DoControl for Shadow Application Governance

The Challenge

Software as a Service (SaaS) applications are omnipresent for the modern business. Business users rely on these applications to drive business enablement, however security needs to be one step ahead in the proliferation of application adoption and utilization by business users. Application-to-application connectivity increases the threat vector by introducing machine identities that are often over privileged, unsanctioned, and not within the Security team's visibility. When machine identities become compromised they can provide unauthorized access to sensitive data within the application that it's connected to.

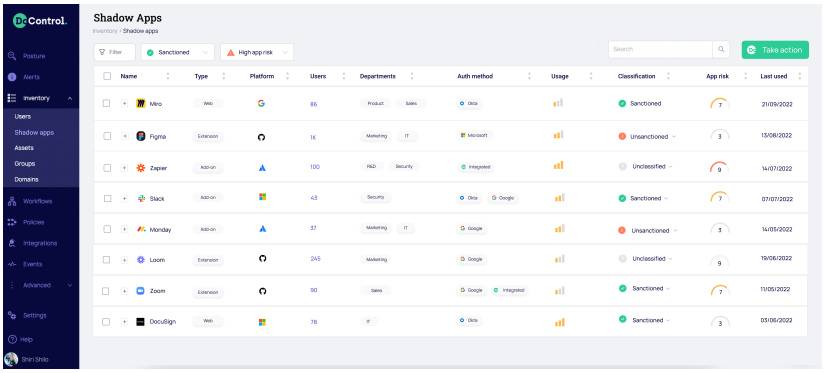
These "non-human" identities can gain permissions to read, write, and delete sensitive data – which can significantly impact an organization's security, business, and compliance risk. Supply-chain based attacks involving machine identities and their associated credentials are more common now than ever before. Modern businesses need to prevent the compromise of risky interconnected applications (i.e. unsanctioned, abandoned, vulnerable, malicious, and over privileged apps) in order to protect business-critical data with the SaaS estate. Organizations need to be able to establish full visibility, including all sanctioned and unsanctioned SaaS applications, and enforce strong governance controls that automatically close compliance gaps and remediate the risk supply chain-based attacks.

