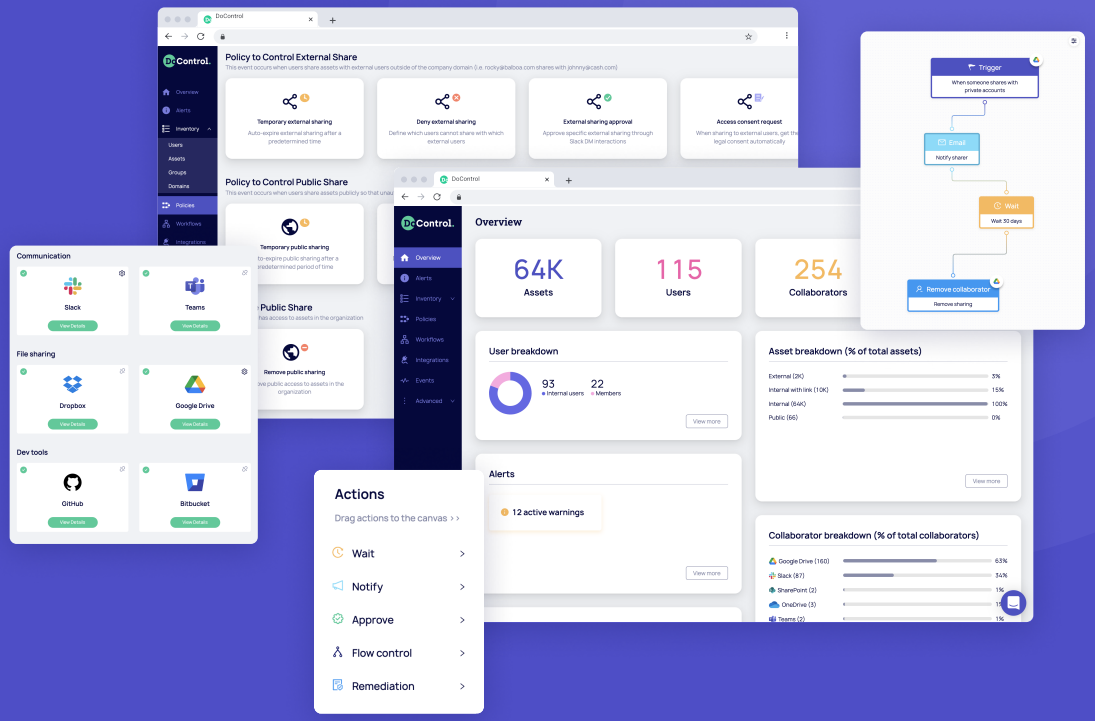
DoControl.



Software as a Service (SaaS) Security Use Cases

docontrol.io

Table of Contents

Introduction

Modern businesses rely on Software as a Service (SaaS) applications for everything from storing sensitive information and PII to driving collaboration on critical projects. These cloud-based applications make it simple for employees to share information and collaborate with external parties, such as vendors, prospective customers, partners, contractors and temporary employees – but this convenience often comes at the cost of security. With no ability to define and enforce consistent data access controls across all the applications used to drive the business, it is nearly impossible to systematically protect company data across the entire SaaS estate. Old sharing permissions remain active long after they are needed, security teams get bogged down with manual work, and unmanageable SaaS data access accumulates, significantly increasing the likelihood of a data breach.

DoControl helps solve the dilemma of SaaS application data access monitoring, orchestration, and remediation. We take a unique, customer-focused approach to the challenge of labor-intensive security risk management and data exfiltration prevention in popular SaaS applications. By replacing manual work with automation, DoControl reduces the overload of work and complexity that security teams are continually faced with. The DoControl platform can address a vast number of data access use cases. This document provides a listing of some of the most common examples for modern businesses leveraging SaaS.

