



 BetterCloud EBOOK

Simplifying Compliance: An Actionable Guide for IT

Effective compliance in a SaaS-based world has a few key tasks. **Successfully complying is about having documented processes for auditors and regulators.**

For SaaS security compliance, at the very least, you need to define processes for:

- Enforcing access privileges
- Protecting your organization's sensitive data
- Retaining data
- Reporting and audit logs to prove compliance

Additionally, successful compliance includes one more critical component: *proving that you comply with those documented processes.*

But the big question remains: How does IT simplify SaaS security compliance?

That answer is automated alerting and workflows.

So here we build on [Conquering Compliance: A Guide for Security and Data Privacy](#). While that guide describes what IT needs to know about compliance programs, **this eBook details essential processes and steps around SaaS security compliance, and the role BetterCloud's workflows play in easing them.**


SaaS security policies start with compliance requirements

In data privacy and security compliance, budgets are center stage.

Organizations can't choose which laws they follow, but they can choose the standards (and levels of those standards) they'll meet. And by "choose," we mean that compliance decisions consider the trade-offs between risk, competitive needs, and budgets to pay for audits. In a nutshell, organizations generally create compliance strategies based on how much they can afford.

After the more strategic compliance decisions are made, IT and compliance teams define data privacy and data security requirements. They then develop security policies—which ultimately drives the security and data privacy processes that IT follows.

Thus, for IT, it all starts with that documented security policy.



Thus, for IT, it all starts with that documented security policy.

Security and data privacy policies for SaaS should be granular

In the world of SaaS, that documented security policy should be a comprehensive, granular view of all users. It defines user types according to roles, departments, or titles. In addition, it also documents the permissions for apps and data each user type can access.

Your security policy also needs rules and policies for super admins, too. For example, there should be policies that limit super admin account activities in the domain.

Regardless of whether it pertains to a super admin role, your security policy should follow the principle of least privilege. It's a security design principle for restricting access rights and program privileges to the lowest degree possible to do the job.

However, access requirements change, so least privilege advocates use of separation of privileges (to place controls on super admins) as well as time-sensitive privileges (for those times when users may temporarily need higher access levels). These best practices reduce the attack surface, thereby increasing security—and successful compliance.

In addition to documenting app permissions, your security policy should define exactly what confidential and personal information is in your organization. Although each organization has different definitions of what that is, you can start with some widely accepted examples, like:

- **Personal identifying information (PII)**
- **Credit card numbers**
- **Social Security numbers**
- **Passport numbers**
- **Passwords**
- **AWS encryption keys**
- **Self-harm content (for EDUs)**

To categorize your data, assign classifications like “proprietary,” “confidential,” or “public.” You could also use watermarks like “for internal uses only.” The goal is to make sure data is accessible to only appropriate individuals, as well as prioritize budget resources so you’re protecting the data that is truly important.

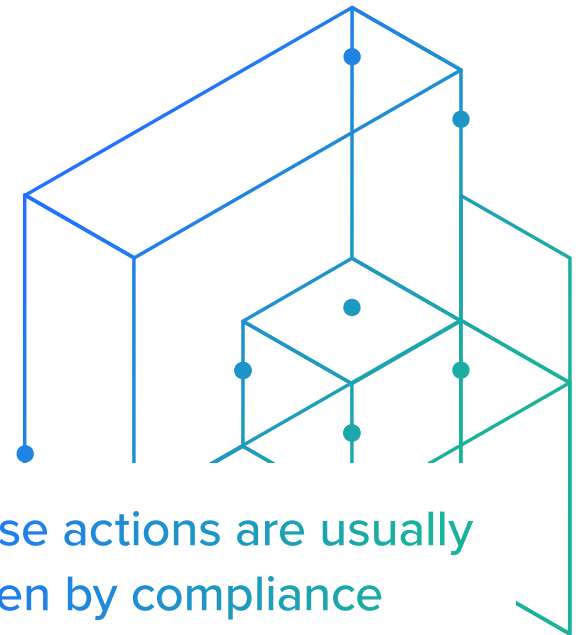
Once your policy [defines users and categorizes data](#), it’s time to define your IT processes. You may also want to define actions for your file sharing policies.

Some examples of processes you might define are:

- **Use a single sign-on tool (SSO) or identity provider (IdP) to enforce VPN access**
- **Use an HR tool to begin an offboarding workflow**
- **Use a SaaS Management Platform (SMP) to manage file sharing settings**

These actions are usually driven by compliance requirements outlined by the laws and standards your organization must follow. This is exactly where compliance and IT intersect.

