)

“Just the other day, I needed to update all our student Google accounts (passwords, org units, etc.) and add 90 new incoming students as well. This was all done in under 15 minutes using BetterCloud,” said the IT manager. Making all the required new school year onboarding changes without BetterCloud would have taken him three to four hours, he estimates.

For new employees, his team also uses BetterCloud to pre-load new users’ signatures and make sure all of their employee data (e.g., manager, phone, location) is filled out before their first day, so that they can hit the ground running.

USER LIFECYCLE MANAGEMENT POLICY #2

Offboarding

What is offboarding?

Offboarding is the counterpart to onboarding, but it is arguably the more important process of the two. When an employee leaves a company, their data access to enterprise applications must be revoked. But offboarding goes way beyond just “turning things off.” A comprehensive offboarding process may include steps like deprovisioning the user’s account(s), changing their password(s), transferring file ownership, delegating their email inbox, and more.

What’s the business value of an offboarding policy?

In the age of SaaS, offboarding an employee doesn’t mean just collecting a keycard from them and calling it a day. Organizations should implement offboarding policies for two primary reasons:

Cost savings. From a financial perspective, if SaaS app licenses are not fully “shut off” for departed employees, organizations will continue to be charged for them. SaaS licenses can be costly. Some editions of Salesforce licenses, for example, cost $3,600 per user annually. This lack of oversight results in wasteful spending.

Security. From a security perspective, improper offboarding can have detrimental—even catastrophic—effects on a business.

If data access is not properly revoked, former employees can continue to log into critical systems and potentially destroy data or steal proprietary information. This is a massive security risk. A recent 2017 survey of 500 IT decision makers revealed that failure to deprovision employees from corporate applications has caused a data breach at 20% of companies.

The research report also revealed that nearly half (48%) of respondents are aware of ex-employees who still have access to corporate applications. A quarter (25%) of respondents take longer than a week to deprovision former employees, and a quarter (25%) do not even know how long accounts remain active after employees leave the company. According to the report, close to half (44%) lack confidence that former employees have been removed from corporate networks at all.

The report noted that the “more ingrained an employee” is in the company, the more challenging it is to deprovision their credentials, as it may be more complex than merely shutting down an account. (We will discuss recommended offboarding steps later in this section.)

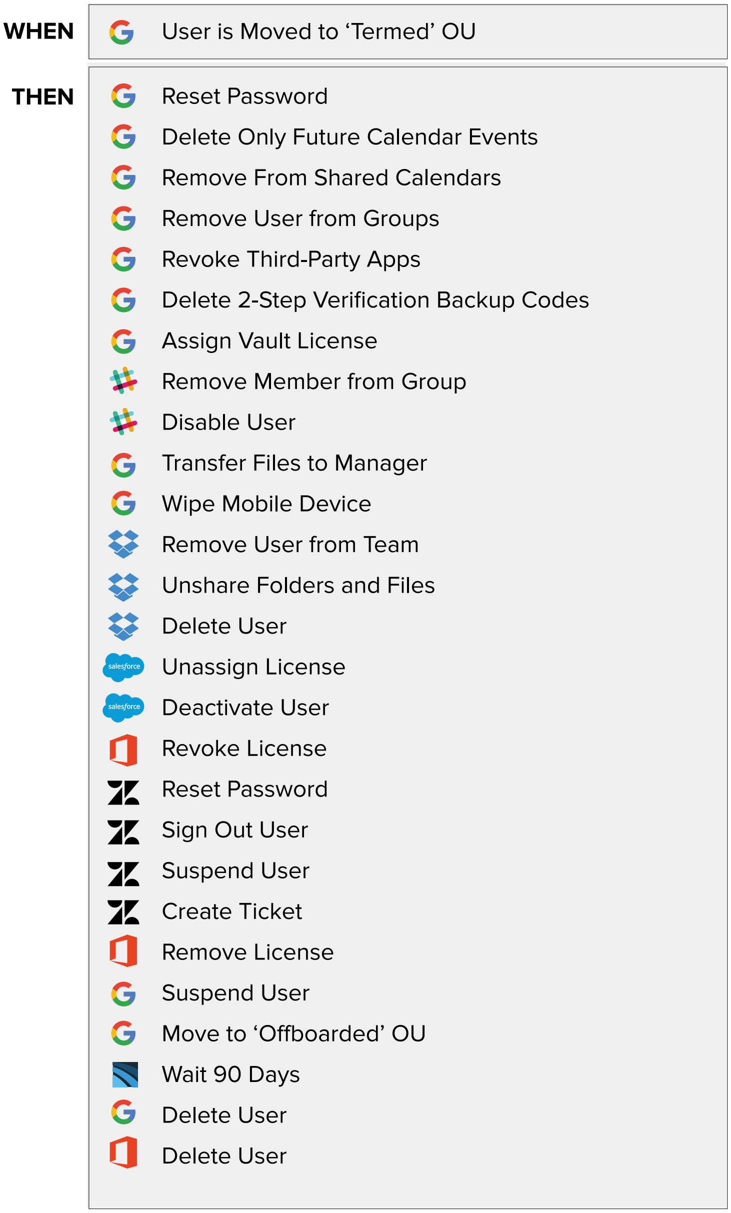
Similarly, according to Osterman Research, a whopping 89% of former employees retained access to Salesforce, email, Sharepoint, or other sensitive corporate apps. Furthermore, 45% retained access to “confidential” or “highly confidential” data, and 49% actually logged into ex-employer accounts after leaving the company.

These statistics, while troubling, are not surprising. Employees can easily retain access in the age of SaaS. Given how many SaaS apps companies use, it is impossible for IT to easily keep track of which users have access to which apps (and what kind of access, at that). By the same token, it is nearly impossible for IT to completely and thoroughly offboard users with 100% accuracy each time, ensuring access is revoked across all their SaaS apps. Indeed, one of the weakest points identified in the Osterman report was the lack of formal IT offboarding procedures.

These statistics mentioned above underscore the importance of a robust, thorough offboarding policy to keep corporate data safe. After all, when employees leave the company—especially if they’re heading to a competitor—the last thing you want is for them to still have access to trade secrets, customer lists, financial reports, etc. The longer a business goes without implementing an offboarding policy, the bigger the security risk is.

If offboarding is not completed correctly, chaos can ensue. Just take a look at these real-life news stories below. They illustrate the havoc that ex-employees can wreak when they retain access to company systems. Consider:

- The fired admin in Baltimore who used his still-active passcode to install keylogging software to steal employee passwords and slip porn into the CEO's PowerPoint presentation while the CEO was presenting to board members.
- The former sysadmin of a Pittsburgh health care facility who retained privileged access for *two years (!)* after he was fired. He deleted business data and patient health information (including medical records), causing at least $5,000 in damages and potentially interfering in the diagnosis and treatment of patients.
- The fired sysadmin of Georgia-Pacific (one of the world's largest manufacturers of paper) who used his previous accounts to access the mill's network and manipulate plant controls, causing multiple system failures and ultimately $1.1 million dollars worth of losses.



WHEN

User is Moved to 'Termed' OU

THEN

Reset Password
Delete Only Future Calendar Events
Remove From Shared Calendars
Remove User from Groups
Revoke Third-Party Apps
Delete 2-Step Verification Backup Codes
Assign Vault License
Remove Member from Group
Disable User
Transfer Files to Manager
Wipe Mobile Device
Remove User from Team
Unshare Folders and Files
Delete User
Unassign License
Deactivate User
Revoke License
Reset Password
Sign Out User
Suspend User
Create Ticket
Remove License
Suspend User
Move to 'Offboarded' OU
Wait 90 Days
Delete User
Delete User

Figure 3

What does an offboarding policy look like?

Offboarding policies will suspend or deactivate terminated accounts across SaaS providers and take all required actions (e.g., transfer, edit, modify) for a user to be offboarded fully. A robust offboarding policy minimizes data loss, business interruption, and/or security vulnerabilities. These policies must be in place to protect the environment and maintain data security. Like onboarding, offboarding processes will differ from employee to employee. The steps will differ based on department, role, employee type, etc. They may also include steps to ensure compliance with regulations.

Figure 3 is an example of an offboarding policy you can implement in BetterCloud.

Note: This is just a sample policy meant to illustrate the wide range of offboarding actions you can take in BetterCloud. Your offboarding policy may not require all of these steps.

What kind of steps should I be including in my offboarding policy?

We analyzed product usage data to see which offboarding actions customers are taking most often in BetterCloud. We found that:

- “Remove from Group” appeared in 74% of all offboarding policies.
- “Hide/Show User in Directory” appeared in 73% of all offboarding policies.
- “Reset Password” appeared in 67% of all offboarding policies.
- “Delete App-Specific Passwords” appeared in 62% of all offboarding policies.
- “Revoke User's Apps” appeared in 61% of all offboarding policies.
- “Delete 2-Step Backup Codes” appeared in 53% of all offboarding policies.
- “Remove from Shared Calendars” appeared in 41% of all offboarding policies.
- “Transfer Drive Files” appeared in 39% of all offboarding policies.
- “Suspend User” appeared in 34% of all offboarding policies.
- “Revoke Delegation Access” appeared in 30% of all offboarding policies.

REAL-LIFE BETTERCLOUD CASE STUDY

(For privacy purposes, we have removed all names from this customer story.)

Story #1: How a large retailer in the UK used policies to save 504 hours of manual offboarding work

A BetterCloud customer, a large retailer in the UK with thousands of employees, is using offboarding policies with great success. By automating large parts of their offboarding workflows, they’ve offboarded over 3,000 employees and saved 504 hours of manpower the first six months alone after purchasing BetterCloud. This equaled approximately £30,000 ($40,000 USD) in cost savings for them.

“With BetterCloud, we have achieved a significant degree of automation with the offboarding process—a stunning result,” said their IT manager.

Story #2: How First Round Capital uses policies to offboard users in 30 seconds and ensure all their access is completely revoked

First Round Capital is a top-tier early-stage venture capital firm with over $700 million in capital under management.

“SaaS creates a lot of exposure for me when employees leave the company,” says Ryan Donnon, the IT and data manager at First Round.

When an employee exits, Donnon uses an automated policy in BetterCloud to accomplish a laundry list of tasks he used to have to remember to do manually.

“The workflow immediately removes them from all groups, deactivates two-factor authentication, resets their password, and revokes authentication tokens for all of the applications that the employee has connected to their account. And most recently, I’ve updated the workflow to actually deactivate their Salesforce account as well,” he says.

Donnon says all he needs is thirty seconds before he can confidently look an investor in the eye and say, “We’re good. Everything sensitive is protected.”

While most of these offboarding tasks are relatively simple, each must be performed immediately when an employee is offboarded, making the workflow orchestration a critical value-add.

“I think offboarding, as opposed to onboarding, is where I have the most exposure. If I mess up, forget a step, and an ex-employee still has access to company data, that’s where I could hurt my reputation the most,” he says.

