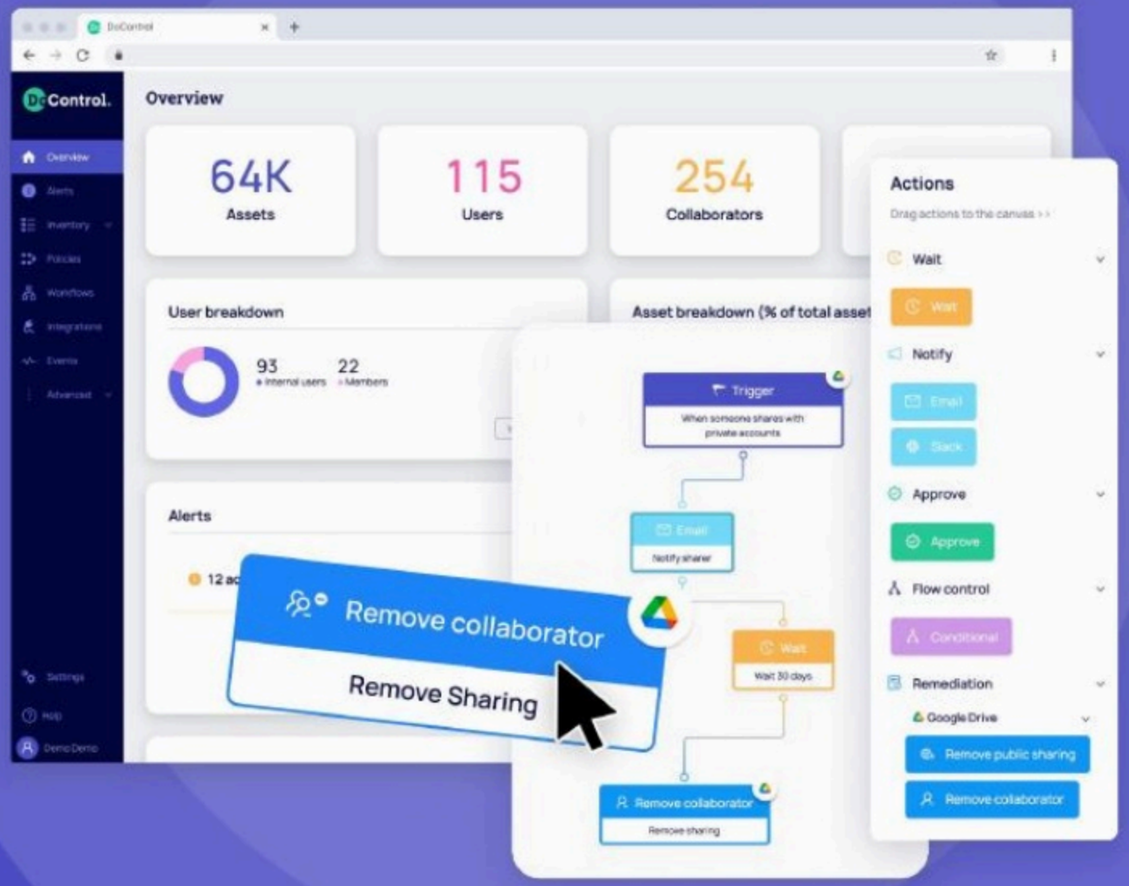
DoControl.

DoControl: No-Code SaaS Security Platform

Modernizing DLP and CASB to Secure SaaS Data



The Current State of SaaS

SaaS Growth:

Industry analysts estimate that the SaaS market will grow by more than 20 percent annually, reaching nearly **$200 billion by 2024,** a level that would represent nearly one-third of the overall enterprise-software market.

How Many Apps?

The average number of applications deployed by larger organizations (2,000 employees or more) is

187

At What Cost?

