EBOOK

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

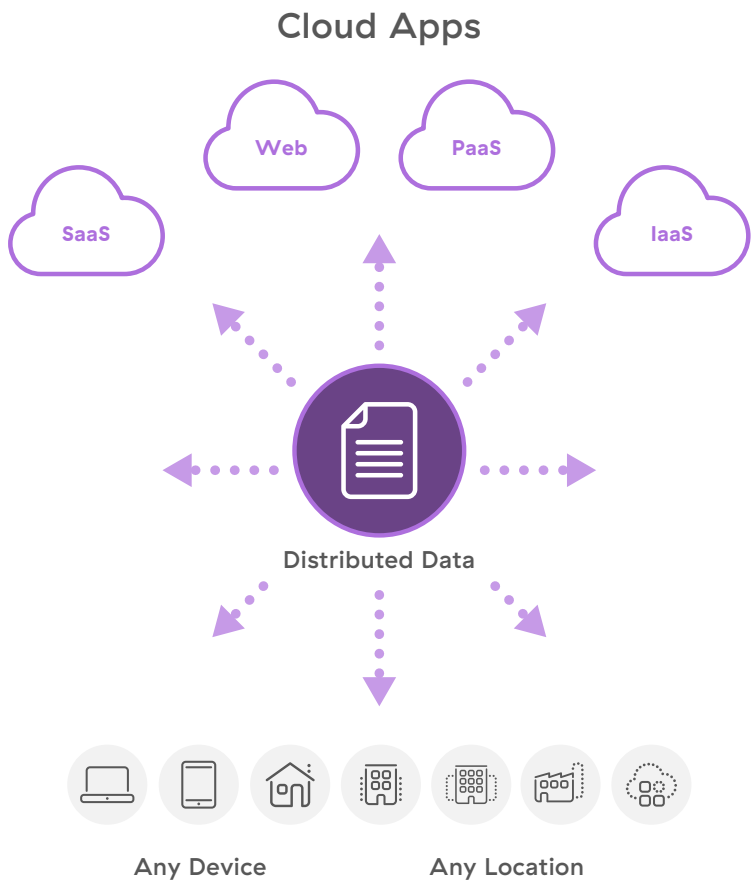
With cloud apps, your data is now widely distributed and your employees are connecting from wherever they're working—which could be anywhere. Traditional data protection approaches can't give you adequate control over your data. Here's why:

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.

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.

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

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



Zscaler Solution

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

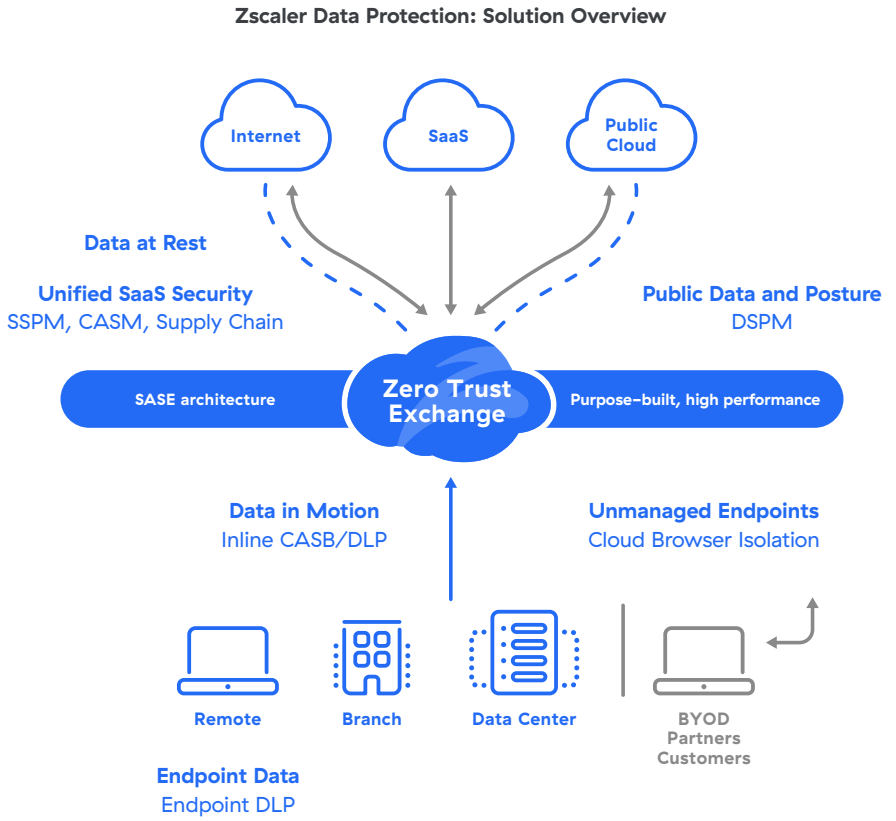
Inspect all SSL traffic for data exposure with unlimited inspection capacity per user.

