

# STUDY GUIDE:

## Zscaler Digital Transformation Administrator (ZDTA) Certification

- Zscaler Digital Transformation..... 3**
  - How to Use This Study Guide..... 3
  - About the ZDTA Exam..... 3
    - Exam Format..... 3
  - Audience & Qualifications..... 4
    - Skills Required..... 4
    - Recommended Training..... 4
  - Core Skills..... 5
    - Identity Services..... 5
      - Authentication and Authorization to the Zero Trust Exchange..... 6
      - SAML Authentication..... 7
      - SCIM Authorization..... 10
    - Basic Connectivity..... 13
      - Connecting to the Zero Trust Exchange (ZTE)..... 14
      - Zscaler Client Connector..... 15
      - App Connectors..... 39
      - Browser Access & Privileged Remote Access..... 43
    - Platform Services..... 46
      - Zscaler's Platform Services Suite..... 47
      - Device Posture..... 48
      - TLS Inspection..... 49
      - Policy Framework..... 62
      - Analytics & Reporting..... 67
    - Zscaler Digital Experience..... 70
      - Introduction to Zscaler Digital Experience..... 71
      - Monitoring Digital Experience..... 82
    - Access Control..... 86
      - Access Control Overview..... 87
      - Zscaler's Access Control Services Suite..... 88
    - Cybersecurity Services..... 96
      - Cybersecurity Overview..... 97
      - Zscaler's Cybersecurity Services Suite..... 104

Basic Data Protection Services.....	117
Data Protection Overview.....	119
Protecting Data in Motion.....	123
Protecting Data at Rest.....	131
Incident Management.....	133
Basic Troubleshooting Tools & Support.....	135
Zscaler Self Help Services.....	136
Zscaler Troubleshooting Process & Tools.....	138
Zscaler Customer Support Services.....	146

# Zscaler Digital Transformation Administrator

## How to Use This Study Guide

Welcome to the Zscaler ZDTA Study Guide, which will serve as your go-to resource in preparing for the ZDTA exam and receiving your ZDTA certification.



## About the ZDTA Exam

The Zscaler Digital Transformation Administrator (ZDTA) is a formal, third-party proctored certification that indicates that those who have achieved it possess the in-depth knowledge to design, install, configure, maintain, and troubleshoot most Zero Trust Exchange implementations.

### Exam Format

**Certification name:** Zscaler Digital Transformation Administrator (ZDTA)

**Delivered through:** Certiverse, our online testing platform

**Exam series:** Zscaler Digital Transformation

**Seat time:** 90 minutes

**Number of items:** 50

**Format:** Multiple Choice, Scenarios with Graphics, and Matching

**Languages:** English

Exam Domain	Weight (%)
Identity Services	4
Basic Connectivity	20
Platform Services	15
Zscaler Digital Experience	10
Access Control	15
Cybersecurity Services	20
Basic Data Protection	16

## Audience & Qualifications

The ZDTA exam is for Zscaler customers as well as all who sell and support the Zscaler platform. By taking the exam, you are demonstrating your deep understanding and knowledge needed to sufficiently drive operational success.

Candidates should have a:

- Minimum of 5 years working in both IT networks and cybersecurity
- Minimum of 1 year experience with the Zscaler platform

## Skills Required

- Ability to professionally design, implement, operate, and troubleshoot the Zscaler platform
- Ability to adapt legacy on-premises technologies and legacy hub-and-spoke network designs to modern cloud architectures

## Recommended Training

Zscaler recommends that you have first attended the Zscaler for Users (EDU-200) course and hands-on lab, or have solid hands-on experience with ZIA, ZPA and ZDX.

## Core Skills

### Identity Services

Identity Integration will teach you how to authenticate users to the Zero Trust Exchange. This chapter will enable you to understand how to authenticate users to the Zero Trust Exchange, and how user attributes are consumed for policy.

---

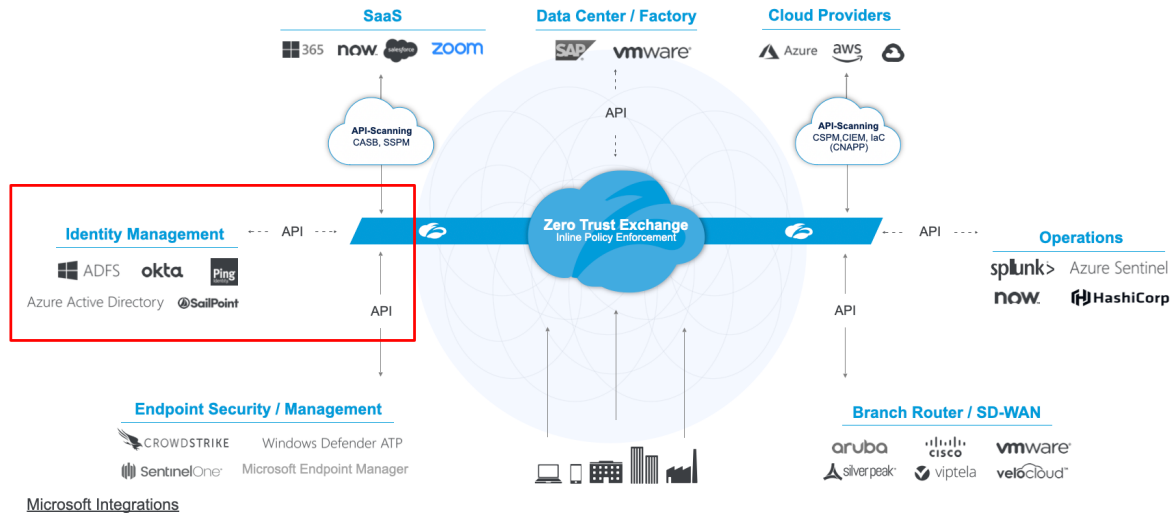
By the end of this chapter, you will be able to

1. **Recognize** how authentication mechanisms work and how they are integrated with Zscaler.
2. **Discover** how to configure Zscaler Identity Integration services and capabilities.

## Authentication and Authorization to the Zero Trust Exchange

### Ecosystem of best-of-breed platforms

Platforms eliminate point solutions and allow for vendor consolidation



The first thing we do when we connect to the Zero Trust Exchange is verify identity and context, while also consuming attributes for policy. Usually that means connecting to a SAML identity provider (IdP), but in the case of Zscaler Internet Access, it could be other methods such as LDAP or a hosted database.

Once we understand the user context, we can control risk through inspection and data protection, and then we can enforce policies such as Allow, Block, Isolate, and Prioritize. Based on attributes of the user and the device, Zscaler Internet Access covers SaaS applications and internet applications. Zscaler Private Access configures connectivity to private applications and resources hosted at Infrastructure as a Service, Platform as a Service, or your private data center.

The identity integration enables us to do SAML or LDAP authentication with customer directories. Once we consume identity, we can apply policy based on that identity and device posture, and then log and report on access activity. Once we consume that information, we're able to apply per-user and per-device-based URL filtering, application segmentation, tenant restrictions, and provide adaptive access to private applications.

Zscaler integrates with multiple partners and we're specifically going to talk about our Identity Management framework and how we integrate with Active Directory, Azure Active Directory, ADFS, Okta, Ping, or really **any SAML 2.0-compliant identity provider**.

In the immediate sections that follow, we will talk about configuring SAML and SCIM for Zscaler Internet Access, and Zscaler Private Access in the power of the Zscaler platform to ensure that users get access to the right resources under the right conditions.

## SAML Authentication

SAML is a mechanism for federating identities between an identity store and applications. It provides a Single Sign-On (SSO) of users into services so that if a user is signed into the Identity Provider, they can access applications transparently without reauthentication. It also enables the exchange of credentials across a few key components.

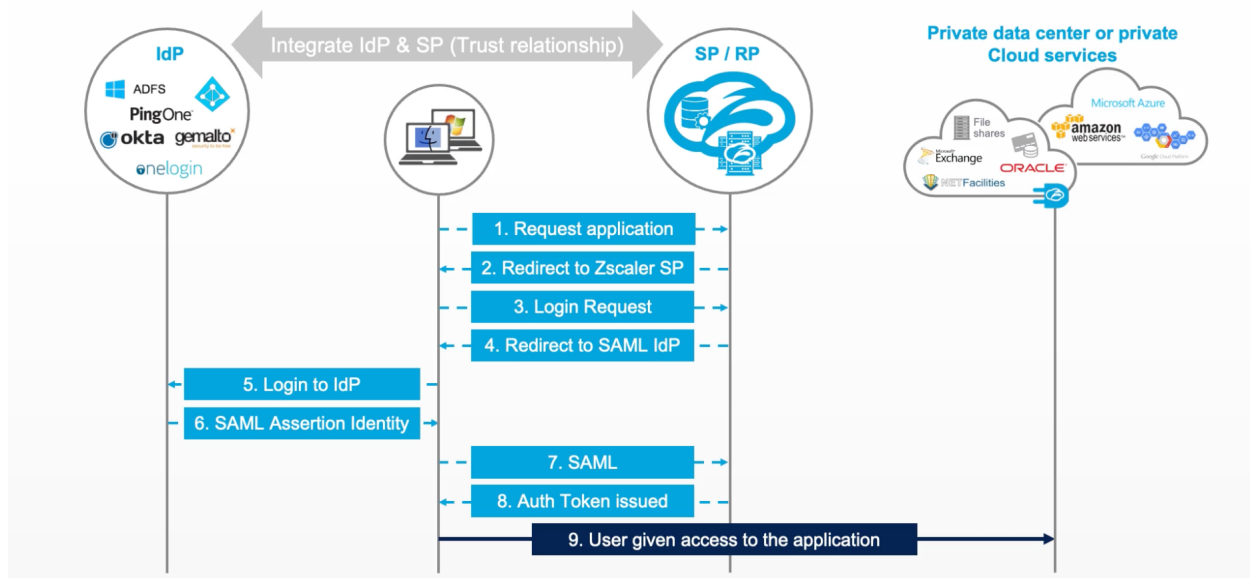
### Components

Service Provider (SP)	Identity Provider (IdP)	Security Assertions
<p>The "Application"</p> <p>Also known as the <b>Relying Party (RP)</b> to the Identity Provider (IdP)</p> <p>Employs the services of an IdP for the Authentication and Authorization of users</p> <p>Zscaler acts as a <b>SAML SP</b></p>	<p>Authenticates Users/Devices</p> <p>Provides <b>Identifiers</b> and <b>Identity Assertions</b> for users that wish to access a service.</p> <p>IdP examples include: Okta, Ping, AD FS, Azure AD</p>	<p>Also known as Tokens</p> <p>Issued to users by the IdP</p> <p>Presented to SPs / RPs to confirm authentication</p> <p>Trust based on PKI</p> <p>Assertions may contain: Authentication, Attribute, or Authorization statements</p>

How SAML authentication works.

We've got the identity provider (IdP) on the left, the users in the middle, and the service provider (SP) on the right is Zscaler. The applications the users will attempt to access on the right-hand side could be public applications like salesforce.com or internal applications that are made available through Zscaler Private Access.

## Authentication Flow: SAML



The first thing that happens is a request is made for an application. Since the user is not authenticated, at **steps 2 and 3**, they are redirected to authenticate at either Zscaler Internet Access or Zscaler Private Access.

Depending on whether the application is public or private, this request to authenticate will, in turn, lead to a SAML authentication request being sent to the SAML identity provider, which is **steps 4 and 5**.

A SAML authentication request is a message that indicates to the identity provider that a user must authenticate and that a SAML assertion should be returned to the SAML service provider. The identity provider must be configured to trust this particular service provider in order to honor the request and ultimately return a SAML assertion. At this point, the user would be challenged by the identity provider to authenticate. The authentication policy is controlled by the configuration at the IdP, so this could be a simple username and password. Maybe it's Kerberos, or it could be multifactor authentication.



Beyond just authenticating users, identity providers can perform additional actions, such as retrieving additional user attributes and group memberships. This data can be included in the SAML assertion.

The final thing the identity provider does is assemble the SAML assertion and cryptographically secure it using a digital signature. The SAML assertion will be delivered to the service provider via the user's browser. This is delivered using a form POST that is automatically submitted via JavaScript, so the experience to the end user is the same as an HTTP redirect. This is shown here in **steps 6 and 7**.

When Zscaler receives the SAML assertion, it validates the digital signature to ensure it came from a trusted source and that the data wasn't tampered with in transit. Assuming it's cryptographically verified, Zscaler issues an authentication token here at **step 8** to the Zscaler Client Connector or a cookie to the user's browser, depending on what client type is being used.

At this point, the user is authenticated at Zscaler, and the request for the application can resume via the Zscaler Zero Trust Exchange in **step 9**.

## SCIM Authorization

Now that you have an understanding of SAML authentication and its workflow, let's take a look at the next identity integration, SCIM, which works to provide authorization and revoke access for disabled users.

### What is SCIM?

The system for cross-domain identity management (SCIM) is the standard for automating the exchange of user identity information between identity domains and provides automatically-driven updates to user attributes on changes in the home directory. It supports the addition, deletion, and updating of users as well as the ability to apply policy based on SCIM user or group attributes.

#### Resource Model

A standard schema is in place for defining resources (e.g. **users, groups**)

Complex resource types are supported (e.g. with **attributes, sub-attributes, multivalued attributes**)

Resources are encoded as SCIM objects in JSON

*It is Zscaler's best practice to utilize SCIM provisioning whenever possible.*

#### REST API - Operations

The following operations can be conducted:

**Create:** Add a resource (e.g. user, group)

**Read:** Get information about a resource

**Update:** Update the attributes of a resource

**Delete:** Remove a resource

**SSO:** Trigger create/update to a third party

**Replace:** Change a resource

**Search:** Find a resource

**Bulk:** Operations on multiple resources

With a group-based policy, it is likely more reliable to leverage SCIM criteria, whereas if you want to apply policy based on the user's accessing device, is it trusted or untrusted, then that would require using a SAML attribute as criteria. Given the SAML assertion is generated as users are authenticating, it's possible to include additional contextual information related to the authentication transaction.

## Advantages and disadvantages of SCIM

Advantages	Disadvantages
<p><b>Updates information automatically:</b> SCIM Information (such as group changes) is updated via the API in real time, whereas SAML Auto-Provisioning is static and requires the users to first log out and then log back in for Zscaler to detect changes.</p> <p><b>Allows users to be deleted:</b> While Auto-Provisioning can add user information, it cannot delete users from the database, but SCIM can.</p> <p>For example, if revoking access or a user gets deleted or disabled in your directory, you can use SCIM to push that request to Zscaler where we will:</p> <ol style="list-style-type: none"><li>1. Consume that information</li><li>2. Automatically disable that user</li><li>3. Revoke access through the platform</li></ol>	<p><b>Not supported by all IdPs:</b> The only drawback of SCIM is that it is NOT supported by all IdPs with Zscaler. On the other hand, Auto-Provisioning is supported by all IdPs.</p>

### SAML Attributes

- SAML attributes are static
- Only applied on authentication
- Only changed on reauthentication
- Can include device and authentication attributes

### SCIM Attributes

- SCIM attributes are dynamic
- User- and group-specific
- They will be updated after a change in the source directory
- Frequency is IdP controlled

### Both SAML and SCIM Attributes

- The best of both worlds

The screenshot shows the 'Edit IdP Configuration' window. It features several configuration options for SAML and SCIM. The SAML section includes 'Status' (Enabled), 'ZPA (SP) SAML Request' (Signed), 'HTTP-Redirect' (Disabled), and 'SAML Attributes for Policy' (Enabled). The SCIM section includes 'SCIM Sync' (Enabled), 'SCIM Attributes for Policy' (Enabled), and a 'SCIM Service Provider Endpoint' field containing the URL 'https://scim1.private.zscaler.com/scim/1/144123139134063153/v2'. There is also a 'Bearer Token' section with a message 'A token already exists for SCIM syncing.' and a 'Generate New Token' button. At the bottom, there are 'Save' and 'Cancel' buttons.

Whether you base policy on SAML or SCIM attributes is dependent on your use cases.

## Operations Supported

**Add Users:** As they are assigned to the ZPA SP in the source IDP

**Delete Users:** Remove ZPA access for users that are either removed from the ZPA SP in the source IdP, or are removed from the directory completely.

**Update Users:** Update SCIM attributes dynamically (e.g. group memberships)

**Apply Policy:** Based on SCIM user or group attributes.

### SCIM Data Management

With SCIM enabled, read-only lists are created in ZPA for:

- SCIM users
- SCIM groups
- SCIM attributes

Users can only be managed in the source directory/IdP

Users, groups, and attributes are updated from the source directory as changes are made.

### SCIM Synchronization

Synchronization happens periodically using the API

- Update interval of ~40 minutes
- Manually triggered at any time

Updates are queued for sync from the IdP when:

- Users are added/removed to/from a group mapped to the ZPA SP
- Users are individually assigned to or removed from the ZPA SP
- Users are removed from the source directory entirely.
- User attributes are changed in the source directory.

## Basic Connectivity

This chapter will explain the different mechanisms to connect to the Zero Trust Exchange, depending on use cases and locations, emphasizing on best practices.

---

By the end of this chapter, you will be able to:

1. **Identify** how zero trust components are established in the cloud.
2. **Recognize** the connectivity services Zscaler has in place to securely connect users and applications to the Zero Trust Exchange.
3. **Discover** how to configure Zscaler connectivity control services and capabilities.

## Connecting to the Zero Trust Exchange (ZTE)

Zero trust components are **established in the cloud**, and **users/devices**, IoT / OT devices, or workloads must establish a connection to this cloud so security controls can be enforced.

Zero trust connections are, by definition, **independent of any network for control or trust**. Zero trust ensures access is granted by never sharing the network between the originator (user/device, IoT / OT device, or workload) and the destination application.

By keeping these separate, zero trust can be properly implemented and enforced over any network. The network can be located anywhere, or it could be built on IPv6, as the network is simply the means of connecting **initiators** to **destination apps**.

Throughout this chapter, we will dive deeper into the connectivity services outlined in the image above including:

Zscaler Client Connector	App Connectors	Browser Access & Privileged Remote Access
Included as part of Zscaler Internet Access (ZIA), Zscaler Private Access (ZPA), and Zscaler Digital Experience (ZDX), Zscaler Client Connector is a <b>lightweight app that sits on users' endpoints and enforces security policies and access controls regardless of device, location, or application.</b>	App connectors provide the secure authenticated interface between a customer's servers and the ZPA cloud.  They establish connections through the Firewall to the Zscaler cloud and the Zscaler cloud facilitates that connection as a reverse connection in order to enable users to access applications.	Browser-based access provides connectivity through a web browser without the Zscaler Client Connector being installed to HTTP and HTTPS applications.  This core connectivity capability also provides access to privileged remote access applications such as SSH or RDP.

## Zscaler Client Connector

### Zscaler Client Connector

Included as part of Zscaler Internet Access (ZIA), Zscaler Private Access (ZPA), and Zscaler Digital Experience (ZDX), Zscaler Client Connector is a **lightweight app that sits on users' endpoints and enforces security policies and access controls regardless of device, location, or application.**

The Zscaler Client Connector is installed on the endpoint to create a tunnel to the Zero Trust Exchange for the protection of SaaS and internet-bound traffic.

This same Client Connector also provides a persistent control plane and dynamic, micro-segmented data plane tunnels to the ZTE for the purpose of internal app protection, and traffic is delivered to the application via a corresponding outbound-only data plane tunnel from the Zscaler App Connector.

The screenshot displays the Zscaler Client Connector interface. At the top, the Zscaler logo and a 'Log Out' button are visible. The interface is divided into a left sidebar with navigation icons for Private Access, Internet Security, Digital Experience, Notifications, and More. The main content area is split into two sections: 'Connectivity' and 'Statistics'. The 'Connectivity' section shows a table with the following data:

Connectivity	
Username	mryan@welshgeek.net
Service Status	ON <a href="#">TURN OFF</a>
Network Type	Trusted Network
Authentication Status	Authenticated
Broker	192.168.1.78
Client	imac.welshgeek.net
Time Connected	10/18/2022 03:06:48 pm
Tunnel Protocol	TLS

The 'Statistics' section shows a table with the following data:

Statistics	
Total Bytes Sent	21.08 KB
Total Bytes Received	9.48 KB

### Features include:

- Consistent Experience on all Platforms
- Strict Enforcement Options (Tamper Proof)
- Simple Enrollment
- Trusted Network Detection
- User Attribution and Asset Identification
- Transparent Authentication for Users
- Install Zscaler or Custom SSL Inspection Certificate

## Authenticated Tunnels

There are a number of different modes for Zscaler Client Connector to function when it's forwarding traffic to Zscaler Internet Access. **The recommended mechanism is to use the Zscaler tunnel.** The tunnel-based approach intercepts traffic at the network level and forwards that traffic through an encapsulated tunnel to the Zscaler platform.

**There are three authenticated tunnel options** (meaning that once the user is enrolled in Zscaler Client Connector, the tunnel is established toward the Zscaler cloud and all traffic that goes into the tunnel is identified as that user and that user-based policy is applied):

ZTunnel - Packet Filter Based	ZTunnel - Route-Based	ZTunnel with Local Proxy
<p><b>Creates Packet Filters (Windows Only)</b></p> <p>The packet filter based on Windows instruments, packet filters that grab traffic, steer the traffic toward the Zscaler Client Connector process that can then make a decision to forward it to the Zscaler cloud.</p>	<p><b>Creates Route Table Entries</b></p> <p>Route-based mode also works in instruments and additional network adapter, which becomes the route for traffic, route-based mode instruments, and additional network adapter, which becomes the route for traffic generated from client applications.</p>	<p><b>Deploys System Proxy to Localhost</b></p> <p>Tunnel with local proxy creates a loopback address that appears as a HTTP, HTTPS proxy, and then instructs the operating system's proxy setting to point the browser at that local proxy. It's then tunneling the traffic toward the Zscaler cloud.</p>

Additional options that support legacy implementations are:

**Enforced PAC** mode, which basically instruments the PAC file in the browser, similar to what you'd get from a group policy object. That means that the browser itself is forced to go to Zscaler Internet Access via a specified proxy.

**None**, meaning that the policy is not going to do any configuration of proxy or tunneling mode, and relies on the group policy object or the default configuration within the browser.



## ZTunnel 1.0 vs. 2.0

Tunnel modes come in two formats, the Legacy Z-Tunnel 1.0 and the modern ZTunnel 2.0:

ZTunnel 1.0	ZTunnel 2.0
<p>The Legacy Z-Tunnel 1.0 is an HTTP <b>CONNECT</b> tunnel. So as traffic is forwarded into the tunnel, it creates a CONNECT method toward the cloud. It doesn't really encapsulate the traffic. It simply adds some header information, which enables the Zero Trust Exchange to understand the user information and the data that's being passed to it.</p> <p>With ZTunnel 1.0, there are essentially two tunnels: a tunnel towards the Zero Trust Exchange for the authentication, enrollment and passing traffic, and another for the policy updates that would occur every 60 minutes against the Zscaler Client Connector Portal where all those configuration changes are made.</p> <p>80 / 443 Proxy Aware Traffic Only</p> <p>No Real Encapsulation of Traffic</p> <p>No Control Channel</p> <p>Limited Log Visibility</p> <p>No Visibility Into Non-Web Traffic</p> <p>Configurable drop of Non-Web Traffic</p>	<p>The more advanced Z-Tunnel 2.0 is a <b>DTLS</b> (Datagram Transport Layer Security) tunnel with fallback to TLS (Transport Layer Security) supporting all client traffic, which means the Zscaler Firewall, as part of the Zero Trust Exchange, could inspect and apply policy on all traffic.</p> <p>With Z-Tunnel 2.0, <b>which is the best practice option</b>, the tunnel is the control channel and a single tunnel from the client to the Zero Trust Exchange. <b>Any notifications from the Client Connector admin portal (aka. "Mobile Admin") are passed through the Zero Trust Exchange directly to the client, and those happen in real time.</b></p> <p>Any TCP, UDP, and ICMP Traffic</p> <p>DTLS runs on UDP = Faster Transport <i>If the client detects that the DTLS tunnel wasn't successful, such as a firewall blocking UDP traffic, we want to fall back to a TLS-TCP connection.</i></p> <p>DTLS uses a TLS tunnel = Integrity</p> <p>Tunnel Provides Control Channel = updates to client (policy changes), available updates, connectivity information, and logging/alerting towards the client.</p> <p>Logging of Client Connector Version, ZTunnel version...</p>

Tunnel Failure: There are also connection timeout options and additional options for redirecting traffic to a local listener ( tunnel with local proxy, providing safe fallback within the client if the tunnel mode connection is not successful.

## Forwarding Profile: Trusted Network Detection

Within the client, there is trusted network detection, which can make a decision if a user is in the office, branch, data center, or similar locations based on certain criteria.

**Add Trusted Network** [X]

NETWORK DEFINITION

Network Name [?]   
 Mandatory

TRUSTED NETWORK CRITERIA

Add Condition [?]   
 Select [v] [Add Condition]

- DNS Server
- DNS Search Domains
- Hostname and IP

**TRUSTED NETWORK CRITERIA**

Add Condition [?]   
 Select [v] [Add Condition]

- Hostname and IP
- Pre-defined Trusted Networks

DNS Servers [?]   
 192.168.1.1 [X]

DNS Search Domains [?]   
 localdomain [X]

Hostname and IP	DNS Search Domains	DNS Server
Does a specific FQDN resolve to an IP address? If those two match, then the condition is true.	The DNS search domain, provided by DHCP, where the client will receive a DNS search domain. If those things match the configuration of the trusted network criteria, the user is on the matching network.	The DNS server looks at the primary network adapter on the client and understands what DNS server is being provided to it through DHCP. If those things are equal, then the DNS server condition is true.

Combining these we can say whether they've all got to be true to identify the user or the device as being on a trusted network, and that trusted network (any number of different locations) can then be a condition to make a decision on how the different forwarding mechanisms are going to be used at that location.

## Forwarding Profile: Multiple Trusted Networks

Now we just need to define each of our **multiple Trusted Networks** so that we can then make the decision as to which forwarding profile matches our desired outcome.

The screenshot shows the Zscaler configuration interface. On the left, the 'Profile Definition' section has a 'Profile Name' field containing 'Mandatory'. Below it, the 'Trusted Network Criteria' section has an 'Add Condition' dropdown menu open, showing options: 'DNS Server', 'DNS Search Domains', 'Host Name and IP', and 'Pre-defined Trusted Networks'. A hand cursor is pointing at 'Pre-defined Trusted Networks'. To the right, another 'Add Condition' dropdown is set to 'Pre-defined Trusted Networks' with an 'Add Condition' button. Below that, a 'Trusted Networks' dropdown is set to 'ALL'. At the bottom right, a selection interface shows 'Unselected Items' (America Center, Sydney Office, Mumbai Office) and '1 Items Selected' (San Jose HQ). A 'Done' button is at the bottom.

**Note:** Forwarding profiles can reference multiple trusted networks.

The screenshot shows the Zscaler Administration console. The top navigation bar includes 'zscaler', 'Dashboard', 'Enrolled Devices', 'App Profiles', and 'Administration'. The left sidebar shows 'Settings' with 'Trusted Networks' selected. The main content area is titled 'Add Trusted Network' and contains a table with the following data:

#	Network Name	Trusted Network Criteria
1	DataCenter	DNS SERVERS 192.168.1.2  DNS SEARCH DOMAINS welshgeek.net  HOSTNAME AND RESOLVED IP router.welshgeek.net:192.168.1.254
2	Branch	DNS SERVERS 10.1.1.250,10.1.1.251  DNS SEARCH DOMAINS welshgeek.net  HOSTNAME AND RESOLVED IP wifi.branch.welshgeek.net:10.1.10.1

## Forwarding Profile: Profile Action for ZIA

Finally, within the forwarding profile, we can select a trusted network criteria and then select from your predefined list of **multiple trusted networks**, confirming which ones are going to apply to the forwarding profile.

This means that for a device on a trusted network, we can make a decision whether to tunnel the traffic, use a tunnel with a local proxy, enforce the proxy, or do 'none'.

While we are here, let's look at and revisit some of the best practices.

The best practice is to use tunnel mode and specifically to use the ZTunnel 2.0, which captures all traffic within the client and tunnels it to Zscaler within a DTLS tunnel. With the ZTunnel 2.0 configuration, default to DTLS, with the ability to fall back to TLS as necessary.

Edit Forwarding Profile

FORWARDING PROFILE ACTION FOR ZIA

On Trusted Network

Tunnel  Tunnel with Local Proxy  Enforce Proxy  None

Tunnel Version Selection  v. 2.0.0+  v. 2.0.0+

Z-Tunnel 1.0  Z-Tunnel 2.0

Advanced Z-Tunnel 2.0 Configuration

Z-Tunnel 2.0 Transport Settings

Primary Transport Selection

DTLS  TLS

DTLS Connection Timeout (In Seconds)

9

TLS Connection Timeout (In Seconds)

5

MTU for Zscaler Adapter  v. 2.1.2+  v. 2.1.2+

Optional

Allow Fallback

TLS

Z-Tunnel 2.0 Setup Failure Behavior  v. 3.4.0+  v. 3.4.0+

Fallback to Z-Tunnel 1.0 and bypass non-web tra...

Redirect Web Traffic to Zscaler Client Connector Listening Proxy

v. 3.8.0+

Use Z-Tunnel 2.0 for Proxied Web Traffic

v. 3.8.0+

## Forwarding Profile: System Proxy Settings

Within the system proxy settings, you can control how the browser, or more specifically the operating system, receives proxy settings.

If you're migrating from an on-premises proxy, you will already have a proxy setting set within the browser or within the system. With a tunnel mode, there is no need to have these proxy settings. So the recommendation is to enforce a no-proxy configuration.

### Enforcing Proxy Action Type:

Configure System Proxy Settings

System Proxy Settings

Proxy Action Type

Enforce    Apply on Network Change    Never

Automatically Detect Settings

Use Automatic Configuration Script

Use Proxy Server for Your LAN

Execute GPO Update

VPN Trusted Network

Same as "On Trusted Network"

Tunnel    Tunnel with Local Proxy    Enforce Proxy    None

Off Trusted Network

Same as "On Trusted Network"

Tunnel    Tunnel with Local Proxy    Enforce Proxy    None

Automatically Detect Settings	Use Automatic Configuration Script	Use Proxy Server for Your LAN	Execute GPO Update
The client sends a WPAD (Web Proxy Auto-Discovery) lookup looking for a proxy.	Explicitly configure where the Zscaler Client Connector sets your custom system PAC file to download and run through that PAC file configuration for traffic to be explicitly proxied to a proxy server.  Also referred to as a <b>forwarding PAC file</b> .	This is a hard-coded proxy import (IP address and a port or an FQDN and a port) with the ability to bypass local addresses. A local address is something that is non-fully qualified.	The Windows machine will provide a GPO (Group Policy Object) update/force from Active Directory to set the proxy settings on the machine.

It's important to understand the behavior of GPO updates, forcing Zscaler Client Connector to set a proxy setting, or forcing Zscaler Client Connector to set a WPAD script, making sure that there is no conflict between these.

You can then make decisions on whether to use exactly the same settings for the untrusted network, for the VPN Trusted Network, and off-trusted network criteria.

Summary: It's really important to understand the distinction between a forwarding PAC and how the forwarding PAC is implemented within Zscaler Client Connector. With a tunnel mode configuration, we do not want to set any forwarding PAC file and have the client intercept the traffic natively as the browser or the client configuration resolves an internet address and intercepts the traffic as it routes toward the internet and tunnels it toward the Zero Trust Exchange through the DTLS tunnels.

## Application Profile

An application profile exists to map the forwarding profiles to different users and different devices based on certain criteria.

You need to configure a specific application profile for your Windows, Mac, iOS, Android, and Linux devices. We'll specifically focus on Windows and Mac devices.

The app profile selects the forwarding profile, which therefore defines the method of tunneling. So, the forwarding profile defines it as Z-Tunnel 2.0, and so we map that to the application profile to forward traffic through the tunnel. This defines the on- and off-trusted network configuration and defines the system proxy is not configured. The app profile PAC URL defines the Zero Trust Exchange node to be used based on the client's geographic IP information.

The most common configuration items here include:

<b>Custom PAC URL</b>	References the PAC file configured in the ZIA Admin Portal, making decisions on traffic that should be forwarded or bypassed from the Zero Trust Exchange.
<b>Override WPAD</b>	Ensures that the system GPO WPAD configuration is prevented, and makes sure that the WPAD configuration in the forwarding profile is used as a precedence.
<b>Restart WinHTTP</b> specific to Windows devices	Ensures that the system refreshes all of the proxy configuration once Zscaler Client Connector is established.
<b>Install Zscaler SSL Certificate</b>	Covered more in the next section. If you aren't pushing out your own certificates from your own Certificate Authority, then simply enabling this option will use the one provided by Zscaler.

**Tunnel Internal Client Connector Traffic**

Ensures that the health updates and policy traffic passes through the Zscaler tunnels towards the Zero Trust Exchange. Or more specifically, it doesn't go direct to the Zero Trust Exchange – it stays within the zero trust tunnels.

**Cache System Proxy**

Ensures that Zscaler Client Connector stores the system proxy state from before it was installed or enabled, and makes sure that when Zscaler Client Connector is uninstalled or disabled, a system proxy configuration is reverted and the user can continue to function as before. And that the Zscaler Client Connector reverts to previous versions of the Zscaler Client Connector software in the event of an upgrade issue.

These last two are about supportability in the case where the client needs to uninstall or revert a previous version, and making sure that they have business continuity in the case of any issue with the updates.



## Deploying Zscaler SSL Inspection Certificates

A critical part of the Zero Trust Exchange is the ability to inspect SSL, and it's important that the client trusts the SSL certificates that are being used for SSL inspection.

Zscaler Client Connector has the ability to deploy the **Zscaler root CA** as well as **custom root CAs** that might be being used within an organization.

The configuration options to upload the root CA from a custom CA to make sure that's deployed is controlled here, as well as the ability within the app profile, as previously mentioned, to control ensuring that the SSL certificate is installed.

The image shows two screenshots of the Zscaler Client Connector configuration interface. The top screenshot is titled "Add Windows Policy" and has a blue header with a close button. It is divided into two sections: "DEFINE POLICY AND SCOPE" and "GENERAL". In the "GENERAL" section, there is a checkbox labeled "Install Zscaler SSL Certificate" which is checked, and a "Log Mode" dropdown menu set to "Debug". The bottom screenshot is titled "ADVANCED CONFIGURATION" and has a grey header. It contains a "DIRECTORY SYNC STATUS" section with a "Next Directory Group Sync Time" of "Thu May 26 2022 11:44:41 GMT-0700 (Pacific...)" and a "Sync Directory Groups Manually" button labeled "Sync Groups". Below this is a "CUSTOM ROOT CERTIFICATE" section with a "Custom Certificate" field that is currently "Not Available" and an "Upload" button.

### 1 Client Connector Install

## Tunnel 2.0 Configuration

When we look at the Z-Tunnel 2.0 configuration, there are a number of options that we need to consider.

There are some specific application bypasses for things like UCaaS. If we want to bypass Microsoft Teams or Zoom traffic from going into the tunnel, we can do that by selecting them under the **application bypass**.

It's important that we make **exclusions and inclusions** for traffic that we want to grab at the adapter level and pass into the Z-Tunnel 2.0. The default excludes the RFC 1918 address space and includes the default 0.0.0.0/0 address range and all ports 1 to 65,535 TCP and UDP. You could configure bypasses and change this if you specifically want to bypass a port from going into the tunnel, an IP address going into the tunnel, or you can ensure that everything goes into the tunnel.

Z-TUNNEL 2.0 CONFIGURATION RESTORE TO DEFAULT

Application Bypass None Selected

Destination Exclusions v. 2.0.0+

Use Enter to Add Multiple Items +

10.0.0.0/8	x
172.16.0.0/12	x
192.168.0.0/16	x
224.0.0.0/4	x

Destination Inclusions v. 2.0.0+

Use Enter to Add Multiple Items

0.0.0.0/0

Enter the DNS domains that Zscaler Client Connector should tunnel through ZIA. You can enter \* to include all, or enter specific domains, such as zscaler.com. For more information, see [Configuring Zscaler Client Connector Profile](#). The maximum number of characters allowed is 65535. Domain inclusions and exclusions take effect only if the DNS server IP address on the client belongs to RFC1918 private subnet ranges that are by default excluded from tunnel2.0

Domain Inclusions for DNS Requests v. 3.2.0+

Use Enter to Add Multiple Items +

Domain Exclusions for DNS Requests v. 3.2.0+

Use Enter to Add Multiple Items +

Zscaler also provides the ability for **inclusions and exclusions of DNS requests**. Zscaler is a DNS resolver, but it's important to understand that the client is going to get a DNS server from its DHCP. If the client gets a DNS server from DHCP that is within the RFC 1918 address range, the client may query that directly, and it's only once the connection comes through Zscaler that we'll be able to see the traffic and make a DNS re-resolution request.

DNS requests are tunneled to the Zscaler cloud, and the Zscaler cloud performs the DNS resolution. **It's not necessary to configure Zscaler as the DNS server** since this configuration intercepts any DNS request to any DNS server and redirects it or tunnels it to the Zscaler cloud for the Zero Trust Exchange to perform the DNS resolution.

## Forwarding Profile PAC vs App Profile PAC

Let's explain the difference between a Forwarding PAC and an App PAC in more detail.

Forwarding Profile PAC	App Profile PAC
<p>Steers traffic <b>toward or away</b> from the <b>Client Connector</b></p> <p>Controls System PAC file - which HTTP Proxy to be used for a URL, tunnel with local proxy or other explicit proxy.</p> <p>Has no bearing where Client Connector will route traffic, only where the user's apps will send traffic.</p>	<p>Steers traffic <b>toward or away</b> from the <b>Zscaler Cloud</b></p> <p>Routes traffic <b>AFTER the Client Connector</b> has received it.</p> <p>Used to determine the geographically closest Zscaler Enforcement Node (ZEN).</p>
<p>A <b>Forwarding Profile PAC</b> gets defined within the forwarding profile and it steers traffic toward or away from Zscaler Client Connector. It's essentially the system PAC file, stating which HTTP proxy is going to be used for a specific URL.</p> <p>If it's the PAC file for a Tunnel with Local Proxy, it's going to point traffic at the loopback address or another explicit proxy. It has no bearing on where Zscaler Client Connector will route traffic, only where the user's applications will send traffic. So a user's application could be the Internet Explorer browser, Edge browser, Chrome browser, Firefox. They would receive the Forwarding Profile PAC that makes the decision how that browser will treat the HTTP traffic and what proxy server it will send it to.</p> <p>And that proxy server could be Zscaler, or that proxy server could be the local proxy that's enabled in Zscaler Client Connector.</p>	<p>The <b>Application Profile PAC</b> steers traffic towards or away from the Zscaler cloud – after traffic has been intercepted by the tunnel mode or after traffic has been directed to it with the local proxy.</p> <p>The Application Profile PAC then processes the traffic and makes a decision which Zscaler node (ZIA Public or Private Service Edge, or ZPA Public or Private Service Edge) is going to process the request afterwards.</p> <p>Finally, that App Profile PAC is then used to determine the geographically closest Zscaler enforcement node to process it.</p>

## ZIA: PAC Files

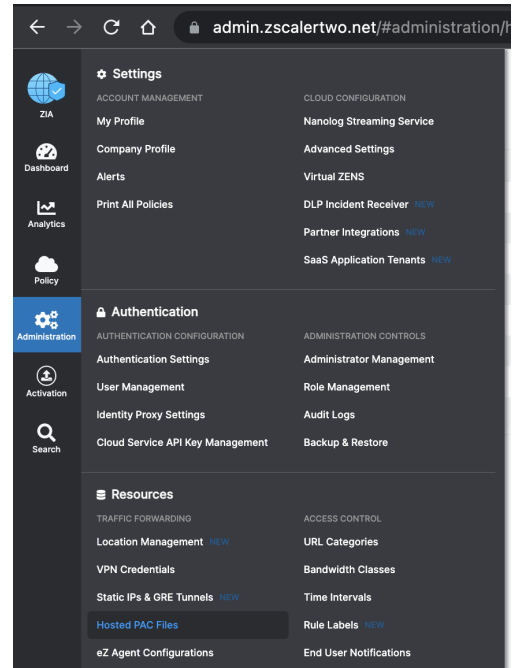
Within the Zscaler Internet Access (ZIA) Admin Portal, we can define the PAC files that are hosted on the cloud. PAC files are essentially JavaScript functions that take two inputs that are dynamically provided to it by the browser, or in the case of the App Profile PAC, through the inspection process.

It takes the input of a URL and a host, and it returns back an answer of sending the traffic “DIRECT” or “PROXY”.

As previously discussed, The Forwarding PAC is processed by the web browser or the system proxy, while the Application Profile PAC is for Zscaler Client Connector to make its traffic routing decisions.

### Migration:

If you're migrating from an on-premises proxy to the Zscaler Internet Access platform, existing PAC files may be migrated to Zscaler. Here you would migrate to Zscaler using Tunnel with Local Proxy, and you might bring in that browser configuration. It remains the same. The PAC file simply returns to Zscaler Client Connector as a proxy, and Zscaler Client Connector tunnels that traffic to the Zero Trust Exchange. And because it's an authenticated tunnel, the Zscaler Zero Trust Exchange understands who the user is.