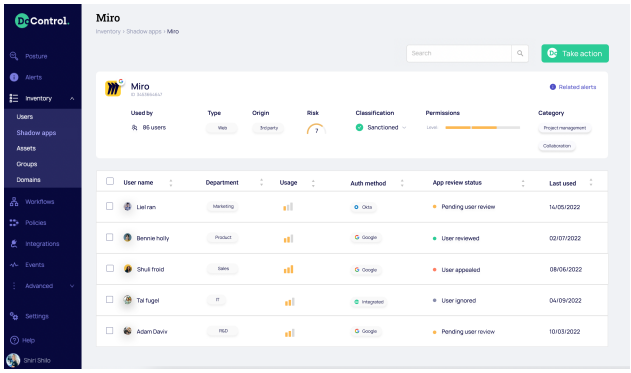
Key Benefits

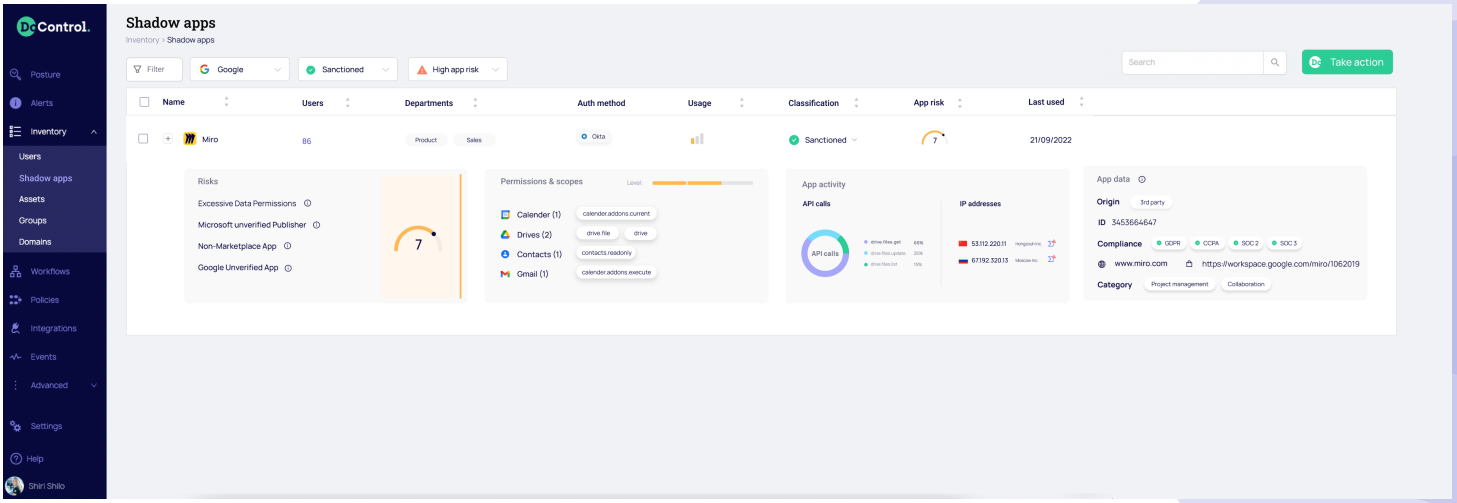
1. Gain end-to-end visibility through a comprehensive inventory of multiple SaaS applications and environments
2. Assess organizational posture through risk scoring and classification assignment across all business-critical applications
3. Establish pre-approval processes and workflows to onboard new applications through end user engagement
4. Reduce the attack surface through automated suspension or removal of potentially malicious applications
5. Alert on rogue, high-risk or vulnerable (i.e. excessive permissions or privileges) applications through smart analytics

The Solution

The DoControl SaaS Security Platform provides comprehensive Shadow Application governance through discovery, control, and automated remediation. The solution will discover all interconnected SaaS applications within the estate, and expose a full mapping and inventory of 1st, 2nd and 3rd party applications. Application reviews with business users are performed through ongoing interaction and engagement (i.e. via Slack). End users can approve certain applications through a business justification, or have applications that might pose certain levels of risk to be either manually or automatically remediated. IT and Security teams can enforce automated security policies across the SaaS application stack, remediating the potential risk sanctioned and unsanctioned applications might expose.



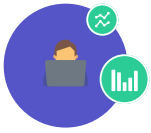




DoControl provides full visibility into sanctioned and unsanctioned applications within the SaaS estate, with full automated remediation via Security Workflows to mitigate the risk of Shadow Applications.

How it Works

Discovery and Visibility: Discover all connected SaaS applications to the core SaaS stack. Identify issues of non-compliance for the entire SaaS application estate to ensure security policies are effectively enforced. Expose a full SaaS-to-SaaS application mapping and comprehensive inventory of 1st, 2nd and 3rd party applications (i.e. installed users, drive access, drive-wide permissions, and more). IT and Security teams can gain a strong understanding of the riskiest SaaS platforms, applications, and users exposed within the SaaS estate.



Monitor and Control: Perform application reviews with business users through ongoing interaction and engagement (i.e. via Slack). Assign a risk-index to each application to enable the assessment and evaluation of the SaaS estate. Create pre-approval policies and workflows that require end users to provide a business justification to onboard new applications. IT and Security teams can quarantine suspicious applications, reduce overly excessive permissions, and revoke or remove applications or access.

Automated Remediation: Automate security policy enforcement across the SaaS application stack that prevents unsanctioned or high risk application usage, and remediates the potential risk those apps might expose (i.e. invalid tokens, extensive or unused permissions, listed vs. not listed apps, etc.). IT and Security teams can automatically reduce risk exposure related to application-to-application interconnectivity (i.e. automatically suspend or remove potential malicious applications) by implementing Security Workflows.

The DoControl SaaS Security Platform

DoControl provides a unified, automated and risk-aware SaaS Security Platform that secures business critical data, drives operational efficiencies, and enables business productivity. DoControl's core competency is focused on protecting business-critical SaaS data through automated remediation. This is achieved through preventive data access controls, SaaS service misconfiguration detection, service mesh discovery, and shadow application governance. The DoControl Platform is built upon three foundational tenants which include Discovery and Visibility, Monitor and Control, and Automated Remediation. DoControl provides SaaS data protection that works for the modern business, so they can drive their business forward in a secure way.

Partner with DoControl and start moving security closer to what drives the modern business forward. Learn more.