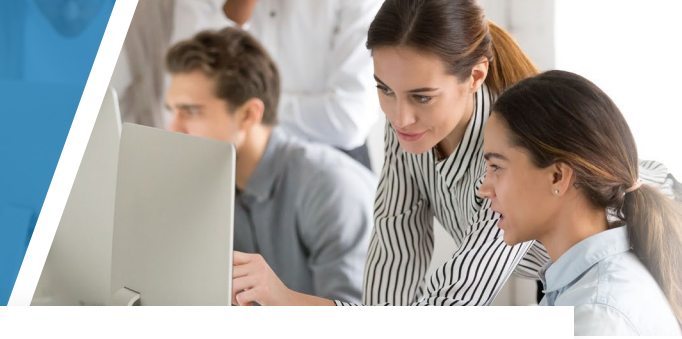
Zscaler™ CASB at a Glance



Zscaler CASB Benefits:

Complete Data Protection
Guarantees data protection across SaaS applications to prevent employees from accidentally sharing sensitive data

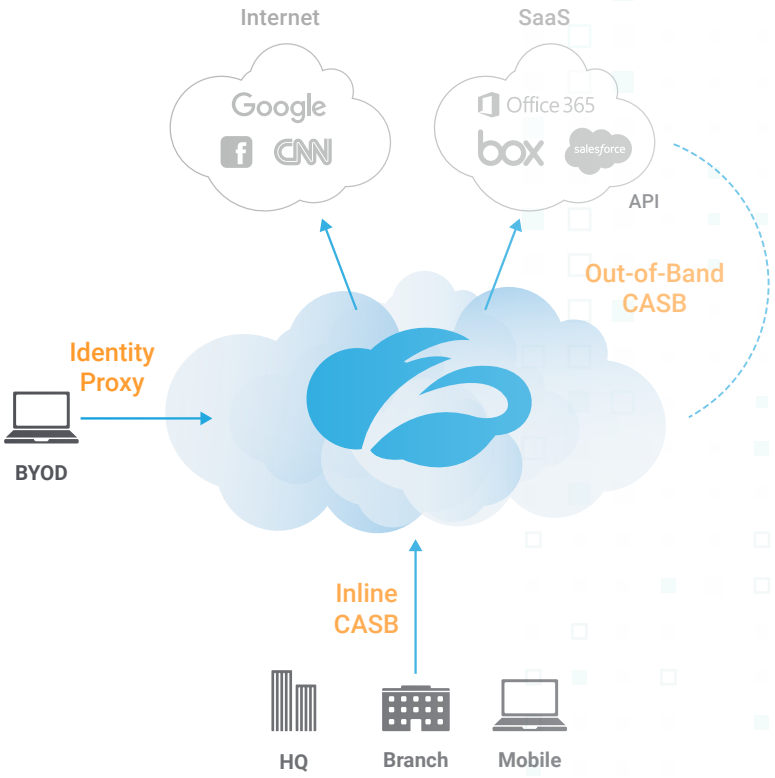
Unified Compliance
Provides compliance visibility and mitigates violations across SaaS applications and cloud service providers

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 jobs and accomplish their corporate goals. The ease of adoption, along with enhanced collaboration and sharing capabilities, has driven the majority of this adoption. The dark side of faster adoption and greatly expanded collaboration, however, is that it can present new risks that are beyond the experience and knowledge of the employees using SaaS apps and services. Unfortunately, it is impossible to ensure that every employee is consistently using security best practices with SaaS applications at all times, and that can lead to costly mistakes for the organization.

The traditional approach to address the risks associated with SaaS is to add a cloud access security broker (CASB) as a 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, which means it is a 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.



Zscaler CASB 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 cloud applications for hidden threats laying dormant within the application or being exchanged between users and prevents their propagation. Via inline inspection, Zscaler Cloud Sandbox integration quickly finds new ransomware and patient zero threats across data-in-motion.

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

Data classification and protection
Zscaler CASB delivers complete protection against leakage for data in motion and data at rest. Advanced classification measures identify sensitive information and keep it safe wherever it goes.

Granular cloud access control
Zscaler CASB provides real-time visibility and controls access and user activity across sanctioned and unsanctioned applications. It also controls access to thousands of apps, and identifies 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
Zscaler CASB enables a unique, single view of cloud usage, which provides key insights through analytics and reporting across cloud applications and users. It also alerts and remediates data exposure violations with context that tells you 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, ensuring 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**

Zscaler Data Protection Components

Capability	Description	ZIA Professional	ZIA Business	ZIA Transformation	ELA
Inline Data Protections (Cloud DLP and Inline CASB)					
Cloud Application Visibility and Control	Discover, monitor, and control access to web applications	Visibility Included	Visibility and Control Included	Visibility and Control Included	Visibility and Control
Identity Proxy for cloud apps	SAML Proxy for controlling BYOD and unmanaged devices connecting to SaaS apps	–	Included	Included	Included
Essentials Cloud Data Loss Prevention	Identify confidential data loss with inline scanning across PCI, PII, and 2 custom dictionaries. Alerting only, no ICAP forwarding.	–	Included	Included	Included
Advanced Cloud Data Loss Prevention	Identify and prevent confidential data loss with inline scanning across all dictionaries.	User per year	User per year	User per year	Included
DLP Exact Data Match	Fingerprint structured data to eliminate DLP false positives; Add-on 1 million cells per 100 seats	$ based on cells per year	$ based on cells per year	$ based on cells per year	1M cells per 100 seats
Upgraded Data Classification	Find and block custom data better. Includes Exact Data Match for fingerprinting structured data and Indexed Document Matching for fingerprinting forms and documents. Requires Zscaler DLP or CASB.	User per year	User per year	User per year	Included
ICAP Connectors	Send DLP detection logs from Zscaler cloud to on-premises DLP server	$ per year	$ per year	$ per year	1 Connector included
Out-of-Band Data Protections (API CASB)					
Essentials Out-of-Band CASB	Prevent data exposure and ensure SaaS app compliance for 1 sanctioned app. No historical scanning.	–	Included	Included	Included
Standard Out-of-Band CASB	Prevent data exposure and ensure SaaS app compliance for 1 sanctioned app (excluding email). Scan 10TB of historical data repositories.	User per year	User per year	Included	Included
Advanced Out-of-Band CASB	Prevent data exposure and ensure SaaS app compliance for all apps. Scan 10TB of historical data repositories.	User per year	User per year	User per year	Included
SaaS Security Additional Historical Data	Additional data for SaaS historical scan (one-time)	$ per TB	$ per TB	10TB included.$ per TB add.	10TB included. $ per TB add.
Out-of-Band App Hygiene (SSPM & CSPM)					
Cloud Security Posture Management	Identify and remediate misconfigurations and assure compliance for IaaS and PaaS applications hosted on public cloud infrastructure	Workload per year	Workload per year	Workload per year	Workload per year
SaaS Security Posture Management	Identify and remediate misconfigurations and assure compliance for SaaS applications, including M365	User per year	User per year	User per year	Included
Data Protection Bundles					
Data Protection Package	Includes Advanced DLP, Advanced OOB CASB and SaaS Security Posture Management for M365	–	User per year	User per year	Included

Learn more about how Zscaler can help you: CASB: **www.zscaler.com/casb** Data Protection: **www.zscaler.com/dp**

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com