Up next, we explore the actions and processes in SaaS environments that help companies successfully achieve compliance goals.



These actions are usually driven by compliance requirements outlined by the laws and standards your organization must follow. This is exactly where compliance and IT intersect.

4 essential security and data privacy processes in a SaaS-powered workplace

Every SaaSops professional—both established and aspiring—operates some fundamental SaaS-related security compliance processes. Here we look at four:

- **Enforcing access privileges**
- **Protecting your organization’s sensitive data**
- **Retaining data**
- **Reporting and auditing**

Fortunately, these four lend themselves well to automated alerts and workflows that dramatically simplify SaaS operations and compliance.

Enforcing access privileges

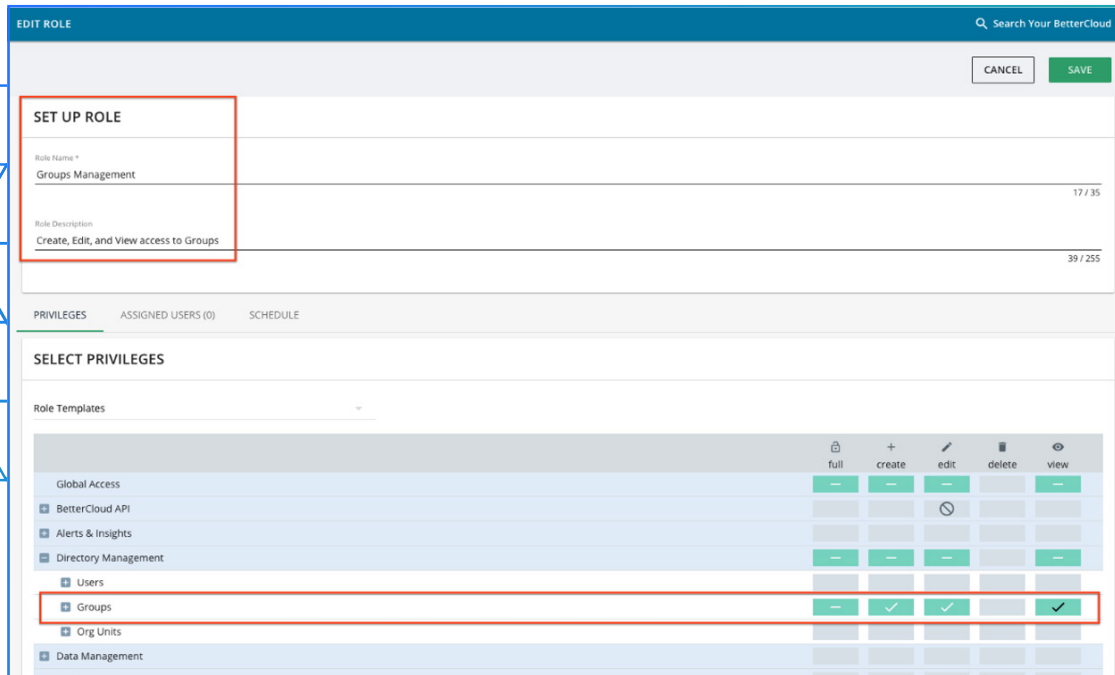
To enforce a granular security policy, which itself is important to your compliance program, you need to set roles and permissions for access. You’ll need to do this for both users and super admins, too.

If you’re concerned about successful compliance, you’re very likely following least privilege.

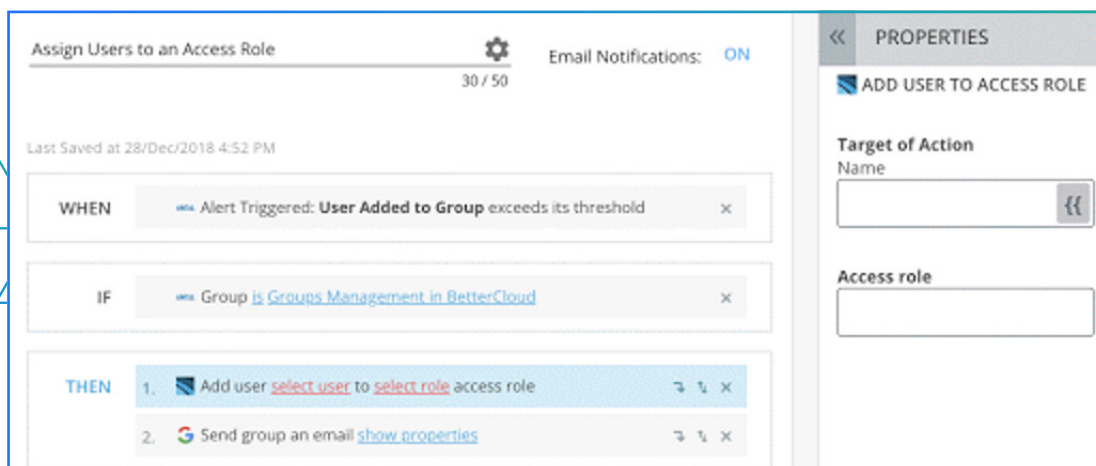
SaaSops is a practice referring to how software-as-a-service (SaaS) applications are discovered, managed, and secured through centralized and automated operations (Ops), resulting in reduced friction, improved collaboration, and better employee experience.

