Safeguarding Your Data in a Work-From-Anywhere World

Keep your critical information safe
with Zscaler Data Protection

Contents

Protecting your data is more difficult than ever

With cloud apps, your data is now widely distributed and your employees are connecting from wherever they're working—which could be anywhere. Traditional data protection approaches can't give you adequate control over your data. Here's why:

Unable to follow users
You can't deliver data protection properly because your cloud apps are accessed over the internet, away from your network and data controls.

Unknown state of compliance
Understanding the state of your compliance has become difficult because your cloud apps are spread across multiple locations and groups.

Limited SSL inspection
Most traffic is encrypted, but because traditional data protection approaches can't inspect SSL/TLS traffic at scale, you are blind to potential risks.

Missing the big picture
Point products and bolt-on approaches create complexity and prevent the unified view you need to understand exposure.

Take back control of all your data with Zscaler

Zscaler Data Protection can help you achieve unparalleled data protection by adhering to these core principles:

Purpose-built SASE architecture

Deliver real-time protection to all users from a high-performance inline cloud distributed across 150 global data centers.

SSL inspection at scale

Inspect all SSL traffic for data exposure with unlimited inspection capacity per user.

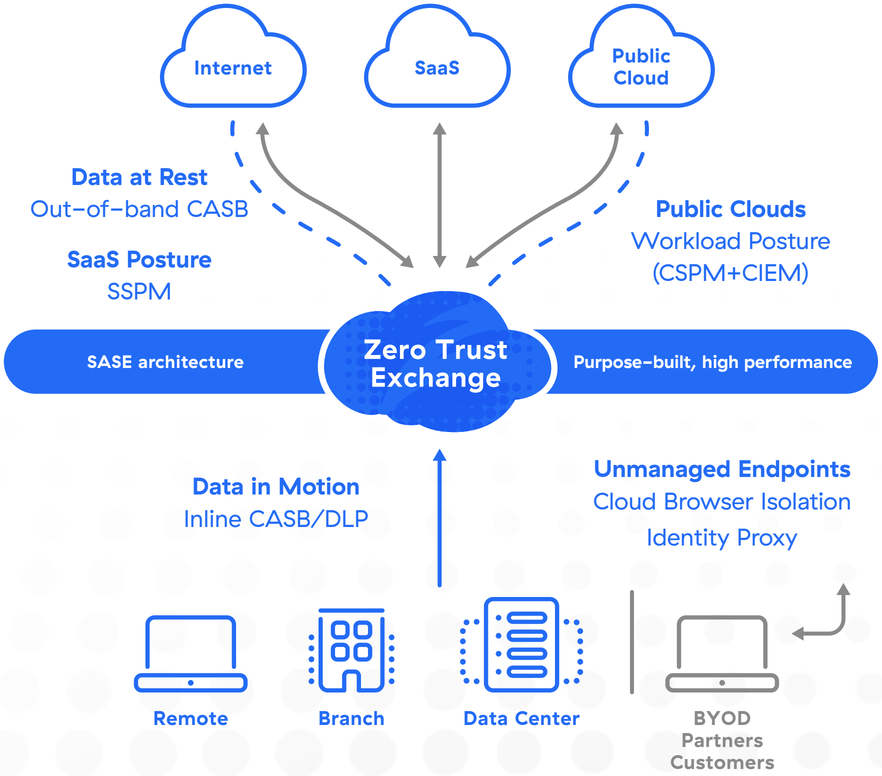
Visibility into compliance

Easily maintain compliance by scanning your SaaS, Microsoft 365, and public clouds for violations and misconfigurations.

One platform, one policy, full visibility

Secure all your cloud data channels—data in motion, at rest, and across endpoints and clouds—with one simple, unified platform.

Zscaler Data Protection: Solution Overview

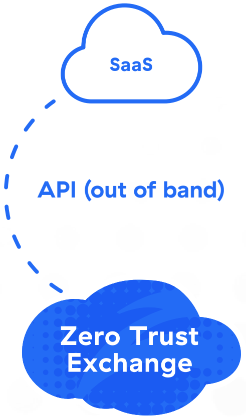


Securely govern sanctioned apps with out-of-band CASB

Your cloud apps can enable better collaboration, especially with many employees working remotely, but they can also expose your data. Employees often unintentionally misuse these apps, which can lead to malicious activity.

