DoControl Cloud Data Loss Prevention (DLP)

The Challenge

Data loss prevention (DLP) tools and processes aim to prevent sensitive data from becoming lost, misused, or accessed by unauthorized users. Traditional DLP programs are struggling to achieve desired outcomes due to the natural evolution of how sensitive data and files are accessed, manipulated, and shared. Every flavor of "as a Service" offering has been increasingly adopted to enable businesses to become more agile. In the process, the IT estate has become significantly more complex, making traditional approaches to DLP less effective. The end result is a high-maintenance program that overwhelms teams with a significant amount of false positives and repeat offenders on a daily basis; taking time and focus away from security events that present material risk to the business.

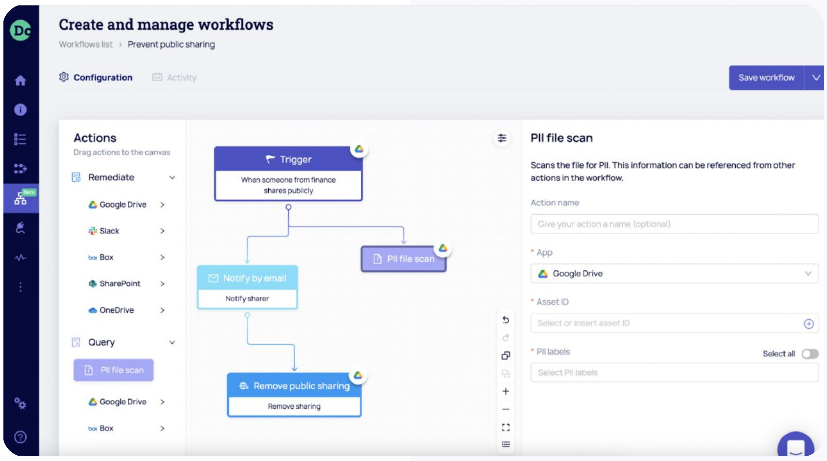
Software as a Service (SaaS) applications are a critical egress channel for modern businesses that are often outside the scope of traditional DLP programs. To help drive business enablement, organizations leverage multiple content and collaboration tools (i.e. Google Drive, Microsoft OneDrive, Box, and Slack). Data is both created and exchanged by internal and external users within these applications, which makes preventing the loss and misuse of sensitive data a challenge at scale. Today, there is more data to steal and more places to steal it from. Modern businesses require a scalable solution that provides secure access to sensitive files and prevents intentional or accidental data loss within SaaS environments.

The Solution

DoControl Cloud DLP provides granular access controls that detect and prevent the loss, leakage and misuse of sensitive data within business-critical SaaS applications. Organizations pursuing a cloud-first strategy can now consistently secure access to sensitive files and data, both at rest and in motion, throughout the disparate applications being utilized by the business. Data that contains Personally Identifiable Information (PII), Protected Health Information (PHI), and Payment Card Industry (PCI) information is automatically scanned throughout all structured, semi-structured and unstructured data within the SaaS application estate. All sensitive data is identified, and the risk of data exfiltration or leakage is remediated automatically through the combination of rich end-user behavioral analytics and dynamic DLP policy enforcement.

How It Works

DoControl extensively monitors all SaaS data movement in real time, and automatically creates relationship graphs to track communication patterns. Sensitive data is discovered and scanned in parallel, classifying the files and content types that are relevant to each organization. Secure workflows are established and triggered automatically by events that present a risk of data loss. The business context for each identity and asset is aggregated, providing



Create and manage workflows

Workflows list > Prevent public sharing

Trigger: When someone from finance shares publicly

Notify by email: Notify sharer

Remove public sharing: Remove sharing

PII file scan

Scans the file for PII. This information can be referenced from other actions in the workflow.

Action name: Give your action a name (optional)

* App: Google Drive

* Asset ID: Select or insert asset ID

* PII labels: Select PII labels

DoControl's Security Workflows enable dynamic DLP policies to be enforced consistently throughout SaaS environments to prevent the loss of sensitive data.