How BetterCloud can help

BetterCloud simplifies SaaS security compliance in how it sets up and manages access privileges. You start with setting up user roles, and granular permissions can be added or elevated for any SaaS app using a centralized view of all users.



For example, you can automatically add users to access roles:

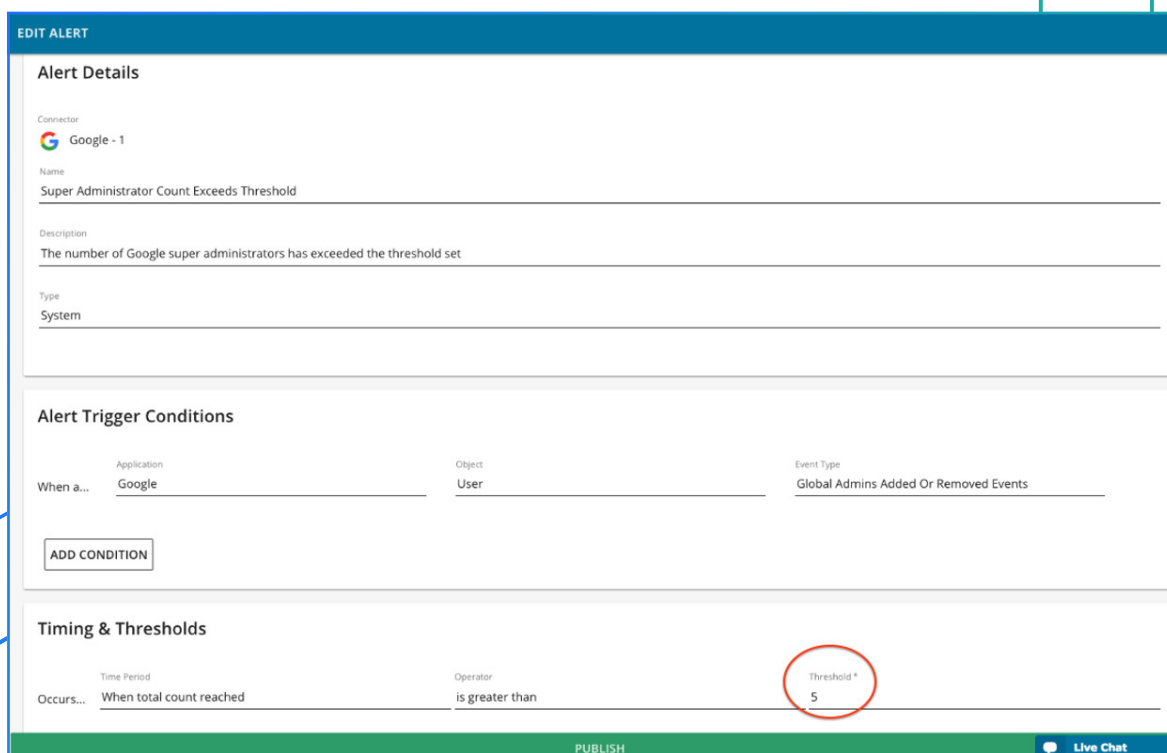
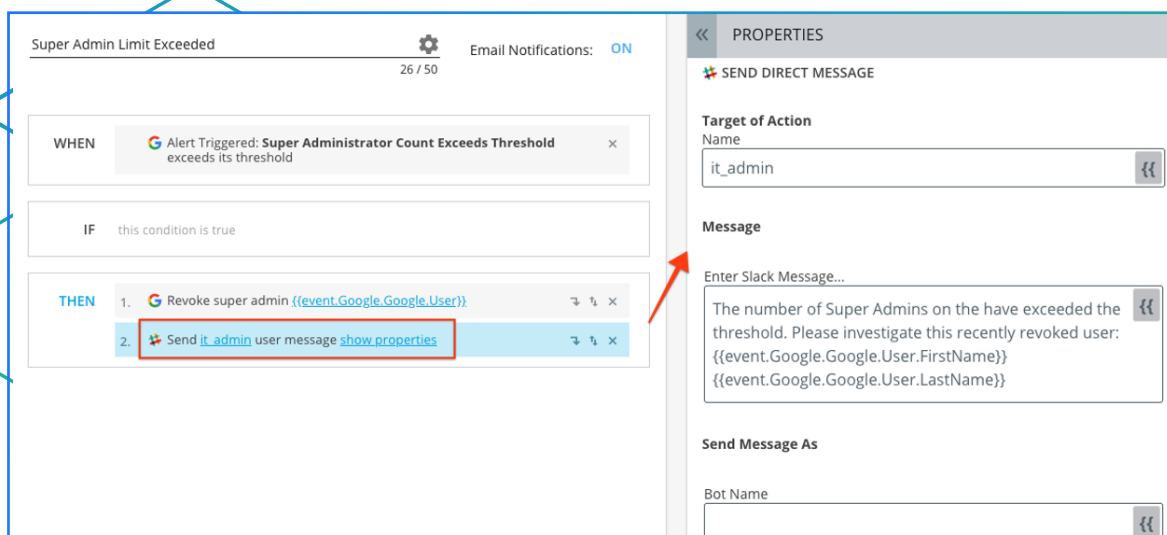