How you can secure your cloud apps and data with Zscaler out-of-band CASB:

- **Secure exposed data at rest**
  Identify critical data in cloud apps and file-sharing services, and enforce DLP policies to control access and exposure.
- **Prevent improper sharing of data**
  Enforce granular policy on sensitive data at rest to ensure it is not shared outside the organization.



- **Remediate threats**
  Scan data repositories in file-hosting services, such as OneDrive or Box, to quickly find and quarantine malicious content.
- **Simplify data protection**
  Avoid point product complexity with a unified platform that delivers one data and threat policy across all data in motion and at rest.

Deliver real-time visibility and control with inline CASB

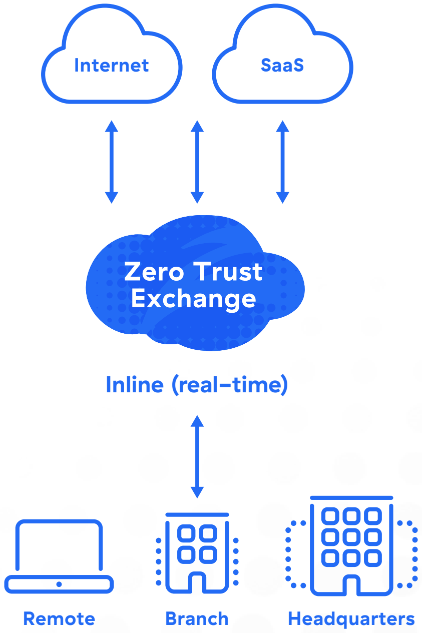
While out-of-band CASB helps secure data at rest, you still need real-time control over your cloud apps. How does inline CASB enable you to safely move to the cloud?

- **Reduces the risk of shadow IT**
  Quickly understand what safe or unsafe cloud apps are being used across the organization.

Example: Block activity to risky apps that access your data, such as online PDF converters or file-sharing sites.

- **Enforces officially sanctioned apps**
  Limit user activity to the cloud apps approved by IT and the organization.

Example: Improve Microsoft 365 sharing and productivity by only allowing OneDrive while blocking Box.



Work-from-anywhere

- **Prevents data loss with file type controls**
  Restrict data transfer by file types with conditional blocking and alerting.

Example: Prevent the uploading or downloading of Word, Excel, or PowerPoint files by user or groups.

- **Enforces tenancy restrictions**
  Control data flows by permitting only specific instances of cloud apps.

Example: Prevent data leakage into personal Microsoft 365 instances by only allowing access to Microsoft 365 for Business.

Protect sensitive data wherever it hides with Cloud DLP

While out-of-band CASB helps secure data at rest, you still need real-time control over your cloud apps. How does inline CASB enable you to safely move to the cloud?

As part of Zscaler's unified data protection solution, Cloud DLP elevates your data protection to safeguard all your critical business data, empowering you to:

- **Protect users on- and off-network**
  Deliver an always-on DLP policy no matter where your users connect.
- **Inspect all your SSL traffic**
  Eliminate blindspots. Inspect all SSL traffic, with no capacity or performance limitations.
- **Restore and maintain compliance**
  Quickly find and control PII, PCI, and PHI data to comply with major regulations.
- **Integrate with GRC workflows**
  Easily add Zscaler visibility into your existing third-party solutions with ICAP and SIEM forwarding.

Find and classify sensitive data in motion with DLP dictionaries

Personally identifiable information (PII)

- Social Security No. (US)
- National Insurance No. (UK)
- National ID No. (Hong Kong)
- Citizen Service No. (Netherlands)

Payment Card Industry (PCI)

- Credit card numbers
- Card expiration and CCV
- Financial statements
- First name, last name

Protected health information (PHI)

- Medical information
- CPT and ICD codes
- Medicare numbers

Custom dictionaries

- Improve protection or matching with custom keywords, regex, patterns, and other identifiers.

Reduce DLP false positives with Exact Data Match

What is Exact Data Match?

