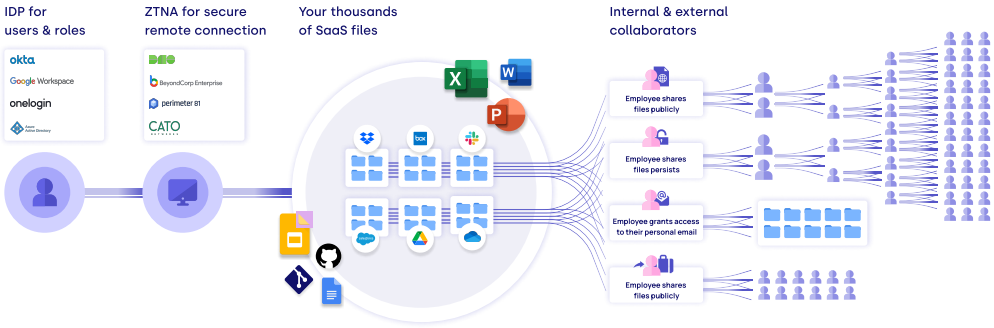
Zero Trust Data Access With DoControl

Extend Zero Trust to the SaaS Application Data Layer

The Challenge

The vast majority of organizations have bought into the concept of Zero Trust, and as such have adjusted their security programs to better align to this modern approach. Initially securing the identity layer via identity provider (IDP) solutions to establish the appropriate level of permissions and entitlements based on roles and responsibilities. Next, ensuring that the users and identities were brokered a secure connection via a Zero Trust Network Access (ZTNA) solution, to any corporate sanctioned resources from the devices they were accessing them from. Lastly, enforcing least privilege and Multi-Factor Authentication (MFA), and other tools and principles to effectively "never trust, always verify."

The challenge organization's are faced with is after bypassing these components, access to sensitive Software as a Service (SaaS) application data – and the files within these business critical collaboration and enablement tools – becomes increasingly insecure. Knowing "who has access" and "to what" is a scalable problem when considering the sheer number of applications being utilized across internal employees, contractors, 3rd party vendors (both current and former), among many other entities. The amount of access generated becomes unmanageable and the risk of overexposure to sensitive files and data runs high.



In order to mitigate this risk and enable business continuity in a secure way, modern organizations need to incorporate a new critical guiding principle that goes further down the stack. By introducing granular data access controls, organizations will improve their security posture and experience a more complete Zero Trust Architecture (ZTA) through deeper levels of security across the SaaS applications that drive the business forward.

The Solution

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.

The DoControl Zero Trust Data Access (ZTDA) solution provides full visibility across all SaaS access for every identity and entity (i.e. internal users and external collaborators) throughout the entire organization.

Continuous monitoring across all SaaS events and activities provides a baseline understanding of normal activity, and automatically identifies anomalous data access events. Granular data access control policies allow for consistent enforcement of least privilege access across the SaaS applications being leveraged by the organization.

Workflows are triggered automatically based on end-user activity that is matched against rich micro-segmentation of users, collaborators, groups, assets, domains, and much more.

Benefits

1. Enforce granular least privilege data access controls – by individual, role, application, or domain – to minimize the risk of data breaches
2. Improve business productivity by enabling collaboration through SaaS applications while lowering the risk of data exfiltration or leakage
3. Demonstrate and report on compliance requirements of relevant regulations while lowering corporate liability risk
4. Reduce the attack surface by ensuring company data is not exposed forever and/or to the wrong personnel
5. A complete lightweight and agentless SaaS application security solution that provides immediate time-to-value

How It Works

DoControl ZTDA is built on three core pillars: continuous monitoring, least privilege, and automation.

Continuous Monitoring: DoControl is an agentless solution that is completely event-driven, integrating with a broad array of SaaS applications via APIs and webhooks. By leveraging the applications being utilized as metadata sources, DoControl provides full visibility across the SaaS application estate as well as deep micro segmentation across multiple levels (i.e. users, assets, groups, employment status, domains, etc.). The events and business context captured by DoControl can then be fed into existing security tools and solutions, enhancing and adding value to those investments.

Least Privilege: DoControl continuously revokes data access in near 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. Enforcing the principle of least privilege to the SaaS application data layer allows for a more comprehensive approach to a Zero Trust model, providing deeper levels of preventative controls beyond the identity, device, and network levels. DoControl's granular data access control policies are easy to define and configure, and allow for the enforcement of least privilege throughout the entire SaaS application environment.

Automation: DoControl provides intuitive no-code workflows that are dynamic, customizable, and enable consistent security controls to be applied across all SaaS applications automatically. Secure workflows are triggered on any of the supported SaaS webhook events, providing greater flexibility to support existing security programs and broad coverage of various threat models. The solution runs detection mechanisms to automatically identify any deviations from the standard course of business. Depending on the severity of the event, notifications can be distributed to individual actors to take action, or IT and security teams can intervene as necessary, creating a strong balance between productivity and security. DoControl provides the automation required to effectively remediate risk both through manual intervention as well as in an automated fashion.

DoControl ZTDA

DoControl ZTDA takes the principle of least privilege and the concept of micro segmentation and extends it throughout SaaS application environments, which are one of the most critical data sources for an enterprise attempting to align to the Zero Trust model.

DoControl 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. Policies and secure workflows are applied to specific identities, events, assets, groups and domains that present different levels of risk to the organization; allowing for the principle of least privilege to be enforced at scale.

ZTDA moves security closer to critical resources that drive the modern business forward. Get started today and request a demo to see how the DoControl solution can improve your organization's approach to Zero Trust.

For more information, please visit www.docontrol.io