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.

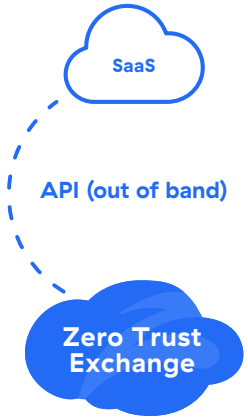


Securely govern sanctioned apps with out-of-band CASB

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, email and file-sharing. 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

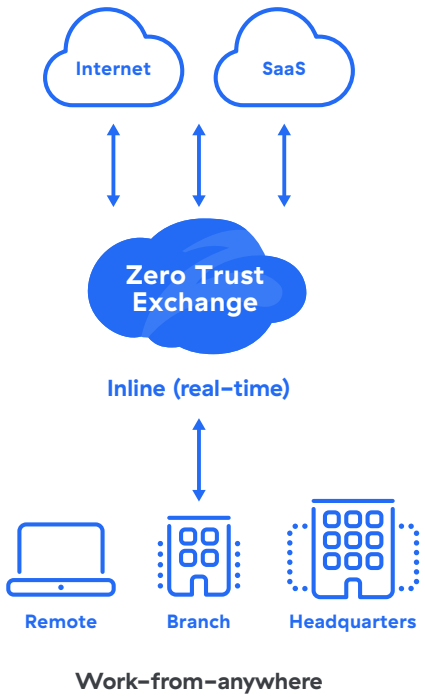
While out-of-band CASB helps secure data at rest, you still need real-time control over your cloud apps. How does inline CASB enable you to safely move to the cloud?

- **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.



- **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.

Simplify how you controldevice data with Endpoint DLP

Great data protection requires an endpoint strategy. With Endpoint DLP you get total device protection, without the complexity of traditional approaches.

- **Unified policy and visibility**
  With a centralized DLP engine, you gain consistent alerting across endpoint, inline, and cloud.
- **Single, lightweight agent**
  Built into Zscaler's existing agent, you get a better user experience by reducing the agents required on your endpoint.
- **Quick deployment**
  Leverage your existing Zscaler DLP policies to get up and running quickly.
- **Faster incident management**
  Respond to incidents faster with workflow automation and in-depth dashboards and forensics.

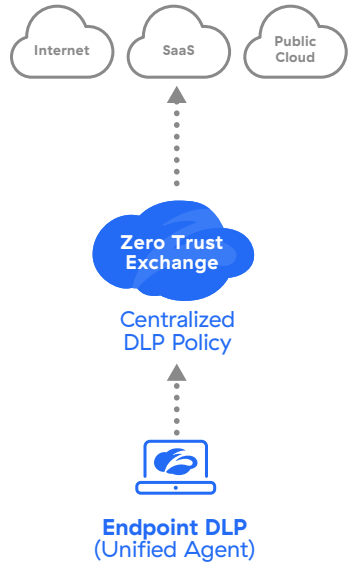
Top Use Cases for Endpoint DLP

Improve data coverage
Ensure valuable data is properly tracked and protected everywhere, without gaps