You can also easily automate access privileges. For instance, a BetterCloud workflow can automate the process of [revoking super admin access](#) from users when you exceed your set limit.

Let's take an example. Let's say your security policy only allows a maximum of four super admins per app. If someone gives super admin access to a fifth person, the system alerts you.

When that alert occurs, it triggers a workflow that automatically cuts super admin access. Once the privileges are revoked, the primary IT admin is notified via Slack. This way, you always adhere to your security policy and stay in compliance. And we'll touch more on this later, but BetterCloud reports and audits prove it.

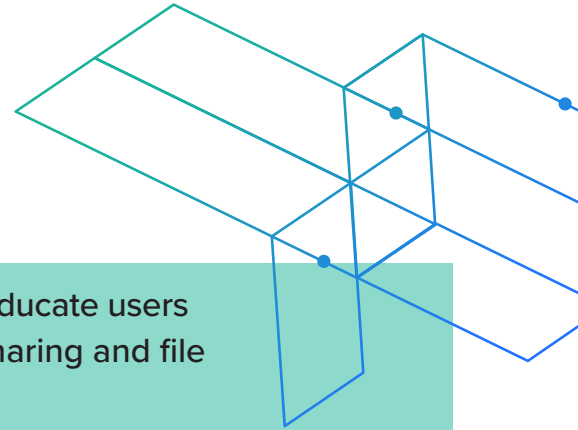
Here's what that workflow looks like in BetterCloud:

Protecting your organization's sensitive data

To identify and protect your organization's data according to your security policy, you need two types of processes. First and foremost, you need processes for protecting sensitive data in your SaaS apps. Second, you also need a process for tracking all the SaaS applications that run on your network, so you can make sure all SaaS app data policies are in accordance with your compliance program.

3 best practices to help safeguard your SaaS apps' sensitive data



1. Train users to increase security awareness. Continually educate users about your organization's security policies, including data sharing and file sharing settings.

2. Prevent unauthorized sharing of sensitive data. Activate any global settings in SaaS apps around data protection (cloud productivity suites have them, but not all SaaS tools do).

3. Understand who uses and transmits sensitive data, and monitor it for unauthorized use. Audit app logs to look for any activity or files that violate your defined policies.

How BetterCloud can help

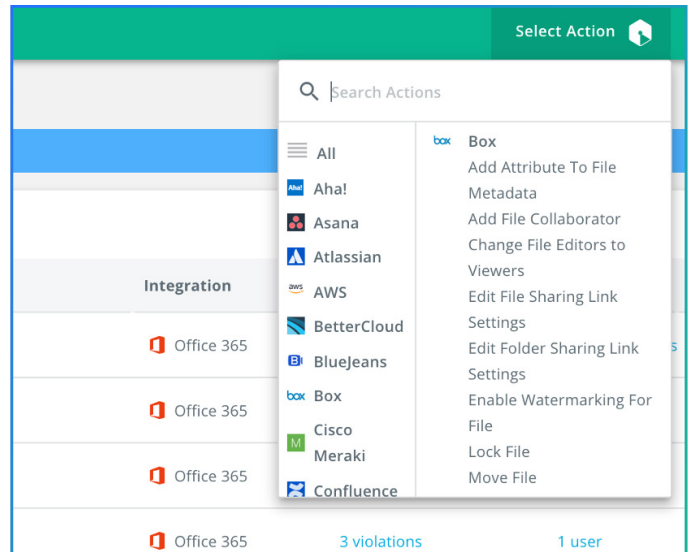
In BetterCloud, you can protect your sensitive data using alerts and workflows. The process looks like this:

