Data Protection Technical:

Five Critical Steps to Secure your Cloud Data

Cloud Apps have helped drive this transformation

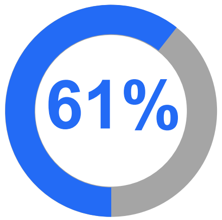
Increases collaboration and productivity - reduces cost and complexity

salesforce now Office 365 workday aws Azure

But are causing new challenges

Distributed data

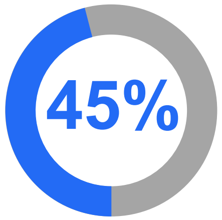
Security appliances weren't built for the cloud



claim their network security can't scale or is too complex[1]

Mobile users

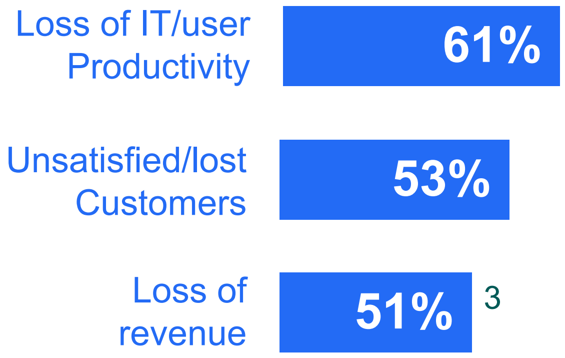
Off network, away from security and using risky unmanaged devices



are struggling with risky BYOD usage[2]

Data Exposure

Cloud data often easily exposed and exfiltrated, causing:



[3]

1,3: Zscaler Data@Risk Report 2: Zscaler VPN Risk Report

Top initiatives to secure data:

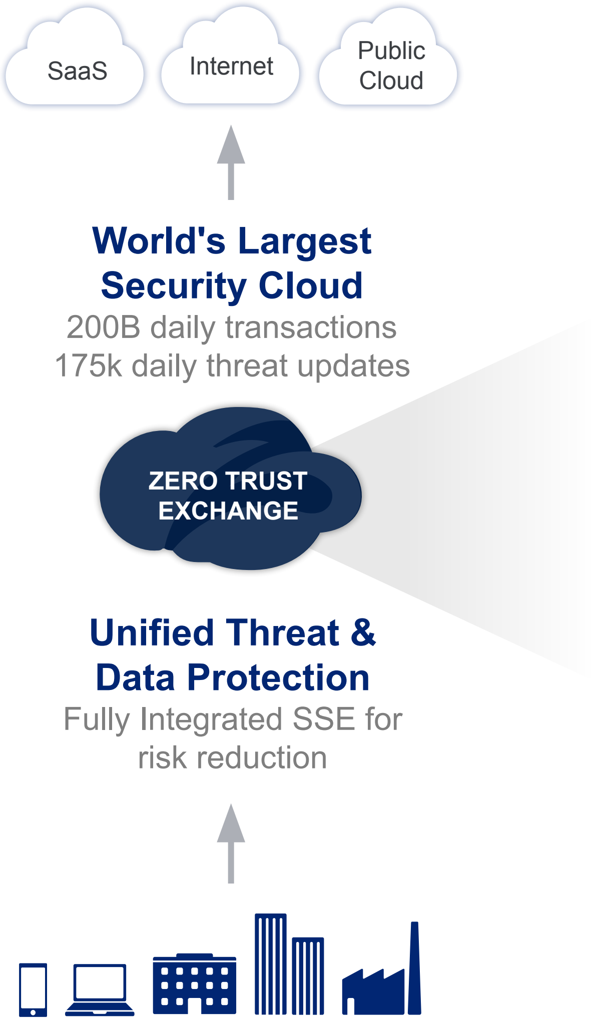
1 **Prevent data loss and breaches**
Secure distributed and sensitive data

2 **Secure data collaboration and prevent exposure**
Get better visibility of collaboration risks

3 **Restore regulatory compliance**
Enforce proper risk controls per requirements

4 **Reduce cost & complexity**
Simplify and centralize data protection operations

Delivering Data Protection with Zscaler Zero Trust Exchange



World's Largest Security Cloud

200B daily transactions
175k daily threat updates

Unified Threat & Data Protection

Fully Integrated SSE for risk reduction

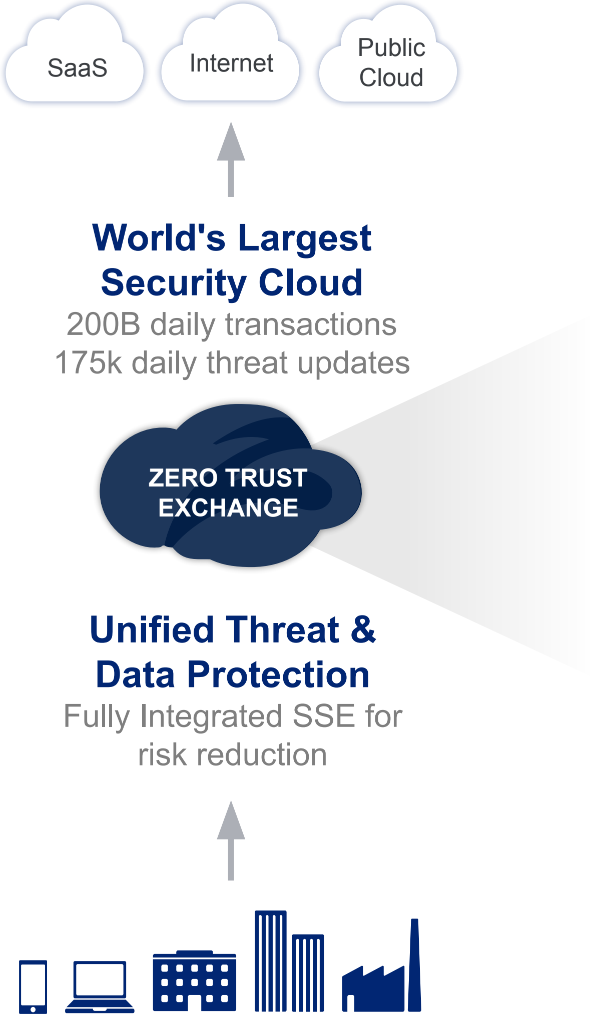
Complete Data Protection:

How to stop both **External** and **Internal** Threats

Recommended Steps

1	**Full Visibility**	Shadow IT, 3rd Party Apps, Endpoints (Activities and Configuration)
2	**Reduce Exposure and Mitigate Risk**	Secure internet, Approved SaaS Apps, Tenancy Restrictions, Cloud App Instances
3	**Gain Control of Content Types**	Block based on File Types, Size, Unscannable Content for Upload/Download
4	**Control Sensitive Data**	Control sensitive data - Device, Network, Cloud
5	**Advanced Incident Management**	Perform DLP incident triage and investigations all in one spot

Delivering Data Protection with Zscaler Zero Trust Exchange



World's Largest Security Cloud

200B daily transactions
175k daily threat updates

Unified Threat & Data Protection

Fully Integrated SSE for risk reduction

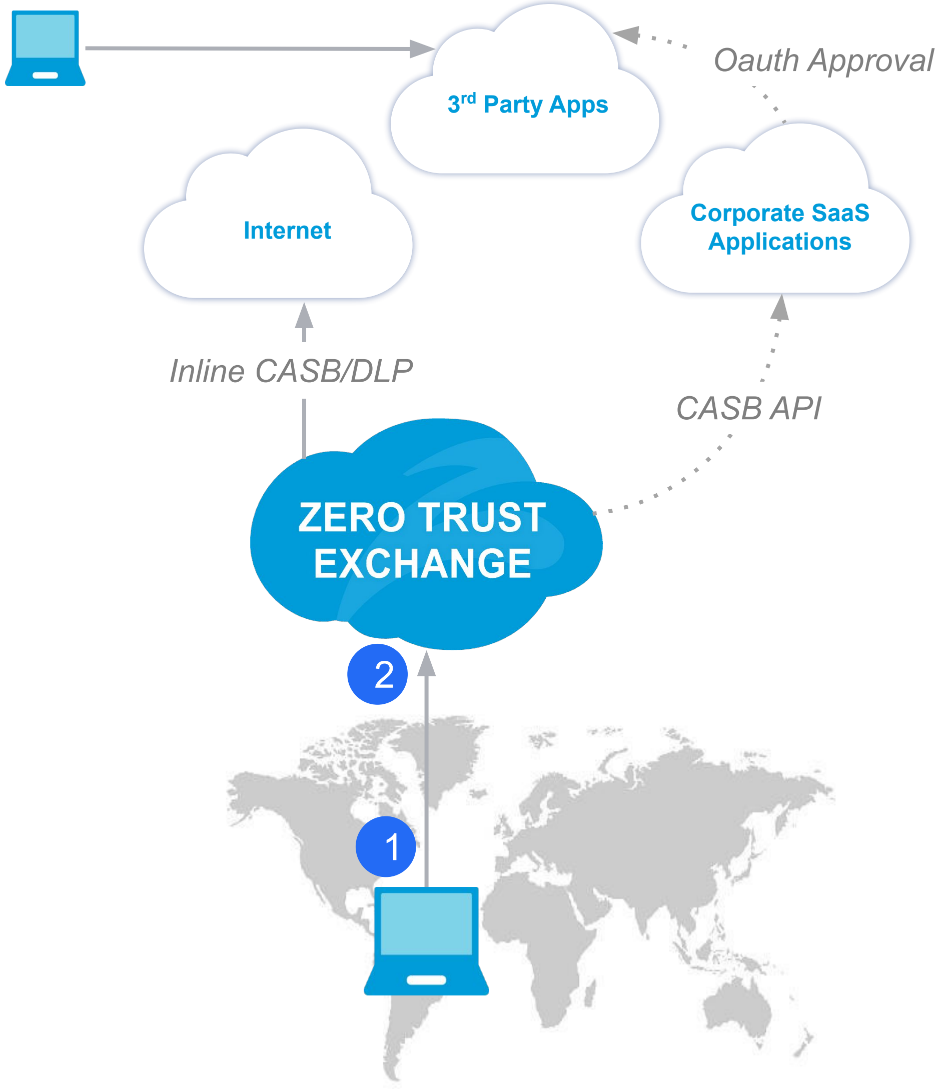
Complete Data Protection:

How to stop both **External** and **Internal** Threats

Required Steps

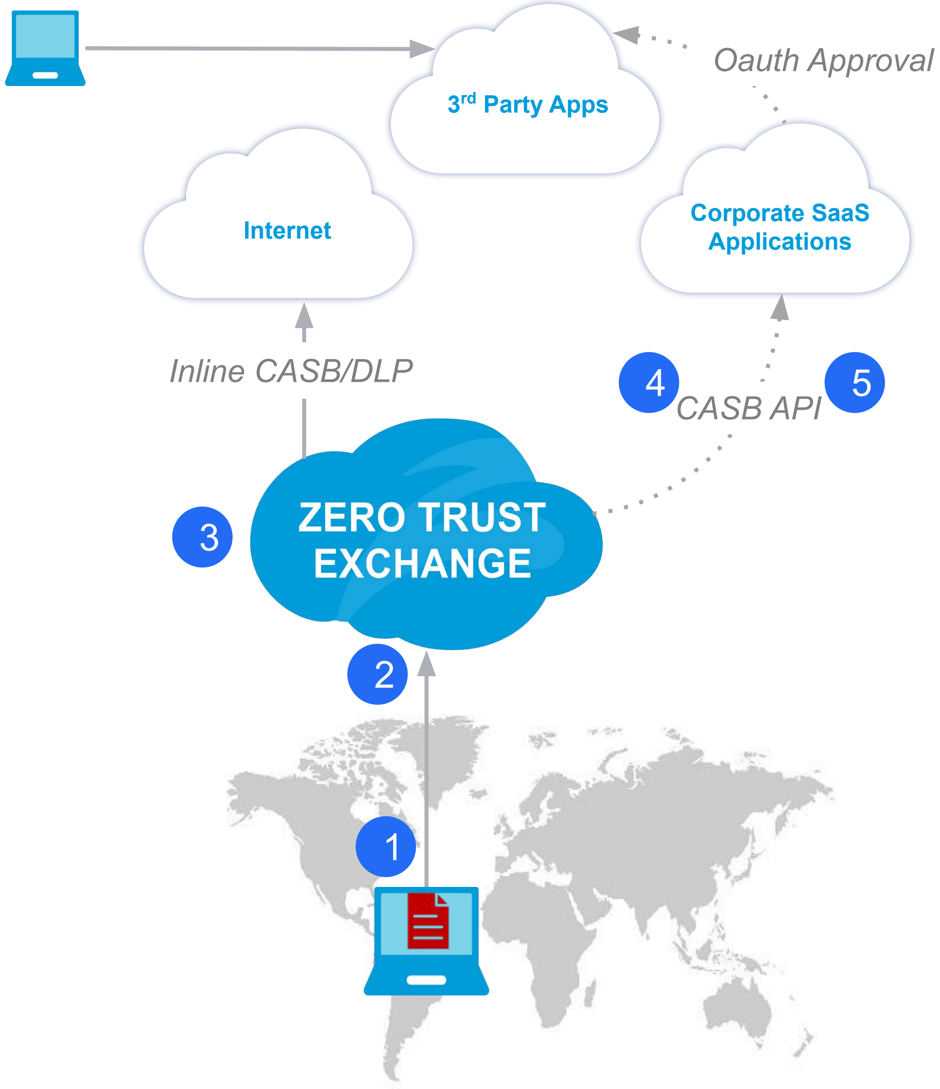
1	**Full Visibility**	Shadow IT, 3rd Party Apps, SSPM (Activities and Configuration)
2	**Reduce Exposure and Mitigate Risk**	Secure Internet, Approved SaaS Apps, Tenancy Restrictions, Cloud App Instances
3	**Gain Control of Content Types**	Block based on File Types, Size, Unscannable Content for Upload/Download
4	**Control Sensitive Data**	Control Sensitive Data-Device, Network, Cloud
5	**Advanced Incident Management**	Perform DLP incident triage and investigations all in one spot

Get Full Visibility to Cloud Apps and Data



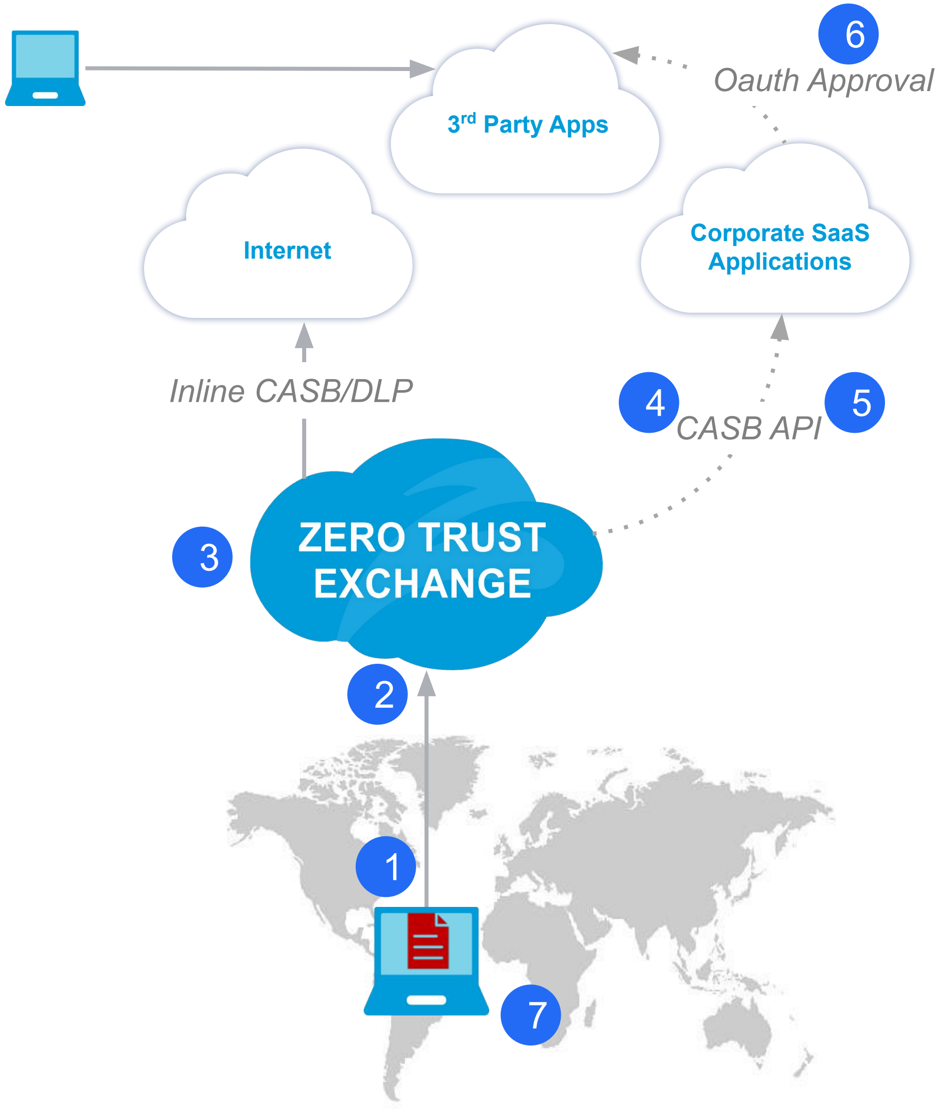
1. Full Visibility of Who is connecting, Access Context, Where is Connection Going.
2. Full visibility with Scalable SSL Decryption and Shadow IT

Get Full Visibility to Cloud Apps and Data



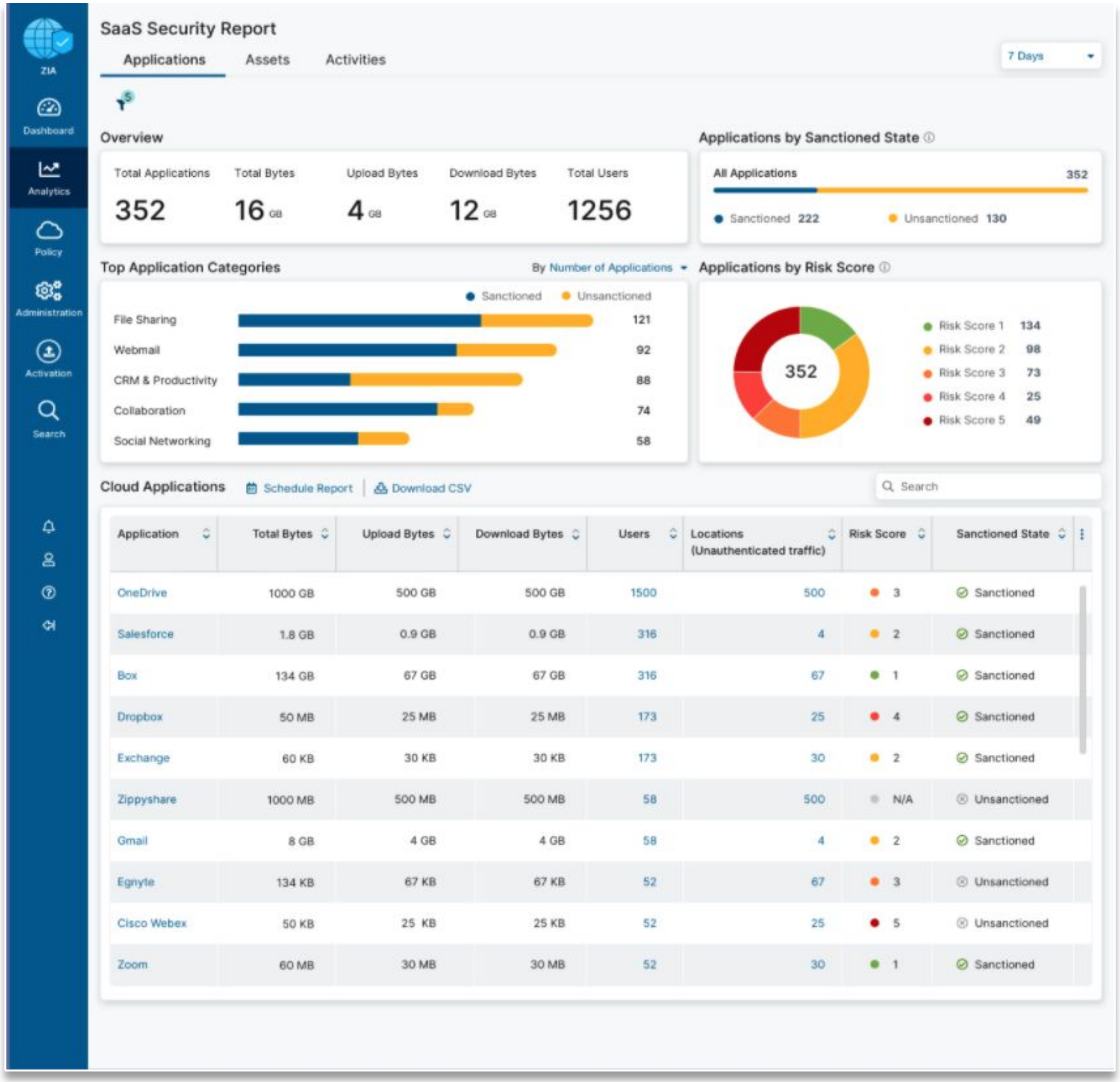
1. Full Visibility of Who is connecting, Access Context, Where is Connection Going.
2. Full visibility with Scalable SSL Decryption and Shadow IT
3. Zero Touch Configuration Data Discovery for data in motion
4. SaaS Misconfigurations
5. Visibility of User Activities to SaaS Application with UEBA

Get Full Visibility to Cloud Apps and Data



1. Full Visibility of Who is connecting, Access Context, Where is Connection Going.
2. Full visibility with Scalable SSL Decryption and Shadow IT
3. Zero Touch Configuration Data Discovery for data in motion
4. SaaS Misconfigurations
5. Visibility of User Activities to SaaS Application with UEBA
6. Visibility of 3rd Party Apps performing Oauth.
7. Visibility of activities that end users take with sensitive data on endpoints

Find cloud app usage with Shadow IT Visibility



SaaS Security Report

Applications | Assets | Activities | 7 Days

Overview

Total Applications	Total Bytes	Upload Bytes	Download Bytes	Total Users
352	16 GB	4 GB	12 GB	1256

Applications by Sanctioned State

All Applications 352

● Sanctioned 222 ● Unsanctioned 130

Top Application Categories — By Number of Applications

● Sanctioned ● Unsanctioned

Category	Count
File Sharing	121
Webmail	92
CRM & Productivity	88
Collaboration	74
Social Networking	58

Applications by Risk Score

352

Risk Score	Count
● Risk Score 1	134
● Risk Score 2	98
● Risk Score 3	73
● Risk Score 4	25
● Risk Score 5	49

Cloud Applications — Schedule Report | Download CSV — Search

Application	Total Bytes	Upload Bytes	Download Bytes	Users	Locations (Unauthenticated traffic)	Risk Score	Sanctioned State
OneDrive	1000 GB	500 GB	500 GB	1500	500	● 3	✓ Sanctioned
Salesforce	1.8 GB	0.9 GB	0.9 GB	316	4	● 2	✓ Sanctioned
Box	134 GB	67 GB	67 GB	316	67	● 1	✓ Sanctioned
Dropbox	50 MB	25 MB	25 MB	173	25	● 4	✓ Sanctioned
Exchange	60 KB	30 KB	30 KB	173	30	● 2	✓ Sanctioned
Zippyshare	1000 MB	500 MB	500 MB	58	500	● N/A	⊗ Unsanctioned
Gmail	8 GB	4 GB	4 GB	58	4	● 2	✓ Sanctioned
Egnyte	134 KB	67 KB	67 KB	52	67	● 3	⊗ Unsanctioned
Cisco Webex	50 KB	25 KB	25 KB	52	25	● 5	⊗ Unsanctioned
Zoom	60 MB	30 MB	30 MB	52	30	● 1	✓ Sanctioned

Get complete visibility of cloud app usage

See Trending Cloud Apps

- Understand trending apps across ALL users - on an off network
- View by Category, Usage, Users, and Search

Identify Cloud App Risks

- Find risky app usage that can lead to data loss
- Sort by risk score and apply sanctioned or unsanctioned tagging

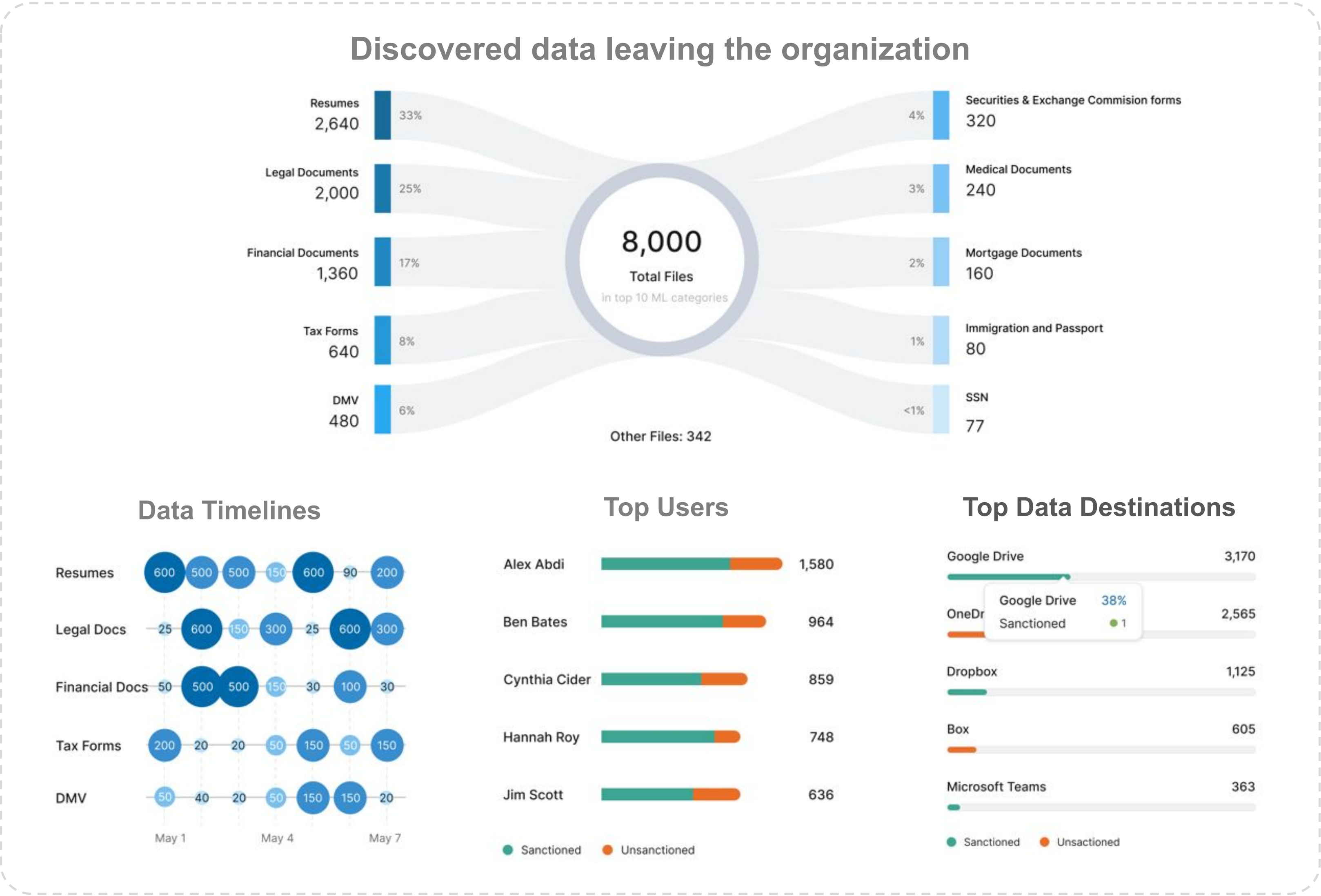
Easily understand data risks with ML-Powered Discovery

ML-Powered Data Discovery

See all data risks with ease

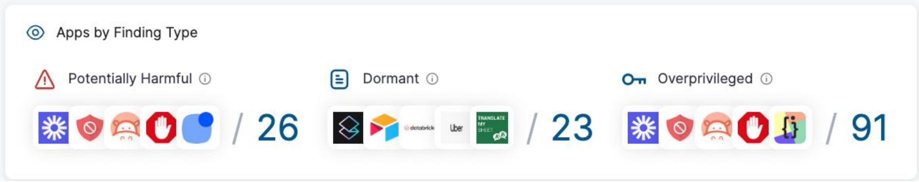
Accelerated deployments –
no administration needed!

