DoControl.

Achieving a Zero Trust Data Access Security Model with DoControl

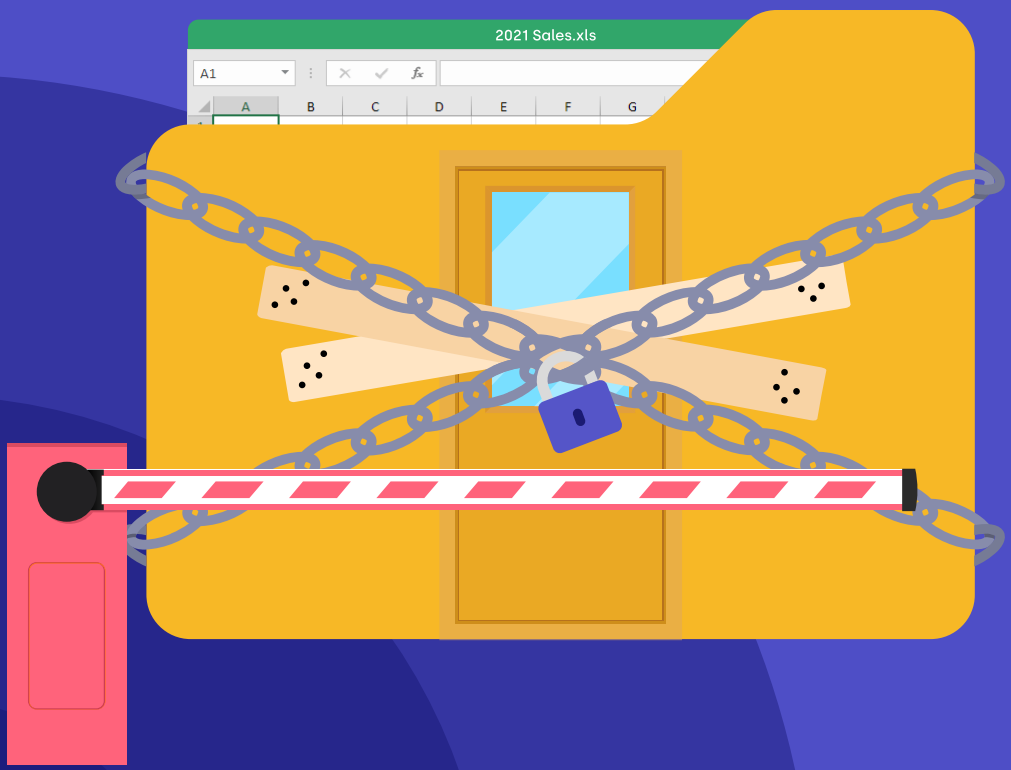


Table of Contents

03 The Next Phase of Zero Trust

04 Zero Trust Data Access (ZTDA)

05 The Three Core Pillars of ZTDA:

- 05 Continuous Monitoring
- 06 Least Privilege
- 07 Automation

08 Extending Zero Trust to the SaaS Application Data Layer

09 About DoControl

The Next Phase of Zero Trust

Zero Trust has become the industry standard approach for enabling the business in today's fluctuating working environment that mitigates the risk of cyber attacks. The vast majority of organizations have adopted this approach, and have executed on their Zero Trust strategies of "never trust, always verify."

The initial components within a Zero Trust Architecture were focused on micro segmentation and micro perimeters. Overtime, as the "traditional" perimeter dissolved, "identity" has become the new perimeter.

Organizations turned to identity providers (IDP) to enforce least privilege via permissions and entitlements based on each identity's role and responsibilities. Next, they provided access to users and identities in a secure way through a Zero Trust Network Access (ZTNA) solution, brokering a secure access pathway from any device, from any location.

Modern organizations need to incorporate a new critical guiding principle that goes beyond the identity, network, and device levels to achieve a more comprehensive Zero Trust strategy.