Next, because First Round Capital uses SAML for most applications other than G Suite, he “kills the ex-employee’s Okta account, which pretty much cuts off access to everything else.” Donnon views BetterCloud and Okta as entirely different, but complementary solutions. “Even if you use Okta for deprovisioning, it can’t do everything that you need to do. BetterCloud picks up where Okta leaves off.”

Since G Suite cannot serve up an auto-reply if an employee is suspended or deleted, Donnon uses BetterCloud to set the auto-reply.

At the end of the two weeks, Donnon goes into BetterCloud again. He takes care of what many forget: recurring calendar events, which often may be consuming shared resources like conference rooms. “If an ex-employee is the owner of any recurring events, I need to work with either their manager or the person that replaced them to figure out who I should transfer those events to.” If not, this can be an especially excruciating task to perform after the fact. “Google does not have a great way to transfer recurring events from a deleted user,” says Donnon.

Next, Donnon backs up the account, transfers all of their shared Google Docs (typically to their manager), and then, unlike many G Suite admins, will actually delete their email account. (Many companies choose to suspend accounts for various reasons, but deleting a user will reduce costs since Google does charge for suspended users.)

Story #3: How a K-12 School used policies to reduce their time spent offboarding by 83%

Another BetterCloud customer, a K-12 school, used policies to reduce their time spent offboarding people by 83%. (For privacy purposes, we have removed all names from this customer story.) It takes the IT manager less than five minutes to offboard a user today.

How does he do it? To start with, he has a triage group in G Suite to hold users who are leaving the organization. Once he moves a user to this organization, it triggers an automated workflow in BetterCloud, which he’s customized to include:

- Suspending the user’s Google account
- Deactivating two-factor authentication
- Removing phone numbers from the account
- Resetting the user’s G Suite password
- Delegating the user’s email
- Transferring the user’s Drive files to their manager
- Disabling IMAP and POP settings
- Removing the user from Slack channels and user groups
- Creating a Zendesk ticket to keep track of this offboarding event

These steps automatically take place, cutting down the manual, repetitive work often associated with offboarding.

"Assuming that I've configured the workflow correctly, it shouldn't take me more than five minutes per user for the total offboarding process. The overall process is about 1/6th of the time," says the IT manager.

In fact, he recently used BetterCloud to offboard users even though he wasn't at his desk. All he did was move those users to the designated org unit, and it automatically kicked off his offboarding workflow. "I actually did it from my phone while I was out, which is a huge plus," he says. "I was able to do it without being at my desk for an hour and a half to go through all these things and create a big checklist, which is really helpful."

He added that this can be particularly beneficial if, for example, someone voluntarily leaves on short notice. He can then trigger an offboarding workflow from virtually anywhere, ensuring that their access is terminated immediately.

CATEGORY #2

Data Loss Prevention (DLP)

Why you should care about the loss of sensitive data

From Equifax to Uber to Yahoo, it seemed like 2017 was the year of data breaches.

DLP is a hot button topic, especially with new regulations like GDPR looming on the horizon. Designed to protect data, GDPR introduces stiff penalties and tight reporting windows for data breaches, so it's especially important to protect sensitive data.

In the age of SaaS, however, it's especially easy to expose sensitive data by accident. There are multiple ways end users can share a file, and often they are unaware of the implications. All it takes is one simple misconfiguration in the sharing settings to expose sensitive data. Files that weren't meant to be shared suddenly are.

Take Stanford University, for example. In late 2017, Stanford suffered three separate data breaches that exposed personal employee information (including social security numbers and salary information), confidential financial aid, and student sexual assault reports. All of this happened due to "misconfigured permissions" on Google Drive. Stanford said that the folder's permissions were changed, making the file "inadvertently accessible" on the business school's shared drive.

Or consider the Docs.com snafu in 2017. Because the default setting for Docs.com was public sharing, many users were unwittingly sharing sensitive docs publicly. Unbeknownst to them, these docs were indexed by public search engines, so anyone could find and view their sensitive data. Researchers found a trove of sensitive data, including logins, passwords, names, social security numbers, bank account numbers, and medical data (including treatment logs and photos).

Here are two policies that will prevent data loss and lock down sensitive information.

DATA LOSS PREVENTION POLICY #1

Content discovery

What is a content discovery policy?

Content discovery policies identify confidential or sensitive data and monitor its movement through a corporate network while ensuring that it does not leave the perimeter. As the name implies, it is designed to identify confidential or sensitive data based on the content of a file.

Content discovery policies often seek to identify information like social security numbers, credit card numbers, bank account numbers, and personally identifiable information (PII) that should not be stored in SaaS apps. If files containing sensitive information or certain high-risk keywords (like “Confidential” or “Attorney Client Privilege”) are shared inappropriately or exposed publicly, content discovery policies can detect this and then remediate it, ensuring that all confidential data stays confidential.

What’s the business value of a content discovery policy?

Content discovery policies create two main benefits for the business:

> **Ensure compliance.** Content discovery policies help companies remain in compliance by protecting specific types of information (e.g., credit card numbers, PII, social security numbers), in order to meet industry, legal, or regulatory compliance requirements. Examples of security and privacy regulations and standards include HIPAA, GDPR, Sarbanes-Oxley, PCI, etc. Under GDPR, which will come into force on May 25, 2018, data breaches must be reported within 72 hours.
>
> **Protect intellectual property or proprietary information.** Content discovery policies can detect and protect critical data that gives an organization their competitive advantage. This can include client lists, product designs, customer lists, merger and acquisition details, trade secrets, patents, source code, financial information, product roadmaps, manufacturing procedures, pricing and sales data, and so forth.

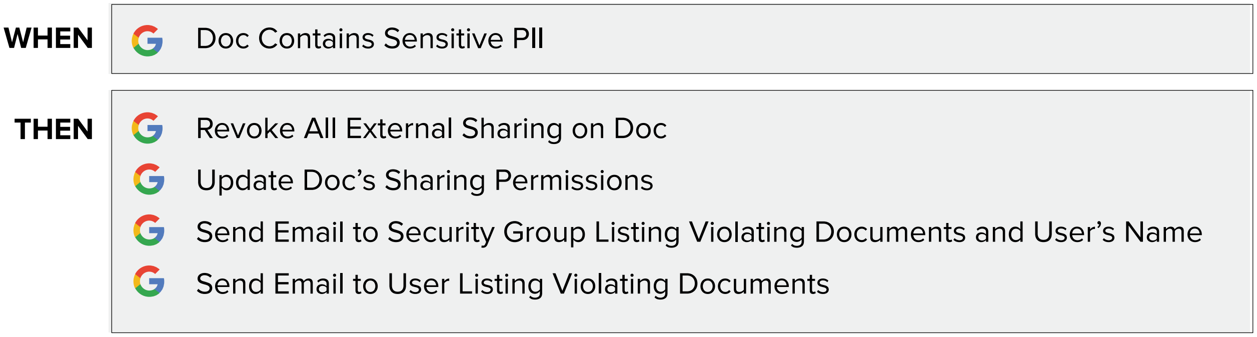
By helping prevent data loss, content discovery policies also help protect against any fallout that would happen if a company were to suffer a data breach: loss of customer trust, reputational damage, decreased revenue, bad PR, etc.

It can take just minutes to compromise a domain, yet more than 75% of data loss incidents aren't discovered for many days, according to a [Sept. 2016 McAfee Labs Threat Report](). A content discovery policy works to immediately protect a business and remediate any potential data exposure or loss.

What does a content discovery policy look like?

A content discovery policy will first identify what it is that you consider sensitive (i.e., what you want to protect). This can be PII, credit card numbers, social security numbers, or a particular keyword. It detects when anyone creates or updates files with this sensitive data, and then it takes some type of action to remediate it, thereby limiting exposure.

Here's an example of a content discovery policy in BetterCloud:



WHEN

- Doc Contains Sensitive PII

THEN

- Revoke All External Sharing on Doc
- Update Doc's Sharing Permissions
- Send Email to Security Group Listing Violating Documents and User's Name
- Send Email to User Listing Violating Documents

Figure 4

What kinds of data should I implement a content discovery policy for?

The content discovery policies you implement depend on many variables, such as your industry, business needs, compliance needs, etc.

In healthcare, for example, protecting PII is mandatory. Hospitals often use BetterCloud to search documents for social security numbers, zip codes, phone numbers, and email addresses. Schools may want to search for obscenities, sexually explicit or profane content, individualized education plans (IEPs), financial aid information, etc. Organizations that must be PCI compliant often search for publicly shared Visa, MasterCard, American Express, and Discover credit card numbers. In BetterCloud, you can even create a custom regex to search for payment types common in your location. Some organizations may want to search for publicly shared documents in general, executable files (.exe), files that are shared with specific domains, and so forth.

REAL-LIFE BETTERCLOUD CASE STUDY

(For privacy purposes, we have removed all names from this customer story.)

Story #1: How a manufacturing company makes sure passwords aren’t stored on Google Drive

A large US-based manufacturing company with over 10,000 employees made a startling discovery one day. The IT team discovered that employees had created several documents in Drive that listed login and password information to shared service accounts. This was a huge security risk. If anyone gained unauthorized access to their Drive files, they would also have credentials to those shared service accounts.

The IT team immediately took action and set up a BetterCloud DLP policy. Because they knew that employees were using the same few service account passwords for various accounts, they implemented a policy that searched for these passwords. If detected, the policy would alert IT and automatically revoke sharing settings on these documents. This ensured that passwords could no longer be stored on Drive—and if they were, the violation would be remediated immediately.

Story #2: How a school district used DLP policies to discover that a student was suicidal

Another BetterCloud customer, a school district in the US, implemented a policy to search for self-harm keywords in their G Suite environment. One day, the IT department received a notification that one of the students had created and shared a suicide note in Google Docs. Immediately, IT notified school officials and they were able to provide crisis counseling for the student. Without the ability to detect sensitive keywords in their G Suite environment, the school (and student’s family) would never have known about this.

This customer story is a good example of how DLP policy use cases can differ by industry. In schools, DLP policies can identify and protect sensitive data such as health records, confidential education records, and inappropriate files that young students should not have access to. They can also identify high-risk keywords, as this story illustrated, and potentially save a student’s life.

DATA LOSS PREVENTION POLICY #2

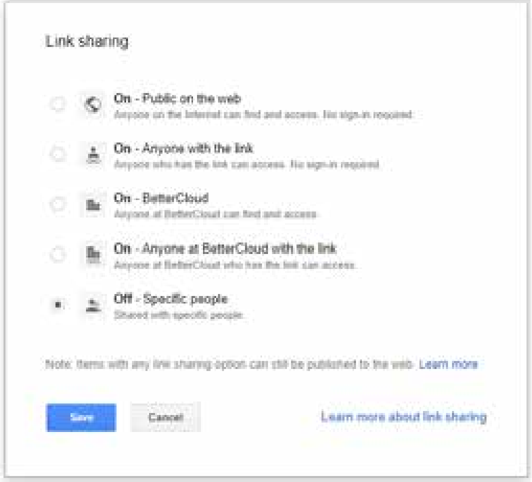
Publicly shared files

What are publicly shared files?