No.	Description	Domain	Hosted URL	Status	
1	App	welshgeek.net	http://pac.zscalertwo.net/welshgeek.net/app.pac	Verified	
2	Kerberos	welshgeek.net	http://pac.zscalertwo.net/welshgeek.net/kerberos.pac	Verified	
3	Recommended PAC	zscalertwo.net	http://pac.zscalertwo.net/zscalertwo.net/recommended.pac	---	
4	Service Default.	zscalertwo.net	http://pac.zscalertwo.net/zscalertwo.net/proxy.pac	---	
5	Service Default.	zscalertwo.net	http://pac.zscalertwo.net/zscalertwo.net/mobile_proxy.pac	---	
6	Service Default.	zscalertwo.net	http://pac.zscalertwo.net/zscalertwo.net/kerberos.pac	---	
7	Welshgeek Default	welshgeek.net	http://pac.zscalertwo.net/welshgeek.net/proxy.pac	Verified	

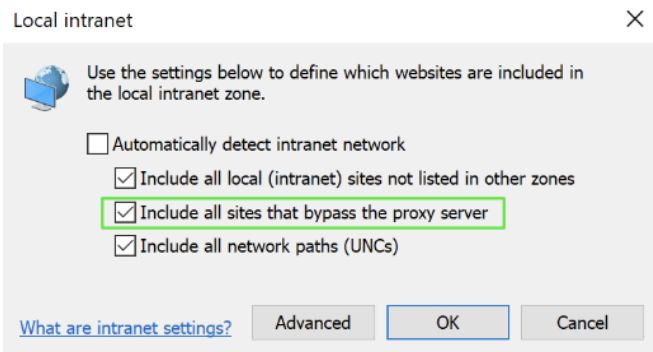
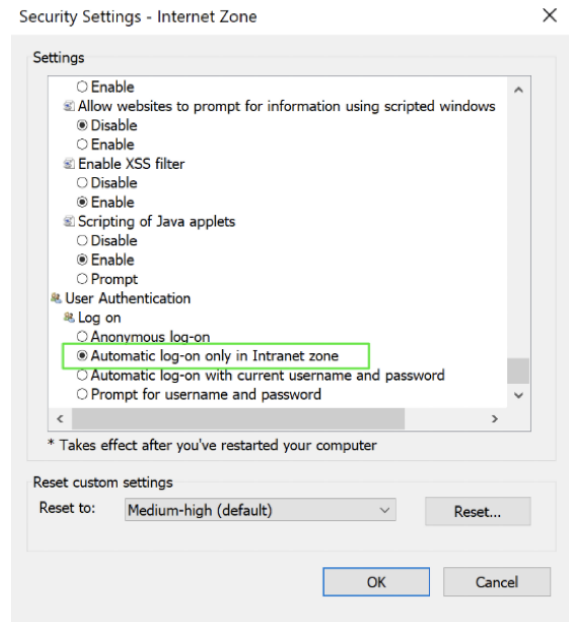
As a migration step, it's a very simple process to take your existing PAC file and move it into the Zscaler Client Connector. However, the recommendation is to use the Z-Tunnel 2.0 forwarding mechanism, and you need to take into consideration how to move from an existing explicit proxy configuration to moving to Zscaler tunnel mode.

## ZIA: Browser Behavior - PAC to Tunnel Mode

As you move from PAC mode to a tunnel mode, or explicit proxy mode to a tunnel mode, there are implications on the way your browser will behave.

### Site Authentication

The browser will automatically understand how it authenticates to intranet sites, so it'll do Kerberos, NTLM (New Technology LAN Manager), and Integrated Windows Authentication (IWA) to websites, which are automatically defined as being in the intranet zone. And the intranet zone is defined as sites which bypass the proxy, so a site which has a direct statement in the PAC file is automatically identified as being an intranet site. Therefore if it challenges for authentication, the user will automatically authenticate, or the browser will automatically authenticate, and the user will be signed in. So if you remove the PAC file configuration and move to tunnel mode, the definition within the browser of what is an intranet site is lost. This means the user may be prompted to authenticate to intranet sites, and it is often seen as a side effect of migrating from PAC file to tunnel mode.



As there is no PAC file in the browser with Tunnel Mode, you need to specifically define the intranet sites in the browser to ensure there's a congruent authentication behavior (single sign-on to intranet applications – because they're defined as intranet sites). In Internet Explorer, you would need to click the Advanced button and add those sites as intranet sites. You are taking that decision away from the browser saying there are

sites that bypass the proxy, and you are explicitly defining them within (1) the intranet zone and saying these sites are my intranet sites that I should then automatically authenticate to within Google, Chrome, Edge browsers, etc... via the (2) AuthServerAllowList. And within Firefox you would add things to the (3) auth.trusted-uris configuration option.

**All of these can be pushed out through group policy objects and identified from your existing PAC file, migrated into the browser configuration, and pushed out before the migration to Zscaler occurs.**

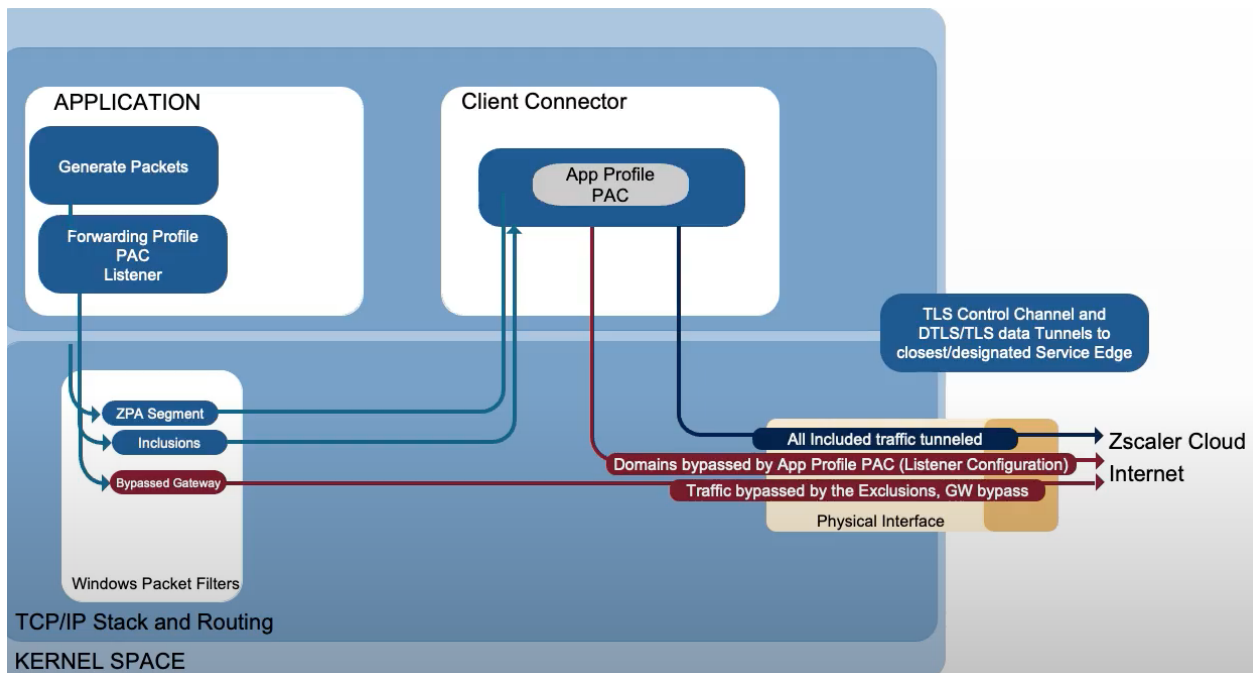
```
mryan@mac-2 ~ % defaults read com.google.chrome
{
  AuthNegotiateDelegateAllowlist = "*.welshgeek.net, autologon.microsoftazuread-ssoc.com";
  AuthNegotiateDelegateWhitelist = "*.welshgeek.net, autologon.microsoftazuread-ssoc.com";
  AuthServerAllowlist = "*.welshgeek.net, autologon.microsoftazuread-ssoc.com";
  AuthServerWhitelist = "*.welshgeek.net, autologon.microsoftazuread-ssoc.com";
  AutoSelectCertificateForUrls = (
    "{\pattern\": \"https://[*.welshgeek.net\", \"filter\": {\ISSUER\": {\CN\": \"WelshGeek-DC1-CA\"}}}}";
  );
  DNSInterceptionChecksEnabled = 0;
```

## Tunnel Mode - Packet Filter Based - ZTunnel 2.0

Now we need to look deeper into the tunnels.

The application is going to generate some traffic, and it may understand what a Forwarding PAC file is. It might look at Internet Explorer and bring in the PAC file. And so that PAC file decision says, should I send it to Zscaler Client Connector? It's also going to understand something that's a ZPA (Zscaler Private Access) segment, based on how it resolves.

The bottom line is that there are going to be exclusions and inclusions. Anything that's included will be sent through to Zscaler Client Connector, or Zscaler Client Connector will physically intercept traffic. Anything that is bypassed or bypassed through the packet filters will go directly out to the internet.

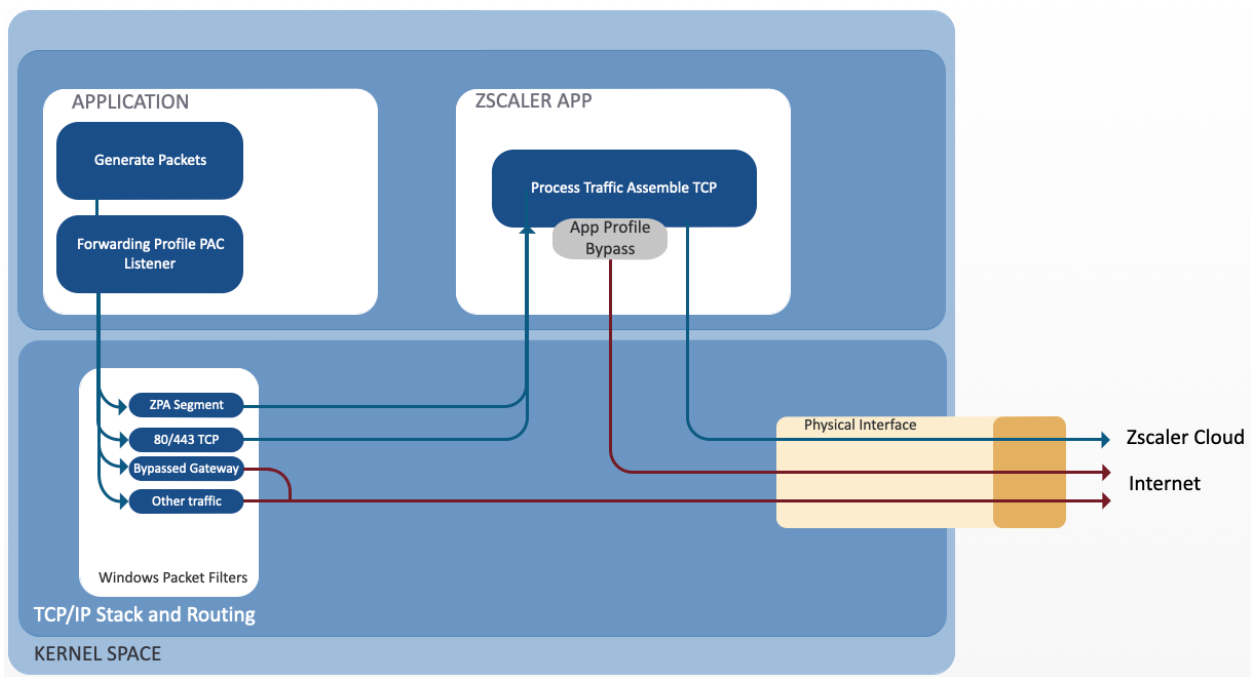


## Tunnel Mode - Packet Filter Based - ZTunnel 1.0

With Z-Tunnel 1.0, it's important to understand that traffic at a network layer will only intercept traffic that's 80 or 443. So if you've got, again, the application generating packets, if it's port 80 or 443, it'll be intercepted and passed to Zscaler Client Connector.

If it's explicitly proxy, do you have a proxy configuration tunnel with local proxy? It'll be passed to that local adapter that's listening, and again, into Zscaler Client Connector.

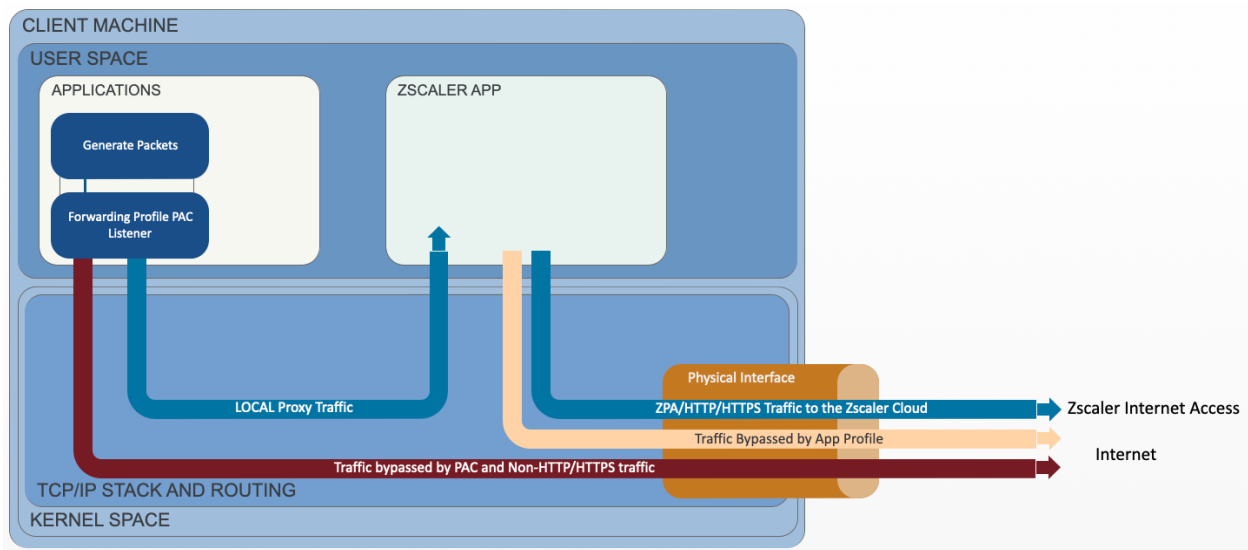
Or again, if it's a Zscaler Private Access segment, we'll intercept that and send the traffic to Zscaler Client Connector. Anything that is none of those, anything that is not a ZPA segment, or 80 and 443, will inherently bypass Zscaler Client Connector and then route directly out through the interface to the internet.



## Tunnel with Local Proxy Flow

With the Tunnel with Local proxy as the only configuration on there, you explicitly need the Forwarding Profile PAC to target traffic directly to the local listener on Zscaler Client Connector. This means the application needs to be proxy-aware. It needs to understand the configuration of what my Zscaler Client Connector proxy listener is, and it will then forward the traffic to that Zscaler Client Connector.

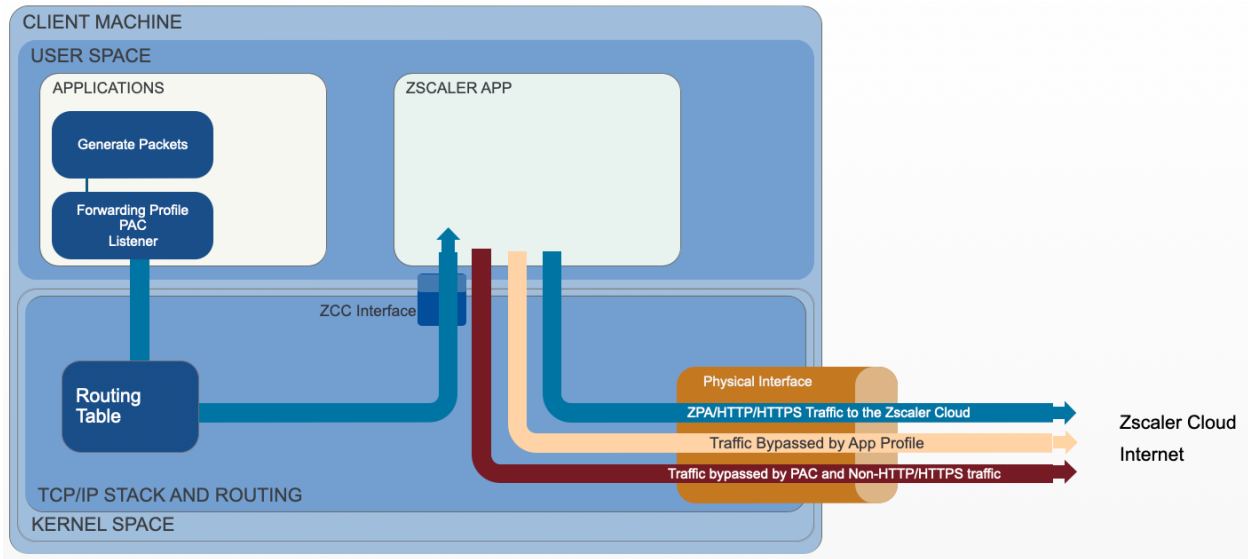
Zscaler Client Connector then passes traffic to Zscaler Internet Access. Any other traffic that's not ZPA will pass out directly to the internet.





## Tunnel Mode - Route-Based Flow

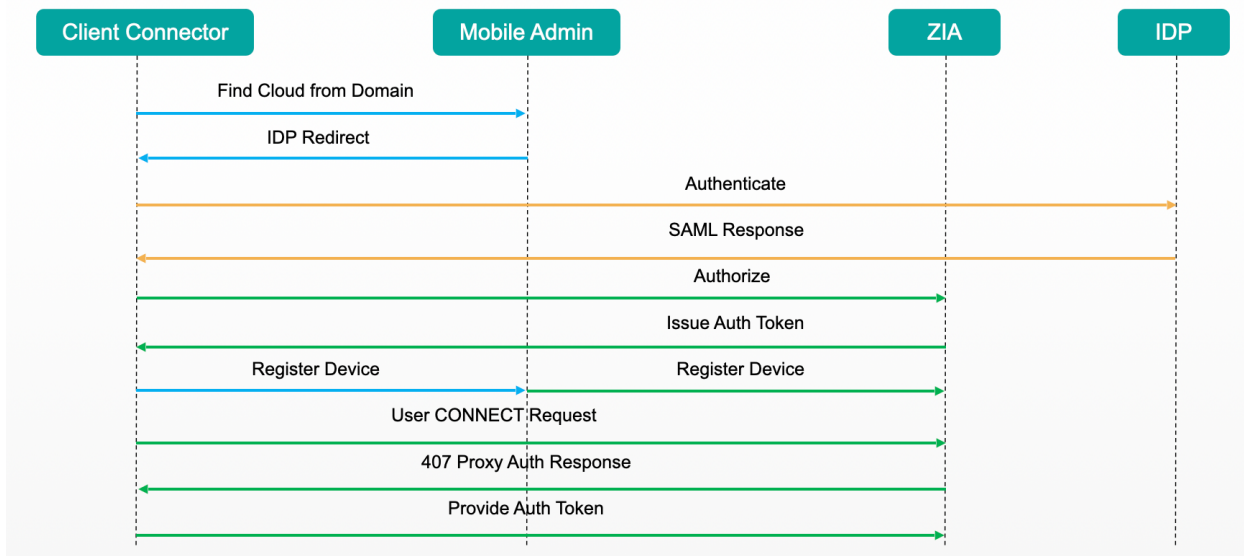
In the route-based mode, again, there is a routed adapter. There's an additional network adapter that's configured on the machine. And in a scenario where the Tunnel with Local Proxy is not configured, the application generates traffic, it follows the routing table, and that traffic routes into the Zscaler Client Connector IP address. The Application PAC processes the traffic, and again, traffic routes either to the Zscaler cloud or it bypasses and routes directly to the internet.



## ZIA Enrollment Process

When Zscaler Client Connector is launched, it needs to enroll, also needing to authenticate to be able to understand who the user is, what policy to apply, what tunnels to create, and how to identify the user through those tunnels.

### Client Connector ZIA Enrollment



As the Zscaler Client Connector launches, it's going to talk to the mobile admin portal (Zscaler Client Connector Portal) and understand what domain the user is in and what SAML identity provider the user should authenticate against.

The user receives that IdP redirect and they are redirected to their SAML IdP, such as Okta, ADFS (Active Directory Federation Service), Azure AD (Active Directory). The user will sign into the SAML IdP and receive a SAML response within the Zscaler Client Connector process. That SAML response is provided to Zscaler Internet Access, which consumes the response, validates it, and if the response is valid, then the user receives an authentication token back to Zscaler Client Connector.

Zscaler Client Connector provides that token to the Zscaler Client Connector Portal, which validates the token and registers the device. At this point, the Zscaler Client Connector Portal understands who the user is, fingerprints the device, consumes that device information, and passes that device registration through to Zscaler Internet Access.

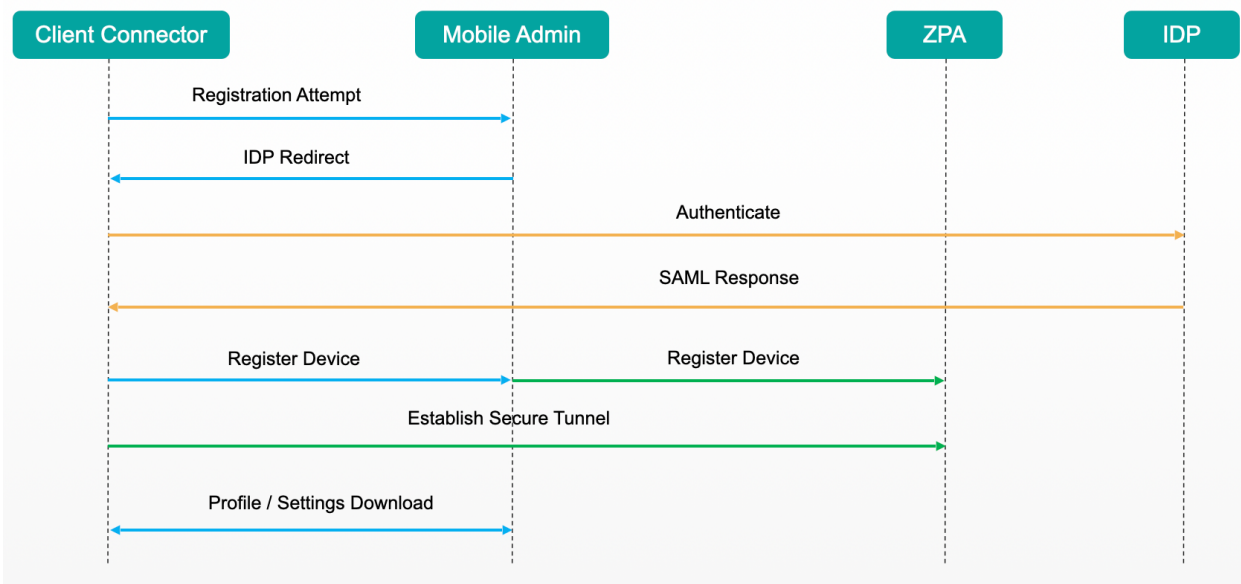
Zscaler Internet Access then provides the client credentials so that when the user makes a request through the Zscaler service, it can authenticate the user and it uses the Zscaler identity token to authenticate the client through the platform.

## ZPA Enrollment Process

With Zscaler Private Access, again, the client is launched as part of the authentication process.

It already understands the domain that the user is in from the Zscaler Internet Access enrollment, so there's an immediate registration attempt, followed by a second IdP redirect as Zscaler Internet Access and Zscaler Private Access are controlled as two separate SAML-reliant party trusts. During this second authentication round where the Zscaler Client Connector talks to the SAML IdP, it will sign in transparently because they're already signed in from the Zscaler Internet Access enrollment. There may be a multifactor authentication at this point, but the IdP authenticates the user and returns the SAML response back to Zscaler Client Connector.

### Client Connector ZPA Enrollment



Zscaler Client Connector provides that response token and registers the device into Zscaler Client Connector Portal, which passes that registration through to Zscaler Private Access, and Zscaler Private Access enrollment then enables the Zscaler Client Connector certificates to be generated and Zscaler Client Connector is enrolled in Zscaler Private Access.

Zscaler Client Connector then generates the secure tunnels to the Zero Trust Exchange, through which the profile and settings are downloaded so the client receives the information about the Zscaler Private Access applications that they're able to access.

## Client Connector Intervals

There are multiple intervals where Zscaler Client Connector will refresh the information it has about the applications, the app profiles, the forwarding profiles, the PAC files, and the policy.

### **On Network Change (connect/disconnect)**

Any time there is a network change, such as when the device comes out of hibernation and reconnects to Wi-Fi, I turn Wi-Fi on and off, or I restart the processes. There'll be a full refresh of all of those objects.

### **Every Two Hours**

Every two hours Zscaler Client Connector will check for software updates.

### **Every Hour**

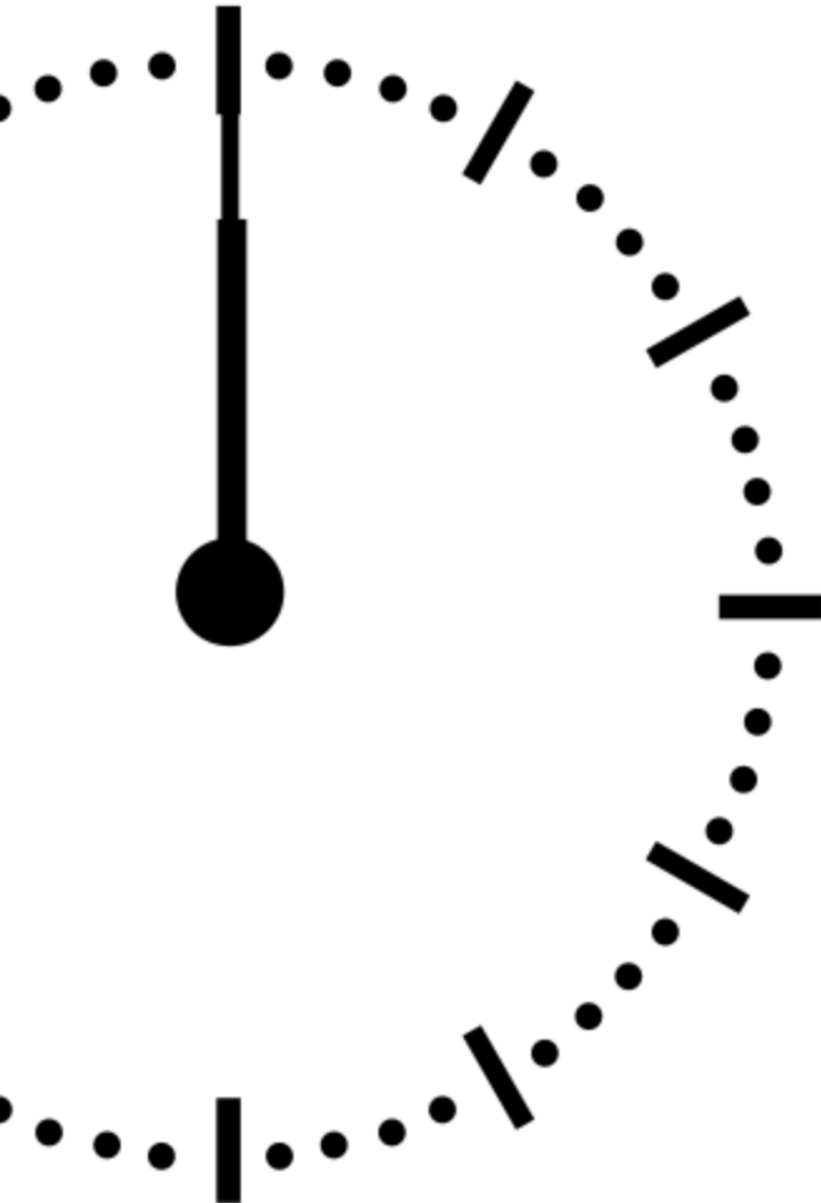
Every hour Zscaler Client Connector will connect and download any policy updates for the app profiles and forwarding profiles. If the PAC files or URLs are changed, it will automatically update every hour as this counts as a profile change.

### **Every 15 Minutes**

However every 15 minutes, Zscaler Client Connector will download the PAC file of the app profiles and the forwarding profiles in case they have changed.

### **Manually**

The end user can obviously also initiate an update through the administration of Zscaler Client Connector and force a check for software updates or force a check for policy change.



## Rotating Passwords with App Profiles

Zscaler Client Connector is locked down to prevent users from logging out, disabling, or uninstalling the application. This is password-protected and the password is generated on a per-configuration basis and available to support personnel through the administration interface that could then be provided to users if there's a need to uninstall, disable, or log out for some service-affecting reason.

### One-Time Passwords

Unique, per-device password that is generated on enrollment

Password changes when used

Password always available in device information

The screenshot shows a 'Compliance Status' interface with several fields:

- Device State:** Outdated
- Last Seen Connected to Zscaler:** Tue Sep 26 2017 07:17:38 GMT-0700 (Pacific ...)
- Last Seen with Zscaler App Active:** Tue Sep 26 2017 08:12:31 GMT-0700 (Pacific ...)
- Last Configuration Download Time:** Tue Sep 26 2017 07:17:38 GMT-0700 (Pacific ...)
- Configuration Download Count:** 1
- Logout, Disable, Uninstall Password:** kllkas87a8sd (with a 'copy' link next to it)

The 'Logout, Disable, Uninstall Password' field is highlighted with a red border.

Administrators and support teams are encouraged to only use the one-time, per-device password and NOT the global passwords within the App Profile, which can be reused.

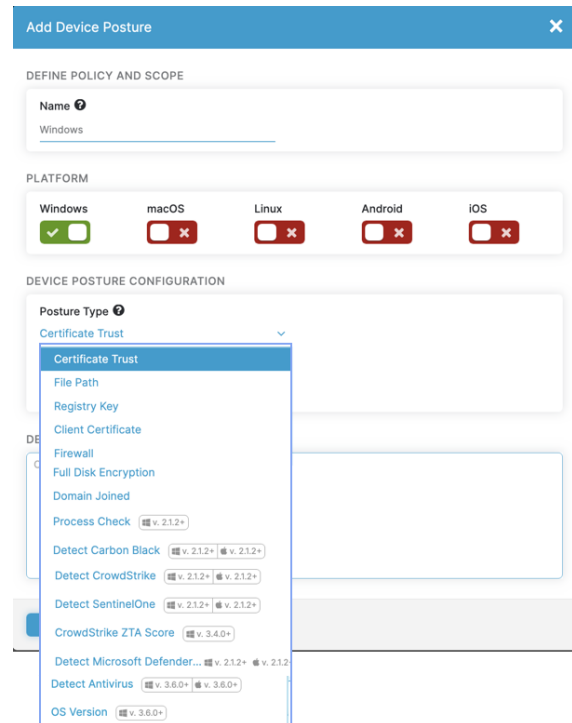
## Device Posture and Posture Checks

Within the Zscaler Client Connector, there is Device Posture. Device Posture enables a level of trust of the device as part of the Zero Trust Network Access policy.

There are a number of these posture checks available to choose from. While Windows and Mac have the ability to check for all of them, iOS and Android have limited capabilities based on their ability to understand if disk encryption is enrolled or they don't have the functionality for domain-joined devices.

These pieces of information then enable us to identify the device.

### Common Examples Include:



#### **BYOD vs. Corporate Devices**

Does the device trust a root CA, which is only internal to an organization? This enables us to consider if it's a BYOD (bring your own device) device versus a corporate device.

A corporate device will be domain-joined. It will have a certain registry entry, certain files on the device, the certificate trust.

We can also check for client certificates and ensure that the client certificate has a non-exportable private key.

#### **Device Security**

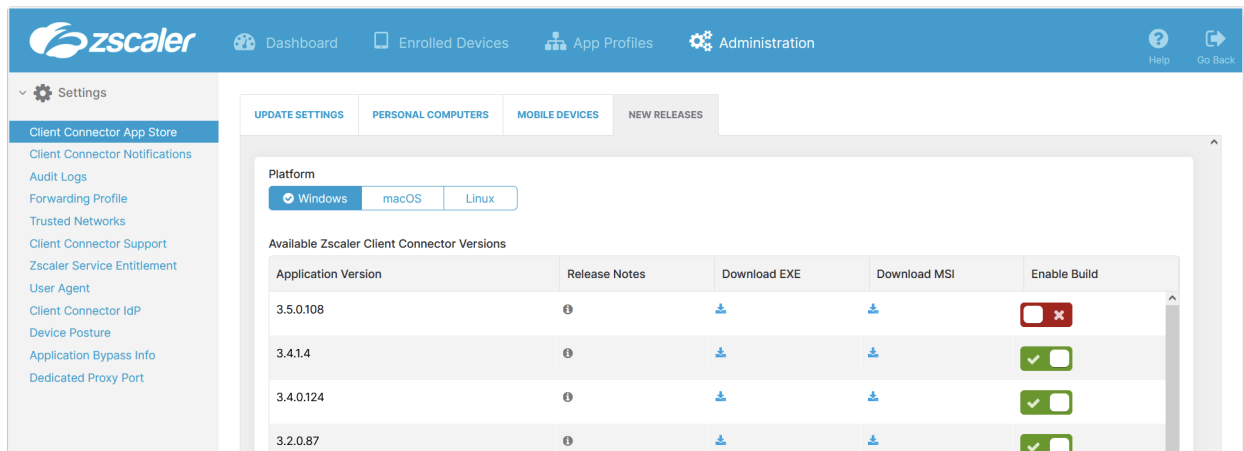
Anti-Virus, OS Version, Disk Encryption, Firewall

#### **Endpoint Protection**

So we can understand the security of the endpoint and use this in policy to provide access to applications. And then we can interface with third-party endpoint protection, such as CarbonBlack, CrowdStrike, SentinelOne, Defender, and the CrowdStrike ZTA score to make policy decisions.

For example, if Defender tells us the device is compromised, then we can prevent access to an application.

## Installing Client Connector



To install and maintain the Client Connector, follow this basic process:

### Download the install file

The files are available through the Zscaler Client Connector Portal. The install files are hosted on AWS, so it is possible to copy the link in order to distribute it to users.

### Install on devices

Always refer to the online help for each of the command line installation options.

Command Line options exist for Windows, Mac, and Linux clients, allowing for silent installations.

The **strictEnforcement** option requires cloudName and policyToken options to ensure that the user is automatically triggered to the right cloud and authentication token, and make sure that the user can not access the Internet until they are enrolled.

Tools such as Intune (Windows) or Jamf (MacOS) are popular ways of distributing to managed devices.

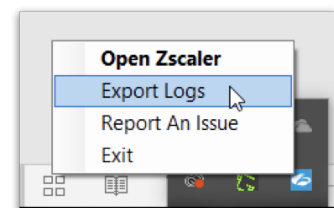
### Update the client

Group-based updates can be readily applied for automatic rollout, such that specific versions can be applied to specific groups of users – useful for testing and staggered rollouts.

### Troubleshooting

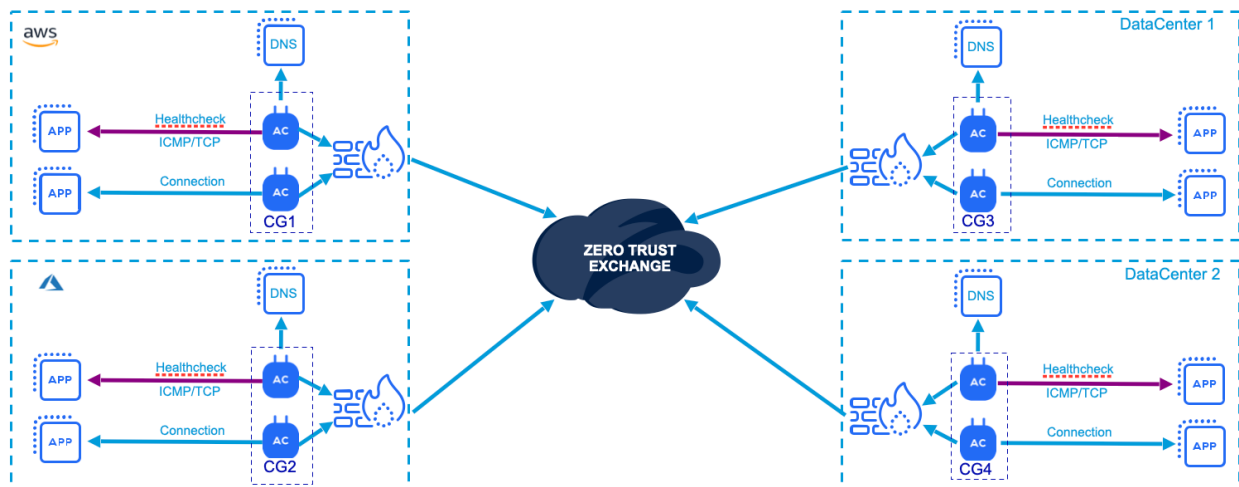
Should you encounter any issues with the installation, logs can be exported from within the client or the built-in packet capture can be used.

As well, they can be manually retrieved from the file system at **c:\ProgramData\zscaler** (Windows) or at either **~/Library/Application Support/com.zscaler.Zscaler/** or **/var/log/zscaler** (MacOS).



## App Connectors

App Connectors provide a secure authenticated interface between a customer's servers and the ZPA cloud. They do so by establishing connections out through the firewall to the Zscaler Cloud, and the Zero Trust Exchange facilitates a reverse connection. At no point are the internal/private servers exposed by public/external DNS or through inbound DMZ firewall holes.



<p><b>Fundamentals</b></p>	<p>Always deploy App Connectors as a pair (minimum) and as a different <b>Connector Group</b> in separate data centers.</p> <p>Ensure app connectors:</p> <ul style="list-style-type: none"> <li>• Can route to the internet and internal applications.</li> <li>• Meet the minimum VM requirements.</li> <li>• Can connect to applications (TCP/UDP) for health checking.</li> <li>• Source IPs are registered in Active Directory Sites &amp; Services, as the requests will be seen as coming from the App Connectors.</li> </ul>
<p><b>Deploy</b></p>	<p>Create a provisioning key for each <b>Connector Group</b></p> <p>Provisioning keys are signed by an intermediate certificate authority and the intermediate trusted by the root CA. Clients are enrolled against a client intermediate certificate authority. <b>Revoking/deleting the intermediates breaks the trust, invalidating the provisioning keys.</b></p> <p><b>Treat provisioning keys as credentials</b> (don't share in cleartext = download from the UI and upload via SCP or copy/paste over SSH or use the API to retrieve or generate dynamically).</p> <p>Deploy Connector Groups – Always refer to the online help and use it as a checklist when deploying app connectors.</p>
<p><b>Server Group</b></p>	<p>Associate the Connector Group(s) with a <b>Server Group</b>. Dynamic Server Discovery on that server group means that either the</p>



group or the connectors will automatically perform DNS resolution and create synthetic server associations that advertise those applications. This is the default (recommended) configuration and, it is not recommended to move away from Dynamic Server Discovery unless for a very specific reason.

**Define Application Segments**

Applications must be defined within an **Application Segment**.

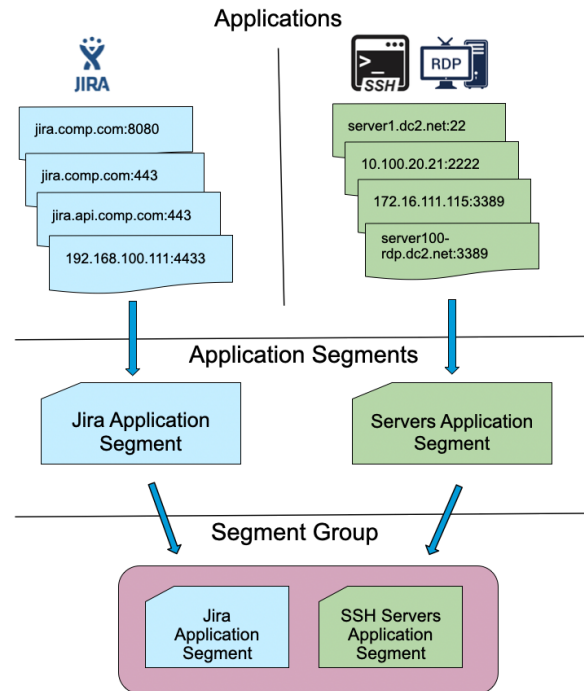
An application segment is a grouping of those applications, those defined FQDNs that make that application function. A segment group is a grouping of similar applications that you want to apply policy to. Let's say, for example, that I wanted Sales to be able to access all of these applications. In such a case, there would be different applications in different segments, possibly in different locations, but they're grouped together because they should provide the same service, and a similar set of users should be able to access that segment.

Begin the first application segment as a wildcard (example: if your internal domain is company.com, then we would use \*.company.com). This way, any time a user wants to access an application that matches that wildcard, ZPA will ask any connector within the server group to DNS resolve and perform a health check of that application. Then, ZPA will steer the client traffic through the App Connector that was able to establish the connection and pass the traffic through to the application. All of this is further based on policy.

Looking at this graphically, an application in the application segment is an FQDN, a wildcard domain, or an IP address on a standard set of ports or range of ports.

IP addresses should be used sparingly and only where an application is accessible by an IP address, or where the payload indicates that it needs to be connected by IP address.