STEP 1:

Use the Sensitive Data Scan Alert template. Make sure it's set up in accordance with your security policy, paying special attention to:

- A** Files shared publicly
- B** Files with public sharing links
- C** Files shared externally
- D** Files shared with domain with link
- E** Files shared with domain

If your company has custom phrases that are considered proprietary, you can use watermarks, custom regular expressions, and keyword search to enforce data protection policies.



STEP 2:

Scan content to audit files that violate your defined security policies. Run an initial baseline.

1/2: Select Files to Scan

Permissions

Public
 External
 Internal

Integrations **File Owner** **Shared With**

FILE SUPPORT

- ✓ File types: PDF, CSV, DOC, DOCX, PPT, PPTX, XLS, XLSX, TXT, Google files (Docs, Sheets, Presentations, Drawings)
- ✓ File size: Less than 50MB, extracted text less than 500kb
- ✗ O365 is not currently supported, but please keep checking as we continue to expand our solutions.

147 FILES SELECTED

⚠ SCANS OVER 500,000 MAY TAKE SIGNIFICANT TIME TO COMPLETE

Cancel Next

2/2: Select Scan Criteria

You may select from a number of categorized scan templates broken out by geographical regions. Add additional scan criteria to search for multiple violations at once.

Scan Name

Match files that contain the following information.

Regional Format:
 Category:
 Data Type:
+

147 FILES SELECTED

⚠ SCANS OVER 500,000 MAY TAKE SIGNIFICANT TIME TO COMPLETE

Back Begin Scan

STEP 3: Review the severity of any violations.

25 ITEMS SELECT ACTION Search Your BetterCloud

Content Scanning | Email Address

Details

Severity:	Major	Threshold:	0
Connector:	Google	Count:	30
Triggered:	15/Apr/2019 1:43 PM	Type:	Custom
Description:	Sensitive data found in a file		

	NAME	VIOLATIONS	TRIGGERED
All 25 items on this page have been selected. Select all 30 items			
<input checked="" type="checkbox"/>	*BetterCloud Sales Deck 2019	1 Match	15/Apr/2019 1:38 PM
<input checked="" type="checkbox"/>	Docs Exposed Externally Report #1	20 Matches	12/Apr/2019 9:00 AM
<input checked="" type="checkbox"/>	Inactive User Report #1	20 Matches	12/Apr/2019 9:00 AM
<input checked="" type="checkbox"/>	Untitled #1	20 Matches	12/Apr/2019 9:00 AM
<input checked="" type="checkbox"/>	Getting started	3 Matches	10/Apr/2019 6:19 AM
<input checked="" type="checkbox"/>	Getting started	3 Matches	10/Apr/2019 4:51 AM

STEP 4: Investigate alerts flagging violations according to your security policy instructions, which will be tied to severity.

DOCS EXPOSED EXTERNALLY REPORT #1 - FILE ACTIONS Search Your BetterCloud

Google

Name	Docs Exposed Externally Report #1	Owner	hannah.stern@demobettercloud.com
Path	—	Visibility	External
File-Type	Google Sheets	Size	0
Created Date	11/Sep/2017 4:03 PM	Last Updated Date	06/Feb/2019 10:54 AM

PERMISSIONS

<input type="checkbox"/>	PERMISSION	TYPE	ACCOUNT
<input type="checkbox"/>	Internal, Domain	VIEW	demobettercloud.com
<input type="checkbox"/>	Internal	VIEW	michael.prairo@demobettercloud.com
<input type="checkbox"/>	Internal	VIEW	nicole.ferrara@demobettercloud.com
<input type="checkbox"/>	External	EDIT	caitlin@bettercloud.com

STEP 5:

Based on your investigation, take action according to your policy. It could be one of the following actions like Move File, Remove File Collaborator, Change File Editors to Viewers, Remove All External File Collaborators, Delete File, Unshare File, Revoke Public Sharing Link, and more.

STEP 6:

Identify areas where your organization needs ongoing content scanning alerts, which can greatly improve your security and compliance success.

