DoControl for Cloud Access Security Broker (CASB)

The Challenge

Cloud Access Security Broker solutions act as an intermediary between end users and cloud hosted services. These tools help identify data and files stored within applications, which end users have access, and allow security teams to implement data protection policies. Traditional CASB policy enforcement points placed between cloud service consumers and providers are often hardcoded, and limited in terms of granularity to effectively interject data access security controls that work. Out-of-band mode lacks real-time context as well as high latency. Inline mode bypasses larger files as it lacks the ability to scan them in a timely manner. Both deployment modes are complex, difficult to manage, and lack real-time propagation to detect and block unauthorized access to sensitive data.

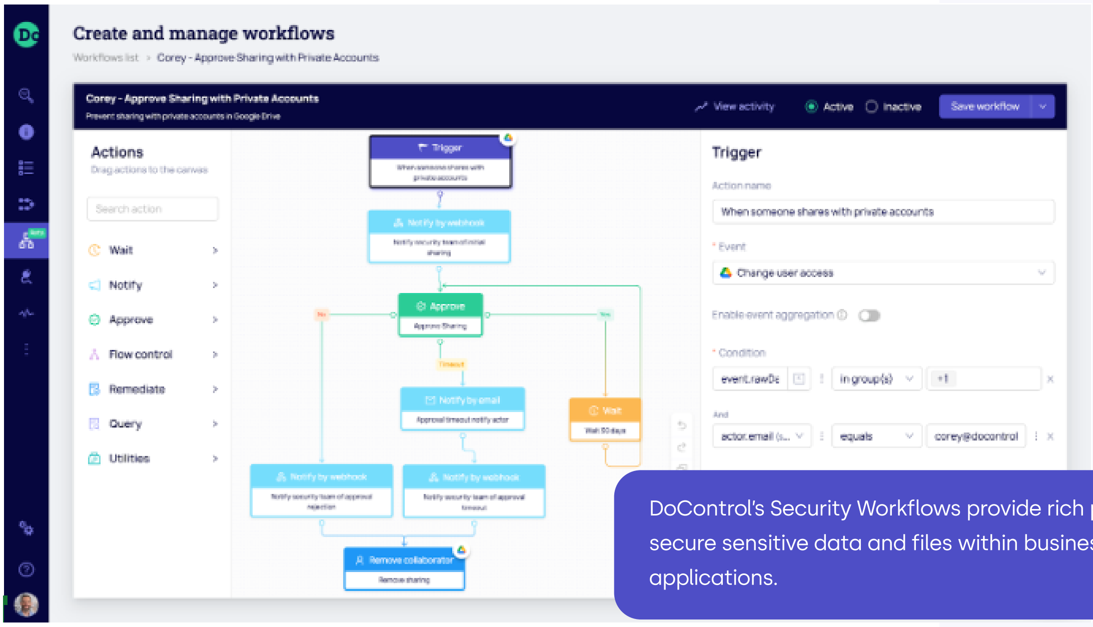
In today's environment Software as a Service (SaaS) applications dominate cloud services, and have become the preferred method in driving business enablement for modern organizations (i.e. Microsoft O365, G-Suite, Salesforce, Slack, etc). CASB solutions initially improved visibility by addressing the challenges associated with Shadow IT, but a new threat vector has emerged with the proliferation of integrated third party applications (i.e. OAuth applications). Modern businesses require a scalable solution that provides the ability to first understand every business critical application and file within the estate, and then be able to implement granular access control policies that aid in the prevention and exfiltration of sensitive company data in real-time.

The Solution

DoControl secures sensitive data and files within SaaS applications through a combination of data access prevention and detection controls. The solution provides strong visibility throughout the IT estate for both sanctioned and unsanctioned cloud applications, continually assesses and exposes cloud application risk, and provides both manual and automated remediation to reduce risk, and support stringent compliance requirements involving cloud governance and access to sensitive data.

Benefits

1. A lightweight, agentless solution that is enterprise-ready and integrated easily with existing technology stacks
2. Strong visibility of every identity, entity and activity with the SaaS estate to continually assess and evaluate risk
3. Centrally enforce granular access control policies to secure sensitive data and files
4. Business-context aware alerting and enforcement to pinpoint material risk within complex SaaS environments
5. Meet stringent compliance requirements that require proper cloud services governance and data protection



Create and manage workflows

Workflows list > Corey - Approve Sharing with Private Accounts

Corey - Approve Sharing with Private Accounts

Prevent sharing with private accounts in Google Drive

Trigger

Action name: When someone shares with private accounts

* Event: Change user access

Enable event aggregation ○

* Condition: event.rawDa | in group(s) | +1

And: actor.email (s... | equals | corey@docontrol

DoControl's Security Workflows provide rich policy enforcement to secure sensitive data and files within business-critical SaaS applications.