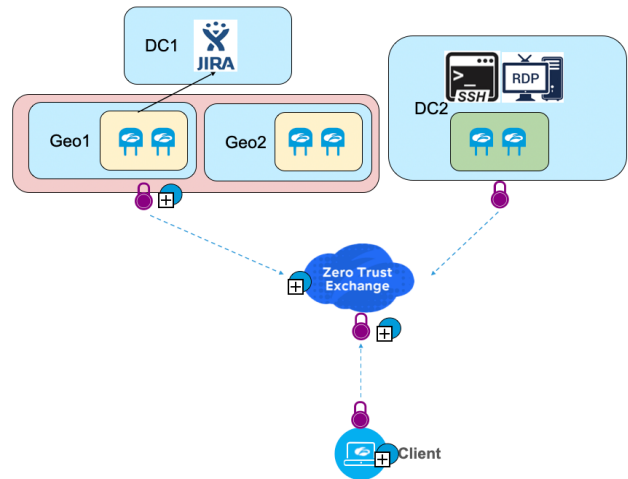
Once that application segment is defined, it's associated by definition with those server groups, and the server group is associated with the app connector group.



## Pulling it Together - Where Each Component Fits

Use case: User accessing Jira in DC1

- Traffic is identified on the client system to determine if it's an application needing to be served by ZPA
- After traffic reaches the Zero Trust Exchange (ZTE), policy evaluation takes place to determine if the user is allowed to access the requested application
- If access is allowed as per the configured policy, then the App Connector group that is closest to the user's location is identified by the ZTE
- Connection is then brokered, and the user is able to access the application



## Browser Access & Privileged Remote Access

### Browser Access (BA)

Browser Based Access provides connectivity through a web browser **without the Zscaler Client Connector** being installed to HTTP and HTTPS applications. This core connectivity capability also provides access to Privileged Remote Access applications such as SSH or RDP.

### Why use Browser Access?

It provides authenticated private website access to third parties without managing a DMZ or internet edge

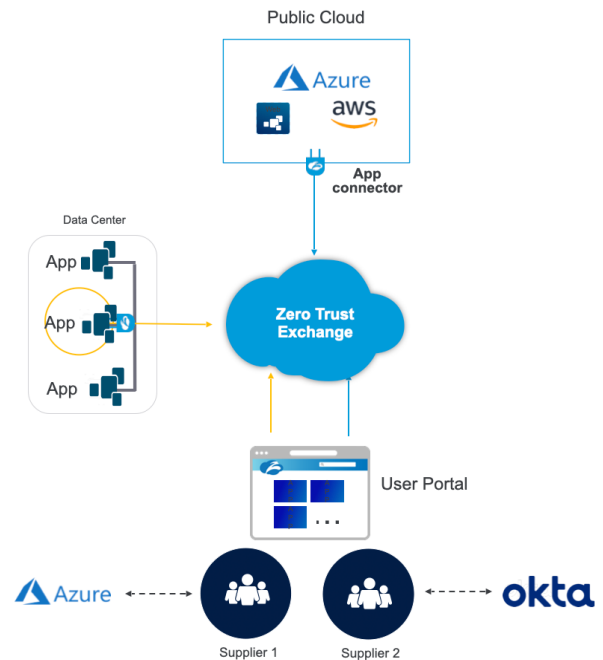
It provides access without using a VPN, browser extension, or any client software

It delivers the same experience a user would go when connecting directly to an intranet website

It allows websites to reside anywhere—in an on-premises data center or in a public cloud

It can inspect requests/response with App Protection to protect your intranet website from OWASP Top 10 & custom signatures

ZTNA policy provides least-privileged access



Zscaler Browser Access enables users to authenticate to internal websites from anywhere, without needing to manage a DMZ, Internet Edge, or a VPN—all with the same user experience as a direct website connection. A User Portal provides a graphical view within the browser of those browser-based access applications that the user has access to.

With added protection from the OWASP (Open Web Application Security Project) Top 10 and Custom Signatures to inspect the web content, as well as ZTNA policy for least privileged access, security gets a huge boost over legacy website access methods.

Now, we can immediately provide day-one access for subsidiaries or acquisitions or partners to access applications. We can further provide limited access to suppliers, contractors, customers, and other third parties through this mechanism, without the need for them to install a Zscaler Client Connector software (BYOD included—which comes down to the trust of the users and the risk associated with accessing those applications without a client-based endpoint solution).

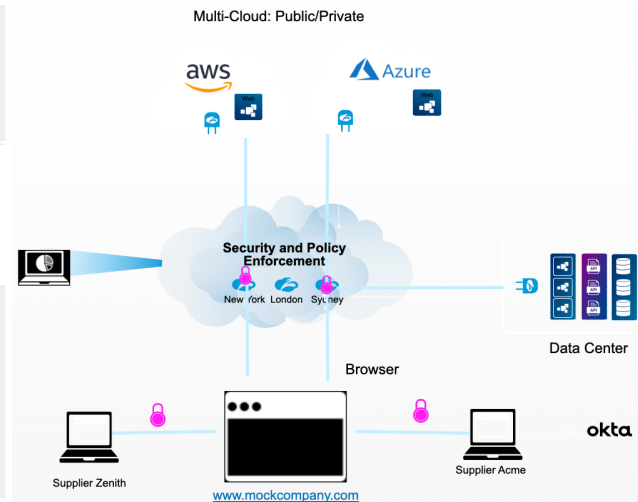
## How Browser Access Works

User types in the URL of internal web application or the User Portal and is redirected to appropriate IDP for user authentication.

The closest connector to requested app creates inside out TLS 1.2 encrypted tunnel over port 443.

The Zscaler broker stitches together apps to user connection in the broker location closest to the user, presenting them with either the direct application or the User Portal, depending on which option the user selected.

Real-time, global visibility into all user and app activity



## Configuration Overview

Fundamentals	<p>SSL is always used for the outside connection, whereas HTTP or HTTPS may be used internally.</p> <p>It's important that the <b>client trusts that server certificate</b>. This might be publicly signed by a public certificate authority (<b>the private key never leaves the Zscaler cloud</b>), or it could be an internal certificate authority where only your internal clients trust that root certificate authority. Once the user has the connection to the Zero Trust Exchange and the policy permits them access, an inside-out tunnel is created between the App Connector and the Zero Trust Exchange.</p> <p>There are <b>three tunnels</b>: The client to the Zero Trust Exchange, the App Connector to the Zero Trust Exchange, and Zero Trust Exchange to the application through the App Connector.</p>
<p>ZPA Admin Configuration</p> <p>Always refer to the online help, using it as a checklist.</p>	<p>As with any other application, the website application must be in an application segment. But in this case, as DNS is utilized, <b>FQDNs are required</b>.</p> <p>If desired, also create a User Portal for added user convenience, especially if there are multiple Browser Access enabled applications, linking those applications to the portal.</p>
DNS Configuration	<p>The Zscaler CNAME (alias) provided by ZPA will be put in the public DNS.</p>

## Privileged Remote Access (PRA)

PRA is an authenticated remote desktop gateway/SSH gateway that relies on Zscaler's Service Edge and the App Connector to allow a user to access IT and OT servers, desktops, and workstations using their browser, typically through an authenticated web portal.

### Privileged Remote Access:

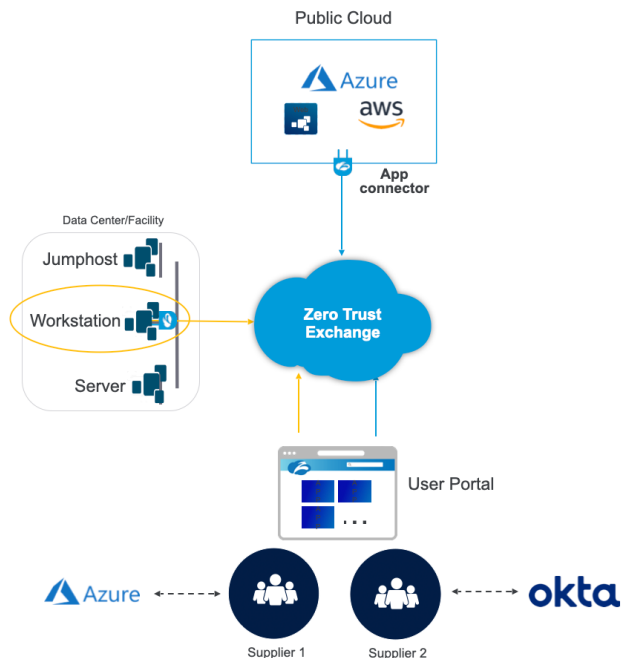
Provides authenticated access to your jump hosts, workstations, servers, and IT/OT equipment from a browser

Allows console sessions to be streamed, meaning no data resides on the user's device

Requires no VPN client, browser extension, or other client software

Eliminates firewalls and DMZs—jump hosts, workstations, and servers can be limited to the App Connector IPs

Allows a user to access only the consoles you specify



Similar to the user portal, the users can connect to the Zero Trust Exchange, and the Zero Trust Exchange provides authenticated access to jump hosts, workstation servers, IT, and OT equipment, all within the browser. The console session is streamed, meaning that no data is stored on the user's device. The user's device has no direct access to that application. It eliminates the need for firewalls, DMZs, and the jump hosts and workstations and servers can be limited to the Zscaler App Connectors' IP addresses. And, based on policy, users can only access the consoles they're permitted access to.

The key driver is the common use case of supporting BYOD devices so the user never needs a corporate device to be able to access privileged resources. Because it's an unmanaged device, you can provide secure access for contractors, suppliers, and other third parties to perform privileged access, such as administration and maintenance tasks.

### Configuring Privileged Remote Access

As with Browser Access, specific configuration steps are contained within the online help and should be referenced during the process.

## Platform Services

Platform Services will allow you to explore fundamental capabilities that Zscaler offers including Private Service Edges, Device Posture, TLS Inspection, Policy Framework, and Analytics & Reporting. Gain an overview of Zscaler's fundamental Platform capabilities. Dive deeper into how these functionalities interact with other services within Zero Trust Exchange and gain knowledge on how to configure Zscaler's Platform Services as they relate to Zscaler best practices.

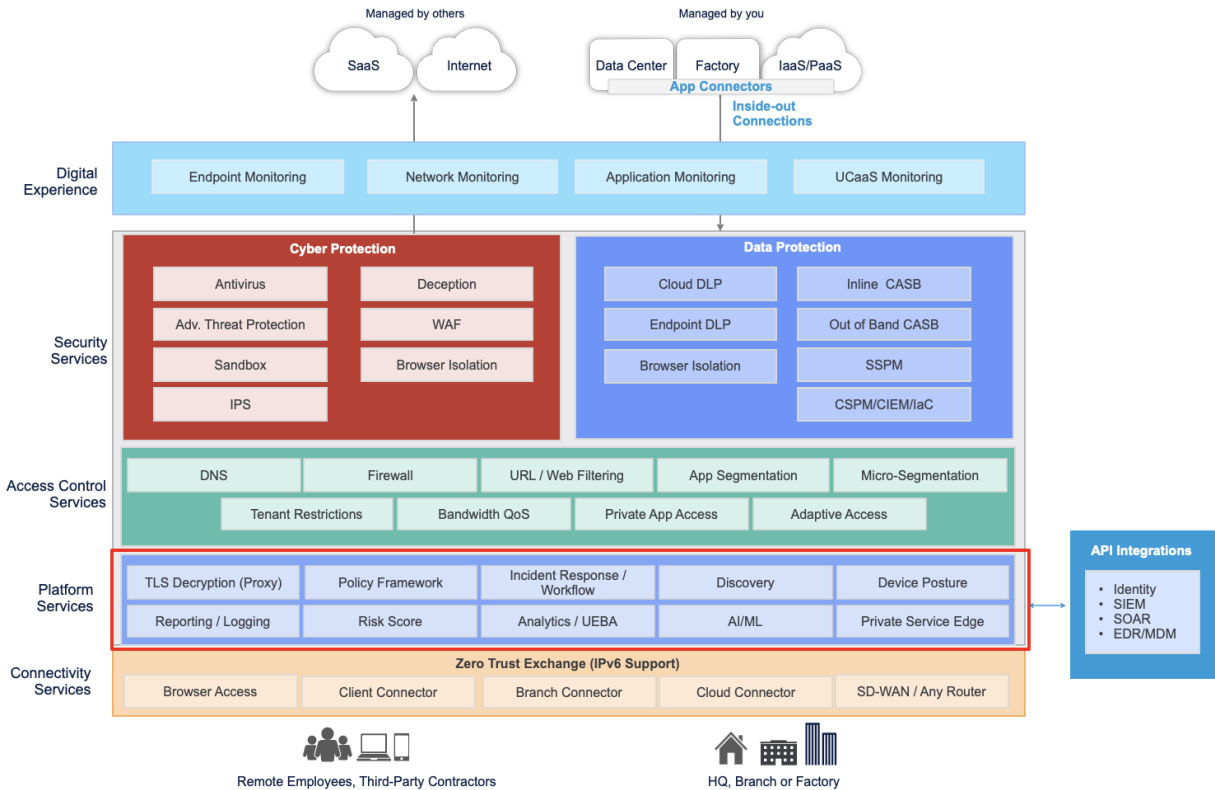
---

By the end of this chapter, you will be able to

1. **Identify** the fundamental set of Platform Services Zscaler provides and how they apply to the Zero Trust Exchange.
2. **Recognize** how policy is consumed, constructed, and passed to other functions of the Zero Trust Exchange (i.e. Connectivity, Access Control, Security, and Digital Experience Services).
3. **Discover** how to configure Zscaler Platform services and capabilities.

## Zscaler's Platform Services Suite

Included in Zscaler's holistic Zero Trust Exchange is Zscaler's Platform Services suite. This important suite contains a set of fundamental functionalities that are common across Zscaler's other services suites such as Connectivity, Access Control, Security, and Digital Experience.



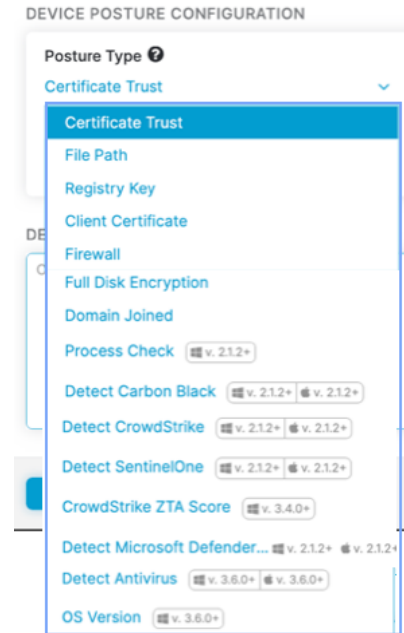
## Device Posture

Device Posture is provided as part of Zscaler's Platform Services suite. It does, however, consume posture from other functionalities in the Zero Trust Exchange such as Browser Access, Zscaler Client Connector in the Connectivity Services suite, and Identity Integration. As such, we don't need to cover it again here, except highlight what a SAML response looks like when it returns Device Attributes.

### Device Attributes

As the client initiates a SAML authentication request, both for Zscaler Internet Access or Zscaler Private Access, a SAML response is returned. Once consumed, Zscaler can apply policy based on those attributes.

Below we can see Azure AD has affirmed the device is managed because it's enrolled in Azure AD and managed by Intune. It's compliant because it's gone through a compliance policy that says the device is running specific software and is compliant with the corporate policy. And "is known" tells us is the device managed by Intune versus corporately managed by something like SCCM (now known as MECM, Microsoft Endpoint Configuration Manager).



## SAML Response to Authentication

### SAML Response Attributes

Through authentication, the SAML IDP will return an assertion (XML Document) which contains attributes the ZTE can apply policy on

ZIA - [https://login.<cloud>.net/cstart?version=1&\\_domain=<domain>&redurl=https://mobile.<cloud>.net](https://login.<cloud>.net/cstart?version=1&_domain=<domain>&redurl=https://mobile.<cloud>.net)

ZPA - <https://samlsprivate.zscaler.com/auth/v2/login?ssotype=test&domain=<domain>>

### Example Response

```
{
  "nameid": "mryan@welshgeek.net",
  "orgid": null,
  "idpEntityID": null,
  "idpid": null,
  "saml_attributes": {
    "http://schemas.microsoft.com/identity/claims/tenantid": "fe4036f5-76ad-4232-9bda-313544c3ad54",
    "http://schemas.microsoft.com/identity/claims/objectidentifier": "86dfb10-ca60-4dc8-b8e5-67e0bada8dd8",
    "http://schemas.microsoft.com/identity/claims/identityprovider": "https://sts.windows.net/fe4036f5-76ad-4232-9bda-313544c3ad54/",
    "http://schemas.microsoft.com/claims/authnmethodsreferences": [
      "http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password",
      "http://schemas.microsoft.com/claims/multipleauthn"
    ],
    "http://schemas.microsoft.com/2012/01/devicecontext/claims/ismanaged": "true",
    "http://schemas.microsoft.com/2014/09/devicecontext/claims/iscompliant": "true",
    "http://schemas.microsoft.com/2014/02/devicecontext/claims/isknown": "true",
    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname": "Mark",
    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname": "Ryan",
    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name": "mryan@welshgeek.net",
    "memberOf": ["Group-OEB", "ADSyncAdmins", "CertificateAuth", "Internet-ZPA-Enabled", "Zscaler", "Private Access - ALL"],
    "Country/Country": "CN",
    "samlassertion": null
  }
}
```

← Device Attributes

Zscaler SAML SP for ZIA and ZPA consume attributes

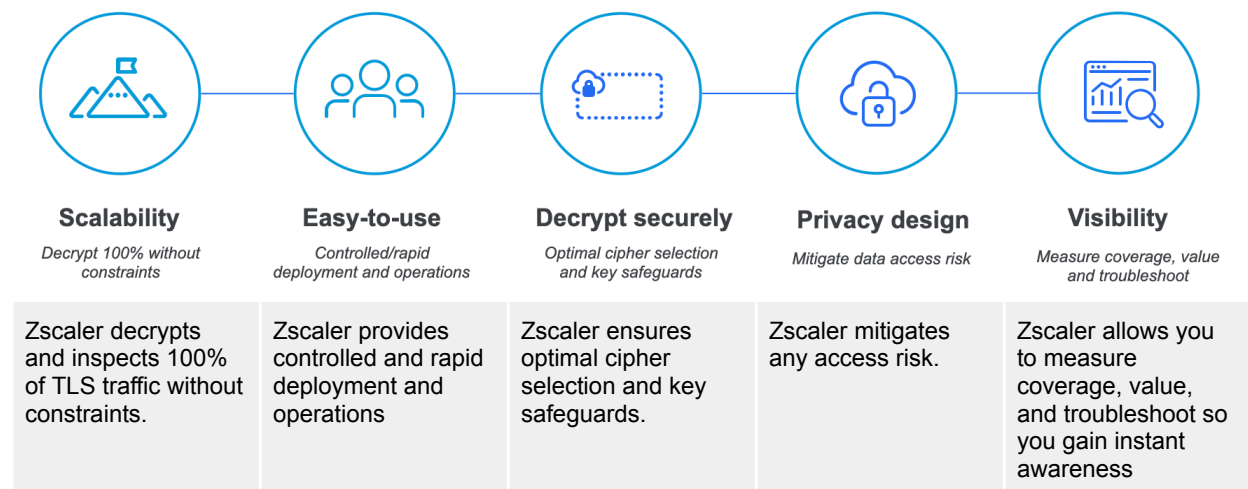
Attributes synchronise from ZIA SAML SP to Mobile Admin portal to use for entitlement and policy objects



## TLS Inspection

As part of the Platform Services suite of capabilities, TLS Decryption or Inspection works to inspect content and enable various Access Control, Cyber Protection, and Data Protection functionalities to apply policy based on the content of those encrypted communications.

### SSL Inspection Key Product Pillars and Functionality



Within the Zero Trust Exchange, there are several facets of how TLS inspection works. The first is Access Control—URL Filtering and Cloud Firewall functionality apply policy based on the request and the response.

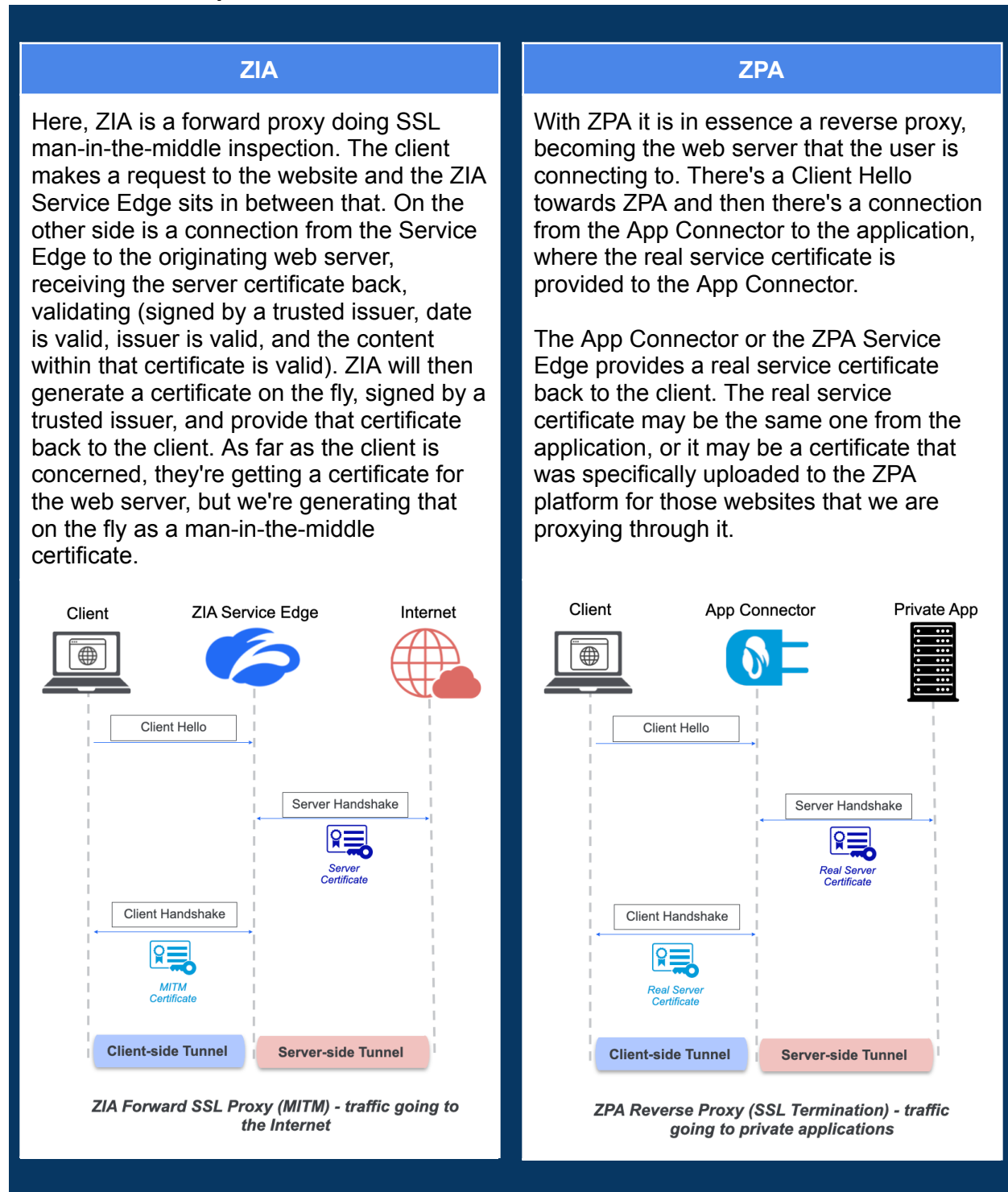
The second part is based around compromise—the actual payload that's coming from or going toward the web server such as malware inspection, antivirus, the Advanced Threat Protection, the IPS signature, and cloud sandbox functionality.

Finally there's the Data Loss or the data protection side. Inline DLP means scanning the payload that's coming from the client to make sure that nefarious users or accidental users are leaking data out to the internet. Being able to provide Granular Application Controls, not just on the FQDN, the URL that's being accessed, but across the entire URI that's being connected to.

All of this is built as a scalable platform, assuming 100% of the transactions will be SSL and 100% of those could be decrypted. Generating intermediate certificates at line speed for all users and all locations enables the best security and data protection outcomes.



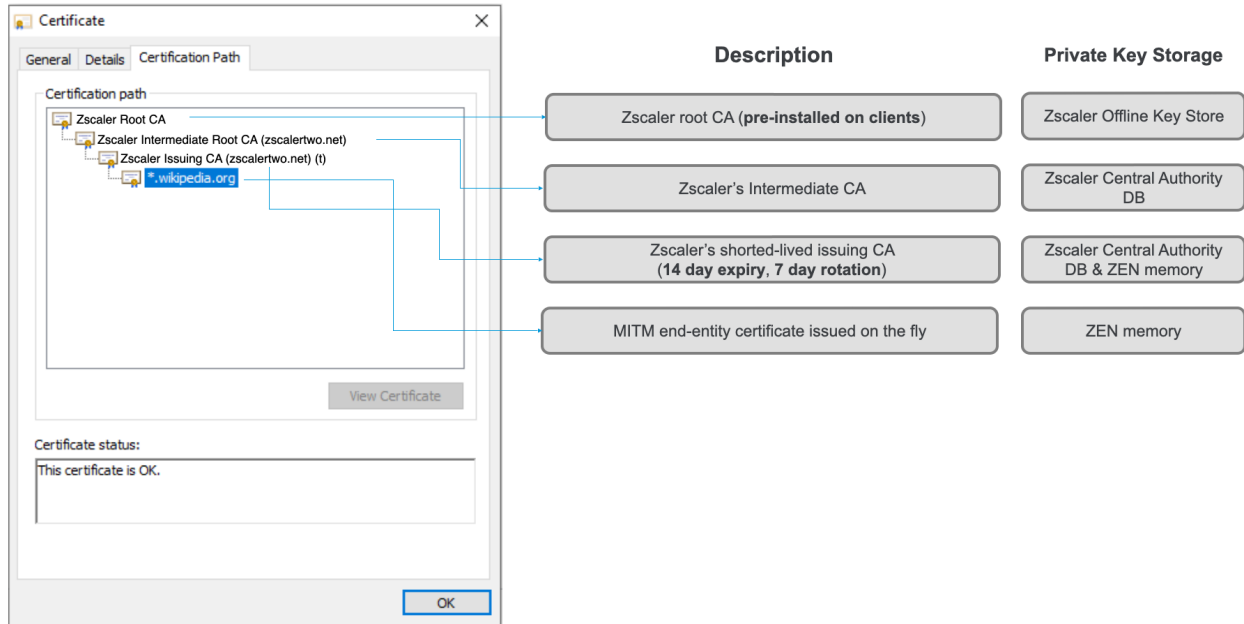
## How Does SSL Inspection Work?



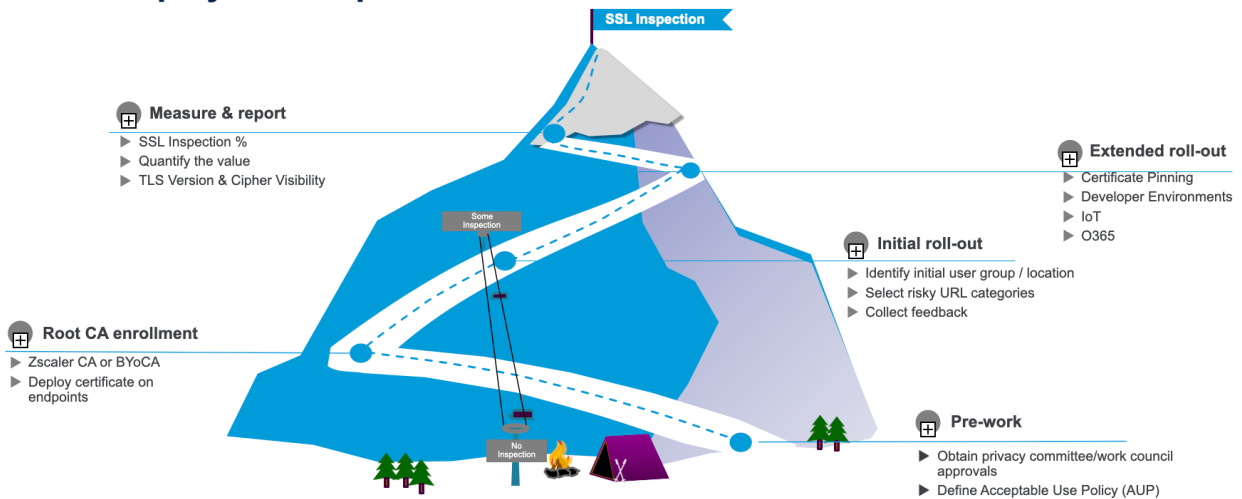
**Short version:** Zscaler Internet Access (ZIA) is a forward proxy interception and Zscaler Private Access (ZPA) is essentially a reverse proxy SSL termination interception.

From a client (end user) perspective, they could look at the certificate chain within their browser session to see which certificate is actually being used. In this case we can see that while they are going to a Wikipedia site, in reality the certificate being used is the one from Zscaler, providing a clear indication that the traffic is now being intercepted and inspected.

## Certificate Chain with SSL Inspection



## How to deploy SSL Inspection



Safe to say, Zscaler knows perhaps more than any company on Earth how to roll out SSL inspection at scale. Let's break it down into manageable steps.

### Pre-Work

Ensure that you have agreement within an organization that SSL inspection is going to be deployed. It's being deployed to support the business. It's not to spy on what users are doing, but to ensure that the business can continue to function making sure that they're not infected with malware and to ensure that data doesn't leak out that affects the customer perception or the reputation of a business, defining the acceptable usage policy and any notifications that are going to be provided to users.

**WARNING \*\* WARNING \*\* WARNING**

You are accessing a [redacted] information system, which includes this computer, the computer network on which it is connected, all other computers connected to this network, and all storage media connected to this computer or other computers on this network. This information system is provided for [redacted] use only. Unauthorized or improper use of this information may result in disciplinary action, as well as civil and criminal penalties.

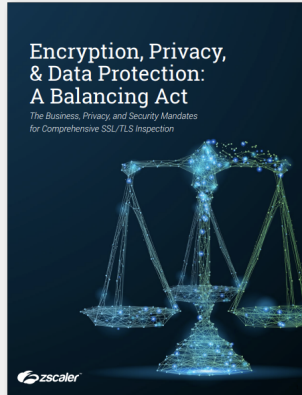
By using this information system you consent to the following:

a. You have no reasonable expectation of privacy regarding any communications or data transiting this network, stored on, or travelling to or from this information system;

Click "I AGREE" to consent to these terms of use.

**WARNING \*\* WARNING \*\* WARNING**

It's important to get buy-in from the legal teams, privacy leaders, the security teams, to understand why this is being done.



This is often a misunderstood step with lofty goals of deploying SSL inspection. You can get wrapped up in lots of red tape as to workers' councils, for example, being concerned about spying on users and what they're doing. But it's really important to get a level set within the organization of why TLS inspection is being done - for the security of the business and the business's reputation, understanding what that encrypted data is, and how Zscaler handles it.

Obfuscating the user and device data, never storing any of the content of the payload onto the disk. Scanning for data protection, for infection, and making sure malware doesn't come into the organization or leak out. And of course to best identify and block command and control services.

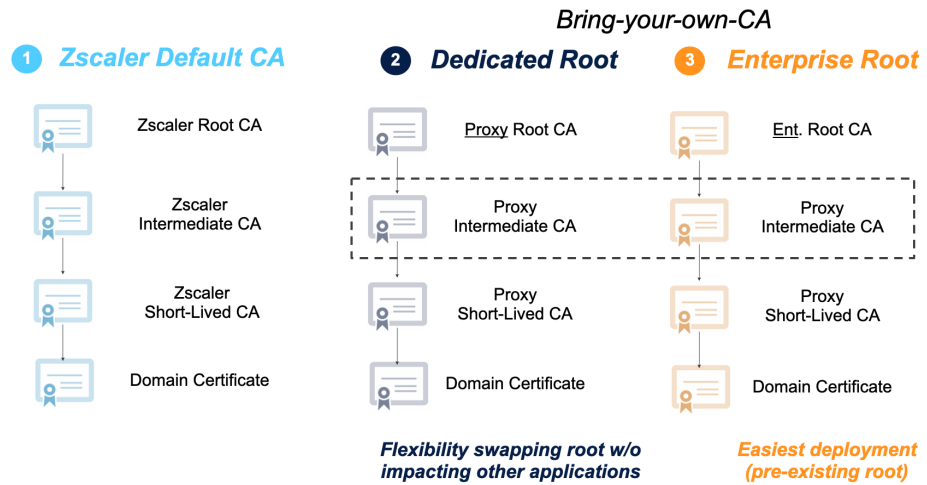
Finally, develop a communication plan for the users. Why are we doing this? Updating the acceptable usage policy, sending out notifications so users understand how to check whether or not SSL is being inspected or not, and what decisions those users can make as to whether or not they're going to continue using their work device to connect to these websites whilst SSL inspection is taking place.

## Root CA Enrollment

Once we have buy-in, we're going to look at rolling out the root certificate authorities to these devices and make sure that all client devices trust the intermediate certificate or trust the certificates that have been inspected.

There are multiple kinds of SSL inspection. The default that comes with Zscaler is the Zscaler root certificate authority which has a Chain of Trust through the intermediate certificate, the short-lived temporary certificate, and the web server domain certificate that's going to be issued on the fly.

Customers also have the ability to bring their own certificate authority and you might take two different routes for this.



- The first one is a dedicated root where you create an offline certificate authority specific for SSL inspection on the proxy and you load that up to Zscaler, and therefore every certificate that is issued is then trusted through that Chain of Trust from the specific proxy certificate, the intermediate certificate, the short-lived certificate, and then that spoofed web server certificate. It means that you're in full control of swapping out the roots and full control of the Chain of Trust all the way down to that domain certificate.
- The alternative is using your existing enterprise root certificate authority. For example, if you have Active Directory, there is a root certificate authority that comes with it and every device that's enrolled within Active Directory the certificate is already inherently trusted. You can generate an intermediate certificate authority from that and upload that to Zscaler and any client should inherently trust that and it simplifies some of the rollout.

Rolling out certificates is relatively simple.

- You can use the Zscaler Client Connector. Zscaler Client Connector can automatically install the Zscaler SSL certificate.
- You can upload your root certificate to Zscaler Client Connector Portal and then when the install Zscaler SSL certificate is checked, both the Zscaler root certificate and your custom

certificate will be installed automatically on devices that run the Zscaler Client Connector.

#### Initial Roll-Out

And then we'll roll out and do some inspection for a select group of users, for specific categories, collecting feedback from the users on their experience of that.

This all starts with configuring the base set of rules before and continuing throughout the pilot phase.

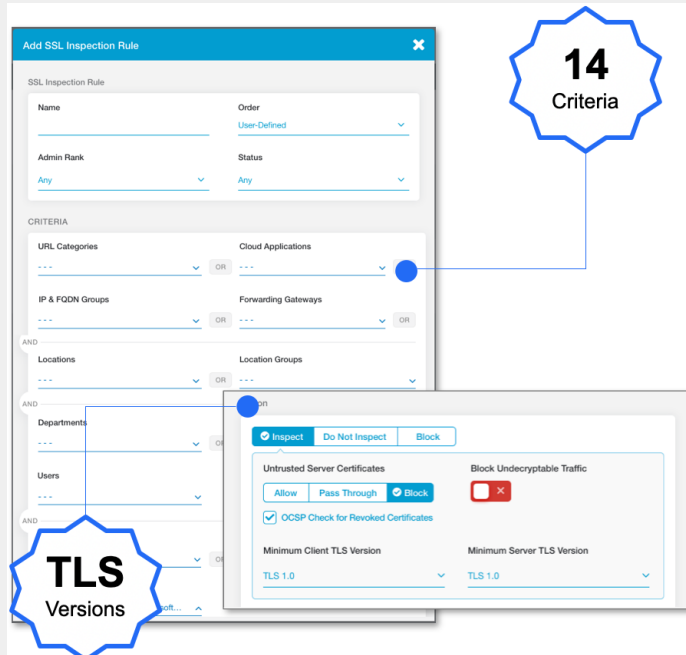
#### **Granular Policy Framework**

The granular policy enables you to make decisions based on the user, group, department, the category, the cloud application, anything around the FQDN, the IP address, and even device types. We can make sure we don't break applications that may have certificate pinning involved. Client operating system-specific user agents – we might be able to see certain device types.

With this policy, we can enforce that only websites with specific TLS versions or the client minimum TLS version is supported, as well as how we control the certificate trust. Is it passed through? Do we block untrusted certificates? Do we block undecryptable traffic and will we perform an OCSP check for that certificate, which is the Online Certificate Status Protocol, to check whether or not a certificate is valid or has been revoked?

With the Zscaler One-Click configuration, we can automatically exclude services like M365 OneDrive, SharePoint from inspection which may have challenges with inspection being implemented.





### Granular rule-based engine

- User/group/department
- URL Category/Cloud App
- Destination IP/FQDN group
- Device: Name, OS, Trust Level

### Avoid breaking cert pinned apps

- Client OS, User Agent, Device

### Enforce secure TLS usage

- Minimum TLS versions
- Certificate validation/revocation for inspected and uninspected traffic

### Exclude from M365 One Click

- Inspect OneDrive, Sharepoint

Rule Order	Rule Name	Criteria	Action	Label and Description
1	Zscaler Recommended Exemptions	URL CATEGORIES Recommended SSL Exemptions	Do Not Inspect Bypass Other Policies	DESCRIPTION Zscaler Recommended Exemptions
2	Office 365 One Click	URL CATEGORIES Office 365; Zscaler Recommended Exemptions Office 365	Do Not Inspect Bypass Other Policies	DESCRIPTION Office 365 One Click Rule creat...
3	Inspect Pilot Group	DEVICE GROUPS Windows  GROUPS Pilot SSL Group  URL CATEGORIES Other Adult Material; Adult Themes; Lingerie/Bikini; Nudity...	Inspect Untrusted Server Certificates Block OCSP Revocation Check Enabled Block Undecryptable Traffic Disabled Minimum Client TLS Version TLS 1.0 Minimum Server TLS Version TLS 1.0	
Default	Default SSL Inspection Rule	Any	Do Not Inspect Evaluate Other Policies Show End User Notifications Enabled Untrusted Server Certificates Allow OCSP Revocation Check Disabled Minimum TLS Version TLS 1.0	DESCRIPTION Default SSL Inspection Rule cre...

For a pilot rule set, we're going to specifically say for a group of users that are in a group called pilot SSL, we're going to inspect some very specific categories. We're going to block untrusted certificates. We're going to do that OCSP revocation check. We're going to block undecryptable traffic, and ensure that the minimum client and server versions are TLS 1.0, and then the default rule is 'do not inspect'.

The higher level rules, rules number 1 and 2, specifically bypass inspection for M365 and other Zscaler-recommended SSL exemptions where we know that applications might break if SSL is employed. It's also important to understand other traffic that might be generated by your browser. For example, the QUIC (Quick UDP Internet Connection) protocol developed by Google is an experimental protocol that uses UDP port 443 to deliver content to the client.

Now it's important to them to block this (and similarly Apple Private Relay) within the firewall, which forces the client to turn back to normal HTTP, HTTPS, over TCP 443 so that the SSL inspection can be done for that protocol. We continue to roll out and we're going to take a look at applications and client environments that may have challenges with inspection.

Rule Order	Rule Name	Criteria	Action
1	Zscaler Proxy Traffic	DESTINATION IP CATEGORIES Zscaler Proxy IPs  NETWORK SERVICES Zscaler Proxy Network Services	Allow
2	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Allow
3	Recommended Firewall Rule	NETWORK SERVICES DNS; HTTP; HTTPS	Allow
4	Block QUIC	NETWORK SERVICES QUIC	Block/Drop
Default	Default Firewall Filtering Rule	Any	Block/Drop

*If sending UDP traffic to Zscaler, drop QUIC in the Cloud Firewall*

Chrome | chrome://flags

● Experimental QUIC protocol  
 Enable experimental QUIC protocol support. – Mac, Windows, Linux, Chrome OS, Android, Fuchsia  
[#enable-quic](#)

Disabled ▾

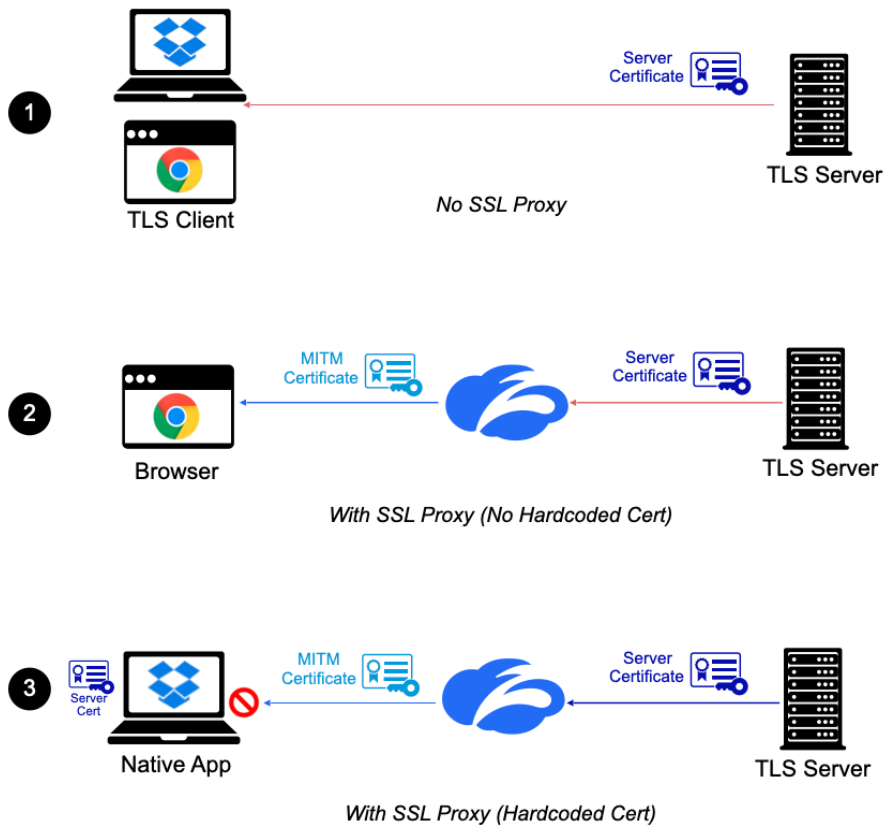
*Disable QUIC on the client using Chrome flags (Chrome Enterprise Cloud Management)*

**Extended Roll-Out**

Now we'll figure out deeper problems that might have existed, such as certificate pinning, how to handle developer environments, IoT environments, and the policy around services like Office 365.

