Zscaler™ CASB At a Glance

Zscaler CASB benefits:

Granular data protection
Prevents malicious and accidental data leakage across cloud-based resources.

Complete threat protection
Stops the spread of threats such as ransomware across cloud and user endpoints.

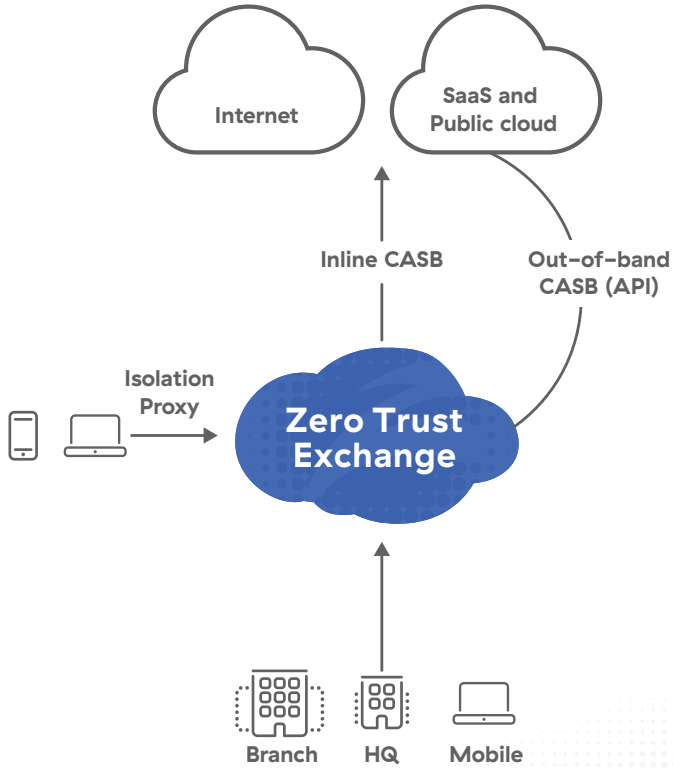
Comprehensive visibility
Delivers in-depth logging and reporting for the complete oversight of all cloud data.

Unified compliance
Provides deep compliance visibility and assurance across SaaS applications.

The adoption of SaaS apps has fundamentally changed how organizations operate, and how employees do their jobs. These apps are easy to deploy, enhance collaboration and productivity, decrease IT costs, and facilitate remote work. However, the legacy security stack that defended the network is ineffective in our cloud-first world, and native SaaS protections are either insufficient or nonexistent. As such, digital transformation also requires security transformation.

Cloud access security brokers (CASBs) are solutions that deliver modern security for enterprises using cloud resources such as SaaS and IaaS. Many organizations have deployed CASBs as additional point-product, security overlays in their IT environments. However, relying on disjointed solutions with disparate capabilities and inconsistent policies leads to poor enterprise security. It also increases IT complexity, adds a significant management burden for admins, and impairs user productivity as traffic is redirected through several different tools.

Zscaler's multimode CASB empowers organizations to secure any sanctioned or unsanctioned SaaS app or IaaS platform. With inline, real-time capabilities and out-of-band scanning functionality, it protects data, blocks threats, grants visibility, and assures compliance to address any cloud security use case. This fully integrated solution eliminates overlay architectures to reduce IT complexity, simplify management, and preserve user productivity. Along with secure web gateway and zero trust network access technologies, Zscaler CASB is part of the company's leading security service edge (SSE) offering that secures any transaction.



Data detection and protection

Zscaler CASB protects against all leakage for data in motion and at rest. Predefined and customizable DLP dictionaries, full SSL inspection, and file sharing controls secure data wherever it goes.

Advanced data classification

Advanced technologies like exact data match and indexed document matching find specific values and forms that need to be protected, while optical character recognition detects data in image files.

Agentless security for BYOD

Zscaler CASB delivers agentless Cloud Browser Isolation to secure BYOD and third-party devices where software installations are infeasible, avoiding the use of reverse proxies and their breakages.

Advanced threat protection

Zscaler CASB stops malware from reaching cloud resources in real time, and finds and remediates threats already at rest. Cloud sandboxing detects new ransomware and other zero-day infections.

Shadow IT discovery

As a natively inline solution, Zscaler CASB automatically identifies unsanctioned apps used by employees and creates a risk score for each so that IT can better understand how to respond.

Cloud app control

Zscaler CASB secures access to specific apps, tenants, and app categories based on user group, device, and more. It can block access, provide read-only access to stop leakage, or restrict usage.

SaaS security posture management

By monitoring SaaS app configuration settings, Zscaler CASB can uncover and fix issues that put data at risk or jeopardize compliance with industry benchmarks and regulatory frameworks.

Part of a larger SSE platform

Zscaler CASB is one part of a complete SSE offering along with market-leading secure web gateway and zero trust network access functionality, securing any transaction for the modern enterprise.

> "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 Zscaler Data Protection can do for you, go to zscaler.com/dp

Zscaler Data Protection components

Capability	Description	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	Included	Included	Included
Identity Proxy for cloud apps	SAML Proxy for controlling BYOD and unmanaged devices connecting to SaaS apps	—	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	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	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	Included
ICAP Connectors	Send DLP detection logs from Zscaler cloud to on-premises DLP server	$ 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.	—	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	Included
SaaS Security Additional Historical Data	Additional data for SaaS historical scan (one-time)	$ per TB	1TB 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
SaaS Security Posture Management	Identify and remediate misconfigurations and assure compliance for SaaS applications	User per year	User per year	Included
Data Protection Bundles				
Data Protection Package	Includes Advanced DLP, Advanced OOB CASB and SaaS Security Posture Management	User per year	User per year	Included

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

zscaler.com