BetterCloud WHITEPAPER

Protecting Google Drive Data

5 Critical Requirements for Data Loss Prevention

The Costs and Causes of Data Loss

The average data breach costs $4 million, according to a 2016 Ponemon Cost of Data Breach Study. For that reason, companies are increasingly allocating attention and budget to the category of data management and protection. In fact, 57% of companies use two or more vendors to prevent data loss, according to the 2016 edition of the Global Data Protection Index.

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 September 2016 McAfee Labs Threat Report. Yahoo was affected by one of the largest data loss events in history (more than one billion accounts were exposed). They remained unaware for three years and the breach wasn't even discovered by their IT or security team.

While cyberattacks might get all the press, many data loss events are the result of human error and privilege misuse, which commonly takes months or years to detect without proper data loss protection (DLP) in place, according to Verizon's 2017 Data Breach Investigations Report.

These breaches can occur due to:

Improper or incomplete offboarding: Companies often have former employees that still have access to company data, even years after exiting. Offboarding that takes hours, days, or even weeks to complete leaves companies vulnerable and is often a significant compliance issue.

Accidental data disclosure: Misdelivery of information is far and away the primary form of human error, making up more than 50% of all error-related data breaches, according to Verizon's 2017 report. With email autofill and human inattentiveness, it's easy to understand how sensitive information escapes to the wrong person via email or accidental document sharing. Organizations should "focus on monitoring designed to capture (and prevent) data transfers" in real time, according to the Verizon report.

Failure to revoke partner, contractor, or consultant access: The "freelance economy" is exploding. In fact, freelancers made up 35% of U.S. workers in 2016. Freelancers, along with partners, consultants, and other external parties are often granted limited time access to information. Many companies fail to revoke that access after the contract or partnership is severed.

Lost or stolen devices: 95% of Americans own a cell phone, nearly 80% own a desktop or laptop computer, and more than 50% own a tablet, according to a 2017 Pew Research Center Mobile Fact Sheet. Losing or having a device stolen is common. Organizations without the ability to perform remote DLP actions, whether it's wiping devices, resetting passwords, or even suspending accounts are vulnerable to a data breach.

Malicious theft: In some cases, existing employees take advantage of the access they're afforded. Many times, cases of malicious data theft have financial motivations, where employees intend to use company data for monetary gain or for a future competitive advantage, according to the Verizon report.

5 Critical Requirements for Data Loss Prevention in Google Drive

Google Drive offers unparalleled collaboration and sharing, but G Suite administrators must balance productivity with the need to remain secure and compliant. As a result, many organizations that use Drive rely on powerful third-party DLP solutions to meet their security demands.

CIOs, security teams, and G Suite admins alike look for Drive DLP solutions that excel in each of the five core categories as defined below:

Auditing. One-off queries of a domain's Drive. This includes searching and identifying documents by their contents and metadata.

Actions. Administrative capabilities that enable admins to act on violations or perform other Drive-related management tasks on behalf of the entire organization, specific teams, or individual employees.

Alerting. Automated notifications that are configured to provide G Suite admins with up-to-date information about a domain's Drive.

Policies. Security configurations that audit and perform automated administrative Drive actions on an ongoing basis, requiring no manual maintenance.

Reporting. Drive content and metadata collection that enables G Suite admins to search and filter information to derive meaningful results.

Selecting a Drive DLP solution that excels in each of these areas will put you in the best position to secure your domain and prevent Drive-related data loss.

1. Auditing

Overview
Audits are necessary to understand how your employees use Drive. They're often used to scan Drive content and identify inappropriate sharing behavior. Audits also serve as test runs to see the potential impact of a policy.

Key Requirements
When selecting a Drive DLP solution, you must find a solution that offers robust auditing functionality. Look for those that can search Drive content for all of the following:

- File owner
- Action performed
- Action description
- Common file type
- Item ID
- User email address
- Date and time range when action occurred
- File size
- OU owner
- File title
- Exposure or current sharing status
- Date of last update
- Domains file is shared with
- Email addresses file is shared with
- Number of external collaborators/ viewers
- Expanded file type (.exe, .pdf, .jpg, .txt, etc.)

