Implementing SaaS Security Workflows in Microsoft OneDrive and SharePoint

The DoControl Impact

DoControl adds a foundational layer of preventative data access security controls to protect business critical data and files in Microsoft OneDrive and SharePoint. The solution integrates with OneDrive and SharePoint to secure all shared data and files accessed by every identity and entity, both internal employees as well as 3rd party collaborators. DoControl connects OneDrive and SharePoint 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 OneDrive and SharePoint.

Integrate Microsoft OneDrive and SharePoint to:

Gain Visibility and Control:

OneDrive and SharePoint lack 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 OneDrive and SharePoint implementation is unmanageably high, creating a scalable problem when attempting to secure the high volume of data and files. The Microsoft administrator console provides visibility into the number of files stored in each location and the external users who have access, but determining the exact exposure for each individual asset requires a significant amount of manual work. DoControl enables IT and security teams to monitor and control every entity accessing corporate data within OneDrive and SharePoint. 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

Providing links to share sensitive files for external users often remain active for far longer than necessary, and – depending on organizational settings – can be changed by any user. Performing manual access reviews to “unshare” files requires identifying each overexposed 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 OneDrive and SharePoint 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 OneDrive and SharePoint application data layer. Access to sensitive data within OneDrive and SharePoint 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

OneDrive and SharePoint do 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,

Key Benefits

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

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 OneDrive and SharePoint environments.

Enforcement Actions

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

- **Example pre-established secure workflow policies include:** alerts for encrypted keys sharing, removal of internal and external collaborators, prevention of sharing to private email accounts, asset monitoring and isolation, and more.
- **Example immediate actions include:** removing public sharing, revoking access to specific users, and more.

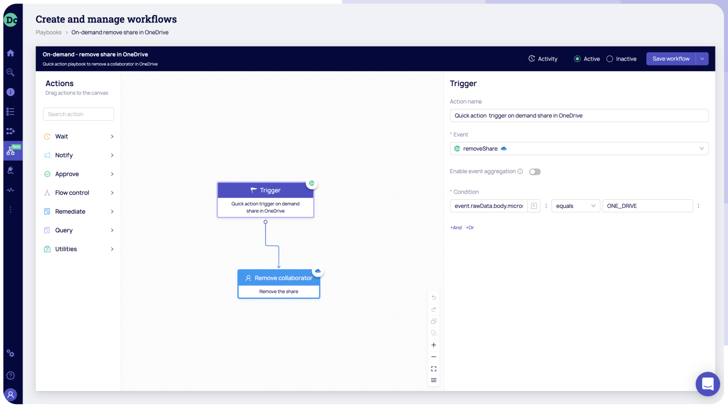
Reach out to a DoControl expert to review additional enforcement actions and threat model coverage.

Secure Workflow Creation

DoControl provides a rich catalog of hundreds of playbooks that can be leveraged to create specific enforcement actions within OneDrive and SharePoint. Policies can be created from scratch, or the playbooks can be adjusted to align to specific security program requirements. Creating secure workflow policies for OneDrive and SharePoint 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 for OneDrive and here for SharePoint. The minimum license required from Microsoft to implement DoControl is the **Business Basic** option for both OneDrive and SharePoint. Once integrated, the DoControl solution is enabled to automatically implement the enforcement actions that've been pre-established (examples listed above), across all OneDrive and SharePoint users and assets.



Create and manage workflows

Playbooks › On-demand remove share in OneDrive

On-demand - remove share in OneDrive

Quick action playbook to remove a collaborator in OneDrive

Activity ● Active ○ Inactive Save workflow

Actions

Drag actions to the canvas

Trigger

Action name: Quick action trigger on demand share in OneDrive

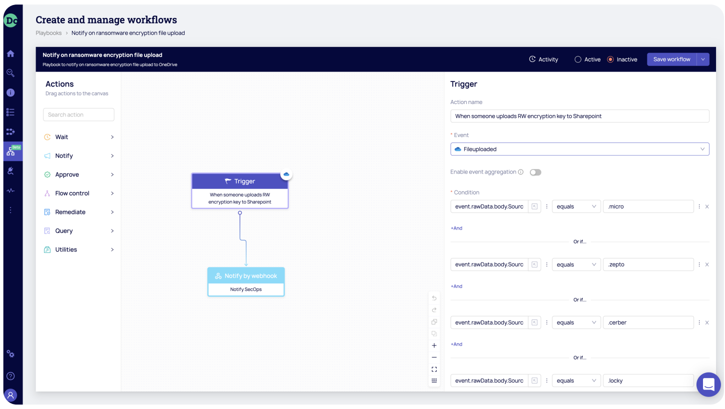
* Event: removeShare

Enable event aggregation

* Condition: event.rawData.body.micro: equals ONE_DRIVE

+And +Or

A Quick Action Playbook for on-demand access removal of an external collaborator in Microsoft OneDrive.



Create and manage workflows

Playbooks › Notify on ransomware encryption file upload

Notify on ransomware encryption file upload

Playbook to notify on ransomware encryption file upload to OneDrive

Activity ○ Active ● Inactive Save workflow

Actions

Drag actions to the canvas

Trigger

Action name: When someone uploads RW encryption key to Sharepoint

* Event: Fileuploaded

Enable event aggregation

* Condition: event.rawData.body.Sourc equals .micro

+And

Or if...

event.rawData.body.Sourc equals .zepto

+And

Or if...

event.rawData.body.Sourc equals .cerber

+And

Or if...

event.rawData.body.Sourc equals .locky

Automated notification to the Security Operations team when ransomware encryption keys are uploaded into Microsoft OneDrive.

About Microsoft OneDrive and SharePoint

Operated by Microsoft. OneDrive enables registered users to share and sync their files, and also works as the storage back-end for the web version of Microsoft Office. Microsoft SharePoint is a web-based collaborative platform that integrates with Microsoft Office. SharePoint is primarily sold as a document management and storage system, but the product is highly configurable and its usage varies substantially among organizations.

Partner with DoControl and start moving security closer to what drives the modern business forward. Learn more.