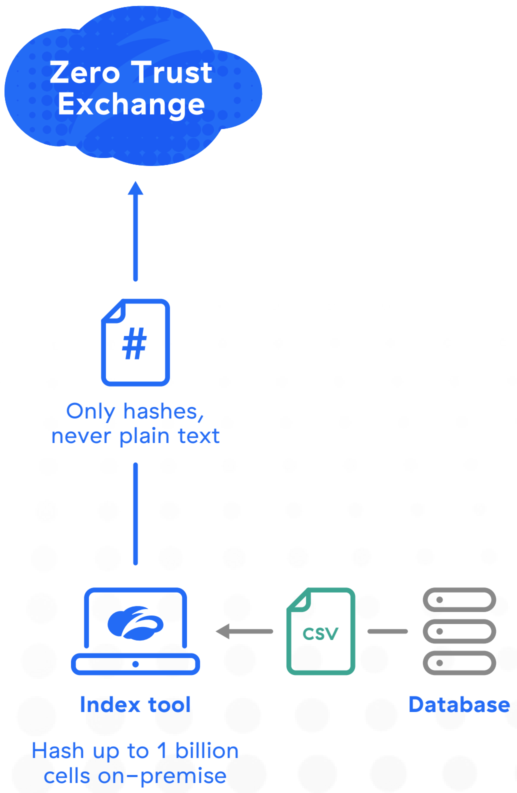
Exact Data Match (EDM) enables you to identify and monitor sensitive information in your databases without having to transfer that data to the cloud. EDM increases detection accuracy and eliminates false positives.

How does EDM reduce false positives?

Instead of blocking all credit card numbers, for example, only credit card numbers stored in your databases would be blocked. An employee making a purchase with a personal credit card would not trigger an alert, nor would an accountant paying invoices.

How Zscaler EDM works:

- Identify the sensitive data you want to index from your records
- Use the Zscaler EDM tool to index the content
- Only file hashes are then sent to Zscaler—never sensitive data
- Fingerprints are loaded into Zscaler Cloud DLP, ready for action


Zero Trust Exchange
#
Only hashes, never plain text
CSV
Index tool
Hash up to 1 billion cells on-premise
Database

Secure sensitive documents with Indexed Document Matching

What is Indexed Document Matching?

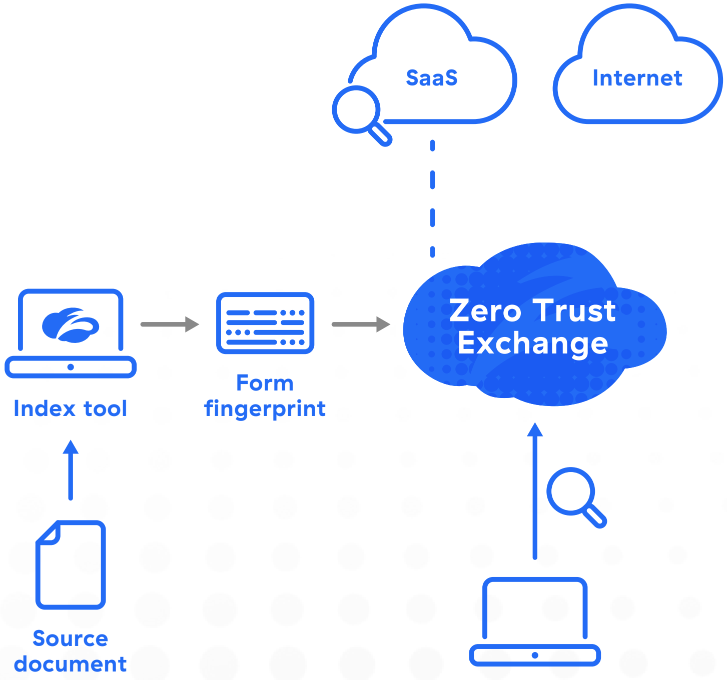
Indexed Document Matching (IDM) allows you to index forms common in your enterprise so that any files leveraging those forms can be automatically identified, whether they're scanned in motion or at rest in the cloud.

Why do organizations need IDM?

In the cloud, organizations store, process, and share a variety of sensitive documents that leverage standardized forms. From personnel, tax, and medical files to accounting, manufacturing, and other documents, they all need to be protected. Zscaler IDM enables organizations to accomplish this by scanning for forms used in documents that typically contain sensitive information.