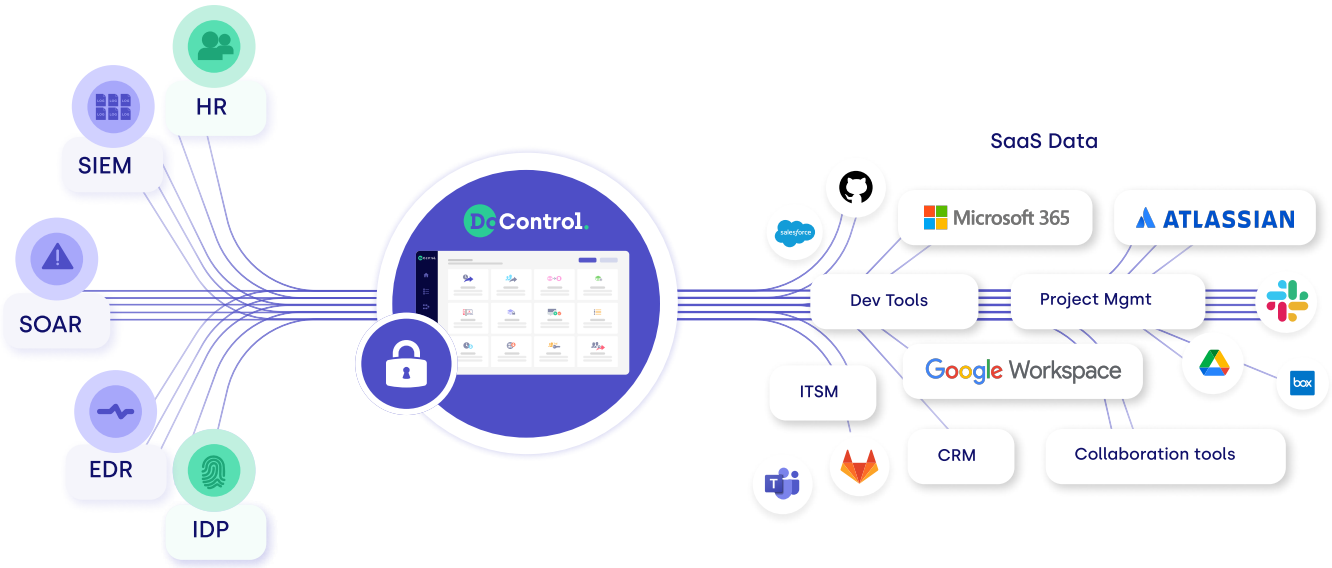
Zero Trust Data Access (ZTDA)

Zero Trust Data Access (ZTDA) takes the principle of least privilege and the concept of micro segmentation and extends it throughout Software as a Service (SaaS) application environments, which are one of the most critical data sources for an enterprise trying to align to the Zero Trust model.

ZTDA is a new guiding principle that provides the granularity required to assume implicit trust is not granted to any user inside or outside the organization, beyond the identity layer and deeply ingrained into the SaaS application level.

The DoControl ZTDA solution provides continuous monitoring of all user activities and events, least privilege data access control policy enforcement at scale, and workflow automation to remediate risk both through manual intervention as well as in an automated fashion. This allows for more targeted security policies to be applied to end users and entities, both internal and external, across all SaaS applications that are interacted with.

ZTDA moves security closer to critical resources that drive the modern business forward.