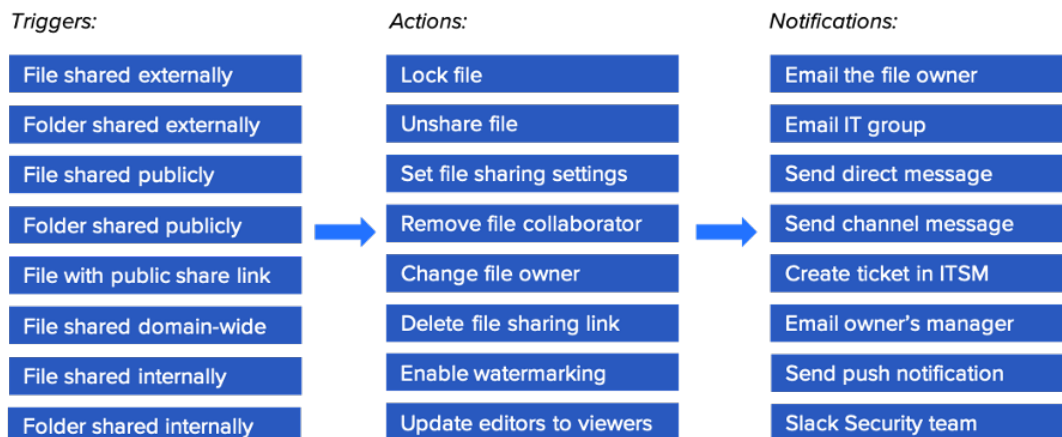
STEP 7:

For those areas, create workflows to stop common or high severity violations, like publicly exposed sensitive files.

Existing solutions:



Desired methods:



This way, if sensitive files are shared publicly, workflows can activate and automatically change sharing settings.

For example, a workflow can send a message to the file owner, informing them of the change and their policy violation. It can help continually train users on your security policy and on best practices, and automatically prevent further violations.

Then another workflow can help monitor and [maintain file security workflows over time](#). Simply add a step to your workflow to email your security team or send a message to the #security Slack channel.

Running automated alerts and workflows are a powerful way to boost your file security and simplify your SaaS security compliance.

Retaining data

When a user departs, compliance requirements generally compel the organization to keep all data for a certain amount of time. Sarbanes-Oxley, for example, requires that publicly traded companies must have and follow a data retention policy. Some industries retain data for 30 or 90 days. In others, like the finance or healthcare industries, it can be much, much longer.

As any SaaSops professional knows, offboarding is a long process—and data retention is a critical part of it.

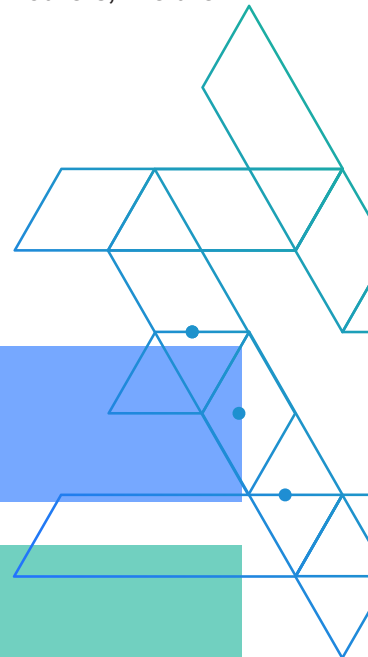
4 best practices for retaining data

1. Determine the hold requirement for the departing user. Look at your security policy to determine the duration of hold for what data and for whom.

2. Archive email. If you're using G Suite, use Google Vault for archiving. If you're using Microsoft O365, you can create and [maintain retention policies](#) or [enable email archiving](#).

3. Hold or transfer departing users' data. Transfer their account including their chat history, files, contacts, and calendar event archives to other users, such as their manager or an archive service account (e.g., backup@mycompany.com).

4. Create a backup. If you're using G Suite, use Google Takeout to do a complete export of the departing user's account. If you're using Microsoft O365, you can back up to a third-party cloud backup provider.



How BetterCloud can help

Data retention is part of [offboarding](#), which has steps that are critical for data security, compliance efforts, and business continuity. When offboarding is done manually, it's long, tedious, and error-prone.

