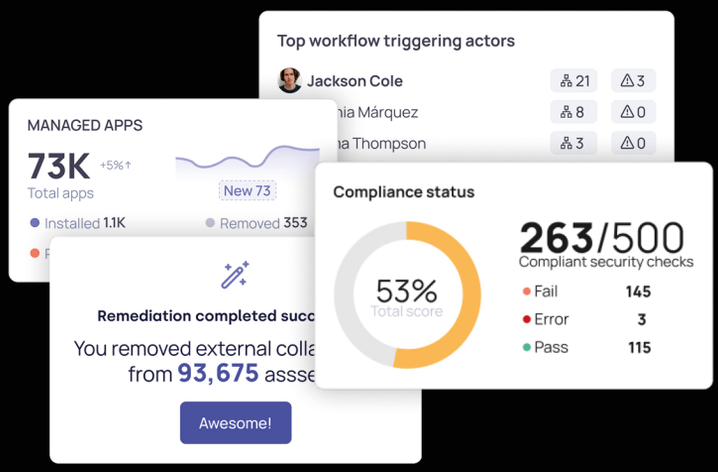
DoControl.

Multi-Layer Defense for SaaS Applications



DoControl secures SaaS data, identities, connected apps & configurations to prevent sensitive data exposure and mitigate insider threats.

DoControl SaaS Security Posture Management

Data Access Governance

- Discover, catalog, and visualize all your SaaS data
- Understand data classification, usage, and exposure levels
- Control data access with automated remediation

Identity Threat Detection & Response

- Aggregate all user data into a single identity posture
- Analyze and benchmark identity risk profiles
- Detect and respond to suspicious user activity

Shadow App Discovery & Remediation

- Discover all used and unused third-party apps
- Assess risk levels of over-permissioned, malicious and dormant apps
- Suspend or remove suspicious or unnecessary apps

SaaS Misconfiguration Management

- Evaluate security configuration posture and risk levels
- Check compliance against relevant standards and company policy
- Implement recommendations to remediate misconfigurations

DoControl.

Why DoControl?

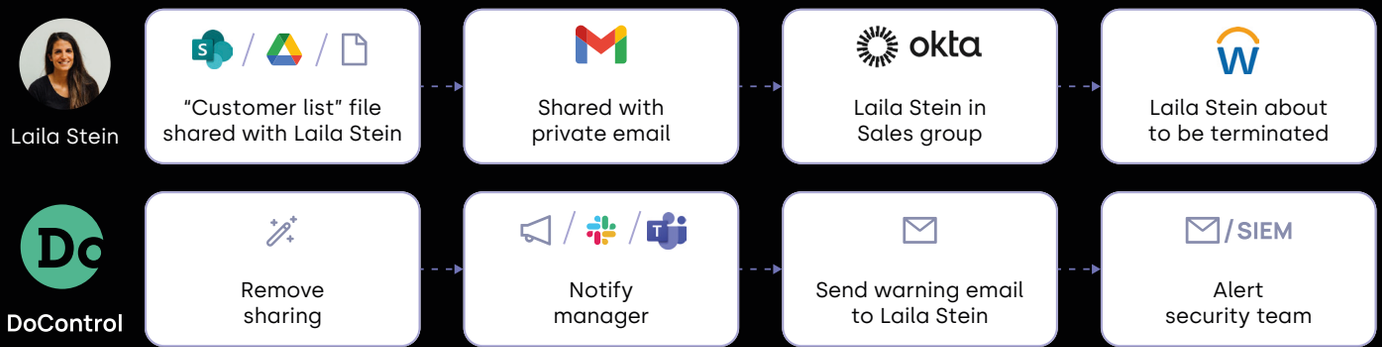
Event-based architecture ensures accurate, fresh SaaS data inventory and real-time detection of threats

Multi-context enrichment from your IdP, HRIS, and EDR enables a risk-based approach, eliminating false positives and alert fatigue

Granular security workflows allow for automated enforcement per application and use case, with no impact on productivity

End-user engagement helps to remediate risky actions, saves time and resources, and educates employees for secure collaboration

How DoControl Works



Trusted by Top Industry Leaders

CROWDSTRIKE databricks DATADOG carta VISTA

grammarly VOXMEDIA unqork EQT KKR

"DoControl is one of the most important parts of our cyber security program. DoControl helps us make sure we know where our data is, who is accessing it, and why".

Mark Jaques, Director of Information Security at VoX Media