Unified Data Access Controls

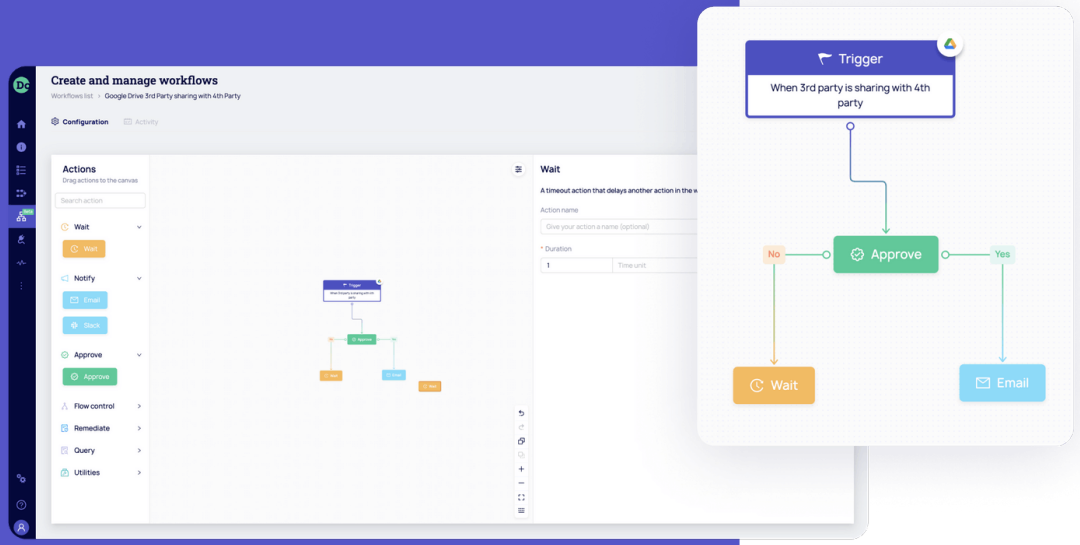
Businesses utilizing multiple SaaS applications have no centralized way to view the significant number of assets stored in each application, no insight into the exposure for each asset (e.g. what is shared and with whom), and no means to take bulk remediation actions when necessary (e.g. remove sharing for a large number of files). Permissions are continuously added and changed as employees and collaborators go about their work, and the overall number of files is continually growing as the business scales out. This creates challenges for security teams to establish consistent data access governance across all SaaS applications.

DoControl gives security teams the tools they need to centrally enforce comprehensive data access policies throughout complex SaaS application environments. Security Workflows can be automatically triggered in response to high-risk SaaS events and activity identified by our anomaly-detection technology. Security teams can create workflows that auto-expire sharing permissions for assets within SaaS applications, establish self- service or automated remediation for threats, and more. DoControl's Security Workflows can help organizations automate the overexposure-prevention process and minimize your SaaS attack surface on a daily basis

Prevent Data Loss in SaaS Ecosystems

Employees routinely share Personally Identifiable Information (PII), Payment Card Industry (PCI) and Personal Health Information (PHI) in overexposed locations such as public Slack channels and Microsoft Teams chats. Leveraging the security controls that are native to each SaaS application does not provide the ability to prevent the sharing of these data or target them for removal, and file-scanning offered by traditional Data Loss Prevention (DLP) solutions creates too many false positives that overload security teams with inaccurate detections to review.

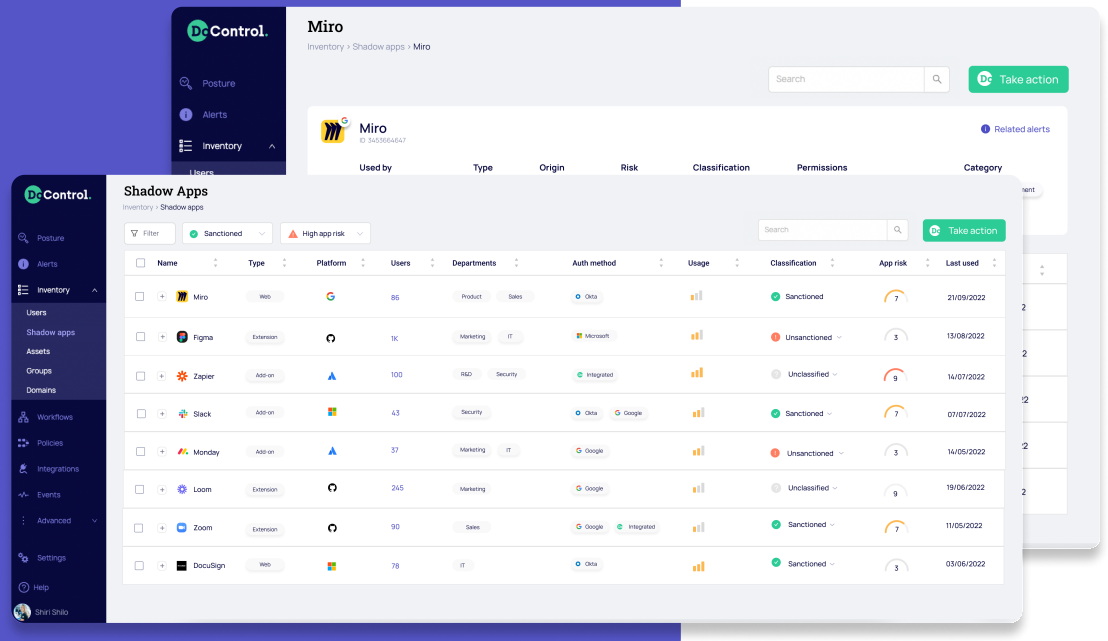
DoControl uses natural-language processing (NLP) to provide real-time scanning and classification for sensitive data types – including PII, PCI and PHI – across all files stored in SaaS applications. DoControl's file-scanning technology detects sensitive information across all structured, semi-structured and unstructured data types, then automatically classifies and/or redacts sensitive information according to the rules that have been established. DoControl's Security Workflows can be customized to solve for any use case; including preventing sharing of sensitive data types in specific SaaS locations, or by/with specific individuals or departments.