The beauty of SaaS apps is that they enable collaboration. Users can share documents, spreadsheets, presentations, etc. with a specific person(s), anyone in the domain, or even publicly, allowing others to read, comment, and/or edit the file.

Public sharing, however, can be dangerous. There are different types of publicly shared files. For example, they may be public in your domain, meaning anyone in your organization can find and access them. Another option is "Public on the web," meaning they are indexed by Google and can be found and accessed by anyone on the internet. No sign-in is required. This is the riskiest sharing setting.

When a user goes to share a file in G Suite, they have several link sharing options available to them:



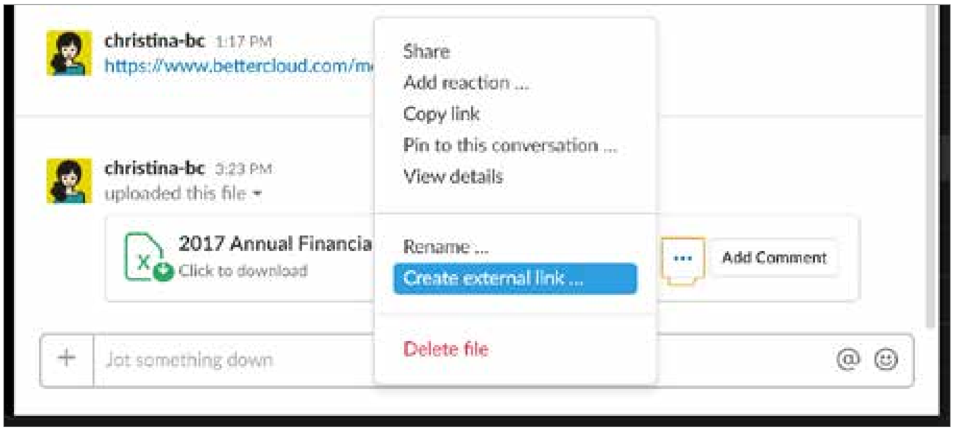
Link sharing

- ○ 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 - BetterCloud
  Anyone at BetterCloud can find and access.
- ○ On - Anyone at BetterCloud with the link
  Anyone at BetterCloud who has the link can access.
- ● Off - Specific people
  Shared with specific people.

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

Figure 5

A user can also create a public link for any file shared within Slack. Admins can disable the creation of public links in their Slack settings, but this option is enabled by default. Users will see an option to Create External Link for files:



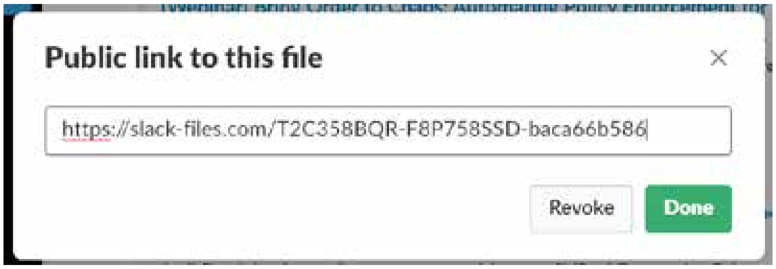
christina-bc 1:17 PM
https://www.bettercloud.com/m

christina-bc 3:23 PM
uploaded this file ▾

2017 Annual Financia
Click to download

Figure 6

This will generate a public link for the file.

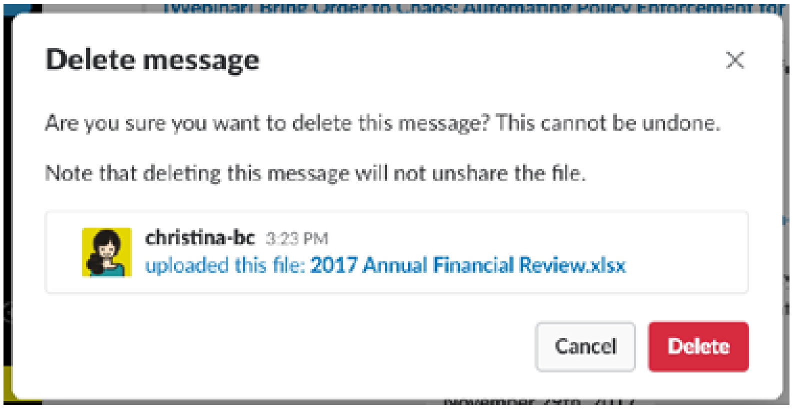

[Webinar] Bring Order to Chaos: Automating Policy Enforcement for
Revoke
Done

Public link to this file

https://slack-files.com/T2C358BQR-F8P758SSD-baca66b586

Figure 7

And even if the Slack message is deleted, the file is not. It still remains public and accessible by anyone on the internet.


[Webinar] Bring Order to Chaos: Automating Policy Enforcement for
Cancel
Delete
November 29th, 2017

Delete message

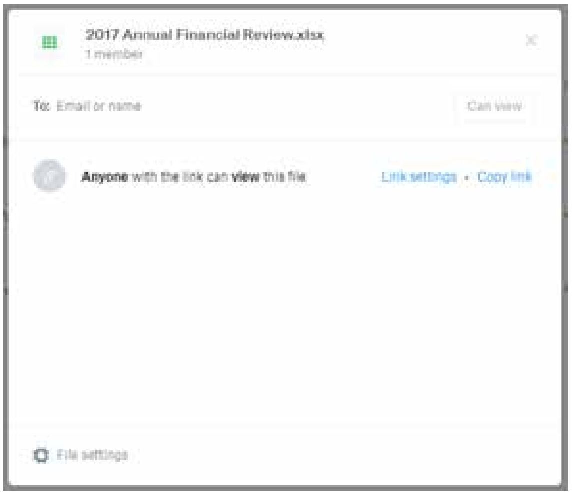
Are you sure you want to delete this message? This cannot be undone.

Note that deleting this message will not unshare the file.

christina-bc 3:23 PM
uploaded this file: 2017 Annual Financial Review.xlsx

Figure 8

Similarly, when a user goes to share a file in Dropbox, they can create public links where anyone with the link can view the file:



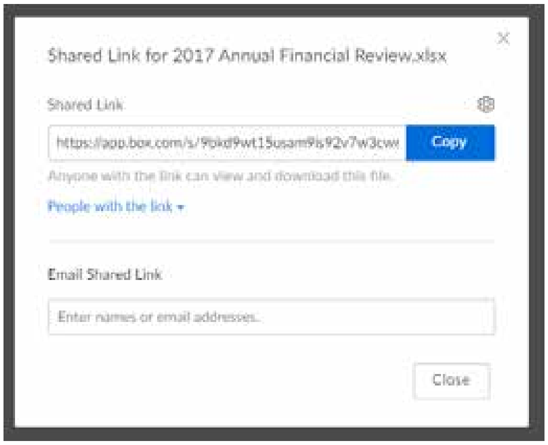
2017 Annual Financial Review.xlsx
1 member

To: Email or name

Anyone with the link can **view** this file

Figure 9

The same goes for Box. Users can create public links, allowing anyone with the link to view and download the file.



Shared Link for 2017 Annual Financial Review.xlsx

Shared Link

https://app.box.com/s/9bkd9wt15usam9is92v7w3cw

Anyone with the link can view and download this file.

Email Shared Link

Enter names or email addresses.

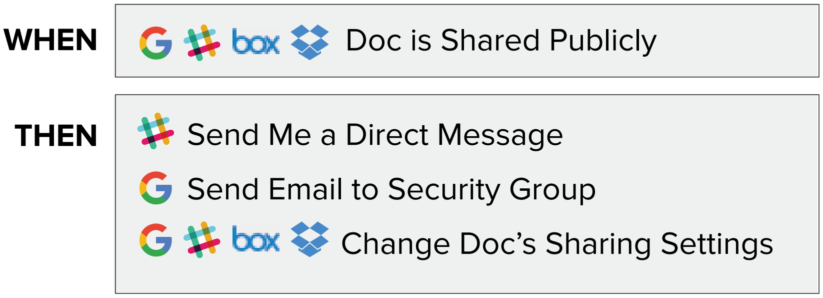
Figure 10

What's the business value of a publicly shared file policy?

Publicly shared files are extremely risky since anyone on the internet (or domain) can find and access them. Similar to the business value of DLP policies, publicly shared file policies help companies stay in compliance and/or protect critical IP by keeping information away from prying eyes.

What does a publicly shared file policy look like?

The purpose of this policy is to gain visibility into any publicly-facing data that your organization has. The broadest form of this policy will flag any files that are publicly shared. More granular policies will search data by attributes like file type, name, content, owner, etc. to ensure that specific types of data are not publicly shared. Not all publicly shared files necessarily translate to a data breach or security risk. Some files may be meant to be public-facing (for example, a community calendar or a customer FAQ document). Policies that are overly broad may result in false positives or irrelevant notifications. It's important for IT to know which files should be publicly shared (if any). A robust policy will specify exactly what kind of publicly shared files your organization is most concerned about, and then remediate the public sharing in some way.



WHEN Doc is Shared Publicly

THEN Send Me a Direct Message
Send Email to Security Group
Change Doc's Sharing Settings

Figure 11

Figure 11 is an example of a policy in BetterCloud.

On average, how many publicly shared files do companies have?

Looking at BetterCloud customer data, we've found that SMBs (50-300 seats) share 10.6% of their files publicly (on average). Mid-market to enterprise companies (300+ seats) share a similar amount: 10.3%. Some companies may need to share more public-facing documents than others, but the average organization typically doesn't need to share many files publicly.

REAL-LIFE BETTERCLOUD CASE STUDY

(For privacy purposes, we have removed all names from this customer story.)

Story #1: How a K-12 school discovered that 800,000 files were shared with everyone in the domain

(For privacy purposes, we have removed all names from this customer story.)

A BetterCloud customer, a K-12 school, recently used BetterCloud to audit and change permissions for 800,000 files.

The IT manager at this K-12 school knows that they have highly sensitive data that must be protected. "It's things like a nine-year-old's medical records—not something to be taken lightly," he says. While student records are not stored on Drive, information about students can easily end up in Drive since teachers work heavily in G Suite. But the complexity of this challenge is twofold. In addition to keeping student data safe, his team has large amounts of enterprise data that they need to secure as well.

Before they purchased BetterCloud, his team was auditing Drive files manually—a Sisyphean task.

"It was very difficult, to the point of impossible," he says. "We can't shrug off security, so we ended up using BetterCloud pretty heavily for auditing and reporting.

"We found that some of BetterCloud's more useful features were actually around things like document management and security. We knew that a lot of our employees were probably not taking security as seriously as they should be, particularly with regards to Google Drive," he added.

He was right. Last summer, he discovered that there were 800,000 files shared with everyone in the domain.

Not all of the files were sensitive; in fact, many of them were blank, trashed, or in the Drives of departed employees. Still, he immediately mass changed the permissions on all of those to "Private," which preserved their intended files shares but reduced their exposure org wide.