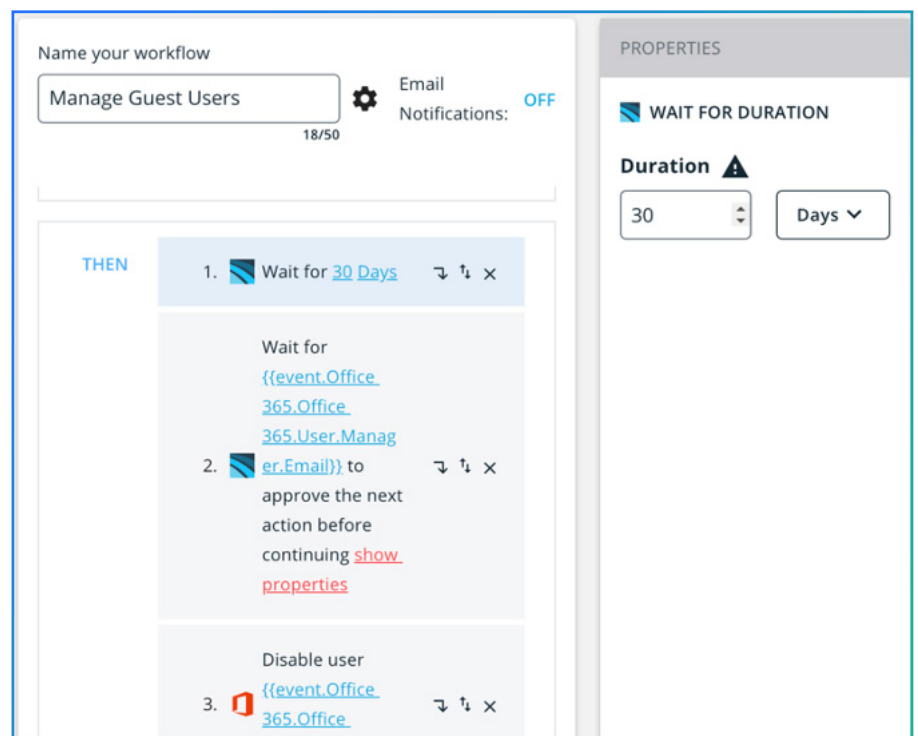
But using BetterCloud automated workflows guarantee that every step—including data retention—happens every time you offboard a user. By automating offboarding, you make sure offboarding is completed quickly and thoroughly to reduce risk and remain compliant.

In addition, robust and customizable [workflow templates](#) make it easy to set up workflows according to your documented processes.

While BetterCloud has the ability to hold or transfer files—which may satisfy your compliance requirements—it does not have the ability to create backups.

If your security policy requires it, you can add a “Send Email” action to your offboarding workflow that sends you a reminder to back up the data. This way, you’ll be sure to download all the user’s data files and store them using Google Takeout, Spanning, Backupify, or whatever backup system you use.

By ensuring adherence to a standard process that includes data retention, automating offboarding goes a long way in simplifying SaaS security compliance.



With BetterCloud, you can automatically build in a waiting period for data retention and compliance purposes.

Reporting and audit logs to prove compliance

As we stated earlier, compliance equals audits. And every auditor needs logs and trails to make sure your company has executed processes according to documented security policies and processes.

Audit logs prove that an organization operates in compliance with the law. And by regularly sharing logs with auditors to comply with standards or regulations, businesses can avoid major fines, penalties, and other market-based consequences like lost customers or tarnished reputations.

To make compliance faster—and frankly, less expensive—your detailed audit logs are priceless. These logs provide an audit trail, proving you actually comply with your documented policies.

Audit logs obviously serve operational purposes as well. They are invaluable to SaaS Ops professionals who need to examine and troubleshoot issues. They give insight into behavior—of what is normal or abnormal, of what worked and what did not.

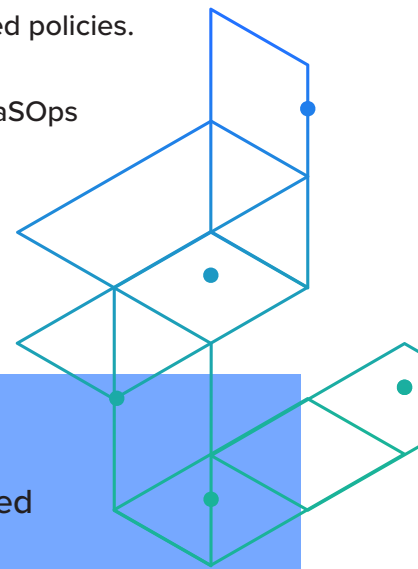
3 best practices for reporting and audit logs

1. Run regular reports according to your security policy. These should include reports on high-business impact tools like Salesforce, your cloud productivity suite, or for certain high-level or highly regulated users as your security policy dictates.

2. Investigate anomalies. Determine if it is an incident and at what severity. If it's at a critical level of severity, act immediately to remediate. If it's less critical, follow up with users to gather more information to determine whether IT needs to act.

