ADAPTIVE SHIELD

CASB vs. SSPM:

Optimizing SaaS Security

CASB (Cloud Access Security Broker) and SSPM (SaaS Security Posture Management) are integral to cloud security, each addressing distinct aspects of SaaS data protection.

Many organizations initially used CASBs to secure their SaaS applications. However, SaaS's evolution has far outgrown CASB's capabilities, and the limitations inherent in CASB make it unsuitable as a modern security tool. CASB solutions are unable to secure the stack for a number of reasons, including:

Configuration Monitoring Requires Extensive Customization

CASBs can't cover the different configurations and security settings in each SaaS application.

Security Policy Application

CASBs normalize policies across an organization's cloud network. However, this approach is inadequate when dealing with diverse SaaS applications that require SaaS-specific rules.

Lack of Adaptability

CASB lacks flexibility in addressing evolving SaaS characteristics and threats.

Security Blindness

CASB focuses on pathways and looking at the app "from the outside," causing it to miss user behavior nuances.

Integration Complexity

CASBs require a proxy, API connections, and considerable cost and effort for each application that it integrates with.

In contrast, SSPMs were designed to secure SaaS applications while working in partnership with application administrators. They provide far better visibility into configurations, users, and third-party apps than any other tool. SSPMs also allow organizations to respond to threats and configuration drifts to mitigate risks. They include remediation steps, alerts, and ticket creation, all of which are lacking in even the most advanced CASB solution.

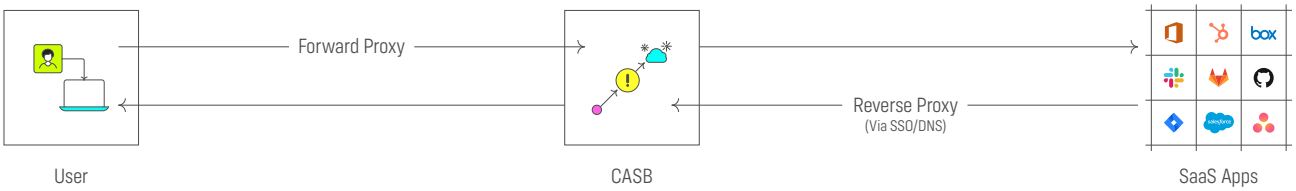
Our security team had used CASBs in previous roles but were frustrated by the high volume of false positives CASBs generated. Additionally, the team felt CASBs were expensive, created user friction, and added an unnecessary layer in securing SaaS applications.

Jason Walton
Executive Director of Information Security, Schrödinger

CASB

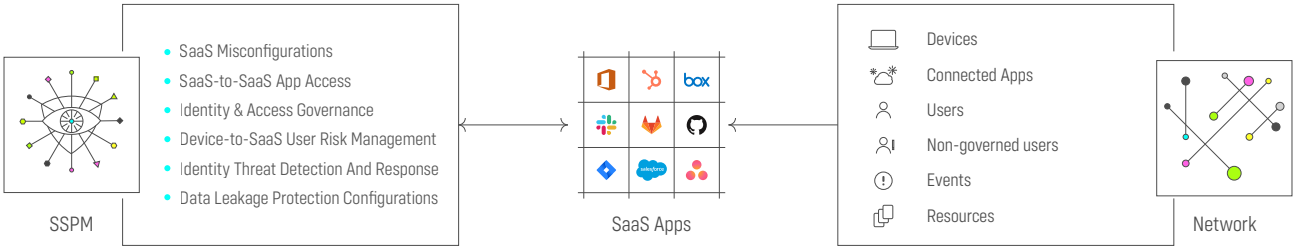
In-line data between SaaS to organization, including users, data access, and authentication

*API only for DLP and events



SSPM

Access all configurations and data at the source from within the SaaS application



	CASB	SSPM
Misconfigurations Management		
Identifies misconfigured settings	Partial support	Supports
Identity Security Posture Management		
Monitor external users	Does not support	Supports
Identifies dormant users	Partial support	Supports
Identifies deprovisioned users	Partial support	Supports
Identifies user threats	Partial support	Supports
Monitors all user access points	Does not support	Supports
SaaS to SaaS Access		
Monitor third-party applications	Supports	Supports
Monitors all app access points	Does not support	Supports
Device to SaaS Access		
Monitor devices used to access apps	Partial support	Supports
Identity Threat Detection		
Identify Suspicious Downloads	Supports	Supports
Reads inline data between SaaS and Organization	Supports	Supports
General		
Integrations	Custom integration	150+ out-of-the-box, custom integration builder
Pricing	High setup costs per application	Cost effective solution to monitor all applications
Compliance Framework Support	Supports	Supports
Object Permission Analysis	Does not support	Supports

Each CASB provider offers different capabilities. This comparison is based on the average CASB.

ADAPTIVE SHIELD

Adaptive Shield, leader in SaaS Security, enables security teams to secure their entire SaaS stack through threat prevention, detection and response. With Adaptive Shield, organizations continuously manage and control all SaaS apps, including 3rd-party connected apps, as well as govern all SaaS users and risks associated with their devices. Founded by Maor Bin and Jony Shlomoff, Adaptive Shield works with many Fortune 500 enterprises and has been named Gartner® Cool Vendor™ 2022.

www.adaptive-shield.com

Follow us on LinkedIn