This depth of functionality will enable you to easily audit your Drive for the following (and much more):

1. **All publicly shared Drive files.**
2. **Externally shared Drive files owned by members of your executive, HR, and finance teams.**
3. **All documents shared externally with contractors that you are no longer working with.**

G Suite admins often take lengthy, roundabout routes to find this information (if it's even possible). The best DLP solutions can perform many comprehensive and granular Drive audits in minutes.

If you've never performed an in-depth Drive DLP audit, you likely have limited insight into your exposure risks. Often times, admins run audits and soon discover hundreds, even thousands, of sensitive Drive documents with "Public" sharing settings.

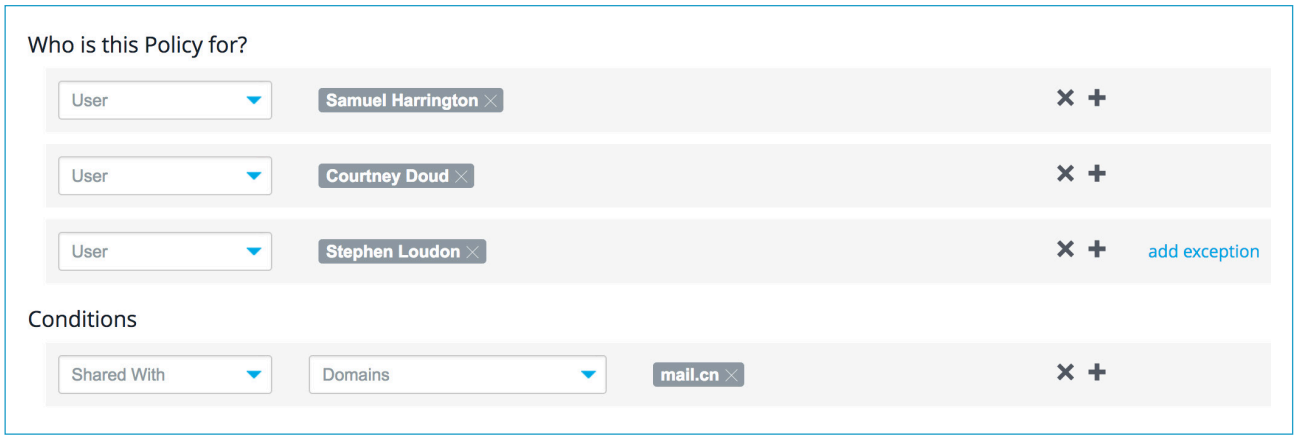
When selecting a Drive DLP solution, look for those that can identify relevant keywords, such as "Confidential" or "Board Deck." This is a must-have auditing feature.

Another essential DLP feature is the ability to use pre-built regular expression templates (or build your own). Regular expressions search Drive for common character patterns and are often used to help admins find things like credit card or social security numbers.

And lastly, a powerful DLP solution must offer advanced filtering capabilities. Without filtering, even a basic audit will return an overwhelming amount of information, making it difficult to drill down and find what's most important.

Auditing in BetterCloud

BetterCloud Drive DLP Auditing scans files across your entire organization's Drive. But the characteristic that separates it from others is its scoping capability. With BetterCloud, you can add multiple conditions (like file owner, sharing setting, etc.) to scope audits down and limit your scan to only what's most relevant.



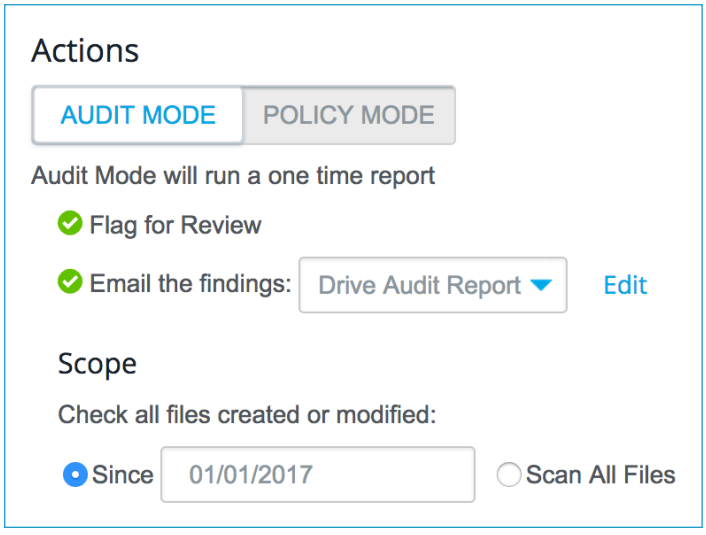
Auditing Use Case:

Investigating a Breach

You've recently started investigating a data breach. Hackers infiltrated several employees' accounts and shared Drive files with a malicious domain. You need to identify all compromised documents, as well as review the contents of the documents themselves.