The average cost of a data breach in 2021 came in at

$3.86M

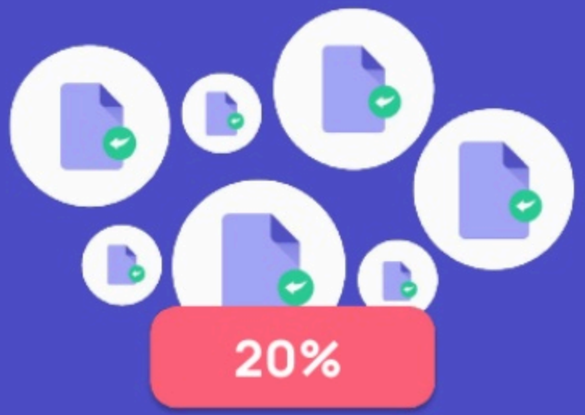
3rd Party Risk

The average company works with approximately 583 vendors. 53% of organizations have experienced at least one data breach caused by a 3rd party, with the breach costing an average of

$7.5 million to remediate.

Data Access Risk Exposure Runs High

Do you know who has access to your data?

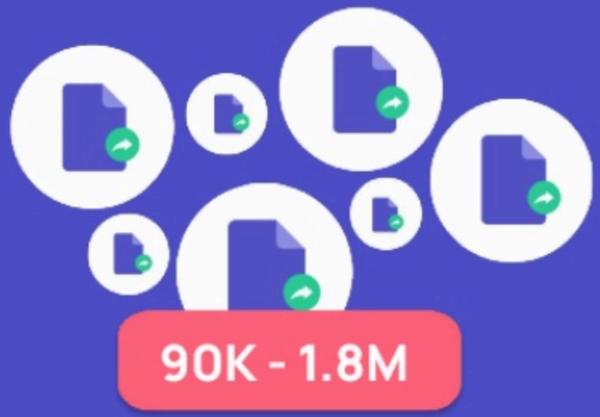


20%

ASSETS SHARED INTERNALLY

15K

EXTERNAL COLLABORATORS



90K - 1.8M

ASSETS SHARED EXTERNALLY

3K

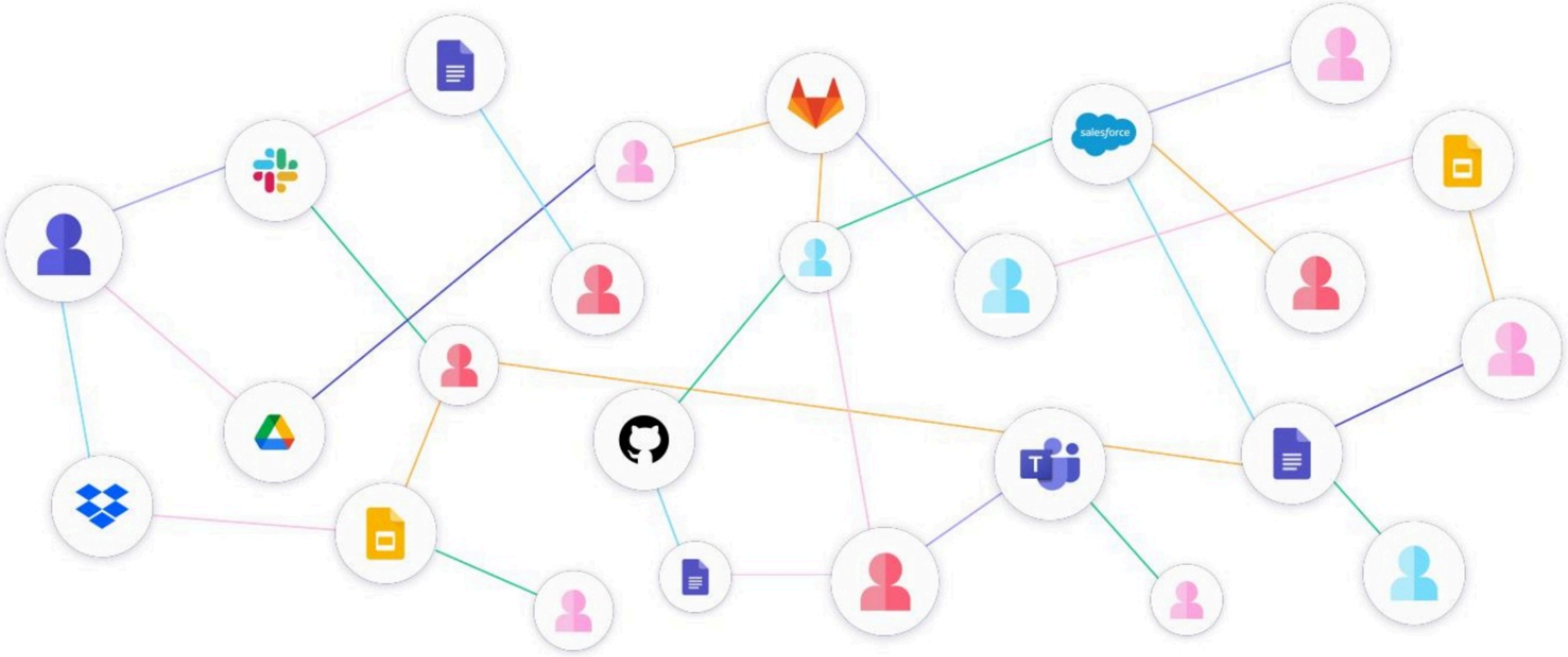
THIRD PARTY COMPANIES

10M

ASSETS IN SHARED APPS

DoControl.