"BetterCloud really improved the ability to make that mass change, rather than attempting to audit them all," he says. "There was certainly a fair deal of things that needed to be reclassified, or things where we had to specifically set aside time with employees to go over their particular practices. In the aftermath, I spent a lot of time giving people permissions back to documents, and I did that through BetterCloud as well."

Story #2: How a large entertainment company found a confidential earnings document shared publicly in Drive

(For privacy purposes, we have removed all names from this customer story.)

A large entertainment company with thousands of employees wanted to know if their employees had stored any sensitive financial information on Google Drive. They implemented a BetterCloud DLP policy to find out. Sure enough, the policy alerted them to an earnings document that was shared publicly in Drive. What was troubling was that this document contained quarterly earnings that had not been publicly announced yet.

Using BetterCloud, they immediately corrected the sharing settings on the document and changed it to private. They also implemented a granular policy for that exact use case and set it to automatically change sharing settings if this scenario ever happened again.

CATEGORY #3

Insider Threats

Why you should care about insider threats

You may be surprised to learn that the most dangerous security threats often don't come from hackers or other external actors.

Headlines like this one from the Harvard Business Review—"The Biggest Cybersecurity Threats Are Inside Your Company"—are common in the security world. Indeed, many data security experts agree that insiders (not outsiders) pose the greatest data security risk to businesses.

Insider threats are attacks, breaches, or exposures that are caused by employees within the organization. Insiders can be particularly insidious (whether intentionally or not) because employees have intimate knowledge of a company's infrastructure, business practices, systems, and applications.

The statistics show how exposed organizations truly are. Employees account for 43% of data breaches, according to Intel, and half of these incidents are accidents. What's more, one in four IT security staff admits to using their privileged login rights to look at confidential information. The vast majority of organizations (74%) feel vulnerable to insider threats, while 56% of security professionals say insider threats have become more frequent in the last 12 months, according to a 2016 Insider Threat Report. Another survey found that an overwhelming majority (88%) of respondents view insider threats as a dangerous and growing concern in defending their organizations.

There are various types of insider threats, and all of them pose a risk. We'll discuss three main types:

malicious, accidental/negligent, or compromised.

Malicious insiders intentionally steal or destroy data. They have nefarious intentions. Armed with insider privileges, they know their way around and therefore know exactly how and where to cause the most havoc. Take, for example, the about-to-be fired IT admin who deliberately wiped multiple Citibank routers, shutting down 90% of the firm's networks in the US. Or take the IT administrator at Columbia Sportswear who, after leaving the company, accessed his former employer's network 700 times, stole information, and turned it over to his new bosses (he was later sued for malicious insider data theft).

In fact, malicious insiders pose such an alarming security threat that the FBI even released a warning a few years ago, cautioning:

> "The exploitation of business networks and servers by disgruntled and/or former employees has resulted in several significant FBI investigations in which individuals used their access to destroy data, steal proprietary software, obtain customer information, purchase unauthorized goods and services using customer accounts, and gain a competitive edge at a new company... businesses incur significant costs ranging from $5,000 to $3 million due to cyber incidents involving disgruntled or former employees."

Accidental/negligent insiders don't intend to expose data. They have no malicious intent. They are employees who happen to have access to confidential or sensitive information, and they accidentally expose it somehow. For example, there was the 36,000-employee data breach at Boeing that occurred all because an employee emailed a spreadsheet to his spouse for formatting help. When you consider that organizations typically give employees much more access than they need—62% of business users report that they have access to company data that they probably should not see—these types of insider threats are especially important to mitigate.

Information Security Forum (ISF) members report that completely inadvertent breaches are more common than malicious ones. According to Verizon's Data Breaches Incident report, accidents accounted for almost 30% of the information security incidents in 2015.

Compromised insiders have accounts that have been compromised by external attackers. They may not even realize they've been compromised. These attackers take advantage of the insider's access to systems, data, applications, etc. Later in this section, we'll discuss a customer story about a compromised insider who was able to identify and fix the insider threat using BetterCloud.

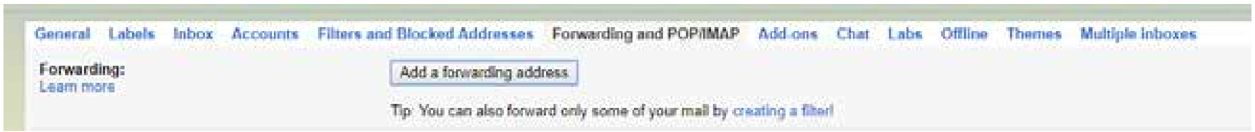
Nearly one-third of all organizations still have no capability to prevent or deter an insider incident or attack, according to the SANS Institute. Because insider threats are so commonplace, IT departments need to be able to detect when they occur so that they can take appropriate action. We'll dive into two key policies that mitigate insider threats.

INSIDER THREATS POLICY #1

Email forwarding to external addresses

What is email forwarding?

In Gmail, users can automatically forward Gmail messages to an external address. They can forward all new messages or only certain types of messages. It's very simple and quick to do. A user can head to their Gmail settings and set up automatic forwarding on their own in a matter of minutes.



General Labels Inbox Accounts Filters and Blocked Addresses Forwarding and POP/IMAP Add-ons Chat Labs Offline Themes Multiple Inboxes

Forwarding:
Learn more

Add a forwarding address

Tip: You can also forward only some of your mail by creating a filter!

Figure 12

What's the business value of an email forwarding policy?

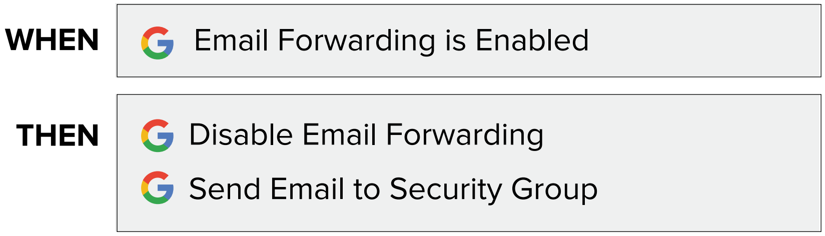
If automatic email forwarding to external addresses is occurring, this means corporate data is automatically leaking outside your domain. Users may be intentionally forwarding data to their personal email accounts, to competitors, or even unknowingly forwarding it to hackers (more on this below). Contractors often receive corporate email addresses but prefer to forward emails to their personal emails and work from there instead.

All of these emails can contain confidential or sensitive data. To keep corporate data safe, IT needs to know if and when users are forwarding email. For example, an ex-Chemours employee was caught stealing trade secrets and IP (valued at $150 million) when the company detected him sending confidential documents to his personal email account.

What does an email forwarding policy look like?

You generally shouldn't permit users to automatically forward any emails to another account. A solid email forwarding policy will detect when a user configures their inbox to be forwarded to another address. It will then remediate the violation, which can include steps like disabling email forwarding on their account and alerting the security team.

Here's an example:



WHEN
Email Forwarding is Enabled

THEN
Disable Email Forwarding
Send Email to Security Group

Figure 13

As a best practice, you shouldn't permit any email forwarding rules in your environment at all. Of course, there may be exceptions. But generally speaking, there are few valid reasons why any user should be automatically forwarding emails to another address.

REAL-LIFE BETTERCLOUD CASE STUDY

(For privacy purposes, we have removed all names from this customer story.)

How hackers set up automatic email forwarding to steal data from a hospital

October 9, 2015, started like any other fall day for Middlesex Hospital, located in Middletown, Connecticut. But they soon discovered that four of their employees had fallen victim to an email phishing scam that potentially resulted in the breach of 946 patients' personal and demographic information. The attackers managed to steal users' credentials through their phishing scam. **Unbeknownst to the victims, the attackers secretly and silently set up email forwarding rules in those four users' compromised Gmail inboxes.**

This was a particularly insidious type of scam, one that was immune to typical responses like resetting users' passwords. Even if users followed recommended best practices and changed their passwords, those email forwarding rules would still continue to exist. As a result, the hackers could continue to forward users' emails without their knowledge.

Luckily, Middlesex Hospital was using BetterCloud's email forwarding report, which displays user accounts with forwarding rules in place, and to which email addresses they're forwarding mail. When the IT team ran the report, they immediately noticed that emails were being forwarded to a suspicious address.

"BetterCloud gave us the ability to identify exactly what happened that led to the breach," said Andrew Shelton, Information Security Manager at Middlesex Hospital.

The IT team quickly resolved the issue, removing the forwarding rules, resetting everyone's passwords just to be safe, and securing the environment. Ultimately, while the breach may have exposed patients' names, dates of birth, medical record numbers, medications, and/or diagnoses, luckily no social security numbers or credit card information was accessed.

INSIDER THREATS POLICY #2

Competitor sharing

What is competitor sharing?

To enable collaboration, SaaS apps permit users to share files with users outside their domain. Competitor sharing is when a user shares a file specifically with a competitor.

What's the business value of a competitor sharing policy?

Competitor sharing policies prevent the loss of IP, which is the lifeblood of any company. If data like trade secrets, research results, financial data, customer lists, and patents fell into the hands of your competitor, it could have serious ramifications.

Here's an example of the damage it can cause. In 2011, an engineer with privileged user access at American Superconductor, a US-based global energy company, was enticed by a Chinese company to steal source code and other intellectual property from his employer. As a result of his theft, the company lost three quarters of its revenue, half of its workforce, and more than $1 billion in market value.

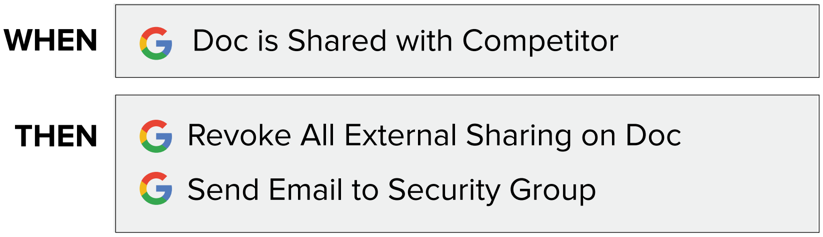
GM and Ford were also burned a few years ago by employees who stole and shared sensitive information with foreign competitors. Ford suffered losses between $50-$100 million in labor costs, and GM said the thousands of documents stolen were worth more than $40 million.

"Among all companies, the greatest impacts of proprietary information loss were increased legal fees and loss of revenue. For large companies (over $15 billion), loss of competitive advantage was the most serious problem. For financial firms, embarrassment was the biggest concern; and for high technology companies, the major issue was loss of competitive advantage," writes Network World.

What does a competitor sharing policy look like?

A competitor sharing policy will detect when a file is shared with an email address containing @ competitor.com. It will then take action to remediate this sharing (such as revoking external collaborators).