Secure employee resignations
Ensure departing employees don't copy device data and take to their next company

Retire legacy endpoint DLP
Get rid of complicated point products and deliver a unified platform

Improve compliance
Maintain regulatory compliance across files and devices



Channels Protected

Removable media	Personal cloud storage sync
Network shares	Printing

Reduce complexity with a unified approach to real-time Email DLP

One of the biggest risks to data is through email. With Zscaler's Email DLP organizations get a powerful approach to adding full DLP control over email data

Legacy approaches to securing Email data can be cumbersome and complex. With the adoption of SSE, IT teams are looking for unified approaches to securing data across email channels that reduce complexity.

With Zscaler's Email DLP leveraging Smarthost, data protection can be easily scaled to Email in real-time. Utilizing SMTP Relay, Zscaler enables effortless integrated into existing email architectures, with complete control over email data and attachments

Advantages of Zscaler's Email DLP:

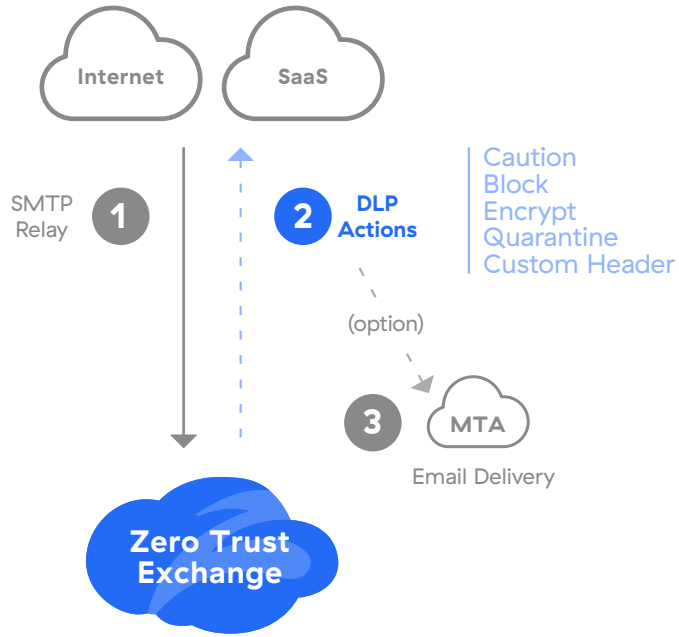
Protocol agnostic
Works on managed, unmanaged devices and even mobile

Easy deployment
No MX record changes required

Flexible policy
Adjustable policy definitions and granular policy evaluations

Centralized and unified
Single UI and DLP Engines across for all channels

Real-time Email DLP



Find and protect data instantly with AI-Driven Data Discovery

Deploying and operationalizing a data protection program can sometimes take months. With Zscaler's innovative data discovery, you can quickly understand the risk and behaviors associated with your data.

AI-Driven Data Discovery:

- Discover data across endpoints, inline and public clouds
- Quickly understand loss risks by users and apps
- Pivot to policy creation within a few clicks

Classify and protect custom data, forms and images from loss

Data classification is the heart of any good DLP program. With advanced data classification, organizations can secure special types of sensitive data from loss.

Exact Data Match (EDM)

Organizations can fingerprint and secure custom company data. Example: Trigger on customer credit card numbers, not all credit card numbers (like from an Amazon purchase).