Risk Scales In-line with SaaS Utilization



How it's Addressed Today

SaaS Native

Decentralized, inconsistent controls and does not scale

CASB

Inconsistent and non-granular remediation

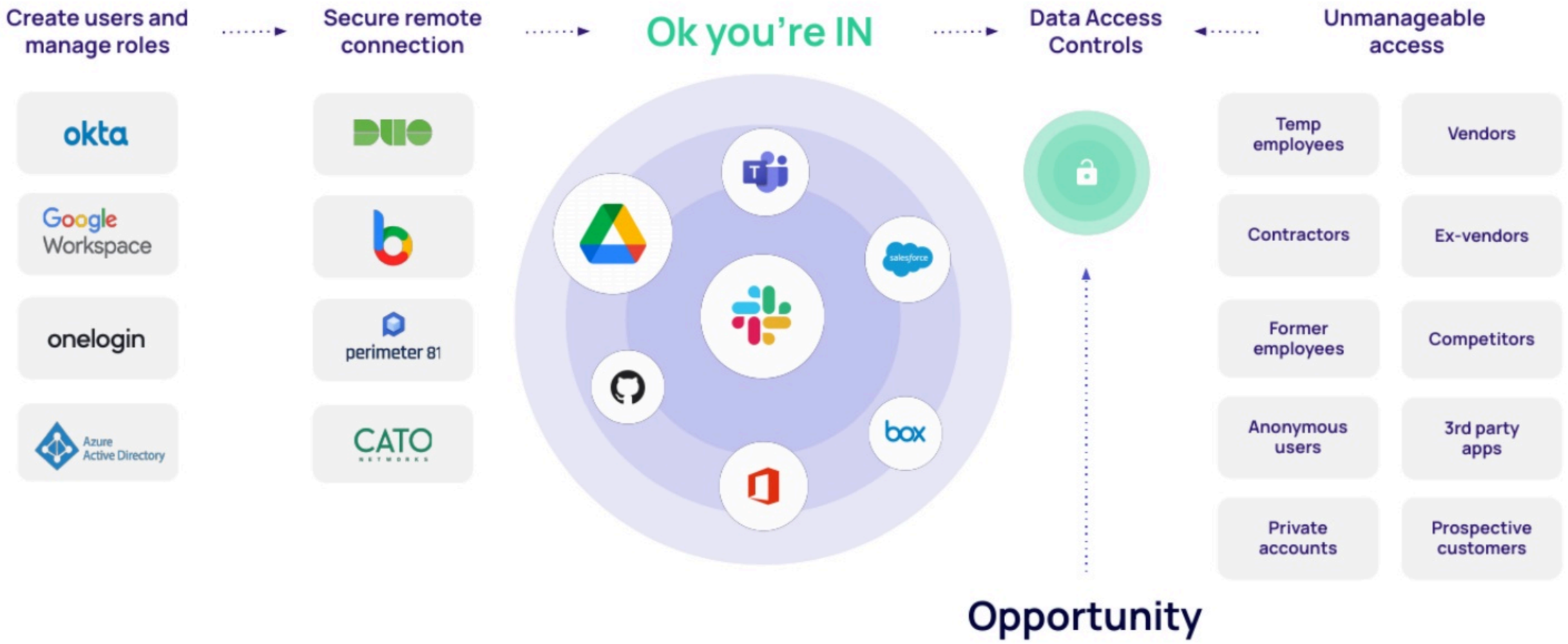
DLP

Full-blown PII scanning creates alert fatigue

SSPM

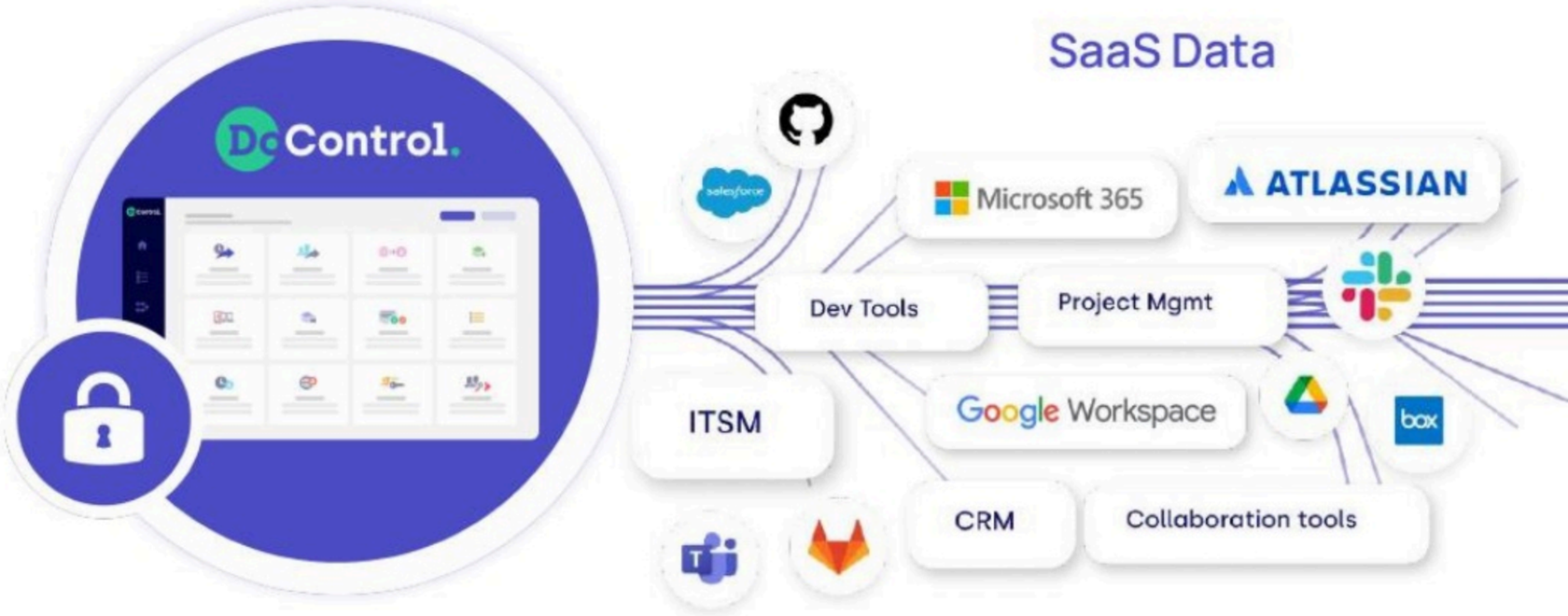
Security mis-configuration focused, no data access risk remediation