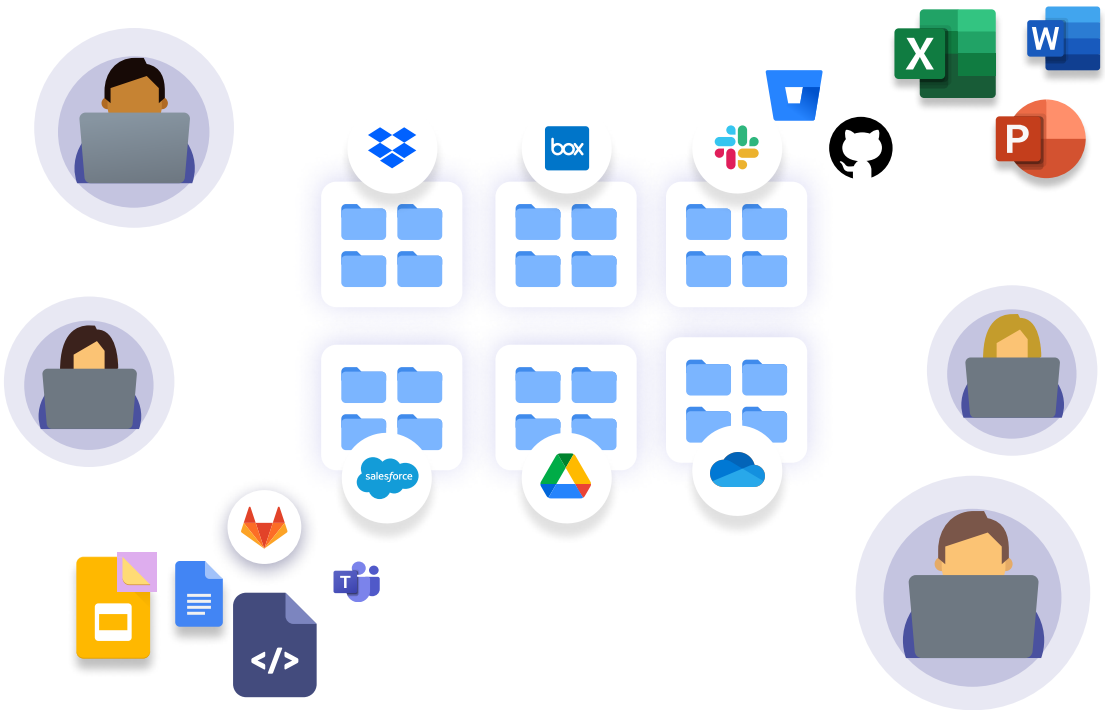
DoControl ZTDA delivers foundational controls that provide visibility across multiple SaaS platforms, continuous monitoring and anomaly detection, as well policy enforcement across all data access.

The Three Core Pillars of ZTDA: **Continuous Monitoring, Least Privilege, and Automation**

1 Continuous Monitoring

DoControl ZTDA is subscribed to all internal and external user activity events, SaaS assets metadata, and data enrichments across a wide range of interconnected integrations (i.e. IDP, Endpoint Detection and Response (EDR), and Human Resources (HR) platforms). All of these critical data points are collected and combined to enable deep micro segmentation across multiple levels – including users, assets, groups, employment status, domains, and many more. DoControl ZTDA keeps a real-time inventory of your SaaS ecosystems metadata without the need to actually replicate and store SaaS hosted data.

Aggregating all critical SaaS-app metadata sources provides a clear view of all identities and assets, both internal and external to the organization. This insight feeds into DoControl's ability to continuously monitor all SaaS application activity, adding a core prevention control to a Zero Trust program.



DoControl ZTDA provides continuous monitoring of data access within SaaS application for real-time visibility of any indicators of a compromise or data breach.

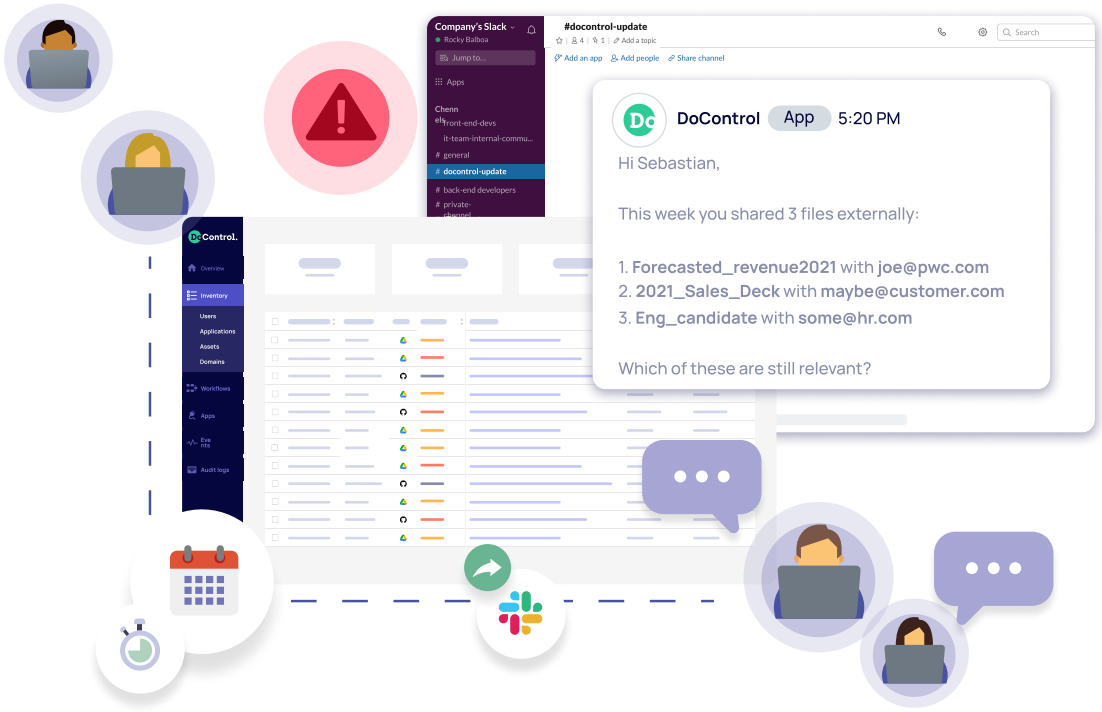
The Three Core Pillars of ZTDA: **Continuous Monitoring, Least Privilege, and Automation**

