Zscaler™ CASB at a Glance

Zscaler CASB Benefits:

☑ **Complete Data Protection**
Data Protection across SaaS applications to prevent employees from accidentally sharing sensitive data

☑ **Unified Compliance**
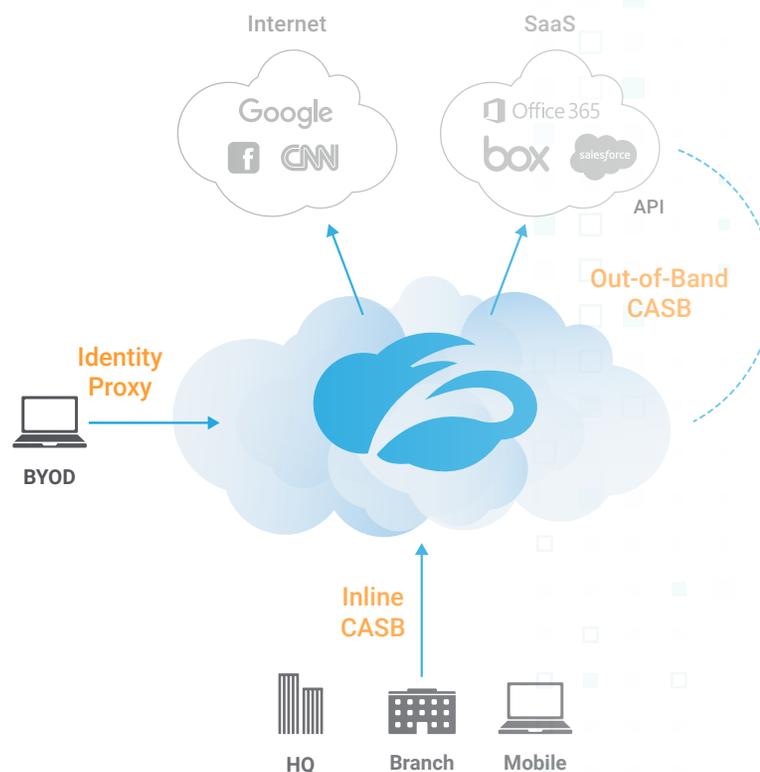Provides compliance visibility and mitigates violations across SaaS applications

☑ **Automated Risk Reduction**
Ensures SaaS apps follow industry and organizational best practices with automated remediation

The adoption of SaaS applications has fundamentally changed the way employees do their job and accomplish their corporate goals. The ease of adoption, collaboration and sharing they enable has driven the majority of this adoption. The darkside of faster adoption and greatly expanded collaboration is that it can present new risks that our beyond the experience and knowledge of the employees adopting them. Unfortunately, It is impossible to train every employee to consistently use security best practices with SaaS applications at all times, and that can lead to costly mistakes for the organization.

The traditional approach to solve this is to add a CASB as separate overlay to report on SaaS usage and provide some level of control. Unfortunately this is independent of the rest of the organization's security offerings and another separate data protection function that adds unneeded complexity without solving the key challenges of SaaS usage.

Zscaler CASB enables organizations to securely adopt and govern the use of multiple SaaS applications. It provides real-time visibility and controls access and user activity across sanctioned and unsanctioned applications.. The fully integrated platform eliminates overlay architectures and simplifies policy creation and administration, ensuring data is protected and compliance is maintained.

Internet | SaaS

Google | Office 365 | box | salesforce

API

Out-of-Band CASB

Identity Proxy

BYOD

Inline CASB

HQ | Branch | Mobile

Key Capabilities

Data exposure reporting and remediation
Zscaler CASB checks SaaS applications and cloud providers' configurations and compares them to industry and organizational benchmarks to report on violations and automate remediation.

Threat identification and remediation
Zscaler CASB checks SaaS applications for hidden threats laying dormant within the application or being exchanged between users and prevents their propagation. Zscaler Cloud sandbox integration identities and remediates zero day attacks across the organization in addition to SaaS applications as part of Zscaler CASB.

Automated compliance assurance
Zscaler CASB provides compliance visibility across SaaS applications against laws, regulations and security standards to identify compliance violations while automating remediation.

Granular cloud access control
Provides real-time visibility and controls access and user activity across sanctioned and unsanctioned applications. Controls access to thousands of apps with the context of whether they are corporate or personal versions of the application, and then provides granular restrictions on upload, download and write access to prevent data loss.

Cloud usage reporting and analytics
Enables a unique single view of cloud usage providing key insights through analytics and reporting across cloud applications and users. Alerts and remediates data exposure violations with the context of what the data is, how it is shared and if the person is an internal employee or an external collaborator.

Part of a larger data protection platform
The Zscaler Cloud Security Platform provides unified data protection with DLP and CASB capabilities for internet, data center, and SaaS applications, and ensures that public cloud applications are configured to prevent data exposure and maintain compliance.

" CASBs provide a central location for policy and governance concurrently across multiple cloud services — for users and devices — and granular visibility into and control over user activities and sensitive data."

– Gartner

To learn more about what Zscalers Data Protection can do for you go to **zscaler.com/dp**

ZSCALER™