How It Works

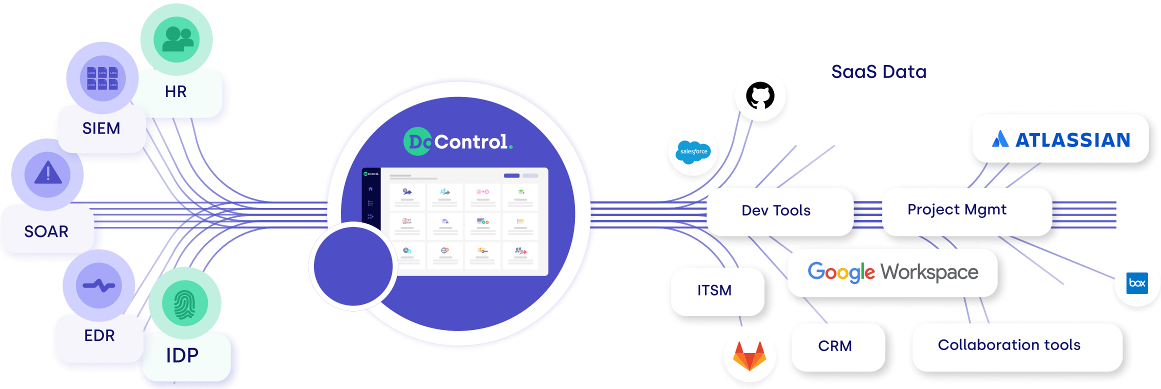
DoControl integrates with business-critical SaaS applications via APIs and webhooks to expose every SaaS user event and data activity within the environment. Known and unknown threats are prevented in real-time through data access control policies, and detected high risk anomalies can also be addressed manually via self service tooling. There are no agent installations, inline redirections (i.e. proxies), or slow API response times that negatively impact the end user experience.

DoControl leverages SaaS metadata as sources and extracts the business-context of each event, allowing for granular data access policies to be orchestrated and initiated consistently across disparate application environments. DoControl exposes the entire API of the SaaS application, allowing the conditions/actions and workflow policies to be set based on any event within the application. DoControl's low-code no-code platform enables IT and security teams to create policies from a centralized control point in a simple and easy way.

Visibility: DoControl provides strong visibility throughout all business-critical SaaS applications and data (i.e. publicly exposed assets), being utilized by every internal and external entity. For all OAuth applications, DoControl can understand which applications are installed, including all sanctioned and unsanctioned apps. The visibility provided exposes potential data access risks, and enables security teams to monitor all SaaS user and data activities and take appropriate action to remediate threats.

Protection: DoControl provides self-service remediation capabilities to take immediate action against detected threats as well as automated, near real-time remediation intervention workflow policies to prevent high-risk or malicious activity. DoControl's Security Workflows provide the ability to define and implement consistent access control policies across all disparate applications within the environment. The combination of self-service and automated remediation help aid in the prevention of sensitive data from becoming overexposed or exfiltrated.

Compliance: DoControl helps provide support for compliance with regional mandates (i.e. General Data Protection Regulation (GDPR)), industry standards (i.e. Payment Card Industry (PCI) Data Security Standard (DSS)), as well as organizational policies that require proper cloud services governance and secure access to sensitive data and files. DoControl provides secure collaboration and sharing of sensitive company information (i.e. data classification and file-scanning for PII, PCI and PHI) to both maintain a strong security posture, as well as avoid non-compliance with regulations, standards and organizational policy.



DoControl SaaS Data Security

DoControl provides foundational data access controls to prevent the loss of sensitive data within business-critical SaaS applications. The solution intelligently exposes every event within the SaaS estate to provide complete visibility into the environment. Security teams can enable granular intervention workflows applied consistently throughout disparate applications. Compliance and risk management teams can meet stringent requirements involving access to sensitive data and cloud services. Strengthen your data access security program today by partnering with DoControl.

For more information, please visit www.docontrol.io