3. Keep logs. Logs in each individual SaaS app need to be updated to prove to auditors that actions were taken according to security policies.

Without a SaaS Management Platform or a logging tool, audit trails are found within each SaaS app's audit log—which makes it manual and time consuming to regularly run reports, identify and investigate anomalies, and keep logs that prove compliance.

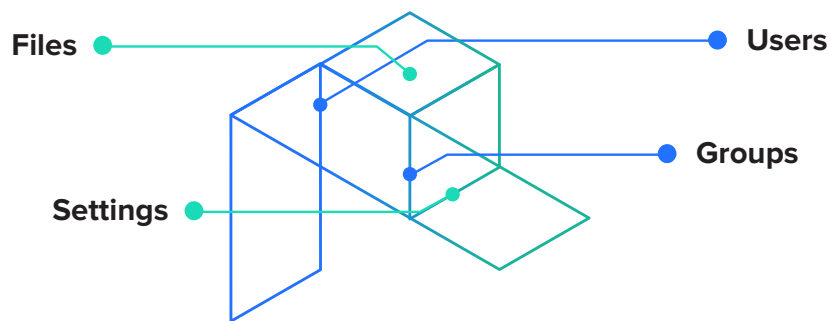


By using a logging tool, you can configure it according to your security policy. Your next step is to regularly review aggregated and automated regular reports. And, of course, you'll need to keep historical records to prove actions were taken.

But if your organization is already mostly SaaS-based, using a logging tool is of questionable value; it's an expensive approach that does not allow IT to change operational settings with those SaaS apps. Instead, IT would have to manually make changes within each SaaS application's admin console. No doubt this could be a slow process that impedes the speed of remediation.

How BetterCloud can help

With a SaaS Management Platform, all actions within your SaaS environment are aggregated into one place. It's one centralized view for real-time SaaS operations across:



A SaaS Management Platform has vast operational value. It actually uses log data to provide operational context on users or files to notify IT. Unlike so many other tools that alert on normal user behavior - and contribute to alert fatigue - a SaaS Management Platform only alerts when an incident is a concern, Together with a workflow engine that can take action across multiple SaaS applications when issues do occur, they are remediated more quickly.

And its byproduct? An audit log that makes it easier and faster to prove compliance.

<input type="checkbox"/>	TIME ↓	ACTOR	INTEGRATION	STATUS
<input type="checkbox"/>	18/Sep/2019 8:49 AM	ron@cloudsandrec.com	-	SUCCESS
<input type="checkbox"/>	18/Sep/2019 8:49 AM	ron@cloudsandrec.com	Google	SUCCESS
<input type="checkbox"/>	18/Sep/2019 8:49 AM	ron@cloudsandrec.com	-	SUCCESS
<input type="checkbox"/>	18/Sep/2019 8:49 AM	ron@cloudsandrec.com	Slack- Main Workspace	SUCCESS
<input type="checkbox"/>	18/Sep/2019 8:49 AM	ron@cloudsandrec.com	-	ERROR
<input type="checkbox"/>	18/Sep/2019 8:49 AM	ron@cloudsandrec.com	Slack- Main Workspace	FAILURE
<input type="checkbox"/>	18/Sep/2019 8:49 AM	ron@cloudsandrec.com	-	ERROR
<input type="checkbox"/>	18/Sep/2019 8:49 AM	ron@cloudsandrec.com	Okta	FAILURE
<input type="checkbox"/>	18/Sep/2019 8:49 AM	ron@cloudsandrec.com	-	SUCCESS

BetterCloud logs are your system of record showing all events, changes, and every action by every user taken in BetterCloud. They also capture how the system responded and whether an action was successfully executed.

An auditor can:

- **View the date and time an action occurred**
- **View the name of the user or entity who took the action**
- **View the integration (app) the action occurred in**
- **View the status of each action**
- **View the exact action taken**
- **View the full text, or records, of actions taken in BetterCloud**
- **Search, sort, filter, and export audit logs**

With BetterCloud, logs with operational data prove that you follow your security policy—thus simplifying SaaS security compliance.

Ease operational and compliance challenges with a SaaS Management Platform (SMP)

With BetterCloud, IT finally has unified visibility into their SaaS environment, along with more actionable insights and less noise.

Now IT has a way to automate routine operational tasks while embedding security best practices and data retention for compliance. The system of record from your SaaS operations will make it simpler to prove compliance to pass those audits every time.

About BetterCloud

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

For more information, please visit www.bettercloud.com.

