Implementing SaaS Security Workflows in Slack

The DoControl Impact

DoControl provides comprehensive data access security that adds a foundational layer of preventative controls to protect sensitive business critical files that are accessed and shared throughout all Slack channels. The solution integrates with Slack 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 Slack with DoControl to:

Enable Secure File Sharing

Slack does not restrict file sharing for sensitive data, and attempting to enforce consistent security controls manually throughout all file types shared across Slack channels is both challenging and cumbersome. When an external channel is created, there's no visibility and control over who can join on behalf of the external organization. Sensitive data that is shared to an approved 3rd party can then be accessed by an unapproved 4th party. In addition, there's no prerequisite for Slack members to register with the company's domain, allowing private emails to be used. Private emails often do not have the required policies a company would demand (i.e 2FA), which creates a higher risk for data exfiltration. DoControl enables IT and security teams to create future-proofed, automated workflows that support secure file sharing throughout Slack instances. Granular data access policies can be established that restrict specific files from being accessed by unauthorized parties or revoke access to authorized users after a predetermined amount of time.

Manage and Monitor Critical Assets

When files are uploaded into a public Slack channel (i.e. channels that are open for the entire organization) they remain accessible to anyone unless they are actively deleted. Sensitive files that contain encryption keys are exchanged over Slack for legitimate business purposes, but are often never removed. Leaving files accessible indefinitely increases the risk of a malicious insider to scrape through Slack channels and exfiltrate sensitive data. Additionally, there are specific users and groups that carry higher levels of risk based on the files that they regularly access as part of their job function. With no ability to monitor and control high-risk individuals and assets, the likelihood of data over exposure and exfiltration increases overtime. DoControl provides full asset management throughout all critical SaaS applications being accessed and shared by internal and external users. IT and security teams can monitor and control all user activity on an individual-level, and take immediate action to remediate risk. Data access control policies can also be enforced to automatically prevent sensitive files from being uploaded, shared and accessed indefinitely across all organizational Slack channels.

Balance Security and Business Enablement

DoControl consolidates and normalizes activity events and assets' metadata across all critical SaaS applications, providing a baseline of normal end-user behavior. From there, IT and security teams can set up Slack webhooks within DoControl's automated security workflows to enable real-time notifications of various scenarios – such as public sharing, encryption key file uploads, sharing with private email accounts, and more. Lower risk events can be directed to

Key Benefits

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

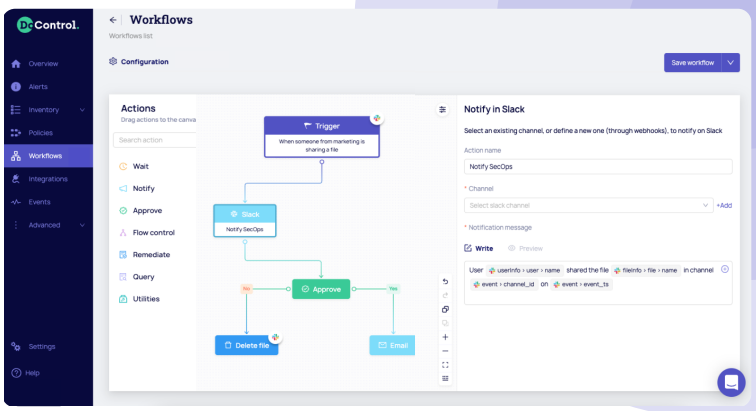
individual actors (i.e. standard business users), and higher risk events can be directed towards the appropriate teams to take necessary action. DoControl automatically offloads lower priority tasks from those teams to allow them to focus on mission-critical projects that add more value to the business.

Enforcement Actions

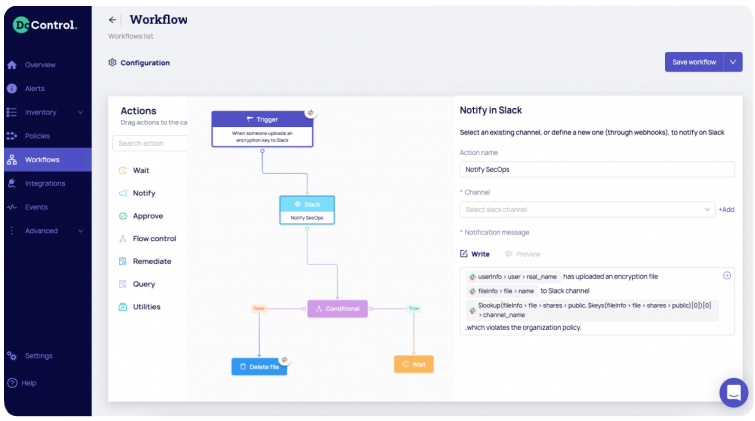
Enforcement actions can be established by defining secure workflow policies that trigger automatically by events within Slack, as well as manual 'immediate actions' that DoControl administrators can execute to reduce risk in real-time.

- **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 to the Security team when a specific high-risk user uploads files into Slack.



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

[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 Slack. Policies can be created from scratch, or the playbooks can be adjusted to align to specific security program requirements. Creating secure workflow policies for Slack 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 license required from Slack to implement DoControl is **Slack Pro** and above. For integration with **Slack Business+** and **Enterprise**, workspaces must be integrated separately, and not at the organizational level. Once integrated, the DoControl solution is enabled to automatically implement the enforcement actions that've been pre-established (examples listed above), across all Slack users and assets.

About Slack

Slack (Searchable Log of All Conversation and Knowledge) is the collaboration hub that brings the right people, information, and tools together to get work done. Slack offers many IRC (Internet Relay Chat)-style features, including persistent chat rooms organized by topic, private groups, and direct messaging. Slack's platform team works with partners and developers globally to build apps and integrations that streamline work, automate mundane tasks and bring context into conversations in Slack.

Partner with DoControl and start moving security closer to what drives the modern business forward. [Learn more.](#)