Enforce Shadow Application Governance

Application-to-application connectivity increases the threat vector by introducing machine identities that are often over privileged, unsanctioned, and not within the Security team's visibility. When machine identities become compromised they can provide unauthorized access to sensitive data within the application that it's connected to. These "non-human" identities can gain permissions to read, write, and delete sensitive data – which can significantly impact an organization's security, business, and compliance risk.

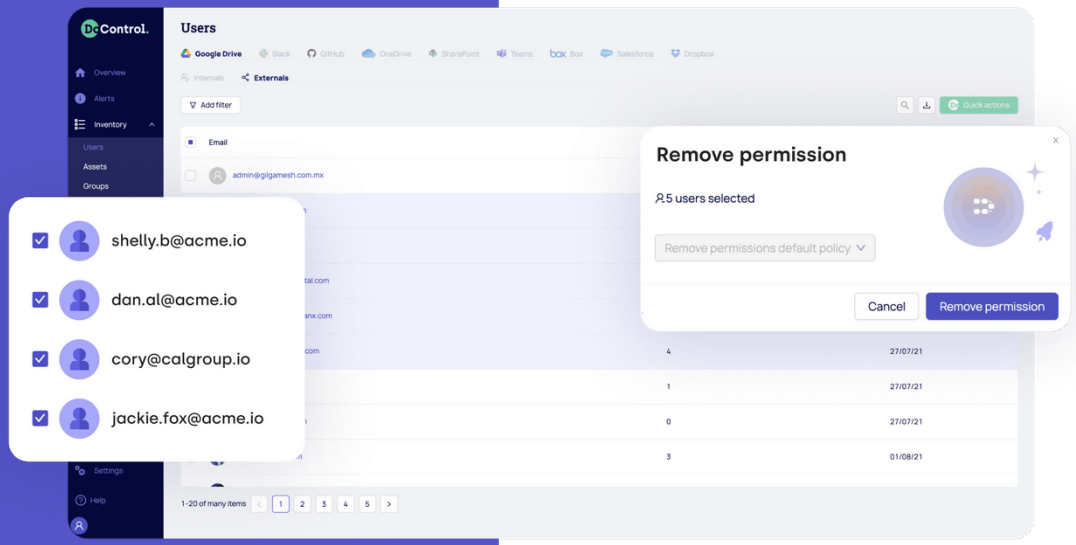
DoControl provides comprehensive "shadow application" governance through discovery, control, and automated remediation. The solution will discover all interconnected SaaS applications within the estate, and expose a full mapping and inventory of 1st, 2nd and 3rd party applications. Application reviews can be performed with business users, and risk scoring can be applied to each application to assess and evaluate risk. Security teams can automate security policy enforcement to prevent unsanctioned application usage, and remediate the risk those applications have the potential to expose (i.e. invalid tokens, extensive or unused permissions, listed vs. not listed apps etc.).



Manage Insider Risk and Threats

Human Resources (HR) and security teams work in silos, but their ongoing work has reciprocal effects. For example, when HR managers initiate employment status changes for departing employees, security teams should be made aware so they can closely monitor these high-risk individuals. Employee's that are terminated or made redundant increases insider threat risk and the propensity for sensitive data exfiltration. HR and security platforms are often disconnected, which increases the likelihood of sensitive information leaving with a departed employee.