Here's an example:



WHEN

Doc is Shared with Competitor

THEN

Revoke All External Sharing on Doc

Send Email to Security Group

Figure 14

CATEGORY #4

Admin Permissions

Why you should care about admin permissions

Administrator permissions, or privileges, is another area where policies are critical.

It's a best practice to implement the principle of least privilege, but the reality is that many users in a SaaS-heavy workplace often have way more privileges than they need.

This happens because many of the less mature SaaS applications offer only binary options: super admin or end user, with nothing in between—it's all or nothing. Therefore, employees who only need a few rights may be made into unwitting super admins. IT teams may not necessarily want to grant an employee *carte blanche*, but they are left with no other option. IT must either hand over all the "keys to the kingdom" or risk impeding employee productivity, as end users must then wait for IT to make user lifecycle and data management changes.

Here's a common scenario. Employees who are working on a specific task or project will request admin access or elevated access in general. There are no granular access roles, so IT has no choice but to give them full super admin access so they can do their jobs. However, this access is never revoked. There's no easy to way to keep track of, much less automate, that in native admin consoles. Some IT teams resort to manually updating spreadsheets, but most teams simply don't track it at all. The default action is to give a user super admin access and leave those permissions open.

As a result, this leads to an over-assignment of super admin privileges across SaaS applications. Employees who only needed super admin access to do one task suddenly have alarming amounts of power for weeks, months, perhaps even years at a time.

Not to mention, these requests for permissions add up: For a 1,000 employee company, the overhead of permissions request tickets can cost up to $180K/year.

Giving employees more employees rights than needed is ill-advised on many levels, mainly because it snowballs into larger security problems down the line. "If you hand out admin privileges like candy, it'll come back to haunt you," writes CSO.com.

Here are two policies that help enforce the least privilege model by keeping super admin access to a minimum.

ADMIN PERMISSIONS POLICY #1

Super admins

What are super admins?

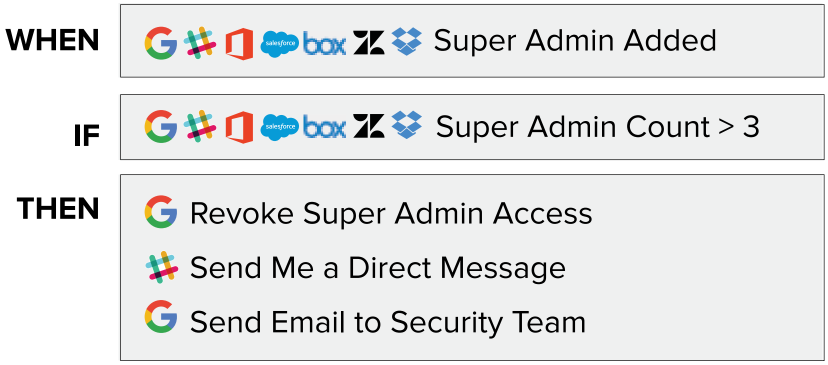
Super admins are users who have full access to all system administrative controls and features in native SaaS admin consoles. They have the highest level of privileges. They manage all aspects of an organization's SaaS apps, controlling the highest-level security and admin settings. Typically they have full create, read, update, delete (CRUD) permissions. Many organizations assign super admin roles to IT, help desk, or security team members since they need full access to perform a specific action (or actions) within the application's admin console.

What's the business value of a super admin policy?

This policy ensures that organizations have only the bare minimum of super admins they need to manage their SaaS applications and/or do their job. Similar to a least privilege model, this is a "least admin model," so to speak. By limiting the number of super admins, organizations greatly minimize the damage that hackers can inflict. Given how prevalent data breaches are, super admin policies proactively protect against data loss and theft.

Why is this? The more super admins you have, the bigger the security risk. "Every additional administrator causes linear-to-exponential growth in risk," according to CSO.com. While everyone likes to trust their administrators, it is best practice to assign super admin access to a few top IT and security professionals and limit other admins to only the tools and data objects they need to do their job. It's not a matter of integrity (or lack thereof). More admins objectively mean more endpoints to hack, more room for error, and more leeway for attackers to access other privileged accounts.

"Every additional admin doesn't just increase his or her own risk; if they're compromised, they add to the takedown risk of all the others. Each admin may belong to groups others do not. If a hacker compromises A and gets to B, B may more easily lead to C, and so on," writes CSO.com.



WHEN Super Admin Added

IF Super Admin Count > 3

THEN
Revoke Super Admin Access
Send Me a Direct Message
Send Email to Security Team

Figure 15

What does a super admin policy look like?

A good policy detects when new super admins are added and whether they exceed a threshold (that you set). It then remediates the violation—whether that means notifying you or automatically taking action.

REAL-LIFE BETTERCLOUD CASE STUDY

(For privacy purposes, we have removed all names from this customer story.)

How excessive super admin access at a technology company led to sensitive data exposure

(For privacy purposes, we have removed all names from this customer story.)

One evening, a BetterCloud customer—a technology company of about 500 people—realized something was very wrong. When users created new files in G Suite, they were automatically shared publicly. The default sharing setting had been changed. Rather than being private to the user, all newly created files were, by default, visible to anyone on the internet.

They soon realized that hundreds of sensitive files—investor decks, operating models, employee reviews—were widely visible to the public.

Panic-stricken and unsure how to fix it, they attempted to change the sharing setting to something more restrictive. It worked—sort of. Now, the default setting for files was “visible to everyone in the domain.” This was marginally better but still problematic. Anyone in their domain could search for and find those files.

Working quickly with the BetterCloud team, they reviewed audit logs and discovered which day the setting had been changed to “Public on the internet.” Using BetterCloud, they set up policies that searched for all files created after that date and then changed the sharing settings in bulk on every file.

How did the default sharing setting change? For a 500-person company, the company had an inordinately high number of IT personnel with super admin privileges: 10 people had them. One of these employees, a junior help desk employee, had been given super admin access for a task but his access had never been revoked. He had inadvertently changed the default sharing settings for the entire organization.

By using BetterCloud, the company was able to delegate access to helpdesk employees and create limited access roles for them, reducing the number of super admins from 10 to three.

This case study illustrates the dangers of having too many super admins in your organization. Assigning super admin rights, but failing to revoke them later, is a very common situation and happens all too easily. Unfortunately, this creates an excess number of super admins, which increases the likelihood of mistakes and security vulnerabilities.

ADMIN PERMISSIONS POLICY #2

Access roles (delegating admin permissions)

What do access roles mean?

Access roles are a way to give (non-super admin) users the ability to only execute specific administrative functions. Access roles outline which administrative functions users can and can't do. Excessive super admin access is a serious security risk, so access roles are an effective way to delegate admin permissions to users and avoid giving them all the keys to the kingdom. IT can assign special roles and specific security levels to different employees.

These privileges are typically role-based, so the type of access rights an employee receives will depend on his function and job duties. By delegating admin permissions, IT can create a hierarchy of privileged rights and controlled access.

What's the business value of an access roles policy?

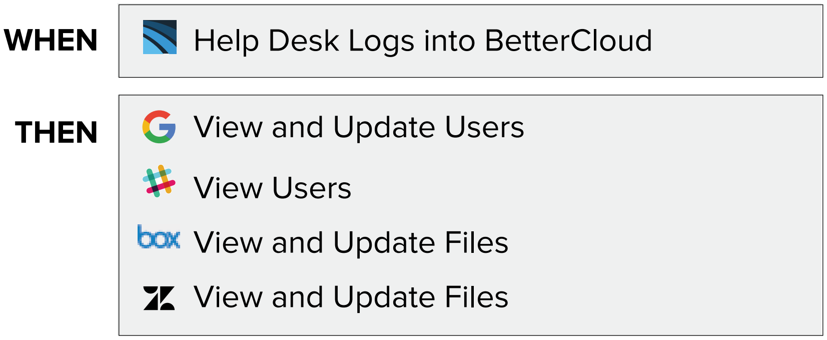
The business value is twofold. First, it greatly reduces exposure to risk. Employees have the least amount of admin privileges they need to do their job and nothing more. This allows organizations to implement the least privilege model, which is a security best practice.

Additionally, because access roles delegate responsibilities, this frees up upper-level IT employees to focus on innovative, strategic work that drives the business forward.

What does a delegation policy look like?

A solid delegation policy implements the principle of least privilege. It gives people the bare minimum—the least level of permissions they need—to do their jobs. By granting granular access, you avoid the need to give people full super admin rights.

Here's an example:



WHEN Help Desk Logs into BetterCloud

THEN View and Update Users

View Users

View and Update Files

View and Update Files

Figure 16

REAL-LIFE BETTERCLOUD CASE STUDY

(For privacy purposes, we have removed all names from this customer story.)

How delegating permissions allowed a large retailer's IT team to focus on value-add work

A large retailer in the UK with thousands of employees built out access roles for multiple levels of each division's help desk personnel (Level 1, 2, and 3). Previously, their Google super admin team had been using scripts to take care of tedious admin tasks. Creating access roles allowed them to delegate these admin tasks to lower-cost support desk personnel. These access roles included permissions related to email delegation, user offboarding policies, group management, user profile management, Drive file troubleshooting, email signatures, auto-reply, and filter and label management.

By using access roles and delegating admin permissions, their higher-level IT teams could turn their attention to other initiatives, which they were tremendously excited about. This allowed them to focus on value-add work (such as roadmaps and early adopter programs), improving internal customer engagement, improving supplier engagement, and realigning business and technology demands.

CATEGORY #5

External Access

Why you should care about external access

External users are people who do not belong to your organization, but need temporary access to your data to do their jobs. Examples include freelancers, interns, consultants, or contractors.

Freelancers are on the rise—by 2020, 50% of the US workforce will be freelancers—so policies on external access will become increasingly critical in the modern workplace. Below are two important policies that help manage external access and keep data secure.

EXTERNAL ACCESS POLICY #1

Groups with external members

What are groups with external members?

Typically, groups in SaaS apps contain only the people in your organization (e.g., your marketing employees, sales teams, managers, etc). But groups can also include external users outside of your domain. The names for these external member roles may vary across SaaS apps. For example, in Slack, they are called Multi-Channel or Single-Channel Guests, and they can have access to multiple channels or just one channel. Adding external users to groups can help facilitate communication and collaboration.

What's the business value of a policy for groups with external members?

Anytime an external member has access to an organization's data, however limited that may be, IT needs to keep a tight rein on group memberships in order to limit external access to corporate data.

But that's easier said than done. It's very easy to forget which external users are in which groups. They might have been added for the right reason initially, but all too often they stay in groups way past their contract end date. There is no easy way to track this in native admin consoles or automate the removal of their access. As a result, external users often end up retaining access to company data for longer than necessary. This increases the risk of sensitive and/or confidential data being accessed in an unauthorized fashion.