Pivot to policy creation
in a few clicks



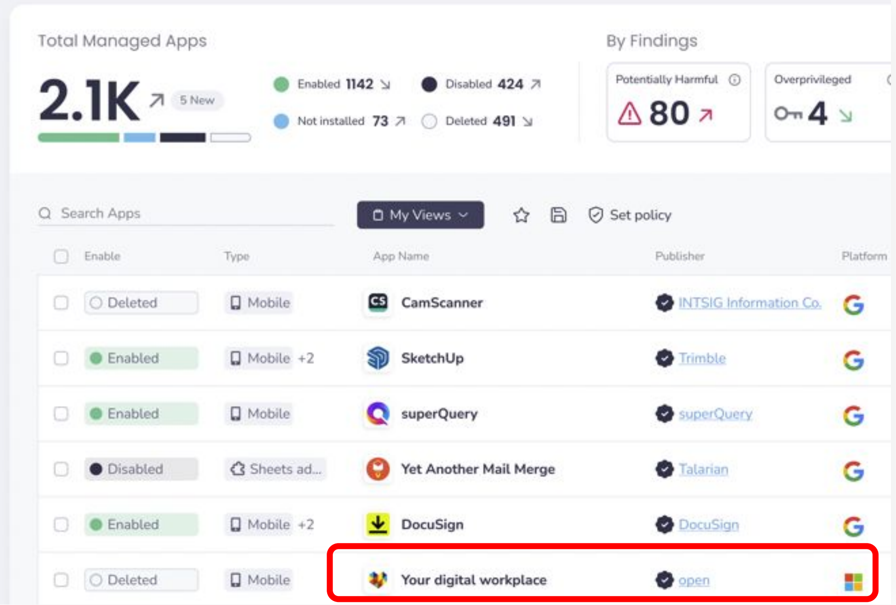
Use AppTotal to govern Third-Party Apps

DISCOVER › **ANALYZE** › **REMEDIATE**



Apps by Finding Type

Potentially Harmful	Dormant	Overprivileged
/ 26	/ 23	/ 91



Total Managed Apps

2.1K ↗ 5 New

● Enabled 1142 ↘ ● Disabled 424 ↗
● Not installed 73 ↗ ○ Deleted 491 ↘

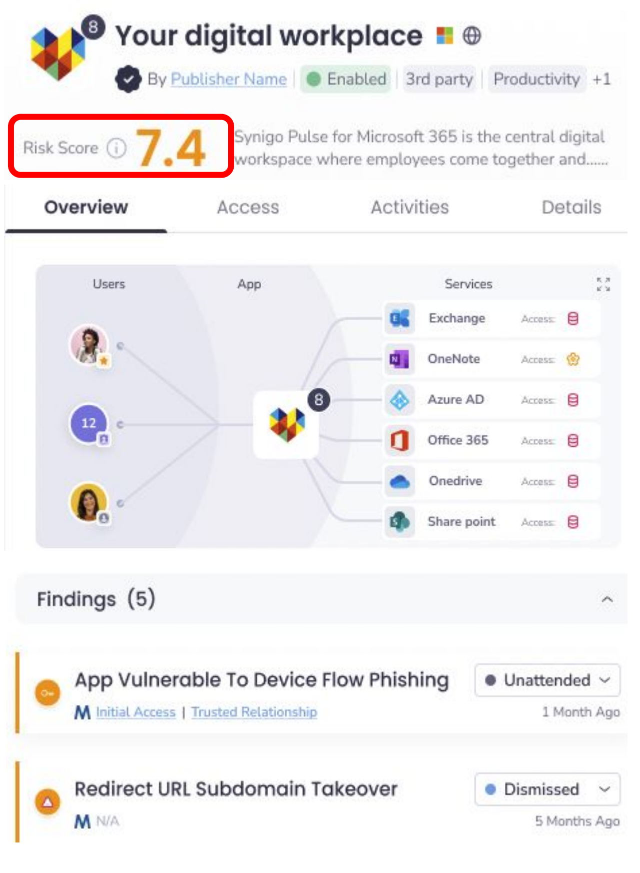
By Findings

Potentially Harmful ⚠ 80 ↗

Overprivileged 4 ↘

Search Apps | My Views | Set policy

☐ Enable	Type	App Name	Publisher	Platform
☐ ○ Deleted	Mobile	CamScanner	INTSIG Information Co.	G
☐ ● Enabled	Mobile +2	SketchUp	Trimble	G
☐ ● Enabled	Mobile	superQuery	superQuery	G
☐ ● Disabled	Sheets ad...	Yet Another Mail Merge	Talarian	G
☐ ● Enabled	Mobile +2	DocuSign	DocuSign	G
☐ ○ Deleted	Mobile	Your digital workplace	open	▦



Your digital workplace

By Publisher Name | Enabled | 3rd party | Productivity +1

Risk Score 7.4

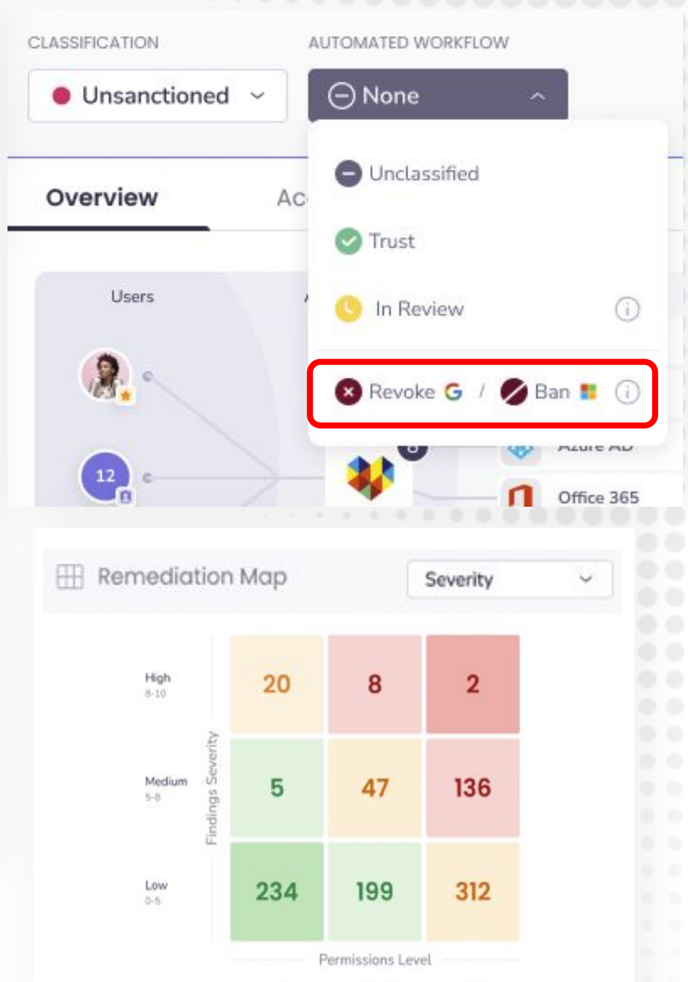
Synigo Pulse for Microsoft 365 is the central digital workspace where employees come together and......

Overview | Access | Activities | Details

Findings (5)

App Vulnerable To Device Flow Phishing — ● Unattended
M Initial Access | Trusted Relationship — 1 Month Ago

Redirect URL Subdomain Takeover — ● Dismissed
M N/A — 5 Months Ago



CLASSIFICATION: ● Unsanctioned

AUTOMATED WORKFLOW: None

- Unclassified
- Trust
- In Review
- Revoke G / Ban ▦

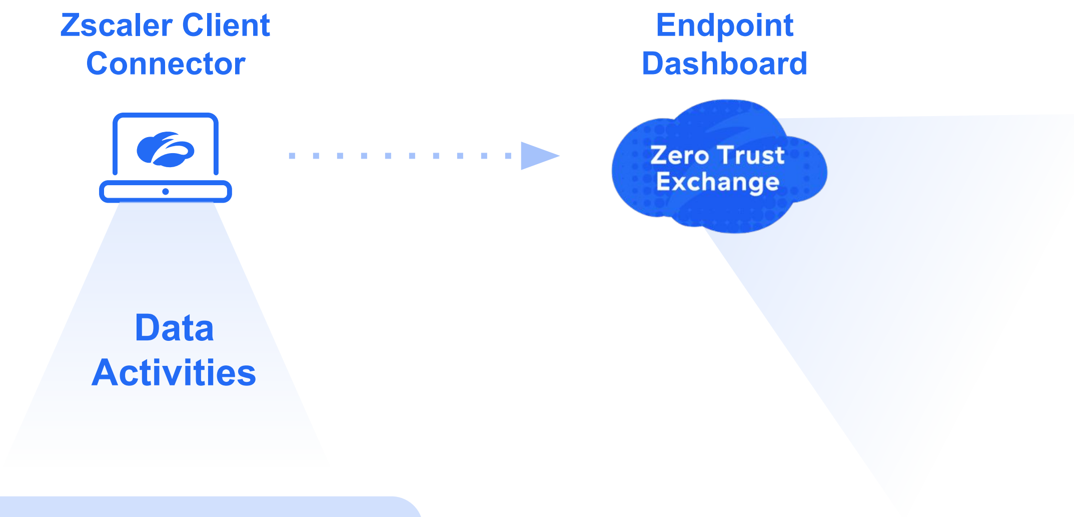
Remediation Map — Severity

Findings Severity			
High 8-10	20	8	2
Medium 5-8	5	47	136
Low 0-5	234	199	312

Permissions Level

Platforms Supported | **50K+ Applications analyzed** | **130K+ App Extensions analyzed**

Instant visibility out of the box with Data Activities



Zscaler Client Connector

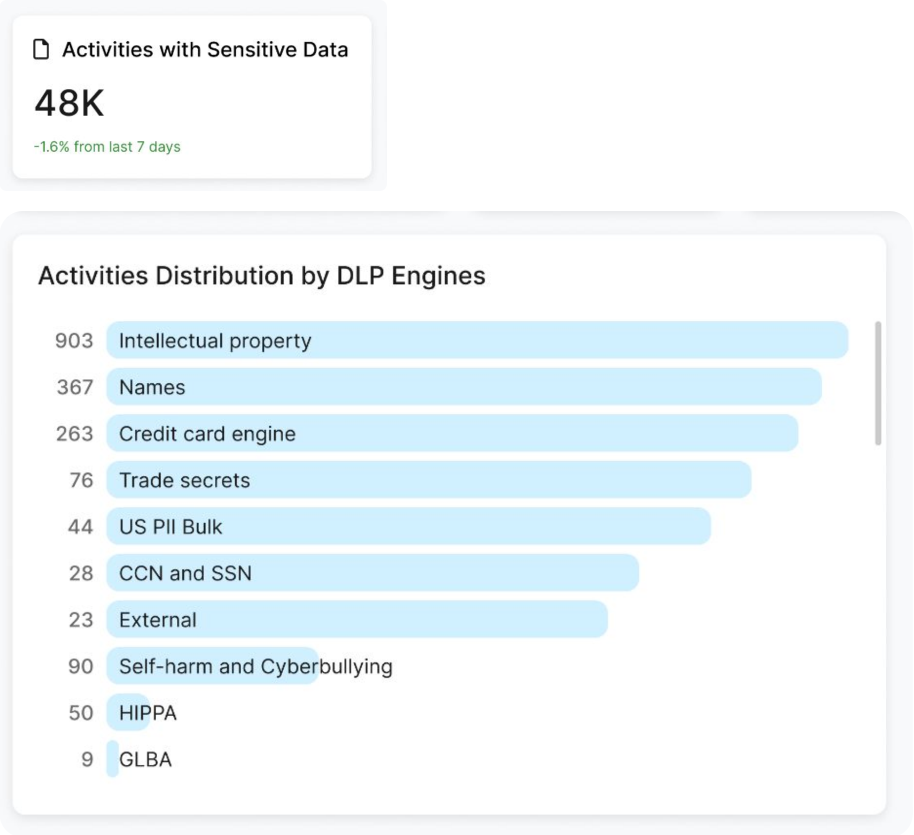
Endpoint Dashboard

Zero Trust Exchange

Data Activities

Immediate visibility post install

No Policy Configuration required



Activities with Sensitive Data

48K

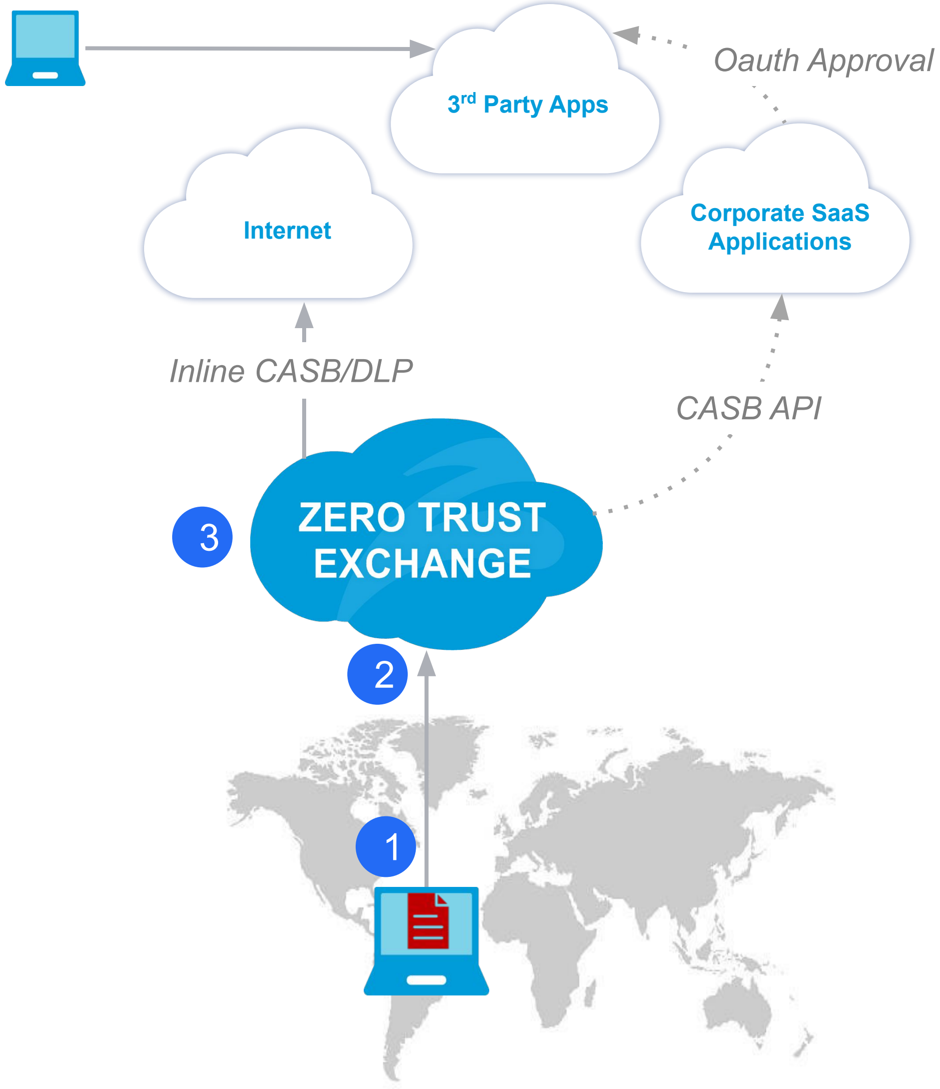
-1.6% from last 7 days

Activities Distribution by DLP Engines

903	Intellectual property
367	Names
263	Credit card engine
76	Trade secrets
44	US PII Bulk
28	CCN and SSN
23	External
90	Self-harm and Cyberbullying
50	HIPPA
9	GLBA

Easily pivot to creating block policies

Get Full Visibility to Cloud Apps and Data

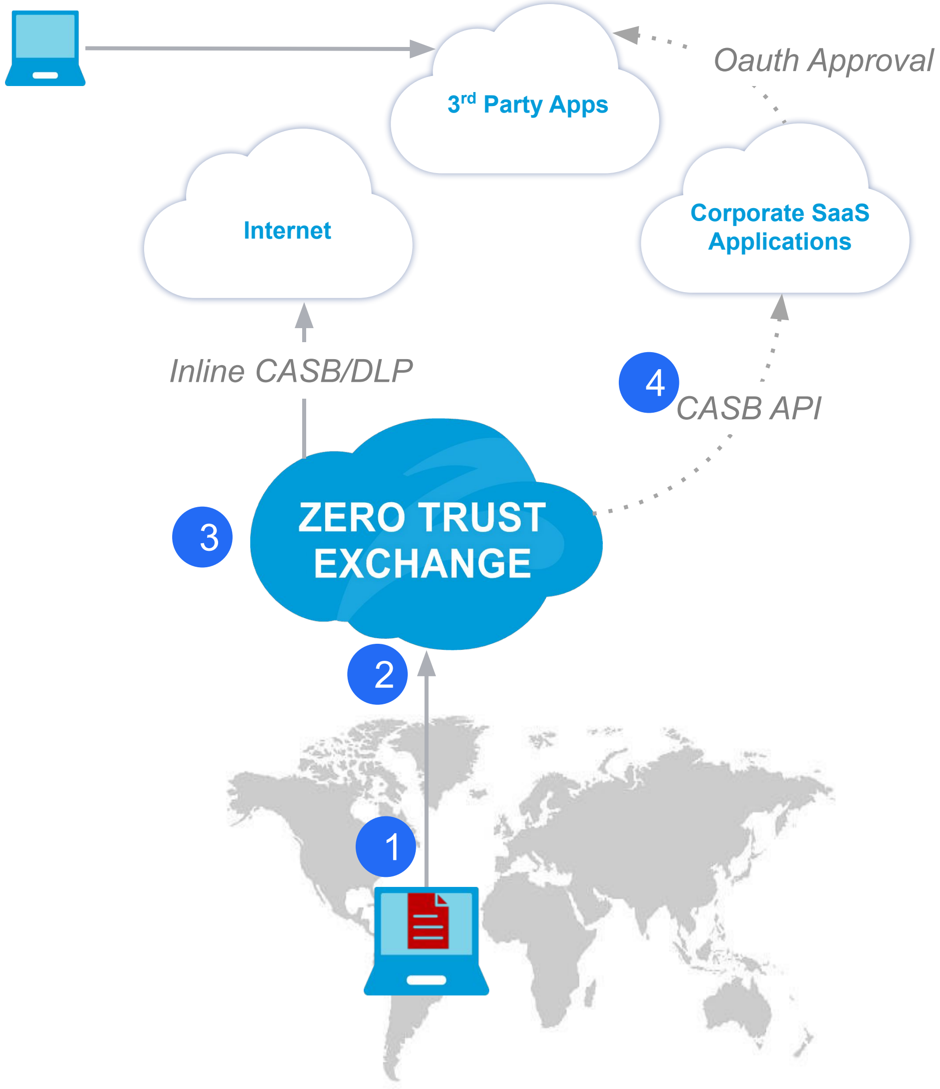


1 Full Visibility of Who is connecting, Access Context, Where is Connection Going.

2 Full visibility with Scalable SSL Decryption and Shadow IT

3 Zero Touch Configuration Data Discovery for data in motion

Get Full Visibility to Cloud Apps and Data



1. Full Visibility of Who is connecting, Access Context, Where is Connection Going.
2. Full visibility with Scalable SSL Decryption and Shadow IT
3. Zero Touch Configuration Data Discovery for data in motion
4. SaaS Misconfigurations

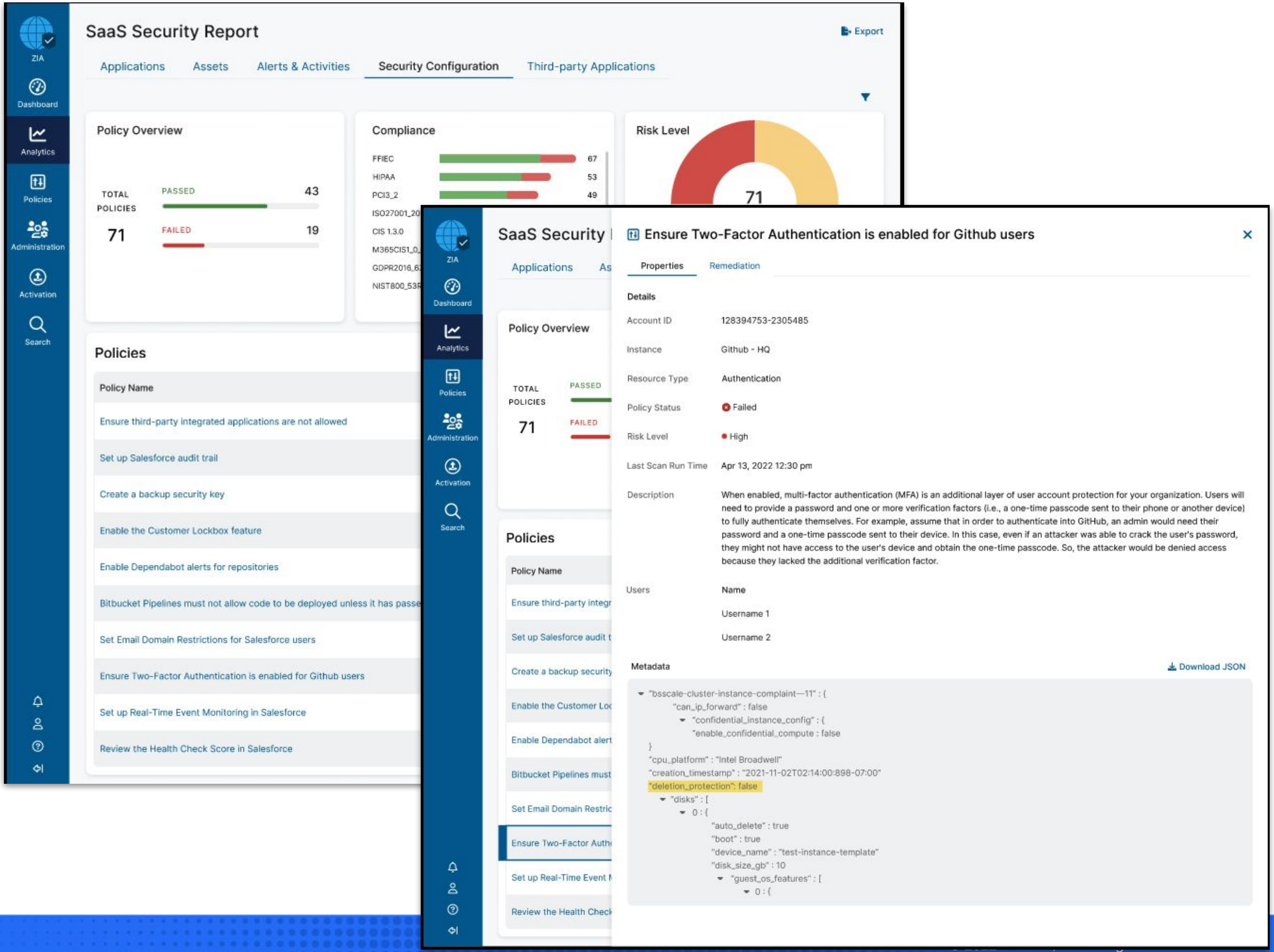
SaaS Security Posture Management (SSPM)

Breadth of Integration

- Support Posture Reporting for O365, Google Workspace, SFDC, Confluence, Bitbucket and GitHub.