Certificate pinning or hard-coded certificates – what is that? It means that the client is going to check for the certificate and expects a specific certificate to be returned. The man-in-the-middle certificate that we deliver will not be trusted. It's not the certificate that's been expected, so the application will fail. A good example of this would be something like Dropbox. The Dropbox client expects a specific certificate to be delivered with a specific serial number, signed by a specific issuer, therefore the man-in-the-middle certificate we deliver isn't trusted, so the Dropbox client will fail. However, Dropbox within the browser will continue to work.

## Certificate pinning/Hardcoded certificates:



We need to be able to identify these certificates. Either configure those clients to treat them as valid or make a decision to bypass SSL for inspection for those applications. It's very common, with iOS and Android, for certificate pinning or hard-coded certificates to be used. DigiCert recommends not to use certificate pinning for some of these reasons.

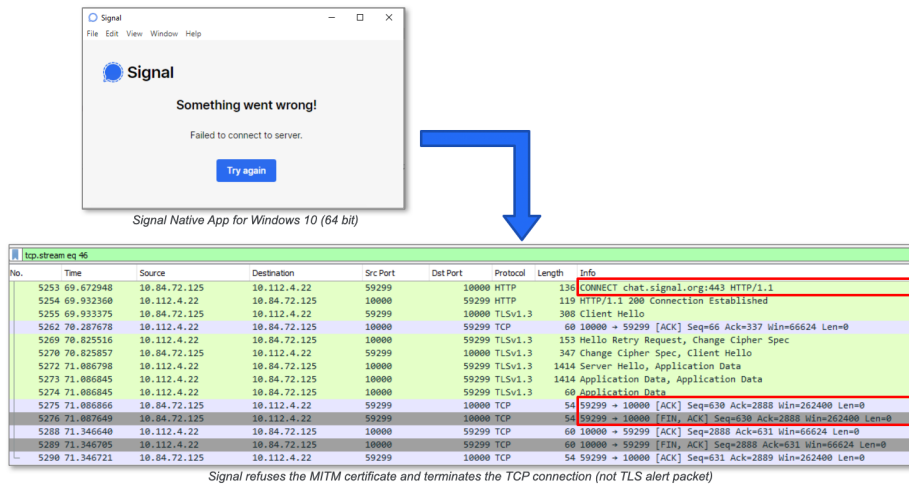
## Troubleshooting

A packet capture will help you understand what's going on. You could look at the certificate when the client makes the request and understand that the certificate was delivered to the client, but the client closed the connection very quickly once the certificate was delivered. That indicates that the client, although connected, decided it didn't trust the certificate and closed down.

We can then also understand by looking in the SSL logs for those transactions within the Zscaler administration interface (now known as ZIA Admin Portal) that the client failed the handshake. The client closed the connection, and therefore we need to do something about this. So what can you do? You can make decisions based on either the specific operating system, the operating system combined with an application to bypass inspection, and you could also do this based on the user agent as well.

We know that it's Android or iOS, they're connecting to this signal application, and there is no user agent provided as part of that CONNECT request. Or there is a user agent but it's not one that we know about, and therefore make a combined policy decision to bypass that inspection.

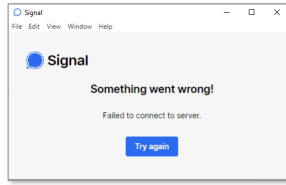
## Hardcoded certificates: How to identify?



The image shows a Signal app error message window and a network packet capture. The error message window, titled "Signal", displays "Something went wrong!" and "Failed to connect to server." with a "Try again" button. Below it, the text "Signal Native App for Windows 10 (64 bit)" is visible. A blue arrow points from the error message to a network packet capture window titled "tcp.stream eq 46". The packet capture shows a series of packets between source IP 10.84.72.125 and destination IP 10.112.4.22. The packets include HTTP CONNECT, HTTP/1.1 200 Connection Established, TLSv1.3 Client Hello, Hello Retry Request, Change Cipher Spec, Server Hello, Application Data, and TCP ACKs. The final packet (No. 5290) is a TCP RST (Reset) with Seq=631, Ack=2889, Win=262400, Len=0, indicating a connection reset.

No.	Time	Source	Destination	Src Port	Dest Port	Protocol	Length	Info
5253	69.672948	10.84.72.125	10.112.4.22	59299	10000	HTTP	136	CONNECT chat.signal.org:443 HTTP/1.1
5254	69.932360	10.112.4.22	10.84.72.125	10000	59299	HTTP	119	HTTP/1.1 200 Connection Established
5255	69.933375	10.84.72.125	10.112.4.22	59299	10000	TLSv1.3	308	Client Hello
5262	70.287678	10.112.4.22	10.84.72.125	10000	59299	TCP	60	10000 → 59299 [ACK] Seq=66 Ack=337 Win=66624 Len=0
5269	70.825516	10.112.4.22	10.84.72.125	10000	59299	TLSv1.3	153	Hello Retry Request, Change Cipher Spec
5270	70.825857	10.84.72.125	10.112.4.22	59299	10000	TLSv1.3	347	Change Cipher Spec, Client Hello
5272	71.086798	10.112.4.22	10.84.72.125	10000	59299	TLSv1.3	1414	Server Hello, Application Data
5273	71.086845	10.112.4.22	10.84.72.125	10000	59299	TLSv1.3	1414	Application Data, Application Data
5274	71.086845	10.112.4.22	10.84.72.125	10000	59299	TLSv1.3	60	Application Data
5275	71.086866	10.84.72.125	10.112.4.22	59299	10000	TCP	54	59299 → 10000 [ACK] Seq=630 Ack=2888 Win=262400 Len=0
5276	71.087688	10.84.72.125	10.112.4.22	59299	10000	TCP	54	59299 → 10000 [FIN, ACK] Seq=630 Ack=2888 Win=262400 Len=0
5288	71.346540	10.112.4.22	10.84.72.125	10000	59299	TCP	60	10000 → 59299 [ACK] Seq=2888 Ack=631 Win=66624 Len=0
5289	71.346705	10.112.4.22	10.84.72.125	10000	59299	TCP	60	10000 → 59299 [FIN, ACK] Seq=2888 Ack=631 Win=66624 Len=0
5290	71.346721	10.84.72.125	10.112.4.22	59299	10000	TCP	54	59299 → 10000 [ACK] Seq=631 Ack=2889 Win=262400 Len=0

Signal refuses the MITM certificate and terminates the TCP connection (not TLS alert packet)

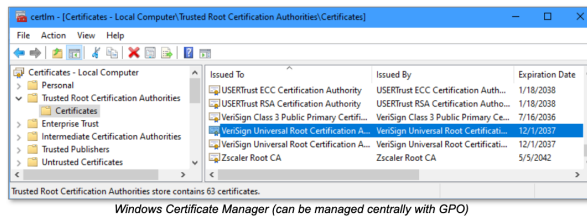


No.	Event Time	Policy Action	Client SSL Handshake Failure Reason...	Client SSL Handshake Failure Aggregat...	URL	Cloud Application...	Protocol
1	Tuesday, May 17, 2022 5:19:38 PM	Denied due to failed client SSL handshake	CLOSE_NOTIFY	3	chat.signal.org	None	SSL
2	Tuesday, May 17, 2022 5:18:44 PM	Allowed	None	None	chat.signal.org...	Signal	HTTP Proxy
3	Tuesday, May 17, 2022 5:18:41 PM	Allowed	None	None	chat.signal.org...	Signal	HTTP Proxy
4	Tuesday, May 17, 2022 5:18:40 PM	Denied due to failed client SSL handshake	CLOSE_NOTIFY	1	chat.signal.org	None	SSL

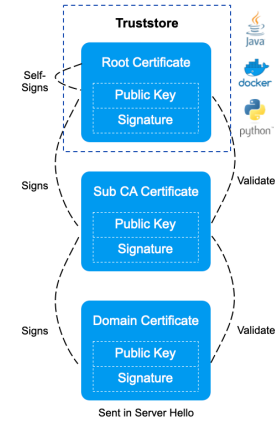
★ Failed client SSL handshake weblogs

### Applications with customer truststores: What are they?

- Every OS has a default system root CA certificate store (root-of-trust)
- Some applications have a custom trust store (e.g. Firefox, Python, Developer Environments)
- Zscaler root CA certificate must be pre-deployed in trust store for MITM to work (establish chain-of-trust)



Windows Certificate Manager (can be managed centrally with GPO)

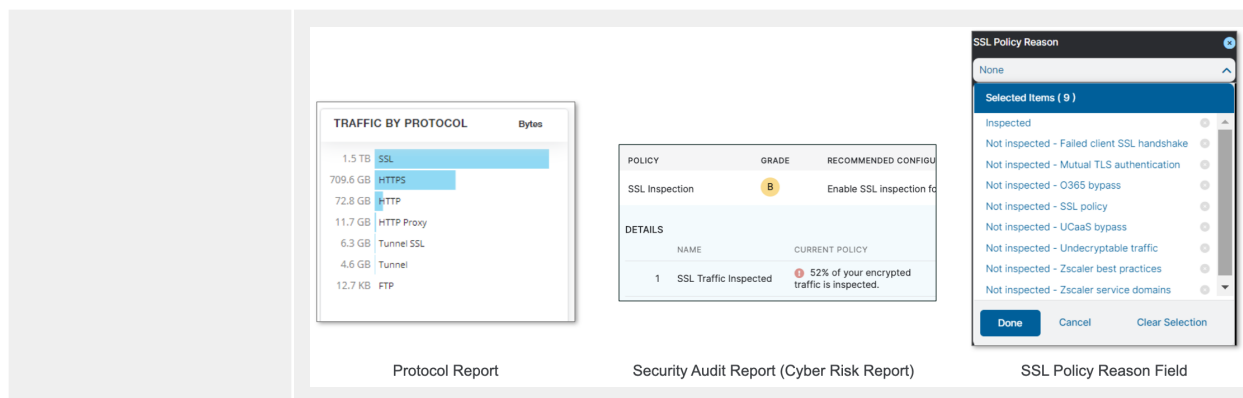


### Measure & Report

Really throughout the rollout it makes sense to measure and report on the capabilities.

- How much SSL inspection has been done? Quantify the value of SSL inspection towards the business.
- How much decryption has been done as well as how much malware and how much DLP has been triggered that supported the business decision?
- And then we can also see these TLS versions and ciphers as we go through to see how this is changing over time and the value that Zscaler brings for the SSL inspection journey.

The Protocol Report, Security Audit Report (Cyber Risk Report) and SSL Policy Reason field are all go-to resources to measure the success.



## Policy Framework

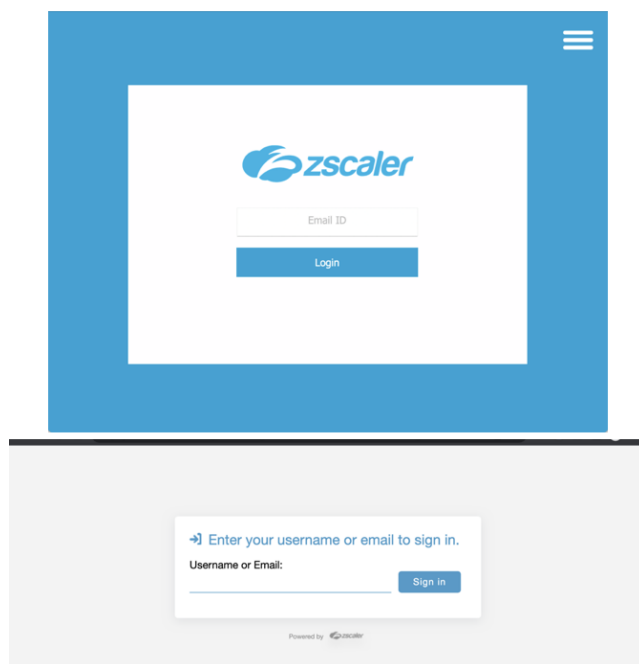
### Authentication Policy

#### How does the Zero Trust Exchange decide how to authenticate a user?

When connecting to the ZTE through Browser Based Access or Client Connector, the user should be automatically redirected to the SAML IDP. However, what criteria are used to determine which IDP to redirect to?

Answer:

- Client Connector - Was the user prompted to enter a Username?  
The Domain (after the @) maps to the Identity Provider, and user is redirected to the Identity Provider to authenticate
- Client Connector - Was the client installed with a –userDomain option  
The Domain maps to the Identity Provider
- Browser-Based Access - Multiple Identity Providers configured? The user is prompted for a username/email. The Domain (after the @) maps to the Identity Provider, and user is redirected to the Identity Provider to authenticate
- Browser-Based Access - Single Identity Provider configured? The user will automatically be redirected to the Identity Provider



Looking at the different policy framework and components, think about how the Zero Trust Exchange identifies the user. Can we give anything as part of install parameters or configuration

to understand which identity providers should be used to authenticate the user? Based on that, should the user be allowed to connect to the Zero Trust Exchange?

We go through an authentication round. The SAML IdP will control whether or not it grants SAML assertions to the user based on its policy. Zscaler consumes that assertion and then makes a decision as to which parts of the Zero Trust Exchange the user is entitled to connect to.

Once the user is connected, we can assess information about how the user is connected, whether they're using browser-based access, privileged remote access, whether we're going to drive them into isolation, or use the Zscaler Client Connector and the Zscaler Client Connector can give us that trusted network policy to understand which network the user is on and what services should be enabled.

Based on that network policy, we can make decisions on how the user connects. Should they connect to public Service Edges or private Service Edges?

Based on the Zscaler Client Connector information, we can understand should we update the user's version of Zscaler Client Connector. What profile should be installed, both the application configuration and the forwarding configuration on the client? Then based on that information and the SAML information that we've provided and device posture, we can make decisions on whether or not Zscaler Internet Access is enabled, Zscaler Private Access, or Zscaler Digital Experience.

There are multiple use cases where we might only want to enable Zscaler Internet Access for a user and not Zscaler Private Access or Zscaler Digital Experience, or vice versa. And then based on those SAML authentications, SCIM provisioning, the SOAR solution, SIM solution, analyzing user access, we can build risk posture and we can pass that through and make decisions about whether the user is allowed to access applications through the Zero Trust Exchange, both public and private. We can understand if the device is managed or unmanaged and make policy decisions to allow access to applications.

And then also making decisions about how we inspect SSL traffic. What should we do about inspection? Should traffic be inspected or not? How do we handle errors with the original web server certificate? If it's unsigned, if it's invalid because of date or SNI (Server Name Indication) missing, do we pass that through, or do we just inherently block that connection?

The Zero Trust Exchange needs to have some information about how to authenticate the user. We're deploying the Zscaler Client Connector as we see in the top image. Or in the bottom image there, we're using browser-based access. If we install a Zscaler Client Connector with user domain and cloud name information, we'll automatically map to an identity provider and redirect the user to that identity provider to authenticate. That authentication could then be certificate-based, form-based, could be multifactor, could be transparent authentication.

## Single vs Multiple Identity Providers

Most organizations will have a single Identity Provider

During Mergers & Acquisitions, or Cloud Migration, multiple Identity Providers may be necessary

Configuration:

- Add IDPs - Add the IDPs in the Administration Configuration
- Configure Domain - Domains map Identity Providers to user domains
- Login - In Zscaler Client Connector or Browser Based Access, the user may be prompted to enter a credential
- Policy - The Policy maps the domain to the IDP. The user may be prompted, or the prompt may be bypassed through installer options in Zscaler Client Connector

With browser-based access, if there is a single domain associated with the browser application or the tenant, again, the user will be automatically redirected to the identity provider to authenticate. However, if multiple domains exist, then the user may be prompted to enter a credential to drive the decision criteria as to which identity provider we're going to redirect them to.

That's predicated on, do we have single identity providers or multiple identity providers? If only a single identity provider, the decisions are easy – redirect the user to the identity provider and authenticate them. But there are use cases, mergers and acquisitions, divestitures, cloud migration, a migration from an on-premises IdP such as ADFS (Active Directory Federation Services) to a cloud IdP such as a Zero AD, where a customer may have multiple identity providers. We need some amount of context to make a decision to which IdP to authenticate to.

The image displays two screenshots of the Zscaler administration console. The top screenshot shows the 'Authentication Settings' page, specifically the 'Identity Providers' tab. It features a table with columns for 'No.', 'ID', 'Name', 'Status', 'Location', 'IdP SAML Certificate ...', 'Authentication Domain...', and 'Default IdP'. Two entries are visible: one for ADFS and one for Azure. The bottom screenshot shows the 'IdP Configuration' page, which includes a table for 'Name', 'Status', 'IdP Entity ID', and 'Single Sign-On'. It also displays configuration details for ZPA (SP) SAML Request, SAML Attributes for Policy, and Authentication Domains.

No.	ID	Name	Status	Location	IdP SAML Certificate ...	Authentication Domain...	Default IdP
1	326618	ADFS	○	None	February 25, 2032	welshgeek.com	○
2	318751	Azure	●	Any	May 25, 2025	Any	●

Name	Status	IdP Entity ID	Single Sign-On	Actions
ADFS	●	http://adfs.welshgeek.net/adfs/services/trust	User	✎ ✕
AzureAD	●	https://sts.windows.net/fe4036f5-76ad-4232-9bda-313544c3ad54/	User	✎ ✕

ZPA (SP) SAML Request: Signed

HTTP-Redirect: Disabled

Single Sign-On URL: https://login.microsoftonline.com/fe4036f5-76ad-4232-9bda-313544c3ad54/saml2?whr=welshgeek.net

Force Authentication: Disabled

SAML Attributes for Policy: Enabled

Authentication Domains: welshgeek.net

Import SAML Attributes: Import

SAML Attributes: Show Attributes >



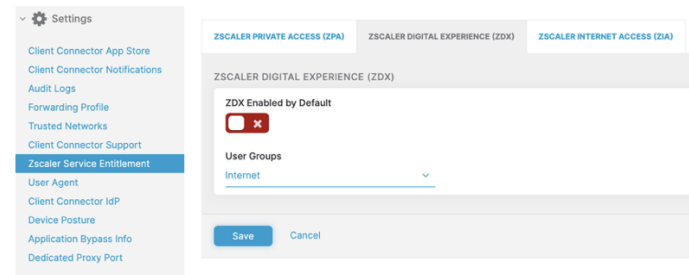
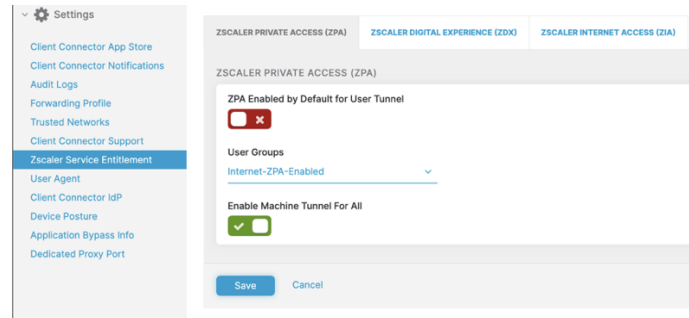
That might be based on the location the user is coming from. It might be a hint as far as the Zscaler Client Connector. It might be that the user is prompted to enter a credential which includes a domain into Zscaler and we use that to trigger the redirect to the identity provider. Obviously, we don't want to get in the way of a good user experience. If we can do anything to make the decision on behalf of the user, then the user experience is better. But there are times where we will have to prompt the user tool to enter something to redirect, but in most cases we can bypass that by putting some hints into the client or moving to a single identity provider environment.

## Service Entitlement

After authenticating to Zscaler Internet Access, the SAML attributes are consumed and passed to Zscaler Client Connector Portal, where the policy controls whether the user will be enrolled in Zscaler Private Access and Zscaler Digital Experience

Configuration:

- Add IDPs - Add the IDPs in Zscaler Internet Access
- Configure Group Attributes - which groups is the user in
- Set Entitlement Policy in Zscaler Client Connector Portal - Which groups are allowed access to ZPA or ZDX
- Alternatively - Policy set to Enabled by Default



The service entitlement can be based on user information (if the user is in a certain group), or we can enable it for all users.

Do we enable things like Machine Tunnel? With Zscaler Internet Access we can base that on device posture. We can understand the posture of the device as a managed or unmanaged device, making the decision of whether the user even gets enrolled into Zscaler Internet Access.

Zscaler Digital Experience has exactly the same context as Zscaler Private Access based on group attributes. Group attributes are synchronized from the authentication around a user to Zscaler Internet Access and then those groups are used for the entitlement policy for Zscaler Private Access or Zscaler Digital Experience.

SCIM attributes are synchronized periodically, and therefore flow periodically into the Zscaler Client Connector Portal. Or if we're just using SAML, those group memberships are transferred immediately through to the Zscaler Client Connector Portal for policy.

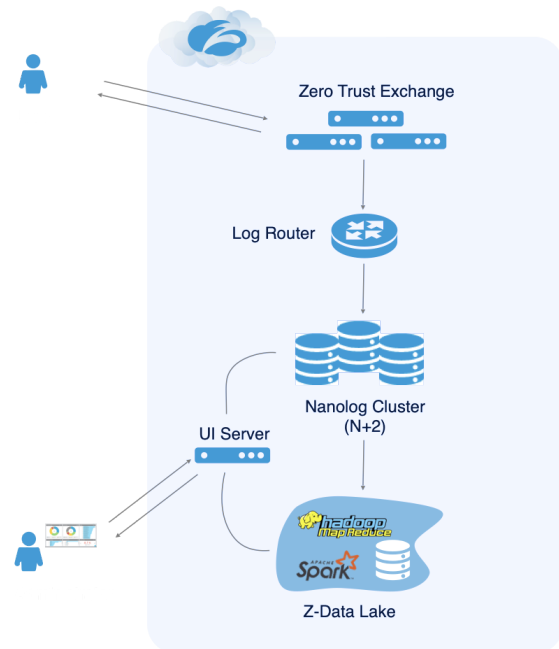
## Analytics & Reporting

The logging of all transactions as they pass through the Zero Trust Exchange is extremely important so that organizations are able to report on user activity and perform analytics that make decisions for future policy.

### Logging Architecture

The logging architecture is for when the user makes a transaction through the Zero Trust Exchange, it passes logs through a log router which decides where those logs will be stored.

Those logs may also feed into the Zscaler data lake that does more analytics and reporting, and then an administrator connects to the UI server that queries both the log clusters as well as the data lake to produce the reporting and analytics that they want.



There's role-based administrator control to access the UI server that might restrict what users are able to see in terms of certain locations, certain data types, and whether or not user information is obfuscated from their reports with the Four Eyes Principle. Zscaler put a lot of engineering effort into making logging as efficient as possible as well as reducing the payload so we're not passing data between all of our nodes.

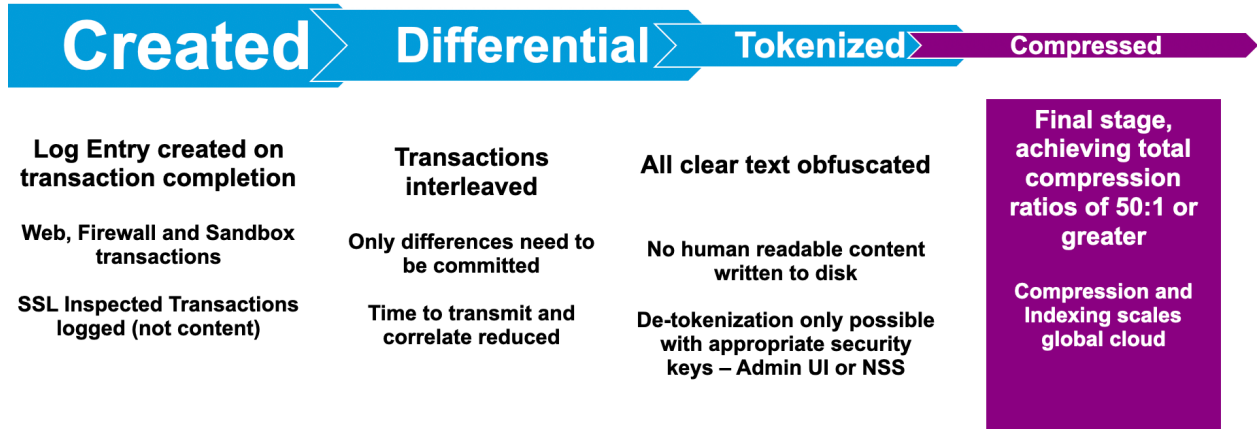
A log entry is created on a transaction completion for Web (including SSL transaction), Firewall and Sandbox transactions are logged. As content passes through an enforcement node is never stored, only processed and forwarded. And the content (payload) is never stored, only the transaction is logged.

The Zero Trust Exchange can also stream log data to SIEM and SOAR solutions for long term storage, and enable business & security policy to be implemented programmatically. Zscaler's API's enable these solutions to make Zero Trust policy changes based on the log stream data, or DevSecOps processes.

Every single transaction is logged, but only those that are different are stored, adding to the overall efficiency. By reducing the amount of data that's being passed, the time to transmit those logs from all of the Zero Trust Exchange service points back to the logging infrastructure is reduced.

Then the data is tokenized on the ZIA Public and Private Service Edges, and ZPA Public and Private Service Edges so that, again, the amount of data is reduced while making sure that that data isn't human-readable.

## ZIA - Nanolog Data Reduction



Having been both reduced and tokenized, it is compressed and sent to the log servers for storage. The end result is 50-to-1 or greater compression rate as well as all of that indexing happening at the point that the log is created so that when the logs are consumed they are very efficient to analyze,

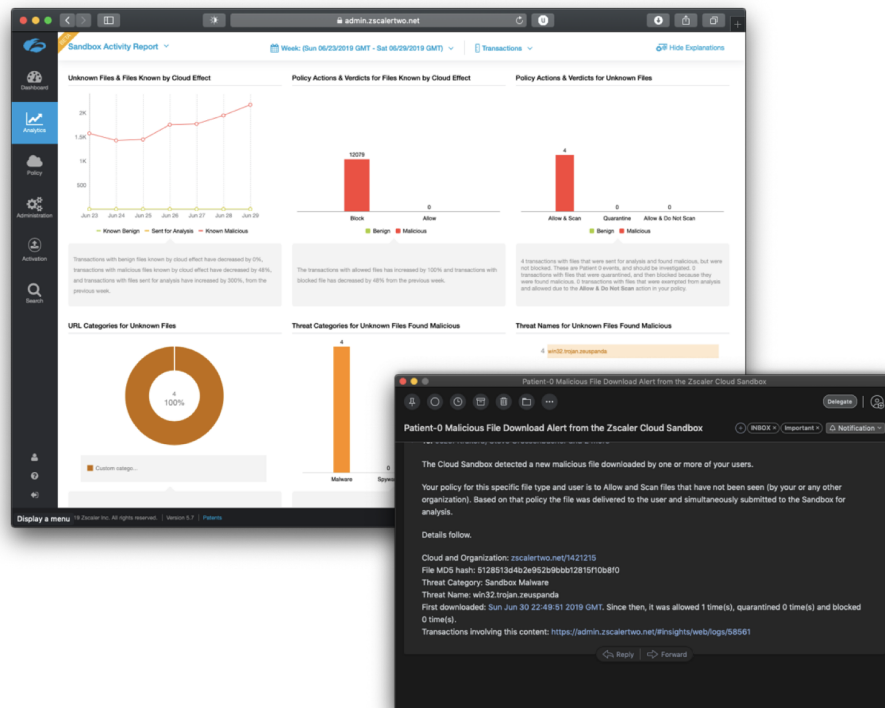
## Big Data Outputs

This enables the creation of big data output via interactive reports, meaning that you can drill down into individual transactions. Whether it's SSL and certificate reports, URL category reports, dashboards showing the company risk score, security audit reports, or threat insight reports, the data and value is easy to extract.

Trending data analysis across the platform and comparing your organization's capabilities with industry standards or other organizations in the same industry as you further helps you understand how traffic flows through the platform from your users and where the applications they're accessing are.

For the executive needs, the Zscaler Executive Insights tool enables executives to instantly get reports on how Zscaler is helping their business, how they're reducing the number of threats coming into the organization, and where they compare to peer organizations and cloud risk scores.

For the threat hunting teams out there, there are even deeper forensic reports, historical sandbox data, and detailed information on patient zero potential infections.



## Zscaler Digital Experience

Digital Experience will introduce you to Zscaler's digital experience monitoring capabilities. Gain an overview of Zscaler's digital experience monitoring capabilities that work to analyze, resolve, and troubleshoot user experience issues. Dive deeper into the components of Zscaler Digital Experience, along with how to configure, monitor, and troubleshoot these features and functions as they relate to Zscaler best practices.

---

By the end of this chapter, you will be able to

1. **Recognize** why a new approach is needed for monitoring user experience and how Zscaler works to provide this visibility to organizations through the Zero Trust Exchange.
2. **Explore** the Zscaler Digital Experience (ZDX) features and functions Zscaler has in place to proactively identify and resolve performance issues.
3. **Recognize** why a new approach is needed for monitoring user experience and how Zscaler works to provide this visibility to organizations through the Zero Trust Exchange.
4. **Explore** the Zscaler Digital Experience (ZDX) features and functions Zscaler has in place to proactively identify and resolve performance issues.

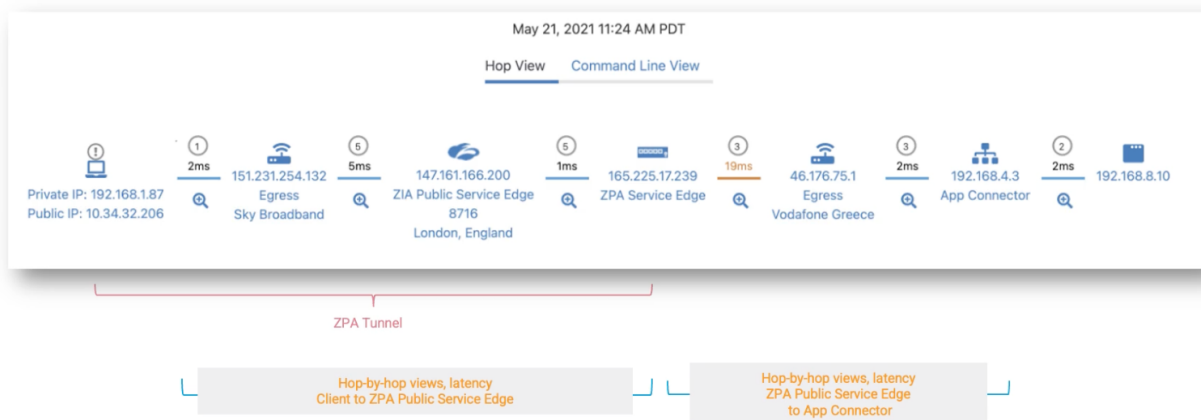
## Introduction to Zscaler Digital Experience

### ZDX Overview

The rapid adoption of cloud and mobility initiatives within organizations and a shift to work-from-anywhere have introduced new monitoring challenges for IT teams. Digital experience monitoring for a hybrid workforce requires a modern and dynamic approach, as IT teams need to continuously monitor and measure the digital experience for each user from the user perspective, regardless of their location.

Traditional monitoring tools take a data center-centric approach to monitoring and collecting metrics from fixed sites rather than directly from the user device. This approach does not provide a unified view of performance based on a user device, network path, or application.

Zscaler provides this unified view through our Digital Experience monitoring solution that sits on top of the Zero Trust Exchange. Zscaler Digital Experience (ZDX) helps IT teams monitor digital experiences from the end user perspective to optimize performance and rapidly fix offending application, network, and device issues.



The power of ZDX is being able to use these calculated scores in order to drill into issues when a score seems to be visibly low. What, however, might cause a good score to go down? The items below highlight the common issues every organization must face:

<p><b>App Issues</b></p>	<p><b>DNS</b></p>	<p><b>App Availability</b></p>
<p>App issues would typically be seen in the <b>Page Fetch Time</b> (PFT) and <b>Server Response Time</b> (SRT) metrics.</p>	<p>Many customers still use sub-optimal DNS that could result in higher overall latency.</p>	<p>The application is not available and users are seeing 5xx errors.</p>
<p><b>Local Wi-Fi</b></p>	<p><b>Device Events</b></p>	<p><b>Network Congestion</b></p>
<p>Local Wi-Fi based signal strength or Wi-Fi &lt; - &gt; egress latency. Example: 2.4 Ghz instead of 5Ghz</p>	<p>Check for device events for bad score triggers: Example: VPN tunnel interface, Wi-Fi change, system restart, etc..</p>	<p>Network congestion would surface as latency, Wi-Fi, or high bandwidth utilization.</p>
<p><b>Device Metrics</b></p>	<p><b>Egress Latency</b></p>	
<p>CPU/memory spikes (or held at 100% translate into slower client (ex. browser) response time and leads to bad user experience.</p>	<p>Latency up to Zscaler: Sub-optimal routing or ISP issues.</p> <p>Latency at Zscaler: High CPU/Traffic on node or ISP issue.</p> <p>Latency between Zscaler and application: If latency going direct is better and this is a trend, notify cloud ops.</p>	

### ZDX Features & Functionality

Zscaler's Digital Experience solution provides many features and functionalities that work to deliver the benefits of:

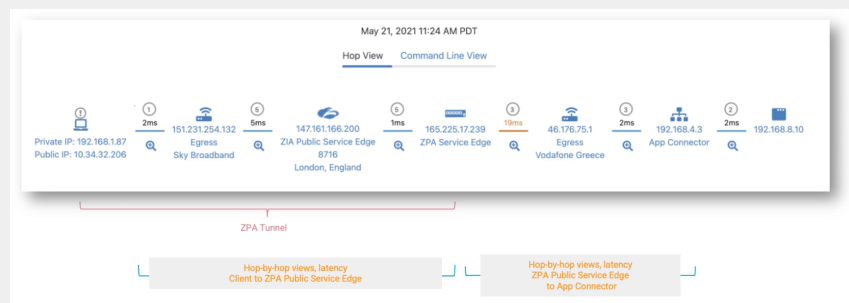
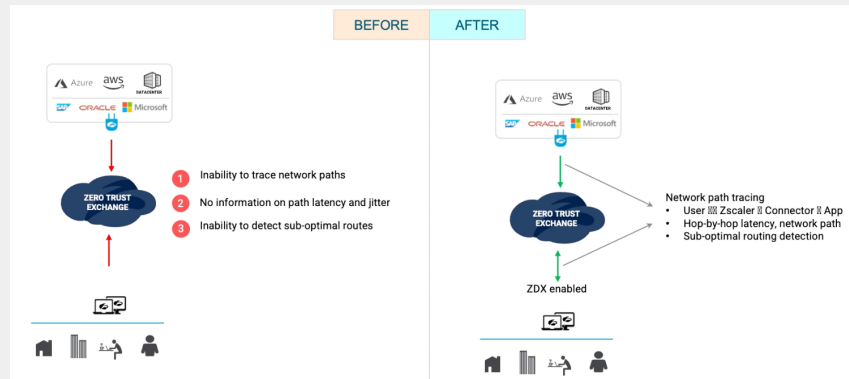
- Being the first to know when the user experience degrades
- Rapidly resolving performance issues
- Ensuring application performance
- Gaining comprehensive network insights
- Getting detailed device insights



Here are just 5 of the key features that are commonly utilized:

### Visibility into SaaS & Private Applications

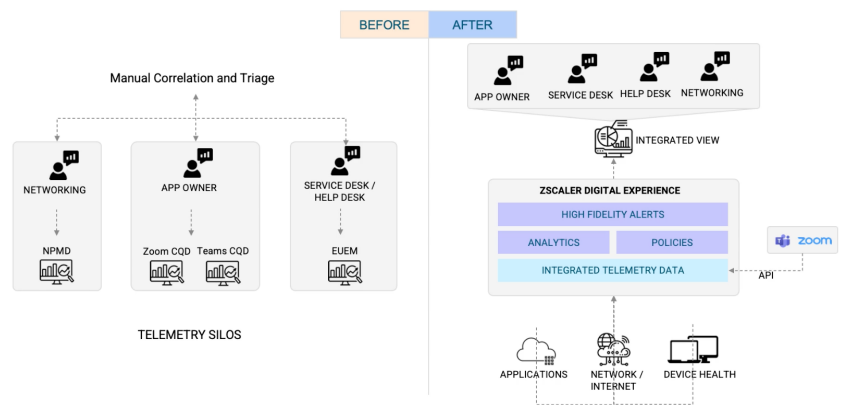
ZDX provides visibility not only into an organization's zero trust environments but into their private and SaaS applications as well.

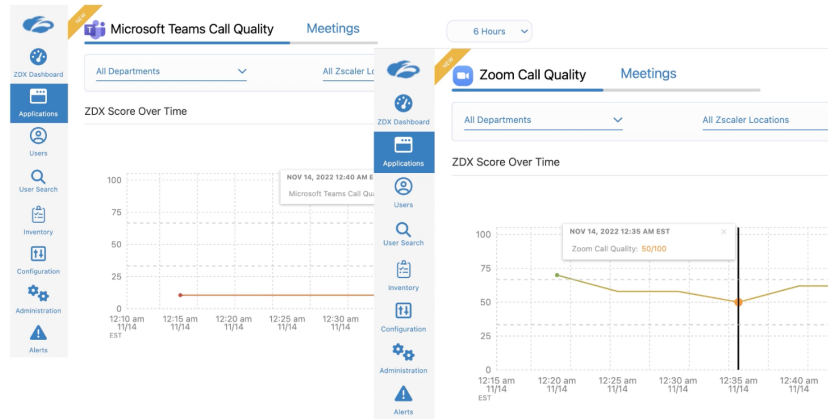


### Unified Communication as a Services (UCaaS) Monitoring

UCaaS Monitoring enables organizations to quickly gain insights and troubleshoot performance issues with Microsoft Teams and Zoom.

#### Bringing One Integrated View for Monitoring UCaaS Services





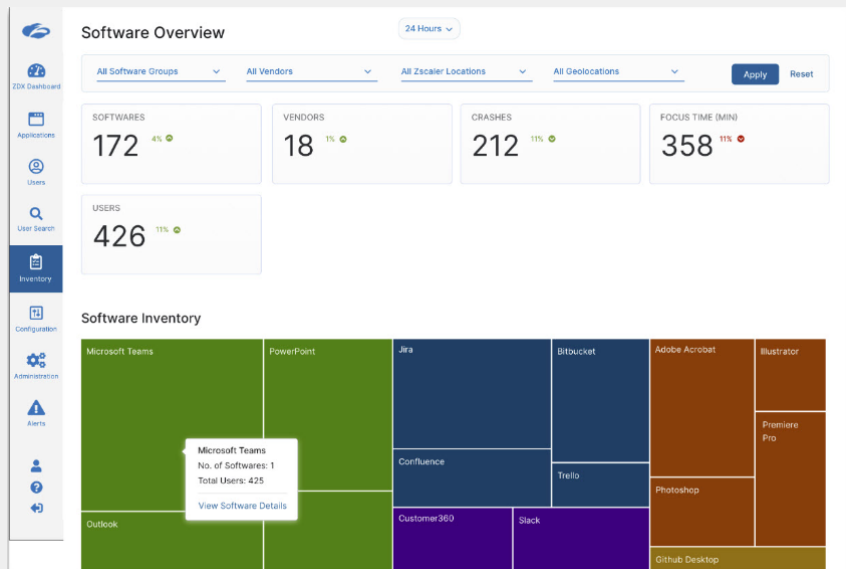
## Software & Device Inventory

Software and Device Inventory is based on the different endpoint metrics that Zscaler collects from the user's device.

A User's device and the software versions it is running plays a major role in the user experience. It is helpful to know if the device in the organization is running the latest OS, Patch, or Software Version. For this purpose, ZDX has both Software and Device Inventory.

