

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.

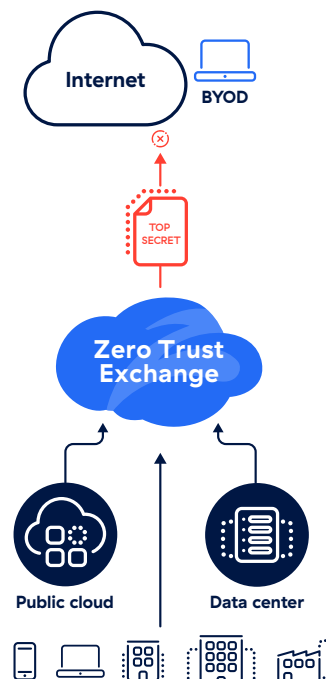
Zscaler Data Protection follows users and the apps they access—protecting anywhere and anytime against data loss. Our Zero Trust Exchange™ inspects inline and cloud data to ensure all data everywhere is secure, while delivering a dramatically streamlined approach to protection and operations.

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.

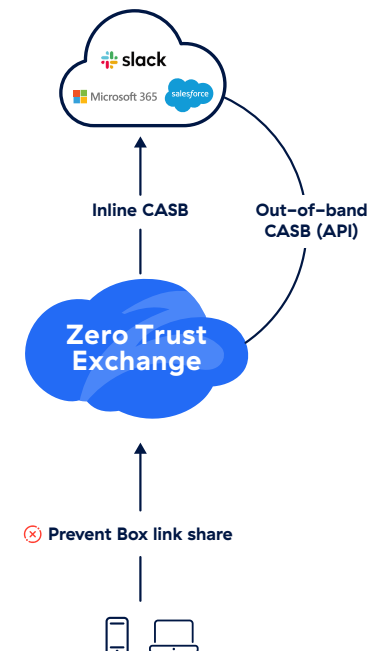
Zscaler is a cloud-native platform that scales to inspect all traffic, everywhere. A single DLP policy protects data across web, SaaS and private apps, along with advanced classification like EDM, IDM and OCR. Leverage browser isolation to safely stream data as pixels to unmanaged BYOD.



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.

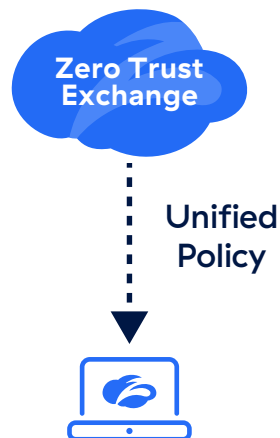
Zscaler's integrated, multimode CASB secures SaaS apps without the cost and complexity of a point product. Inline functionality delivers full shadow IT discovery and control. Out-of-band DLP and ATP remediate risky file sharing and malware at rest in the cloud, respectively.



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.

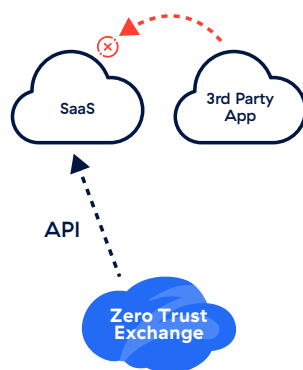
With Endpoint DLP, organizations can enforce consistent DLP policy across endpoints to ensure sensitive data remains protected. Control USB drives, bluetooth, printing or network shares with always-on DLP protection.



Unified SaaS Security (SSPM, SaaS Supply Chain, CASB)

Many cloud breaches are caused by dangerous misconfigurations, access or third-party apps connected into SaaS Platforms. Understanding and governing your SaaS posture is an important step to secure the vast amounts of sensitive data in these clouds.