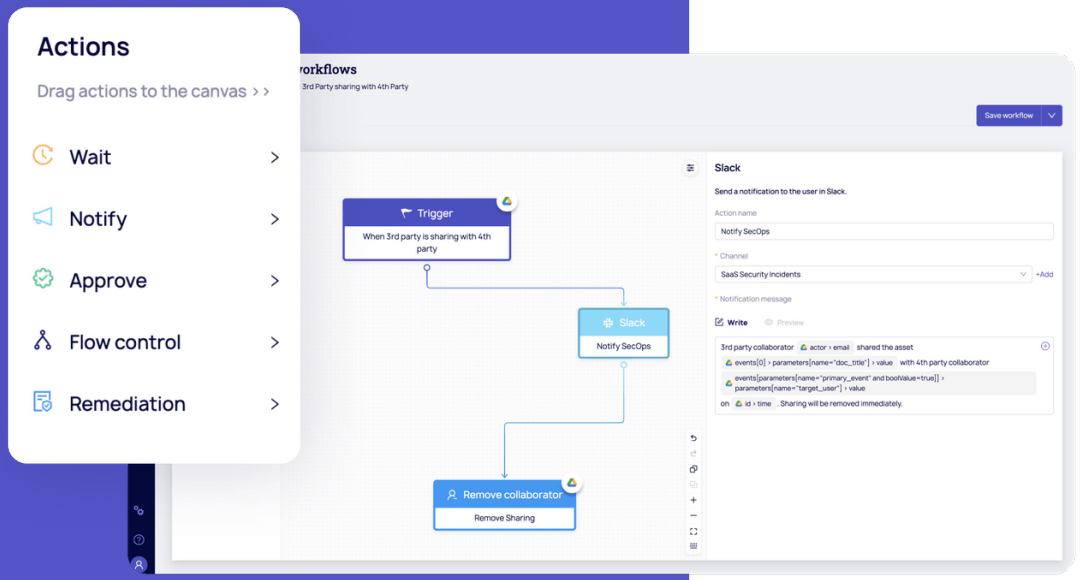
DoControl closes this gap by integrating with modern HR applications (i.e. BambooHR and Workday) to continually sync the list of departing and terminated employees. Anomaly-detection technology identifies inappropriate end-user behavior – such as external sharing of sensitive data by a departing employee – and sends real-time notifications to security teams. Automated Security Workflows can be initiated in real-time when employment status changes are triggered to block sharing and prevent departing employees from exfiltrating data (i.e. via emailing sensitive files to personal email accounts) stored in SaaS applications.



Streamline Incident Response Efforts

Modern SaaS environments are characterized by constant exchanges of data and files across content collaboration tools like Google Drive, Box, Dropbox, and Slack. As a result, security teams are inundated with security alerts and detections to analyze. The lack of business context for each alert creates a high number of false positives, makes identifying high-risk activity a significant challenge, and increases MTTR for actual threats to the business.

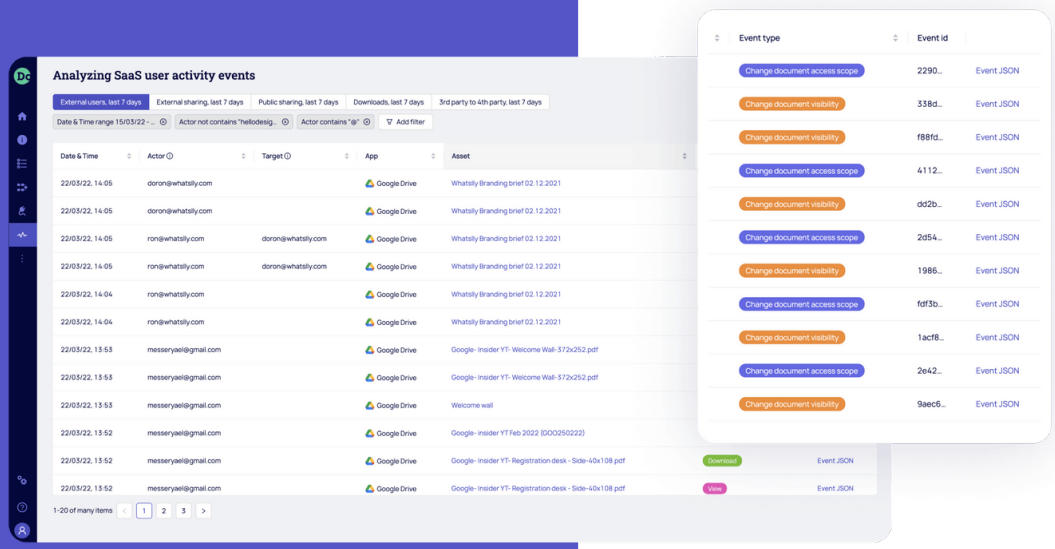
DoControl integrates with your SIEM/SOAR solutions to provide a data feed highlighting end-user activity and SaaS access anomalies that present material risk to the business. Anomaly-detection mechanisms identify and send real-time notifications for deviations with end-user "normal" behavior across common user actions (i.e. share, download, delete, upload, etc.). One-click remediation paths are available to address risky SaaS activity by removing external collaborators' access to company data, revoking public links, changing data ownership, and more. DoControl simplifies incident response processes through both self-service and automated remediation capabilities.