2 Least Privilege

Based on the unified inventory and data enrichments, DoControl ZTDA continuously revokes data access in real-time to both internal and external users to achieve the least privilege model at scale. Users in return can always share or request access in a "just in time" manner, to the very same data over and over so that business enablement continues as it should.

DoControl integrates with an organization's most critical business SaaS applications, and provides consistent and granular data access controls that can be easily customized and applied to different organizational departments synced from the HR SaaS application or idp solution.

Enforcing the principle of least privilege at the IDP layer is not enough to provide end-to-end protection. With DoControl, organizations will benefit from the granular data access controls and protection that is layered throughout the entire SaaS application environment.



DoControl ZTDA centralizes the enforcement of least privilege at scale, throughout an organization's entire estate of SaaS applications.

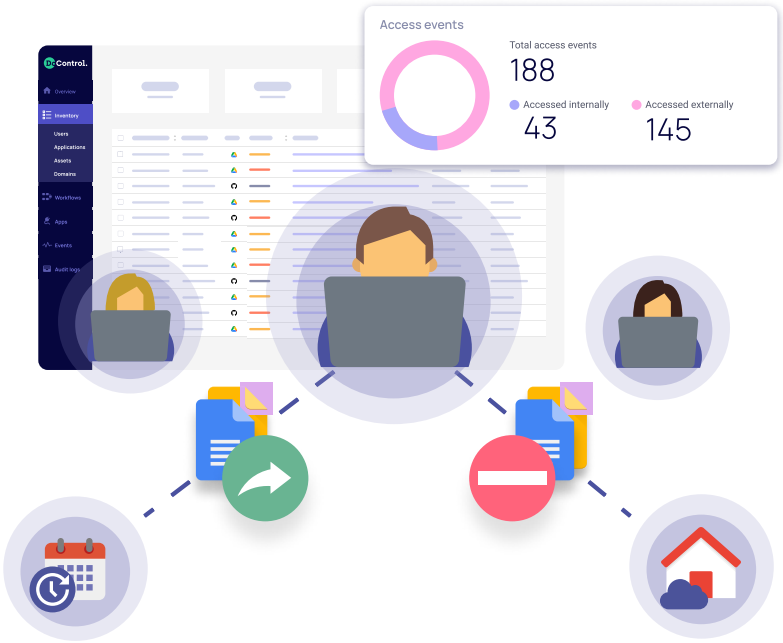
The Three Core Pillars of ZTDA: **Continuous Monitoring, Least Privilege, and Automation**

3 Automation

DoControl ZTDA offers automated workflows powered by comprehensive micro segmentation around users, collaborators, assets, groups, and more. These automated workflows are not opinionated or: hard coded but rather highly flexible and customizable to be triggered based on any end-user activity event and/or identified anomalous activity. The DoControl ZTDA solution offers a rich catalog of workflows – based remediation paths, either on-demand or fully automated.

DoControl consolidates and normalizes end-user activity events to provide a unified view of user behavior, and create an established baseline of what is considered to be "normal activity." From there, the solution runs anomaly detection mechanisms to automatically identify any deviations with the end-user normal behavior across common user actions such as share, download, delete, upload, etc.

DoControl ZTDA provides the automation required to effectively remediate risk both through manual intervention as well as in an automated fashion.