Deep Security Checks

- Continuous Periodic Posture Evaluation
- 150+ predefined policies
- Multiple Compliance Frameworks: FFIEC, PCI 3.2, GDPR, HIPAA, NIST 800-53, ISO 27001:2013, SOC2 AICPA, CIS 1.3.0, M365 CIS 1.0.0
- Contextual Reporting: Provides metadata around ‘resources type” ‘Status’ and ‘Risk level’
- Remediation Change with Threat & likely Impact information



Policies

Policy Name
Ensure third-party integrated applications are not allowed
Set up Salesforce audit trail
Create a backup security key
Enable the Customer Lockbox feature
Enable Dependabot alerts for repositories
Bitbucket Pipelines must not allow code to be deployed unless it has passe
Set Email Domain Restrictions for Salesforce users
Ensure Two-Factor Authentication is enabled for Github users
Set up Real-Time Event Monitoring in Salesforce
Review the Health Check Score in Salesforce

Ensure Two-Factor Authentication is enabled for Github users

Details

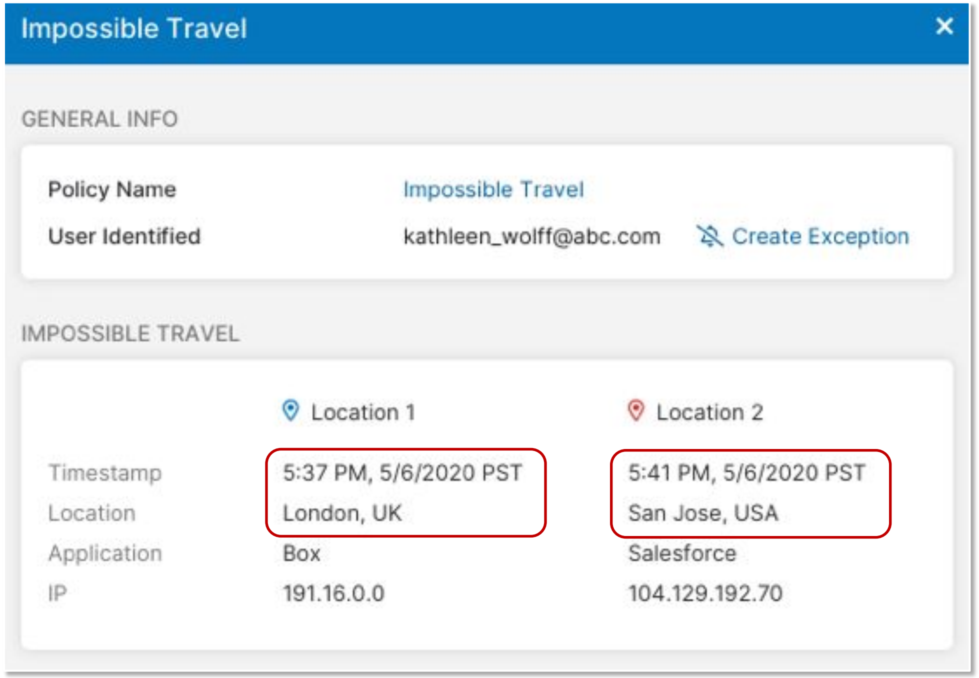
Account ID	128394753-2305485
Instance	Github - HQ
Resource Type	Authentication
Policy Status	Failed
Risk Level	High
Last Scan Run Time	Apr 13, 2022 12:30 pm
Description	When enabled, multi-factor authentication (MFA) is an additional layer of user account protection for your organization. Users will need to provide a password and one or more verification factors (i.e., a one-time passcode sent to their phone or another device) to fully authenticate themselves. For example, assume that in order to authenticate into GitHub, an admin would need their password and a one-time passcode sent to their device. In this case, even if an attacker was able to crack the user's password, they might not have access to the user's device and obtain the one-time passcode. So, the attacker would be denied access because they lacked the additional verification factor.
Users	Name Username 1 Username 2

Metadata

```
"bsscale-cluster-instance-complaint—11" : {
        "can_ip_forward" : false
      "confidential_instance_config" : {
        "enable_confidential_compute : false
  }
  "cpu_platform" : "Intel Broadwell"
  "creation_timestamp" : "2021-11-02T02:14:00:898-07:00"
  "deletion_protection": false
    "disks" : [
      0 : {
          "auto_delete" : true
          "boot" : true
          "device_name" : "test-instance-template"
          "disk_size_gb" : 10
        "guest_os_features" : [
          0 : {
```

Identity Risky SaaS App Behavior with UEBA

User and Entity Behavior Analytics



Impossible Travel ✕

GENERAL INFO

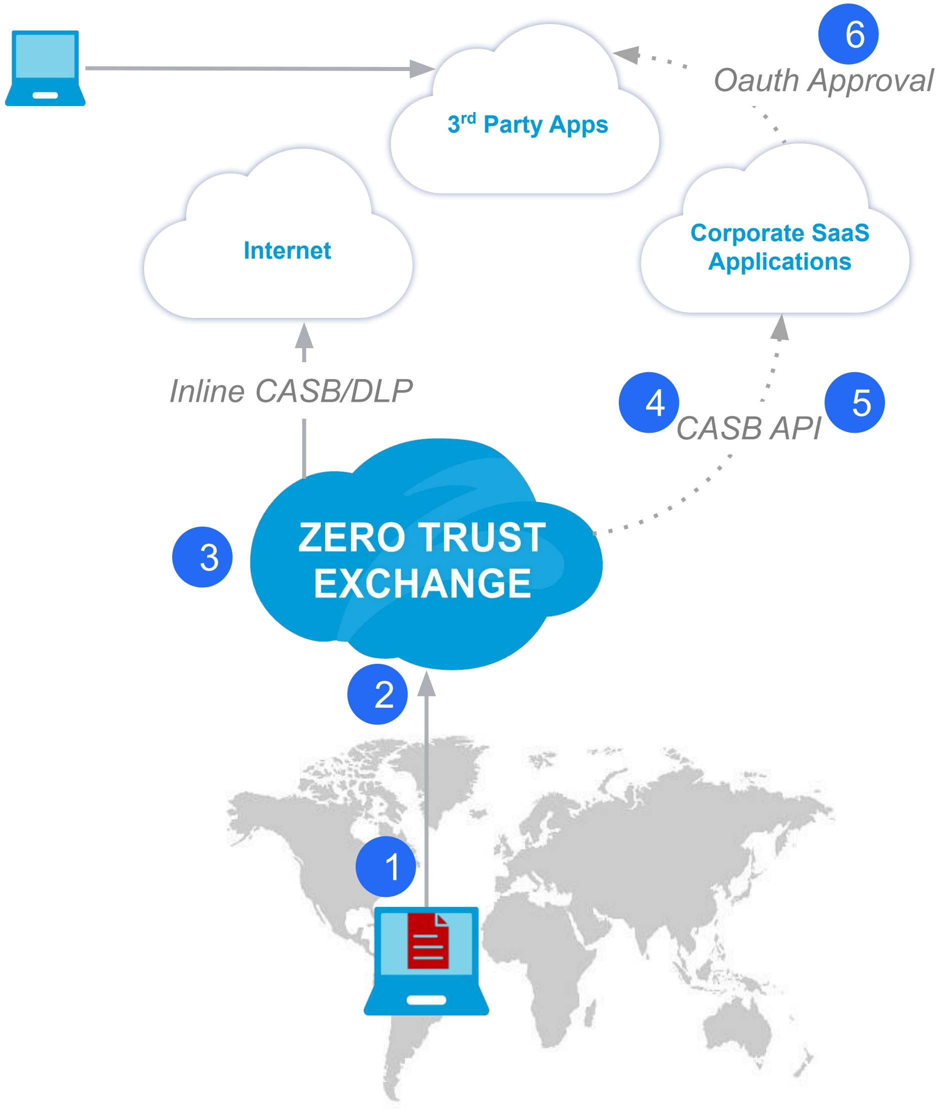
Policy Name	Impossible Travel
User Identified	kathleen_wolff@abc.com Create Exception

IMPOSSIBLE TRAVEL

	Location 1	Location 2
Timestamp	5:37 PM, 5/6/2020 PST	5:41 PM, 5/6/2020 PST
Location	London, UK	San Jose, USA
Application	Box	Salesforce
IP	191.16.0.0	104.129.192.70

- Identify risky cloud app behaviors like:
  - Impossible Travel
  - Bulk Downloads
  - Bulk Uploads
  - Failed Logins
- Full UEBA Dashboard enables quick filtering and sorting

Get Full Visibility to Cloud Apps and Data



1 Full Visibility of Who is connecting, Access Context, Where is Connection Going.

2 Full visibility with Scalable SSL Decryption and Shadow IT

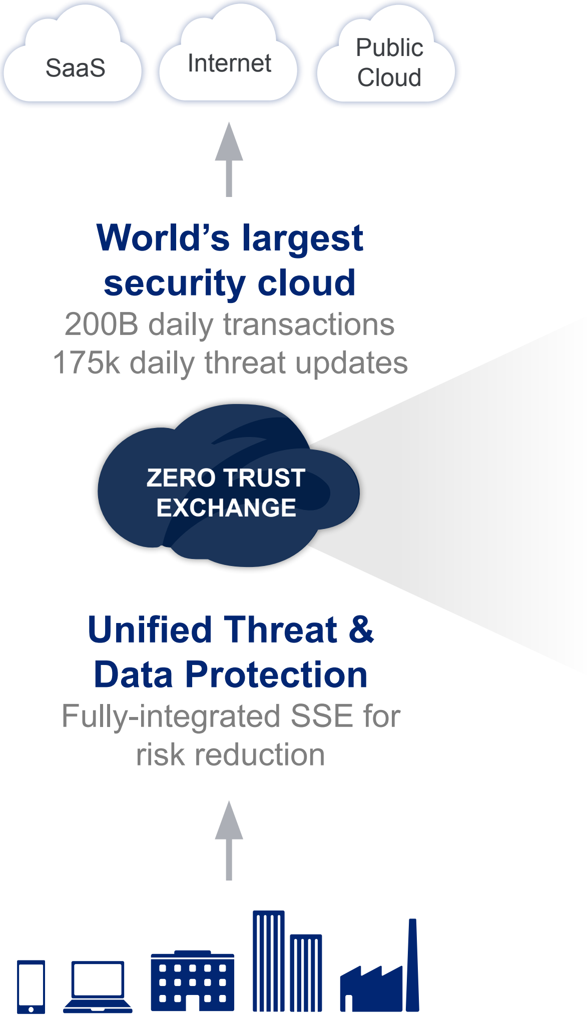
3 Zero Touch Configuration Data Discovery for data in motion

4 SaaS Misconfigurations

5 Visibility of User Activities to SaaS Application with UEBA

6 Visibility of 3rd Party Apps performing Oauth.

Delivering Data Protection with Zscaler Zero Trust Exchange


SaaS
Internet
Public Cloud
World's largest security cloud
200B daily transactions
175k daily threat updates
ZERO TRUST EXCHANGE
Unified Threat & Data Protection
Fully-integrated SSE for risk reduction

Complete Data Protection:

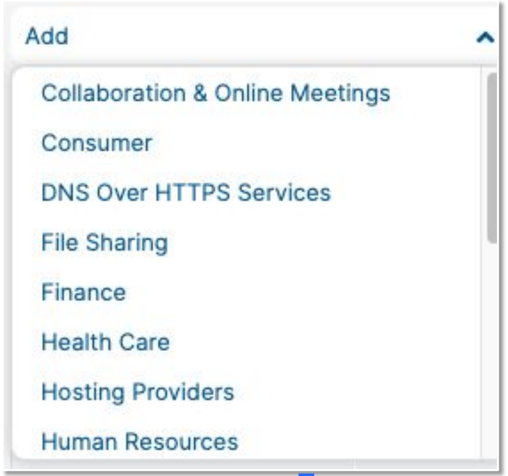
How to stop both **external** and **internal** threats

Required steps

1	Full visibility	Shadow IT, 3rd Party Apps, SSPM (Activities and Configuration)
2	**Reduce Exposure and Mitigate Risk**	Secure internet, Approved SaaS Apps, Tenancy Restrictions, Cloud App Instances
3	Gain Control of Content Types	Block based on File Types, Size, Unscannable Content for Upload/Download
4	Control Sensitive Data	Control Sensitive data - Device, Network, Cloud
5	Advanced Incident Management	Perform DLP incident triage and investigations all in one spot

Control Data Flows with Cloud App Control

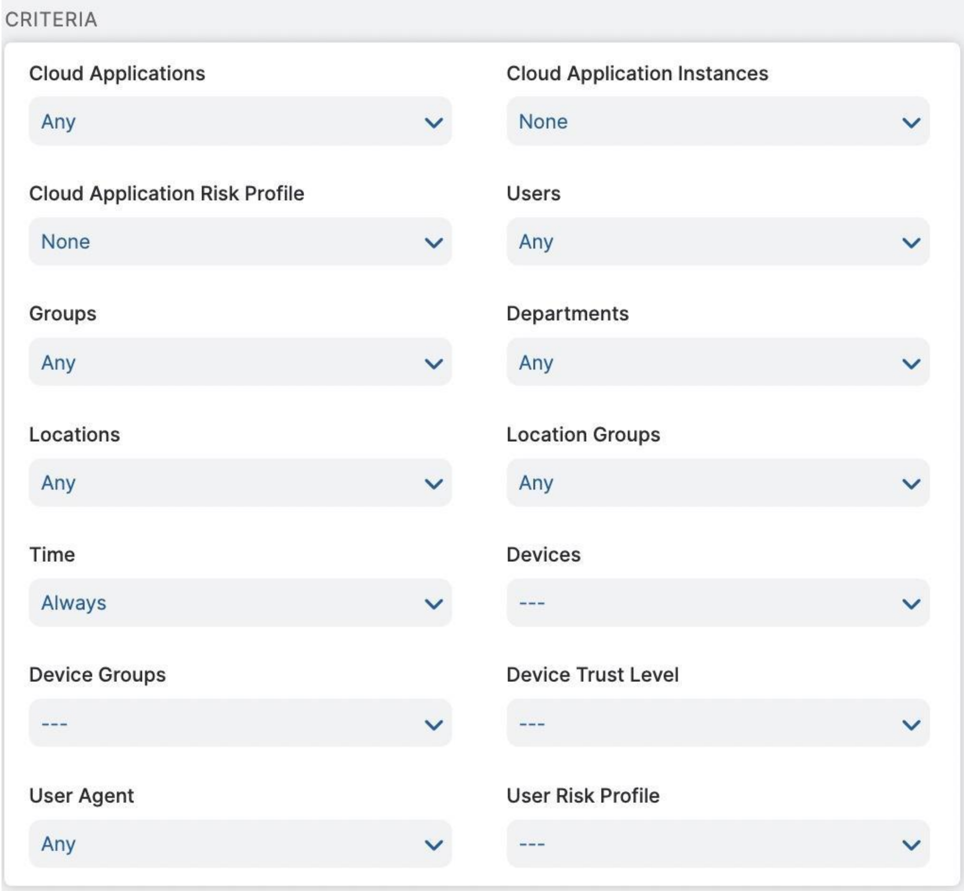
Restrict activity or prevent sensitive data leakage



Add

- Collaboration & Online Meetings
- Consumer
- DNS Over HTTPS Services
- File Sharing
- Finance
- Health Care
- Hosting Providers
- Human Resources

Simple Setup
Get started quickly with App Categories



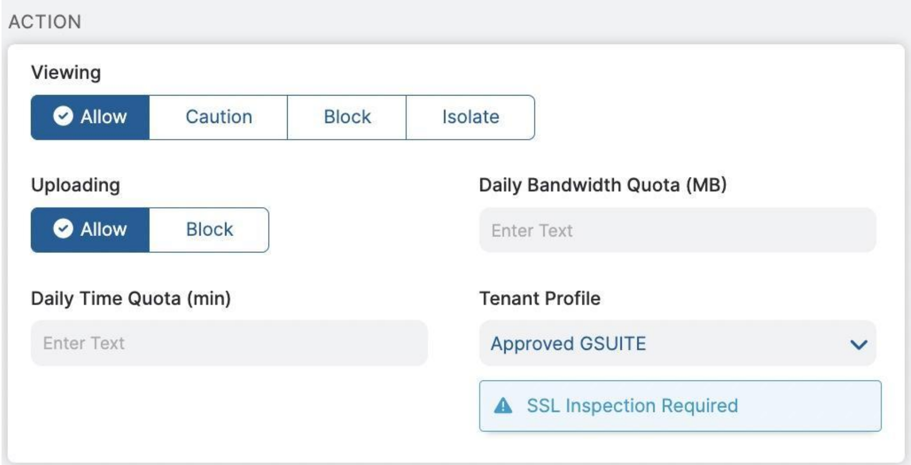
CRITERIA

Cloud Applications Any	Cloud Application Instances None
Cloud Application Risk Profile None	Users Any
Groups Any	Departments Any
Locations Any	Location Groups Any
Time Always	Devices ---
Device Groups ---	Device Trust Level ---
User Agent Any	User Risk Profile ---

Granular Control
Enforce by app category, users, group, locations or risk profile

Flexible actions like:

- View but no uploads
- Define by tenant profile
- Enforce browser isolation for safe data access



ACTION

Viewing
[✓ Allow] Caution Block Isolate

Uploading
[✓ Allow] Block

Daily Bandwidth Quota (MB)
Enter Text

Daily Time Quota (min)
Enter Text

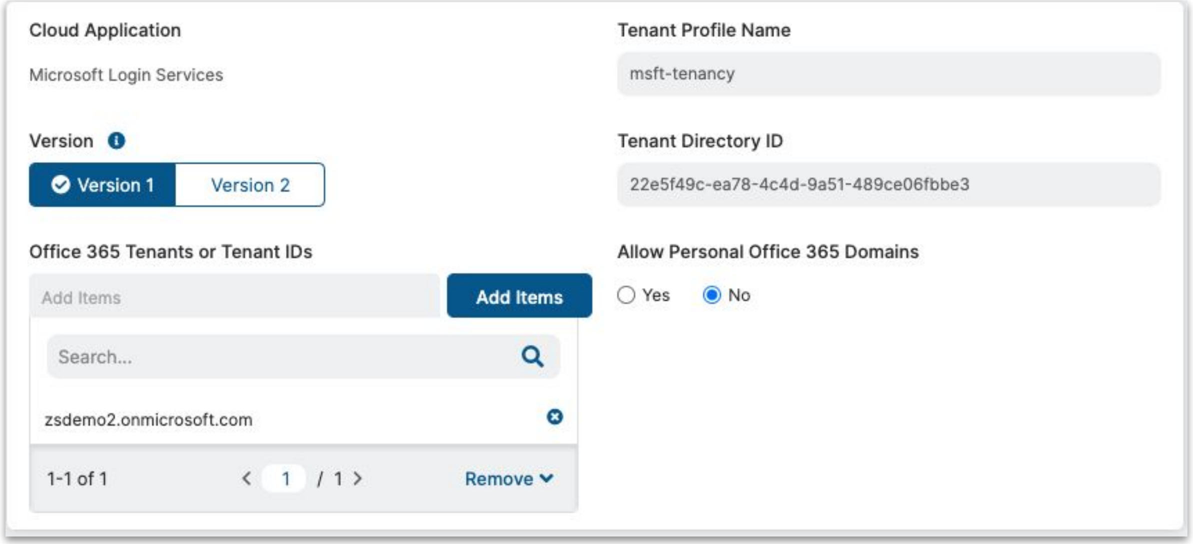
Tenant Profile
Approved GSUITE

⚠ SSL Inspection Required

Tenancy Restrictions and Cloud App Instance Control

- Ability to distinguish between and enforce policy on different enterprise instances of Apps such M365, Slack, Gsuite, Youtube, Dropbox etc
- Support for M365 TRv1 and TRv2
- Support for AWS

- Different DLP policies for different instances of apps such as OneDrive, SharePoint, Box etc



Cloud Application
Microsoft Login Services

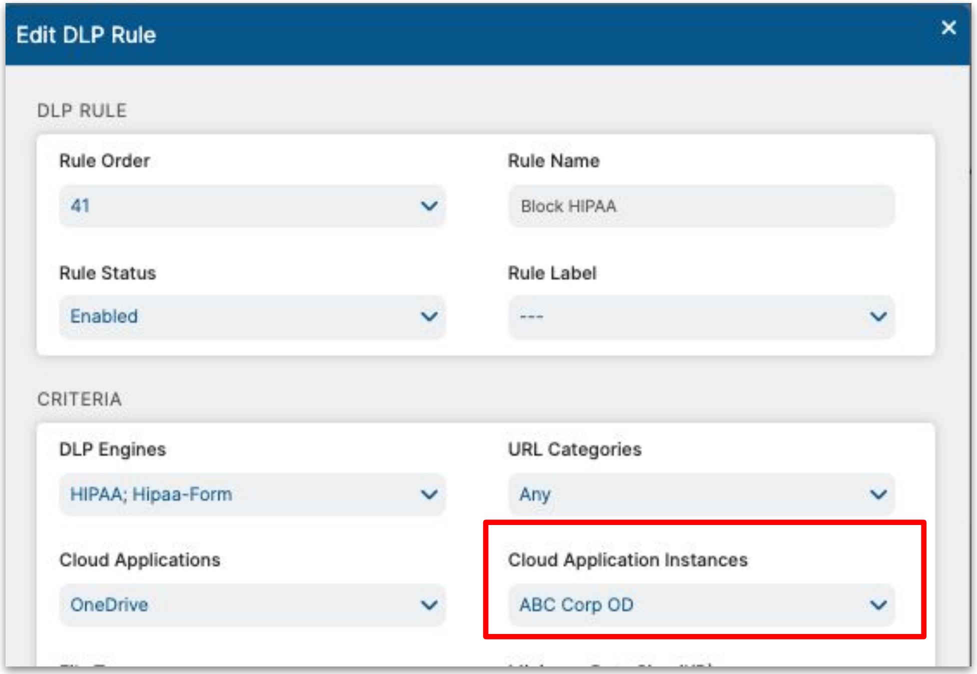
Tenant Profile Name
msft-tenancy

Version
Version 1 (selected) | Version 2

Tenant Directory ID
22e5f49c-ea78-4c4d-9a51-489ce06fbbe3

Office 365 Tenants or Tenant IDs
Add Items | Add Items
Search...
zsdemo2.onmicrosoft.com
1-1 of 1 < 1 / 1 > Remove

Allow Personal Office 365 Domains
○ Yes ● No



Edit DLP Rule

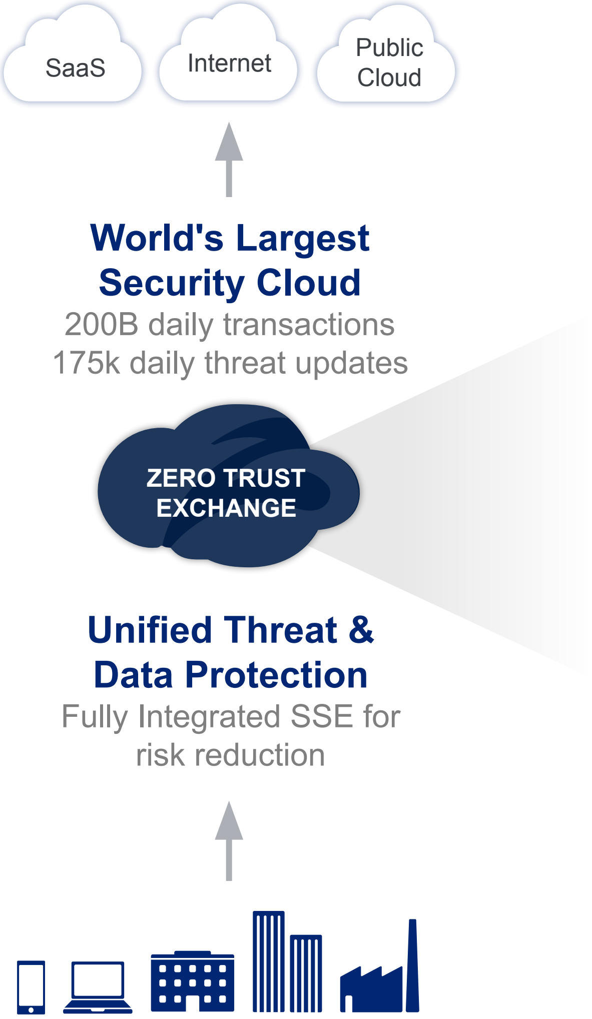
DLP RULE

Rule Order: 41
Rule Name: Block HIPAA
Rule Status: Enabled
Rule Label: ---

CRITERIA

DLP Engines: HIPAA; Hipaa-Form
URL Categories: Any
Cloud Applications: OneDrive
Cloud Application Instances: ABC Corp OD

Delivering Data Protection with Zscaler Zero Trust Exchange



World's Largest Security Cloud

200B daily transactions
175k daily threat updates

Unified Threat & Data Protection

Fully Integrated SSE for risk reduction

Complete Data Protection:

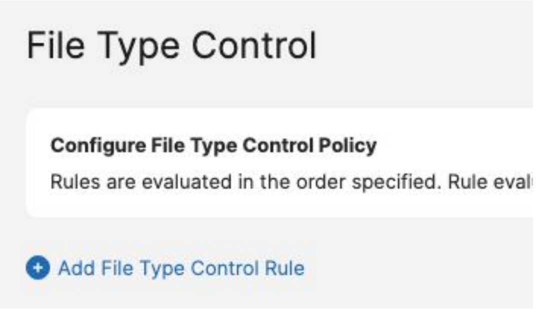
How to stop both **External** and **Internal** Threats

Required Steps

1	Full Visibility	Shadow IT, 3rd Party Apps, SSPM (Activities and Configuration)
2	Reduce Exposure and Mitigate Risk	Secure internet, Approved SaaS Apps, Tenancy Restrictions, Cloud App Instances
3	**Gain Control of Content Types**	Block based on File Types, Size, Unscannable Content for Upload/Download
4	Control Sensitive Data	Control sensitive data - Device, Network, Cloud
5	Advanced Incident Management	Perform DLP incident triage and investigations all in one spot

Monitor/Block content

Prevent potential sensitive data leakage



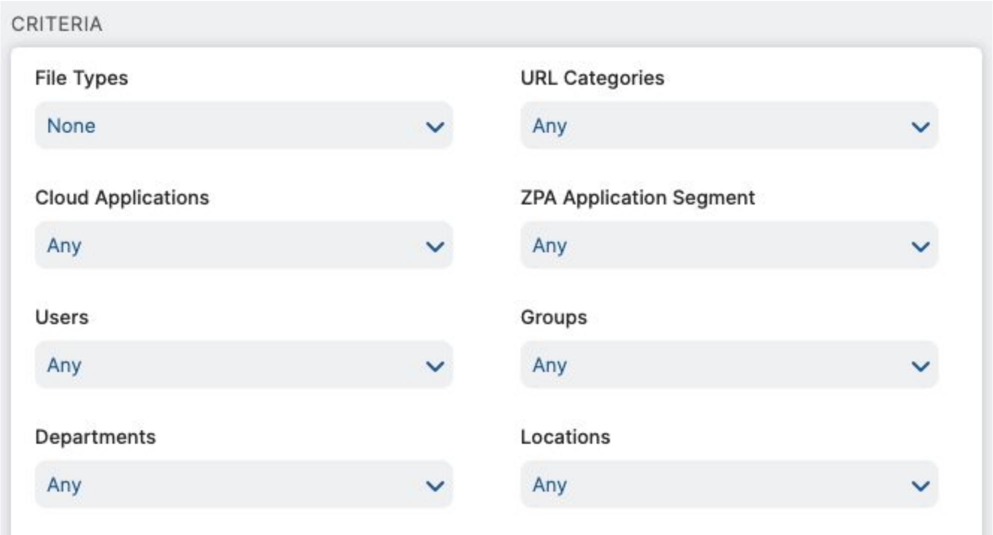
File Type Control

Configure File Type Control Policy

Rules are evaluated in the order specified. Rule eval

Rule without Content Inspection

Select without content inspection



CRITERIA

File Types: None

URL Categories: Any

Cloud Applications: Any

ZPA Application Segment: Any

Users: Any

Groups: Any

Departments: Any

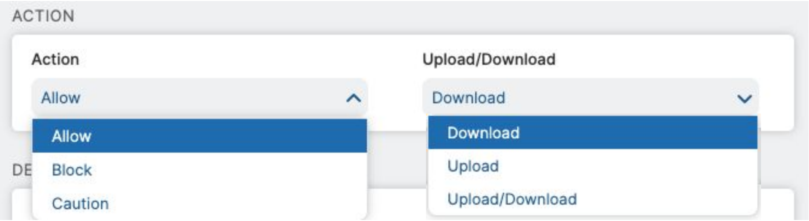
Locations: Any

Select File Type

Use File Type to detect Password Protected/Encrypted Files

Actions

- Allow – Monitor
- Block
- Caution
- Uploads or Downloads



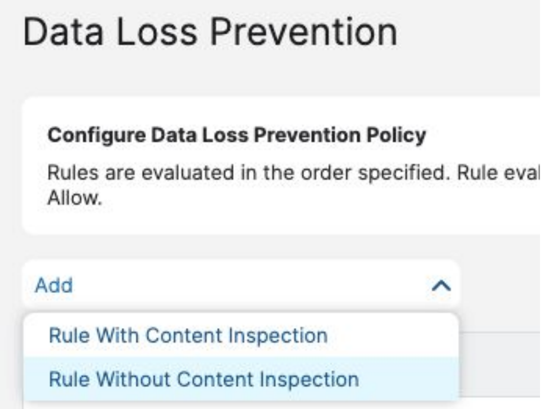
ACTION

Action: Allow

Upload/Download: Download

Monitor/Block content as a DLP Incident

Prevent potential sensitive data leakage



Data Loss Prevention

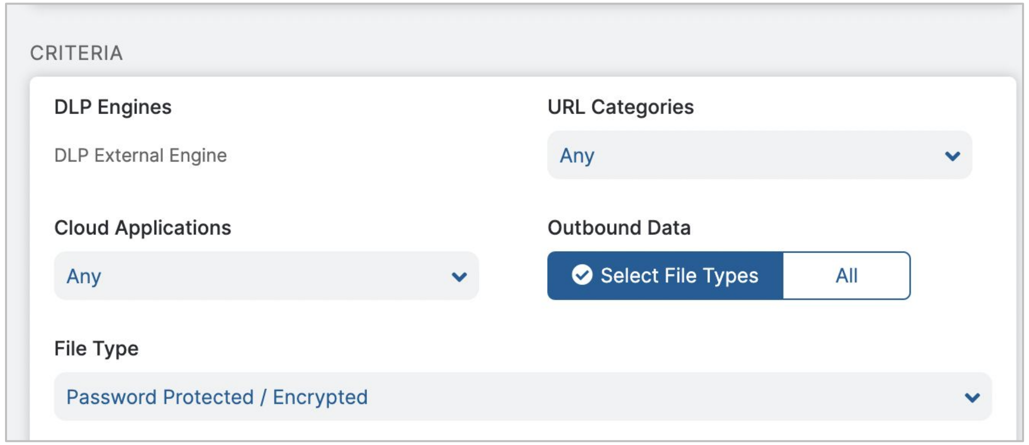
Configure Data Loss Prevention Policy

Rules are evaluated in the order specified. Rule eval
Allow.