Satisfy Audit and Compliance Requirements

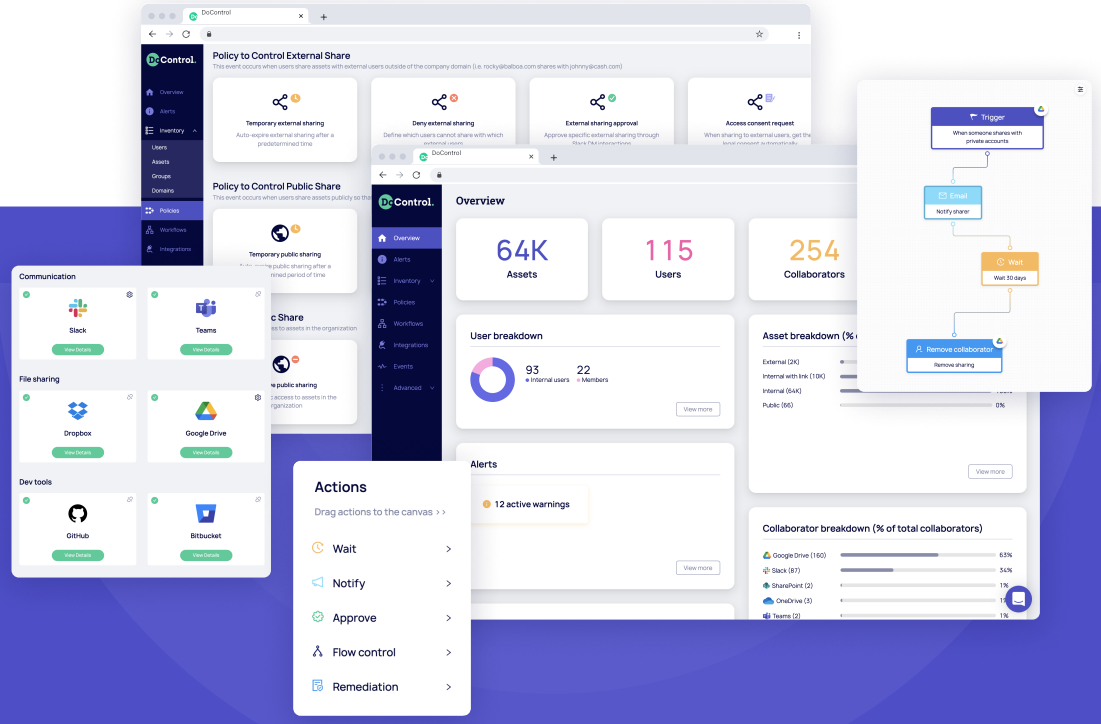
Modern businesses must balance business enablement with the need to comply with various security regulations such as Payment Card Industry Data Security Standard (PCI DSS), General Data Protection Regulation (GDPR), and more. For cloud-first organizations, remaining compliant across all sensitive data stored in SaaS applications is a complex challenge. Security teams must manually review and analyze SaaS activity to determine the right remediation paths – an incredibly labor-intensive process at enterprise scale.

DoControl provides a complete audit trail of all end-user activity and events within SaaS applications to simplify the process of gathering compliance evidence. To maintain adherence with strict confidentiality mandates, security teams can establish preventative controls that enforce granular, role-based access to highly sensitive data. DoControl's Security Workflows help provide compliance support by auto-expiring access to sensitive data, blocking internal and/or external sharing, establishing automated or self-service remediation paths for non-compliant SaaS activity and permissions, and more.



Conclusion

DoControl provides security teams the automated, self-service tools required for data access monitoring, orchestration, and remediation within SaaS applications. The solution helps organizations of all sizes and types prevent data breaches in the most popular SaaS applications, and bring balance between security and business enablement. DoControl's Security Workflows enable teams to address near limitless use cases, through fully customizable and granular data access control policies. Get started today by requesting a personalized solution demonstration to review use cases that are unique to your business.



contact@docontrol.io