Benefits

1. High-impact, low-maintenance solution to prevent the loss, leakage and misuse of sensitive data within business-critical SaaS applications
2. Centrally enforce dynamic DLP data access control policies to reduce the risk of data exposure
3. Rich end-user behavioral analytics to help prevent the risk of malicious insiders from exfiltrating sensitive company data
4. Streamline incident response efforts through an exhaustive audit trail of end-user SaaS events and activities
5. Enforce data-handling controls and measures that comply with data protection and privacy regulations

more accurate alerting and clearer remediation paths. By leveraging the business-context, DoControl provides full visibility and insight into which actions present actual risk, versus events that are standard business practice.

DoControl Cloud DLP Provides The Following Essential Capabilities:

Manage: DoControl provides the foundational technology and process requirements to manage a high impact, low maintenance DLP program. Security teams can define enterprise data usage policies, report on policy violations, and implement secure workflows on a low code/no code platform that automatically prevent the exfiltration of data. DoControl is a completely event-driven platform that leverages SaaS application metadata as sources, allowing security teams to better understand when data is at risk within their SaaS environment. The solution helps streamline incident response efforts by providing a deep audit trail of both internal user and external collaborator activities, detecting anomalies and high-risk SaaS events, as well as both automated and self-service remediation.

Discover: DoControl's sensitive data scanning service is a natural-language processing (NLP) tool that uncovers valuable insights and connections through machine learning. The scanning service processes text within cloud application files and documents to extract key phrases, entities and sentiment which can then be further analyzed. Files and documents are automatically scanned throughout all structured, semi-structured and unstructured data types. Organizations can protect and control who has access to data by identifying and redacting sensitive information. Security teams can classify the sensitive information that is relevant to their business, and from there create dynamic DLP policies through DoControl's Security Workflows engine. The combination of DoControl Cloud DLP's file-scanning and data access workflows enable organizations to adhere to stringent compliance and regulatory requirements.

Monitor: The DoControl analytics service provides security teams the context to distinguish which activities are "trusted" and which present a risk of data loss. Every SaaS interaction is tracked and monitored, and a baseline of "normal" activity is established for each individual user. Any deviations from that baseline or indicators that present a risk of data loss are detected and blocked. The DoControl analytics engine combines past end-user behavioral patterns with deterministic behaviors to prevent malicious insiders from exfiltrating business-critical data. Sensitive files are automatically isolated in the event of unauthorized access attempts. DoControl's data access anomalies can also be fed directly into existing SIEM/SOAR technologies and correlated with other detections for a more holistic view of DLP security events.

Protect: Dynamic DLP policies can be implemented across any application or use case, providing a more effective and targeted DLP strategy that minimizes false positives. Security teams can take a "risk-based approach" to DLP by applying specific policies to groups, domains, and individuals based on risk. Access can be provided and revoked on-demand, and the principle of least privilege can be enforced at scale via DoControl's Security Workflows. Triggered by hundreds of SaaS event types, Security Workflows enable consistent, granular, and customizable data access controls to protect sensitive data and address an unlimited number of DLP use cases. Policies can be configured to distribute automated notifications via Slack, Microsoft Teams, or email to alert specific personas (i.e. security teams, business line managers, or individual actors) on policy violations. Overtime, DoControl will intelligently recommend policies to empower security teams to fine-tune their DLP workflows.

DoControl Cloud DLP

DoControl Cloud DLP provides next-generation data loss prevention throughout business-critical SaaS applications. The solution monitors all sensitive SaaS application data activity, performs end-user behavioral analytics to prevent insider threats, and automatically initiates secure workflows to prevent the loss, leakage, and misuse of sensitive company data. DoControl Cloud DLP provides security teams with the foundational components, both technology and process, to create effective DLP programs within SaaS environments. Strengthen your DLP program today by partnering with DoControl.

For more information, please visit www.docontrol.io