The Opportunity for DoControl



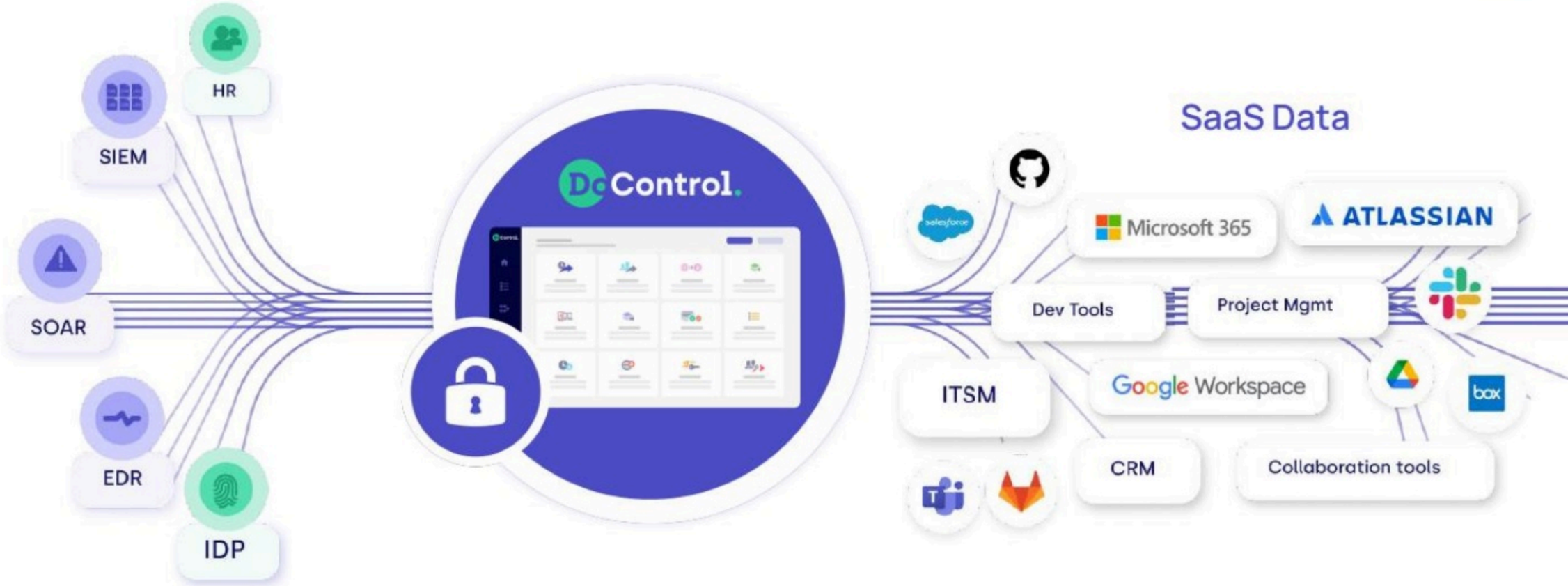
The DoControl Platform

SaaS Apps as Metadata Sources

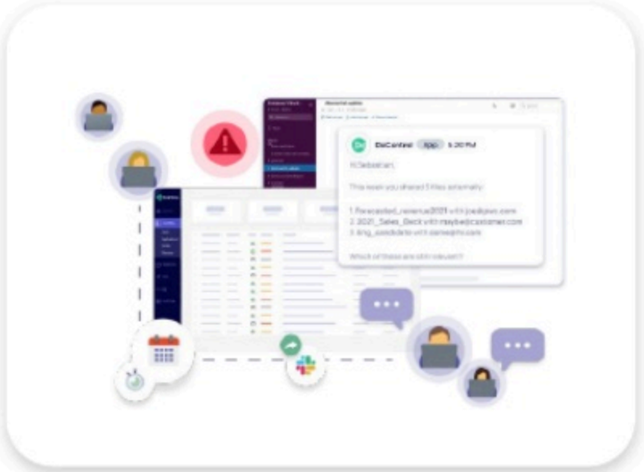


Value-add to Existing Security Investments

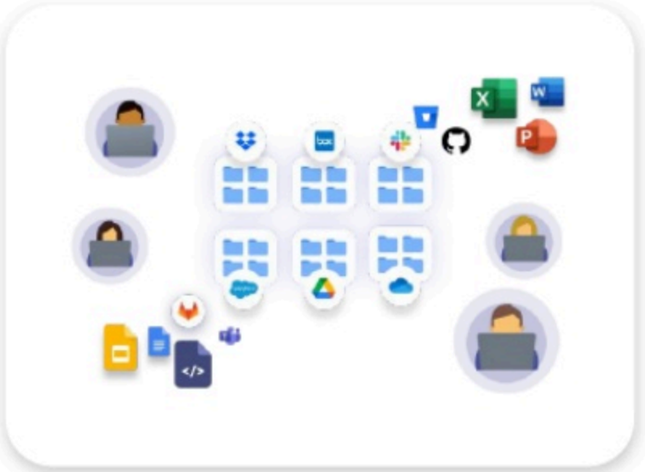
Foundational Data Access Controls for SaaS



The DoControl Platform



Visibility
and Control



Continuous
Monitoring

Automated
Remediation

Enforce consistent data access security from a single control point

DoControl.

Data Loss Prevention (DLP)

The Problem

Cloud-based, collaborative work has become a pillar of modern business, and security teams need a comprehensive strategy for detecting and preventing the loss, leakage or misuse of sensitive company information stored across disparate SaaS applications. Traditional DLP vendors perform only broad data scanning, which inundated security teams with false alarms.

The Solution

- Targeted file scanning (PII, PCI, and PHI) across all structured, semi-structured and unstructured data types
- Rich user behavioral analytics that combine past end-user behavioral patterns and deterministic behaviors to mitigate the risk of insider threats
- Dynamic DLP policy enforcement across critical SaaS applications to minimize false alarms and provide for a more effective and targeted approach to DLP

Third-party Vendor Management

The Problem

It is standard business practice to collaborate on projects with external users such as vendors, partners, and customers, but in most cases revoking SaaS data access for these third-party users is forgotten at the end of a business exchange. Manually deprovisioning access and removing files after projects are completed becomes a strain on security and IT resources.

The Solution

- Create custom security workflows to automatically revoke external access after a predetermined time period