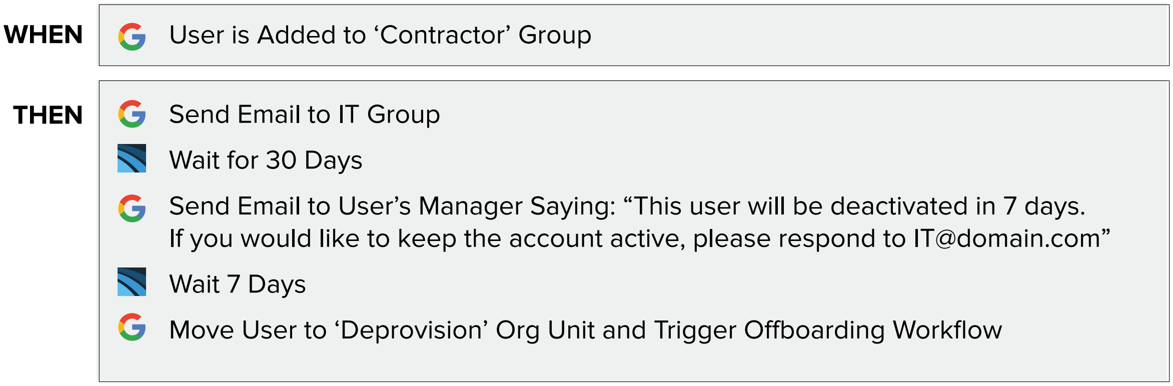
What makes this policy especially valuable is that it can be very easy for end users to add external members to groups on their own. IT does not need to be involved at all. Depending on your SaaS app configuration, in some cases end users can create their own groups, add external addresses to groups, and allow anyone outside the domain to join groups. In G Suite, even if this option is disabled later, any external addresses already added will remain in those groups.

If IT doesn't know about these external members, then there's no way to control their access—meaning corporate data is not secured.

What does a policy for groups with external members look like?

A robust policy will notify IT when an external user is added to a particular group in a SaaS app. The granularity may vary depending on an organization's needs. The policy will then revoke the external user's group membership (in some cases, after waiting a certain amount of days) and offboard them if necessary.

Here's an example:



WHEN User is Added to 'Contractor' Group

THEN
- Send Email to IT Group
- Wait for 30 Days
- Send Email to User's Manager Saying: "This user will be deactivated in 7 days. If you would like to keep the account active, please respond to IT@domain.com"
- Wait 7 Days
- Move User to 'Deprovision' Org Unit and Trigger Offboarding Workflow

Figure 17

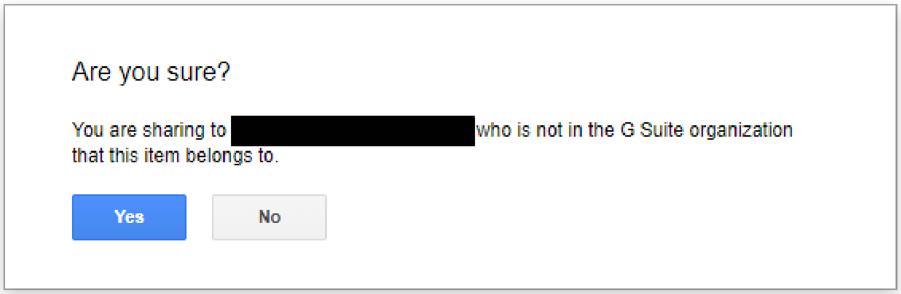
EXTERNAL ACCESS POLICY #2

Files shared externally

What is an externally shared file?

An externally shared file is one that is shared with someone who does not belong to your organization.

In G Suite, for example, users have the ability to share files with people outside their domain. When they do so, they will see this message appear:

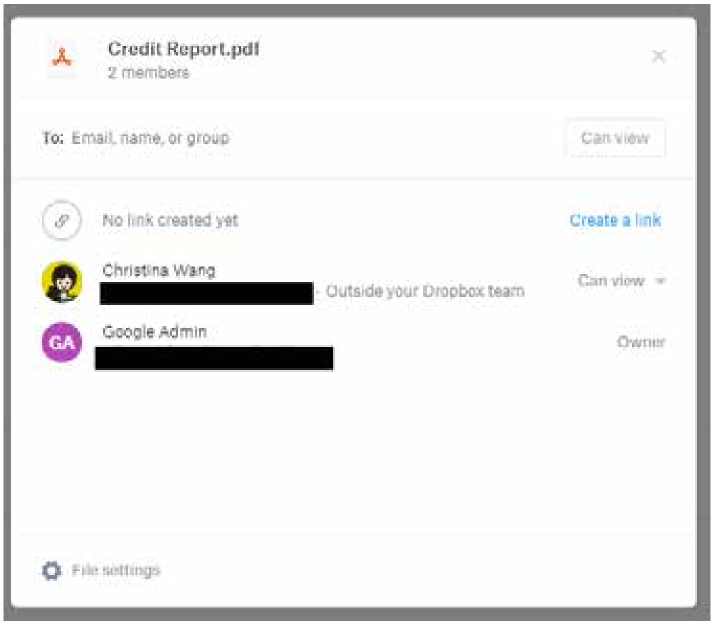


Are you sure?

You are sharing to [redacted] who is not in the G Suite organization that this item belongs to.

Figure 18

In Dropbox, users can do the same thing. The application will indicate who outside your domain a file is shared with:



Credit Report.pdf
2 members

To: Email, name, or group — Can view

No link created yet — Create a link

Christina Wang
[redacted] · Outside your Dropbox team — Can view

Google Admin
[redacted] — Owner

Figure 19

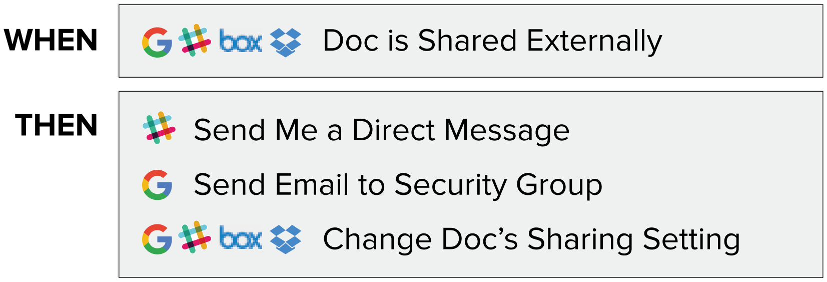
What's the business value of an externally shared file policy?

When corporate data leaves the perimeter of your organization, IT faces heightened risk. To safeguard data, IT needs to be aware if files are being shared externally (and if so, if the domains are suspicious). For example, if files are being shared with competitors, then this is a huge security threat. If confidential data and IP are being shared, then it could potentially result in loss of revenue and competitive advantage.

External sharing also magnifies risk because if that person is compromised, then so are your corporate files. This exact scenario happened to a BetterCloud customer. One of the customer's employees was sharing work files with his personal email account. Then one day his personal account was hacked, meaning all of his company's corporate data was at risk as well.

What does an externally shared file policy look like?

Here's an example:



WHEN

Doc is Shared Externally

THEN

Send Me a Direct Message

Send Email to Security Group

Change Doc's Sharing Setting

Figure 20

REAL-LIFE BETTERCLOUD CASE STUDY

(For privacy purposes, we have removed all names from this customer story.)

How a large retailer uses policies to automatically remove external collaborators who no longer need file access

Another BetterCloud customer, a retailer in the UK, runs a monthly policy to examine documents that haven't been updated in the last 90 days. The "last updated" criteria is a common one to use; prolonged inactivity usually signals that the project has been completed or is no longer a priority. The policy then automatically removes all external collaborators who aren't on a whitelist, ensuring that external users do not retain access for longer than necessary (or indefinitely).

CATEGORY #6

Groups Management

Why you should care about groups management

In July 2017, a data breach made news headlines. Surprisingly, the breach wasn't caused by hackers, ransomware, or insider threats.

Instead, the headline read: "Hundreds of Companies Expose PII, Private Emails Through Google Groups Error."

That's right. A simple Groups misconfiguration led to serious data exposure for firms like IBM's Weather Company, Fusion Media Group (the parent firm of companies including Gizmodo, The Onion, and Lifehacker), as well as helpdesk support service provider Freshworks.

So how did this happen? In G Suite, customers control the privacy settings on their groups. These Groups were all set to the "Public on the internet" sharing setting, rather than "Private." This simple oversight meant that messages sent between members (and any sensitive data contained within) were publicly exposed and viewable by anyone on the internet.

Researchers found that "email addresses, email content, PII including employee salary compensation, sales pipeline data, customer passwords, names, and home addresses at hundreds of companies were left online for the world to see."

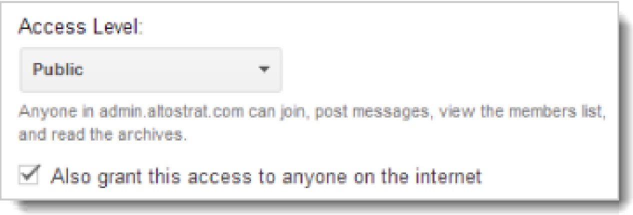
Groups settings are not always controlled by administrators. In some applications, groups can be managed by an end user or team admin, who have access to change the group's settings. It is very easy for end users with group management roles to change these settings without a full understanding of its implications. This is all the more reason to implement policies that control, manage, and secure groups. There are far too many admin settings to manually ensure they are always properly configured. Larger organizations with multiple admins are particularly vulnerable to an uncaught admin error.

GROUPS MANAGEMENT POLICY #1

Inappropriate group exposure (public groups)

What is a public group?

In Google, groups can have varying access levels. One of the broadest options is "Public," meaning that anyone in the domain can join, post messages, view the members list, and read the archives. However, there is also the option to make the group "Public on the internet," which grants the same access to anyone outside your domain. This means anyone on the internet can join the group, send messages, and view the discussion archives.



Access Level:

Public

Anyone in admin.altostrat.com can join, post messages, view the members list, and read the archives.

☑ Also grant this access to anyone on the internet

Figure 21

What's the business value of a public group policy?

If groups are publicly exposed, it can have devastating effects for businesses.

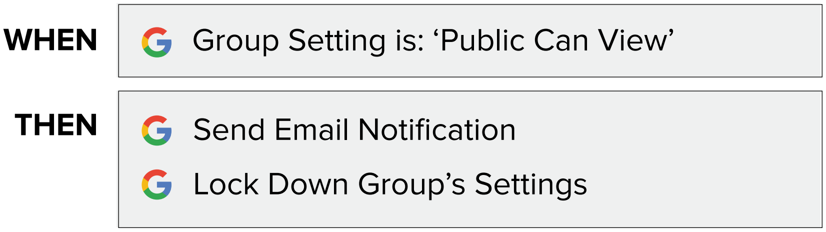
"Corporate accounts could be hijacked, information can be mined for phishing attacks, and sensitive conversations not suitable for the public sphere may be leaked," writes ZDNet.

If companies implement public group policies, incidents like the PII leak caused by the Google Groups error could have been avoided. Without policies, organizations have no way of knowing if their groups have dangerous visibility settings, which puts their corporate data at great risk.

What does a public group policy look like?