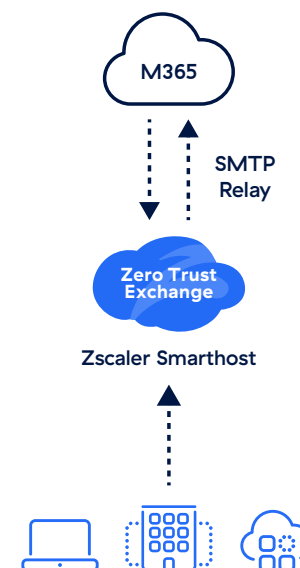
With Zscaler's Unified SaaS Security, organizations get a unified approach to scan and secure SaaS Platforms like Office 365 or Google. Get in-depth visibility into dangerous misconfigurations and app integrations, with auto remediation, guidance, and control over revoking risky connected apps.



Email DLP via Smarthost

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.

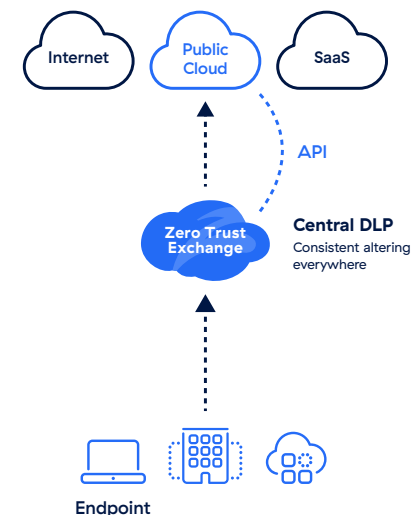
With Zscaler Email DLP, security administrators get a powerfully simple way to insert DLP inspection into their email architecture. Implemented as a Smarthost, Zscaler can be added as the next hop after your email service via SMTP relay. Enforce DLP inspection and actions like blocking, encrypt and quarantine, all with minimal changes to your Email or MTA settings.



Data Security Posture Management (DSPM)

Sensitive data stored in public clouds like AWS and Azure can be very dynamic. From excess privileges and vulnerabilities to shadow data, IT teams need a better way to discover, catalog and secure public cloud data.

Zscaler's DSPM quickly discovers sensitive data, understands risk, and controls access and posture. Best of all, Zscaler's integrated DSPM leverages the same DLP engine as all other channels (Endpoint, Network, SaaS), so alerting is consistent, no matter where your data moves to.



Zscaler Data Protection key capabilities

✦ Unified protection with unlimited SSL

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

✦ Gen AI App Security

Protect data from risky Gen AI apps with in-depth visibility over user input prompts and granular policy controls.

✦ AI-Powered Data Discovery

Delivered across endpoint, network and cloud, Zscaler’s auto discovery everywhere drastically accelerates data visibility and risk response times.

✦ Workflow Automation and User Coaching

purpose-built platform for data loss incident management, with powerful user justification and education options.

Zscaler Data Protection Components		Zscaler Essentials Platform	Zscaler Platform
Data Protection Standard	Stop data loss with Cloud App Control, Shadow IT, Tenancy Restrictions, Inline Web DLP (Monitor Only) and CASB for 1 app	Included	Included
Inline Web DLP – All Apps	Prevent data loss with complete Inline Web DLP across Web, Gen AI and Private Apps	Add-On	Included
Email DLP	Real-time data loss protection for corporate Exchange online	Add-On	Add-On
Endpoint DLP	Secure data in use across endpoint devices	Add-On	Add-On
Unified SaaS Security (CASB, SSPM & Supply Chain)	Govern and control SaaS data and posture in one unified platform	Add-On	Add-On
Data Classification & Encryption Advanced	Use EDM, IDM, OCR to fingerprint custom data, forms and images (screen shots). Redact, encrypt and watermark data	Add-On	Add-On
BYOD Isolation Advanced	Prevent BYOD and unmanaged device while accessing SaaS apps (User Portal 2.0)	Add-On	Add-On
Data Security Posture Management (DSPM)	Quickly discover, classify, and protect sensitive data in public clouds	Add-On	Add-On

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

