



Zscaler™ Data Protection at a Glance

The adoption of SaaS and public cloud has rendered data widely distributed and difficult, if not impossible, to secure with legacy protection appliances. As such, it is easy for both careless users and malicious actors to expose enterprise cloud data.

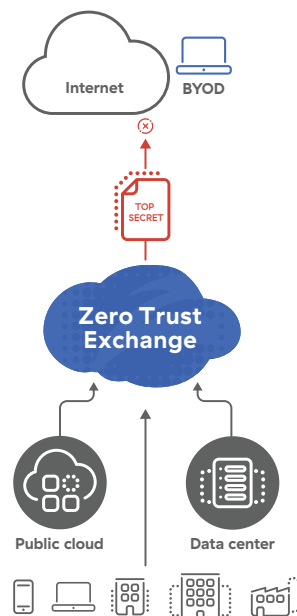
Zscaler Data Protection follows users and the apps they access—protecting anywhere and anytime against data loss. Our Zero Trust Exchange™ inspects traffic inline, encrypted or not, and ensures your SaaS and public cloud apps are secure, while delivering a dramatically streamlined approach to protection and operations.

Zscaler Data Protection delivers integrated protection across all sources of data loss:

Prevent inline data loss to Web and BYOD

When users access the internet and its risky destinations, it is a threat to enterprise data. Legacy appliances can't follow users off-network or secure their web traffic.

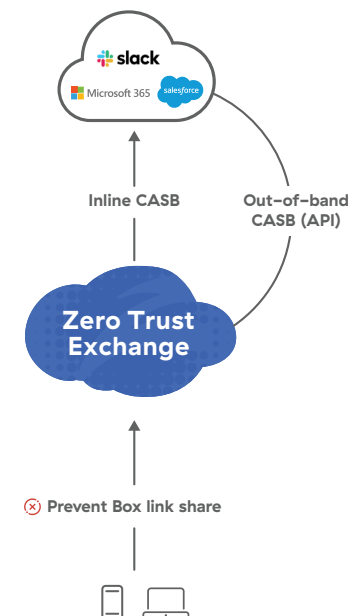
Zscaler is a cloud-native platform that scales to inspect all traffic, everywhere. A single DLP policy protects data across web, SaaS and private apps, along with advanced classification like EDM, IDM and OCR. Leverage browser isolation to safely stream data as pixels to unmanaged BYOD.



Secure SaaS data with CASB

Securing data at rest in SaaS apps is critical for security—it only takes two clicks to share data with an unauthorized user through apps like Microsoft OneDrive.

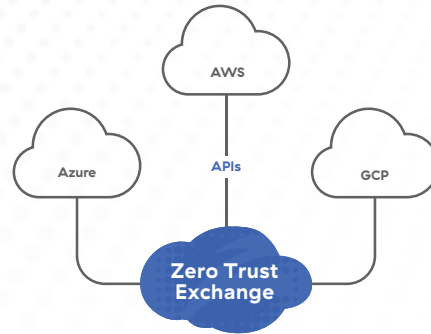
Zscaler's integrated, multimode CASB secures SaaS apps without the cost and complexity of a point product. Inline functionality delivers full shadow IT discovery and control. Out-of-band DLP and ATP remediate risky file sharing and malware at rest in the cloud, respectively.



Close dangerous misconfigurations

Most cloud breaches are caused by dangerous misconfigurations or permissions. As SaaS and IaaS are highly dynamic, such gaps are often overlooked and exploited.

Zscaler SaaS Security Posture Management (SSPM) finds and remediates potentially fatal misconfigurations, compliance violations, permissions, and entitlements; continuous scanning prioritizes risk. Support for major SaaS platforms including Microsoft 365, Salesforce, and Google Workspace.



Secure endpoint data

Data in use on endpoints can be easily lost across multiple channels. From removable media, to printing to network shares, users often expose sensitive data to unnecessary risks, or maliciously exfiltrate data when leaving for another company.

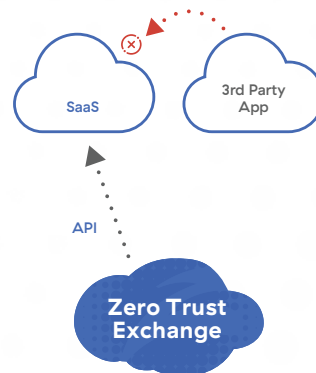
With Endpoint DLP, organizations can enforce consistent DLP policy across endpoints to ensure sensitive data remains protected. Control USB drives, bluetooth, printing or network shares with always-on DLP protection.



SaaS Supply Chain Security

Every time a user grants a third-party access into their Google or Microsoft 365 account, your attack surface grows. Most companies are blind to these connections, which often have read and write privileges to sensitive data.