A public group policy will detect if any of your organization's groups are publicly exposed. There are several potentially dangerous public exposure settings for groups in G Suite: "Anyone Can Join," "Anyone Can Post," "Anyone Can View," and "Allow External Members." When any of these are detected, the policy will take action to remediate it.

Here's an example:



WHEN Group Setting is: 'Public Can View'

THEN Send Email Notification

Lock Down Group's Settings

Figure 22

REAL-LIFE BETTERCLOUD CASE STUDY

(For privacy purposes, we have removed all names from this customer story.)

How a government agency accidentally set their groups to “Anyone Can Join” with GAM

An IT admin at a state government agency was using GAM to manage his domain. However, one day he realized the script had broken and as a result, his Google Groups had been set to “Anyone Can Join.” Using BetterCloud, he was able to revert the settings for all of his Groups and set them to a more private setting.

GROUPS MANAGEMENT POLICY #2

Correct group membership

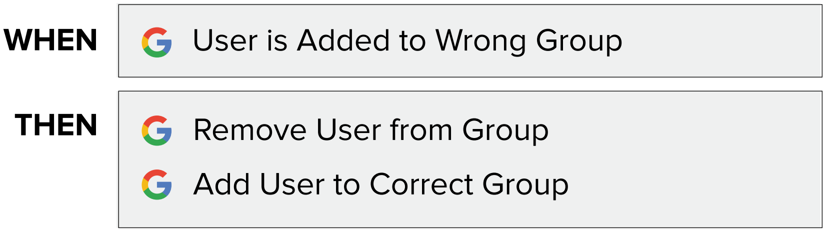
What is group membership?

Groups provide a way for users to communicate with groups of people they often contact or collaborate with. In G Suite, you can send an email to everyone in a group with one address, invite a group to an event, or share documents with a group. Organizations often create groups by department, office location, ad-hoc projects or events, common interests, and so forth.

What’s the business value of a correct group membership policy?

This policy helps lock down corporate data. For example, if a salesperson is wrongly placed in a finance group, they would have access to confidential financial data that they shouldn’t be privy to. Correct group membership also enables productivity. If that salesperson isn’t in the sales group like he should be, then he’s missing out on critical updates and information from his team.

What does a correct group membership policy look like?



WHEN
User is Added to Wrong Group

THEN
Remove User from Group
Add User to Correct Group

Figure 23

This policy will detect if a user belongs to the wrong group (for example, if a user on the marketing team is suddenly added to a finance group). Then the policy will take remedial action, such as removing them from the erroneous group and placing them in the correct one. *Figure 23* is an example of a correct group membership policy.

CATEGORY #7

Licenses

Why you should care about licenses

Without SaaS licenses, users cannot do their jobs. Therefore, it's imperative for the business that licenses are assigned correctly so that people can remain productive. Then there's the issue of unused licenses. Research shows that a 200-person startup will lose $236,000 a year on excess licenses and usage. How many licenses do you have sitting in a suspended state? When is the last time someone used Applications X, Y, and Z? Are all your licenses being actively used?

IT teams run into the same problems as they do with super admin access. They assign licenses to new hires, but usage is not tracked or revoked appropriately down the line. IT has no idea if users truly need these licenses. Whereas excessive super admin access is a security issue, excessive licenses are more of a cost issue.

These two policies below will help reduce license costs and enable productivity for users.

LICENSES POLICY #1

Inactive users

What are inactive users?

Inactive users are users who have a SaaS app license but are not actively using it. Perhaps they no longer need the app to do their job and they haven't used it for months, or perhaps they've left the company and their access was not properly "turned off."

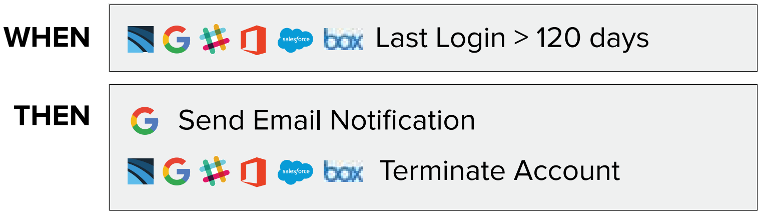
What's the business value of an inactive user policy?

Inactive users create wasteful spending. Even though these licenses are not being used, often the organization still gets charged for them. SaaS app licenses are usually billed per user and can be quite expensive.

An inactive user policy eliminates needless costs. It ensures that unused licenses are tracked and eliminated (or recycled), resulting in significant cost savings for the business. If dozens of employees are inactive, and they each use multiple SaaS apps, this can add up to thousands of dollars.

What does an inactive user policy look like?

A good policy will look at various criteria that indicate who your inactive users are. Criteria can be the last time someone logged in, the last time a document was created, etc. Then the policy will remediate it by terminating the account and freeing up the license. *Figure 24* is an example of an inactive user policy.



WHEN Last Login > 120 days

THEN Send Email Notification

Terminate Account

Figure 24

REAL-LIFE BETTERCLOUD CASE STUDY

(For privacy purposes, we have removed all names from this customer story.)

How a media company saved $100,000 in unused licenses

Fullscreen Media has nearly 1,000 employees and more than 206 SaaS applications in use. When their IT team dug deep, they discovered excessive amounts of misallocated licenses. “It was outrageous,” says Shira Harrison, IT Director. Now, BetterCloud has enabled Fullscreen to be much more deliberate about license allocation. There are no more wasted expenses on unneeded licenses. Harrison estimates that the company will save at least $100,000 in less than a year as a result of adopting BetterCloud.

LICENSES POLICY #2

Assigning correct licenses based on department

What are correct licenses based on department?

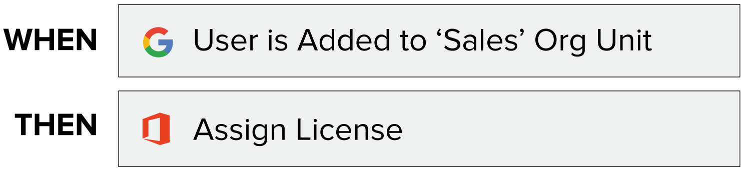
Different departments require licenses for different SaaS apps. For example, sales may need an app license that finance does not.

What’s the business value of a correct license assignment policy?

Manually assigning licenses across SaaS apps in native admin consoles is a time-consuming process for IT. If you know that finance users will always need a specific SaaS license, then you can set up a policy that assigns it to them. A license assignment policy helps save time, reduce error, and improve productivity (for both IT and the user).

What does a license assignment policy look like?

Based on certain conditions (e.g., a user’s department), the policy will assign (or remove) a specific license.



WHEN User is Added to ‘Sales’ Org Unit

THEN Assign License

Figure 25

CATEGORY #8

Maintenance

Why you should care about maintenance

This category of policies may not seem as dire as the previous ones. However, it's important enough from a day-to-day management perspective to include on our "must have" list.

Gardens need to be pruned every now and then. The same goes for SaaS environments. Users join and leave organizations; groups become empty and abandoned; blank documents clutter up folders. This can hinder productivity, cause confusion, and create a poor user experience.

SaaS environments need basic maintenance—some tidying up—periodically. These two policies below will help keep your SaaS environment organized and easy to use.

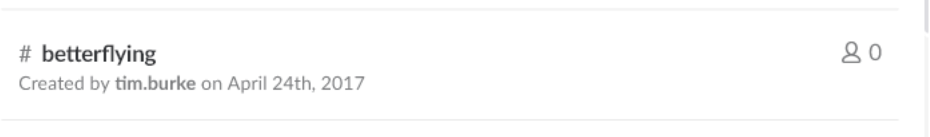
MAINTENANCE POLICY #1

Cleaning up empty public Slack channels

What's an empty public Slack channel?

Sometimes Slack channels are created on a one-off, ad-hoc basis: perhaps for a temporary event, or to discuss an emergency blocker.

When these channels are no longer needed, users will leave them. The channel stays open, but they have zero members in them. This is what an empty Slack channel looks like:



betterflying

Created by tim.burke on April 24th, 2017

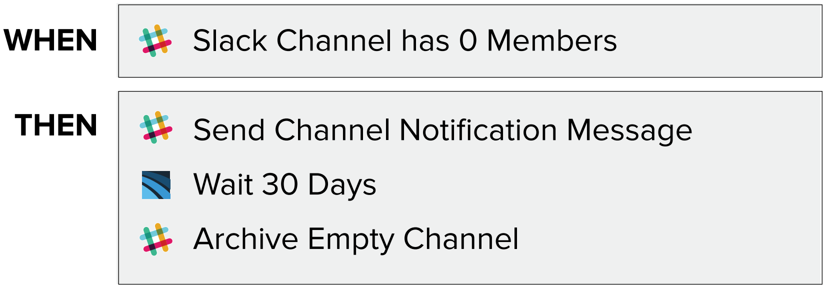
Figure 26

What's the business value of an empty channel policy?

Empty Slack channels can cause frustration or confusion for end users, ultimately hindering their productivity and preventing them from doing their jobs effectively. For IT, this represents another blind spot. IT has no way of easily seeing how many empty public channels there are in their Slack instance, and they have no way of managing them. By implementing an empty channel policy, IT can keep their Slack instance clean and uncluttered, enabling users to be more productive.

What does an empty Slack channel policy look like?

An empty Slack channel policy detects when a channel is empty and then remediates it (for example, archiving the empty channel).



WHEN
- Slack Channel has 0 Members

THEN
- Send Channel Notification Message
- Wait 30 Days
- Archive Empty Channel

Figure 27

REAL-LIFE BETTERCLOUD CASE STUDY

(For privacy purposes, we have removed all names from this customer story.)

How a K-12 school cleans up a “graveyard of empty Slack channels”

(For privacy purposes, we have removed all names from this customer story.)

Here’s how one BetterCloud customer (a K-12 school) uses BetterCloud to clean up what their IT manager calls “a graveyard of empty Slack channels.”

A side effect of having a “particularly Slack-happy company” is that empty or redundant channels accumulate over time, according to the IT manager. Unfortunately for new hires, this creates a jarring onboarding experience.

“When new employees join, they have this extremely daunting list of empty Slack channels—many of which may appear useful based on the name but actually have no users in them,” he says.

For example, some departments create temporary, need-based channels, which then become unused. These empty ad-hoc channels result in a channel graveyard.

With BetterCloud, the IT manager is able to easily remove all empty public Slack channels with one click, and do this on an ongoing basis through an automated policy. This basic housekeeping task creates a smoother onboarding experience and declutters the application for everyone.