Indexed Document Match (IDM)

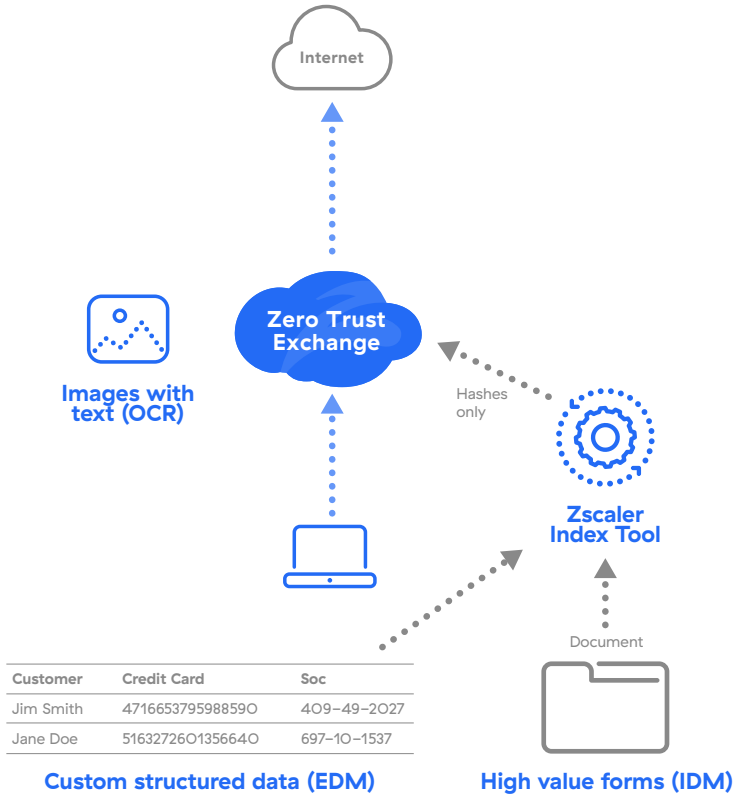
Use to fingerprint and secure custom documents and forms. Example: Fingerprint a blank tax or mortgage form and block any other filled out copy.

Optical Character Recognition (OCR)

Find and prevent data loss by identifying text within images. Example: Monitor for screen shots that may contain sensitive content.

Zscaler Indexing Tool

Companion fingerprint tool for EDM and IDM. Creates hashes of EDM and IDM data and loads into Zscaler Cloud for policy creation.



Get maximum visibility and control over Gen AI Apps

Controlling the loss of sensitive data to Generative AI apps is key to enabling these Shadow apps for productivity. Zsclaer's new innovative approach brings all protection and visibility into one place

Generative AI apps have the potential to improve productivity across your organizations. But you need complete visibility and control over these apps to be better blocking decisions

Zscaler's innovative Gen AI Security enables IT teams to discover all Gen AI Apps across the organization, and delivers unprecedented visibility including prompt level inputs, all so they better blocking decisions can be made

Benefits

- See Input prompts sent to AI App by users for complete contextual visibility
- Flexible policy controls across DLP inspection and Cloud App Control
- Enforce isolated access and protect data in Zscaler's Cloud Browser.

Gen AI Visibility

Shadow AI Discovery
Complete app catalog of all popular AI applications

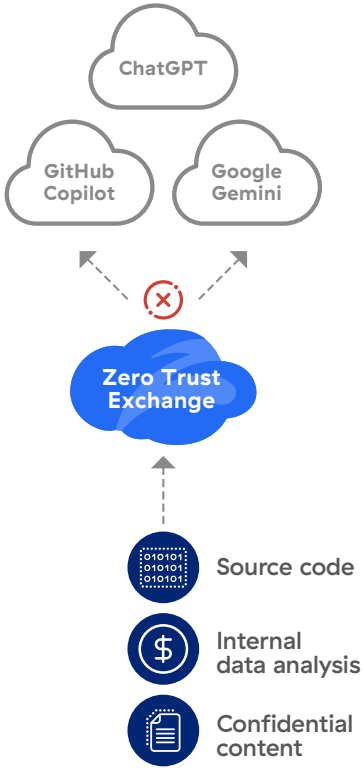
Input Prompt Visibility
See actual input prompts users are sending to AI Apps

