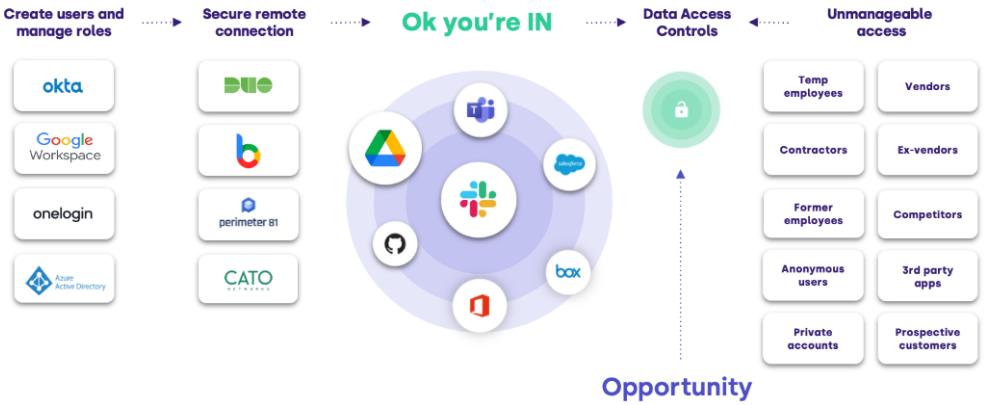
Automate and Scale Software as a Service (SaaS) Data Access Controls

Do You Know Who Has Access to Your SaaS Data?

Modern businesses leverage identity providers (IdP) to manage users and permissions, as well as Zero Trust Network Access (ZTNA) solutions to secure remote access to systems and applications. From there, internal users and external collaborators connect to SaaS applications to drive business enablement. But this also creates significant data security risks that can stem either from within your company or from outside your security perimeter.

Knowing "who has access" and "to what" is a challenge at scale when you consider the high number of applications and users, coupled with the volume of events that are generated. SaaS applications offer very different native data access controls that are completely uncorrelated. The complexity of business needs and requirements that are introduced cannot all be quantified by Security teams. The end result is a high amount of lingering, unmanageable data access that poses significant risk to your organization and increases the likelihood of a data breach.



DoControl Automatically Identifies And Remediates SaaS Data Access Threats

Insider Threats

- Malicious insider performs a mass download before leaving the company
- Negligent insider shares sensitive data over a public link in Slack or Teams channels
- Encryption keys and production credentials uploaded to a shared drive

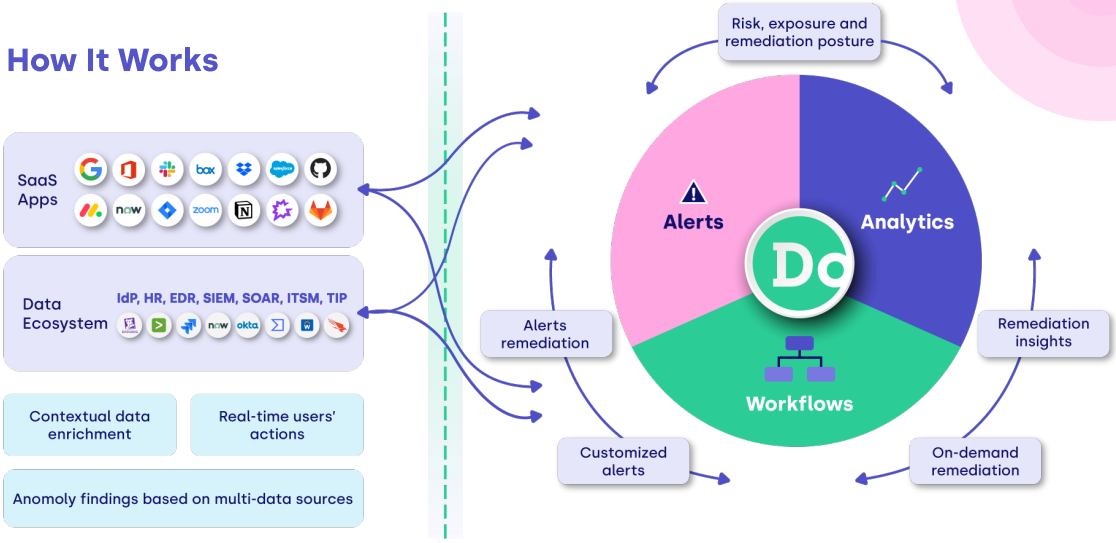
External Threats

- Sensitive data shared publicly to anyone with a link
- Critical data shared with personal accounts
- 3rd-party users share with 4th-party users
- Former vendors retain data access

Key Benefits

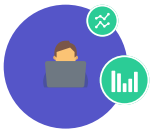
1. Improve business productivity by enabling collaboration through SaaS applications while lowering the risk of data exfiltration or leakage.
2. Gain full visibility into users (both internal and external), groups, domains, assets, and third-party OAuth applications.
3. Implement risk-based granular data access controls – by individual, role, application, or domain – to minimize the risk of data breaches.
4. Automate the application of dynamic security policies through workflows designed to improve operational efficiencies of IT and Security teams.
5. Demonstrate and report on compliance requirements of relevant regulations while lowering corporate liability risk.

How It Works



DoControl is an agentless No-Code SaaS Security Platform that secures sensitive data and files within business-critical SaaS applications. The solution is an event-driven platform that leverages APIs and webhooks to integrate with SaaS applications, aggregates all relevant metadata sources, and enables Security teams to create granular data access control policies to reduce the risk of data overexposure and exfiltration. DoControl provides full asset management and visibility into the SaaS estate by creating a complete inventory to include users, groups, domains, assets, and third-party OAuth applications. The solution extracts the business-context of every SaaS user interaction and activity to drive the following key product capabilities:

Alerts: DoControl provides sophisticated, cross-system and application anomaly and exposure calculations; with full customization alerting based on risk to minimize false positives and streamline incident response efforts. Security teams can apply a risk-index to events and activities that present material risk to the business. Detected anomalies generate real-time alerts which are displayed into the console, or can be redirected to SIEM/SOAR solutions.



Analytics: DoControl performs end user behavioral analytics to gather insights throughout all identities and entities connecting to business-critical SaaS applications. Behaviors are collected and normalized, Security teams can then monitor and control all user activities in real time, and SaaS-related threats are detected and remediated automatically.

Workflows: DoControl provides granular data access control policies via Security Workflows. Security teams can streamline secure automated workflows via a no-code, "drag-and-drop" platform to close the gap on existing SaaS application vulnerabilities and risks through automated, self-service remediation. A wide range of data access control use cases can be addressed through the event-driven nature of the DoControl platform.

Each of these key product capabilities are interconnected, providing intelligent and actionable insights. For example, attaching automated remediation to a specific alert type; the alert will trigger a Security Workflow, or the Workflow can create a customized alert. DoControl provides the necessary foundational data access controls for organizations to drive their business forward in a secure way.

About DoControl

Founded in 2020 and headquartered in New York, DoControl is an automated data access controls platform for SaaS applications, improving security and operational efficiency with ease for enterprises. DoControl is backed by investors Insight Partners, StageOne Ventures, Cardumen Capital, RTP Global and global cybersecurity leader CrowdStrike's early stage investment fund, the CrowdStrike Falcon Fund. The company's leadership team combines product, engineering and sales experience across cybersecurity, enterprise and SaaS innovators. For more information, please visit www.docontrol.io. Follow us on Twitter and LinkedIn.