DoControl ZTDA provides automated secure workflows and risk remedation across complex SaaS application environments.

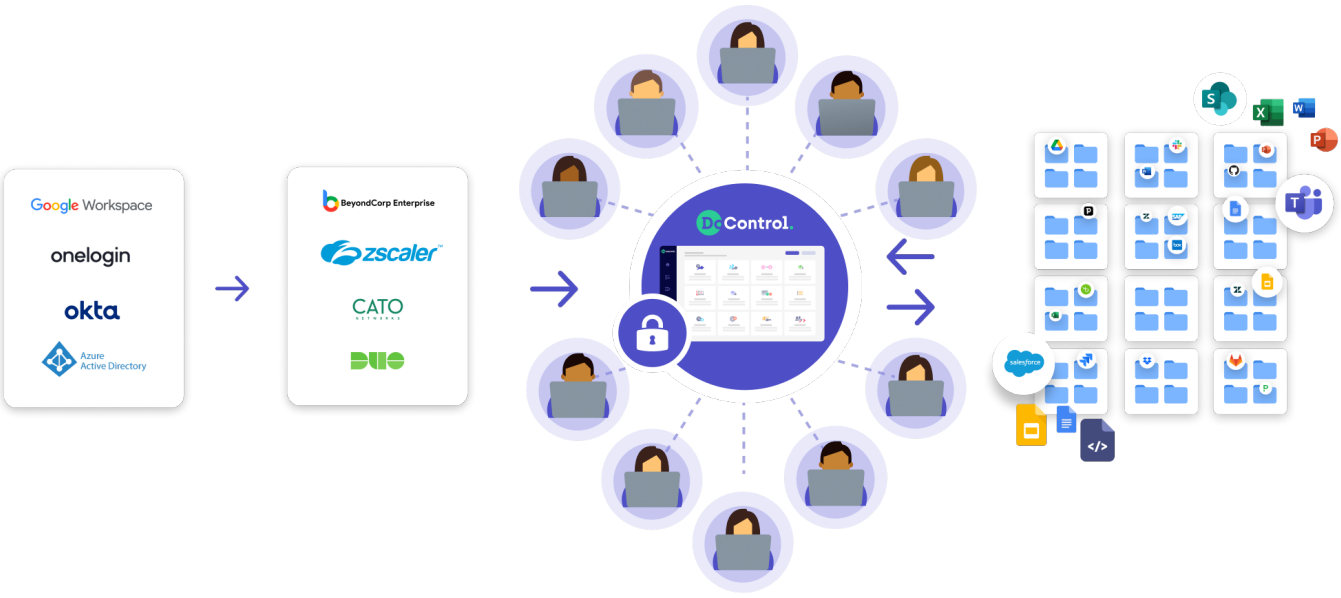
Extending Zero Trust to the SaaS Application Data Layer

DoControl provides a single security strategy that centralizes the enforcement of least privilege – beyond the identity, network, and device levels – throughout an organization's entire estate of SaaS applications. Existing SaaS application providers either lack these capabilities altogether or they lack the granularity required to be effective in preventing major breaches and data exfiltration. Relying on the native security capabilities of each individual SaaS application is ineffective and does not provide a consistent way to implement data access controls throughout all SaaS application types.

Attackers are going to get in. Insider threats are real. The DoControl ZTDA solution was architected with an "assume breach' mindset to prevent critical SaaS application data from inadvertently getting out. DoControl is able to trigger workflows based on any SaaS end-user activity event matched against rich micro-segmentation of users, collaborators, groups, assets, domains, and much more.

The solution provides continuous monitoring of all user activities and events, least privilege data access control enforcement at scale, and workflow automation to remediate risk both through manual intervention as well as in an automated fashion. The DoControl ZTDA solution adds a necessary layer of preventative controls to modern Zero Trust strategies.

Experience a more complete ZTA, and move the business forward in a secure way.
[Request a demo and get started today.]



About DoControl

DoControl helps organizations prevent data breaches in the most popular SaaS applications, and balance between security and business enablement. Founded by former Google Cloud Cybersecurity members, DoControl provides security teams the automated, self-service tools they need for data access monitoring, orchestration, and remediation within SaaS applications.

DoControl is backed by investors RTP Global, StageOne Ventures, Cardumen Capital 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 us here.