Add

- Rule With Content Inspection
- Rule Without Content Inspection

Rule without Content Inspection
Select without content inspection



CRITERIA

DLP Engines: DLP External Engine

URL Categories: Any

Cloud Applications: Any

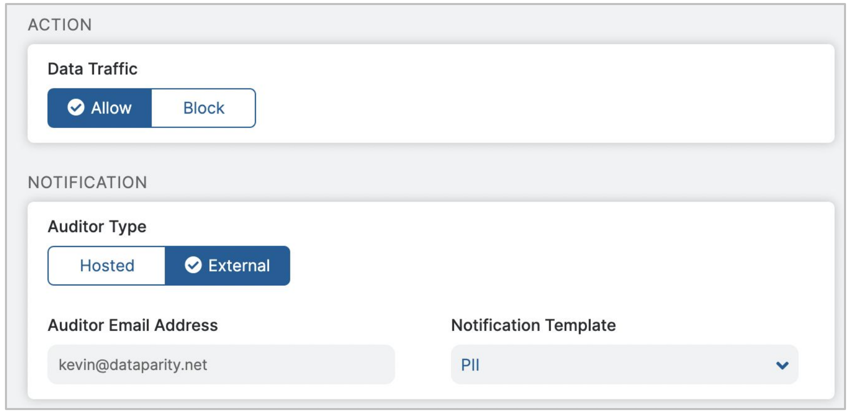
Outbound Data: ✓ Select File Types | All

File Type: Password Protected / Encrypted

Select File Type
Use File Type to detect Password Protected/Encrypted Files

Actions for Monitor or Block

- Allow – Monitor
- Block



ACTION

Data Traffic: ✓ Allow | Block

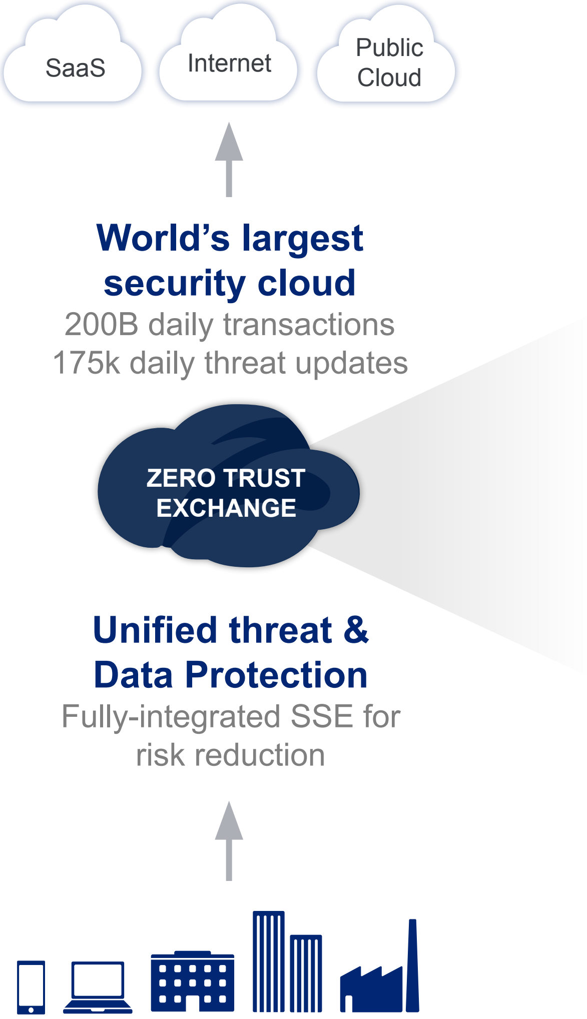
NOTIFICATION

Auditor Type: Hosted | ✓ External

Auditor Email Address: kevin@dataparity.net

Notification Template: PII

Delivering Data Protection with Zscaler Zero Trust Exchange



World's largest security cloud

200B daily transactions
175k daily threat updates

Unified threat & Data Protection

Fully-integrated SSE for risk reduction

Complete Data Protection:

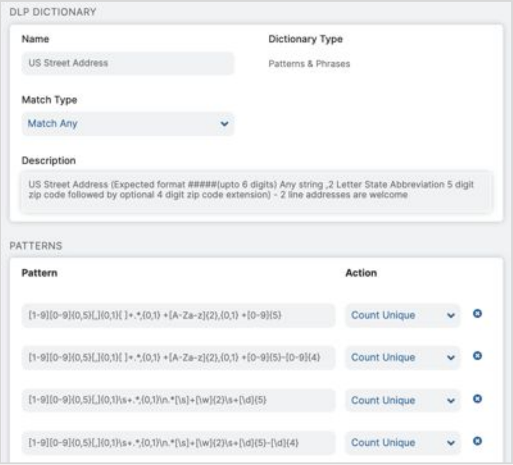
How to stop both **external** and **internal** threats

Required steps

1	Full visibility	Shadow IT, 3rd Party Apps, SSPM (Activities and Configuration)
2	Reduce Exposure and Mitigate Risk	Secure internet, Approved SaaS Apps Tenancy Restrictions, Cloud App Instances
3	Gain Control of Content Types	Block based on File Types, Size, Unscannable Content for Upload/Download
4	**Control Sensitive Data**	Control sensitive data - Device, Network, Cloud
5	Advanced Incident Management	Perform DLP incident triage and investigations all in one spot

Zscaler content inspection capabilities & custom dictionaries

Inspection Category	Inspection Technique		
Described content	Regex		
	Single & multi word keywords with proximity		
	Preconfigured data patterns	• Citizen service # (Netherlands) • National ID # (Hong Kong) • Social insurance # (Canada)	• Social security # (US) • National insurance # (UK) • NRIC # (Singapore)
Trained data sets	Pre-trained engines	• Credit card number • Financial statements	• Card expiration & CCV • First name, last name
Fingerprinting	Structured fingerprints (EDM & IDM)	• Medical information • Medicare number	• CPT & ICD codes • High value documents/forms



DLP DICTIONARY

Name: US Street Address

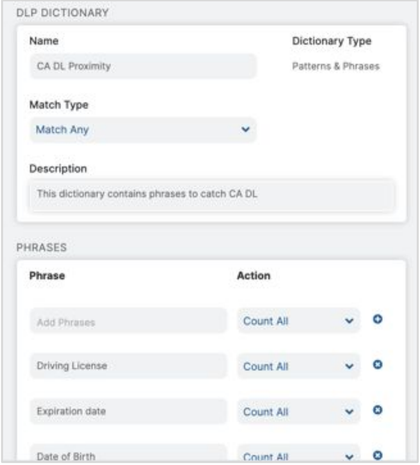
Dictionary Type: Patterns & Phrases

Match Type: Match Any

Description: US Street Address (Expected format #####(upto 6 digits) Any string ,2 Letter State Abbreviation 5 digit zip code followed by optional 4 digit zip code extension) - 2 line addresses are welcome

PATTERNS

Pattern	Action
`[1-9][0-9]{0,5}[,]{0,1}[ ]+.*{0,1} +[A-Za-z]{2},{0,1} +[0-9]{5}`	Count Unique
`[1-9][0-9]{0,5}[,]{0,1}[ ]+.*{0,1} +[A-Za-z]{2},{0,1} +[0-9]{5}-[0-9]{4}`	Count Unique
`[1-9][0-9]{0,5}[,]{0,1}\s+.*{0,1}\n.*[\s]+[\w]{2}\s+[\d]{5}`	Count Unique
`[1-9][0-9]{0,5}[,]{0,1}\s+.*{0,1}\n.*[\s]+[\w]{2}\s+[\d]{5}-[\d]{4}`	Count Unique



DLP DICTIONARY

Name: CA DL Proximity

Dictionary Type: Patterns & Phrases

Match Type: Match Any

Description: This dictionary contains phrases to catch CA DL

PHRASES

Phrase	Action
Add Phrases	Count All
Driving License	Count All
Expiration date	Count All
Date of Birth	Count All

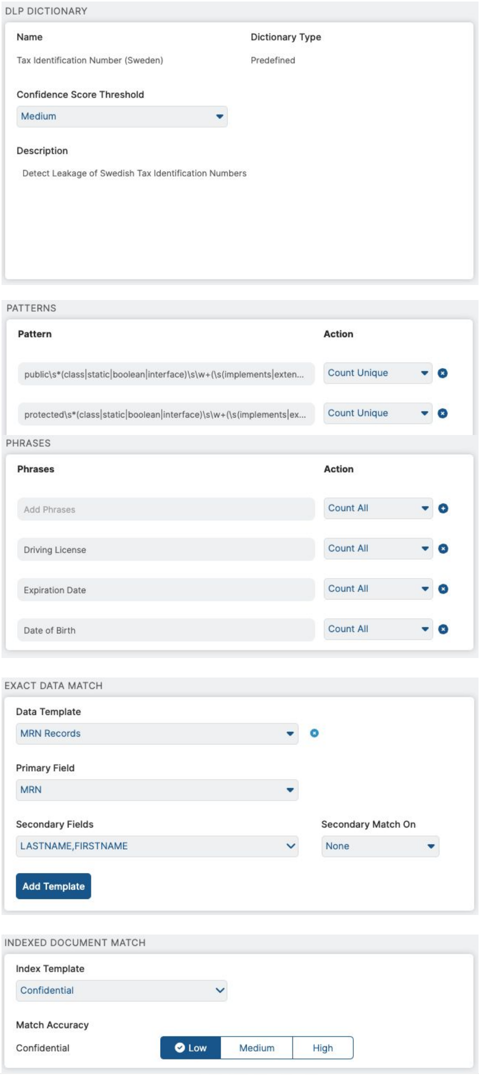
Unified Data Identifiers for Inline and OOB

Preconfigured data patterns

Regex/Phrases/ MIP Labels

EDM

IDM



DLP DICTIONARY

Name	Dictionary Type
Tax Identification Number (Sweden)	Predefined

Confidence Score Threshold: Medium

Description

Detect Leakage of Swedish Tax Identification Numbers

PATTERNS

Pattern	Action
public\s*(class|static|boolean|interface)\s\w+(\s(implements|exten...	Count Unique
protected\s*(class|static|boolean|interface)\s\w+(\s(implements|ex...	Count Unique

PHRASES

Phrases	Action
Add Phrases	Count All
Driving License	Count All
Expiration Date	Count All
Date of Birth	Count All

EXACT DATA MATCH

Data Template: MRN Records

Primary Field: MRN

Secondary Fields: LASTNAME,FIRSTNAME

Secondary Match On: None

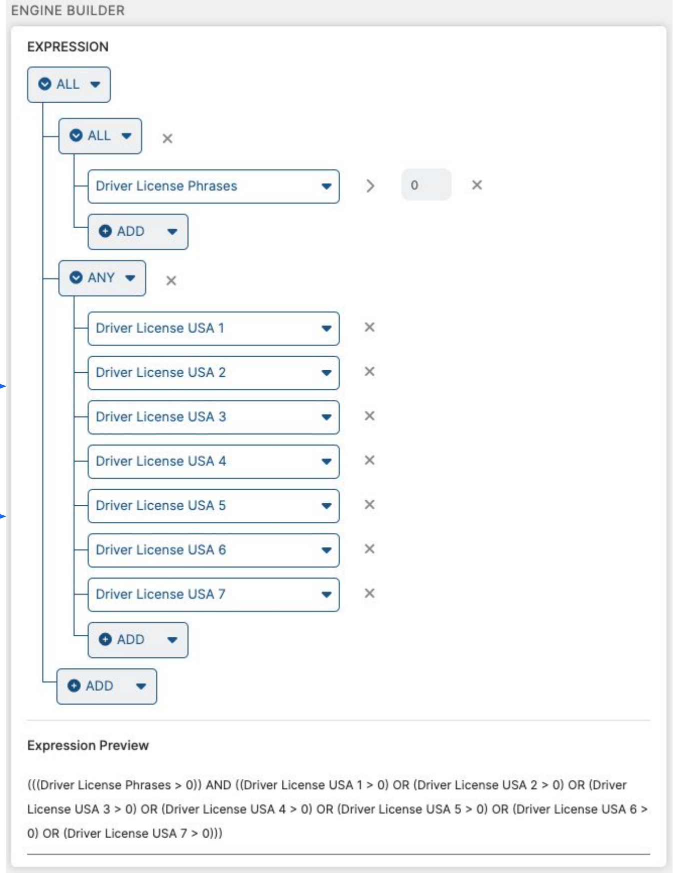
Add Template

INDEXED DOCUMENT MATCH

Index Template: Confidential

Match Accuracy

Confidential ● Low | Medium | High



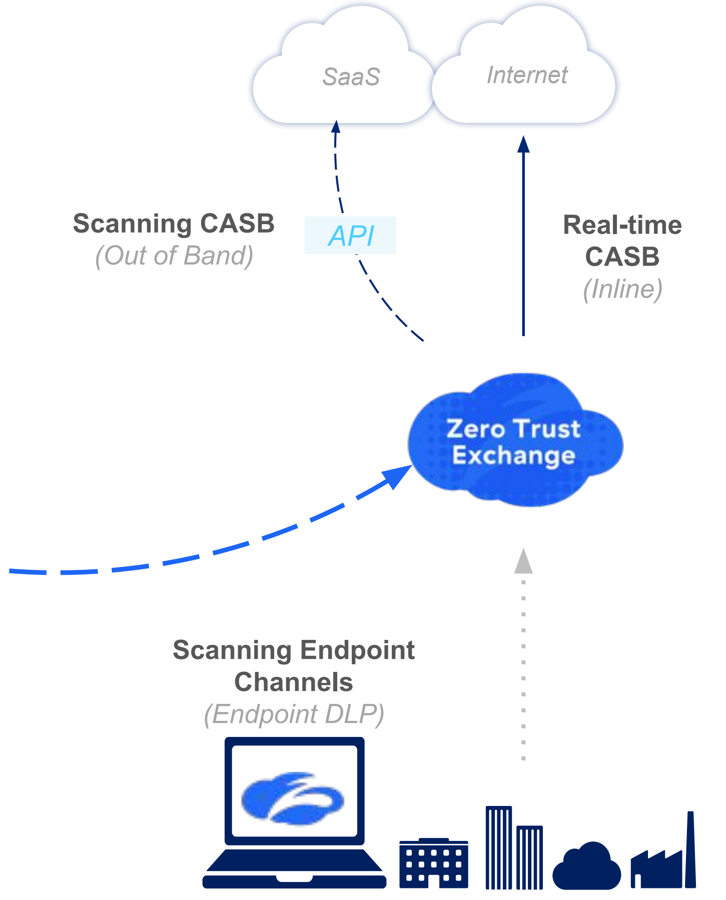
ENGINE BUILDER

EXPRESSION

```
ALL
  ALL  ×
    Driver License Phrases  >  0  ×
    ADD
  ANY  ×
    Driver License USA 1  ×
    Driver License USA 2  ×
    Driver License USA 3  ×
    Driver License USA 4  ×
    Driver License USA 5  ×
    Driver License USA 6  ×
    Driver License USA 7  ×
    ADD
  ADD
```

Expression Preview

(((Driver License Phrases > 0)) AND ((Driver License USA 1 > 0) OR (Driver License USA 2 > 0) OR (Driver License USA 3 > 0) OR (Driver License USA 4 > 0) OR (Driver License USA 5 > 0) OR (Driver License USA 6 > 0) OR (Driver License USA 7 > 0)))



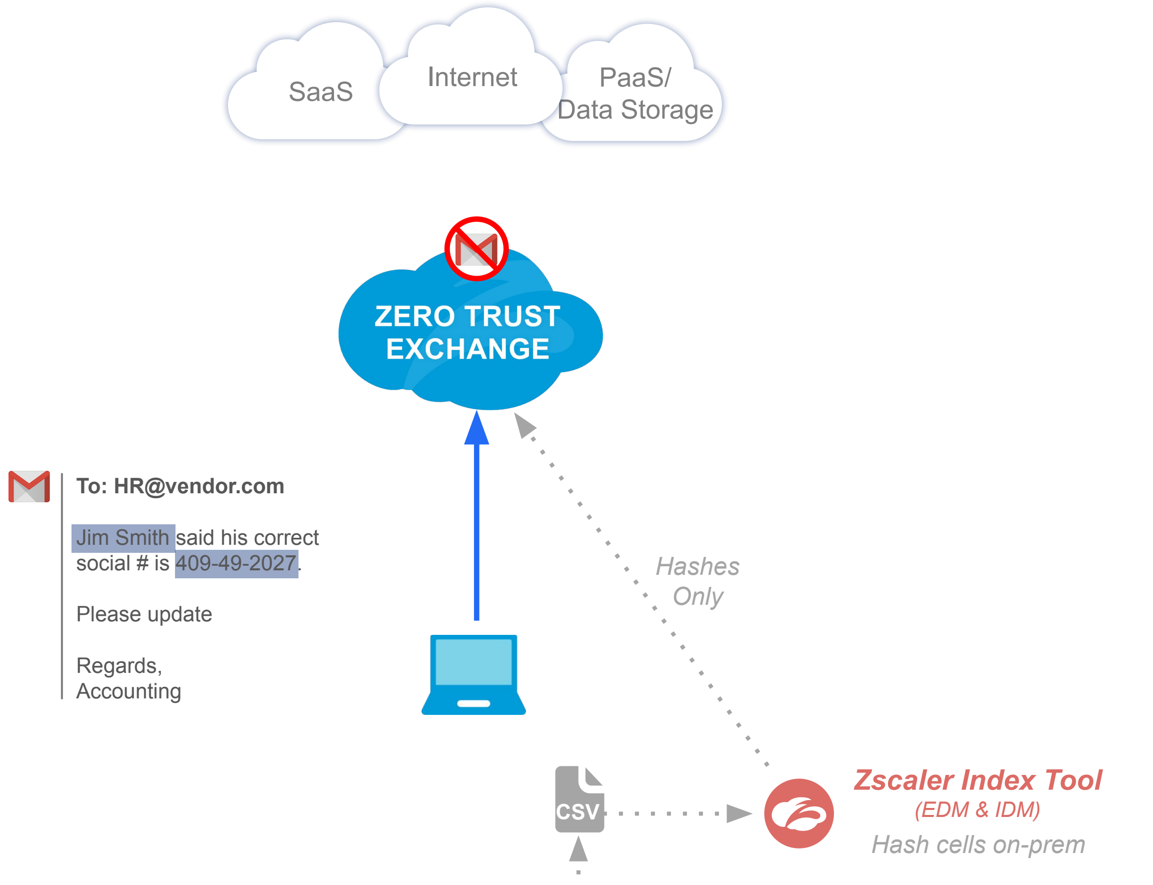
Scanning CASB
(Out of Band)

Real-time CASB
(Inline)

Scanning Endpoint Channels
(Endpoint DLP)

Users, data centers, workloads and IoT/OT

Secure Custom Data with Exact Data Match



To: HR@vendor.com

Jim Smith said his correct social # is 409-49-2027.

Please update

Regards,
Accounting

Name	Credit Card	SSN	Street Address	City	Zip Code
Jim Smith	4716653795988590	409-49-2027	123 Main St	Burbank	91505
Jane Doe	5163272601356640	679-10-1537	456 Central Ave	Burbank	91505

Custom Structured Data

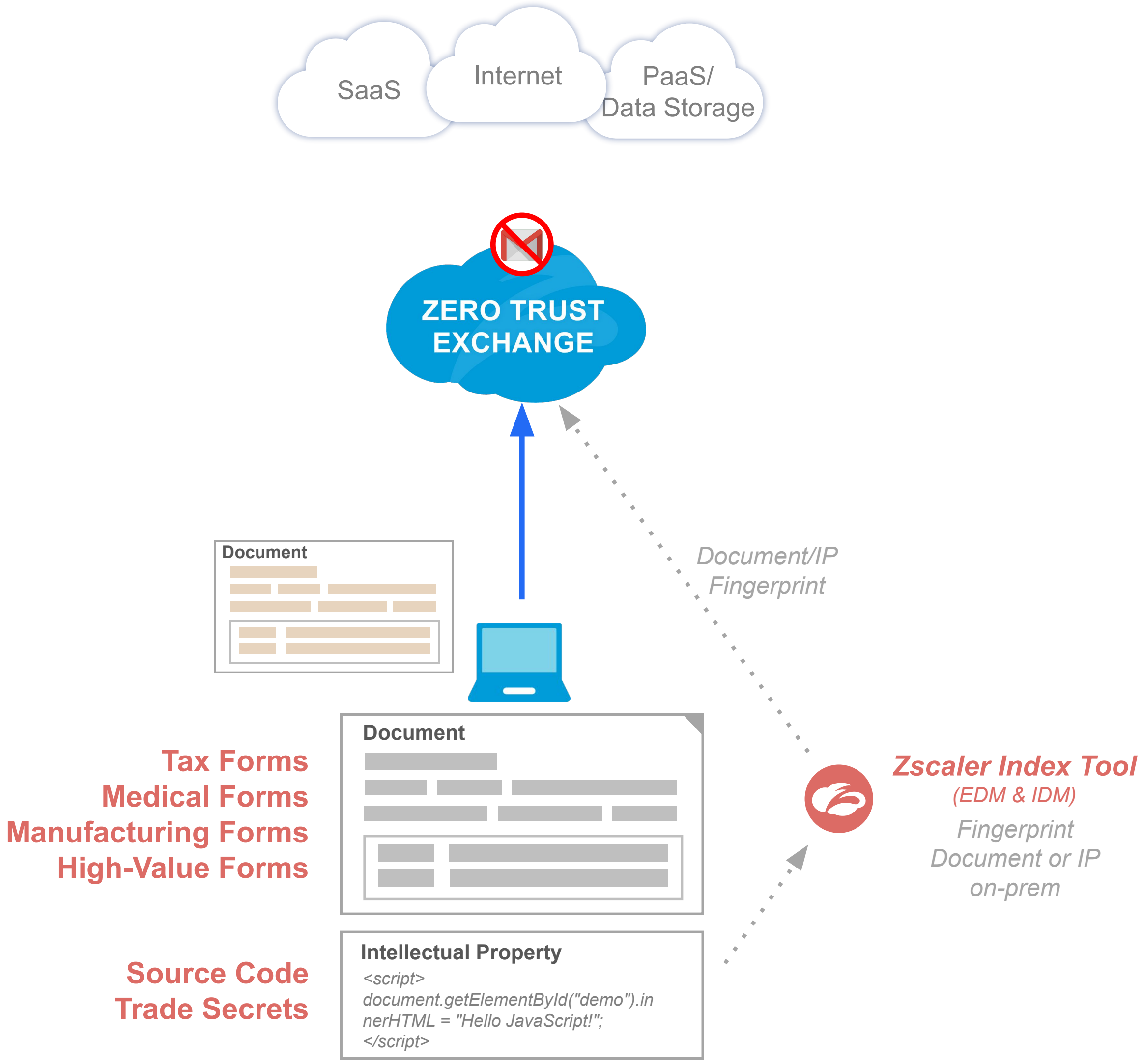
How Exact Data Match Works

1. Structure custom data you want to secure
2. Index data and send only hashes to Zscaler
3. Zscaler ready to find custom data
4. Prevent data loss with DLP block policies

Benefits of Zscaler EDM

- **Secure high value sensitive data**
  PCI, PII, HIPAA, Inventory Codes, Membership #s, ect.
- **Reduce DLP False Positives**
  Ex: Trigger on meaningful SSNs, not all SSNs
- **VM-based Index tool keeps things simple**
  High-value data doesn't leave premises
  Used for both Exact Data Match & Index Document Matching

Secure Custom Forms and IP with Index Document Matching



SaaS

Internet

PaaS/
Data Storage

ZERO TRUST
EXCHANGE

Document/IP
Fingerprint

Document

Tax Forms
Medical Forms
Manufacturing Forms
High-Value Forms

Document

Source Code
Trade Secrets

Intellectual Property

```
<script>
document.getElementById("demo").in
nerHTML = "Hello JavaScript!";
</script>
```

Zscaler Index Tool
(EDM & IDM)
Fingerprint
Document or IP
on-prem

How to use Index Document Matching

1. Identify high-value Form or IP to protect
2. Fingerprint Form or IP with Index Tool
3. Zscaler ready to find other instances of Form or IP
4. Prevent data loss with DLP block policies

Benefits of Zscaler EDM

- **Secure high-value documents and IP from loss**
- **Managed docs with ease by mounting SMB drives**
  Index up to 100GB of files
- **Powerful VM-based Index tool**
  Fine-tune detection with adjustable match accuracy
  Used for both Index Document Matching & Exact Data Match

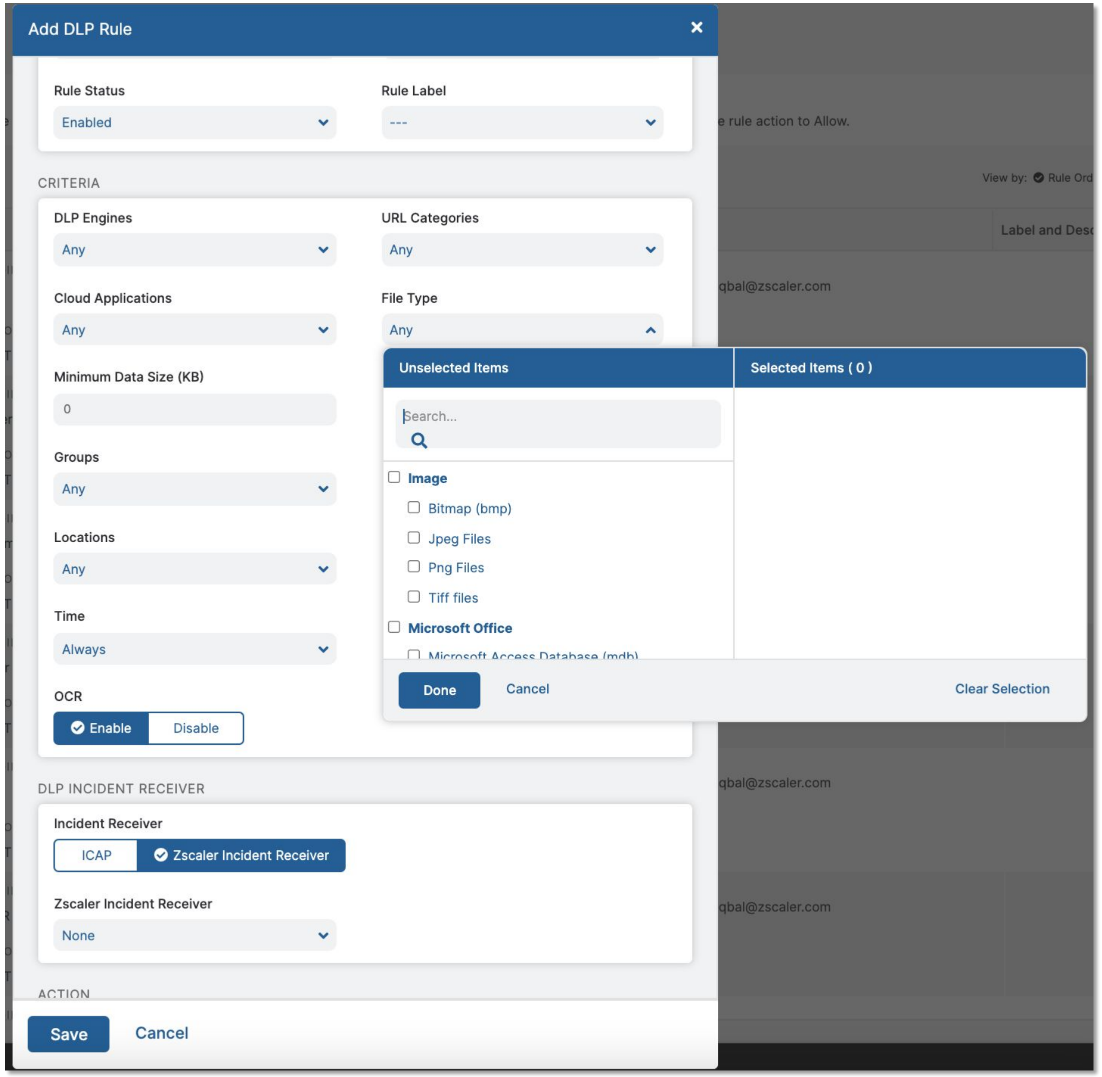
OCR Powered by ML & AI

Secure image files, embedded images, handwritten texts

Advanced Data Classification

Advanced ML & AI is utilized to extract contextual data

Recognizes sensitive data in image files, within embedded images.