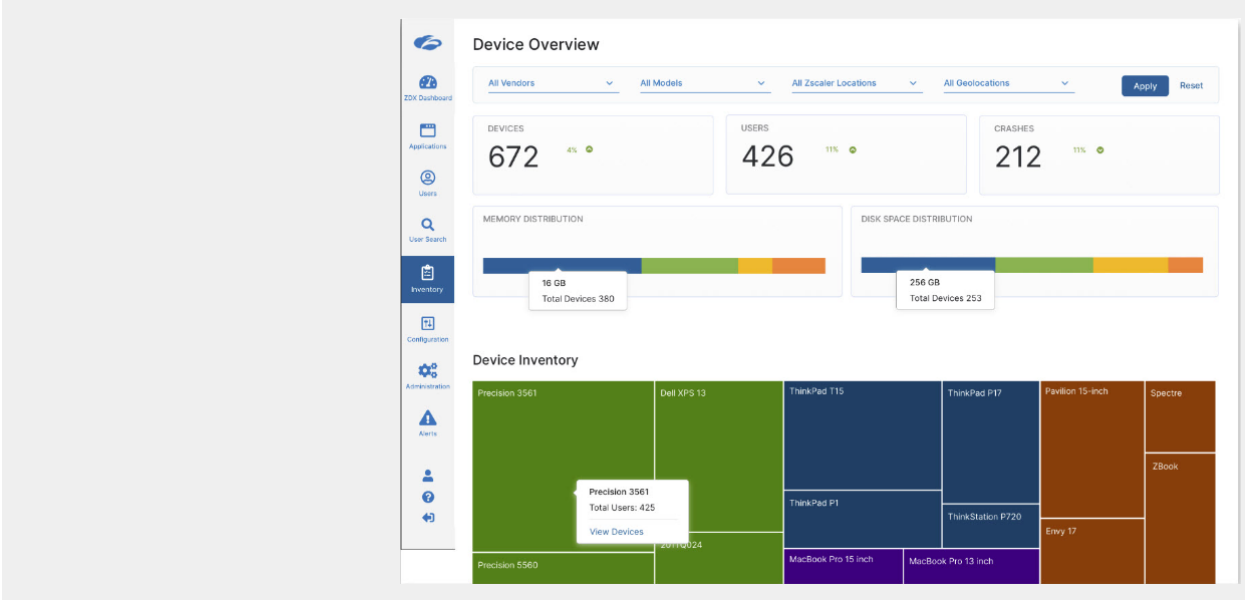
### Software Inventory

Software Inventory allows you to view current and historical information about software versions and updates on your users' devices.



### Device Inventory

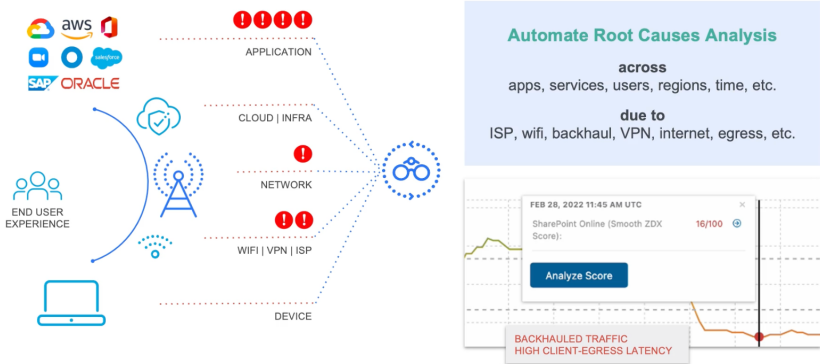
Device Inventory allows you to view current information about your organization's devices and their associated users.



Y-Engine (Automated Root Cause Analysis)

ZDX's Y-Engine (Automated Root Cause Analysis) allows an organization to automatically isolate root causes of performance issues, spend less time troubleshooting, eliminate finger-pointing, and get users back to work faster.

**ZDX Y-Engine Automates Root Cause Analysis**



ZDX APIs

ZDX's APIs integrate digital experience insights with popular ITSM tools like ServiceNow to provide additional insights and trigger remediation workflows.

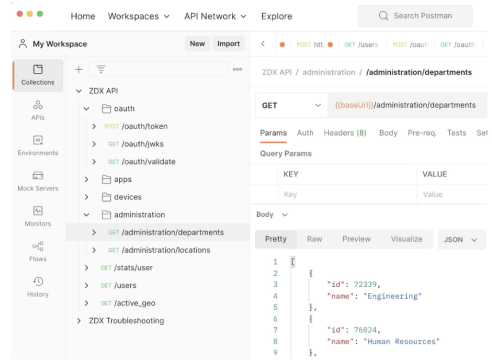
## ZDX APIs

Optimize resource allocation and ensure compliance

- Access ZDX data to get more insights for specific scenarios
- Useful for integration with third-party platforms like ITSM (ServiceNow) & AIOps (Moogsoft)

### API Endpoints

Auth	Reports
Configuration	Users Applications Devices
Troubleshooting Deeptrace ML-based RCA	Administration Location Department

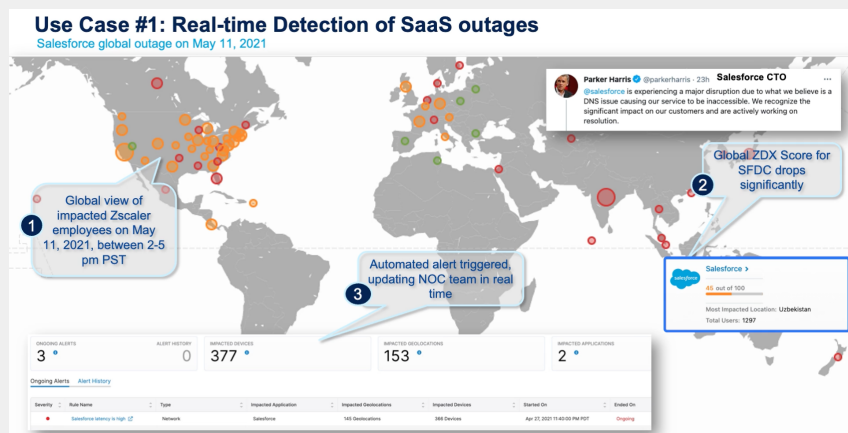


## ZDX Use Cases

Did you know that hybrid work has increased ticket resolution time by 30%? Did you also know that almost 70% of businesses rely on virtual meetings (according to Metrigy research)?

Zscaler addresses both of these use cases and more with its powerful end-user monitoring capabilities. Here are just six common use cases that ZDX addresses:

### Real-time Detection of SaaS Outages



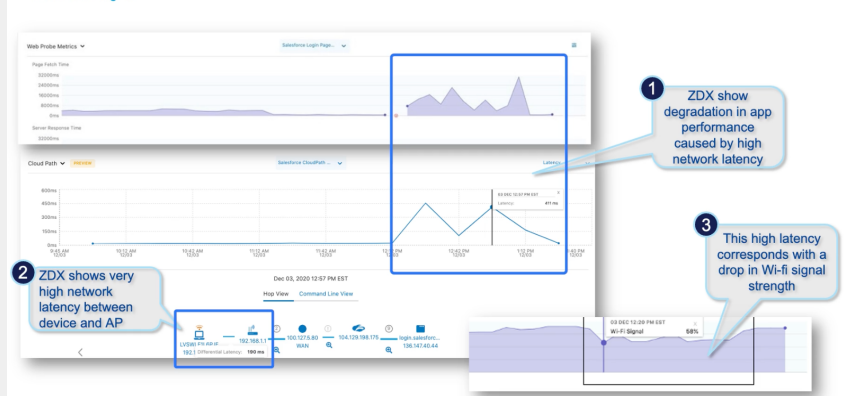
## Baselining Performance Between Office and Working from Anywhere

### Use Case #2: Baselining Performance Between Office and Working from Anywhere



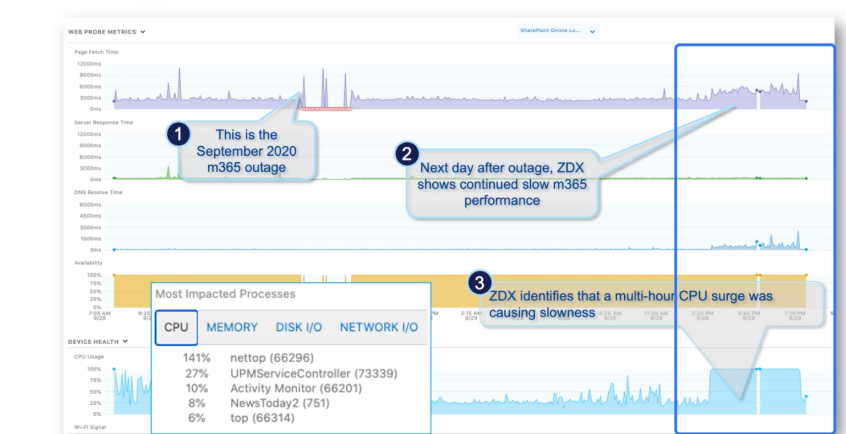
## Detecting Employee Home Wi-Fi Issues

### Use Case #3: Detecting Employee Home WiFi Issues



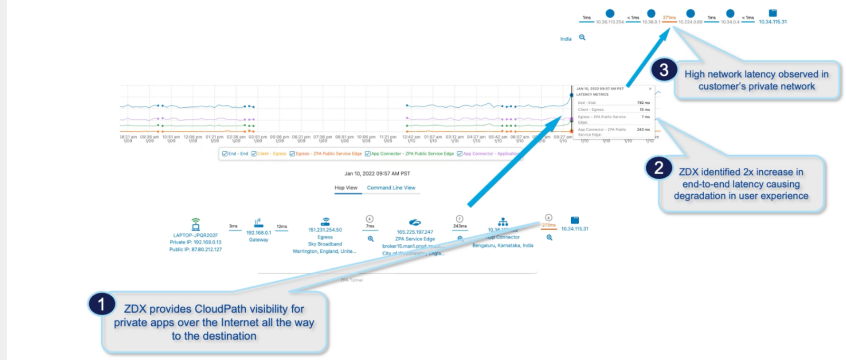
## Detecting High CPU Causing Application Degradation

### Use Case #4: Detecting High CPU Causing Application Degradation



# Visibility into Private Applications via ZPA

## Use Case #5: Visibility into Private Applications via ZPA



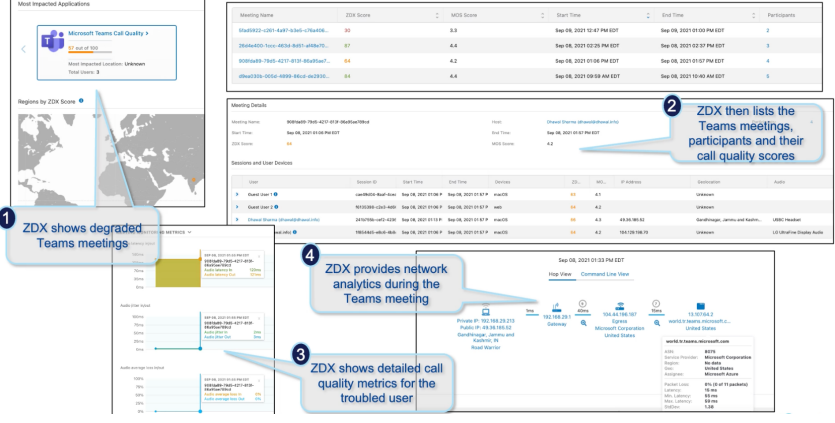
1 ZDX provides CloudPath visibility for private apps over the Internet all the way to the destination

2 ZDX identified 2x increase in end-to-end latency causing degradation in user experience

3 High network latency observed in customer's private network

# Call Quality Monitoring for Microsoft Teams and Zoom

## Use Case #6: Call Quality Monitoring for Microsoft Teams and Zoom



1 ZDX shows degraded Teams meetings

2 ZDX then lists the Teams meetings, participants and their call quality scores

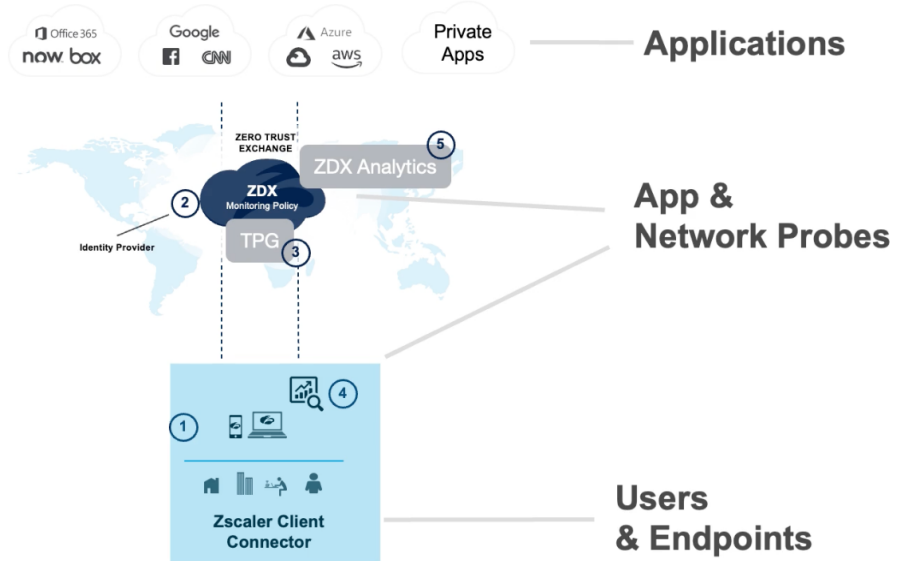
4 ZDX provides network analytics during the Teams meeting

3 ZDX shows detailed call quality metrics for the troubled user

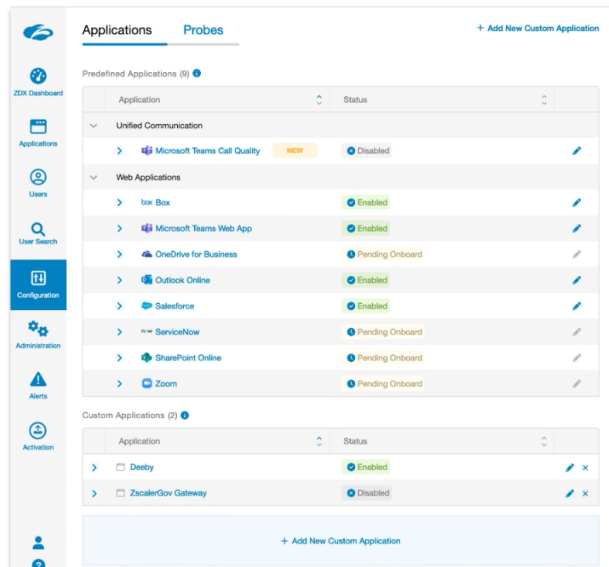
## ZDX Architecture overview

Understanding the basics of ZDX's architecture is important as it will help you to more clearly navigate, configure, and troubleshoot the various features, functionalities, and issues that arise within the Digital Experience console.

Once a monitored application is configured in ZDX it is sent to the client, which then probes the application at 5 minute intervals. That data is then sent to the **Telemetry and Policy Gateway (TPG)** which is then sent to the **Analytics Engine** where it feeds into the **ZDX Dashboard**.



Applications come as **predefined** or **custom**. Those that are predefined have minimal configuration needs, which are usually along the lines of providing the tenant ID, while custom applications require at least one web probe created.



**Predefined Applications:** Predefined applications are available in the ZDX Admin Portal when you log in. The predefined applications provide quick and seamless application onboarding for admins.

**Custom Applications:** Customizable SaaS or web applications that you can create and onboard in the ZDX Admin Portal for your organization.

## Probes

### Web Probe

**Web Probes** always pull objects from the server and are used to collect metrics like:

- **Page Fetch Time** - network fetch time for the specified URL
- **DNS Time** - time it took to resolve the DNS name
- **Server Response Time** - time to the first byte
- **Availability** - is the service available, yes or no

**Edit SharePoint Online Login Page Probe**

1 Configure Probe 2 Additional Parameters 3 Review

WEB PROBE CONFIGURATION

Probe Name	Application Name
SharePoint Online Login Page Probe	SharePoint Online

Request Type  
GET

Destination URL  
https:// m365x167135 .sharepoint.com

Request Header

Name	Value
------	-------

+ Add More

HTTP Response Status Codes

Type to add new

- Informational responses (100-199) x
- Successful responses (200-299) x
- 300 Multiple Choices x

+ HTTP Status Codes for successful availability

Number of Attempts: 1

Timeout (seconds): 60

Follow Redirect: Enable

Maximum Redirects: 5

### Cloud Path Probe

**Cloud Path Probes** discover the network elements of the application, basically what are the network hops the user is taking on the way to the application.

Metrics collected include:

- **Hop Count**
- **Packet Loss** - for each hop
- **Latency Information**

Protocols include:

- **Adaptive** - the best protocol for each leg in the cloud is selected by an auto-discovery process
- **ICMP** - default value, processed by router CPU
- **TCP** - processed by router ASIC, immune to rate limiting
- **UDP** - some routers only respond to UDP packets, RFC recommended port of 33434

**Copy SharePoint Online CloudPath Probe**

1 Configure Probe 2 Additional Parameters 3 Review

CLOUD PATH PROBE CONFIGURATION

Probe Name	Application Name
Copy of SharePoint Online CloudPath Probe	SharePoint Online

Protocol: Adaptive

TCP Port: 443

UDP Port: 33434

Packet Count: 11

Interval (ms): 1000

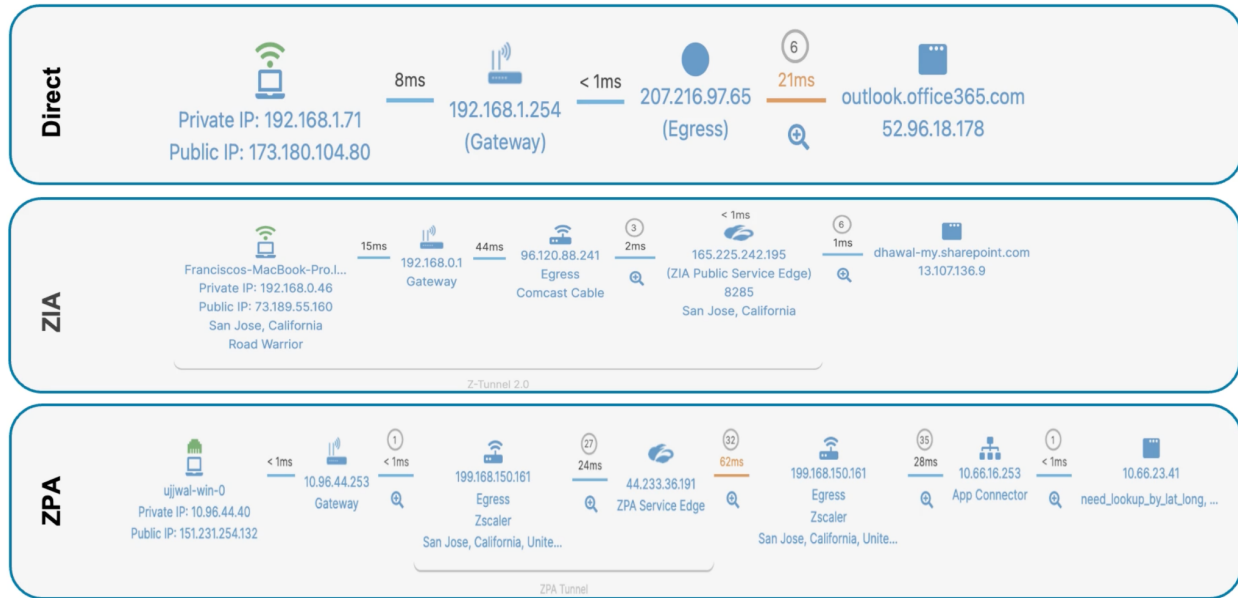
Timeout (ms): 1000

Cloud Path Host: m365x167135 .sharepoint.com



As the data from the Cloud Path Probe is collected, administrators and support staff have deep visibility and insight at their fingertips, greatly reducing resolution time for existing issues and even preventing future ones.

## What is Cloud Path - Common Scenarios

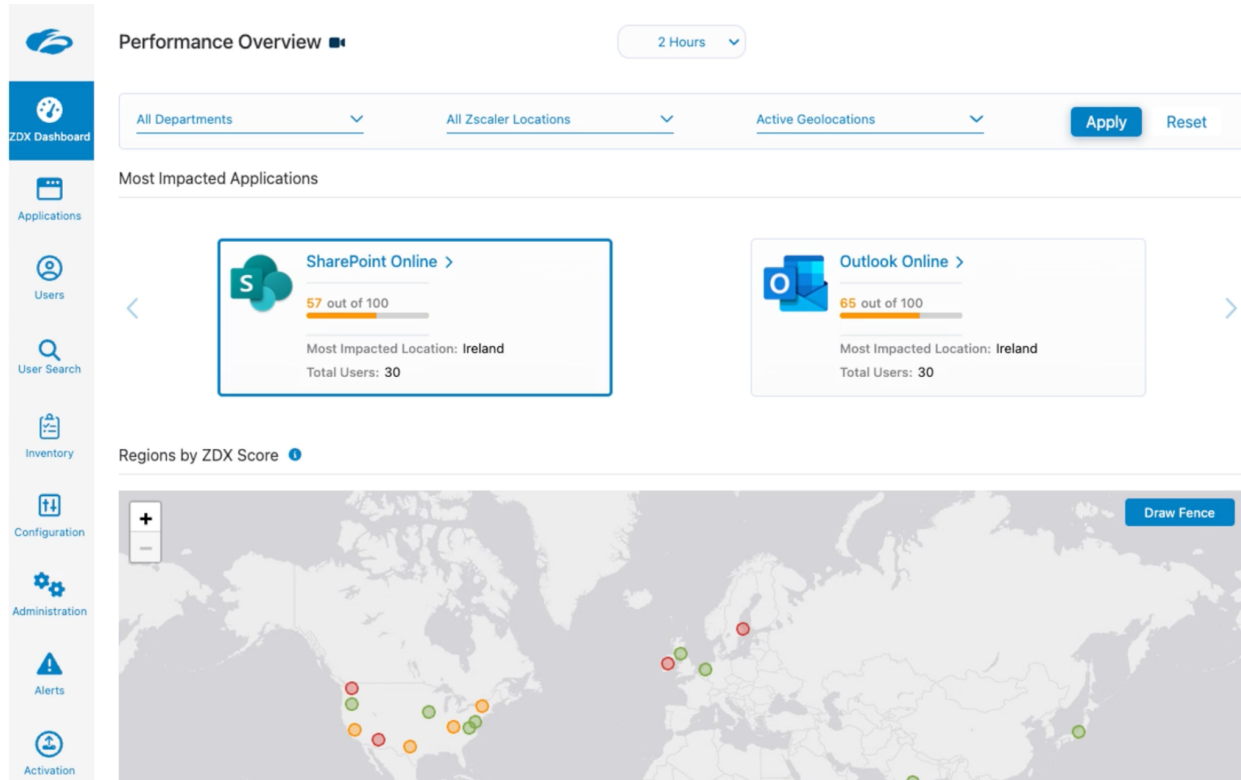


## Command-Line View

IP	Address	Hop	Direction	Service Provider	Region	Geo	ASN	Assignee	Packet Loss	Packets Failed/	Differential	Average	Min.	Max.	StdDev
1	192.168.0.46	-	Client	-	San Jose, California	US	-	-	-	-	-	-	-	-	-
2	192.168.0.1	↓	Egress	Comcast Cable	-	United States	7922	Comcast Cable	0%	0/11	15	15	2	115	31.46
3	96.120.88.241	↑	Egress	GTT Communication...	-	United States	3257	GTT Communication...	0%	0/11	44	59	43	75	7.58
4	141.136.105.130	↑	Egress	GTT Communication...	-	United States	3257	GTT Communication...	0%	0/11	2	2	1	12	3.05
5	173.205.44.93	↑	Egress	Zscaler	-	United States	22816	Zscaler	0%	0/11	0	0	0	2	0.66
6	165.225.242.2	↑	Egress	Zscaler	San Jose, California	United States	22816	Zscaler	0%	0/11	0	0	0	0	0
7	165.225.242.195	↓	Egress	Zscaler	-	United States	22816	Zscaler	-	-	-	-	-	-	-
8	165.225.242.3	↓	Egress	Zscaler	-	United States	22816	Zscaler	0%	0/11	0	0	0	0	0
9	206.223.177.603	↓	Egress	Microsoft Corpo...	-	United States	-	-	27.27%	3/11	1	1	0	8	1.94
10	104.44.43.156	↓	Egress	Microsoft Corpo...	-	United States	8075	Microsoft Azure	0%	0/11	0	1	1	8	1.48
11	104.44.238.239	↓	Egress	Microsoft Corpo...	-	United States	8075	Microsoft Azure	0%	0/11	0	1	1	2	0.29
12	No Response	↓	Egress	-	-	-	-	-	100%	11/11	-	-	-	-	-
13	No Response	↓	Egress	-	-	-	-	-	100%	11/11	-	-	-	-	-
14	13.107.136.9	↓	Application	Microsoft Corpo...	Redmond, Washington	United States	8068	Microsoft Azure	0%	0/11	0	1	1	1	0

## Monitoring Digital Experience

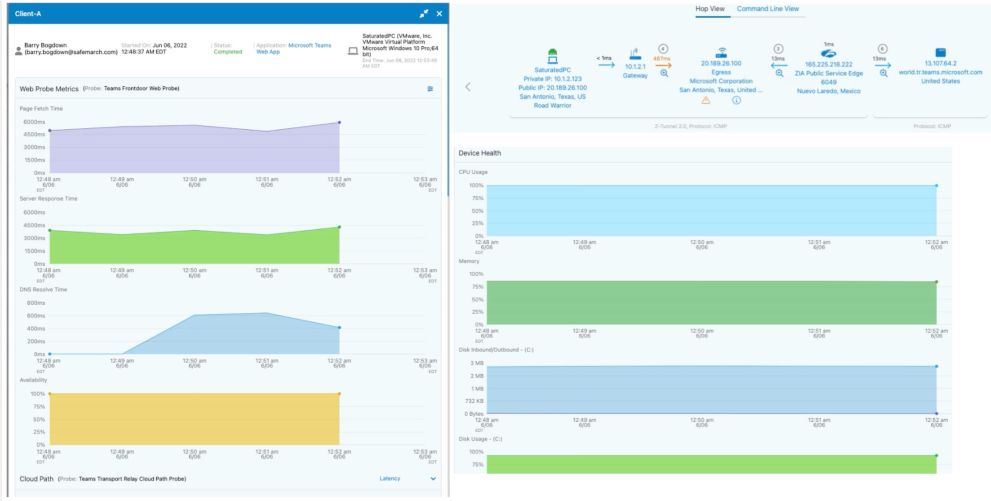
The ZDX dashboard provides an overview of the application performance and user experience, providing filters to focus on any scenario that might arise. Each application shows a **ZDX Score**, based on the selected time range, where the probes act on the user's behalf so there is not need for them to interact with the application to generate the data that drives the dashboard.



## Top Troubleshooting Administrator Experiences

**Deep Tracing** Collects more information about the user's device. Instead of 5-minute intervals (the default), administrators can run an on-demand deep trace on the user's machine, targeting a specific application.

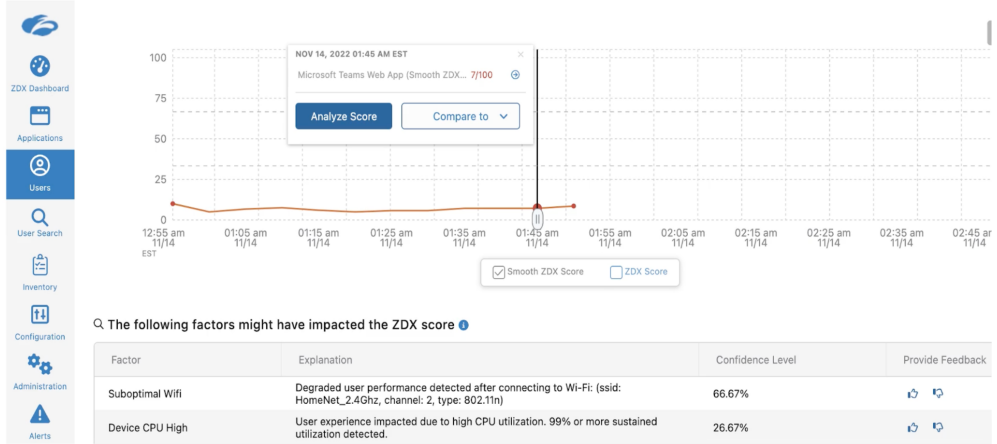
# Troubleshooting with ZDX (Deep Tracing)



# Y-Engine

Helps you get to the root cause of a problem quickly, automating your root causes analysis for the impacted ZDX Score.

## Y-Engine (Single Point Score) Automate Root Cause Analysis

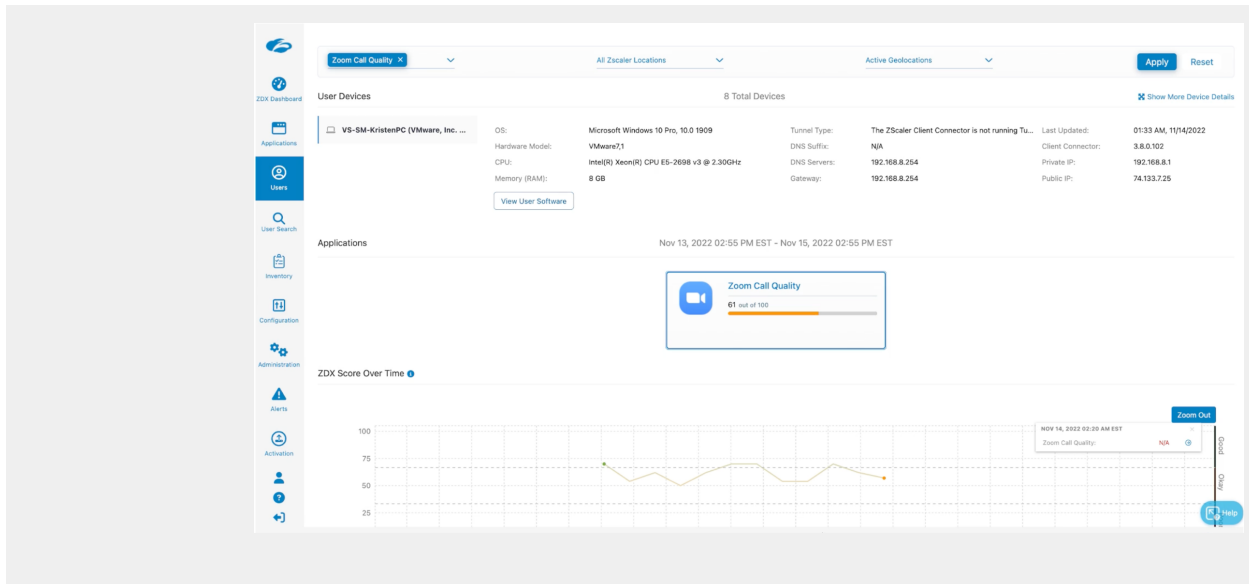


This includes the ability to compare the same data point to past ones.



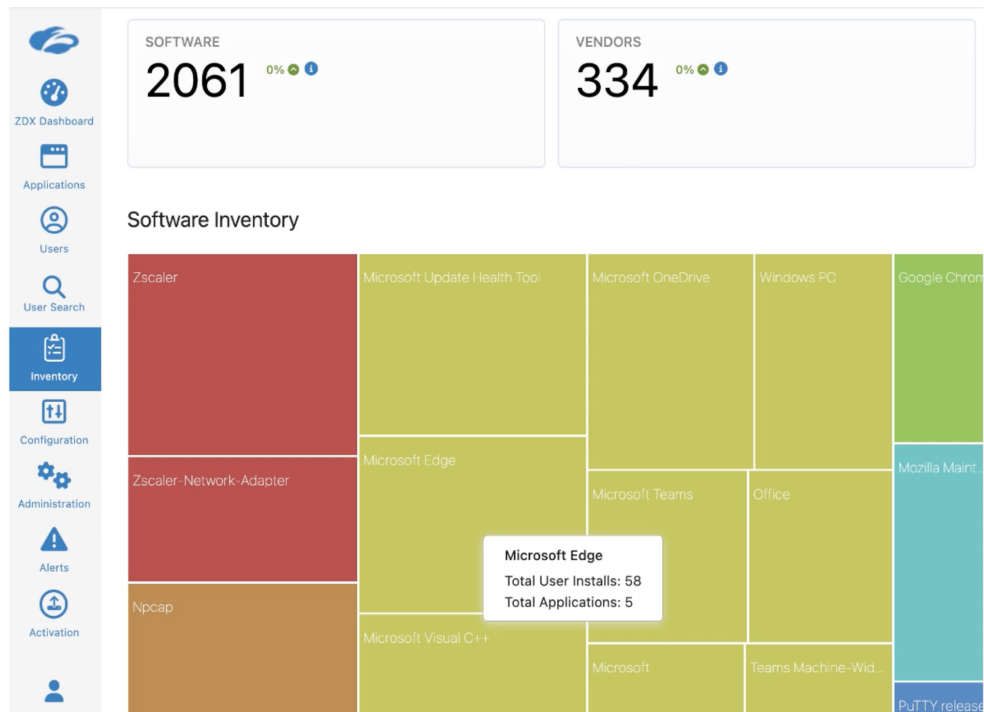
# UCaaS Monitoring

Monitoring and looking at call quality for users (Zoom, Teams) over time, with the ability to focus on specific meetings (participants, locations, devices...)



**Software & Device Inventory**

Provides the ability to drill down all the way on a specific user or device to learn what software is present, at what level, to help correlate if a specific software or devices might be impacted.



## Access Control

Access Control Services extend segmentation and policy control with capabilities such as Firewall, DNS, URL Filtering, and more. In this chapter we extend segmentation and policy controls to understand how the Zero Trust Exchange applies policy for applications, as well as how the Zero Trust Exchange handles DNS and shortest-path selection for application experience optimization.

Gain an overview of Zscaler's Access Control capabilities, dive deeper into specific policy controls for applications, and gain knowledge on how to configure Zscaler's Access Control Services as they relate to Zscaler best practices.

---

By the end of this chapter, you will be able to

1. **Identify** why traditional firewalls fall short of protecting and preventing enterprises from having effective and efficient access control policies and how Zscaler solves these challenges.
2. **Recognize** the Access Control Services Zscaler has in place to protect internet and SaaS-based applications.
3. **Define** how Zscaler's Access Control capabilities and policies protect end users when accessing private applications.
4. **Discover** how to configure Zscaler Access Control Services and capabilities.
5. **Recognize** Zscaler's Customer Support Services and Touch Points.

## Access Control Overview

### The challenge of legacy firewalls

Traditional legacy on-premise firewalls are no longer suitable in a world where users require access to the corporate network anywhere, anytime, on any device.

The challenge is that legacy firewall appliances are zone-based architectures. They establish barriers between trusted internal and untrusted external networks, where user policies and criteria are made available. This poses three main risks for organizations around security, performance, and cost and complexity.

Here are the common **LEGACY FIREWALL** risks and their consequences:

Security	Performance	Cost & Complexity
Broad network access	Performance drops with TLS inspection and threat prevention	Increases cost to turn on full stack security
Unwanted lateral movements	Scale - Cannot sustain peak ramp rate	Onus on customer harden and penetration test
Fall short at preventing compromise	Long-lived connections to apps - consume available ports	High cost of maintenance and operations
Increased attack surface	Availability - Downtime due to patching and maintenance (both planned and unplanned)	

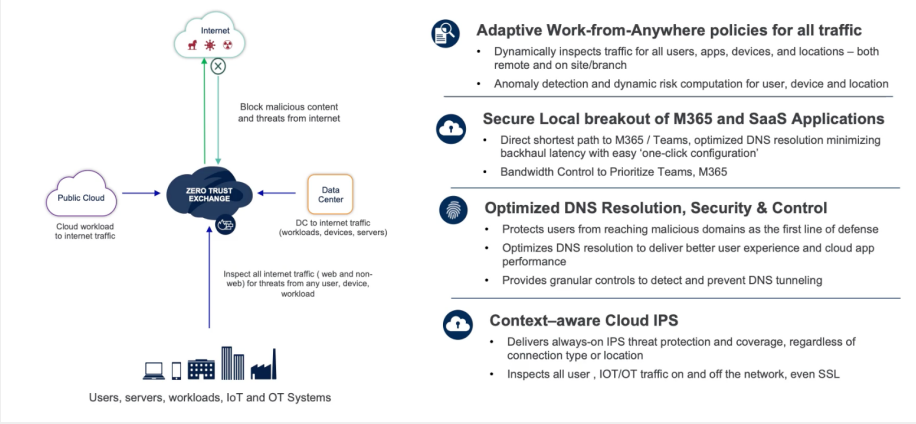
Zscaler solves these challenges through its holistic approach to providing a platform of services that enables organizations to bring true zero trust to every endpoint - whether a user, application, or IoT device.

Firewall

The Zscaler Cloud Firewall is a NextGen firewall that provides complete control over all ports and protocols as well as applications and/or services for all Zscaler users regardless of location or device type. As previously described, the Zscaler Cloud Firewall provides unlimited scale and is not hampered by the limitations of legacy hardware.

Here are the three most important use cases which **cloud generation firewalls** enable enterprises to benefit from.

**Cloud Firewall Use-Cases**



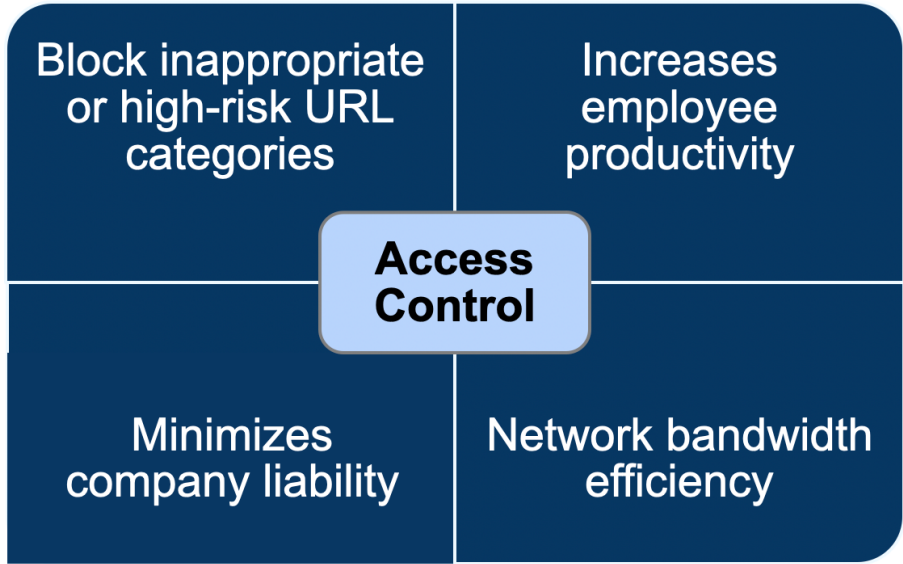
The **first and foremost use case** is being very adaptive and consistent when it comes to accessing applications – no matter where you are – especially post-COVID, with hybrid work becoming the common norm for all enterprises. Making sure customers get the same stack of next generation firewall capabilities and security irrespective of their location is very critical. As mentioned earlier, traditional on-premises appliances have inconsistent security postures configured because they have to handle the remote users in different policies and different appliances, versus what is there on the physical sites or premises of branch offices.

The **second key use case** is for customers to migrate from their hub-and-spoke architecture to more direct-to-internet architecture for making their most important SaaS applications like M365, Salesforce, and other key applications more secure. It is very important to have a product with capabilities which can completely identify, have visibility, and prevent all sorts of threats from an access control perspective.

And the **third use case** is whenever an end user is trying to access an application over the internet, DNS plays a critical role. Optimizing and securing DNS acts as a first line of defense for many enterprises to prevent half of the threats right at the DNS level itself. And the most important capability from an NG (next generation) firewall perspective

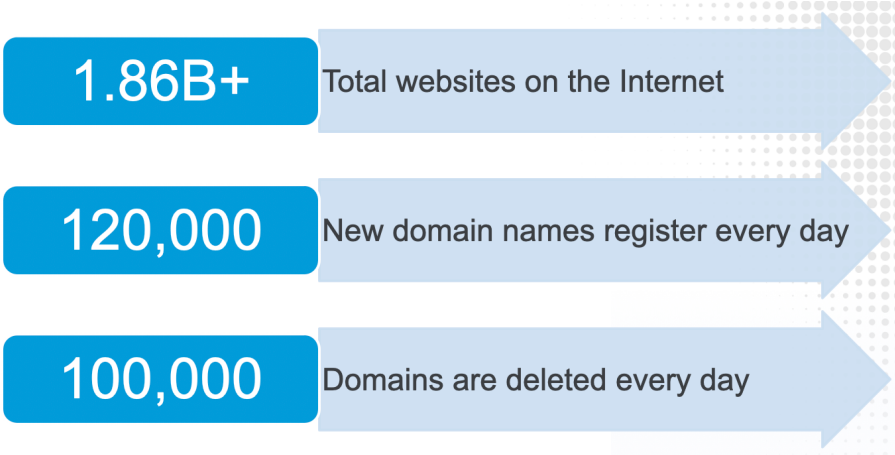


	<p>is to provide a scalable cloud intrusion prevention and detection, which has complete context.</p> <p>Further supporting these use cases are a wide range of architectural features and benefits:</p> <ul style="list-style-type: none"> <li>● Proxy-Based Firewall Architecture</li> <li>● Dynamic, Risk-Based Access Policy (Cloud Device Posture)</li> <li>● Granular, Context-Aware, <b>Cloud IPS</b> for all Web &amp; Non-Web Applications</li> <li>● APIs for Cloud Firewall Management</li> <li>● Granular Policy Control</li> <li>● Dynamic Application Services</li> <li>● Detailed Logging &amp; Reporting</li> </ul> <p>And of course a whole list of best practices for each of these.</p>
<p>URL Filtering</p>	<p>URL Filtering is the first line of defense that an organization needs to leverage in order to provide effective and efficient access security control for users. This allows those enterprises to:</p> <ul style="list-style-type: none"> <li>● <b>Restrict</b> basic content that a user or endpoint may be trying to access</li> <li>● <b>Protect</b> the end users from accessing inappropriate or harmful web content while browsing the web</li> <li>● <b>Boost</b> employee productivity and performance by restricting access to certain types of applications and destinations within the internet</li> </ul> <p>Let's discuss the top use cases in which enterprises deploy URL Filtering or are leveraging this capability.</p> <p>The <b>basic use case</b> is it starts with basic access control with deeper granularity. Like different departments, different users need to access certain websites but not others. So it acts as a simple access control mechanism based on the business needs, on who should access what content, from which device, and from which location they can access the content.</p>



The **second top use case** we are increasingly seeing is new websites getting added. Oftentimes it is very difficult for any platform to quickly identify whether a website is good or bad because a lot of these websites are registered and there isn't any content. By the time you flag a website as good, there is a possibility that the content is bad. Bad actors have leveraged that domain for posting and used it for phishing and other suspicious activity. So the key use case is when there is a certain notion of whether a destination is safe or unsafe.