You can run a BetterCloud Audit on everyone, or you can run it on one or multiple domains, OUs, or even users. In this case, you decide to run the audit on the three affected users. In BetterCloud, you configure audits in the form of a policy such as the one above.

The domain used by the malicious hacker was "mail.cn" in this example. Running this BetterCloud Policy in Audit mode will fetch a full report of all files shared with anyone using the mail.cn domain.



2. Actions

Overview

The ability to take action on Drive violations (both manually and automatically), without having to request permission from the file owner, is one of the most sought after Drive DLP features. Very few DLP solutions offer any remediation functionality, even in its most basic form. What if the employee is on vacation? What if the employee knows he or she is in violation but is acting with bad intentions? G Suite admins need more control over their Drive files.

Key Requirements

Without the ability to take action and remediate violations, a Drive DLP solution is nothing more than a reporting engine. Actions allow admins to perform behind-the-scenes tasks that enable better governance. These actions include:

- Change sharing settings
- Transfer ownership
- Change all editors to viewers
- Remove all collaborators (or add collaborators)
- Remove external collaborators
- Send alerts to any group, user, or external address
- Flag file as a violation

Without actions, Drive DLP solutions will leave you in a position of paralysis. You might know your company is non-compliant, but you won't be equipped to fix it.

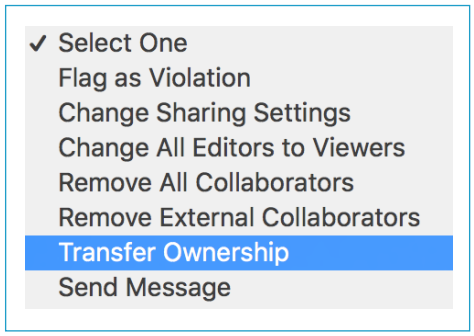
Often times, issues won't arise in isolation. They are widespread and pervasive. A best-in-class DLP solution enables admins to take actions that affect many files, users, domains, or OUs at once. Bulk actions virtually eliminate the time and energy wasted on tedious, repetitive tasks, all the while reducing human errors and resolving issues faster.

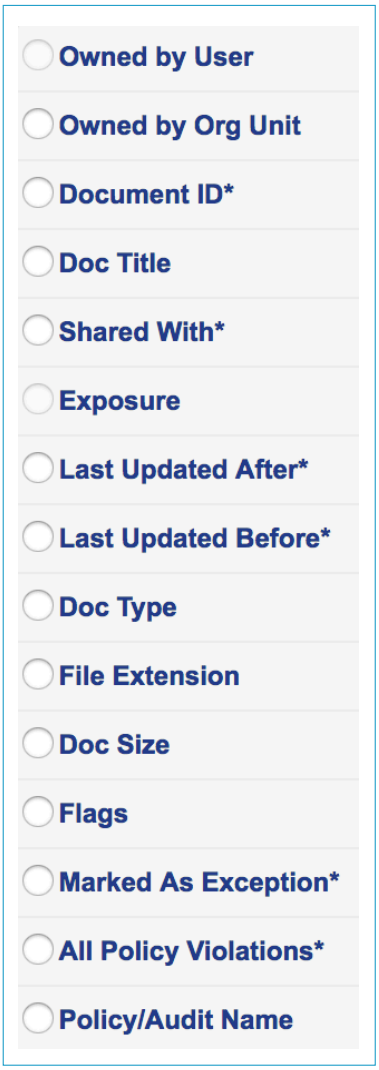
Actions in BetterCloud

BetterCloud's Drive DLP solution was built with actions in mind, going far beyond basic allow/block sharing and notification functionality. With an easy-to-use interface, BetterCloud's DLP solution is designed to carry out actions above either manually, in bulk, or through automated policies. Admins can do so across any number of files, users, domains, or OUs.