Add DLP Rule ×

Rule Status: Enabled

Rule Label: ---

CRITERIA

DLP Engines: Any

URL Categories: Any

Cloud Applications: Any

File Type: Any

Minimum Data Size (KB): 0

Groups: Any

Locations: Any

Time: Always

OCR: ● Enable | Disable

Unselected Items | Selected Items (0)

Search...

- □ Image
  - □ Bitmap (bmp)
  - □ Jpeg Files
  - □ Png Files
  - □ Tiff files
- □ Microsoft Office
  - □ Microsoft Access Database (mdb)

Done | Cancel | Clear Selection

DLP INCIDENT RECEIVER

Incident Receiver: ICAP | ● Zscaler Incident Receiver

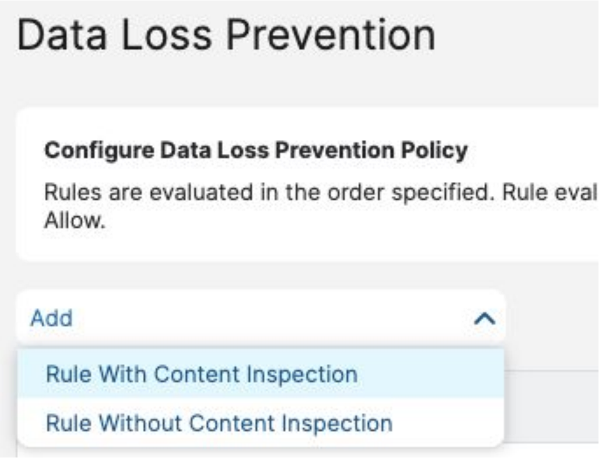
Zscaler Incident Receiver: None

ACTION

Save | Cancel

Control Sensitive Data - Inline CASB

Prevent sensitive data leakage



Data Loss Prevention

Configure Data Loss Prevention Policy

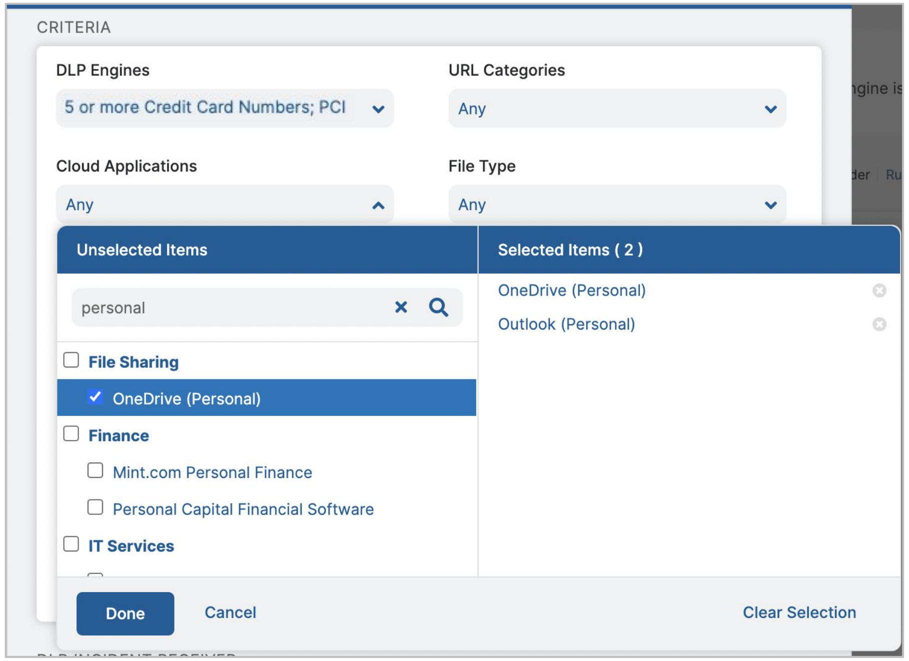
Rules are evaluated in the order specified. Rule eval
Allow.

Add

Rule With Content Inspection

Rule Without Content Inspection

Rule with Content Inspection
Create Rule DLP Rule



CRITERIA

DLP Engines: 5 or more Credit Card Numbers; PCI

URL Categories: Any

Cloud Applications: Any

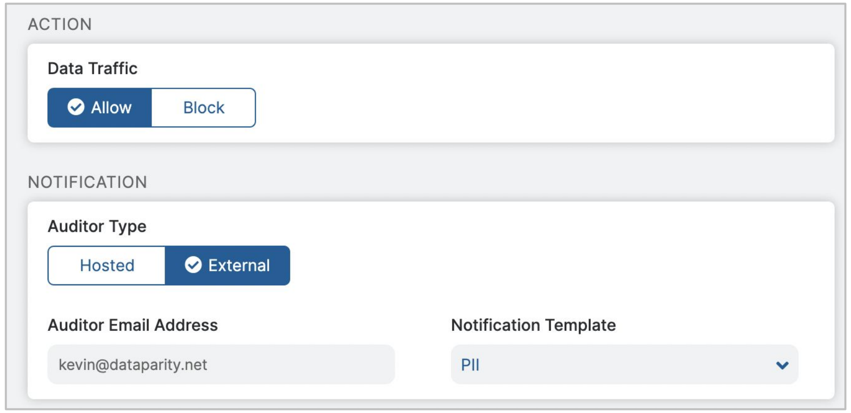
File Type: Any

Unselected Items	Selected Items (2)
personal	OneDrive (Personal)
□ File Sharing	Outlook (Personal)
☑ OneDrive (Personal)	
□ Finance	
□ Mint.com Personal Finance	
□ Personal Capital Financial Software	
□ IT Services	

Select Personal Apps
Enforce by app such as
Personal vs Enterprise

Actions for Monitor or Block

- Allow – Monitor
- Block



ACTION

Data Traffic: [✓ Allow] Block

NOTIFICATION

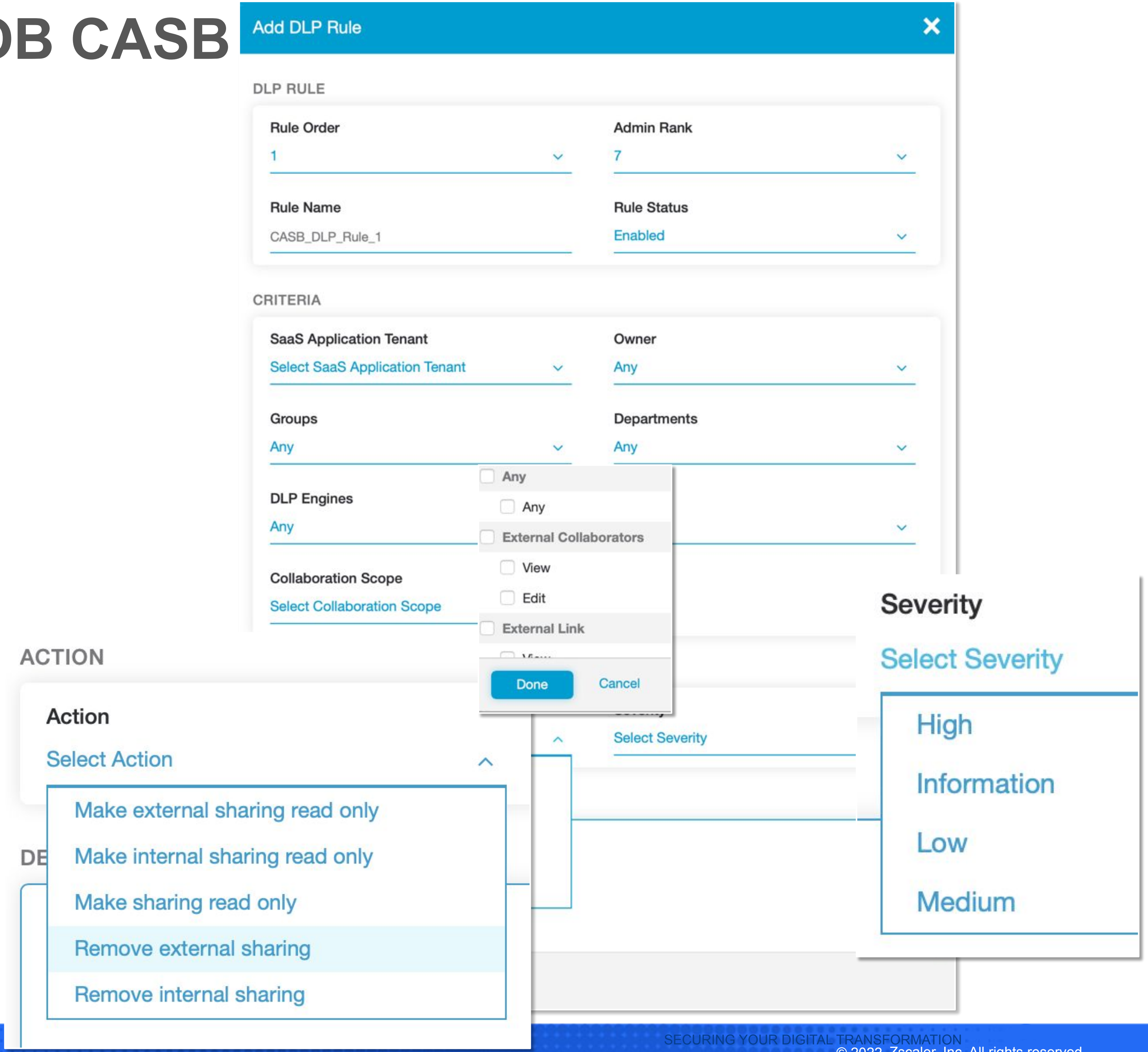
Auditor Type: Hosted [✓ External]

Auditor Email Address: kevin@dataparity.net

Notification Template: PII

Control Sensitive Data - OOB CASB

- Leverage DLP engine against defined CASB tenants
- Actions and collaboration scope change dependent on the API capabilities of the selected SaaS tenant
- Apply policy based on incident severity



Add DLP Rule

DLP RULE

Rule Order: 1

Admin Rank: 7

Rule Name: CASB_DLP_Rule_1

Rule Status: Enabled

CRITERIA

SaaS Application Tenant: Select SaaS Application Tenant

Owner: Any

Groups: Any

Departments: Any

DLP Engines: Any

Collaboration Scope: Select Collaboration Scope

□ Any
□ Any
□ External Collaborators
□ View
□ Edit
□ External Link

Done Cancel

Select Severity

ACTION

Action: Select Action

- Make external sharing read only
- Make internal sharing read only
- Make sharing read only
- Remove external sharing
- Remove internal sharing

DE

Severity: Select Severity

- High
- Information
- Low
- Medium

Zscaler Endpoint DLP: Streamline & simplify endpoint data protection

Zscaler Endpoint DLP

Streamlined Protection
Use single DLP policy and unified agent

Unparalleled Visibility
See sensitive data movement immediately –
no policy required

Endpoint Channels Protected:

Removable Media

Printing

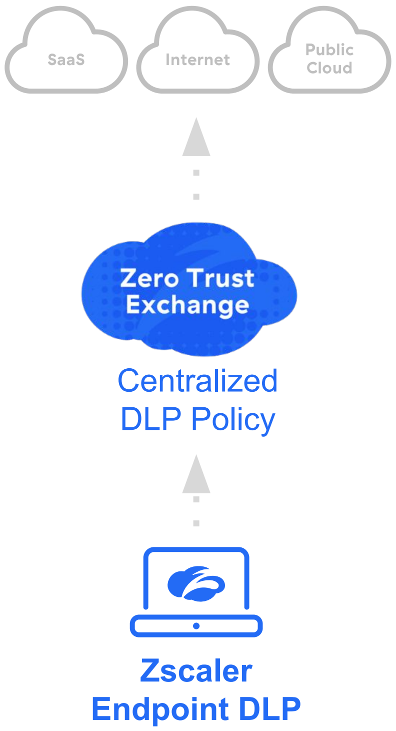
Network Shares

Personal storage sync

Dropbox

box

OneDrive



SaaS

Internet

Public Cloud

Zero Trust Exchange

Centralized DLP Policy

Zscaler Endpoint DLP

Benefits

Quick Deployment
Leverage existing Zscaler DLP policy controls

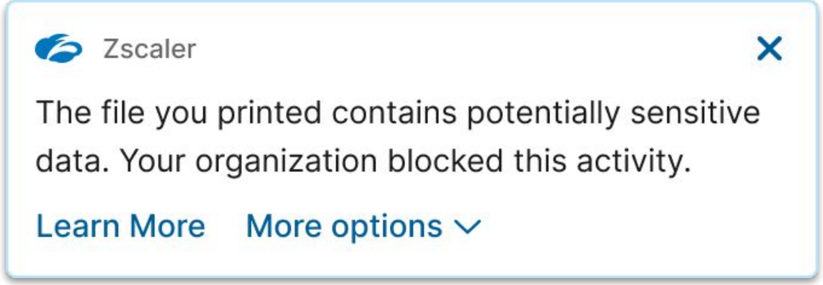
Unified Policy
Consistent alerting across Endpoint, Inline & Cloud

Consolidated Agent
Streamlined, lightweight approach

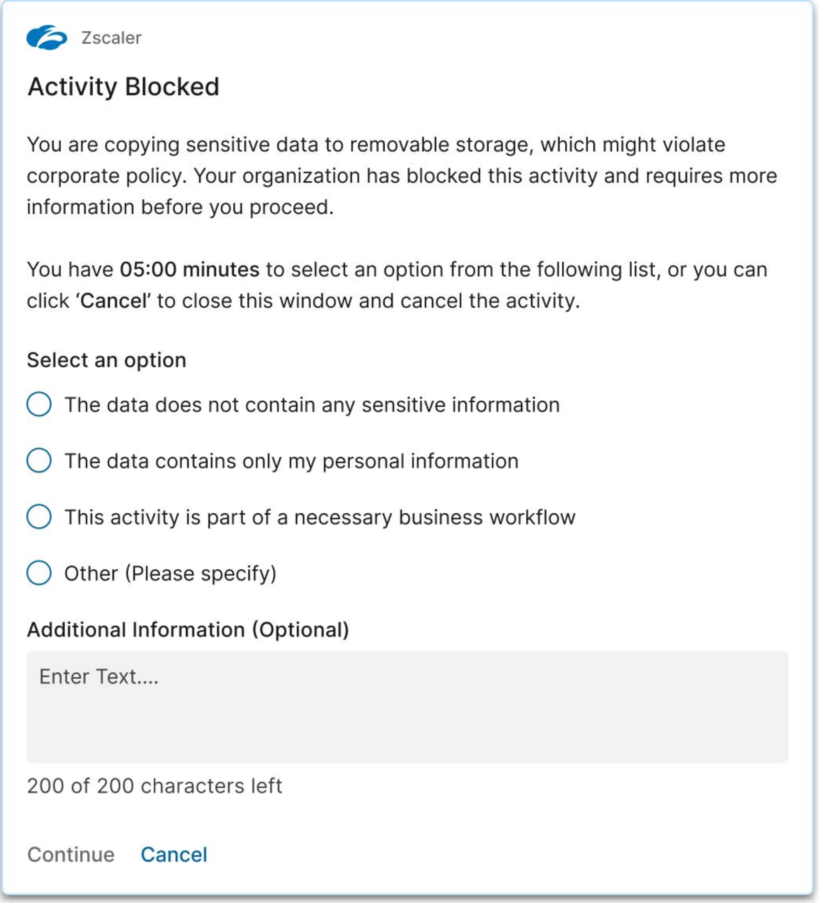
Faster Incident Management
In-depth dashboards and forensics

Endpoint DLP - End User Experience

- **Windows & macOS** support
- Policy rule action options: **Allow**(=Monitor), **Confirm**, **Block**
- End-user interaction
  - **Notification dialog** - optional for Allow/Block actions
    - Show - Provides context to block action
    - Hide - Stealth monitoring
  - **Confirmation dialog** - for Confirm action (excellent tool for user coaching
  - **Request exemption**
    - Exemption from being blocked (policy still in place)
    - 12 Hours - non configurable in V1



The file you printed contains potentially sensitive data. Your organization blocked this activity.



Activity Blocked

You are copying sensitive data to removable storage, which might violate corporate policy. Your organization has blocked this activity and requires more information before you proceed.

You have **05:00 minutes** to select an option from the following list, or you can click ‘**Cancel**’ to close this window and cancel the activity.

Select an option

○ The data does not contain any sensitive information

○ The data contains only my personal information

○ This activity is part of a necessary business workflow

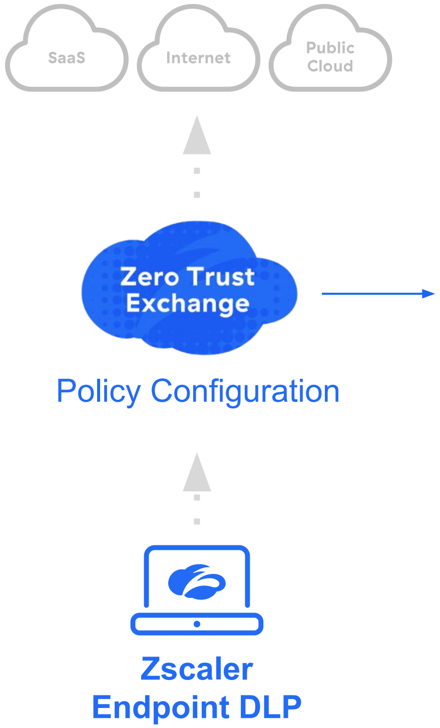
○ Other (Please specify)

Additional Information (Optional)

Enter Text....

200 of 200 characters left

Policy Configuration



Channel

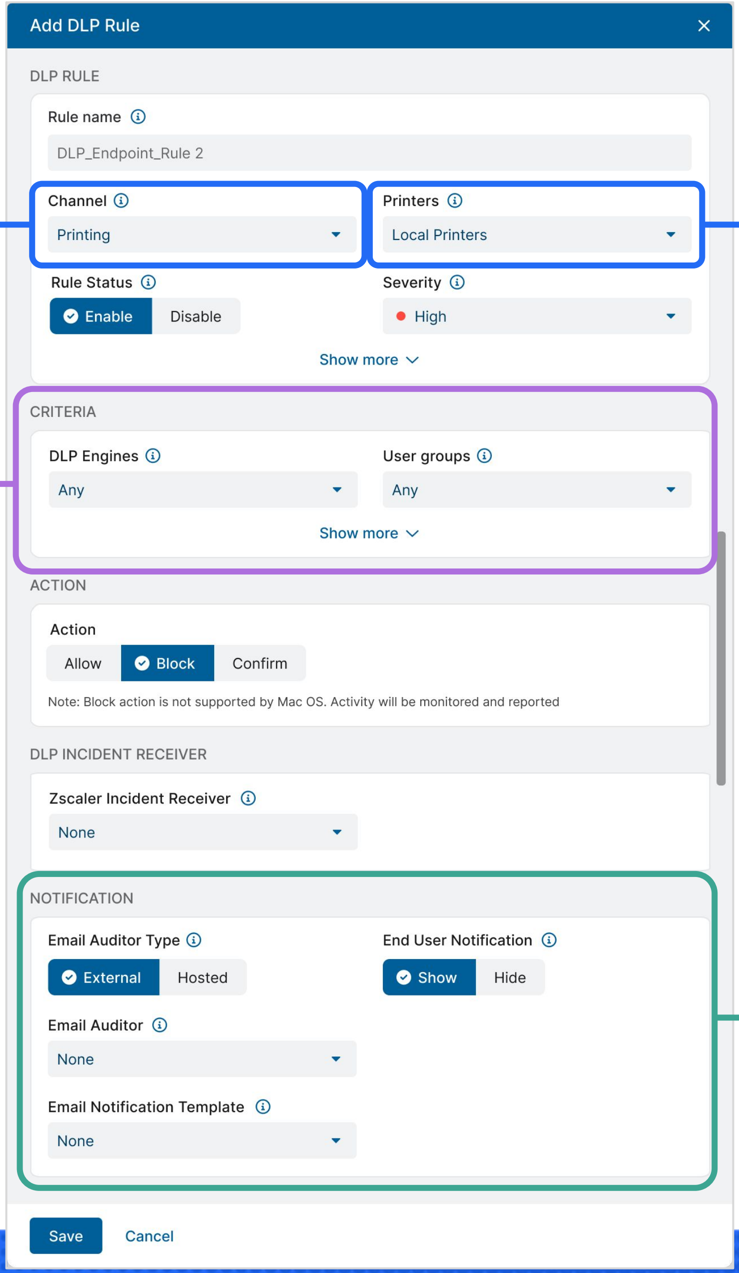
Select Channel:

Removeable Media
Network Share
Printing
Cloud Storage sync

Criteria

Rules based on:

Users,
DLP engines,
Devices,
U]ser risk profile,
File type,
And more



Add DLP Rule ×

DLP RULE

Rule name ⓘ: DLP_Endpoint_Rule 2

Channel ⓘ: Printing ▾

Printers ⓘ: Local Printers ▾

Rule Status ⓘ: [✓ Enable] Disable

Severity ⓘ: ● High ▾

Show more ⌄

CRITERIA

DLP Engines ⓘ: Any ▾

User groups ⓘ: Any ▾

Show more ⌄

ACTION

Action: Allow [✓ Block] Confirm

Note: Block action is not supported by Mac OS. Activity will be monitored and reported

DLP INCIDENT RECEIVER

Zscaler Incident Receiver ⓘ: None ▾

NOTIFICATION

Email Auditor Type ⓘ: [✓ External] Hosted

End User Notification ⓘ: [✓ Show] Hide

Email Auditor ⓘ: None ▾

Email Notification Template ⓘ: None ▾

Save Cancel

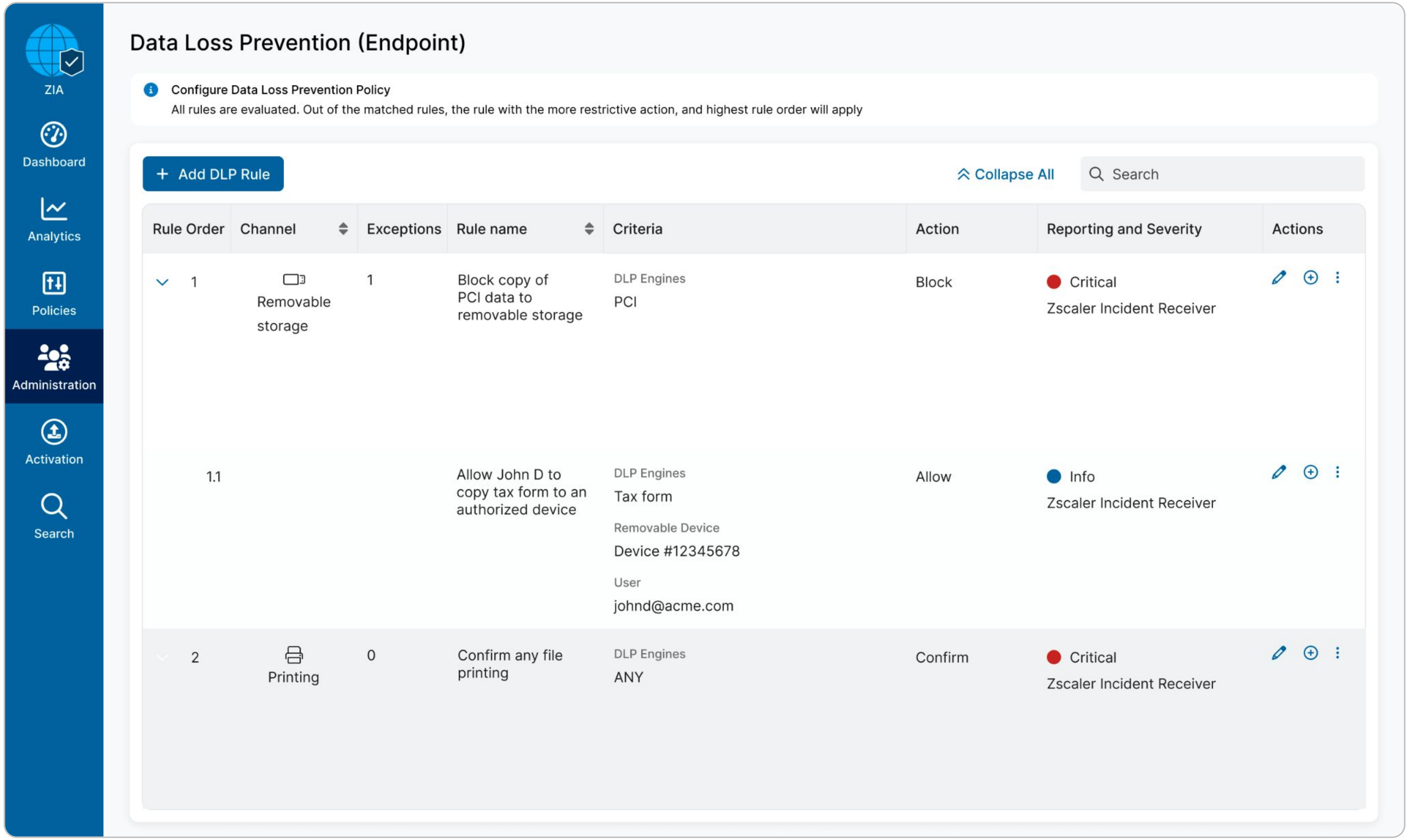
Channel Settings

Changes based upon channel selected

Notifications

Stakeholder emails or push notifications to users

Endpoint DLP - Policy Rules



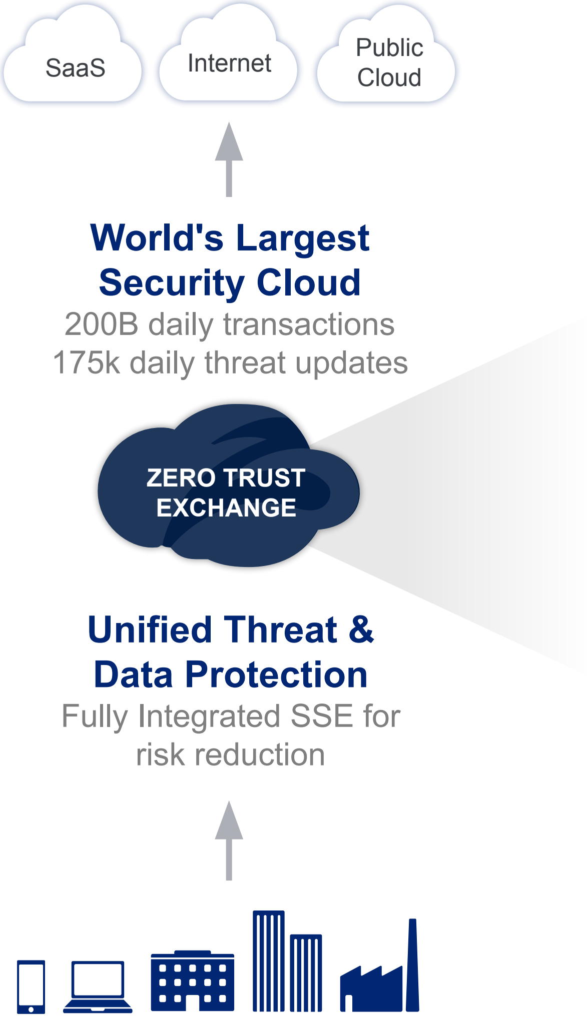
Data Loss Prevention (Endpoint)