- Enable business users to provision and deprovision access to approved third parties on-demand
- Restrict third-party collaborators from sharing your SaaS-hosted data with unapproved fourth parties, such as their own vendors or personal accounts

Establish Automated Remediation

The Problem

In high-risk situations, security teams need to act quickly to remediate data access issues and prevent data exfiltration before irreparable damage is done. Remediation actions are often performed manually across different SaaS applications, which is not operationally efficient and increases the time to response.

The Solution

- Centrally enforce comprehensive data access workflows throughout complex SaaS application environments
- Trigger automated workflows based on high-risk SaaS events and activities
- Leverage out-of-the-box workflows or create customizable workflows to meet specific security requirements

Automate Access Workflows

The Problem

Security teams receive constant alerts for suspicious user activity across the SaaS environment, but they lack the business context from an end-user perspective to determine whether an action is legitimate or problematic. Security teams must manually query users to understand their business needs and adjust access accordingly. This process is both labor-intensive and creates unnecessary interactions between security teams and business users.

The Solution

- Leverage out-of-the-box workflows to immediately address deviations with appropriate end-user behavior across common user actions (share, download, etc.)
- DoControl Slackbot triggered by customizable workflows inquires directly with end-users
- Users can approve, reject, or ignore the Chatbot interaction to prompt the workflow's next-step action as defined by the DoControl administrator (i.e. delete files, revoke access)