Implementing SaaS Security Workflows in Google Drive

The DoControl Impact

DoControl adds a foundational layer of preventative data access security controls to protect business critical assets in Google Drive. The solution integrates with Google Drive to secure all shared data and files accessed by every identity and entity, both internal employees as well as 3rd party collaborators. DoControl connects Google Drive activity with business context from identity providers (IdP), Human Resources applications, Endpoint Detection and Response solutions (EDR/XDR), and other existing platforms. This bidirectional feed enhances the value of existing IT and security investments, as well as provides complete visibility into the complex IT estate. Fine-grain data access controls help prevent data overexposure and exfiltration, automatically remediate the risk of insider threats, and allow for secure content collaboration throughout Google Drive.

Integrate Google Drive with DoControl to:

Gain Visibility and Control

Google Drive lacks the visibility required to manage and control access for groups and domains that regularly manipulate and share sensitive company data. The number of users and assets within a standard Google Drive implementation is unmanageably high, creating a scalable problem when attempting to secure the high volume of data and files. Google Drive administrators are limited to view only the shared drives that they have access to as a standard user. With no insight into the full inventory of shared drives, it's not possible to comprehensively protect and validate user access throughout the organization. DoControl enables IT and security teams to monitor and control every entity accessing corporate data within Google Drive. With full visibility into all public and private drives, teams can create automated secure workflows and policies to allow for secure file sharing between all users, both internal and external.

Enforce Granular Data Access Controls

Google Drive administrators are limited to "public" and "private" for file permissions. Links to assets can remain publicly accessible for far longer than they need to be, and depending on organizational settings can be changed by any user. Performing manual access reviews to "unshare" files requires the identification of each individual asset and removing permissions individually. In addition, there's no ability to query the data for filtering or grouping (i.e. by vendors, email, sharing status, etc.) within Google Drive

Key Benefits

1. Gain visibility into individual user interactions within Google Drive, as well as a comprehensive view of the entire organization
2. Experience a risk-based approach to securing Google Drive by prioritizing the necessary identities and assets that carry higher levels of risk
3. Establish secure workflows that are future-proofed to mitigate the risk of data overexposure and exfiltration
4. Implement the granular access required to maintain business continuity by granting each group/ department with the the sharing capabilities required
5. Centrally enforce consistent data access controls throughout Google Drive, and all other critical SaaS applications

environments. DoControl enables IT and security teams to analyze all SaaS user activity events, and filter by date and time, actor, target, asset, event type and event ID to understand the true scope of their data overexposure risk. From there, data access security gaps can be minimized through the enforcement of least privilege access to the Google Drive application data layer. Access to sensitive data within Google Drive is provided for the necessary amount of time before it's revoked, users can then share or request access in a "just in time" manner to balance out security and end-user productivity.

Secure 3rd Party Access

Google Drive does not provide the ability to enforce the prevention of sharing documents on a shared drive from an approved 3rd party, to other vendors (i.e 4th party vendor). Once assets are shared out to approved 3rd parties, what those users then do with the data is out of the scope of control for the organization who has ownership over the file.

DoControl provides secure workflows for approved external collaborators that prevent the sharing of sensitive files to unauthorized parties. In addition, DoControl will automatically expire external and public sharing, reducing the risk of data overexposure. The solution helps address the downstream effect of file sharing to potentially unapproved vendors by mitigating the risk of data leakage, providing a strong security posture in Google Drive environments.

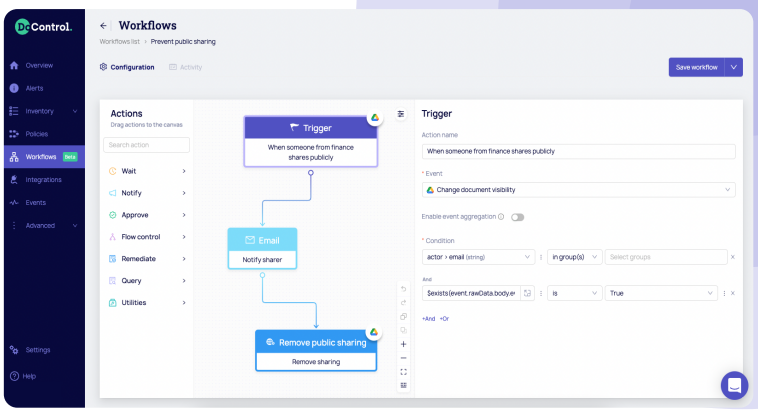
Enforcement Actions

Enforcement actions can be established by defining secure workflow policies that trigger automatically by events within Google Drive, as well as manual 'immediate actions' that DoControl administrators can execute to reduce risk in real-time.

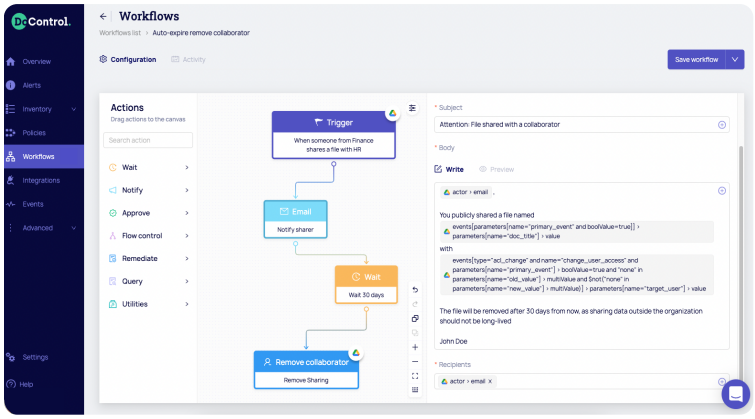
- **Example pre-established secure workflow policies include:** prevention of public asset sharing, auto-expiration of public sharing, removal of external collaborators, notification of encrypted keys sharing, prevention of sharing to private email accounts, asset monitoring and isolation, and more.

- **Example immediate actions include:** removing public sharing, changing file ownership, revoking access to specific users, and more.

Reach out to a DoControl expert to review additional enforcement actions and threat model coverage.



Preventing public sharing in Google Drive



Automatically removing 3rd party collaborator access in Google Drive

Secure Workflow Creation

DoControl provides a rich catalog of hundreds of playbooks that can be leveraged to create specific enforcement actions within Google Drive. Policies can be created from scratch, or the playbooks can be adjusted to align to specific security program requirements. Creating secure workflow policies for Google Drive with DoControl can be achieved in a few simple clicks. The playbooks can be found directly within the DoControl console by accessing the **Workflows** tab.

Permission Scopes

A full listing of required read/write permissions scopes are available in the DoControl documentation portal, which you can find here. The minimum license required from Google to implement DoControl is the **Business Standard** option. Once integrated, the DoControl solution is enabled to automatically implement the enforcement actions that've been pre-established (examples listed above), across all Google Drive users and assets.

About Google Drive

Google Drive is a file storage and synchronization service that allows users to store files in the cloud, synchronize files across devices, and share files. In addition to a web interface, Google Drive offers apps with offline capabilities for Windows and macOS computers, and Android and iOS smartphones and tablets. Google Drive encompasses Google Docs, Google Sheets, and Google Slides, which are a part of the Google Docs Editors office suite that permits collaborative editing of documents, spreadsheets, presentations, drawings, forms, and more. Files created and edited through the Google Docs suite are saved in Google Drive.