Gen AI App Controls

DLP Inspection
Block sensitive data & content headed to AI Apps

Cloud App Control
Control AI apps access across users, departments and locations

Browser Isolation
Confine data and app useage in secure cloud browser

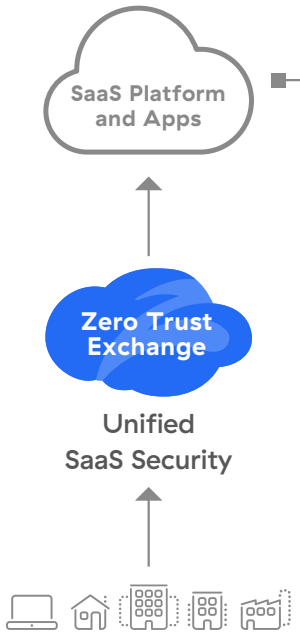


Defend your SaaS Platform with a completely integrated approach

Securing SaaS clouds and data requires too many tools. Unifying SSPM with other key SaaS Security approaches helps drastically simply how IT teams protect SaaS data and posture.

Many cloud breaches are caused by dangerous misconfigurations 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 SaaS Security Posture Management (SSPM), 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.



Unified SaaS Security
Everything to secure SaaS in one place

SaaS Security Posture Management (SSPM)
Fix misconfigurations and configuration drift

SaaS Supply Chain Security
Close risky third-party integrations

API CASB
Prevent risky sharing of sensitive data

User Activity
Monitor for risky access and collaborators

Improved context, correlation and risk reduction

Data Security Posture Management (DSPM)

Secure Public Clouds and Data with a fully integrated data protection approach

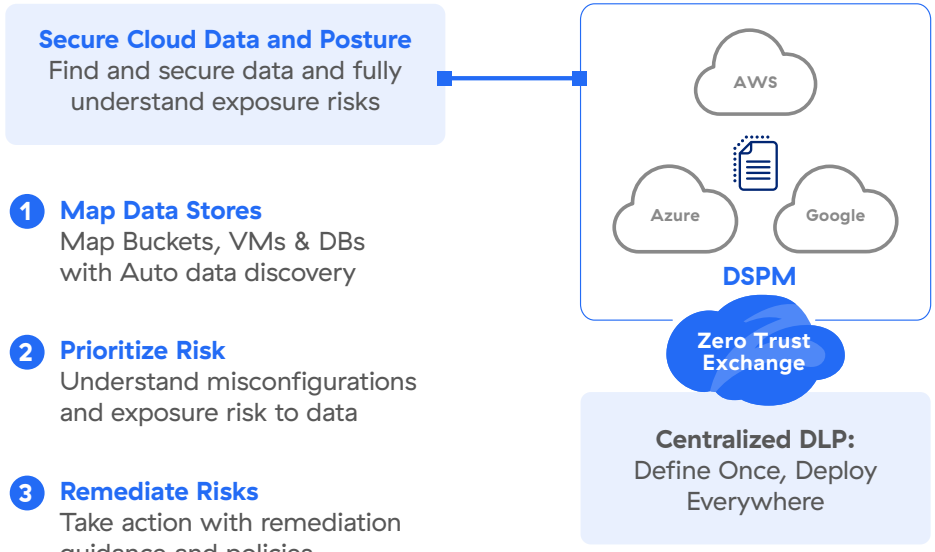
Data Protection teams need a unified approach to securing public cloud data. Zscaler's Data Security Posture Management integrates seamlessly into existing data protection programs

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, classify and secure public cloud data.

Zscaler 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.