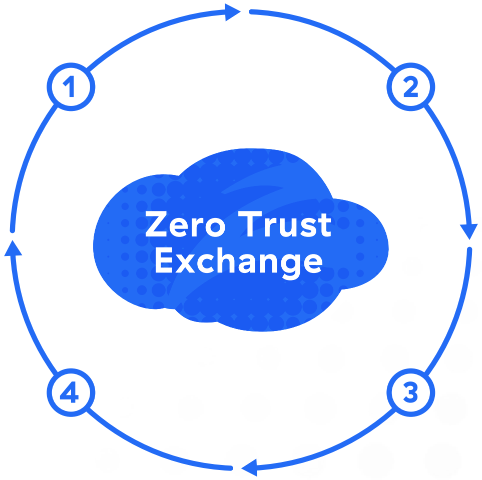
How Zscaler IDM works:

- Zscaler's Index Tool fingerprints the files of your choosing
- Form fingerprints are uploaded to the Zero Trust Exchange
- The fingerprints can then be used to identify key files



Prevent dangerous misconfigurations in workloads and SaaS

Many data loss incidents are due to misconfigurations and risky permissions in workloads and SaaS clouds. Zscaler Workload Posture (CSPM+CIEM) and SaaS Security Posture Management (SSPM) help you quickly fix them to prevent data loss and compliance issues. Here's how:



1 **Scan and discover**
Set up Zscaler to automatically scan your public or SaaS clouds, such as AWS, Azure, Google, Microsoft 365, and Salesforce.

2 **Identify findings**
Find risky permissions and dangerous misconfigurations from more than 3,000 signatures and 15 compliance frameworks.

3 **Prioritize your risks**
Receive risk-based prioritization of findings based on impact and likelihood.

4 **Remediate issues**
Quickly fix issues with manual, guided, or automatic remediation with ITSM integration.

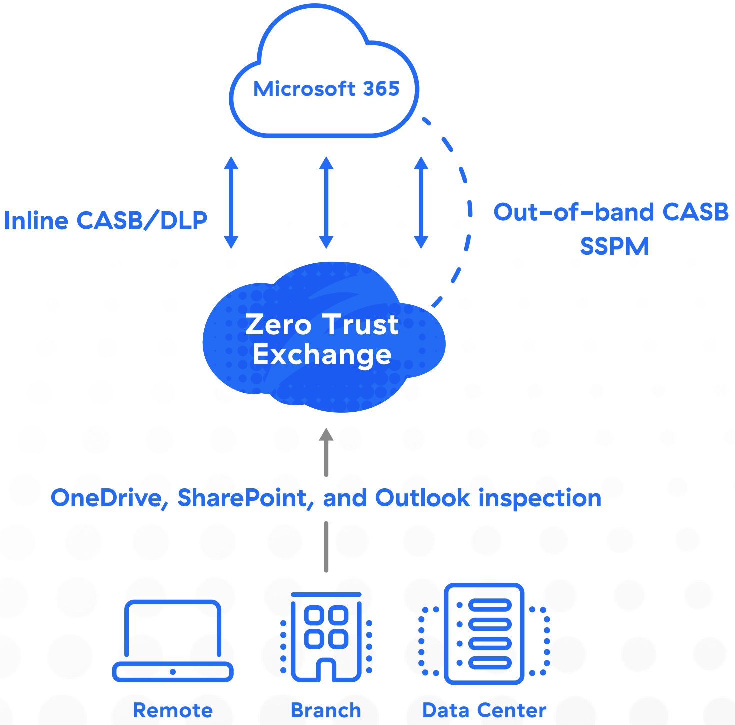
Control your critical data across Microsoft 365

Microsoft 365 is critical for enabling remote collaboration and productivity. But you need visibility and control across Microsoft 365 to ensure your data isn't exposed.

- **Enforce real-time Microsoft 365 inspection**
  With Zscaler Data Protection, you can enable real-time inspection of traffic headed to Microsoft 365. You can also enforce DLP policies to prevent business-critical and confidential data from being uploaded.

- **Scan data at rest for exposure**
  Zscaler lets you quickly identify critical data across OneDrive and SharePoint, and gives you visibility and control over who is sharing sensitive content outside the organization.

- **Identify dangerous SaaS misconfigurations**
  Zscaler SaaS Security Posture Management (SSPM) can scan your Microsoft 365 deployment for misconfigured settings that could lead to data loss, such as admin accounts without multifactor authentication (MFA) enabled, or improperly shared public folders.



Control access for unmanaged devices

Employees, partners, and customers sometimes require access to your data while using unmanaged devices. How do you ensure this data stays secure?