Actions Use Case:
Remediating Violations

Taking Action on Violations
After running an audit of your finance team's Drive behavior, you realize that a junior member of the team is the owner of several high-priority documents. The team member, who is entry-level, must have created copies of existing Drive files without understanding the security implications. You decide to transfer the ownership of these files to your CFO.





With BetterCloud, you can use multiple filters to comb through all Drive files (or the files related to a specific audit). This gives you the capability to find exact files easily--in this case, the files that require an ownership transfer. Once identified, you can select the files and immediately perform the necessary action(s).

3. Alerting

Overview
Alerting should be an asset, not an annoyance. Admins need alerting to stay up to date with their employees' Drive behavior, but they should also use it as a communication and education platform.

Key Requirements
You should avoid Drive DLP solutions that are unable to distinguish important alerts from minor ones. Without this capability, you'll find your inbox overflowing with unnecessary notifications. Look for solutions that enable admins to set alert thresholds and priority levels. This will help you weed out what's not important and avoid alert fatigue.

With some DLP solutions, alerting is limited to super admins only. Best-in-class Drive DLP alerting enables you to send alerts to anyone (even non-IT staff or external domains).

Additionally, an often overlooked aspect of alerting is context. If you're digging through illegible audit logs to find what's important, how are you supposed to take meaningful action? Alerts must carry meaning and relevance. To meet this requirement, alerts need to be customizable and dynamic to the situation, meaning they can change depending on the person receiving the alert and the policy that was violated.

For example, with an advanced Drive DLP solution, you can:

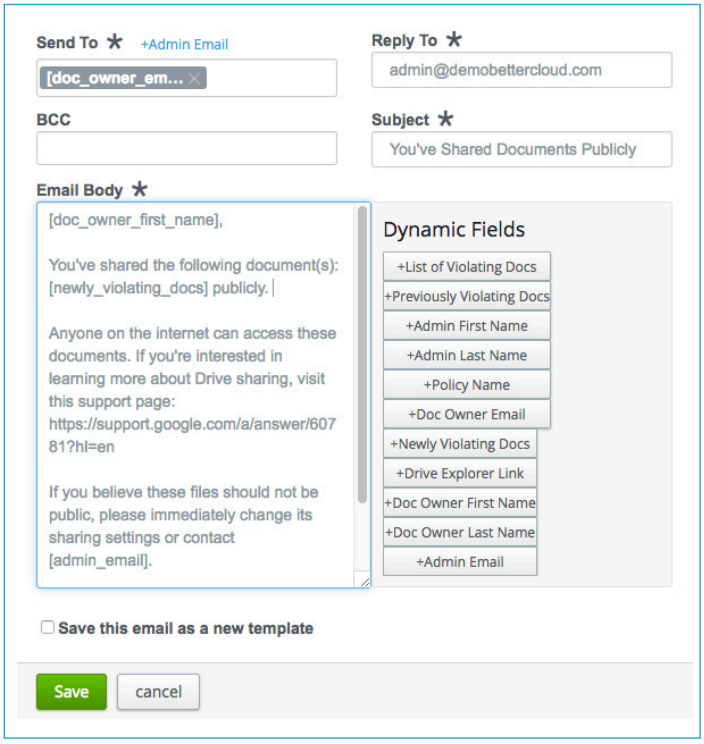
- Configure a policy that sends an alert to multiple people, including the employee in violation.
- Customize the alert to include a message highlighting the files that violated the policy and the actions taken on the user's behalf (if any). The alert can also give users the ability to request an exception.

