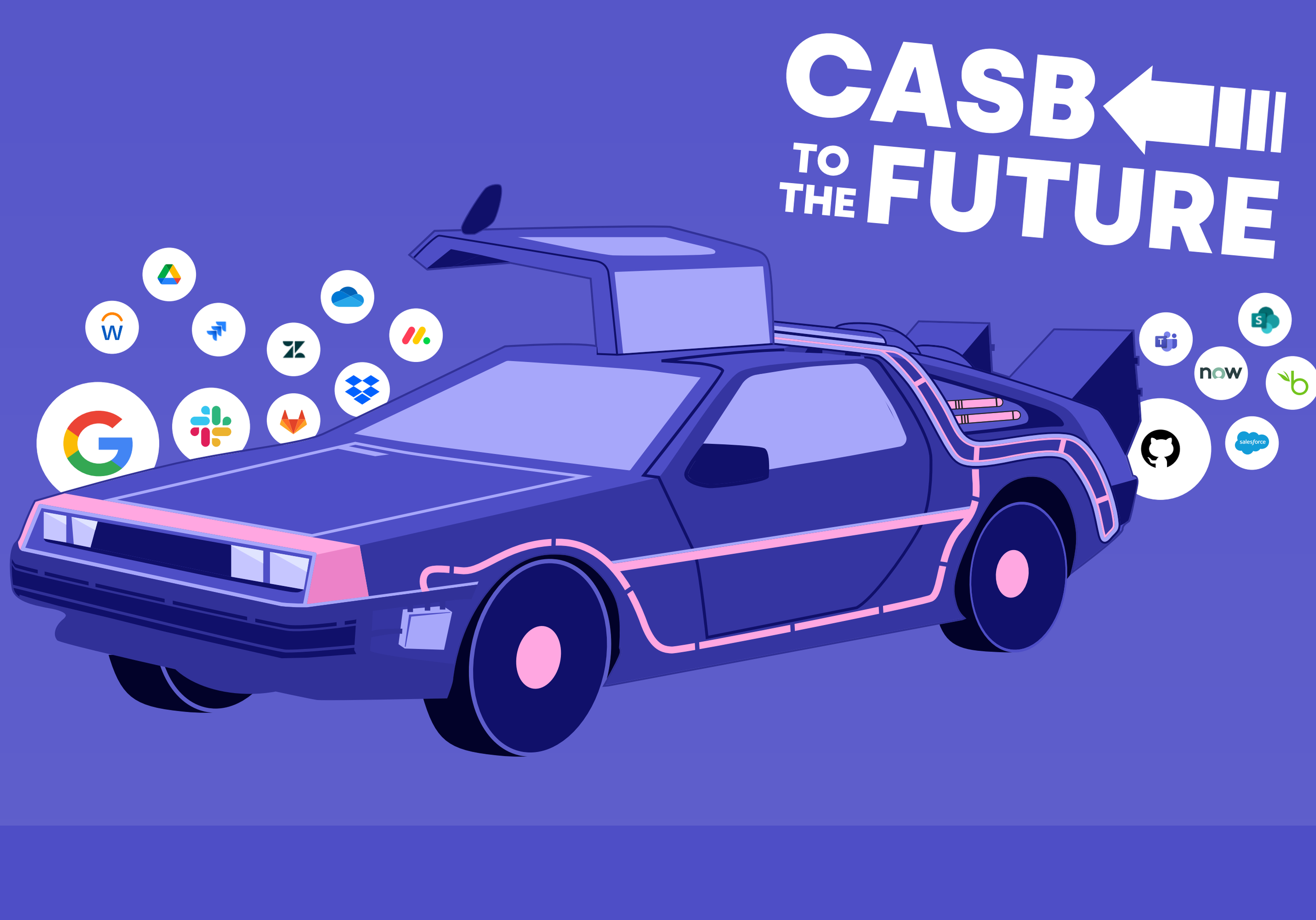
DoControl.