That is where the isolation of web pages is very critical for customers. Oftentimes, things are not white or black, they could be gray, which means the categorization cannot be done immediately or more time is needed to flag it as a genuinely good website or something harmful. It involves a certain time and a certain amount of insights to really get to that categorization.



**Another top use case** is device OS-based policies. A lot of organizations have the need to provide access control based on

certain supported operating systems of endpoints, and those use cases can be easily handled as well.

Additional basic URL filtering use cases include:

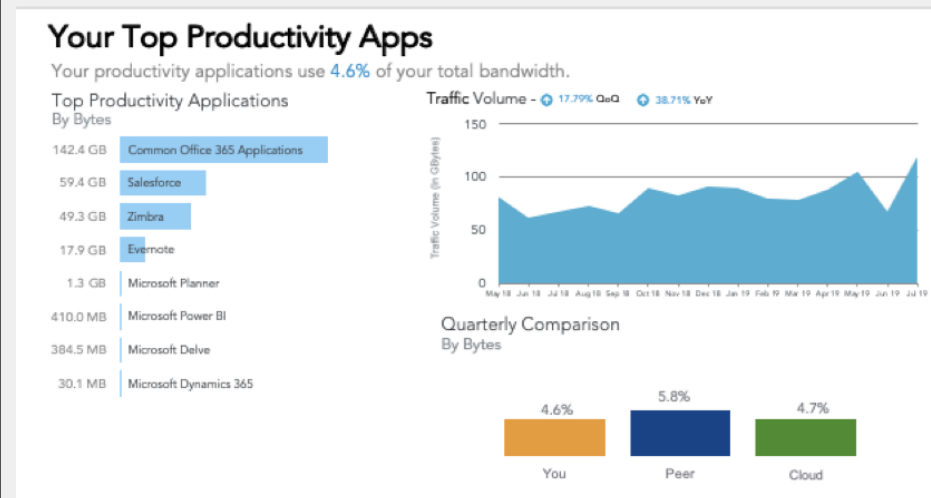
- Cautioning Users
- User-Agent Based Policies
- Time-Based Policies
- Time-Based Policies
- Rule Expiration
- Bandwidth Quota Supported

As well as various Advanced URL filtering use cases:

- AI/ML Content Categorization
- SafeSearch
- CIPA
- Embedded Sites Categorization
- Newly Registered & Observed Domain Lookup
- Block Override

## Bandwidth Control

Bandwidth Control is one of the core capabilities of Zscaler's services from an access control perspective ready to provide secure connectivity to the internet and private applications.



Five common use cases for Bandwidth Control:





1. Need to improve performance of productivity apps (O365, Salesforce, etc.) in some or all locations
2. Need to limit bandwidth consumption by non-productivity apps (YouTube, Facebook, Netflix, etc.)
3. Need to limit bandwidth for non-productivity apps during working hours only

- 4. Need to limit bandwidth for Windows and iOS updates
- 5. Need to limit bandwidth for certain applications in branch locations only

Microsoft Office 365 (M365)

By leveraging various Access Control Services already discussed including URL Filtering and Bandwidth Control as well additional Platform and Connectivity services such as TLS Inspection, Policy Framework, and the Zscaler Client Connector, the Zscaler Zero Trust Exchange is able to enable organizations to deploy M365 and ensure an optimized user experience.

**Issues with the traditional model for Office 365 traffic**

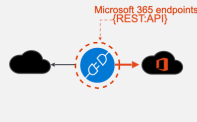

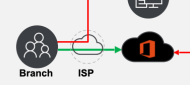

Exchange Online	Microsoft Teams	SharePoint Online & OneDrive for Business	Office and Windows updates
			
Latency due to distance and operations	Traditional proxies don't handle User Datagram Protocol (UDP) traffic	Additional persistent connections by client	High update frequency
Outlook requires multiple TCP connections per user (5-10)	Additional persistent connections by client	Large amount of data movement	Risk of bandwidth saturation due to repeated downloads for each machine
Designed for transient rather than persistent connections	Teams media traffic prefers UDP for transport	Same destination IP used for all connections	Microsoft 365 app updates range from about 100-500 MB and can be numerous each year depending on channel
	Media traffic can add high load		

Just focusing on the load on firewalls and proxies:

- Office 365 creates a high number of long-lived sessions that quickly exhaust firewall ports (we've seen 12-20 connections per user)
- Around 2,000 clients can be supported by a single public IP safely (may require architectural changes)
- Office 365 use will require more than Web browsing (ports 80/443) — uses ephemeral ports

With legacy approaches, user experience will surely be impacted, such as random hangs and connection issues (Outlook in a disconnected state)

## Microsoft 365 network connectivity principles

 <p><a href="https://aka.ms/o365ip">aka.ms/o365ip</a></p>	 <p>Datacenter Branch</p>	 <p>Branch ISP</p>	
<p><b>Optimize Microsoft 365 traffic</b></p> <p>Use the endpoint categories to differentiate Microsoft 365 traffic from generic internet traffic for more efficient routing.</p>	<p><b>Enable local egress</b></p> <p>Egress Microsoft 365 data connections through internet as close to the user as practical with matching DNS resolution.</p>	<p><b>Enable direct connectivity</b></p> <p>Enable direct egress for Microsoft 365 connections. Avoid network hairpins and minimize network latency (RTT) to Microsoft's global network.</p>	<p><b>Modernize security for SaaS</b></p> <p>Avoid intrusive network security for Microsoft 365 connections. Assess bypassing proxies, traffic inspection devices, and duplicate security already available in Microsoft 365.</p>

The best practice is to:



**Provide direct access to M365**

Enable local internet breakouts and remove VPNs



**Stop backhauling and hairpinning**

Eliminate costly and slow MPLS connections



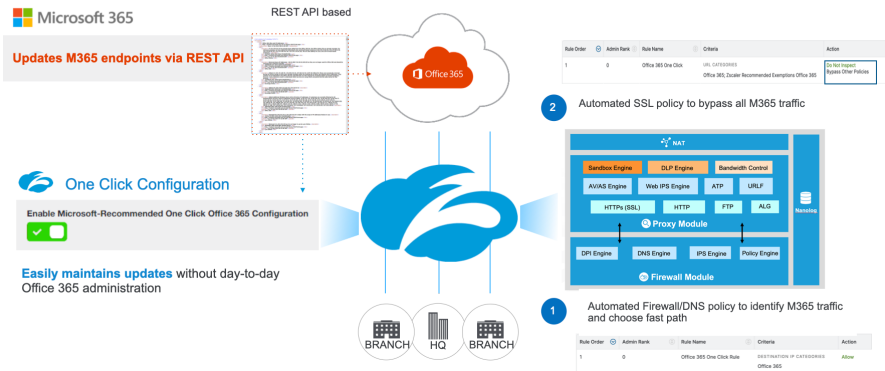
**The optimal path to M365**

150+ global edge locations includes direct geographic peering

And of course enabling...

## Zscaler One Click Configuration

Simplify day to day Office 365 administration



## Segmentation & Condition Access through Policies

Zscaler's Private Application Access securely makes connections into an organization's private applications regardless of the user's location and device.

Zero trust is at the heart of our approach to application access, ensuring a user is not brought onto a corporate network and can only access the applications they need and are authorized to access.

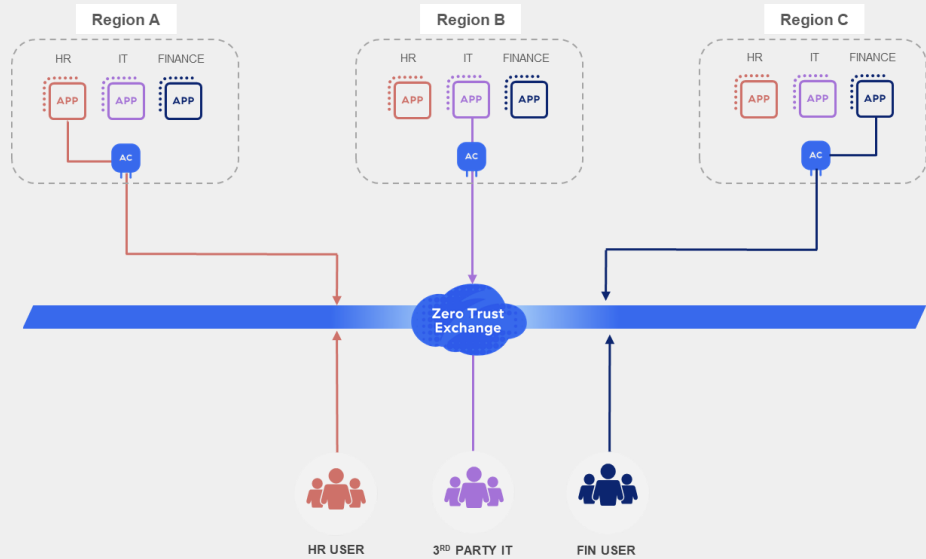
### Why Segmentation?

Segmentation limits the network access only to the application or resource required. Contrast to traditional VPNs that provide access to all resources on the network when the user or device connects.

Eliminates discovery of applications not granted access to.

Segmentation uses policies to provide conditional access when the application is requested. Policies are based on:

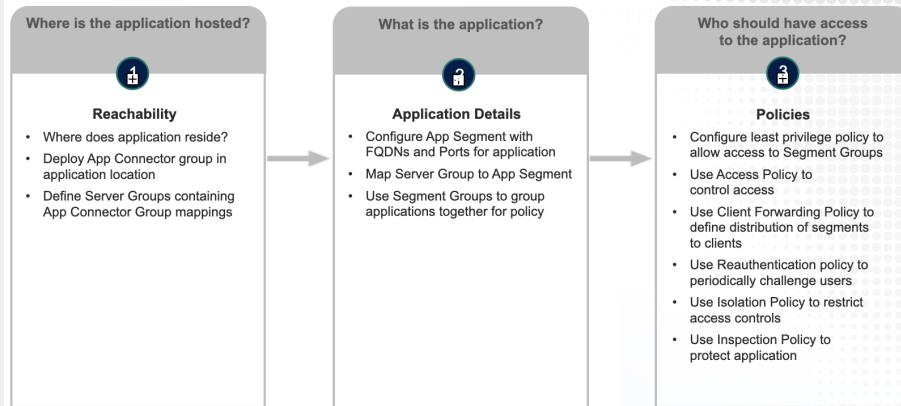
- **Identity** — is the user who they say they are?
- **Device posture** — Is the device secure?
- **Access** — Should the user have access to the application?



The core use cases for leveraging Private Application Access connections and segmentation are:

1. Remote Access
2. Third Party Access
3. Segmentation
4. Mergers & Acquisitions (M&A)
5. Transformation

### Overview of configuration steps for secure private application access



### 5 steps for segmenting applications



## Cybersecurity Services

Go deep into the essential security capabilities of the Zero Trust Exchange. The Zero Trust Exchange is fundamentally a security platform, and in this chapter, we will explore its traffic inspection capabilities and how Zscaler's Single-Scan, Multi-Action functionality optimizes the inspection of traffic. We will also learn about how deception works in a zero trust environment. You will get an overview of Zscaler's cybersecurity and protection capabilities, dive deeper into Zscaler's advanced threat protection and antivirus as part of the Zscaler security service suite, and learn how Zscaler provides detection and response through its alerting framework.

---

By the end of this chapter, you will be able to

1. **Explain** what cybersecurity is, how attacks happen, and how Zscaler holistically stops them.
2. **Identify** Zscaler's advanced threat protection capabilities and demonstrate the steps in Threat Protection ZIA configuration.
3. **List** common malware types and identify how Zscaler protects against malware attacks.
4. **Identify** how Zscaler provides detection and response capabilities built into the ZIA offering.



## Cybersecurity Overview

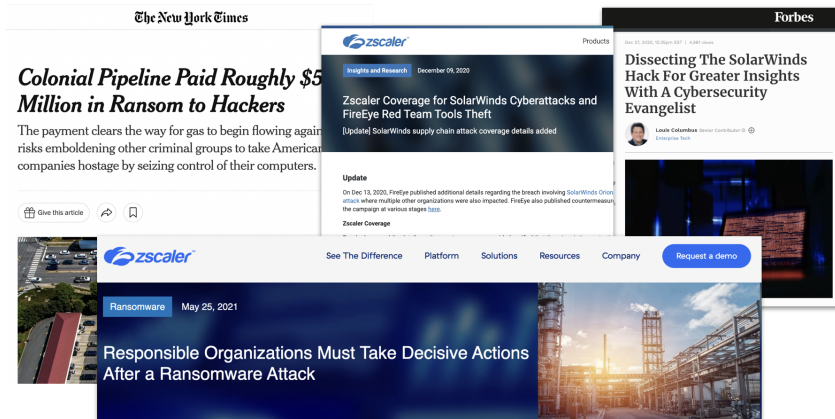
Cyberattacks are becoming more and more common. Attackers' techniques are becoming more sophisticated as ransomware, phishing, malware, and other attacks hit one after the other.

More than ever, it is critical for every organization to have a set of cybersecurity services that analyze organizational risk and defend against cyberattacks so they can rest assured they will not be compromised.

Zscaler solves these challenges through a holistic platform of services that stops these attacks before they can cause harm.

Before diving into what cybersecurity functions Zscaler provides and how they should be configured, let's look at a clear overview of:

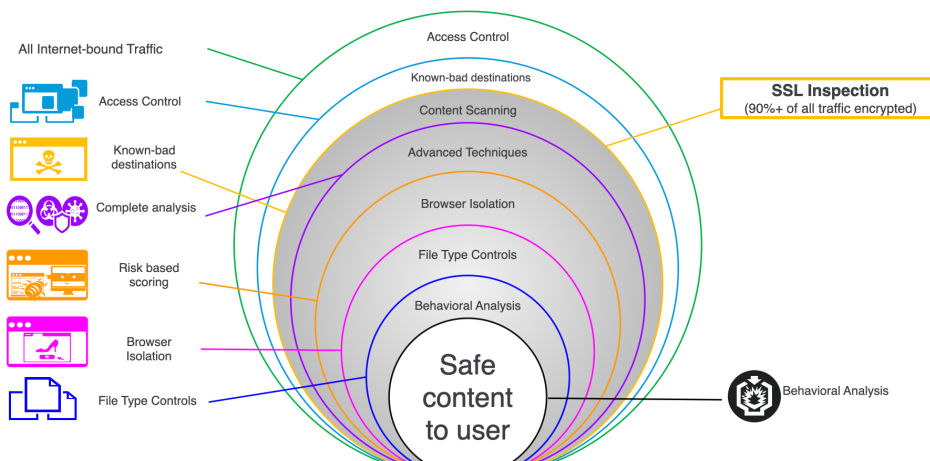
- How cyberattacks happen
- What different types of attacks can occur
- How the Zscaler Zero Trust Exchange Platform holistically comes together to stop these attacks



To start, we should understand how frequently these attacks occur. A significant data breach makes the news at least every few months. For instance, we recently heard about the data breach at companies like Twilio. The above are some examples of notorious attacks like

Colonial Pipeline and SolarWinds.

### Layered approach to threat and malware protection



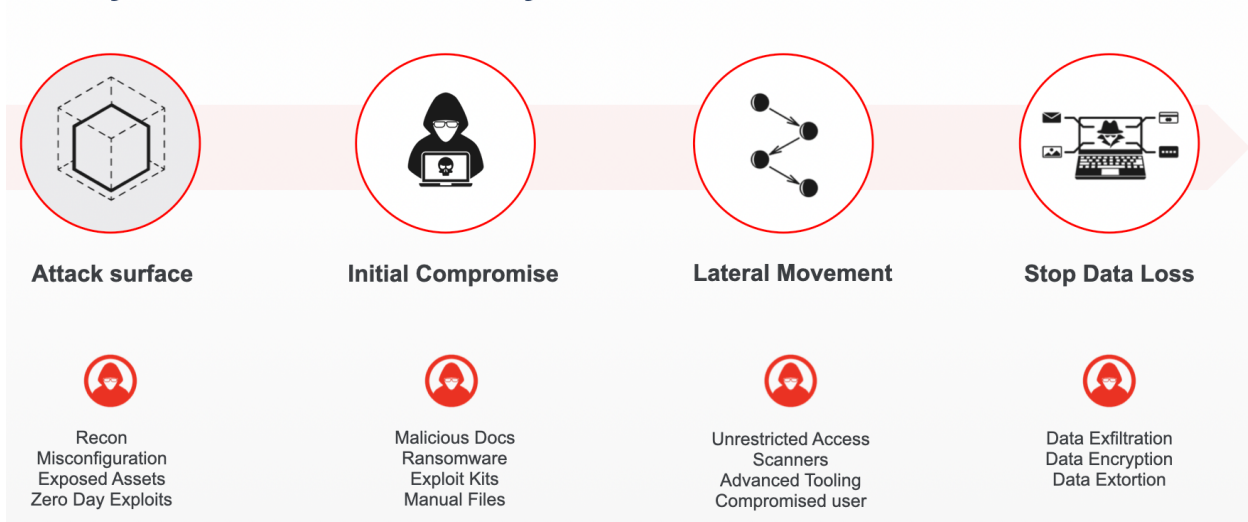
These attacks have started happening more often, and they are becoming more sophisticated, changing the shape

of both the cyberthreat and cybersecurity landscapes.

To understand the current cybersecurity landscape and some of the problems our customers are facing, it is important to understand three points:

1. Attackers are increasingly using automation, and it has become exceedingly easy for just anyone to launch an attack. Many attacks, the Colonial Pipeline attack for instance, use ransomware-as-a-service, where ransomware is run on demand by a third party. Many attacks also involve credential theft, including phishing, often done using phishing kits, which are widely and readily available for any popular productivity suite, like Microsoft 365. With these premade kits and services, you don't have to be an expert at coding to launch these attacks.
2. Over the last decade, many enterprise customers have invested a great deal of money in cybersecurity, steadily acquiring multiple best-of-breed products to stop advanced attacks. Unfortunately, acquiring many different point products creates operational complexity, and integration is often difficult. Context is not shared across these products, so it's fragmented, making it difficult for anyone to get the full picture of threats, in addition to creating the third problem, the adoption gap.
3. The adoption gap has been an issue for some time, but when you have multiple point products, it gets compounded. Generally, you have a lot of technical debt when you're replacing a legacy product with the next-generation product. After replacement, you have inertia to move away from that technical debt, compounded even further when your point products don't talk to each other. Attackers take full advantage of this adoption gap: for instance, a lot of these attacks happen with customers using VPN products.

## Every attack has the same story

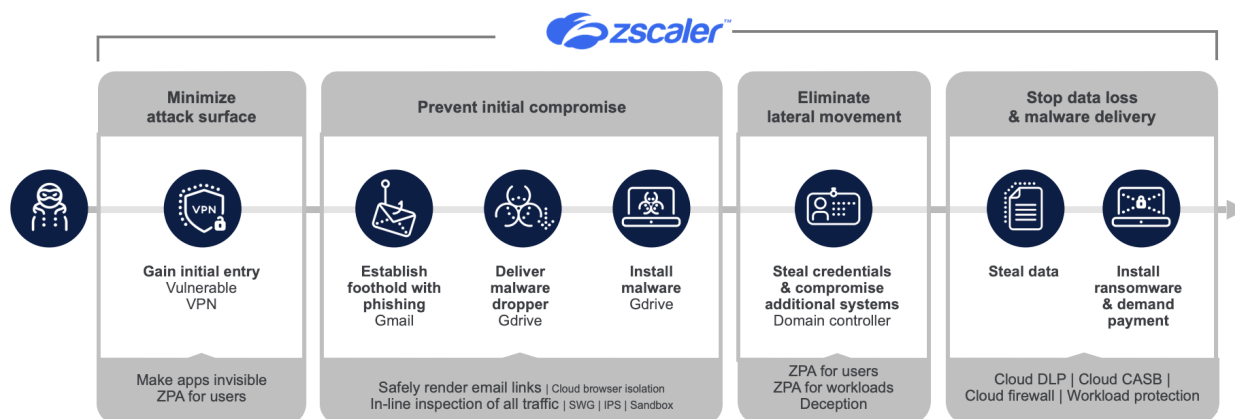


If you focus on attacks, they all have basically the same story. The MITRE ATT&CK framework breaks down 12 different stages of an attack, but you can simplify it into the above four high-level stages.

The first stage is about the attack surface. Attackers are looking for exposed endpoints. These could be your exposed public servers, your VPN users etc. Once attackers have found the attack surface, they can use different techniques to execute their initial compromise. This is where they may send a phishing document or spear phishing email. They'll try to lure victims to a website where they can download a malicious file, or perhaps the website itself is running active malicious JavaScript. Once they succeed and land on a target system, the first thing they want to do is find your most critical and sensitive data and assets.

Attackers want to move laterally to identify those, and they can do this in various ways. If your network or environment is not segmented, or if your applications are otherwise exposed, it becomes very easy for them. They can use techniques like “living off the land” to find out what your most sensitive assets are. Once they get to those assets, they start stealing data. For example, in the case of ransomware, they can use the stolen data in a “double extortion” attack, where they encrypt your data in addition to exfiltrating it, giving them extra leverage.

Any attack, from advanced supply chain attacks to ransomware, can be mapped to this simple framework. Now, let’s look in a little more detail at how this manifests in an attack, and the specific Zscaler products that can stop attacks at these stages. Suppose an attacker has gained initial entry using a vulnerable VPN.



Once the attacker has gained initial entry, then they move on to the initial compromise, where they will establish some level of foothold with spear phishing or broad credential phishing. They may deliver malware using an innocuous looking .docx file with a malicious macro inside it. As soon as the user opens or installs this file, the malware installs itself. At that point, the attack can start moving laterally. It may use techniques like malvertising or keylogging to steal credentials, or start figuring out what and where your other sensitive assets are, such as your domain controllers.

In one of these attacks, attackers found out a specific domain controller held passwords for other domain controllers or other infrastructure. That is what they used to do privilege escalation. Once they do that, the next phase is to steal the data, and after they have made that theft of data, the next thing is that they will install this ransomware and demand payment. So this is a good example of how ransomware attacks proceed. Now, you can also see underneath what are all the different capabilities that come together to stop this.

In our attack surface, we have ZPA capabilities. To prevent initial compromise we have a lot of our ZIA capabilities around secure web gateway, IPS, Cloud Sandbox, and Cloud Browser Isolation. Again, to eliminate lateral movement, we have ZPA for users, we have ZPA for workloads, we have our Deception capabilities. And, last but not least, to stop data loss, we have our data protection capabilities around cloud DLP, cloud CASB, and Workload protection. So, now that we have understood how a lot of these attacks happen, what is the right approach to stopping a lot of these attacks?

There are three elements mapping this out.

- First and foremost, we believe the right way to solve these attacks is a platform approach. Now, you may hear the platform approach from everyone out there in the industry, but when we say a platform approach, it means a very adaptive platform. It means a platform that is scalable, that can inspect SSL at scale for all your users, without you having to worry about how much of the traffic can you decrypt. It has to be a platform that supports APIs where you can signal into the platform and signal out of the platform, which makes it very programmable, and it has to be a platform that uses AI and ML to learn constantly to adapt itself to the most sophisticated attacks and deliver the most superior outcomes.
- The second thing that I want to talk about is an automated and integrated platform. Any product that has to solve cyber security challenges today has to do both of these. Essentially, we want to deliver accelerated outcomes for our customers by leveraging automation and reducing the time it takes to detect and respond. Integration means that we should be able to integrate with other products that a customer has acquired over the last few years. We should be able to talk to their SIEM. We should be able to talk to their EDR products. What we mean by automation is when we find out that something or a specific endpoint or system is malicious, how do we quickly quarantine it? How do we signal across the entire platform that this specific user is a compromised user and we need to limit further damage?

## The right approach to stopping attacks



### Adaptive Platform

A platform that is scalable, programmable and learns to deliver superior outcomes



### Automated & Integrated

Deliver accelerated outcomes by leveraging automation to reduce time to detect & respond

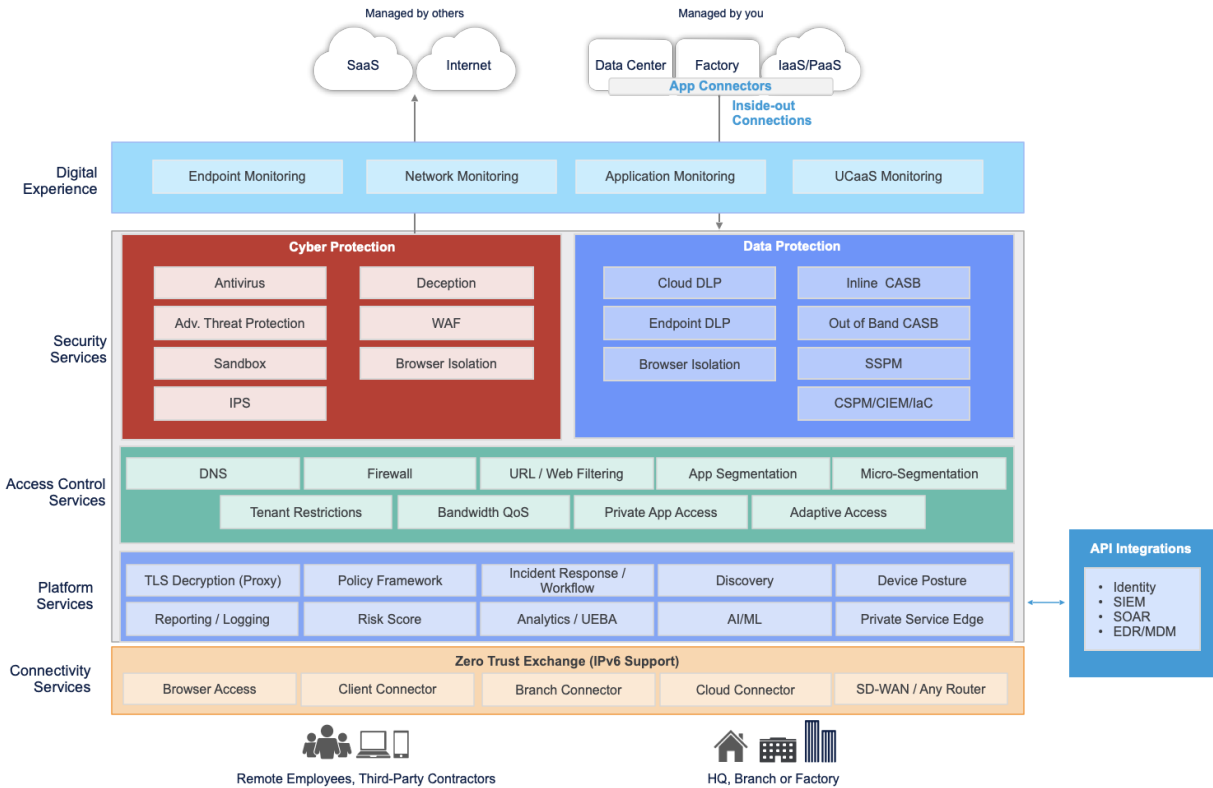


### Layered Defense

Provide layers of protection to catch even the most advanced attacks and stay in the game until the very end

- And last but not least, which is very, very critical, is the concept of layered defense. Now, defense in depth has been around as a concept for a very long time, but when you put layered defense as a platform approach versus point product, it works a lot better. The reason it works a lot better is because the context is not fragmented, it is shared. With the Zero Trust Exchange, you know what user, what identity is trying to get to what resources, and you can inspect the content and you provide layers of protection so that you increase the cost of the attacks so much for the attacker that they actually give up and move on to a different target. A good example of this would be how advanced Cloud Sandbox and Cloud Browser Isolation work together or work hand in hand. You can in fact use both of them in tandem to not only secure your users, but also deliver a very compelling user experience.

For example, while you analyze and detonate the file in a sandbox environment, you can give your user a PDF-rendered safe version of the same file using isolation technology. You can also protect them from going to suspicious websites. So we'll go into all those details in each of these specific sections, but this is what we believe is the right approach to stopping attacks.



Now, this is how it looks like for the Zscaler Zero Trust Exchange Platform. If you can see here, you have things at the bottom, which are connectivity services, above which we have the platform services, above which we have built the access control, followed by security services and data protection services, followed by digital experience. What we will do here is that we will go into more detail for each one of these sections to understand this in more detail and see how you actually use the Zscaler products to achieve the best possible security outcomes for customers. Now, if we are to step back a little bit and see how this all comes together, this is what it actually looks like.

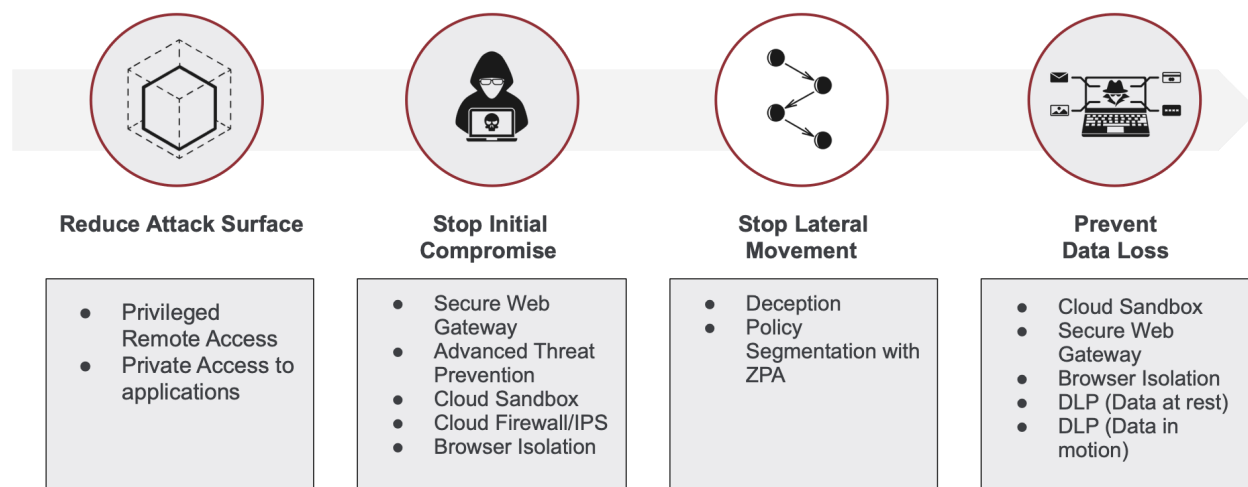
What we have built is a holistic approach to cyberthreat protection. We prevent compromise, we reduce the attack surface, and we prevent lateral movement. All of this comes together to provide a layered approach to threat and malware prevention. So we start by, first of all, creating a level of access control for all internet bound traffic. So the starting point is internet bound traffic. As it goes out, you create access control policies. This is where you use things like URL filtering. You use the security controls within URL filtering, followed by filtering of known bad destinations. These are destinations that we know based on reputation are actually bad. These could be domains, these could be IPs, these could be URLs. These could actually also be known bad files based on their hash signatures.

Then further inside, you do a full complete analysis using content inspection, using a SSL inspection, followed by the likes of PageRisk. PageRisk is a proprietary technology that we have built, which dynamically in-line calculates different risk attributes of any given website on the

world wide web. Then we have technologies like browser isolation where we can actually stop someone from going onto a suspicious website. This kind of attack is called a watering hole attack, where a commonly known website has malicious content like malicious JavaScript running on it. This is where we can provide another layer of defense using Browser Isolation, followed by File Type Control, followed by our Cloud Sandbox technology, which uses advanced AI / ML and behavioral analysis to find out if a file is malicious or not.

And at the end, we deliver safe content to the user. All of this comes together to look like a Zero Trust Exchange Platform, which maps to the same four-stage attack model we discussed above. So you have the reduced attack surface. This is where our ZPA product offering comes into play, where you can actually give privileged remote access, You can give private access to applications. Your applications are not visible on the internet. Then the second piece is to stop initial compromise. This is where a lot of ZIA capabilities around secure web gateway, advanced threat protection, Cloud Sandbox, Cloud Firewall, IPS, and Browser Isolation come together, followed by how you stop lateral movement. This is where Deception capabilities and policy segmentation kind of capabilities come together, followed by the prevention of data loss. This is where again, the secure web gateway DLP capabilities along with Browser Isolation and Cloud Sandbox come together.

### Zero Trust Exchange prevents cyber attacks



What we have understood here is just to summarize, why do attacks continue to happen? What has changed, what the current threat landscape looks like, how customers are struggling, and we've also discussed a platform approach on what is the right approach with a little bit of detail on what are the different components of this platform approach with the Zscaler Zero Trust Exchange Platform.

## Advanced Threat Protection

Advanced Threat Protection is one of the key capabilities of Zscaler's Secure Web Gateway portfolio within Zscaler Internet Access (ZIA).

It protects users going out to the internet against common attacks such as phishing.

Gaining access to phishing kits and creating phishing websites to enable

these attacks has become extremely easy. This is why an organization's need for a threat protection capability is so strong in today's digital world.

It is also important to understand command and control channels as they are a part of every cyber attack. Once a phishing attack occurs and a user is directed to malicious content, the following typically happens:

- One or more files could be downloaded
- The attacker may try to download secondary level payloads as well onto the end users machine
- Once the endpoint has been exploited attackers establish an outbound command and control channel to the adversaries' infrastructure
- The adversaries want to have full control over the remote users endpoint

Adversaries want to see if there is a specific family of malware or second-stage payload that they would like to send to the user to make the attack more effective. To do all of this they need to communicate to the end-user device that they have compromised. This is what the command and control channel does.

There's a common open-source tool called Cobalt Strike which has often been used by adversaries to create different levels of command and control traffic.

One way to block any attack is to disrupt this command and control channel. Zscaler has the power to do this through our **Advanced Threat Protection** capability.

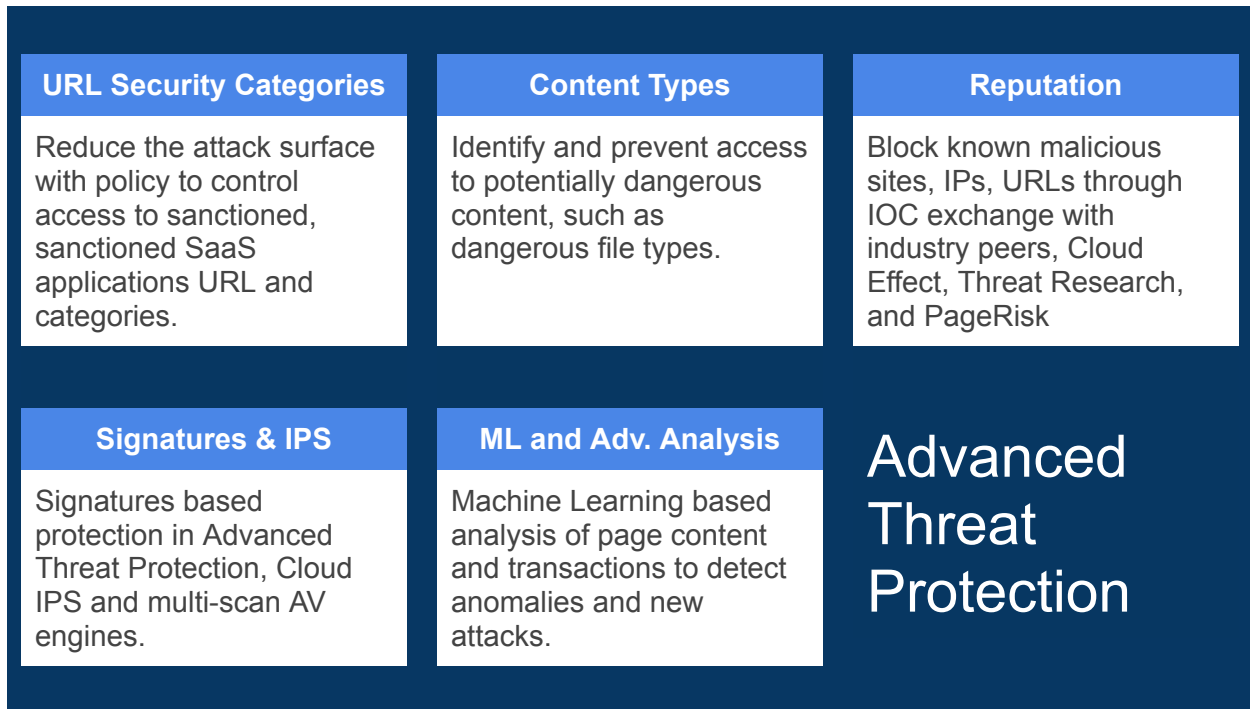
Our controls allow us to disrupt these known and even unknown command and control channels so that your users are always protected.

This further allows us to create an early warning system for your enterprise, ensuring that all of these capabilities are working together to provide a layered defense.





This broad spectrum of services is what comprised Advanced Threat Protection:



Now let's explore what can – and should – be blocked:

<b>Content Type</b>	<p>Content can be blocked using all of these individually configurable settings:</p> <ul style="list-style-type: none"><li>• High risk URL categories</li><li>• Embargoed countries</li><li>• Unscannable or password protected</li><li>• Newly registered domains</li><li>• Non-RFC compliant web traffic</li><li>• High risk file types (outright or by URL category)</li></ul> <p>For example, looking just at high risk files, these could be binary files or executable files from untrusted locations.</p> <p>Blocking any Windows executable files from websites that are not categorized is a great measure. It's completely okay for users to download an .exe file from a Windows website, but if it's an uncategorized website, then most likely that file is going to be malicious.</p>
---------------------	---

**FILE TYPE CONTROL RULE**

**CRITERIA**

<b>File Types</b>	<b>URL Categories</b>
Windows Executables (exe, exe64, scr); ... ▾	Miscellaneous; Other Miscellaneous ▾

**ACTION**

<b>Action</b>	<b>Upload/Download</b>
Block ▾	Download ▾

### Newly Registered & Observed Domains

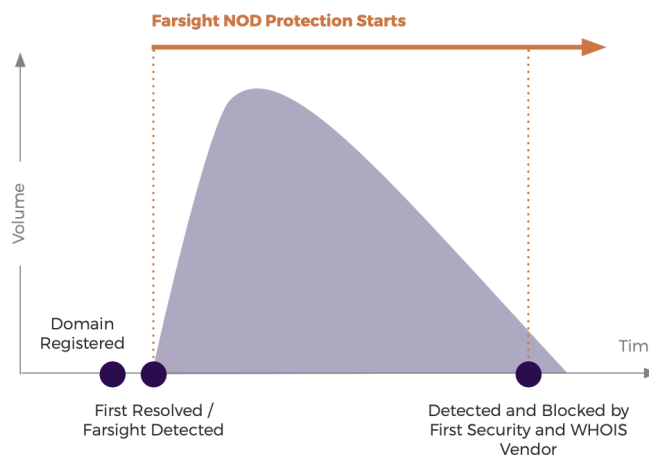
There are three domain approaches to implement when it comes to domain defense, they are:

- **Newly Registered** are domains that were registered within the last 24 hours.
- **Newly Observed** covers where domains are brought up for an attack and actually closed within a few hours. So, 24 hours is not short enough for us to capture those domains, which is why we have a newly observed domain feed in addition to registered domains, which we actually acquire from Farsight.

Farsight has the world's most advanced DNS sensor network. With this they are able to immediately find a domain with new activity and send this to Zscaler. Within three minutes of a domain becoming publicly available and one of the Farsight sensors seeing this DNS request, we are able to learn these domains, feeding right into the newly registered and observed domains category, which you can select within URL filtering and then make a decision, either you want to block it or you can even put an isolate action on it and actually isolate traffic to such websites using remote, using Cloud Browser Isolation. The domains in this feed are categorized after 30 days.

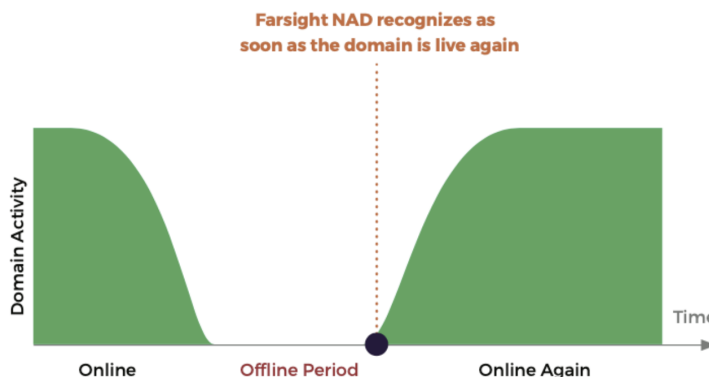
Furthermore, whatever you see in this feed will very likely be categorized as miscellaneous, which is our category for something which does not have a category – and rightfully so. But after 30 days, this domain will get categorized as another URL category.