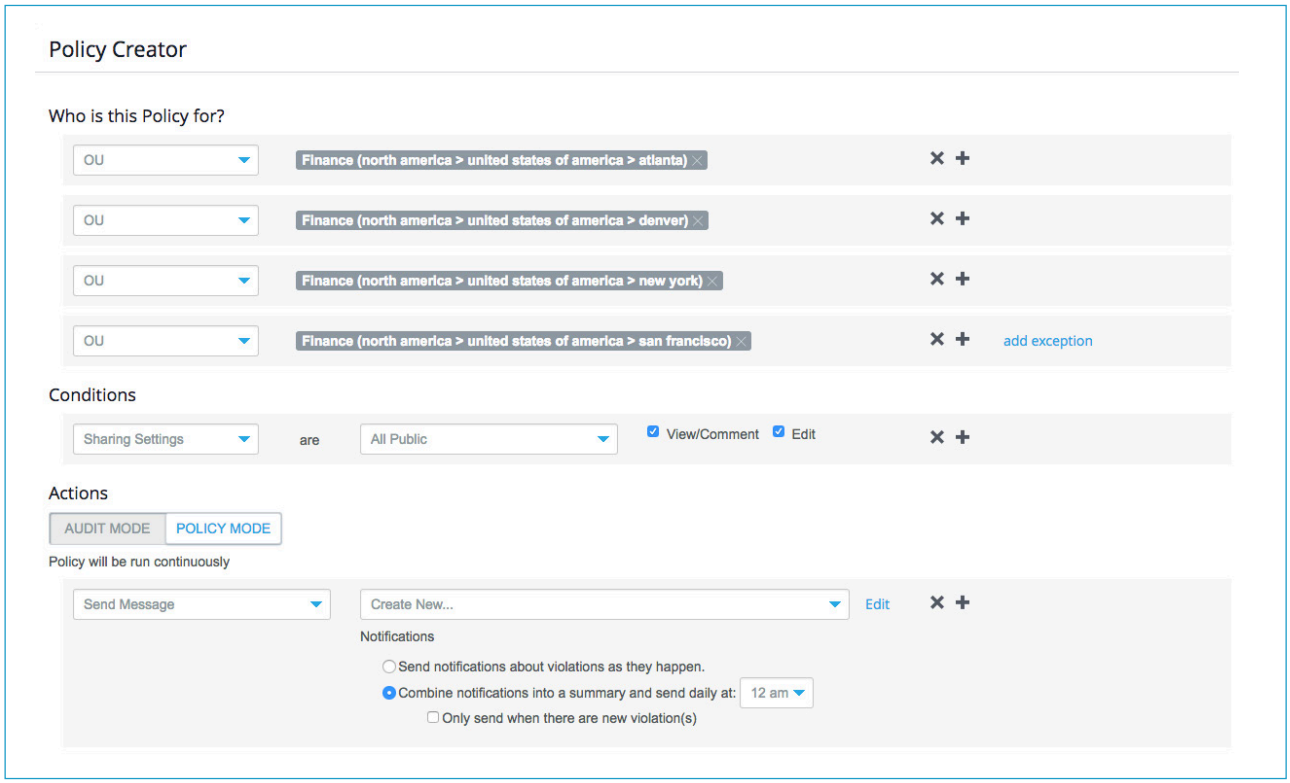
Alerting in BetterCloud
BetterCloud Alerts can be sent to multiple people, regardless of role, as many times as necessary. In addition, Alerts offer the context needed to make the right decisions. Finally, within BetterCloud, violations are located in one place, making it easy to assess the health of your domain and take action when necessary. Without BetterCloud Alerts, admins are left unaware of potential malicious or dangerous behavior.

Alerting Use Case:
Educating End Users

You want to ensure your employees take full advantage of Drive's collaboration capabilities. However, you don't want employees, particularly those on the finance team, sharing files recklessly. They need to understand exactly how their Drive sharing behavior impacts your company's security.

To do this, you configure a BetterCloud Policy. When violated, an alert is sent to the employee in violation and sends them educational materials. Because your company is global and multilingual, this policy should only apply to your North American finance team, which operates in four different locations.





4. Policies

Overview

Ideally, you never have to take a manual Drive DLP action. To achieve this, you'll need to select a solution with a robust Drive DLP policy engine. Policies are a powerful combination of audits, actions, and alerts that run continuously.

Key Requirements

It's impossible for anyone to to monitor their Drive activity 24 hours a day, 365 days a year. That's what makes policies powerful. They work whether you're on the clock or on vacation. Policies are often implemented as admins recognize patterns and realize they're running the same audits and taking the same actions over and over.

Policies identify violations and act automatically. For example, you should configure a policy that monitors your Drive to look for files shared with blacklisted domains. The policy should also automatically remove all collaborators and revert the sharing settings of a file to private when this behavior is detected.

This, and the examples below, are a few of the many policies that are only possible to configure with the help of a powerful Drive DLP solution.