Configure Data Loss Prevention Policy

All rules are evaluated. Out of the matched rules, the rule with the more restrictive action, and highest rule order will apply

Rule Order	Channel	Exceptions	Rule name	Criteria	Action	Reporting and Severity	Actions
1	Removable storage	1	Block copy of PCI data to removable storage	DLP Engines PCI	Block	● Critical Zscaler Incident Receiver	
1.1			Allow John D to copy tax form to an authorized device	DLP Engines Tax form Removable Device Device #12345678 User johnd@acme.com	Allow	● Info Zscaler Incident Receiver	
2	Printing	0	Confirm any file printing	DLP Engines ANY	Confirm	● Critical Zscaler Incident Receiver	

Delivering Data Protection with Zscaler Zero Trust Exchange



World's Largest Security Cloud

200B daily transactions
175k daily threat updates

Unified Threat & Data Protection

Fully Integrated SSE for risk reduction

Complete Data Protection:

How to stop both **External** and **Internal** Threats

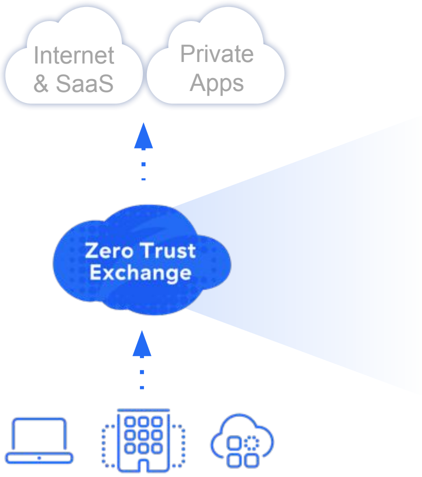
Required Steps

1	**Full Visibility**	Shadow IT, 3rd Party Apps, SSPM (Activities and Configuration)
2	**Reduce Exposure and Mitigate Risk**	Secure internet, Approved SaaS Apps, Tenancy Restrictions, Cloud App Instances
3	**Gain Control of Content Types**	Block based on File Types, Size, Unscannable Content for Upload/Download
4	**Control Sensitive Data**	Control sensitive data - Device, Network, Cloud
5	**Advanced Incident Management**	Perform DLP incident triage and investigations all in one spot

Streamline incident control with Workflow Automation

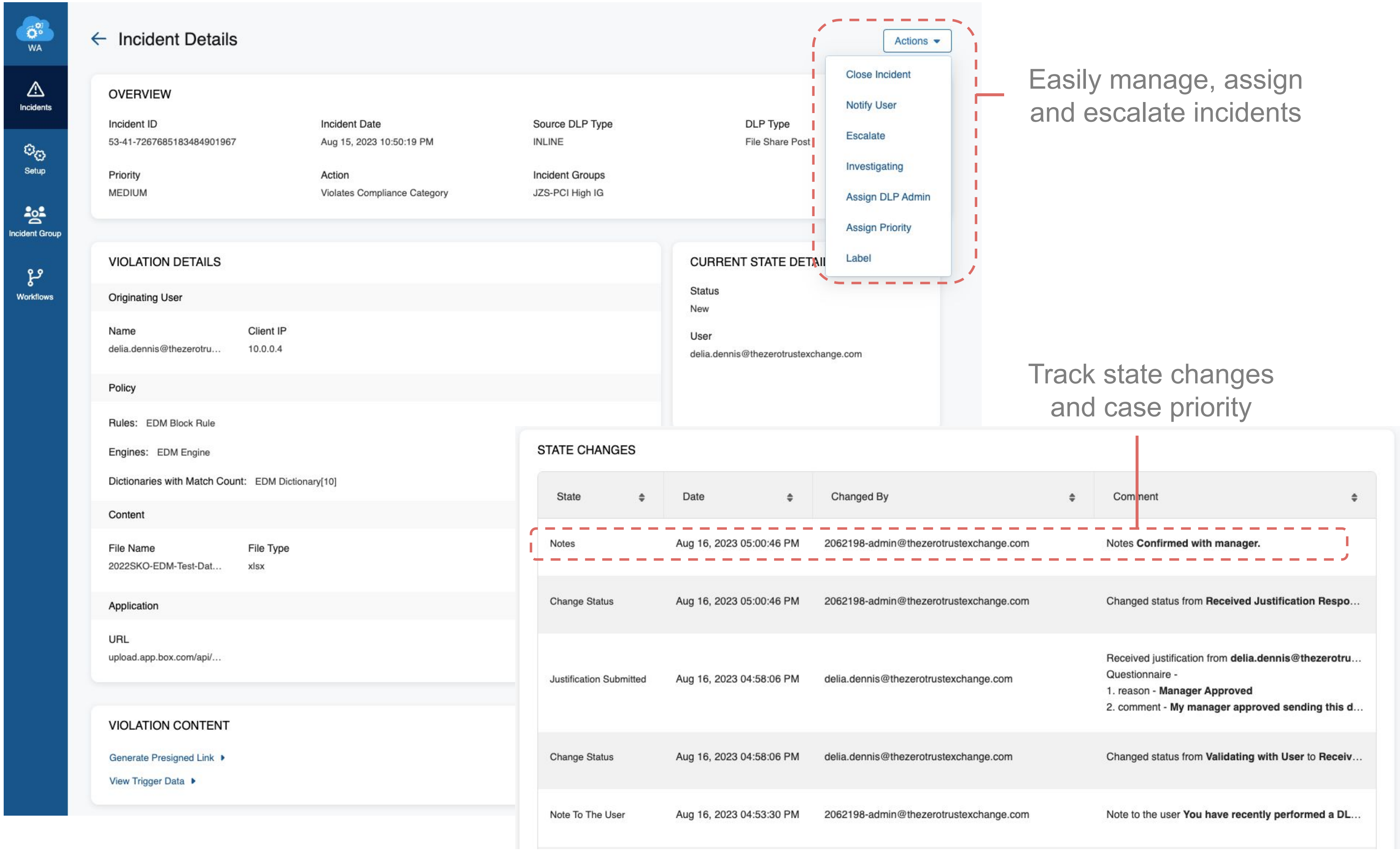
Workflow Automation

Cloud Hosted incident management



Incident justification across users & managers

User Coaching - Improve protection program



Incident Details

OVERVIEW

Incident ID	Incident Date	Source DLP Type	DLP Type
53-41-7267685183484901967	Aug 15, 2023 10:50:19 PM	INLINE	File Share Post
Priority	Action	Incident Groups	
MEDIUM	Violates Compliance Category	JZS-PCI High IG	

VIOLATION DETAILS

Originating User

Name	Client IP
delia.dennis@thezerotru…	10.0.0.4

Policy

Rules: EDM Block Rule

Engines: EDM Engine

Dictionaries with Match Count: EDM Dictionary[10]

Content

File Name	File Type
2022SKO-EDM-Test-Dat…	xlsx

Application

URL
upload.app.box.com/api/…

VIOLATION CONTENT

Generate Presigned Link ▸

View Trigger Data ▸

CURRENT STATE DETAI

Status
New

User
delia.dennis@thezerotrustexchange.com

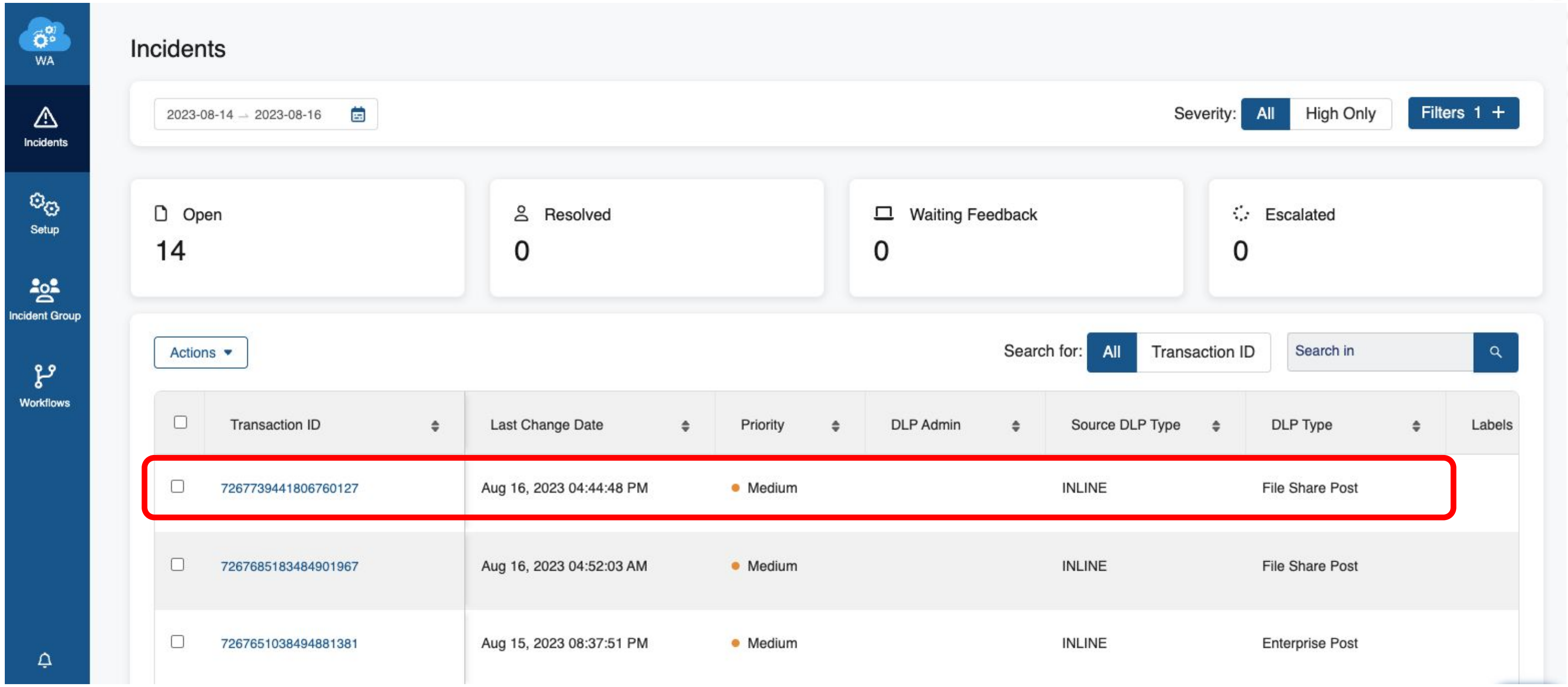
STATE CHANGES

State	Date	Changed By	Comment
Notes	Aug 16, 2023 05:00:46 PM	2062198-admin@thezerotrustexchange.com	Notes **Confirmed with manager.**
Change Status	Aug 16, 2023 05:00:46 PM	2062198-admin@thezerotrustexchange.com	Changed status from **Received Justification Respo…**
Justification Submitted	Aug 16, 2023 04:58:06 PM	delia.dennis@thezerotrustexchange.com	Received justification from **delia.dennis@thezerotru…** Questionnaire - 1. reason - **Manager Approved** 2. comment - **My manager approved sending this d…**
Change Status	Aug 16, 2023 04:58:06 PM	delia.dennis@thezerotrustexchange.com	Changed status from **Validating with User** to **Receiv…**
Note To The User	Aug 16, 2023 04:53:30 PM	2062198-admin@thezerotrustexchange.com	Note to the user **You have recently performed a DL…**

Easily manage, assign and escalate incidents

Track state changes and case priority

Sales Employee Uploads EDM Data to Box



Incidents

2023-08-14 → 2023-08-16

Severity: All High Only

Filters 1 +

Open 14

Resolved 0

Waiting Feedback 0

Escalated 0

Search for: All Transaction ID

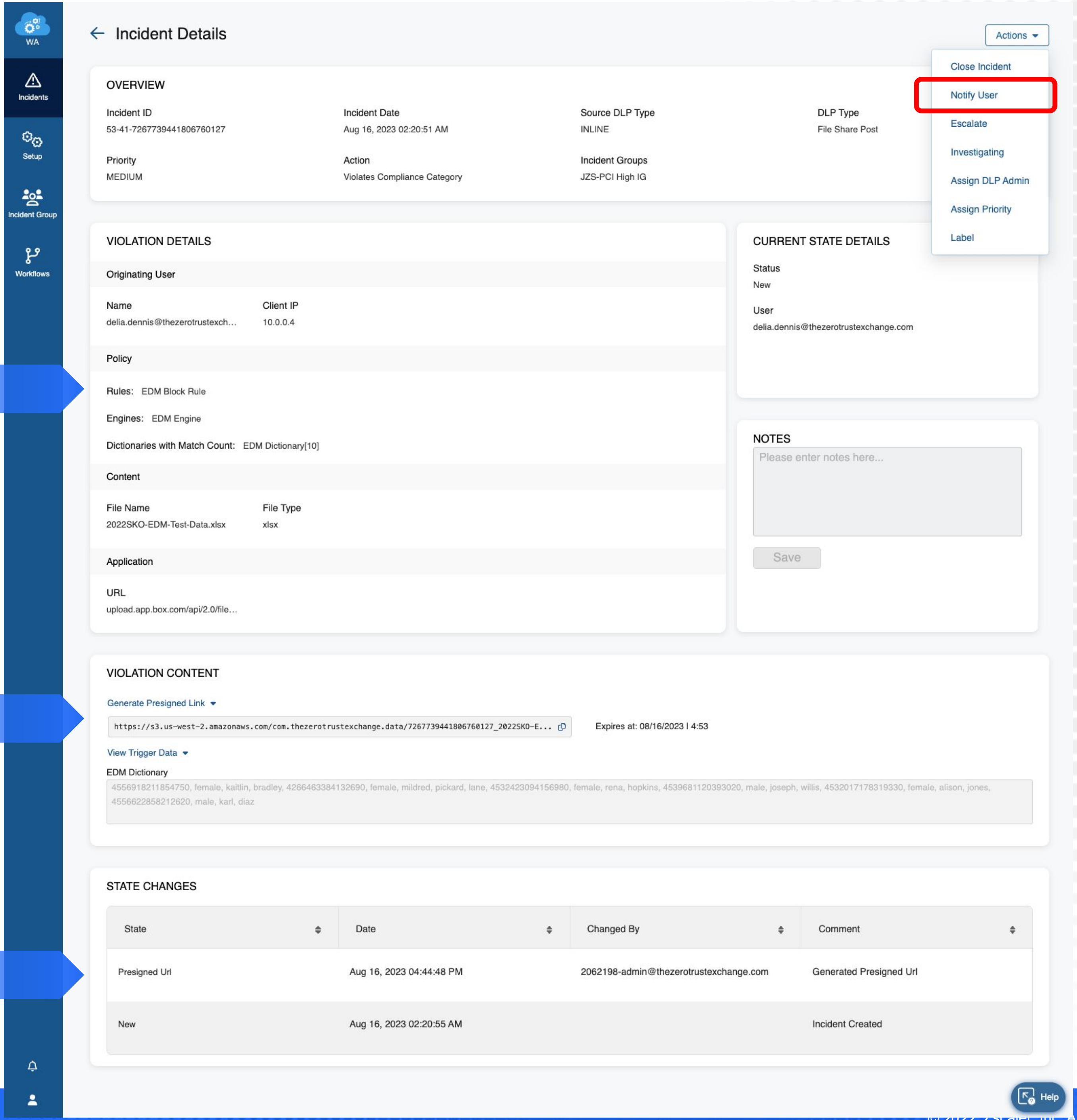
Search in

□	Transaction ID	Last Change Date	Priority	DLP Admin	Source DLP Type	DLP Type	Labels
□	7267739441806760127	Aug 16, 2023 04:44:48 PM	● Medium		INLINE	File Share Post	
□	7267685183484901967	Aug 16, 2023 04:52:03 AM	● Medium		INLINE	File Share Post	
□	7267651038494881381	Aug 15, 2023 08:37:51 PM	● Medium		INLINE	Enterprise Post	

Violation Details

Violating Content

State Changes



Incident Details

OVERVIEW

Incident ID	Incident Date	Source DLP Type	DLP Type
53-41-7267739441806760127	Aug 16, 2023 02:20:51 AM	INLINE	File Share Post
Priority	**Action**	**Incident Groups**	
MEDIUM	Violates Compliance Category	JZS-PCI High IG	

VIOLATION DETAILS

Originating User

Name	Client IP
delia.dennis@thezerotrustexch...	10.0.0.4

Policy

Rules: EDM Block Rule

Engines: EDM Engine

Dictionaries with Match Count: EDM Dictionary[10]

Content

File Name	File Type
2022SKO-EDM-Test-Data.xlsx	xlsx

Application

URL
upload.app.box.com/api/2.0/file...

CURRENT STATE DETAILS

Status
New

User
delia.dennis@thezerotrustexchange.com

NOTES

Please enter notes here...

VIOLATION CONTENT

Generate Presigned Link

`https://s3.us-west-2.amazonaws.com/com.thezerotrustexchange.data/7267739441806760127_2022SKO-E...`

Expires at: 08/16/2023 | 4:53

View Trigger Data

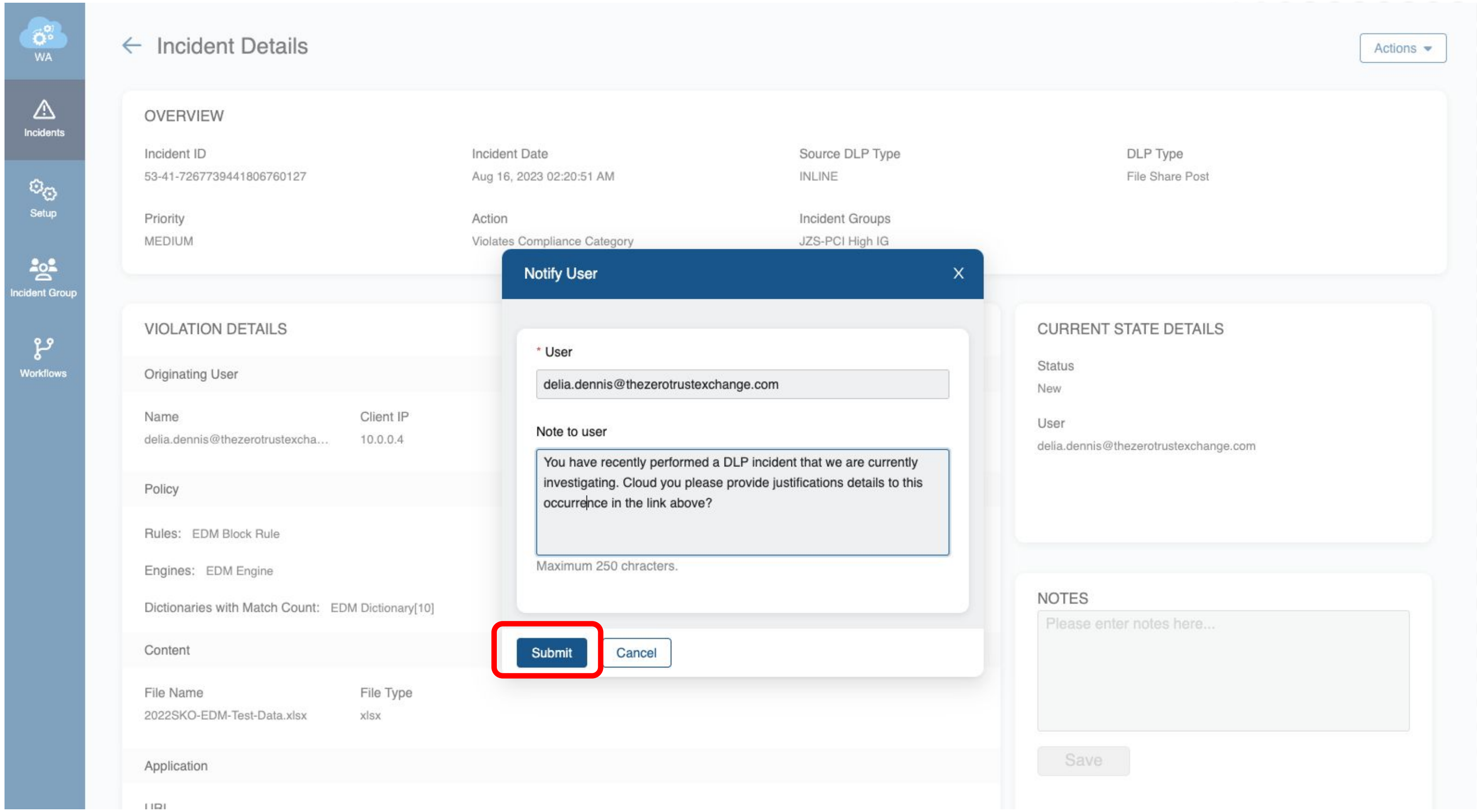
EDM Dictionary

4556918211854750, female, kaitlin, bradley, 4266463384132690, female, mildred, pickard, lane, 4532423094156980, female, rena, hopkins, 4539681120393020, male, joseph, willis, 4532017178319330, female, alison, jones, 4556622858212620, male, karl, diaz

STATE CHANGES

State	Date	Changed By	Comment
Presigned Url	Aug 16, 2023 04:44:48 PM	2062198-admin@thezerotrustexchange.com	Generated Presigned Url
New	Aug 16, 2023 02:20:55 AM		Incident Created

Notify the user from directly within the Incident Management Portal and ask for justification.



Incident Details

OVERVIEW

Incident ID: 53-41-7267739441806760127

Incident Date: Aug 16, 2023 02:20:51 AM

Source DLP Type: INLINE

DLP Type: File Share Post

Priority: MEDIUM

Action: Violates Compliance Category

Incident Groups: JZS-PCI High IG

VIOLATION DETAILS

Originating User

Name: delia.dennis@thezerotrustexcha...

Client IP: 10.0.0.4

Policy

Rules: EDM Block Rule

Engines: EDM Engine

Dictionaries with Match Count: EDM Dictionary[10]

Content

File Name: 2022SKO-EDM-Test-Data.xlsx

File Type: xlsx

Application

URL

Notify User

* User: delia.dennis@thezerotrustexchange.com

Note to user: You have recently performed a DLP incident that we are currently investigating. Cloud you please provide justifications details to this occurrence in the link above?

Maximum 250 chracters.

Submit Cancel

CURRENT STATE DETAILS

Status: New

User: delia.dennis@thezerotrustexchange.com

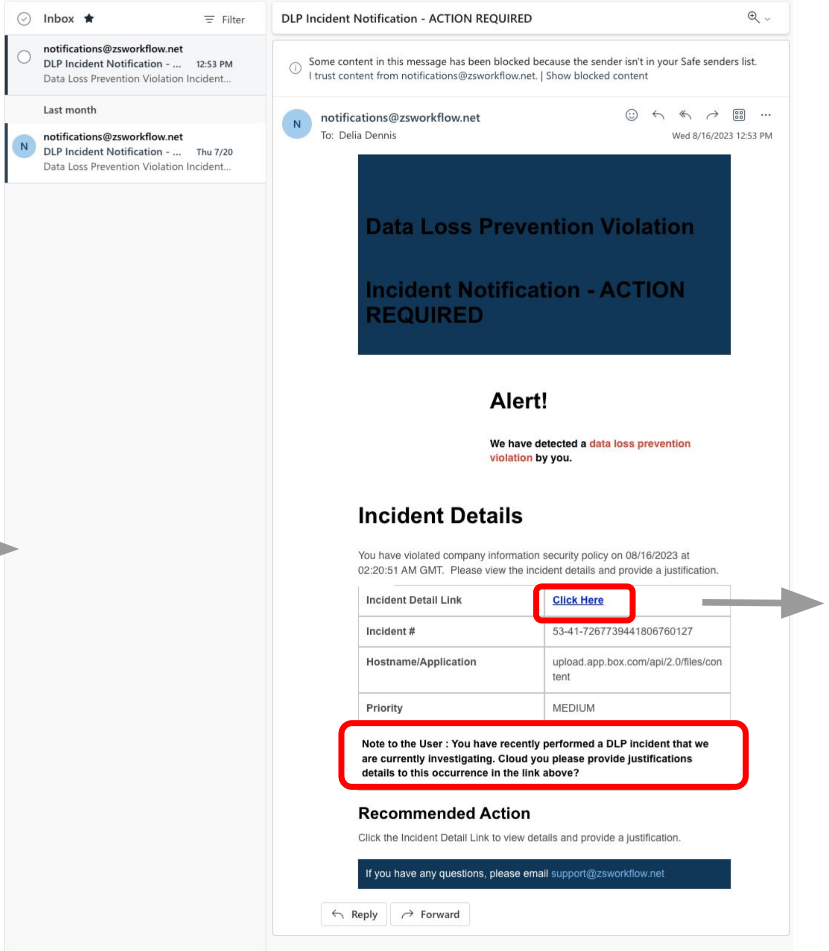
NOTES

Please enter notes here...

Save

User receives email about violation and gets access to their own portal for justification.