### Newly Observed Domains Provides Early Protection



- Newly revived domains** are very unique and differentiated. Because with some really sophisticated attacks, such as the Solar Winds supply chain attack where one of the domains that they used was a regular domain that had been sitting idle for many years. The attackers acquired that old existing domain which had built good reputation and repurposed it to serve command and control activity for this specific attack.

Because of this we also have as a feed within URL categorization or URL filtering, which is available as a category, is something called newly revived domains. These are domains that went offline for a certain period of time and then came back online.



As you can see in the graph here, we get this feed (also from Farsight) where a domain is showing certain activity within a few days and then it just disappears. Anything that has actually gone offline for more than 10 days and has

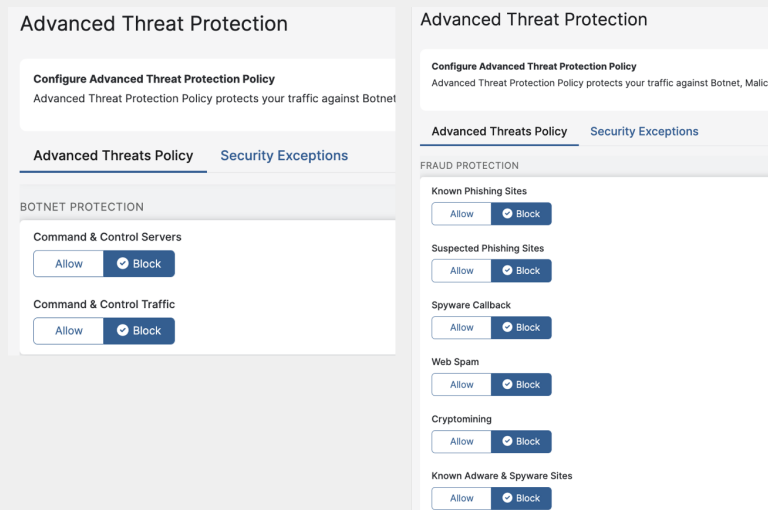
come back again is captured as a newly revived domain.

Of course completely blocking newly revived domains may not be a very good strategy because you may end up blocking a little more than you would want to. But activating multiple methods of security inspection on newly revived domains, such as turning on Advanced Cloud Sandbox policies enabling browser isolation for these domains can actually be a very sound tactic to block a lot of these attacks at volume.

So these two feeds, to summarize, the newly registered and observed domains and the newly revived domains are very simple, yet very effective methods of blocking all kinds of phishing sites and other sites that serve command and control in a very scalable way.

## Command-and-Control (C2), Phishing

- **Botnet protection** is essentially command and control. Any infrastructure that an adversary sets up to serve command and control is called a botnet. You can block command and controlled servers and you can block command and control traffic. With the command and control server, it blocks connections to known command and controlled servers.



Any time an adversarial infrastructure is discovered, information is shared across different cybersecurity companies, which is how we also know that this is a command and control server. A lot of this actually is being discovered by:

- **Zscaler ThreatLabz** where they're constantly analyzing malware and how it is communicating.

- **Cloud Sandbox** where these malicious files are detonated in a sandbox environment. Here they are closely observed for what kind of servers they're establishing command and control channels to and then using the **Cloud Effect**, we deliver all of that intelligence through Advanced Threat Protection to all customers instantaneously (even a customer who does not have advanced Cloud Sandbox still gets this intelligence via another customer who may have actually downloaded a sample in advanced Cloud Sandbox)

- **Phishing protection** could be for known or suspected phishing sites, where unknown phishing sites are blocked using AI / ML.

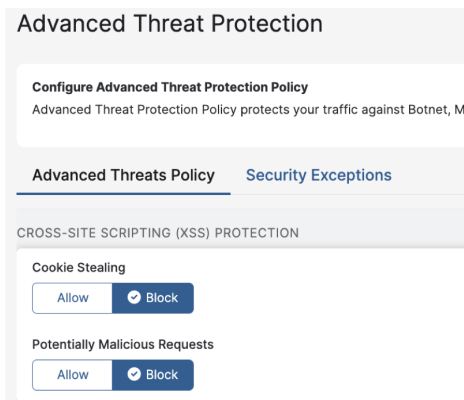
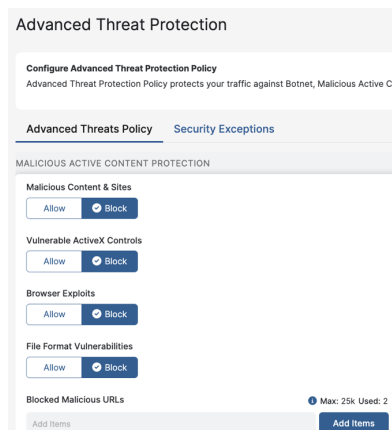
Using these controls, you also block a lot of adware, spyware, spam pages, and also websites that run crypto mining activity (these specific sites sometimes can actually hijack your browser and use the resources to do crypto mining without you even being aware of it). And all of this with a simple toggle switch for each.

### Malicious Active Content & Server Side Vulnerabilities

Malicious active content and server-side vulnerabilities. These could be:

- Malicious content and sites.
- Malicious ActiveX controls
- Browser exploits
- File format vulnerabilities.

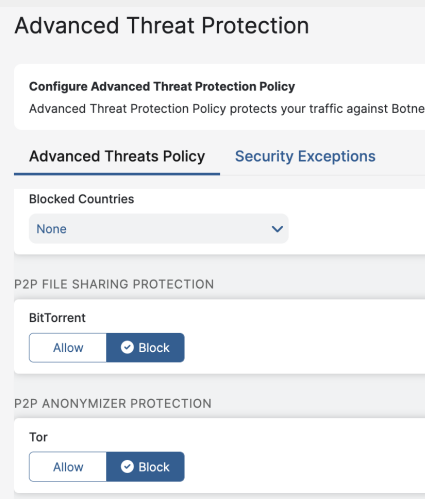
If a connection is going to a website that is running an exploit kit or malicious adware and we actually know about it, using our content inspection we can block a lot of these as well in-line.



When it comes to **cross-site scripting protection** where a web server has vulnerabilities that allow malicious threat actors to inject code into the site, that is what we can block using these settings.

## Anonymizers & Peer-to-Peer (P2P)

- **Anonymizers** are very popular where someone can download one of these VPN clients and try to masquerade their activity. This is very, very popular in K-12 environments or schools where students would use some of these anonymizers like XVPN to masquerade their activity so that they can go to all kinds of different websites, which creates a bigger attack surface.



- **P2P** – Many very resourceful users can also use P2P anonymizers like Tor and file sharing like (BitTorrent). These are all very evasive software connections where users even attempting to use without approval are heavily and quite appropriately scrutinized by security operations teams.

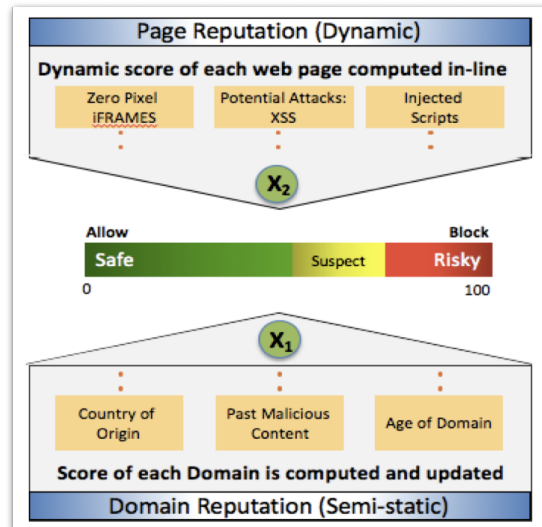
## PageRisk Engine Detection via Web Page & Domain Features

PageRisk is a simple slider control for administrators to decide how much risk is acceptable. Under the covers is the PageRisk engine, dynamically creating a score for each location.

This is a very powerful capability which we are able to actually scale linearly across all web content. And this creates a risk score, which can either be safe, suspicious, or risky. Customers can actually choose the slider to an acceptable level of what they will allow.

Throughinspect in-line all the content of a webpage and we use a multi-data algorithm applied to the webpage to determine its riskiness. So this risk is based on several factors.

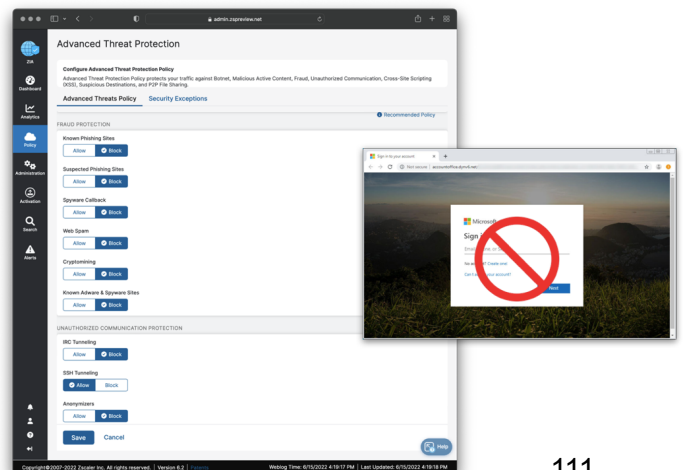
- Suspicious Content Protection (aka PageRisk)
  - Multi data algorithm applied to web page (not file)
  - The algorithm determines the riskiness
  - Blocked based on customer set threshold



- Risk (0-100) is based on several factors
  - Risk Top-Level Domain TLD (.tk, .ru, etc.)
  - Unknown user agent
  - Missing HTTP headers (User-Agent, Accept, etc.)
  - High entropy domain name
  - zero-pixel IFRAME
  - Script or IFRAME before the tag or after the tag (code injection)
  - Obfuscated Javascript
  - Signatures for suspicious URL path, HTML/Javascript/CSS code

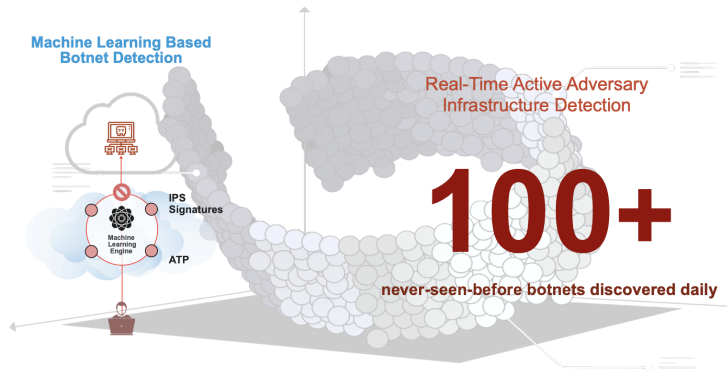
## Preventing Unknown Threats

With AI-powered phishing detection, even the most advanced phishing attacks can be stopped. This is the same control as previously discussed, but now with actually looking at all the HTML content of any SSL inspected webpage in-line. We take **form, structure, domain age, refer, hosting, brand popularity, certificate information, post structure**, and we use these as features in an ML model where all of this is fed into the ML model. And the ML model spits out a decision if this is a phishing page or not.

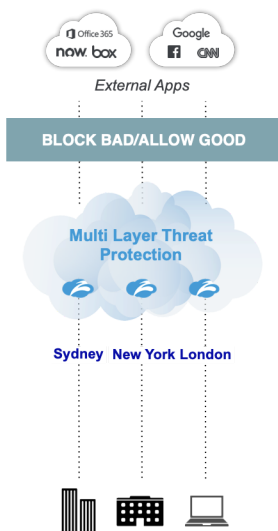


With this technique, we are even able to detect some of the most advanced phishing sites, which are using man-in-the-middle attacks, where the adversary has created an entire phishing infrastructure where he can actually frontend the entire website to the user, but on the backend, they are still transmitting all those credentials to the actual website to give the user a very native

end-to-end experience. But the user does not know that anything that is being entered on that front-ended website is actually being sent to the attacker. These attacks have become exceedingly common. We have seen this technique being used often, which is why this is a very powerful capability where we can even block patient zero phishing pages.



How you use it is very straightforward. You turn on the knobs in Advanced Threat Protection and all this AI / ML capability starts working in the backend on its own. The next capability around AI-powered detection and prevention is AI-powered C2 detection or command and control detection. So we also created an ML model where we not only try to detect phishing but we look at all the traffic and then we pass it through our machine learning engine to detect command and control. And once we can detect command and control, we can block it, but it also allows us to map out adversary infrastructure or discover new botnets.



And there are some statistics here which will of course change over time, which will go bigger and bigger. But on a daily basis, we are able to discover more than a hundred botnets. The important thing here to understand is that we also have the ability to detect and block unknown command and control, which is a very strong way to block any attack because any attack that you see today will always use command and control from the most commodity-based attack to the most advanced attack. So blocking that, disrupting that command control channel also allows us to block a lot of these attacks.

The Advanced Threat Protection capabilities allow us to create an early warning system for every organization, where we take all these trillions of signals to train the AI / ML models and we provide more than 250,000 daily protection updates, 7 billion threats are stopped per day. And all of this happens because of all these capabilities working together, providing layered defense.



## Key differentiator: The world's largest security cloud



## Antivirus / Malware Protection

Antivirus or Malware Protection is a key component of how Zscaler protects organizations and their users from malicious files and attacks. Like Advanced Threat Protection, Antivirus sits under Zscaler’s Cyber Protection capabilities in our Security Services suite.

To understand this capability, we first need to be able to identify common malware types that are targeting the enterprise.

<p><b>Maldocs</b></p> <p>Malicious delivery documents, typically Microsoft Office or Adobe PDFs.</p>	<p><b>Downloaders</b></p> <p>Malware used specifically to deliver other malware. Common families include Emotet, SmokeLoader, and Pony.</p>	<p><b>Ransomware</b></p> <p>Malware that steals data and encrypts everything. Common families include Ryuk, REvil, Maze, and EKANS.</p>
<p><b>Information Stealer</b></p> <p>Malware used to steal sensitive information from target systems. Common families include Trickbot, Qakbot, Agent Tesla, and Usrnif.</p>	<p><b>Post Exploitation Tool</b></p> <p>Tools deployed after the adversary has gained access. Common tools include Mimikatz, Meterpreter, and Empire.</p>	<p><b>RAT (Remote Access Trojan)</b></p> <p>Malware that can provide full remote access to a target system. Common families include Nanocore, njRAT, and Remcos.</p>

Having identified the common malware types, let’s explore the common delivery mechanisms and what protections Zscaler provides against these attacks

### Common Delivery Mechanisms

Malicious code looking to exploit browsers or browser related code for non-interactive malware delivery. Usually targets Browsers, Plugins, etc



**Phishing**



**Exploit Kits**

Using email to deliver malware, either via links or attachments. Most common delivery mechanism today

Compromise or unauthorized access initially executed by a different operator and sold to the highest bidder



**Watering Hole**



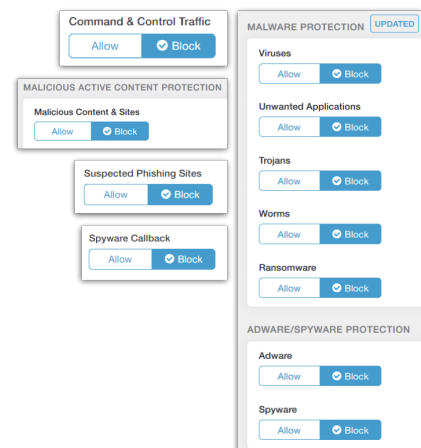
**Pre-existing Compromise**

Targeted or non-targeted malware planted on commonly accessed services.

Phishing	Phishing specifically when you're delivering a file is called spear phishing. This is using email to deliver malware, either as an attachment to that email or a link where the user will click. And unbeknownst to them, this specific file will download. This is the most common delivery mechanism used today.
Exploit Kits	Exploit Kits are essentially malicious code looking to exploit browsers or vulnerabilities within browsers. This was very, very popular when Internet Explorer was still a very common browser, but as Google Chrome has become more popular as a browser, we are seeing less and less of exploit kits. But still, there's plenty of Internet Explorer out there. There are still plenty of exploit kits out there, and we are seeing some advanced exploit kits, even for the most common advanced browser like Google Chrome.
Watering Hole	A watering hole is when you take a very popular website and you put malicious content on it. This could be malicious JavaScript. This could be a malicious driver download. And when anybody goes to that website, they will, unbeknownst to them, download a specific malware that was actually put on this website. The way attackers do this is typically by renting advertising space on the website because the creator of that website may not completely track what advertisements are coming and how they're actually being rendered on the website. So a very common way to actually land a malicious code on a website is to use the advertisement space.
Pre-existing Compromise	More than a few years ago, Forbes.com was one of the websites which was a victim of a watering hole attack. The last one is a pre-existing compromise. This actually means that compromise or unauthorized access is initially executed by a different operator and then it is sold to the highest bidder. So the attackers will compromise a device and then they will see, okay, maybe there is someone actually who is a different attacker, can have better use of it. So they will actually send this off to the other attacker.

Now let's take a look at what **protections** are provided **against these attacks**.

So the malicious file protections that we provide are delivered through the malware protection configuration. So as you can see here, you can block spyware or adware or you can block viruses, unwanted applications, trojans, worms or password-protected files. You can even block any active content or unscannable files. If we take a better look on what this looks like in the configuration, most of these are antivirus

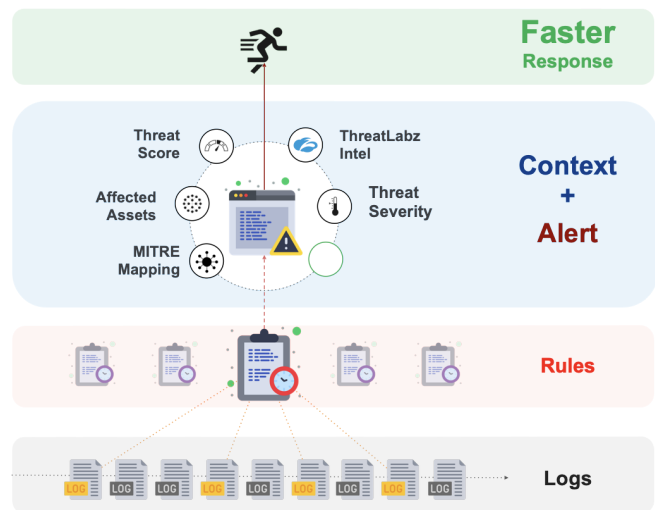


signatures that are mostly file based. With this we actually block the most common threats in malware. A lot of these signatures or engines are the AV engine that is running. These are signatures that identify binary payloads. A lot of these signatures are based on MD5 hashes, where we know that the file is malicious. And a lot of this actually can also be done using AI / ML, where we can identify if a file that is being downloaded is malicious or not.

## Detection & Response

As with prevention, it is also important to understand how Zscaler provides detection and response capabilities. This detection and response is the correlated threat insights and alerting framework.

This is enabled via the correlation where predefined rules correlate disparate atomic log events to create very consumable and actionable alerts for impacted systems or compromised users. This allows us to provide context along with the alert for faster prioritization and response by the customers. And of course all these can be forwarded to a customer's favorite SIEM products, orchestrating even more advanced playbooks.



Trickbot

Alert Overview

Alert ID: #456821

Event Type: Botnet Callback

File Information

File Name: authtostati.cab

Sandbox Category: Malware

Sandbox Verdict: Known Malicious

File Type: EXE

File Size: 550 KB

MD5: 03090168126746

SHA256: 4d2f08cae3b7354

Alert Details

Last Known Attempt: Jun 23 11:03:34 GMT

First Known Attempt: Jun 18 06:33:45 GMT

Duration: 1 Week

Allowed/Total Transactions: 22 / 64

Allowed/Total Bytes: 200 / 1000

Evaluation Status: Ongoing

First Destination

Destination IP: 173.231.184.58

Host Name: Disorderstatus.ru/order.php

URL Category: File Host

Application: Dropbox

Application Risk Score: 66

Application Category: File Sharing

SSL Inspected: Yes

Threat Summary

First observed in 2016, Trickbot is a banking trojan and has become one of the most prevalent and dangerous malware strains in today's threat landscape. It is modular in structure and has numerous capabilities to control both the targeted system and the network.

SOME OF THE KEY CAPABILITIES OF TRICKBOT TROJAN INCLUDE THE FOLLOWING:

- Steals banking login information
- Steals credentials of various applications from the target system using a Password grabbing module
- Deploys crypto currency miners such as the Monero mixer, XMRIG
- Uses lateral movement techniques to infect other hosts in the target network
- Performs reconnaissance to discover point-of-state (POSD) devices in the target network
- Steals information from email clients such as Microsoft Outlook on the target machine
- Uses a hidden VNC module to control the infected machine remotely using VNC

Mitre Matrix

There have been 8 attack techniques and 4 tactics detected for this threat. See the full Mitre Matrix for more details.

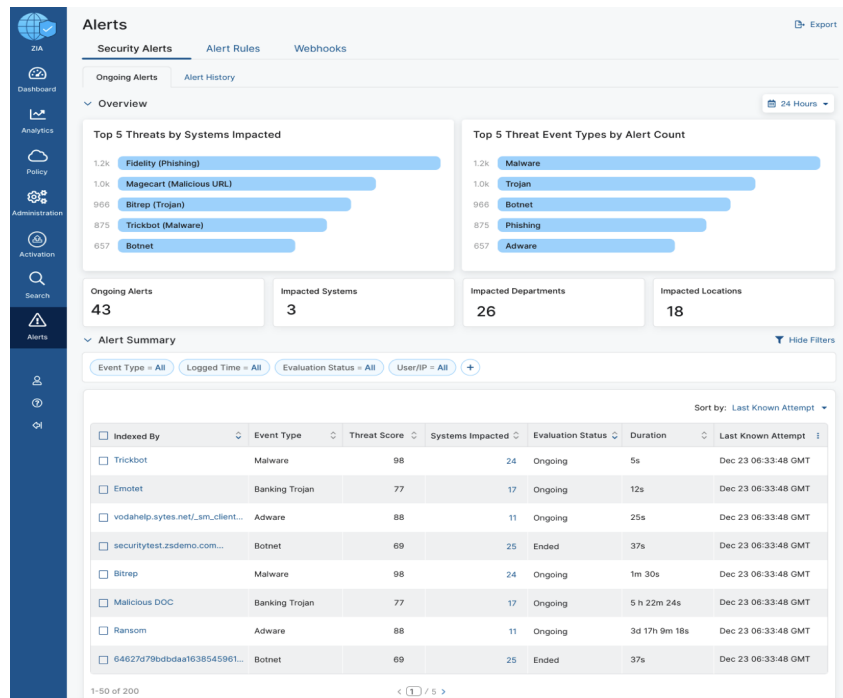
Discovery	Execution	Collection	Persistence	Initial Access	Defence Evasion	Command and Control
File and Directory Discovery	Execution through API	Data from Local System	Registry Run Keys / Startup Folder	Spearfishing Attachment	Deobfuscate/Decode Files or Inf...	Commonly Used Port
Process and Discovery	Scripting			Spearfishing Link	File Deletion	Data Encoding
Query Registry	User Execution				Hidden Files and Directories	Data Obfuscation
System Information Discovery					Masquerading	Multi-layer Encryption
System Time Discovery					Modify Registry	Remote File Copy
					Obfuscated Files or Information	Standard Application Layer Protocol
					Process Hollowing	Standard Cryptographic Protocol
					Software Packing	

At a high level, the way it works is we provide an alert, as you can see here. Instead of asking the customers to go and look at different logs, we build that correlation engine, which actually correlates all these disparate log events to create an alert where we are saying the TrickBot campaign has been detected in your environment.

This is what the threat is all about. So we have a threat summary, we also map it to the MITRE matrix and we also provide a list of impacted systems. So we'll actually go through the whole workflow on how an administrator will actually be using this capability to do really fast detection and response to such events.

Let's take a deeper look at how the detection and response workflow will look like with this capability.

The admin will first go to the alert screen where they will actually see a bunch of security alerts that have been predefined. These security alerts are predefined by us based on the intelligence we gathered from our ThreatLabz team and other leading resources. All work together to create different alert rules that we have defined here. There is one for TrickBot, there is one for Emotet, there is one for Bitrep for instance. These correlation rules can be added over time, so we will keep adding more and more and customers can also define their own.



There's also a lot of contextualized information about this specific alert. What TrickBot is, for instance, is a banking trojan. That means someone has inadvertently downloaded a banking trojan. The next step you would naturally feel is to find out who this specific user is. So you go to impacted systems. Once you are within impacted systems, you will actually see the number of systems by department. You'll also see the number of impacted systems by location. And here you can actually find out there's a total of 64 systems that have been impacted. The usernames are defined here, shown along with the client IP, the first time that these systems were impacted, what department they're in, what location it is.

For customizing, admins can create their own alert rules and get the notification of these alerts outside of the UI using email or through webhook third-party support for applications including ServiceNow, Slack teams, OpsGenie, PagerDuty, and Splunk.

This is our capability around detection and response, where we built a correlation engine within the ZIA product that can actually take all these logs, correlate them, and provide very meaningful actionable consumable alerts that the SOC team can use to go and do meaningful detection and response activity.

## Basic Data Protection Services

Basic Data Protection Services will allow you to explore the breadth of the data protection capabilities of the Zero Trust Exchange.

Gain an overview of Zscaler's Data Protection capabilities, dive deeper into specific functions, and gain knowledge on how to configure Zscaler's Data Protection Services as they relate to Zscaler best practices.

---

By the end of this chapter, you will be able to

1. **Recognize** why a new approach is needed to data protection and how Zscaler works to provide these protections to users through the Zero Trust Exchange.
2. **Identify** the Data Protection Services Zscaler has in place to protect data in motion and at rest.
3. **Understand** how to manage data protection incidents within Zscaler's administrator portals.
4. **Discover** how to configure Zscaler Data Protection Services and capabilities.

## Data Protection Overview

### What is Zscaler Data Protection

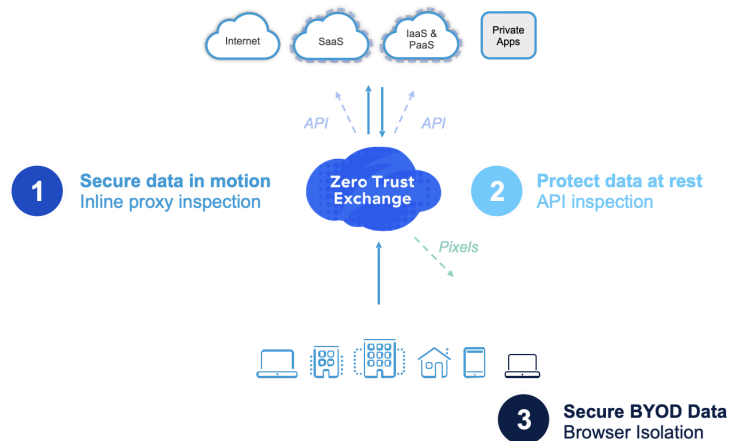


The adoption of SaaS and public cloud has rendered data widely distributed and difficult, if not impossible, to secure with legacy protection appliances. As such, it is easy for both careless users and malicious actors to expose enterprise cloud data.

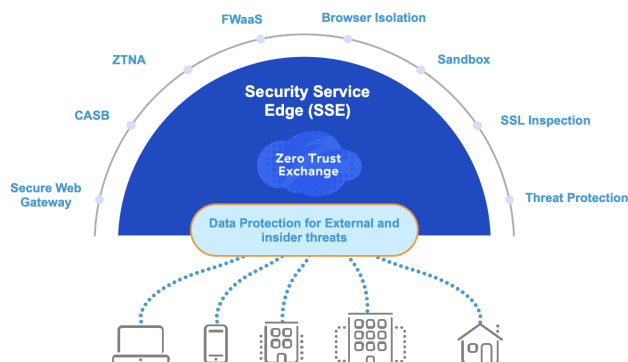
Unlike complex legacy approaches that can't follow users, Zscaler Data Protection is a simple but powerful way to secure all cloud data channels. Zscaler protects all users anywhere and controls data in SaaS and public clouds, all with a robust and intuitive data discovery engine.

In addition, Zscaler realized that the **number one data exfiltration** channel is no longer the USB and external drive on the endpoint, but rather a user's personal cloud storage, collaboration, and cloud-based personal email applications.

The Zero Trust Platform far exceeds standalone DLP (data loss prevention) or CASB (cloud access security broker) products. This enables the delivery with high performance, high scalability, high accuracy, and efficacy. And from a data security perspective, what we really delivered is a solution that protects your data - from data in motion, data at rest, as well as the data that is sitting on BYOD (bring your own device) and unmanaged assets. The way we

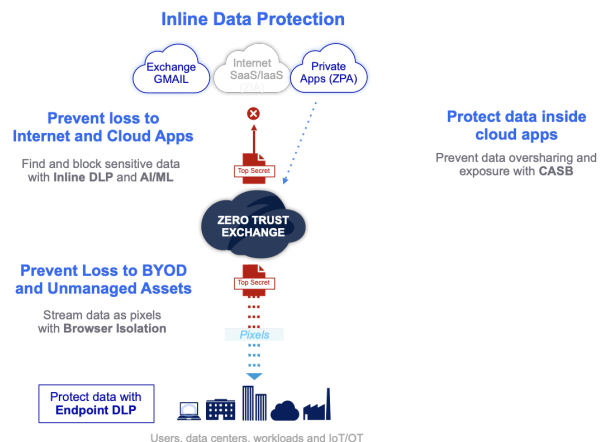


delivered it is not in isolation; it is all part of our secure Service Edge platform. Secure Service Edge (Zscaler Private Edge and Zscaler Public Edge) combines the data protection from external threats, as well as insider threats, your employees and their activities in different cloud channels and other channels.

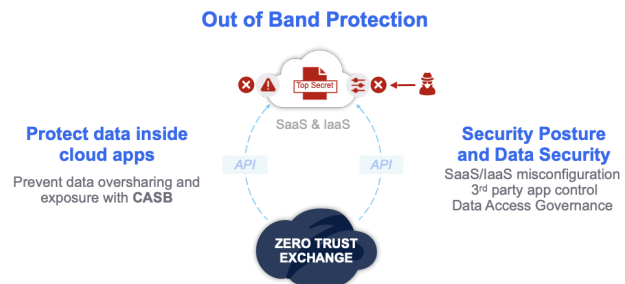


When Zscaler talks about data protection, essentially we are talking about two different segments.

- DLP:** From a DLP perspective, how do we do data loss prevention for cloud traffic? How do we protect your data on the endpoint? How do we protect your secure data through email, your corporate exchange, and Gmail? And how do we protect your sensitive assets and crown jewels when the data is sitting with your private apps? And all these capabilities behind the scene are using our data classification engine, which is essentially a data loss prevention engine.



- CASB:** From a CASB perspective, CASB (Cloud Access Security Broker) was designed to protect your crown jewels from SaaS-based services. This is a multi-mode CASB solution (known as SaaS Security API), which is inline forward proxy-based CASB. We also offer out-of-band CASB for data address and for BYOD and unmanaged assets. We are protecting your data, using an isolation proxy. And then within CASB, we have SaaS Security Posture Management (now known as Zscaler Cloud Security Posture Management), which is SSPM, and we protect your data from SaaS-to-SaaS communication, which is essentially third-party applications, API tokens, service accounts, and so on.



Let's review, via 4 use cases, the drivers behind Zscaler's Data Protection strategy:

Cloud Application Data Loss	How do we prevent data loss to internet and cloud applications? In this mode, we are a man-in-the-middle proxy. All your internet bound traffic is egressing through us. Every single transaction we are inspecting on the wire. Most of your internet-bound traffic today is HTTPS-encrypted. So at ingress, we will crack open that SSL connection, and then once we crack open that SSL connection, we are ready to inspect your content, your payload. And we do that with different types of DLP classification techniques. Then we enforce policy based on the user
-----------------------------	---



groups and departments they're coming from. On the destination side, this is based on cloud applications, URL category, cloud applications, specific activities, and so on.

The simple use case example here is why my users are uploading zip folders and encrypted files to a random website, or why I am seeing so many users uploading my office documents to an application called Pdfconverter.com, or why user John is uploading sensitive PII (personal identifiable information) data to his personal OneDrive account. We are delivering this visibility at real time with our man-in-the-middle proxy. And then all the policies that we are enforcing, these are all real time. The actions could allow the transactions, block the transactions, or monitor the user, coach the user, send user notification, and so on. And once again, this is all in-line transactions. This is our strength, this is our bread and butter, because when you have to monitor all your internet-bound traffic and all these transactions, you really have to think about scale, speed, and efficacy.

#### BYOD and Unmanaged Assets

How do you protect your sensitive data from BYOD and unmanaged assets? If you think about the situation that we are in today, post-COVID, everybody's working from home. Most of the time, perhaps they're using their corporate assets, but once in a while they're using their personal Mac, their personal Windows, and they're going straight to their critical cloud-based applications like Office 365 and Salesforce. Remember, these devices are unmanaged assets. That means there is no footprint on this device. There is no Zscaler Client Connector, there is no special PAC file.

The company, the IT admin, the DLP admin - they have absolutely no visibility into what users are doing when they're connecting to these critical cloud applications. So in this mode, we interject ourselves during the authentication time and then through SAML proxy and identity proxy, we will identify if the user is coming from an untrusted device. And then once we identify this untrusted device, then we forward this session to our Cloud Browser Isolation. Once the traffic is using Cloud Browser Isolation, then we control that entire channel. We enforce different types of conditional access policies so that we can always protect your data.

#### Data at Rest

How do we protect data at rest? When organizations deploy applications like Office 365 or Google, or even from a public cloud infrastructure perspective, they're probably storing a lot of data in their S3 (Amazon Web Services (AWS) Single Storage Service) bucket, Azure block, and

GCP (Google Cloud Platform). There is no concern if the user was storing sensitive data because these applications essentially are their corporate applications. These applications are their official storage application and collaboration application. Once again, if a user from finance is uploading financial statements and storing them in corporate OneDrive, that behavior is okay. But what we see in the market is once the data sits there, there is a tremendous amount of accidental data loss through data exposure.

An example would be HR creates a folder in your corporate OneDrive account. She uploads every employee's PII information. And then during the collaboration time, accidentally expose that folder with a public URL or external link. Or a developer in your company is using GitHub, and then they're uploading company source code, but they're exposing that source code with an external collaborator called Fu@gmail.com. So in this particular mode, we are scanning your data. We are identifying which assets are sensitive, and then our primary goal is to protect that data from an exposure perspective.

#### Cloud Misconfiguration

A lot of data exfiltration, data loss, today is happening because of cloud misconfigurations. This misconfiguration at the application level is done by admin users as well as end users. With our SSPM module and our third-party app integrations SaaS-to-SaaS API connections, we monitor these misconfigurations. And then whenever we find a serious violation, we trigger remediation actions.

These are some of the top use cases that are really driving our data protection adoption today. We extended the same classification stack, the data protection stack, to protect your data that is sitting with your private apps. These private apps might be hosted in your on-premises location or from public cloud infrastructure. But again, we extended our same classification, the data classification engine to protect your data from private apps.

## Protecting Data in Motion

### Inline Data Protection

There are four Data Protection capabilities that Zscaler provides through the Zero Trust Exchange to ensure data security for Data in Motion.

- Cloud Data Loss Prevention (DLP)
- Endpoint DLP
- Email DLP (primarily for corporate Exchange and Gmail)
- DLP for Private Apps

At the same time, from a Cloud Access Security Broker (CASB) perspective, Data in Motion means that CASB is running in inline forward proxy mode and with Browser Isolation (Isolation Proxy).

When you think about in-line data protection, there are several use cases that are very critical for you to protect your data in-line in real time.

#### Shadow IT and Data Discovery

Everything starts with visibility. You can't really secure what you don't see, so application discovery for Shadow IT (applications that are not corporate-sanctioned and perhaps being utilized by individual users, different views).

### Auto classification & Data discovery powered by AI/ML

#### Problem Help IT staff who aren't experts

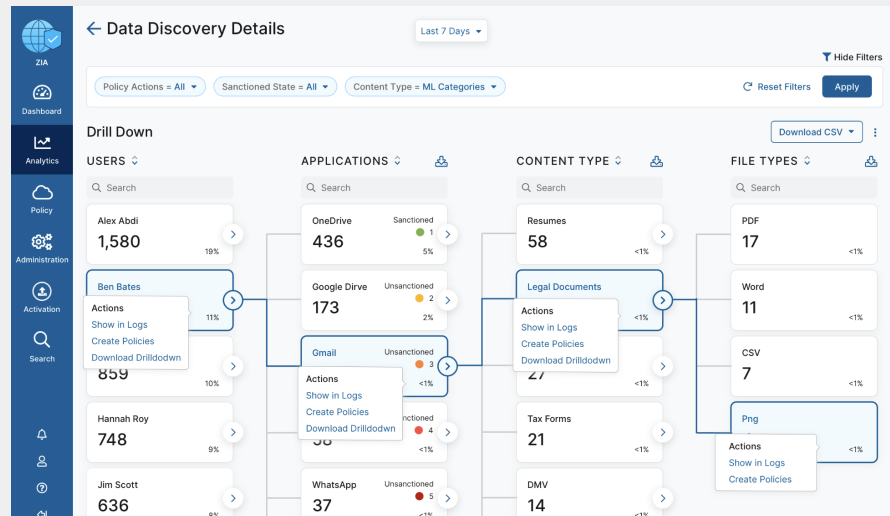
- No Rules, regex or complicated policies
- No end user markup or classification

#### Solution Find and secure sensitive content

- Deep learning engine
- Thematic Data Categories
- Customer defined categories
- Supervised learning model
- NLP, document clustering
- Vector learning



We offer complete application discovery. Our application database has about 45,000 cloud applications that bubble up in our Shadow IT and Shadow IT discovery report. Each application is tagged with the risk score. In order for us to come up with the risk score, we have a very large application research team looking at different threat characteristics as well as hosting characteristics.



The risk algorithm is designed with about 75 attributes at the backend.

### Application

When our research team does application research, essentially they're basically taking that application and putting that application in a sandbox.

- What kind of encryption and SSL channel this application is using for data in motion.
- Is this application evasive?
- If we close Port 80 and 443, does this application look for other open ports to get out?

### User

From the actual users of these applications - from the threat character's perspective, where we look at different characteristics.

### Hosting

From the hosting character's perspective, we are looking at what kind of certifications this application has.

- Is it PCI (Payment Card Industry)-certified, SOC (System and Organization Controls)-certified, GDPR (General Data Protection Regulation)-certified?
- What kind of Ts and Cs (terms and conditions) does this application offer?

You'll be surprised to find out about many SaaS-based services - especially file sharing and collaboration

applications - their terms and conditions will say, "If you upload any data to our cloud, that data becomes our intellectual property." And the users never pay attention to these terms and conditions. They continue to use this application, putting the organization at a serious risk.

As part of Shadow IT discovery, we will discover all these applications and tag every single one with a risk score. Our customers should be able to modify that risk score depending on their environment. For example, if an application does not support encryption, but our customers don't care about encryption because they might have a compensating control, they can go and they can change the default risk score. Then we immediately readjust that risk score for that specific tenant, for that specific customer.

### Cloud App Control

When you have visibility with a single policy, you can block all these applications, bad applications. You can also block specific activities within applications. So when you build a Cloud Application policy, you can say all applications that are higher than a risk 4 should be automatically blocked. Or you can build a very granular policy saying all applications that are not PCI-certified should not be utilized by our finance team. So the Shadow IT visibility eventually bubbles up to your policy constructions. And then not only do you have that complete visibility, but you can take different actions based on application risk score.

### Access Control - 16 Categories, 40K Apps

The screenshot displays a policy configuration interface with three main sections:

- Criteria:** A list of application categories on the left (e.g., Collaboration & Online Meetings, Consumer, DNS Over HTTPS Services, File Sharing, Finance, Health Care, Hosting Providers, Human Resources). The main area contains a grid of criteria:
 

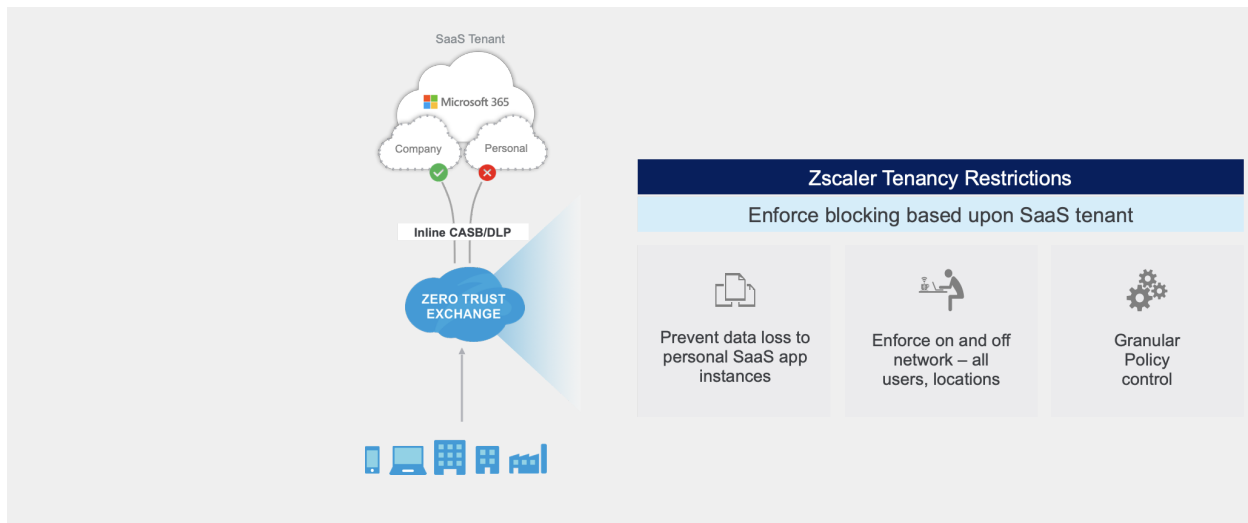
Cloud Applications	Cloud Application Risk Profile
2Shared; Box.net; Dropbox; Dropsend...	None
Users	Groups
Departments	Locations
Location Groups	Time
Devices	Device Groups
User Agent	
- Flexible Actions:** A list of actions:
  - View but no uploads
  - Define by tenant profile
  - Enforce browser isolation for safe data access
- Action Configuration:** A detailed view of an action with options for 'Viewing' (Allow, Block, Isolate) and 'Uploading' (Allow, Block). It also includes fields for 'Daily Bandwidth Quota (MB)' and 'Daily Time Quota (min)', and a 'Tenant Profile' dropdown.