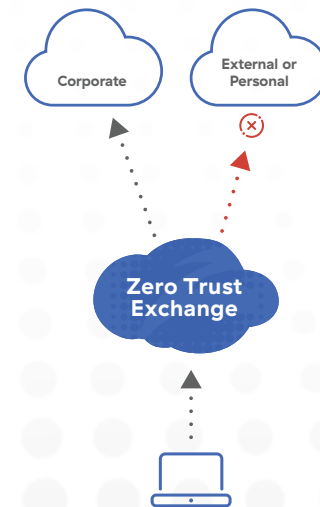
Zscaler SaaS Supply Chain Security platforms, giving you instant visibility over all third-party app connections. Easily analyze and remediate over-privileged access and enable control policies.



Email DLP

Email is one of the most common channels for data loss. Users can easily forward sensitive data out of the organization or to personal email accounts.

With Zscaler Email DLP, security administrators get full control over email attachments and destinations. Ensure sensitive data is not attached to emails and prevent content from being forwarded outside the organizational domain.



Zscaler Data Protection key capabilities

Unified protection

Zscaler Data Protection provides consistent, unified security for data in motion and data at rest across SaaS and public cloud applications.

Unlimited SSL Inspection

Inspect all your SSL traffic without any limitations. Find more data loss where it hides, without typical hardware limitations.

ML-Powered Data Discovery

Quickly understand data behaviors and risks. Innovative discovery automatically finds and classifies all data out of the box.

Compliance reporting and remediation

Zscaler enables unified compliance across SaaS and public cloud apps, measuring configurations against 17 frameworks and automating remediation.

Zscaler Data Protection Components

		Data Protection Advanced	Data Protection Prime
Enterprise DLP Solution			
Cloud App Control	Find and control risky or unsanctioned apps (Shadow IT)	Included	Included
Inline Web	Prevent data loss with inline scanning across all dictionaries (DLP)	Included	Included
SaaS API	Prevent data exposure and ensure SaaS app compliance (CASB). All apps except email	Included	Included
Email	Inline and API data protection across Microsoft and Google web email	Included	Included
Private Apps	Prevent data loss with inline scanning across private apps (ZPA)	Included	Included
Unmanaged Devices	Prevent data loss to BYOD by streaming data as pixels only (Browser Isolation)	Included	Included
Zscaler SaaS Supply Chain Security	Protect SaaS Platform from risky third-party backdoor connections	Add-On	Included
Endpoint DLP	Secure data in use across endpoint devices	Add-On	Add-on or in Data Protection Unlimited
Advanced Classification			
Exact Data Match (EDM)	Fingerprint and secure custom company data		Included
Index Document Match (IDM)	Fingerprint and secure custom documents and forms		Included

Optical Character Recognition (OCR)	Find and prevent data loss in images and screenshots		Included
Advanced Incident Management			
Workflow Automation	Cloud-hosted incident management tool enables streamlined investigations across Admins, Managers and Users		Included
ICAP Connectors	Send DLP logs from Zscaler cloud to on-premises DLP/ICAP server		Included
Incident Receiver	On-premise or cloud tool able to securely receive Zscaler DLP Logs		Included

Data Protection availability in Zscaler Internet Access Editions

		Business	Transformation	Unlimited
Data Protection Standard (DLP and CASB Essentials)	Find and control risky and unsanctioned apps (Shadow IT)	Included	Included (+) SaaS API retro scan	Included
	Inline DLP alerting across PCI, PII, and 2 custom dictionaries (no blocking)			
	Prevent data exposure and ensure SaaS app compliance (CASB). Only 1 sanctioned app.			
Data Protection Advanced	Complete Enterprise DLP Solution	Add-on	Add-on	Included
Data Protection Prime	Complete Enterprise DLP Solution including Advanced Classification and Advanced Incident Management	Add-on	Add-on	Included

Data Protection availability in Zscaler for Users Editions

		Business (Plus or Prime)	Transformation (Plus)	ELA
Data Protection Inline Web and CASB Standard	Find and control risky and unsanctioned apps (Shadow IT)	Included	Included	Included
	Full inline data loss prevention for sensitive data in motion (DLP)			
	Prevent risky data sharing and exposure across one (1) SaaS app, excluding email (CASB)			
Data Protection Advanced	Complete Enterprise DLP Solution	Add-on	Included	Included
Data Protection Prime	Complete Enterprise DLP Solution including Advanced Classification and Advanced Incident Management	Add-on	Add-on	Included

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

 | Experience your world, secured.™

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at zscaler.com or follow us on Twitter @zscaler.

© 2024 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ and other trademarks listed at zscaler.com/legal/trademarks are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.