For the majority of organizations, we suggest auto-reverting all publicly shared documents containing:

- The keyword "Confidential"
- The phrase "For Internal Use Only"
- The phrase "Attorney Client Privilege"

> *"We value BetterCloud's DLP capabilities as it gives us and our clients the knowledge that our G Suite data is secure and not being shared incorrectly. We can automatically block or report on sharing violations based on a policy. Without BetterCloud DLP that is not possible."*
>
> **- Colin McCarthy, IT Director, North America, Essence**

As a precaution, SSNs, credit card numbers, bank account numbers, personally identifiable information (PII), private keys, or certificates should not float freely inDrive. If this type of information is irresponsibly shared or accidentally exposed publicly, it's best to have a Drive DLP policy in place that recognizes this content and automatically takes remediation steps, revoking any external access and removing all viewers and collaborators, as well as transferring ownership of the file if necessary.

Many companies also have passwords that are commonly used by various people for various applications. If you are aware of these passwords, configure a regular expression or keyword policy that scans Drive for these and takes automated action similar to ones mentioned in the example above.

Policies should also be set for suspicious activity, such as employees sharing documents with personal email accounts or a competitor's domain.

Policies in BetterCloud

BetterCloud Policies offer the scanning and scoping capabilities of an Audit, the administrative power of Actions, and the dynamic communication of Alerts. With BetterCloud Policies, you can take a “set-it-and-forget-it” approach to monitor your Drive in an automated, always-on fashion. If implemented correctly, BetterCloud Policies will greatly reduce the risk of data loss and help you operate a far more compliant and secure organization.

Policies Use Case:

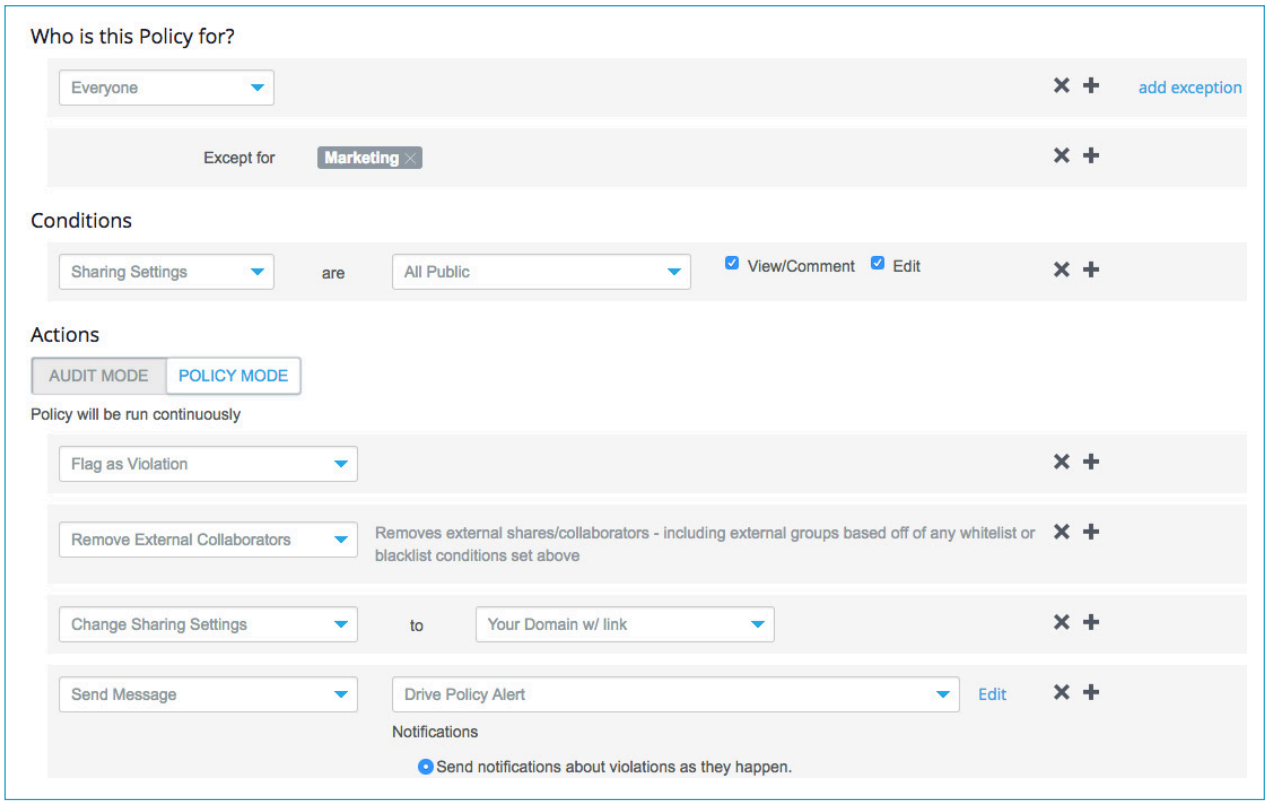
Auto-Reverting Sharing

A few months after rolling out Drive, you decide to see if employees are abiding by a rule you established in a recent Drive security training. The rule was simple: Do not share any Drive files publicly. You run an audit which quickly returns hundreds of publicly shared Drive files.

Realizing that training is unreliable and that you need safeguards in place, you configure a policy to auto-revert all publicly shared documents to a more secure sharing setting.

However, you know your marketing team requires an exception to this policy because they use publicly shared Google Docs for external education purposes.

With BetterCloud, you can set up and turn on this policy in seconds, remediating sharing issues in near real-time. You can even configure an exception for your marketing team.



5. Reporting

Overview
Reporting enables admins to create spreadsheets filled with rich data. Much like audits, reports help provide you with information about your Drive. However, audits are more focused on the content inside a file, while reports tend to offer more information about the file's metadata.

Key Requirements
Admins need DLP reporting that offers advanced filtering capabilities. Without this, reports will contain an overwhelming amount of unnecessary information. However, there is also the need to compile extensive reports as well, adding columns full of extra details. Best-in-class DLP solutions enable you to run a report on essentially everything that you can audit--and even a bit more.

> *"I haven't found a product yet with better reporting. BetterCloud has deeper insights that we couldn't otherwise generate."*
>
> **- Andrew Shelton, Information Security Manager, Middlesex Hospital**

An advanced DLP solution will let you run an automated report once a month that can do any of the following (and much more):

- Show all publicly shared docs for your domain
- Show all documents in violation of a policy
- Show all documents owned externally