Sales employee justification request



notifications@zsworkflow.net
DLP Incident Notification - ... 12:53 PM
Data Loss Prevention Violation Incident...

notifications@zsworkflow.net
DLP Incident Notification - ... Thu 7/20
Data Loss Prevention Violation Incident...

DLP Incident Notification - ACTION REQUIRED

Some content in this message has been blocked because the sender isn't in your Safe senders list.
I trust content from notifications@zsworkflow.net. | Show blocked content

notifications@zsworkflow.net
To: Delia Dennis
Wed 8/16/2023 12:53 PM

Data Loss Prevention Violation

Incident Notification - ACTION REQUIRED

Alert!

We have detected a data loss prevention violation by you.

Incident Details

You have violated company information security policy on 08/16/2023 at 02:20:51 AM GMT. Please view the incident details and provide a justification.

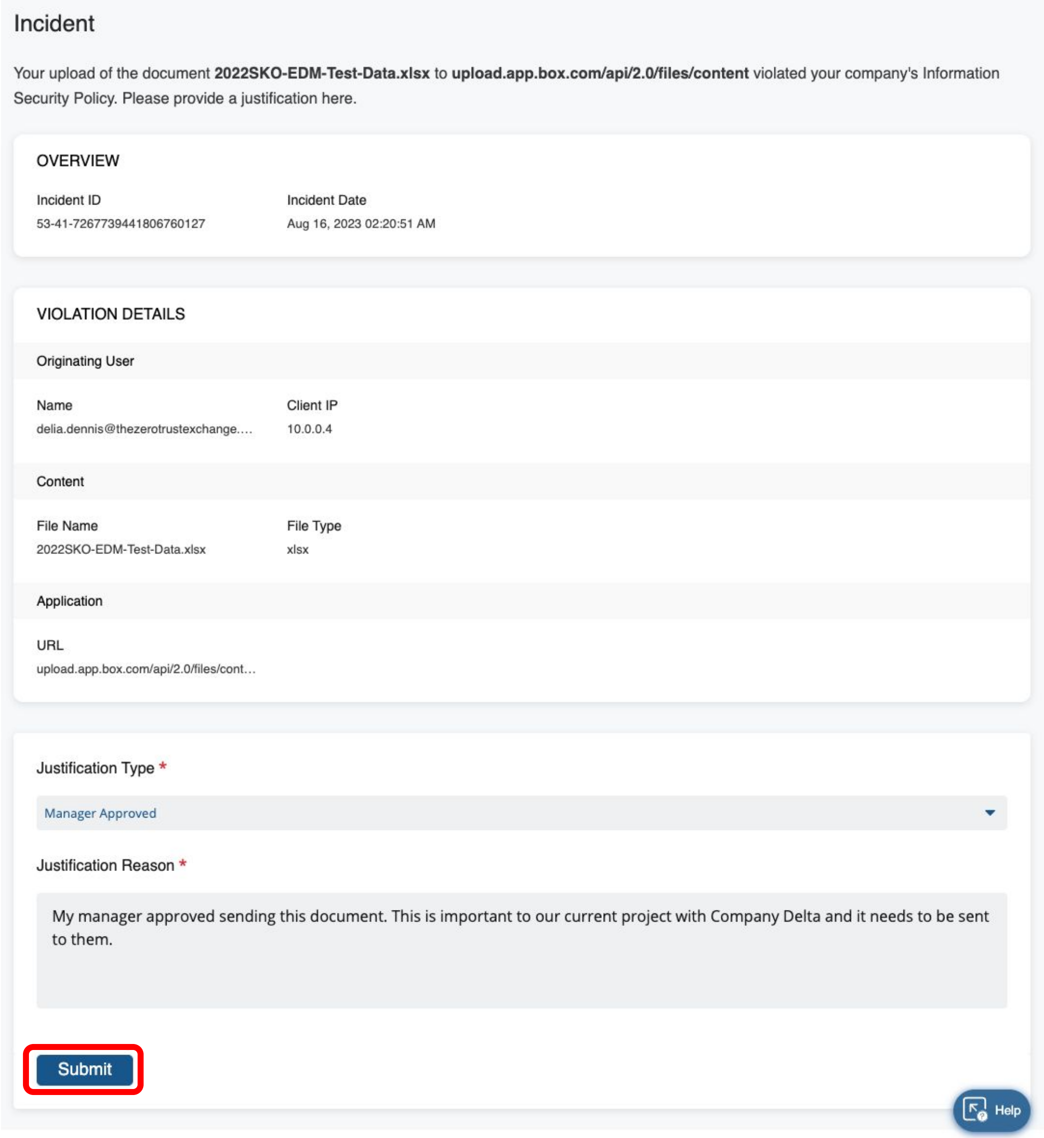
Incident Detail Link	Click Here
Incident #	53-41-7267739441806760127
Hostname/Application	upload.app.box.com/api/2.0/files/content
Priority	MEDIUM

Note to the User : You have recently performed a DLP incident that we are currently investigating. Cloud you please provide justifications details to this occurrence in the link above?

Recommended Action

Click the Incident Detail Link to view details and provide a justification.

If you have any questions, please email support@zsworkflow.net



Incident

Your upload of the document **2022SKO-EDM-Test-Data.xlsx** to **upload.app.box.com/api/2.0/files/content** violated your company's Information Security Policy. Please provide a justification here.

OVERVIEW

Incident ID	Incident Date
53-41-7267739441806760127	Aug 16, 2023 02:20:51 AM

VIOLATION DETAILS

Originating User

Name	Client IP
delia.dennis@thezerotrustexchange....	10.0.0.4

Content

File Name	File Type
2022SKO-EDM-Test-Data.xlsx	xlsx

Application

URL
upload.app.box.com/api/2.0/files/cont...

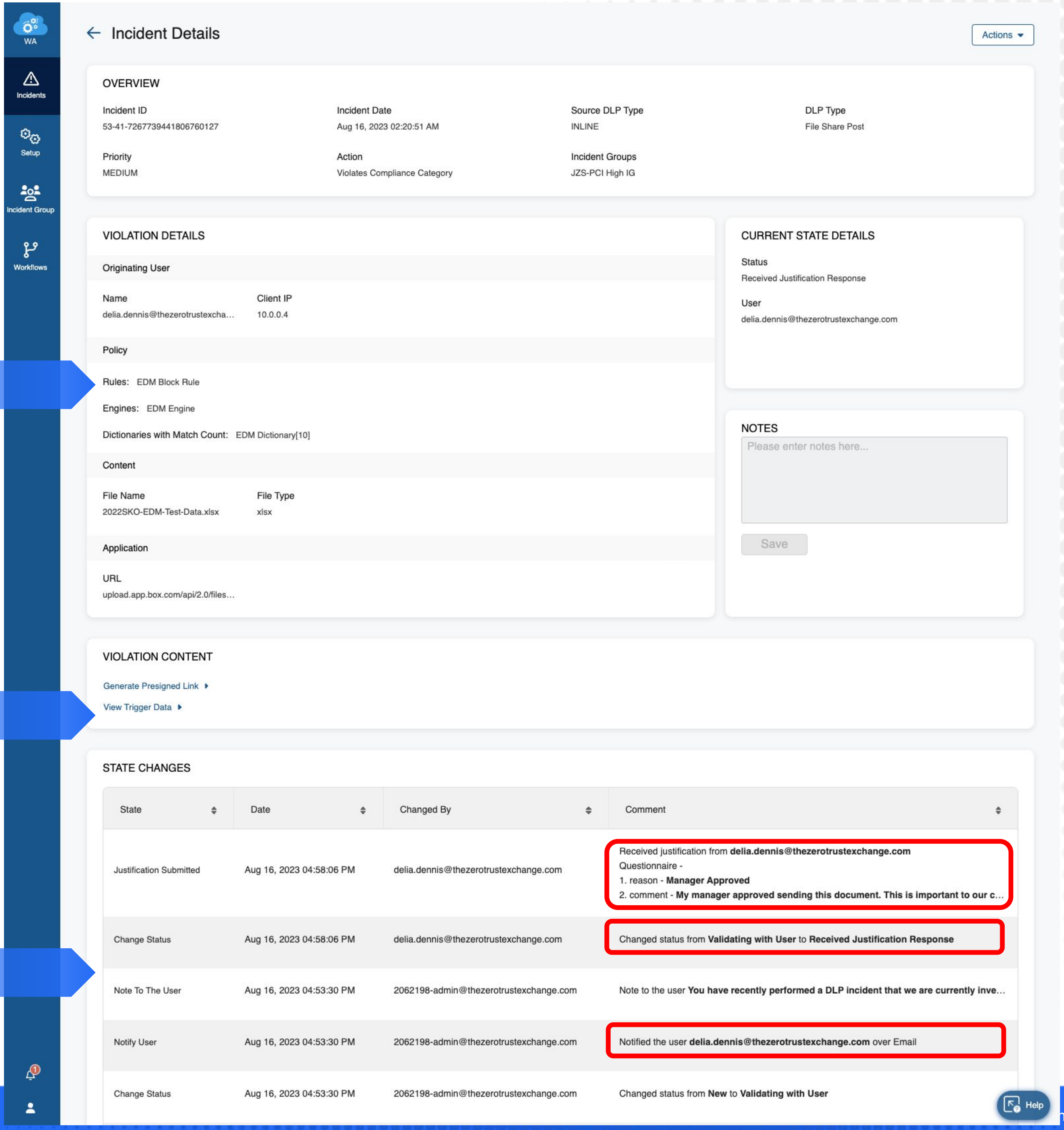
Justification Type *
Manager Approved

Justification Reason *
My manager approved sending this document. This is important to our current project with Company Delta and it needs to be sent to them.

Violation Details

Violating Content

State Changes



Incident Details

OVERVIEW

Incident ID 53-41-7267739441806760127	Incident Date Aug 16, 2023 02:20:51 AM	Source DLP Type INLINE	DLP Type File Share Post
Priority MEDIUM	Action Violates Compliance Category	Incident Groups JZS-PCI High IG	

VIOLATION DETAILS

Originating User

Name

delia.dennis@thezerotrustexcha…

Client IP

10.0.0.4

Policy

Rules: EDM Block Rule

Engines: EDM Engine

Dictionaries with Match Count: EDM Dictionary[10]

Content

File Name

2022SKO-EDM-Test-Data.xlsx

File Type

xlsx

Application

URL

upload.app.box.com/api/2.0/files…

CURRENT STATE DETAILS

Status

Received Justification Response

User

delia.dennis@thezerotrustexchange.com

NOTES

Please enter notes here...

Save

VIOLATION CONTENT

Generate Presigned Link ▸

View Trigger Data ▸

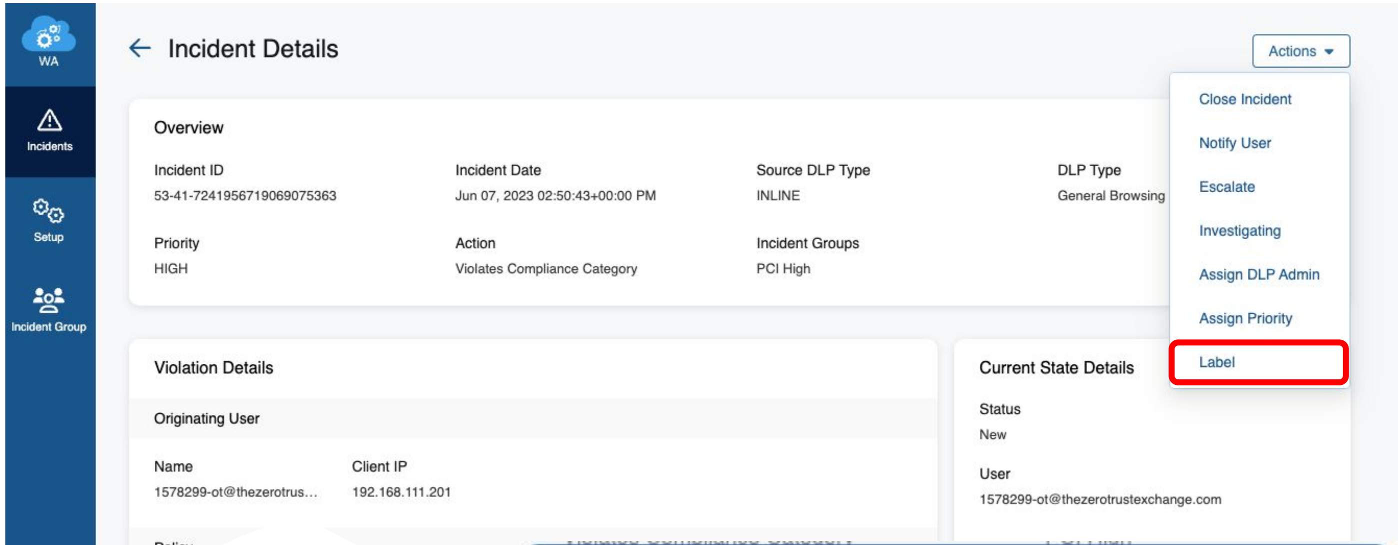
STATE CHANGES

State	Date	Changed By	Comment
Justification Submitted	Aug 16, 2023 04:58:06 PM	delia.dennis@thezerotrustexchange.com	Received justification from **delia.dennis@thezerotrustexchange.com** Questionnaire - 1. reason - **Manager Approved** 2. comment - **My manager approved sending this document. This is important to our c…**
Change Status	Aug 16, 2023 04:58:06 PM	delia.dennis@thezerotrustexchange.com	Changed status from **Validating with User** to **Received Justification Response**
Note To The User	Aug 16, 2023 04:53:30 PM	2062198-admin@thezerotrustexchange.com	Note to the user **You have recently performed a DLP incident that we are currently inve…**
Notify User	Aug 16, 2023 04:53:30 PM	2062198-admin@thezerotrustexchange.com	Notified the user **delia.dennis@thezerotrustexchange.com** over Email
Change Status	Aug 16, 2023 04:53:30 PM	2062198-admin@thezerotrustexchange.com	Changed status from **New** to **Validating with User**

Implement Workflows for Incident Triage

- Label Incidents
- Escalate to Managers
- Assign to other Admins

All from one location through investigation and after completion control follow-ups and assignments to get resolution.



Incident Details

Overview

Incident ID
53-41-7241956719069075363

Incident Date
Jun 07, 2023 02:50:43+00:00 PM

Source DLP Type
INLINE

DLP Type
General Browsing

Priority
HIGH

Action
Violates Compliance Category

Incident Groups
PCI High

Violation Details

Originating User

Name
1578299-ot@thezerotrus...

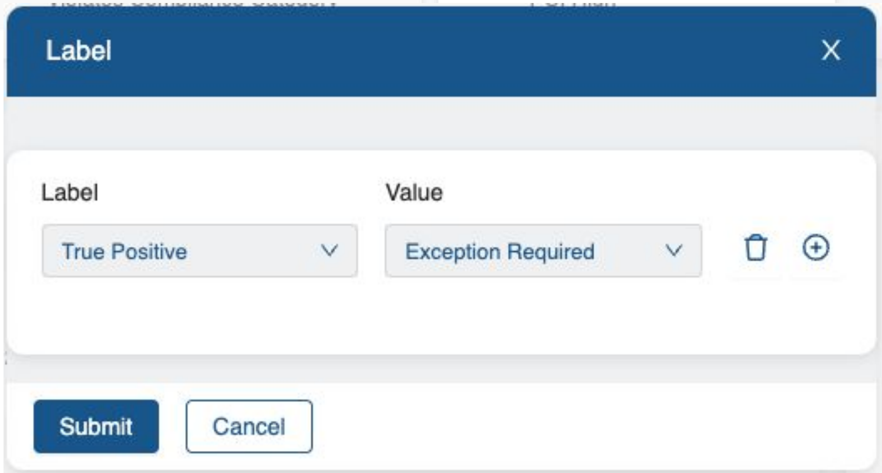
Client IP
192.168.111.201

Policy

Current State Details

Status
New

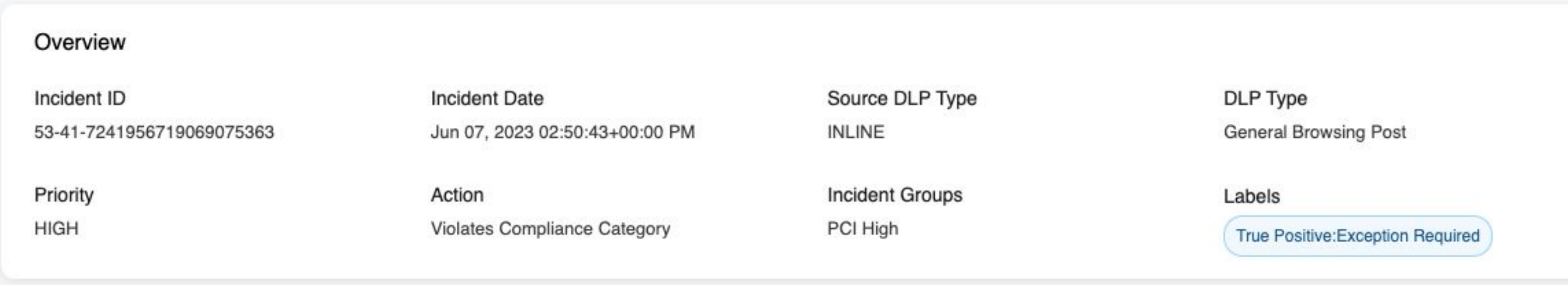
User
1578299-ot@thezerotrustexchange.com



Label: True Positive

Value: Exception Required

Label Incidents for Followup
Label Incident for further follow up for exception.



Overview

Incident ID
53-41-7241956719069075363

Incident Date
Jun 07, 2023 02:50:43+00:00 PM

Source DLP Type
INLINE

DLP Type
General Browsing Post

Priority
HIGH

Action
Violates Compliance Category

Incident Groups
PCI High

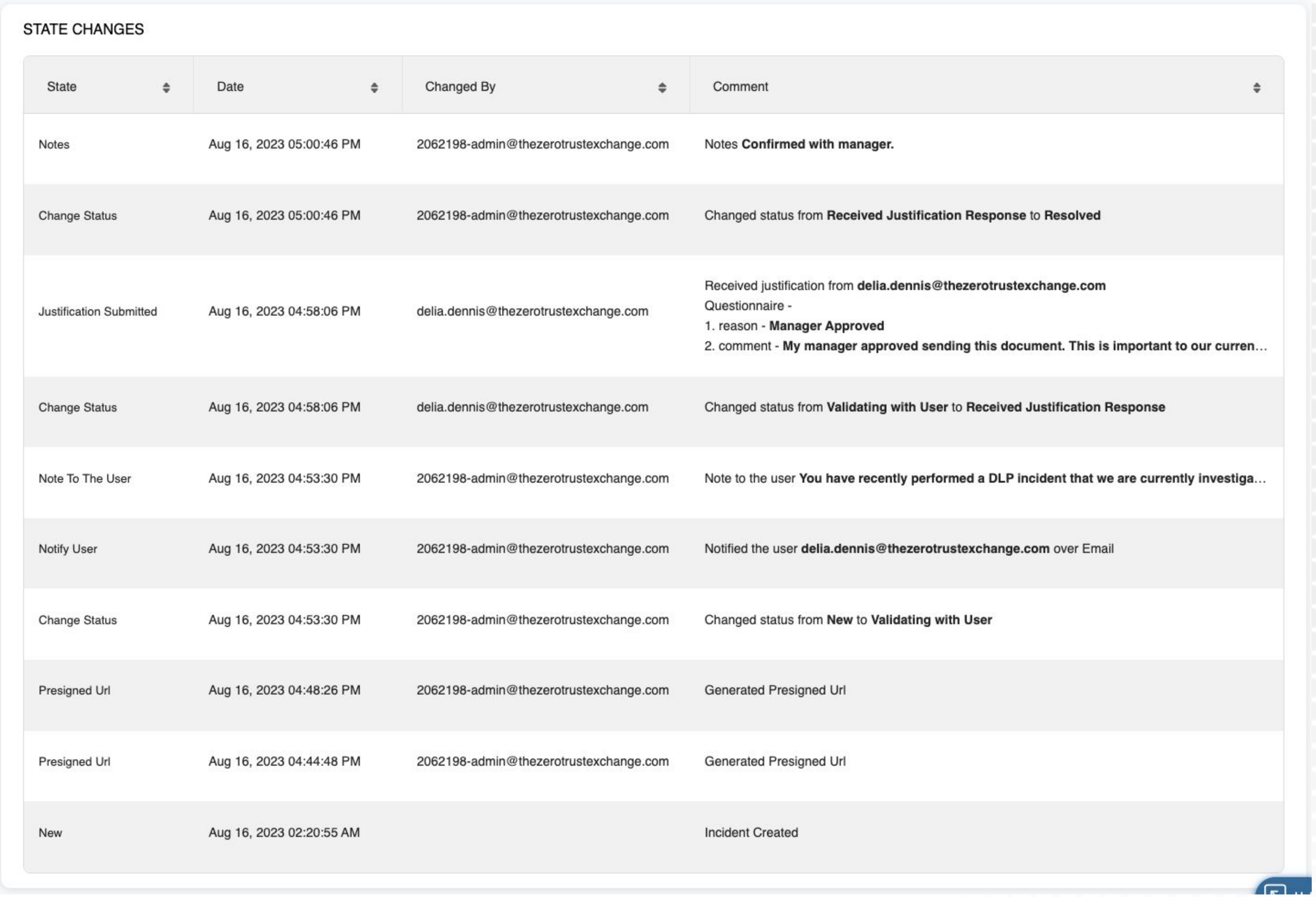
Labels
True Positive:Exception Required

Label Controls
Assign via label to appropriate groups for review after investigation

Ensure everything that occurs during Incident Management is audited.

- All State Changes
- Assignments
- Notifications to Users or Management
- Escalations
- Closures
- Labeling

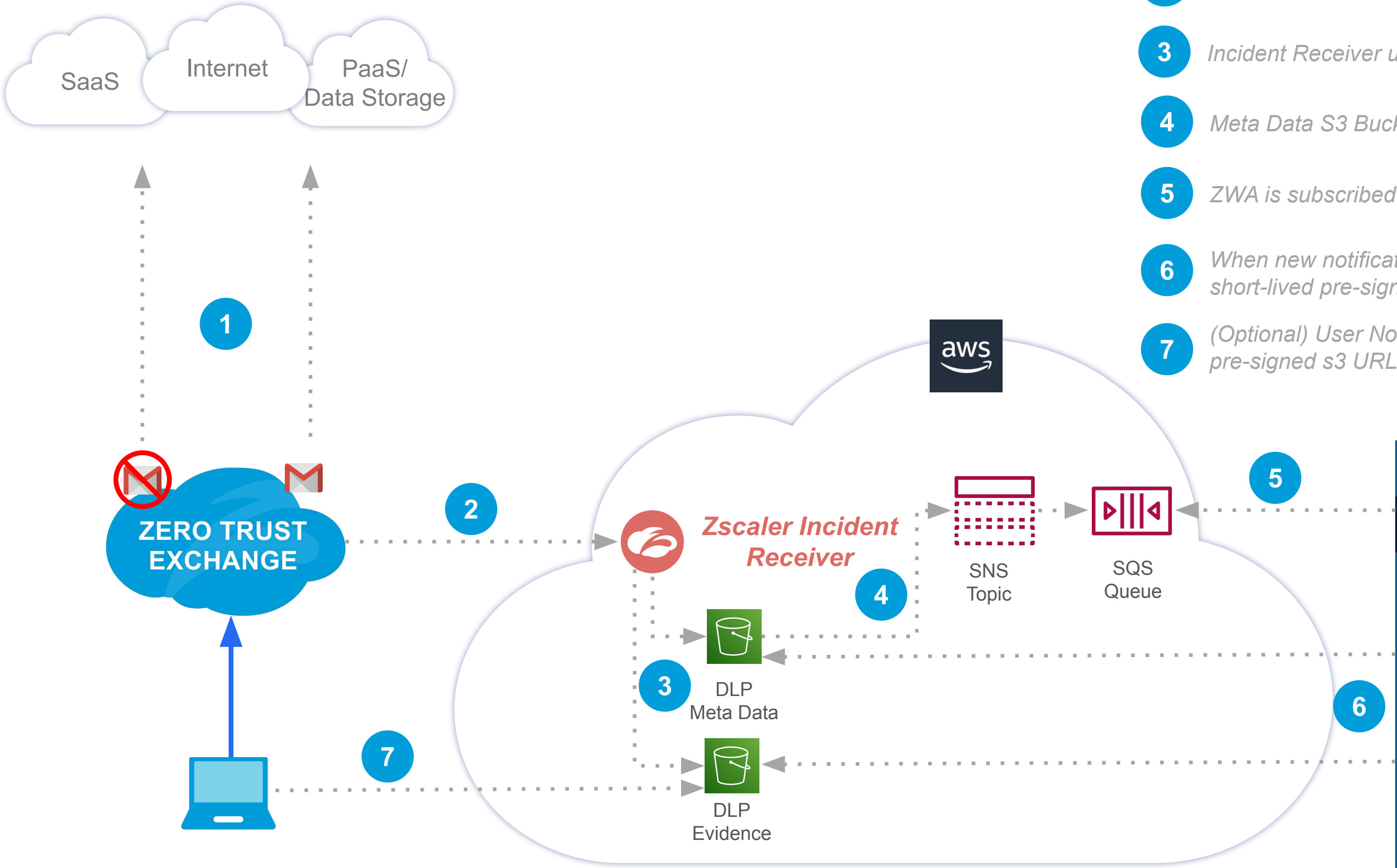
Everything that is performed on the incident will be tracked and reviewable.