Benefits

- Quickly find sensitive data with AI-powered auto discovery
- Correlate misconfigurations, exposure, and vulnerabilities to get greater understanding of cloud data risk
- Extend existing DLP dictionaries to public cloud data for better visibility and context
- Quickly close risks with actionable guidance on remediation



Browser Isolation

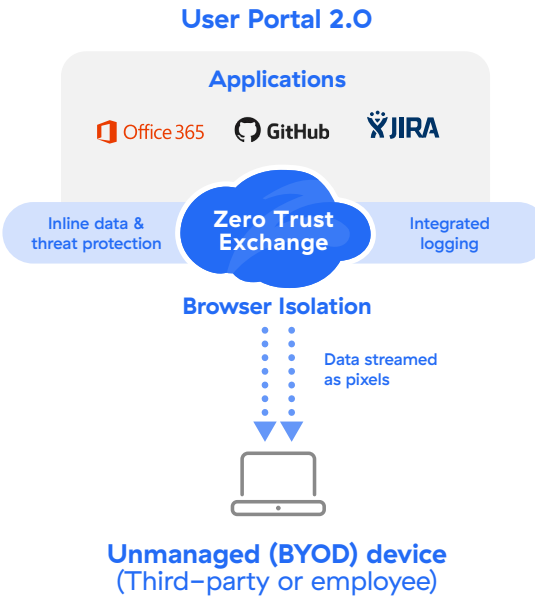
Secure web app data and access for BYOD devices

Partners, contractors, or employees sometimes require access to your data while using their personal devices. How do maintain control over this data when these devices are unmanaged?

With Zscaler User Portal 2.0 and Browser Isolation, organizations can safely support unmanaged devices. Here's how:

How User Portal 2.0 secures assess and data:

- Users, without endpoint agent requirements, authenticate into portal for a dashboard view of authorized web apps (SaaS or Private).
- Users access app within a contained/isolated browser. Data is then safely streamed to endpoint as pixels.
- App is fully interactive, however cutting, pasting, download and printing is blocked, and screen shots are even watermarked.



BYOD Benefits:

Threat and data protection

All traffic inspection by Zscaler inline, ensuring same level of security as managed devices.

Data and file isolation

View docs or share files (across apps), without download or clipboard capability on the endpoint.

Integrated DLP policies

Leverage business policies to ensure consistent protection and alerting of sensitive data.

Manage data loss incidents better with Workflow Automation

To take your data protection program to the next level, you need a powerful incident management tool that streamlines operations and enables user coaching.

Many protection programs struggle because of disjointed incidents and tools. Additionally, users never learn what risks behaviors they made when handling data incorrectly.

Zscaler Workflow Automation delivers a dedicated tool for DLP admins to supercharge incident management.

With all forensics in one place, admins can quickly understand risky behaviors, assign incidents to users for justification, and quickly implement policy actions to resolve incidents

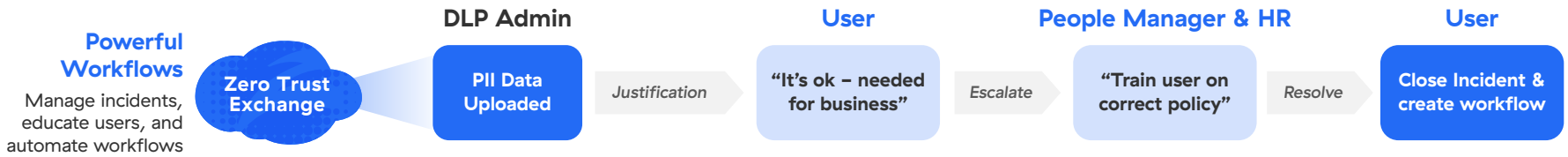
How Workflow Automation helps your data protection program

Faster incident management
Save time with a purpose-built platform for data loss incident management

User coaching
Justify incidents with users via Slack, Teams, or email, while educating about data protection best practices

Automated routines
Streamline daily operations by using workflows to automate repetitive tasks and escalations

Fully integrated
Avoid common protection program failures by delivering a comprehensive incident handling system



Summary

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.**

See customer success stories about Zscaler data protection >

Get the ebook

Learn more about the Zscaler data protection platform >

zscaler.com/dlp

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 SSE–based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com