Implementing SaaS Security Workflows in Dropbox

The DoControl Impact

DoControl provides comprehensive data access security that adds a foundational layer of preventative controls to protect sensitive business critical data and files in Dropbox. The solution integrates with Dropbox to secure all shared data and files accessed by every identity and entity, both internal employees as well as 3rd party collaborators. DoControl's fine-grain data access controls help prevent data overexposure and exfiltration, automatically remediate the risk of insider threats, and allow for business enablement to be achieved in a secure way.

Integrate Dropbox with DoControl to

Gain Visibility and Control

Dropbox 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 Dropbox implementation is unmanageably high, creating a scalable problem when attempting to secure data and files within the application. Gaining insight into which files are publicly accessible and which are not, identifying which assets have a password or expiration date, and tracking external user access – all prove to be a challenge within the Dropbox admin console. DoControl enables Dropbox users to gain full awareness of every entity that is accessing corporate data to identify what needs to be protected, and then create policy that allows for secure file sharing between all internal and external users.

Close Permissions and Enforcement Gaps

Establishing permissions to Dropbox users lacks the required granularity to implement effective data access control policies. Applying settings that are based on specific users and departments, or other similar relevant parameters, is not supported in Dropbox. For example, sales and marketing teams are more likely to share files externally compared to engineering and R&D teams. Dropbox does not provide the ability to apply specific workflow policies to different groups and departments. Company-wide data access policies also lack granularity, and are limited to generic CRUD (create, read, update and delete). Discovering public URLs are easy to find within the Dropbox admin console, however enforcement actions are limited to being established after the fact (e.g. removing external sharing), which is not a trivial process. DoControl provides future-proofed, secure workflows for specific users and groups that present higher-levels of risk to the business. DoControl can address limitless security use cases within Dropbox, as the platform is completely-event driven by all SaaS activity within the application. Once defined, secure data access policies will be triggered in real-time, adding a critical layer of preventative controls to minimize file over exposure and over sharing.

Key Benefits

1. Gain visibility into individual user interactions within Dropbox, as well as a comprehensive view of the entire organization
2. Experience a risk-based approach to securing Dropbox 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 Dropbox, and all other critical SaaS applications

Secure 3rd Party Access

Dropbox 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.

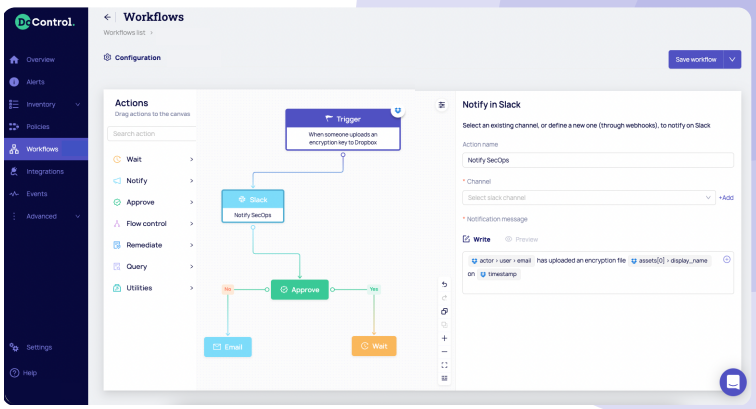
DoControl provides secure workflows for approved external collaborators that prevent the sharing of sensitive files to unauthorized parties. In addition, DoControl will automatically expire external and public sharing, reducing the risk of data overexposure. The DoControl solution helps address the downstream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

Enforcement Actions

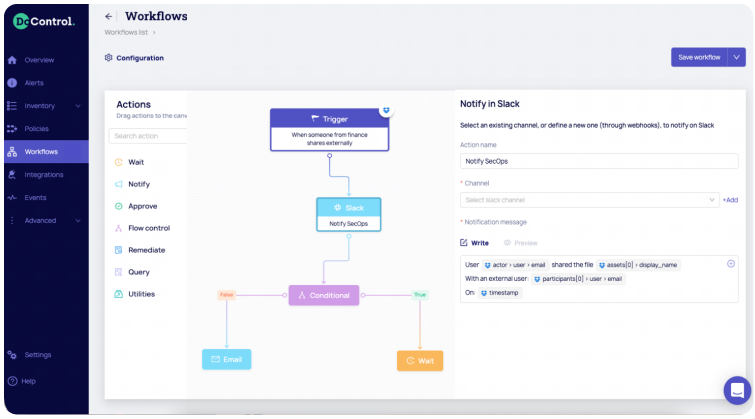
Enforcement actions can be established by defining secure workflow policies that trigger automatically by events within Dropbox, as well as manual 'immediate actions' that DoControl administrators can execute to reduce risk in real-time.

- **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.



Notification of encryption keys being uploaded into a Slack channel from Dropbox, with an approval process for the Security Operations team.



Notification of an external share from Dropbox with conditional steps for the Security Operations team to respond.

[Reach out to a DoControl expert] to review additional enforcement actions and threat model coverage. DoControl provides a rich catalog of hundreds of playbooks that can be leveraged to create specific enforcement actions within Dropbox. Policies can be created from scratch, or the playbooks can be adjusted to align to specific security program requirements. Creating secure workflow policies for Dropbox 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]. Integrating DoControl with Dropbox requires a **Basic Plan**, and the integrator must be a 'Team Administrator.' Once integrated, the DoControl solution is enabled to automatically implement the enforcement actions that've been pre-established (examples listed above), across all Dropbox users and assets.

About Dropbox

Dropbox is a file hosting service that offers cloud storage, file synchronization, personal cloud, and client software. Dropbox allows users to create a special folder on their computers, which Dropbox then synchronizes so that it appears to be the same folder regardless of which computer is used to view it. Files placed in this folder are also accessible via the Dropbox website and mobile apps. Dropbox provides client software for Microsoft Windows, Mac OS X, Linux, Android, iOS, BlackBerry OS and web browsers, as well as unofficial ports to Symbian, Windows Phone, and MeeGo.