Modernize Your Cloud Access Security with DoControl

The use of cloud technologies is imperative in order to remain competitive in the marketplace. Like any tool that allows the business to become more agile and go-to-market faster, security needs to be integrated into the technology stack. Cloud Access Security Broker (CASB) solutions were originally developed to extend on-premises security policies into cloud environments. Today, traditional CASB technologies are less relevant. They lack the ability to enforce granular access control policies, they're costly, difficult to manage, and provide a less than ideal end user experience.

CISOs and security practitioners require a modern solution to effectively enforce data access controls so their business users can safely leverage Software as a Service (SaaS) applications.



Quantifying the Risk of Unmanaged Data Access

2% of all SaaS data is confidential.*

10M assets stored in SaaS applications.*

18% of all SaaS assets are shared externally and/or publicly.*

Cloud Adoption by the Numbers

*Gartner estimates that SaaS is the largest cloud revenue generator and that it will grow at a compound annual rate of around 20% through 2025, while the PaaS and IaaS sectors are smaller but growing much faster. Rapid cloud adoption creates a need to simplify and consolidate security delivered from the cloud for the cloud, rather than try to force traffic through on-premises networks and data centers to secure access.

> The DoControl solution provides us with the visibility, control and enforcement capabilities we need to deliver secure access to our critical SaaS applications and data.

similarweb — **Raz Karmi**, Director of Information Security, CISO, SimilarWeb

Traditional Approaches Break Down

Inline Scanning

Break and inspect SSL Transactions in Band

Pros:

- Real-time for some use cases
- Leverages exisiting SWG/SSe platform

Cons:

- Slows down UX
- Only works for managed endpoints
- Does not native content or sharing
- May not cover sync clients

CASB API

Scan All Content Iteratively and React

Pros:

- Scans all content
- Does not affect UX (out of band)

Cons:

- "Brute Force" scanning approach
- House or days of delay between risky action and detection/action
- Limited options for detection (DLP myopia)

Event Log API

Trigger on Log of Event then React

Pros:

- Faster time to react than CASB API
- Does not affect UX

Cons:

- No SLA on logs from SaaS vendors means unpredictable delay between log entry and detection/action
- Limited options for detection (DLP myopia)

DoControl

The SaaS Event Triggers the Security Reaction

Pros:

- Faster time to react than CASB API or
- Event Log API
- Context aware
- Flexible
- Does not affect UX

Cons:

- Not real time (but as close as you can get without the penalty of inline)

Say Goodbye to Hardcoded Policies

DoControl is an event-driven platform that takes a modern approach to securing cloud-hosted data and files. DoControl's No-Code SaaS Security Platform enables security teams to create granular data access control policies that mitigate the risk of data overexposure and exfiltration within business-critical SaaS apps.

The solution provides strong visibility throughout the IT estate (i.e. users, assets, groups, domains, 3rd party apps), continually assesses and exposes cloud application risk, and provides both manual and automated remediation. Modern businesses partner with DoControl to reduce organizational risk and support stringent compliance requirements involving cloud governance and access to sensitive data.

Accelerate Cloud Access Security

Visibility

DoControl exposes potential data access risks, and enables security teams to monitor all SaaS user and data activities and take appropriate action to remediate threats.

Protection

DoControl provides security teams with self-service remediation capabilities to take immediate action against known threats as well as automated, near real-time remediation intervention workflow policies.

Compliance

DoControl helps provide support for compliance with regional mandates, industry standards, as well as organizational policies that require proper cloud services governance and secure access to sensitive data and files.

Request a Demo

*Gartner estimates that SaaS is the largest cloud revenue generator and that it will grow at a compound annual rate of around 20% through 2025, while the PaaS and IaaS sectors are smaller but growing much faster. Rapid cloud adoption creates a need to simplify and consolidate security delivered from the cloud for the cloud, rather than try to force traffic through on-premises networks and data centers to secure access.

*Magic Quadrant for Security Service Edge, February 15th, 2022, John Watts | Craig Lawson | Charlie Winckless | Aaron McQuaid

*Reference: Gartner® Magic Quadrant™ for Security Service Edge, February 15th, 2022, John Watts | Craig Lawson | Charlie Winckless | Aaron McQuaid

*DoControl Data Report, "Quantifying the Immense Risk of Unmanaged Data Access," August 24th 2021