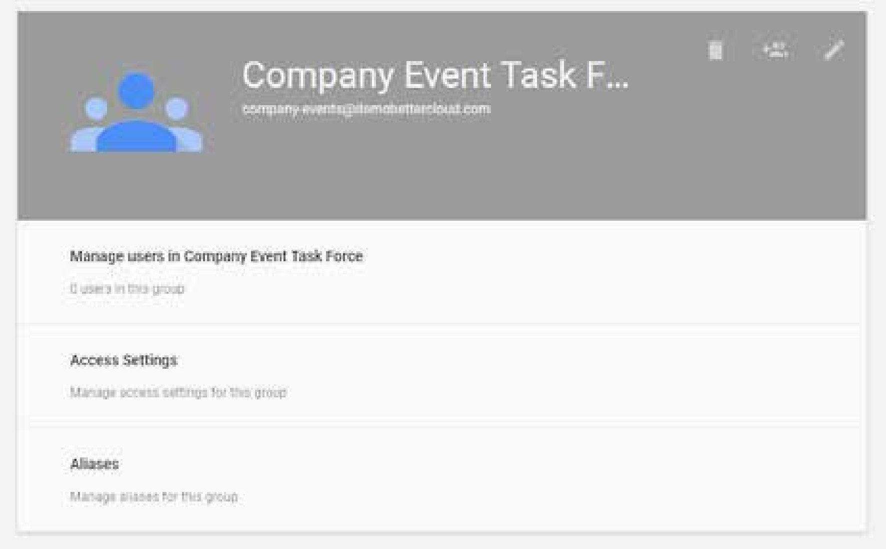
MAINTENANCE POLICY #2

Cleaning up empty public Google or Dropbox Groups

What are empty public Google or Dropbox groups?

Similar to empty Slack channels, public Google and Dropbox groups can also become empty. They are not automatically archived or deleted, however. They stay open.

Here's an example of an empty Google group:



Company Event Task F...

company-events@demobettercloud.com

Manage users in Company Event Task Force

0 users in this group

Access Settings

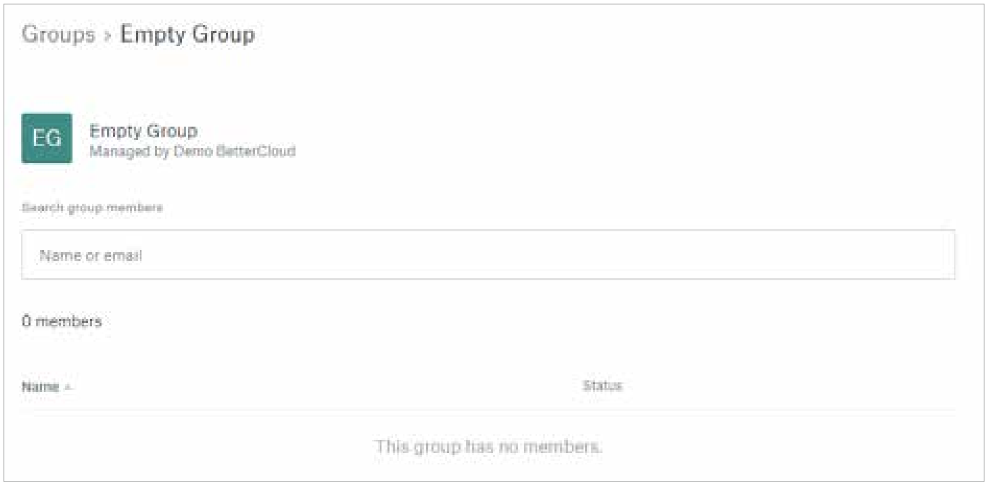
Manage access settings for this group

Aliases

Manage aliases for this group

Figure 28

And an example of an empty Dropbox group:



Groups › Empty Group

EG

Empty Group

Managed by Demo BetterCloud

Search group members

Name or email

0 members

Name ▲ Status

This group has no members.

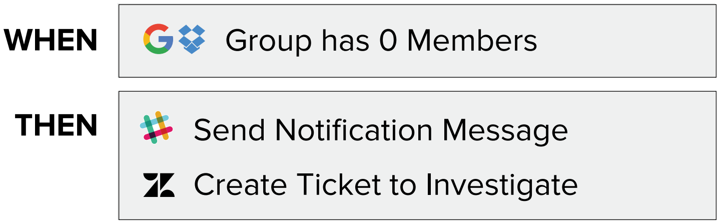
Figure 29

What's the business value of an empty group policy?

Removing empty groups improves productivity for the business. Imagine a user who thinks he's emailing the right group of people and is awaiting a response, but in reality, the group is empty. This results in wasted time, loss of productivity, and frustration and confusion for the user. This policy ensures that users are emailing actively used groups and using their time productively at work.

What does an empty groups policy look like?

Because IT has no easy way to see how many empty public Google and Dropbox groups there are, this policy would identify empty groups and then remediate it. See *Figure 30* for an example.



WHEN Group has 0 Members

THEN Send Notification Message

Create Ticket to Investigate

Figure 30

REAL-LIFE BETTERCLOUD CASE STUDY

(For privacy purposes, we have removed all names from this customer story.)

How a retailer saves $133,000 per month by reducing administrative tasks

A BetterCloud customer, a large retailer in the UK with thousands of employees, has been implementing general maintenance policies to reduce friction.

"There are tremendous savings attributed to having a clean Google domain where users don't need to open tickets for tedious, administrative tasks," said the IT manager.

"By reducing mistakes and simplifying processes, the general health of our G Suite domain increases."

These tasks aren't just limited to cleaning up empty Google Groups. They also include maintenance and "clean up" steps like clearing resource calendars of meetings, updating document settings, and removing deprovisioned users from groups.

They've calculated that they've saved £98,000 ($133,000 USD) per month by cutting down on tickets and calls for administrative clean-up tasks.

Sample policy "checklists" for various scenarios

We recommend that you implement all eight categories of policies we discussed throughout this whitepaper. However, we want to highlight a few particularly important policies for companies in varying scenarios. Of course, this is not an exhaustive list, but it will get you thinking about which policies are most critical for your organization's needs.

A company preparing to go public/IPO:

- **Sensitive data exposure policies** will be critical for data protection. When companies go public, the pressure on IT increases. IT must be able to face the scrutiny of auditors and ensure their organization can meet the data security requirements of a public company. SOX compliance also becomes a consideration for publicly traded companies and companies preparing to go public.
- **Admin permission policies** will be important to illustrate that users have only the least amount of privileges they need to do their jobs and nothing more, thus minimizing the risk of a security threat.
- **Groups management** and **external access policies** will help lock down sensitive data and reduce the risk of unauthorized access. Any headlines about data breaches could seriously jeopardize an IPO.

A company that needs to be compliant with GDPR, HIPAA, or other regulations:

- **Sensitive data exposure policies** are critical to implement. Under GDPR, data breaches must be reported within 72 hours. Therefore, you need to know immediately if and when sensitive data is exposed. Consequences for GDPR non-compliance include hefty fines, scrutiny by local supervisory authorities, and negative PR.
- **External access policies** are important. GDPR exists to protect data, so you need to know who has access to your data, especially if they don't belong to your organization.
- **Insider threat policies** are also important. You need to make sure data is not being exposed (either maliciously or accidentally). To avoid hefty fines, it's prudent to implement an insider threat policy to reduce the chances of unauthorized access.

A rapidly growing startup:

- **Onboarding policies** are critical for a company that's experiencing explosive growth. Often these companies face scaling challenges, particularly in terms of streamlining IT and ULM processes, because they must operate lean. Onboarding policies will help the scaling process by giving new hires the right access and letting them hit the ground running on day one.

- **Groups policies** may also be valuable. In the early days of a startup, there may be no (or very few) formal IT personnel. In some cases, end users take on some of the IT work and are granted admin privileges. They may not be aware of all the different group privacy settings and what the implications are, so these policies will ensure that sensitive data is locked down.
- **Admin permission policies** will also be critical. At companies that are growing very quickly, there simply isn't enough time to regulate who gets admin access and when that should be taken away. To move quickly and keep the business running, admin access is given out liberally, which can create serious security risks.

A company that recently underwent a merger or acquisition:

- **ULM policies** are important. When two companies are merged (or one is acquired), there are various lifecycle tasks to take care of: email signatures need to be updated with new information, user profiles must be updated, etc.
- **Admin permissions policies** will also be valuable. Two companies may have drastically different policies on admin privileges. Perhaps Company A is lax about them and everyone has elevated privileges, and Company B is the opposite. This can create confusion after a merger or acquisition. It's important to implement a policy that enforces the same standards across the entire company.
- **Groups policies** will be important as well. Groups may be restructured and shuffled after a merger or acquisition, so it's important to make sure everyone is in the right groups and receiving the information they need.

A company with frequent turnover or seasonality

- **Onboarding and offboarding policies** will be important for companies that employ extra part-time or temporary employees to help during seasonal fluctuations. This means spikes in on- and offboarding at various points throughout the year. Due to seasonality, turnover tends to be high. Employees can leave with little to no notice. Communication with HR about departing employees can be minimal. Departing employees can fall through the cracks, meaning steps are often left out, forgotten, or the offboarding process is overlooked entirely. Policies ensure that these on- and offboarding processes are executed thoroughly and completely.
- **License policies** will also be important for cost savings. With so much turnover, it's very easy to lose track of inactive users and rack up fees for unused licenses.

A company that owns multiple domains or properties

- **ULM policies** will be important here. Users often move laterally across domains or properties while they are at the company, so these policies will ensure a smooth transition.
- **Groups policies** will also be key. The average enterprise G Suite domain has over 1,500 groups. With multiple domains, the web of sprawling groups can quickly become unmanageable.
- **License policies** will also be valuable. It's difficult to keep track of inactive users across multiple domains or properties, so these policies will reduce costs and ensure all unused licenses are terminated or recycled.

A large company with multiple offices

- **Groups policies** will be important for companies that have offices spread across different locations. Because the average enterprise has over 1,500 groups, it can be a formidable and time-consuming task to manually manage group settings.
- **ULM policies** will also be important. Employees may move between office locations, and these policies will ensure they have access to the correct data.
- **License policies** are valuable as well. With hundreds (perhaps thousands) of users in offices around the country or world, it is nearly impossible for IT to know when someone isn't using their SaaS licenses. License policies will identify inactive users and cut down on excess licenses, reducing costs.

If you're new to BetterCloud and would like to learn more about implementing policies, please visit https://www.bettercloud.com/demo-policywp/. If you're a current BetterCloud customer, please email success@bettercloud.com.

Conclusion

IT is plagued by multiple blind spots in SaaS environments today. They have no visibility into critical areas, like publicly shared files, admin permissions, and underutilized SaaS licenses. This creates wasteful spending, security risks, and compliance issues.

By creating standard processes, policies can cut down your IT tickets by 90%, lock down files immediately when they're shared incorrectly, and automate routine processes like offboarding. Implementing policies will lend critical visibility into the major blind spots IT is facing today, empowering you to manage and secure your SaaS environment effectively.

If you're new to BetterCloud and would like to learn more about implementing policies, please visit https://www.bettercloud.com/demo-policywp/. If you're a current BetterCloud customer, please email success@bettercloud.com.

About BetterCloud

BetterCloud empowers IT to define, remediate, and enforce management and security policies across SaaS applications. Take control of your SaaS environment by setting up custom listeners, auditing activity, quickly taking action, and fully automating policy remediation.