STATE CHANGES

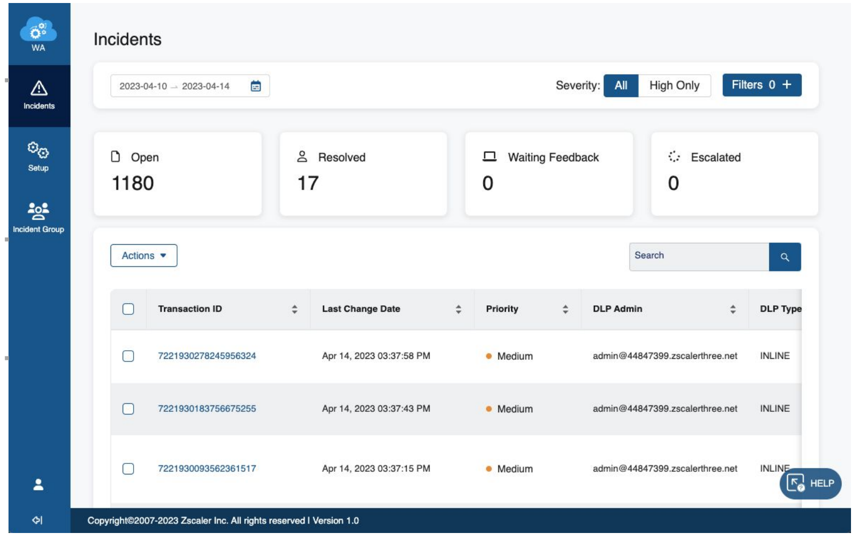
State	Date	Changed By	Comment
Notes	Aug 16, 2023 05:00:46 PM	2062198-admin@thezerotrustexchange.com	Notes **Confirmed with manager.**
Change Status	Aug 16, 2023 05:00:46 PM	2062198-admin@thezerotrustexchange.com	Changed status from **Received Justification Response** to **Resolved**
Justification Submitted	Aug 16, 2023 04:58:06 PM	delia.dennis@thezerotrustexchange.com	Received justification from **delia.dennis@thezerotrustexchange.com** Questionnaire - 1. reason - **Manager Approved** 2. comment - **My manager approved sending this document. This is important to our curren...**
Change Status	Aug 16, 2023 04:58:06 PM	delia.dennis@thezerotrustexchange.com	Changed status from **Validating with User** to **Received Justification Response**
Note To The User	Aug 16, 2023 04:53:30 PM	2062198-admin@thezerotrustexchange.com	Note to the user **You have recently performed a DLP incident that we are currently investiga...**
Notify User	Aug 16, 2023 04:53:30 PM	2062198-admin@thezerotrustexchange.com	Notified the user **delia.dennis@thezerotrustexchange.com** over Email
Change Status	Aug 16, 2023 04:53:30 PM	2062198-admin@thezerotrustexchange.com	Changed status from **New** to **Validating with User**
Presigned Url	Aug 16, 2023 04:48:26 PM	2062198-admin@thezerotrustexchange.com	Generated Presigned Url
Presigned Url	Aug 16, 2023 04:44:48 PM	2062198-admin@thezerotrustexchange.com	Generated Presigned Url
New	Aug 16, 2023 02:20:55 AM		Incident Created

Data Protection: Reporting, Analytics & Incident Management with ZWA



How Zscaler Workflow Automation works

1. *DLP Rule configured to Send Incident for Allow or Block to Incident Receiver*
2. *Incident Details and Evidence file sent via ICAPS to Incident Receiver in AWS*
3. *Incident Receiver uploads incident Meta Data and Evidence Files to appropriate S3 Buckets via SCP*
4. *Meta Data S3 Bucket publishes notifications to SNS Topic which posts on the SQS Queue*
5. *ZWA is subscribed to the SQS Queue and receives notifications from SQS about new SNS Topics*
6. *When new notifications are received on SQS Queue the meta data is read for the event is read and a short-lived pre-signed s3 URL link is collected by ZWA using IAM cross-accounts*
7. *(Optional) User Notifications can contain link to original evidence file for their viewing. A short-lived pre-signed s3 URL Link can also be provided.*



Incidents

2023-04-10 → 2023-04-14

Open	Resolved	Waiting Feedback	Escalated
1180	17	0	0

□	Transaction ID	Last Change Date	Priority	DLP Admin	DLP Type
□	7221930278245956324	Apr 14, 2023 03:37:58 PM	● Medium	admin@44847399.zscalerthree.net	INLINE
□	7221930183756675255	Apr 14, 2023 03:37:43 PM	● Medium	admin@44847399.zscalerthree.net	INLINE
□	7221930093562361517	Apr 14, 2023 03:37:15 PM	● Medium	admin@44847399.zscalerthree.net	INLINE

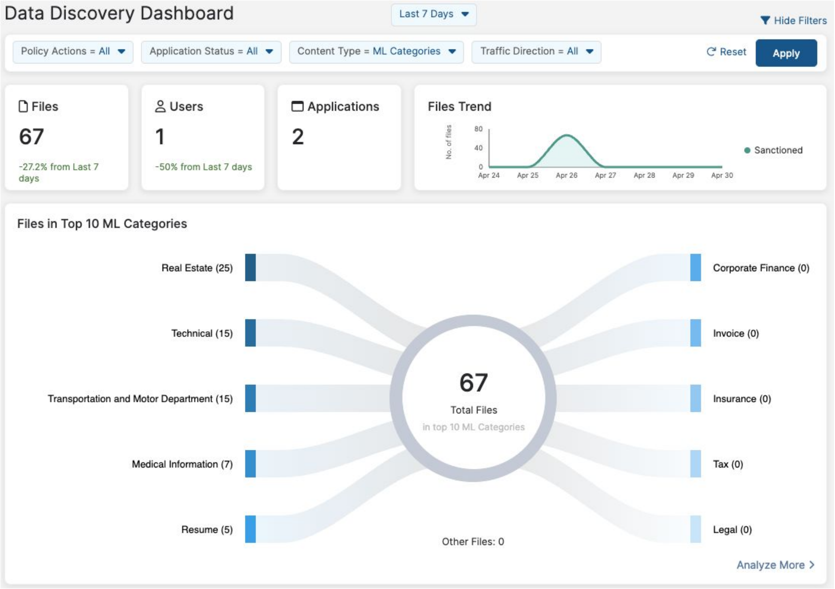
Copyright©2007-2023 Zscaler Inc. All rights reserved I Version 1.0

Thank you

One to Rule Them All

Data Discovery Dashboard

Machine Learning Classification



Data Discovery Dashboard

Last 7 Days ▾ | Hide Filters

Policy Actions = All ▾ | Application Status = All ▾ | Content Type = ML Categories ▾ | Traffic Direction = All ▾ | Reset | Apply

Files 67 -27.2% from Last 7 days

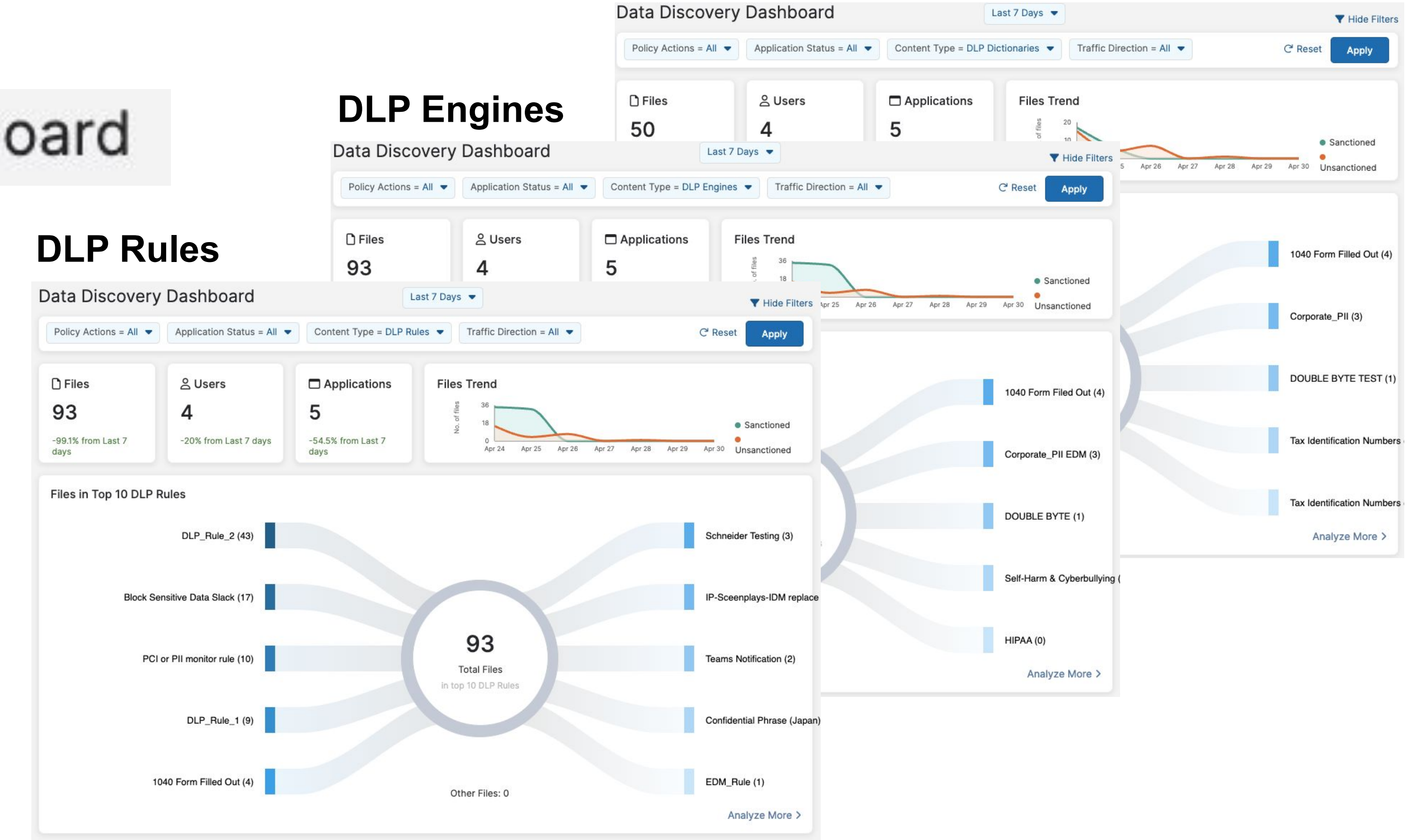
Users 1 -50% from Last 7 days

Applications 2

Files Trend

Files in Top 10 ML Categories

DLP Dictionaries



DLP Engines

DLP Rules

Data Discovery Dashboard

Last 7 Days ▾ | Hide Filters

Policy Actions = All ▾ | Application Status = All ▾ | Content Type = DLP Rules ▾ | Traffic Direction = All ▾ | Reset | Apply

Files 93 -99.1% from Last 7 days

Users 4 -20% from Last 7 days

Applications 5 -54.5% from Last 7 days

Files Trend

Files in Top 10 DLP Rules

Data Discovery Dashboard

Last 7 Days ▾ | Hide Filters

Policy Actions = All ▾ | Application Status = All ▾ | Content Type = DLP Engines ▾ | Traffic Direction = All ▾ | Reset | Apply

Files 93

Users 4

Applications 5

Files Trend

Data Discovery Dashboard

Last 7 Days ▾ | Hide Filters

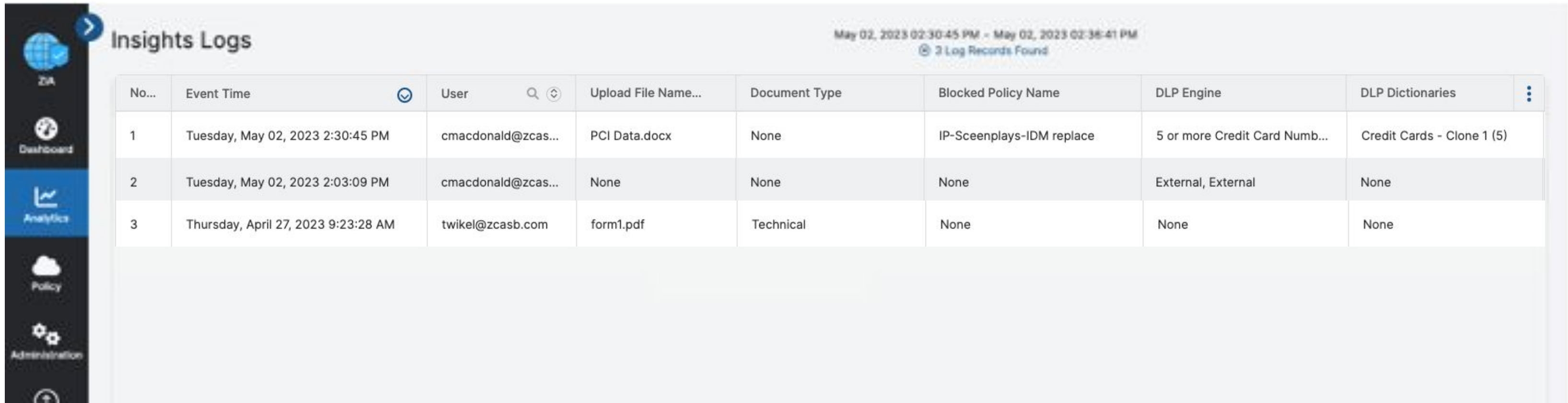
Policy Actions = All ▾ | Application Status = All ▾ | Content Type = DLP Dictionaries ▾ | Traffic Direction = All ▾ | Reset | Apply

Files 50

Users 4

Applications 5

Files Trend



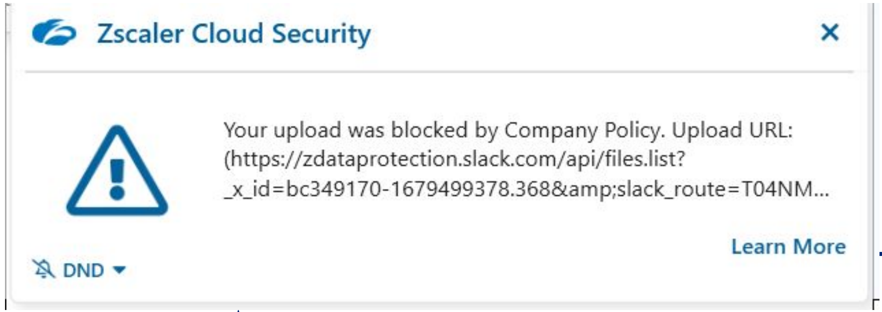
Insights Logs

May 02, 2023 02:30:45 PM – May 02, 2023 02:36:41 PM

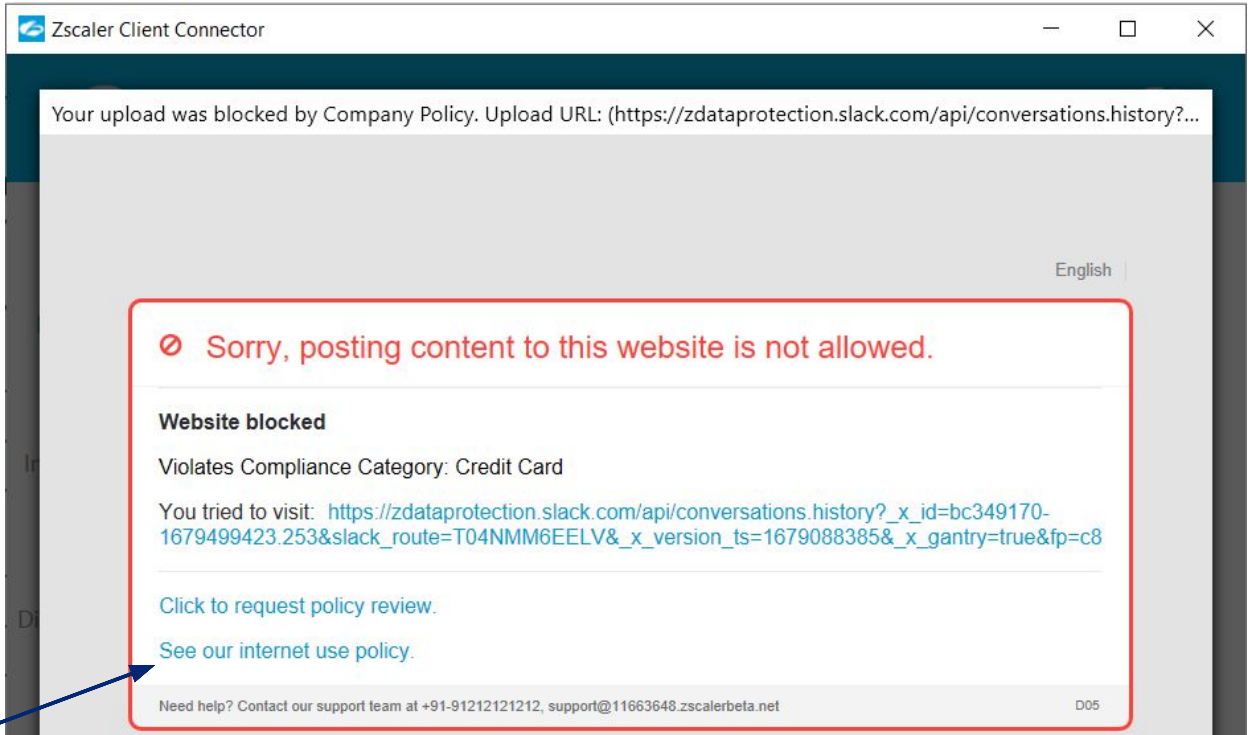
3 Log Records Found

No...	Event Time	User	Upload File Name...	Document Type	Blocked Policy Name	DLP Engine	DLP Dictionaries
1	Tuesday, May 02, 2023 2:30:45 PM	cmacdonald@zcas...	PCI Data.docx	None	IP-Sceenplays-IDM replace	5 or more Credit Card Numb...	Credit Cards - Clone 1 (5)
2	Tuesday, May 02, 2023 2:03:09 PM	cmacdonald@zcas...	None	None	None	External, External	None
3	Thursday, April 27, 2023 9:23:28 AM	twikel@zcasb.com	form1.pdf	Technical	None	None	None

End User Notification for DLP



Your upload was blocked by Company Policy. Upload URL: (https://zdataprotection.slack.com/api/files.list?_x_id=bc349170-1679499378.368&amp;slack_route=T04NM...



Your upload was blocked by Company Policy. Upload URL: (https://zdataprotection.slack.com/api/conversations.history?...

⊘ Sorry, posting content to this website is not allowed.

Website blocked

Violates Compliance Category: Credit Card

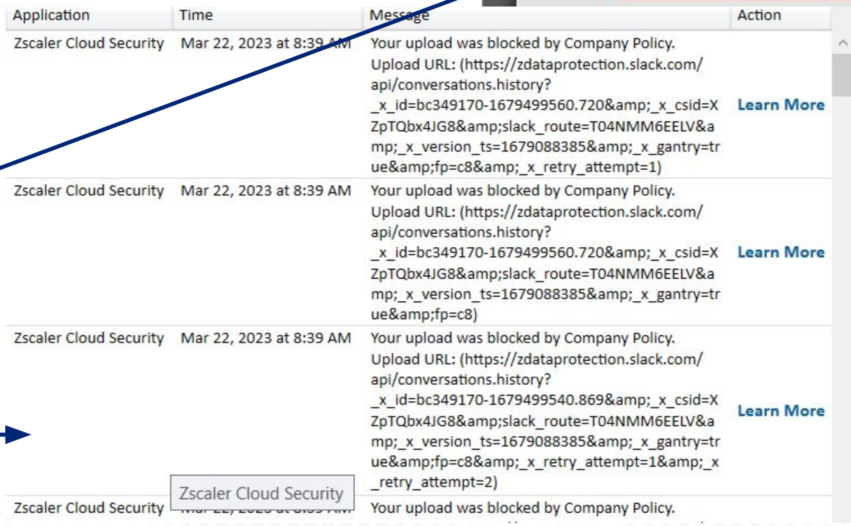
You tried to visit: https://zdataprotection.slack.com/api/conversations.history?_x_id=bc349170-1679499423.253&slack_route=T04NMM6EELV&_x_version_ts=1679088385&_x_gantry=true&fp=c8

Click to request policy review.

See our internet use policy.

Need help? Contact our support team at +91-91212121212, support@11663648.zscalerbeta.net D05

Your organization has selected Zscaler to protect you from internet threats.



Application	Time	Message	Action
Zscaler Cloud Security	Mar 22, 2023 at 8:39 AM	Your upload was blocked by Company Policy. Upload URL: (https://zdataprotection.slack.com/api/conversations.history?_x_id=bc349170-1679499560.720&amp;_x_csid=XZpTQbx4JG8&amp;slack_route=T04NMM6EELV&amp;_x_version_ts=1679088385&amp;_x_gantry=true&amp;fp=c8&amp;_x_retry_attempt=1)	Learn More
Zscaler Cloud Security	Mar 22, 2023 at 8:39 AM	Your upload was blocked by Company Policy. Upload URL: (https://zdataprotection.slack.com/api/conversations.history?_x_id=bc349170-1679499560.720&amp;_x_csid=XZpTQbx4JG8&amp;slack_route=T04NMM6EELV&amp;_x_version_ts=1679088385&amp;_x_gantry=true&amp;fp=c8)	Learn More
Zscaler Cloud Security	Mar 22, 2023 at 8:39 AM	Your upload was blocked by Company Policy. Upload URL: (https://zdataprotection.slack.com/api/conversations.history?_x_id=bc349170-1679499540.869&amp;_x_csid=XZpTQbx4JG8&amp;slack_route=T04NMM6EELV&amp;_x_version_ts=1679088385&amp;_x_gantry=true&amp;fp=c8&amp;_x_retry_attempt=1&amp;_x_retry_attempt=2)	Learn More
Zscaler Cloud Security	[illegible]	Your upload was blocked by Company Policy.	

Alert from Client

Web Block

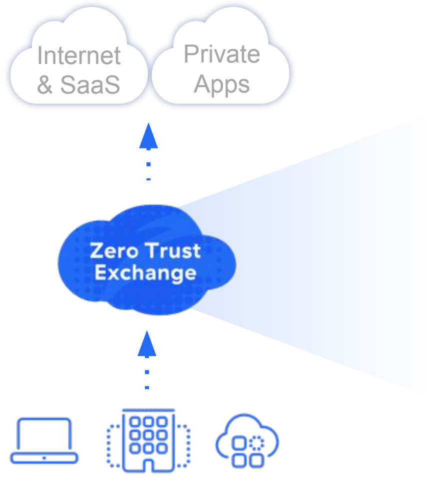
Client logs

Workflow Automation

Streamline workflows with automated closed-loop investigations

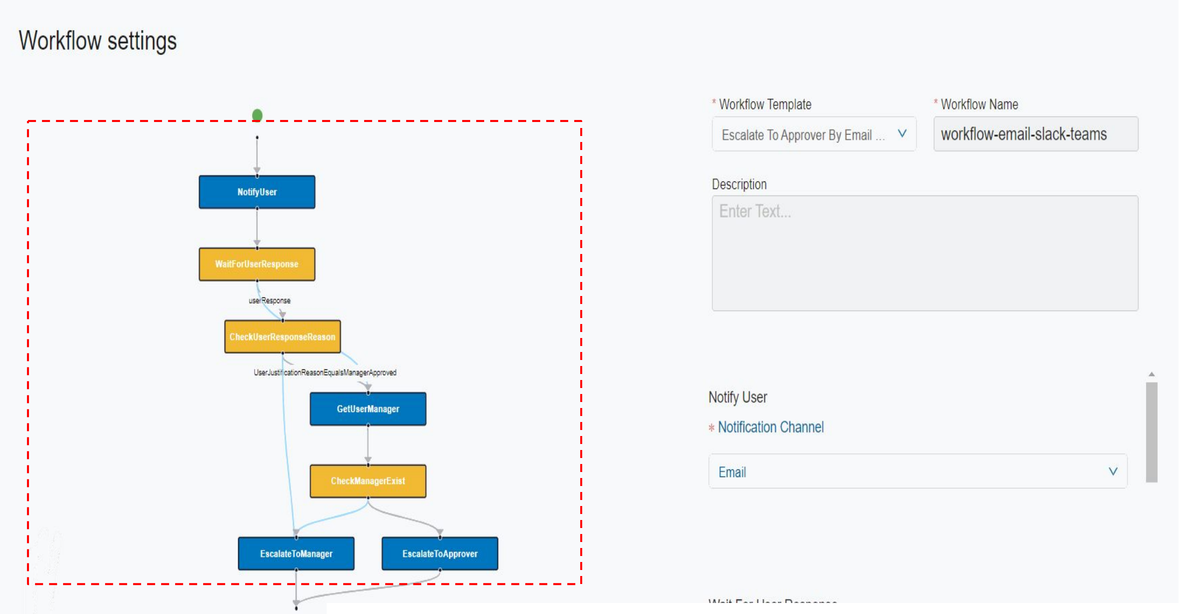
Workflow Automation

Cloud Hosted incident management



Incident justification
across users & managers

User Coaching -
Improve protection program



Workflow settings

* Workflow Template: Escalate To Approver By Email ...

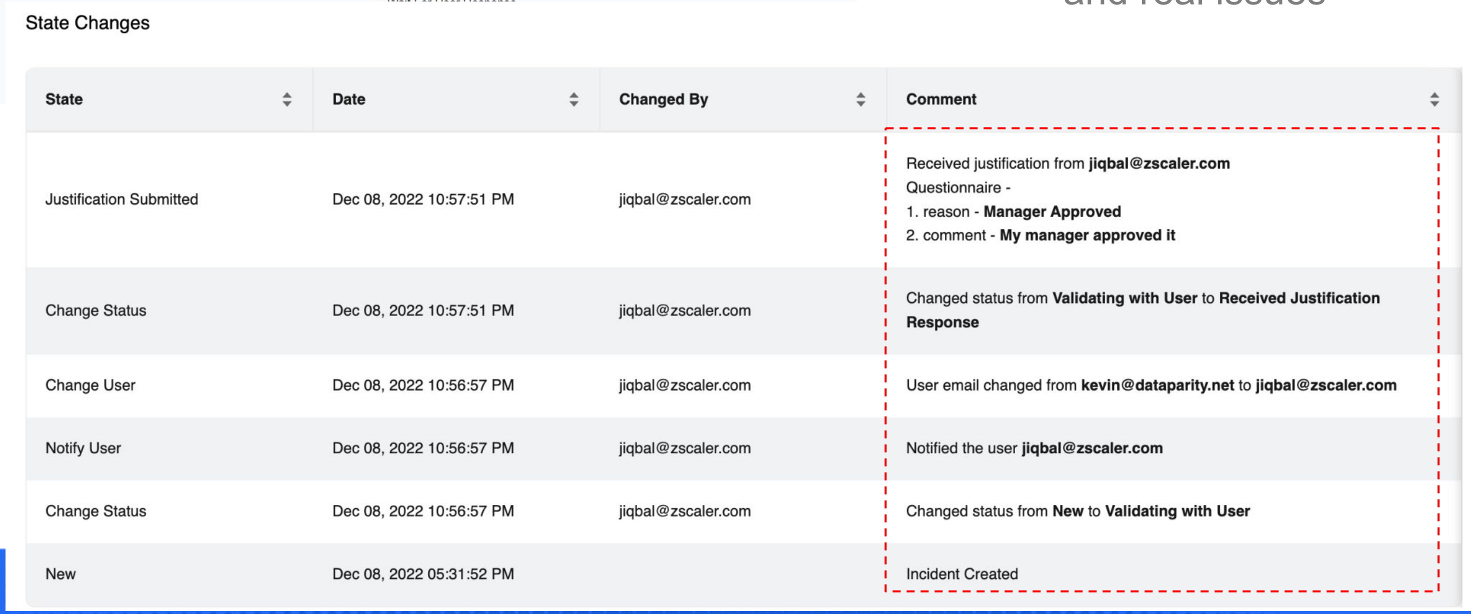
* Workflow Name: workflow-email-slack-teams

Description: Enter Text...

Notify User

* Notification Channel: Email

Automate the incident Triaging with conditional workflow management



State Changes

State	Date	Changed By	Comment
Justification Submitted	Dec 08, 2022 10:57:51 PM	jiqbal@zscaler.com	Received justification from **jiqbal@zscaler.com** Questionnaire - 1. reason - **Manager Approved** 2. comment - **My manager approved it**
Change Status	Dec 08, 2022 10:57:51 PM	jiqbal@zscaler.com	Changed status from **Validating with User** to **Received Justification Response**
Change User	Dec 08, 2022 10:56:57 PM	jiqbal@zscaler.com	User email changed from **kevin@dataparity.net** to **jiqbal@zscaler.com**
Notify User	Dec 08, 2022 10:56:57 PM	jiqbal@zscaler.com	Notified the user **jiqbal@zscaler.com**
Change Status	Dec 08, 2022 10:56:57 PM	jiqbal@zscaler.com	Changed status from **New** to **Validating with User**
New	Dec 08, 2022 05:31:52 PM		Incident Created

Reduce manual triaging , help IR team focus on optimization and real issues