Control access with Zscaler Identity Proxy

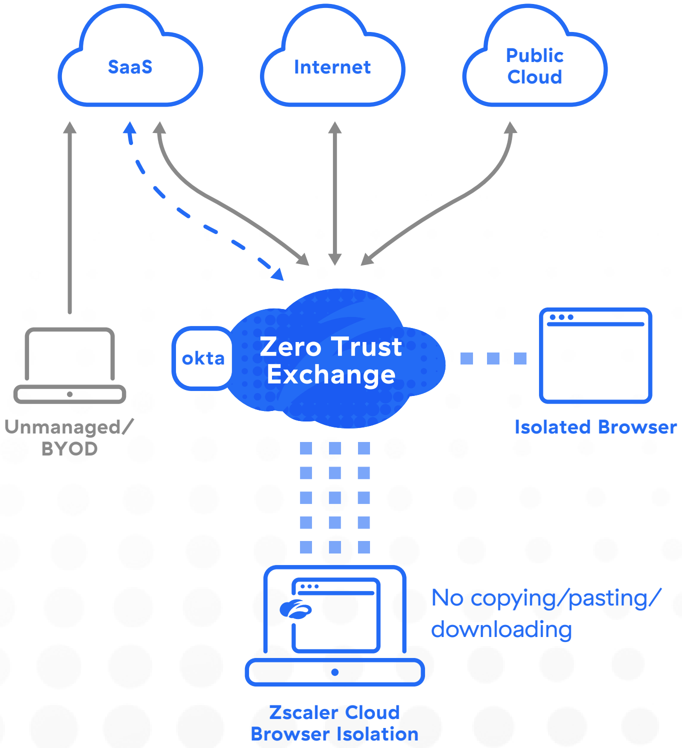
Restrict access to Microsoft 365 and Salesforce by only allowing traffic that's proxied through Zscaler and your DLP policies.

No-risk data viewing with Zscaler Cloud Browser Isolation

Data is streamed to the endpoint only as pixels. It doesn't persist on the endpoint and can't be copied, pasted, downloaded, or printed.

How Cloud Browser Isolation works to keep data safe:

- Zscaler redirects the user to an isolated browser
- Zscaler loads cloud app data into the isolated browser
- Content is streamed to the user's browser as pixels, but is fully interactive and fast



Case Study

Guild mortgage

Guild Mortgage's investment in Zscaler pays off

Guild Mortgage is a residential real estate mortgage company founded in 1960 in San Diego. After a period of explosive growth, the company needed a data protection strategy that could handle its continued expansion.

Guild Mortgage needed:

- Full inspection of all SSL traffic to prevent data loss incidents
- A security solution that could handle aggressive company growth
- Real–time visibility into data and threat incidents across the company

Zscaler provided:

- A full cloud native proxy that inspects all SSL traffic across all data in motion
- Integrated data protection across DLP and CASB, which allows for easy scalability
- Always–on policies for threat context across all connections, on– or off–network

> "Zscaler is providing us with the visibility necessary to determine what we really need to protect and how to mature our data protection program."
>
> **Josh Pernot**
> IT Security Engineer, Guild Mortgage

Maximum protection, minimal effort

Zscaler data protection follows your users and the applications they are accessing to protect your data in the cloud and mobile world. The Zscaler Zero Trust Exchange™ is a purpose-built platform that delivers the protection and visibility you need to simplify compliance and make data protection painless.

The Zero Trust Exchange:

- ✓ **Provides identical protection**
  so you can deliver a consistent data protection policy for all users, regardless of their connection or location.
- ✓ **Inspects all your SSL traffic**
  to eliminate SSL blind spots—all backed by the industry's best SLAs.
- ✓ **Simplifies compliance**
  so you can find and control PCI, PII, and PHI data with ease while improving your ability to maintain compliance requirements.
- ✓ **Eliminates complexity**
  with a unified platform that allows you to secure all your cloud data channels: data in motion, at rest, and across endpoints and clouds.

Get data protection built for a cloud-first, mobile world

Your data no longer resides in the data center. It is everywhere and accessible by employees working from outside the office and practically anywhere. Your existing security approaches can't protect data in a cloud and mobile world. With Zscaler data protection services, you can provide identical protection for your critical data regardless of where users connect or where applications are hosted. **Let us show you how.**

Learn more about the Zscaler data protection platform: zscaler.com/dp

zscaler™ | **Experience your world, secured.™**

About Zscaler
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**.