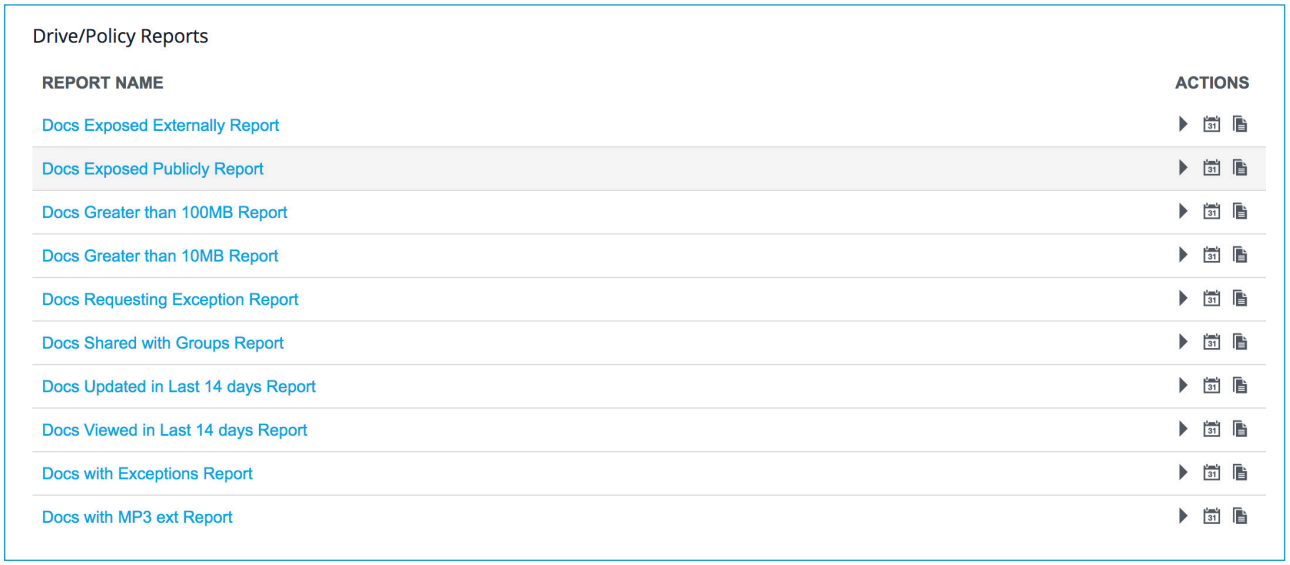
Reporting in BetterCloud

BetterCloud DLP Reporting takes the granularity of a BetterCloud Audit, but adds the ability to run the audit automatically on a schedule. These reports can then be shared automatically with whoever you want, whenever you want.

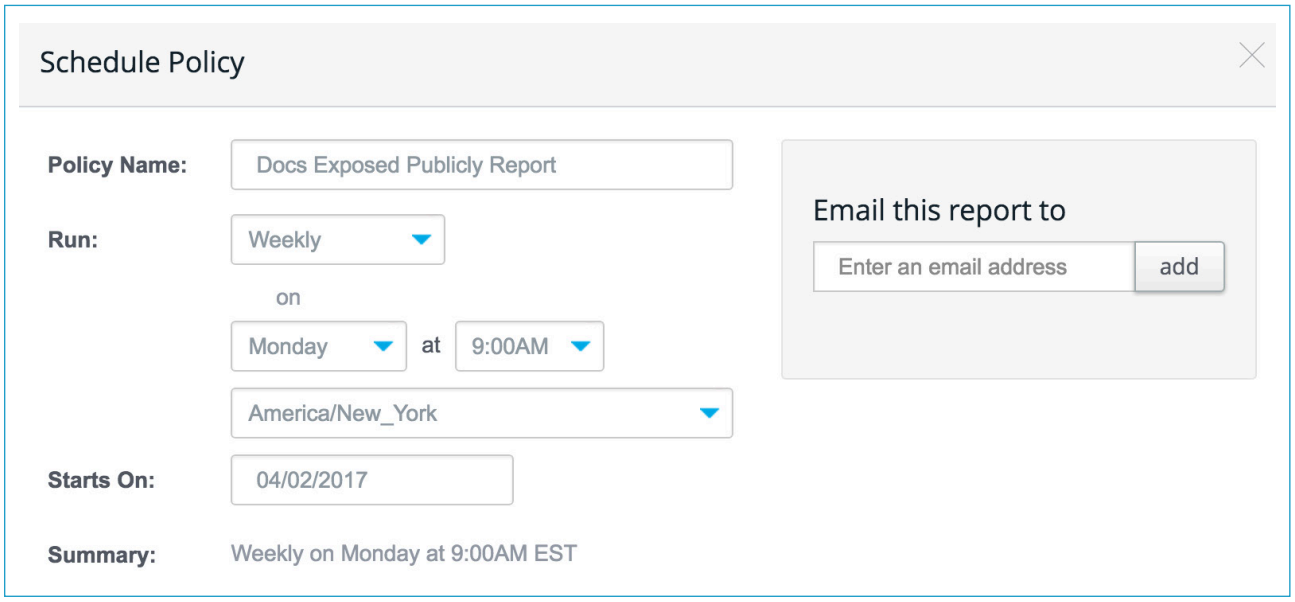
Reporting Use Case:
Understanding Exposure

At the beginning of every week, you'd like to run a report to monitor all publicly shared Drive files. You'd like the report to run precisely at 9:00 AM on Mondays and want the results sent to you and your company's technology trainer (who is focused on educating employees).

With BetterCloud, this is one of many templated Drive-related reports:



After choosing the report and customizing it to your needs, you can schedule it to run exactly when you'd like.



Demo BetterCloud today.

ABOUT BETTERCLOUD

BetterCloud is the first Multi-SaaS Management Platform, enabling IT to centralize, orchestrate, and operationalize day-to-day administration and control across SaaS applications. Every day, thousands of customers rely on BetterCloud to centralize data and controls, surface operational intelligence, orchestrate complex actions, and delegate custom administrator privileges across SaaS applications. BetterCloud is headquartered in New York City with engineering offices in Atlanta, GA. For more information, please visit www.bettercloud.com.