Annotations on the screenshot include:

- Simple Setup:** Get started quickly with App Categories (pointing to the category list).
- Granular Control:** Enforce by app category, users, group, locations or risk profile (pointing to the criteria grid).

### Tenancy Restrictions

Personal vs. Corporate - Granular Policies  
Tenancy restrictions for sanctioned apps



## DLP Inline for Web & SaaS

- **Dictionaries** - A DLP dictionary contains a set of patented algorithms that are designed to detect specific kinds of information in your users' traffic. The Zscaler service provides predefined dictionaries that you can modify and, in some cases, clone. You can also create custom dictionaries for content not covered by predefined dictionaries. For example, you can create custom dictionaries that trigger based on specific patterns and phrases, or trigger based on exact data matching.
- **Exact Data Match (EDM)** - With Zscaler EDM, you can easily find and control any occurrence of specific data. From employee records to customers' personal data and credit card numbers, EDM lets you fingerprint sensitive data and improve detection accuracy while reducing DLP false positives.
- **Indexed Document Matching (IDM)** - With Zscaler IDM, you can secure high-value documents that typically carry sensitive data. Fingerprint tax, medical, manufacturing, or other important forms and detect documents that use those templates across all your cloud data channels.
- **Optical Character Recognition (OCR)** - Data doesn't only appear in plain text—so you need DLP that secures visual data as well. Zscaler OCR scans images to perform data classification for files like PNGs and JPEGs, and for images embedded in other file types (e.g., Microsoft Word documents). It even works in tandem with EDM and IDM functions.
- **Azure Information Protection (AIP) / Microsoft Information Protection (MIP) Labels** - Microsoft Information Protection (MIP) provides sensitivity labels, which you can use to identify and protect files with sensitive content. These MIP labels are maintained by Microsoft and, through the addition of an MIP Account in the ZIA Admin Portal, these labels can be retrieved from Microsoft so that

they can be used when defining a Data Loss Prevention (DLP) policy in the ZIA Admin Portal.

UEBA (user and entity behavior analytics) and Adaptive Access

Bulk upload/download, impossible travel, MFA

UEBA and adaptive access is one of the critical components of data protection. This has a lot to do with contextual DLP based on different anomalies, and different unusual behavior. You might want to enforce different types of actions. And then once you do - all of that in forward proxy mode - then you also have to think about BYOD and unmanaged assets, data that is sitting on these unmanaged assets. But the devices are completely unmanaged. How do you protect your crown jewels from these unmanaged assets?

Data Security on BYOD Isolation Proxy

### Data Loss Prevention

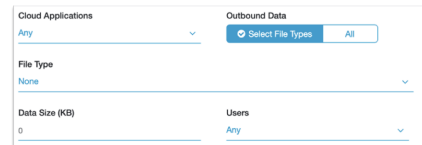
What happens when you are now ready to do the content inspections with Zscaler's DLP features?

The first feature that is very popular within data loss prevention is policies based on file types. Zscaler DLP supports hundreds of file types and you can simply pick and choose a specific file type and you can protect that data. The use case here is if any of my users are uploading Office documents to an application called Pdfconverter.com, I want to block it. And in this case, you go to our policy engine, you select a specific file type, and then for that specific file type and file size, you allow or block all applications, you allow or block different actions and activities.

#### Three Levels of Inspection File Type Identification

Policies for more file types, including undecodable files

- Archive**
  - Bzip2 (bz, bz2)
  - Cab Archive (Cab)
  - GZIP (gzip, gz)
  - ISO Archive (Iso)
  - RAR Files (rar)
  - Stuffit Archive (stuffit\_sit, stuffit)
  - Tar (tgz, gtar, tar)
  - ZIP (zip)
- Image**
  - Bitmap (bmp)
  - Gif Files
  - Jpeg Files
  - Photoshop (psd)
  - Png Files
  - Window Meta Files (wmf)
- Microsoft Office**
  - Microsoft Excel (xls, xlsx, xism, xlam, xlsb, slk)
  - Microsoft MDB (mdb)
  - Microsoft Outlook Message (msg)
  - Microsoft PowerPoint (ppt, pptx, pptm, potx, ppsx)
  - Microsoft RTF (rtf)
  - Microsoft Word (doc, docx, docm, dobx)
- Other Documents**
  - HTTP Form data
  - PDF Documents (pdf)
- Other**
  - Password Protected / Encrypted**
  - Web Content**
  - Adobe Flash (swf)
  - Java Applet (jar, class)
  - JavaScript (js)
  - Text File



Applicable to any Outbound Data

Make the Internet read only with Outbound Data blocks

### 3 Levels of Inspection

Behind the scenes, when we are enforcing policy based on file type, we are not just simply looking at the file extension. If we did that, then it's going to be very easy for users, malicious users, to bypass by simply changing the file extension. Instead, we do three levels of inspection.

- First, we look at some of the early bytes that we call Magic Bytes.
- Second, we will look at the mime type,
- Third, we will look at the file extension.

These three levels of inspection gives us a lot of confidence that we are not generating any false positives. The file type based data loss prevention is a very popular, simple policy. You can combine a policy where you are not only looking at the file type, but you are utilizing our Cloud App Control to enforce a granular policy based on that specific cloud application’s activity.

Now look at how we look at the content and do deep content inspection with different types of DLP bells and whistles.

## Zscaler Content Inspection Capabilities & Custom Dictionaries

Inspection Category	Inspection Technique								
Described content	Predefined Dictionaries	<ul style="list-style-type: none"> <li>• PII (US and International)</li> <li>• PCI (CC#, ABA Bank routing)</li> <li>• PHI (Patient Records, ICD10)</li> <li>• Source Code</li> <li>• Adult Language/Profanity</li> <li>• GDPR Data</li> </ul>							
	Single & multi word keywords and phrases	<div style="border: 1px solid #ccc; padding: 5px;"> <p><b>DLP DICTIONARY</b></p> <p>Name: US Street Address      Dictionary Type: Patterns &amp; Phrases</p> <p>Match Type: Match Any</p> <p>Description: US Street Address (Expected format #####(upto 8 digits) Any string, 2 Letter State Abbreviation 5 digit zip code followed by optional 4 digit zip code extension) - 2 line addresses are welcome</p> </div>							
	Regex	<div style="border: 1px solid #ccc; padding: 5px;"> <p><b>PATTERNS</b></p> <table border="1"> <thead> <tr> <th>Pattern</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>[1-9]([0-9]{3,12})[0-9]{4}[-]*(0,1)[A-Za-z]{2}(,0,1)[0-9]{5}</td> <td>Count Unique</td> </tr> <tr> <td>[1-9]([0-9]{3,12})[0-9]{4}[-]*(0,1)[A-Za-z]{2}(,0,1)[0-9]{5}[-]{0-9}(4)</td> <td>Count Unique</td> </tr> <tr> <td>[1-9]([0-9]{3,12})[0-9]{4}[-]*(0,1)n*(0,1)(w)(2)(s+)(d)(3)</td> <td>Count Unique</td> </tr> </tbody> </table> </div>	Pattern	Action	[1-9]([0-9]{3,12})[0-9]{4}[-]*(0,1)[A-Za-z]{2}(,0,1)[0-9]{5}	Count Unique	[1-9]([0-9]{3,12})[0-9]{4}[-]*(0,1)[A-Za-z]{2}(,0,1)[0-9]{5}[-]{0-9}(4)	Count Unique	[1-9]([0-9]{3,12})[0-9]{4}[-]*(0,1)n*(0,1)(w)(2)(s+)(d)(3)
Pattern	Action								
[1-9]([0-9]{3,12})[0-9]{4}[-]*(0,1)[A-Za-z]{2}(,0,1)[0-9]{5}	Count Unique								
[1-9]([0-9]{3,12})[0-9]{4}[-]*(0,1)[A-Za-z]{2}(,0,1)[0-9]{5}[-]{0-9}(4)	Count Unique								
[1-9]([0-9]{3,12})[0-9]{4}[-]*(0,1)n*(0,1)(w)(2)(s+)(d)(3)	Count Unique								

**What sets Zscaler Data Protection apart?**

Granular DLP policy based on users, groups, dept and location

Extended boolean logic for building exceptions

Incident Mgmt. via SIEM, email, ticketing & on-prem incident receiver

So the first one is the predefined dictionary. With the Zscaler DLP engine we provide hundreds of predefined classifiers to identify PCI data, PII data, and PHI (protected health information) data. Of course, within the PCI industry, credit card number is a very popular dictionary. If you are trying to protect PII data, it is perhaps someone’s Social Security number in the US, but a UK tax ID number for UK users, or Canadian Scene (now known as Scene+) numbers, or different countries that have different PII IDs. We support hundreds of them today. In the PHI world, we are looking at ICD-10 (International Classification of Diseases, Tenth Revision) codes, CPT (Current Procedural Terminology) codes, different medical dictionaries, and things like that.

Many of these predefined dictionaries are built based on standard regex and PCRE (Perl Compatible Regular Expressions) engines. But in many of these dictionaries we have also utilized AI and ML. For example, we have a dictionary that identifies source code. You cannot



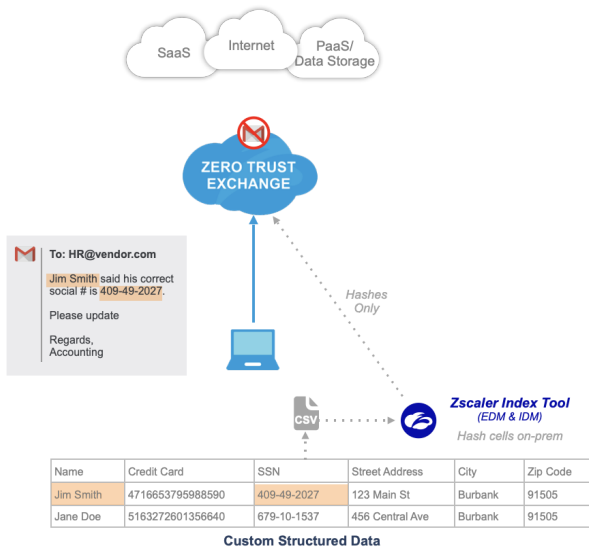
write a regex to identify source code, so we had to lean on AI and ML. Same thing for financial statements, profanity, adult languages, and so on.

Beside predefined dictionaries, we also offer a custom dictionary engine. Our customers can build their own dictionary based on different phrases, keywords and patterns, and regular expressions. Perhaps you are trying to protect documents that have a header and footer company-confidential or internal-use only. So you can definitely leverage our custom dictionaries for that. Now the way the DLP policy works is that you take these predefined dictionaries and custom dictionaries, you build a DLP engine, perhaps by combining both predefined dictionaries and custom dictionaries using different Boolean logic - like AND or NOT. And then once you build these DLP engines, then you take those engines and apply that to a policy.

Let's take the Zscaler credit card dictionary. Any document that has 50 credit card numbers, I'm interested to know. And, combine that with another predefined dictionary called employee's first name, and then combine these two dictionaries with a custom dictionary that says Company Confidential. Essentially you have combined a predefined dictionary with a custom dictionary with different Boolean logic. You build that DLP engine, and then now you take that engine and apply that engine to a policy. The predefined dictionaries, custom dictionaries, the engines, those are basic building blocks for DLP.

Many large enterprise customers - majors - go above and beyond just building DLP policies using dictionaries and engines. Exact data match is a very popular feature within our existing install base. Here, the customers want us to match their exact data and then based on their exact data, they want us to take different actions. So here we are not triggering a DLP policy because we saw a generic credit card number, but instead we are looking at a very specific credit card number that belongs to that organization.

## Secure Custom Data with Exact Data Match



### 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

EDM (exact data match) was designed to learn from your structured data. Let's say you have a very large database and you want to protect the data. Or let's say you have a large CSV file, where you have 200 million rows, 10 different columns. Each row is representing, let's say, one of your employee's PII info - their first name, their last name, their credit card number, their Social Security number, their address - all of that structure data can be fed to Zscaler's EDM engine, and then the EDM engine will learn from your own data. And then once the learning happens, then the EDM engine is looking at all cloud transactions and matching your exact data and then triggering different types of actions.

The question is how do you feed that data? We never ask our customers to upload their sensitive data in our cloud environment. Instead we give our customers an on-premises VM. That on-premises VM is basically the index tool for EDM. So you would take that on-premises VM, it's essentially a VM image where you would deploy it to your on-premises locations and then you start feeding your data to this on-premises VM. By the way, nobody from Zscaler has access to this on-premises VM because, again, this is a VMware image that you install, you deploy, and you control.

When you feed your structured data to this on-premises VM, it doesn't have to be a manual process. You can automate that whole process. You can point your database to this on-premises VM and then, incrementally, the index tool will fetch your data and then index your data.

Next we take each one of these data elements, create a hash, and then there is a persistent connection between that index tool and our cloud. Then the index tool - as and when it's

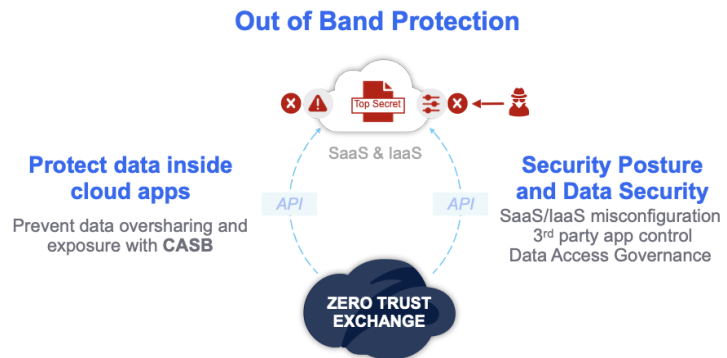
creating a hash for each and every single data element - pushes that hash to our cloud. So in our cloud, we don't store your exact data. All we are storing are a bunch of hash and tokens. And then once that indexing is done - let's say someone is trying to exfiltrate Jim Smith's personal data via email, in the email we see Jim and Smith, we see his exact credit card number - we will do a hash-based lookup and we will hit the exact match. And because of that exact match, then we will take different actions.

## Protecting Data at Rest

### Out of Band Data Protection & SSPM

There are three Data Protection capabilities that Zscaler provides through the Zero Trust Exchange to ensure security for Data at Rest.

When you think about out-of-band CASB, primarily it is designed to secure your data that is sitting at rest in different SaaS-based services and public cloud infrastructure. There are different modules that you should be aware of when you are trying to do dat-at-rest scanning.



#### Top Out-of-Band Use Cases:

<b>Data Discovery</b>	Data at rest introspection
<b>Prevent Data Exposure</b>	Public share, external share
<b>Secure Apps from Threats</b>	Known and unknown malware
<b>Secure Corporate Exchange and Gmail</b>	<ul style="list-style-type: none"> <li>● Inbound email = threat prevention</li> <li>● Outbound email = data loss</li> </ul>
<b>SaaS Security Posture Management (SSPM)</b>	Misconfiguration and Compliance Within data at rest scanning, our out-of-band CASB is also offering SSPM, SaaS security posture management.

There are three things that you need to pay attention to.

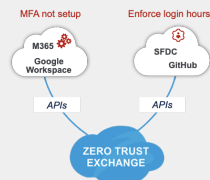
- Today a lot of data exfiltration is happening from your cloud application because someone misconfigured your app. You might have a lot of administrators, some admins are managing your Office 365. Some other admin is managing your Salesforce. With SSPM, what we basically focus on is cloud misconfiguration. So we have built a long list of predefined signatures and then as soon as you onboard your application, we will fire up the signatures. We will get a snapshot of your current configuration and then looking at your configuration, we know which ones are good, which

ones are bad. For example, if the admin did not turn on multi-factor authentication for all your Office 365 apps, that's not a good idea. And we will highlight it based on the signatures and predefined policies that we built.

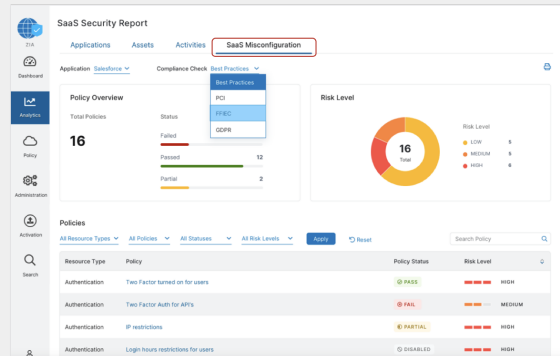
- The second thing about SSPM is all these signatures are automatically mapped to different compliance frameworks. It could be cloud security-based practices, PCI compliance, FFIEC, GDPR. So not only do we highlight your misconfigurations, but we map those misconfigurations into different compliance frameworks so that you don't have any issues with compliance.
- And the third thing about SSPM is when you use applications like Office 365 or Google, potentially, there are hundreds of applications that are connected to your instance of Google and Office 365 from their marketplace. And the users authorize these third-party apps to connect to your corporate Exchange and corporate Gmail, and your OneDrive and SharePoint, and all these cloud applications. That's not a good idea because some of these applications are malicious. So as part of SSPM, we give you a complete discovery of all these third-party apps that are connected via API tokens, service accounts, and so on. And once you have that visibility, then you can build a policy that says, "If you see this application, called Calendly, is connected to my corporate Exchange, to my email application, then revoke the permission, revoke the token so that this application is no longer connected to my corporate instance."

**Protect Data with SSPM (SaaS Security Posture Management)**

**Close dangerous misconfigurations**



- Support for O365, Google Workspace, SFDC and GitHub
- Scan and prioritize risk for non-compliance configurations



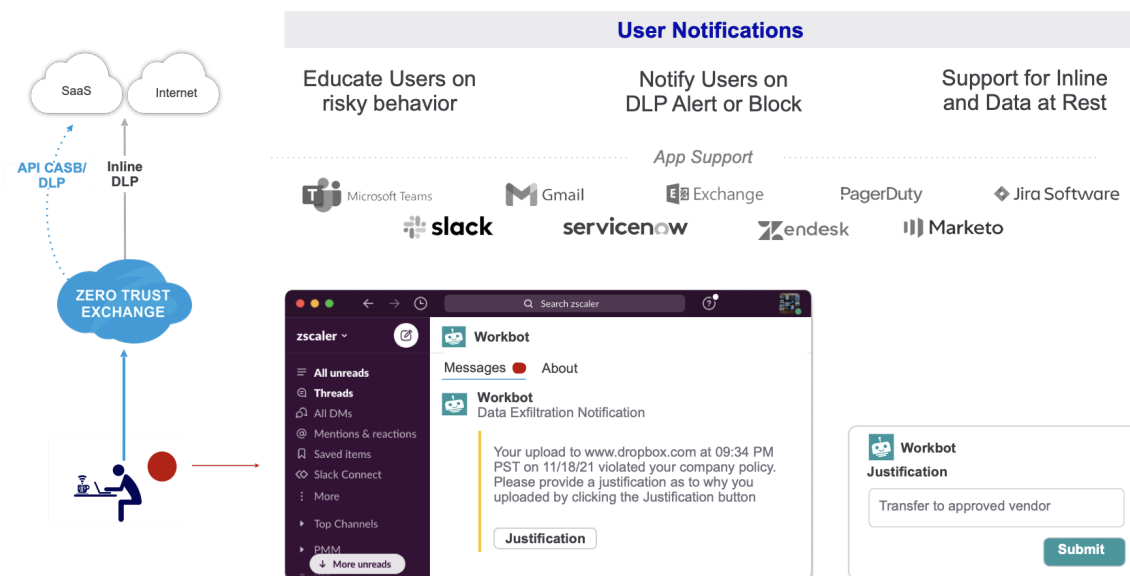
## Incident Management

### Incident Management Capabilities

When adopting Data Protection capabilities such as DLP and CASB, there may be cases where alerts are generated and Administrator teams are asked to troubleshoot and effectively manage these incidents.

When it comes to incident management, the very first thing is about how do I enable the end user so that I can delegate (back to the user) a lot of the violations that I'm seeing today? There are different options available within Zscaler DLP, and CASB. (Our CASB is known as SaaS Security API.)

### User Notifications: Improve Data Protection Workflows



#### Browser-Based

You can use a browser-based notification where you can customize that page with your logo, with your verbiage, and then send those notifications to tell the end user what's going on. If a user is trying to upload sensitive PCI data to their personal Dropbox account, you can block that transaction, you can allow that transaction, but at the same time, you send a user notification through the browser.

#### Application-Based

In many organizations the communication between IT and the end user is happening not through browsers. They prefer a connector where they can actually use Slack notification channels or Teams. And we have built both connectors in our solution. So when you see these violations, you can notify the user via Slack and Teams. And then when you notify

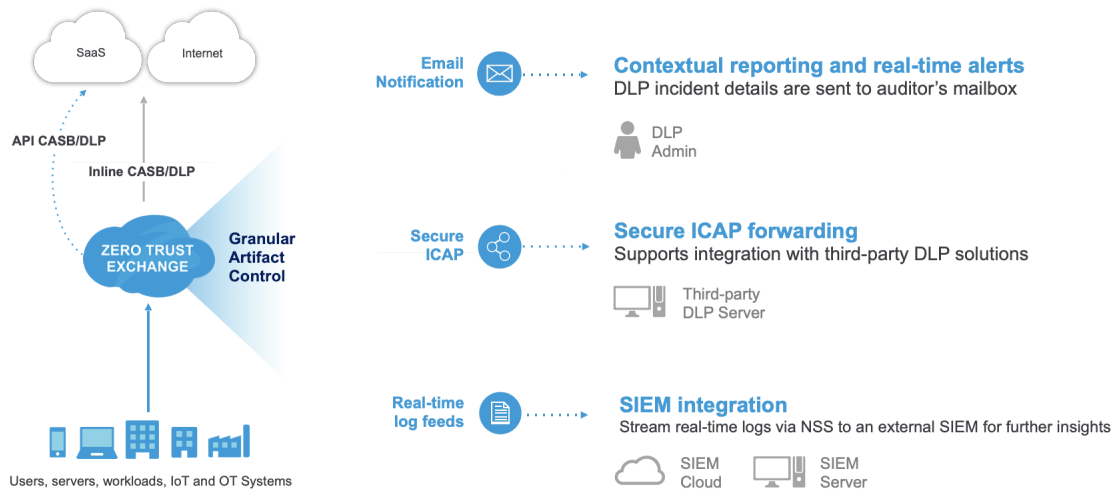
or try to coach the user, you can also do a form POST where you can ask for a justification. That justification comes back to the admin.

### Client Connector Pop-Up

And then the last option we give you is a pop-up through our Zscaler Client Connector that is running on your endpoint. So again, the same idea. If you block a transaction, the Zscaler Client Connector will pop up and then it'll communicate with the user and basically ask for justification, or ask the user not to do this type of violation in the future.

Now focusing on the admin side, there are lots of options available for admins when they have to deal with DLP and CASB incidents. One of the options is email notification. We can also do incident management through SecureICA protocol, and of course we can stream real-time logs and feed that to your SIEM (security information and event management) tools.

### Data Protection: Reporting, Analytics & Incident Management



## Basic Troubleshooting Tools & Support

Troubleshooting & Support will teach you about Zscaler's support ecosystem and how to troubleshoot common issues. Understanding what is happening within the Zero Trust Exchange is important to troubleshoot issues, or to simply report on user access. This chapter explores the reporting capabilities within the platform, and how to extract data. We will also explain how to raise a support ticket, and how to provide necessary data to allow support to assist you in troubleshooting and issues. Learn about Zscaler's Support Services ecosystem and how to troubleshoot common issues by leveraging Zscaler's best practice processes and tools.

---

By the end of this chapter, you will be able to

1. **Leverage** the Self Help support options offered by Zscaler.
2. **Identify** common issues by utilizing Zscaler processes and tools.
3. **Recognize** Zscaler's Customer Support Services and Touch Points.



## Zscaler Self Help Services

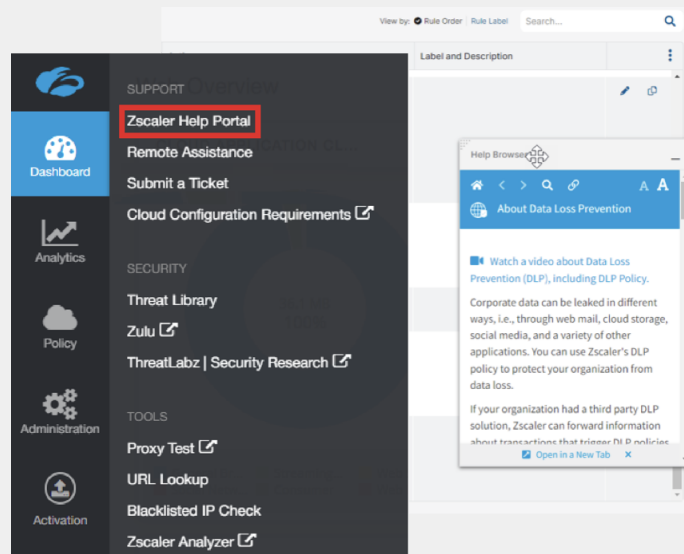
Inevitably, as you go through your secure digital transformation, you will come across questions that you would like answers to and problems that you would like to know how to resolve.

Zscaler provides a valuable Support Services ecosystem to help you more quickly find the information you need in real time and troubleshoot any common issues that may occur.

To get you started in learning about the troubleshooting and support resources Zscaler has available, let's first explore our Self Help Service options.

### Zscaler Help Documentation Portal

Zscaler's Help Documentation portal is the first place you want to go for questions about what something is, how it works, how to configure various capabilities and features, as well as basic troubleshooting with Zscaler.



The portal includes all documentation by product including release notes that are updated as frequently as Zscaler updates products and capabilities in the cloud.

You can also go to the Submit a Ticket option, which will provide a search function within the Customer Portal.

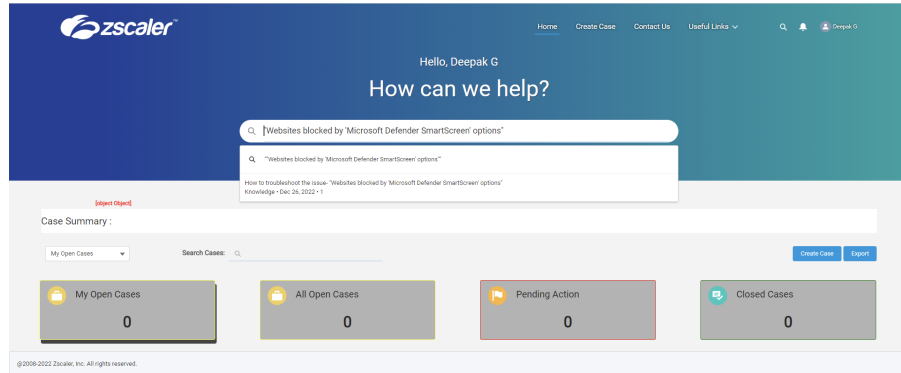
### Zscaler Knowledgebase (KB)

If you run into a more specific problem that you cannot find the answer to within the Help Documentation portal, Zscaler's Knowledge Base (KB) is the next place you will want to look.

Our Knowledge Base is maintained by our Global Customer Service

Engineers, and contains documentation on specific symptoms and solutions that they have worked through with customers.

Knowledge base articles are searchable directly from the Customer Support portal by typing specific topics into the search bar.



## Zscaler Communities

Zenith Community is an open collaborative knowledge base for customers, partners, and users to engage in discussions pertaining to Zscaler products, solutions, programs, events, and training.

These conversation threads contain a rich source of knowledge and information from others around the same topics you may have questions about.

**Zscaler** | **Zenith Community**

- > Faster issue resolution with **self-service**
- > Access to **high-quality content**
- > **Recognition** as a valued participant

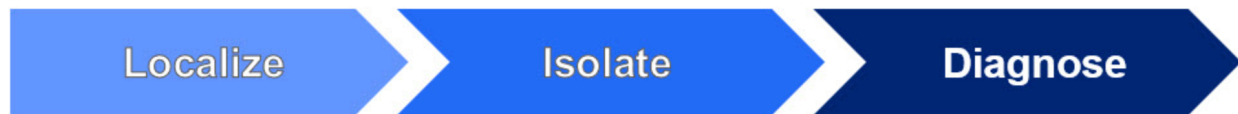
You can be an **Influencer Advocate Engager** on [community.zscaler.com](https://community.zscaler.com)

**Zenith Community**  
Inform, Inspire, Act.

THE ENGAGER | THE INFLUENCER | THE ADVOCATE

## Zscaler Troubleshooting Process & Tools

When issues do occur, it's important to have a methodology and logical approach in determining how to localize, isolate, and then diagnose the problem.



Zscaler provides a framework for troubleshooting common issues that occur within Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA).

### Troubleshooting Process

**Localize** With an Internet access connection through Zscaler, an issue can occur in any of the following areas:

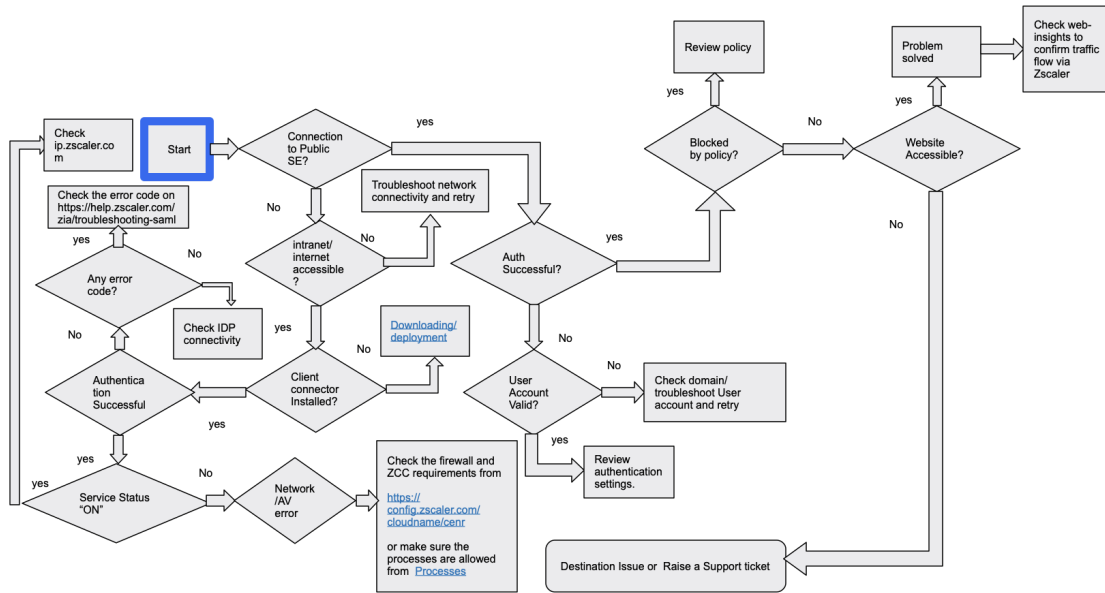
- The end user's device
- Local network (either the user's home network/corporate LAN or coffee shop etc.)
- Between the end user's Corporate Firewall and the Zscaler Cloud
- Between the end user and Zscaler directly
- Between the end user and the identity provider (authentication issues)
- Between Zscaler and the internet (i.e., the third-party website or service)
- With Zscaler Service (infrastructure issues, or misconfigurations of settings or policies, etc.)

**Isolate** Next, isolate which logical process is failing:

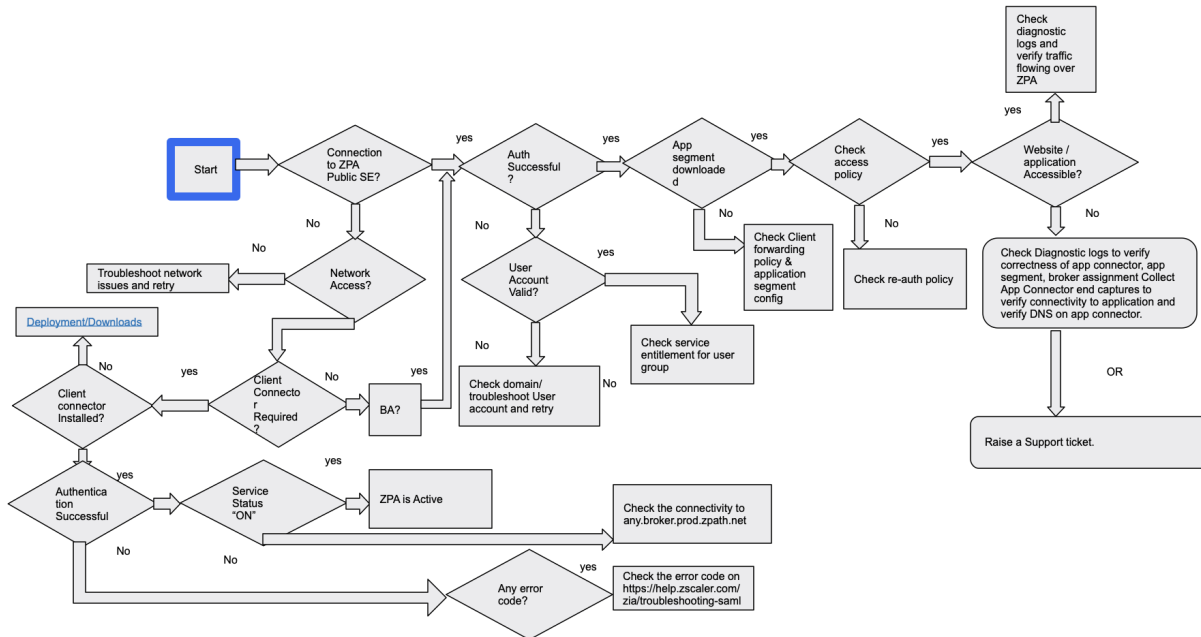
- Are there network connectivity problems?
- Is there a connection issue between specific infrastructure entities?
- Is there some form of misconfiguration of either the network connections or a Zscaler policy?

**Diagnose** Ascertain what the problem is from the information you gathered in the previous steps and plan remedial action

## Zscaler Troubleshooting Process: Troubleshooting Flow: ZIA Connection > Auth > Policy > Internet



## Zscaler Troubleshooting Process: Troubleshooting Flow: ZPA Connection > Auth > Policy > Internet



- Authentication
- Traffic flow through Client Connector
- Application connection - DNS, Firewall, TCP/UDP Networking
- Policy - Allow/Deny, Reauth, Caution, Redirect
- Security - TLS, Inspection, Sandbox
- Data Protection - Rules/Triggers
- Digital Experience - Probes, logs

## Troubleshooting Tools

Proxy Test	The URL <a href="https://ip.zscaler.com/">https://ip.zscaler.com/</a> can be used to verify if you are going through the Zscaler service
Performance Testing	The URL <a href="https://speedtest.zscaler.com">https://speedtest.zscaler.com</a> provides performance testing from the client to the Zscaler service
Admin UI Logs	Load the Insights report from the Zscaler Analytics menu with respect to the modules such as web, firewall, tunnel, or DNS and export the related logs to a file.
Zscaler Analyzer Output	Run Zscaler Analyzer and capture the page load and latency data to the destination in question, both with and without Zscaler
ZCC Packet Capture	Run ZCC packet capture to capture all the traffic from the machine.
ZCC Network Test	The URL <a href="http://127.0.0.1:9000/ztest?q=user@domain.com">http://127.0.0.1:9000/ztest?q=user@domain.com</a> to collect the data: DNS/UDP Reachability, Traceroute, Throttling, Fragmentation, File download Direct/ZCC, Upload/Download bandwidth with/without Zscaler.
Zscaler Trust	The URL <a href="https://trust.zscaler.com/[cloudname].net">https://trust.zscaler.com/[cloudname].net</a> provides information on the overall status of Zscaler services, service availability by DC, information about any recent incidents or advisories, and maintenance notifications. Checking the trust page first when facing any service issues can save a lot of troubleshooting time and effort.

## ZCC Troubleshooting Tools

Zscaler offers troubleshooting tools online and on the Zscaler Client Connector application. On Zscaler Client Connector, you can see the available tools in the Troubleshoot section of the More tab. However, you can enable or disable these tools for users from the Zscaler Client Connector Portal (Administration > Client Connector Support > App Supportability)

Packet Captures: A packet capture is sometimes needed to analyze the network traffic so that we have the option to capture it directly from the ZCC:

Enable Packet Capture	Running the Packet Capture
<p><b>Enabling</b> the Start Packet Capture Option: To enable packet capture for Zscaler Client Connector:</p> <ol style="list-style-type: none"><li>1. In the Zscaler Client Connector Portal, go to Administration.</li><li>2. In the left menu, click Client Connector Support.</li><li>3. On the User Privacy tab, select Enable Local Packet Capture in Zscaler Client Connector if it's not already enabled.</li><li>4. To confirm that the filter driver is enabled from within the Zscaler Client Connector, click More. If the driver is enabled, the Start Packet Capture option appears.</li></ol>	<p><b>Using</b> the Start Packet Capture Option – When reproducing an issue that requires packet capture:</p> <ol style="list-style-type: none"><li>1. In the Zscaler Client Connector, click More.</li><li>2. In the Troubleshoot menu, click Start Packet Capture.</li><li>3. Reproduce the issue.</li><li>4. Click Stop Packet Capture after you reproduce the issue.</li></ol>

Once we export the logs and extract that we receive two pcap files:

CaptureAdapters	CaptureLWF
<p><b>CaptureAdapters.pcap:</b> This shows the entire computer traffic, namely, the tunneled http/https toward Zscaler plus all the other traffic. Everything is handled by ZCC and is to be transferred to the physical interface</p>	<p><b>CaptureLWF.pcap:</b> Show what comes directly from applications (Firefox, Chrome), like all web traffic for tunnel 1.0 or all traffic for Tunnel 2.0, also it will show the ZPA traffic where the destination is from 100.64.x.x range.</p>

A Zscaler Best Practice is to collect the log files using the Export Logs function which will include the packet captures also (if captured) so that they can be exported as a zip file and attached to a support ticket

ZCC Logs: Zscaler offers troubleshooting tools online and on the Zscaler Client Connector application. On Zscaler Client Connector, you can see the available tools in the Troubleshoot section of the More tab. However, you can enable or disable these tools for users from the Client Connector Portal (**Administration > Client Connector Support > App Supportability**)

You can set different log modes determining the type of information the logs store:

Error	logs only when the app encounters an <b>error</b> affecting functionality
Warn	logs when the app is functioning but encountering <b>potential issues</b> or when conditions for the Error log mode are met
Info	logs <b>general app activity</b> or when conditions for the Warn log mode are met
Debug	logs <b>all app activity that could assist Zscaler Support</b> in debugging issues or when conditions for the Info log mode are met

To collect the log files manually, navigate to the following directories for each Operating System (OS):

Windows	C:\ProgramData\Zscaler
MacOS	~/Library/Application Support/com.zscaler.Zscaler/ /Library/Application Support/Zscaler/
Linux	/var/log/zscaler/.Zscaler/logs

Exporting Logs from ZCC: Right click on Tray Icon to Export the logs or Export Logs from “More” options in debug mode. Exporting logs is the preferred method (ZIP file).

When to open which log file:

AppInfo	To leverage information about system, application, CPU utilization, Route print etc. for troubleshooting issues.
Setupapi.dev	To troubleshoot installation issues (such as driver error coming during the installation).
ZSAAuth	To extract Authentication logs / API admin keepalives.
ZSAService	To extract sessions and registry information <a href="https://help.zscaler.com/z-app/zscaler-app-registry-keys">https://help.zscaler.com/z-app/zscaler-app-registry-keys</a>
ZSATray	To inspect anything that is coming up as an error on the Zscaler client connector would be there under ZSATray logs
ZSATunnel	To inspect connection to service edge, Zscaler Client Connector Portal, or any application we are accessing.
ZSAUpdate	To dissect issues arising when the ZCC is attempting to update to any particular version or to the latest version.

By checking the respective log files corresponding to the issue, you can identify where the issue is so that you can take the required action accordingly e.g. If you are facing an authentication issue, then you can refer to ZSA Auth logs.

### **SAML: Understanding and Collecting Logs**

SAML logs can be collected via header traces to see the exchange of SAML either using:

- **browser’s settings > More tools > Developer Tools > Network**
- **Fiddler**

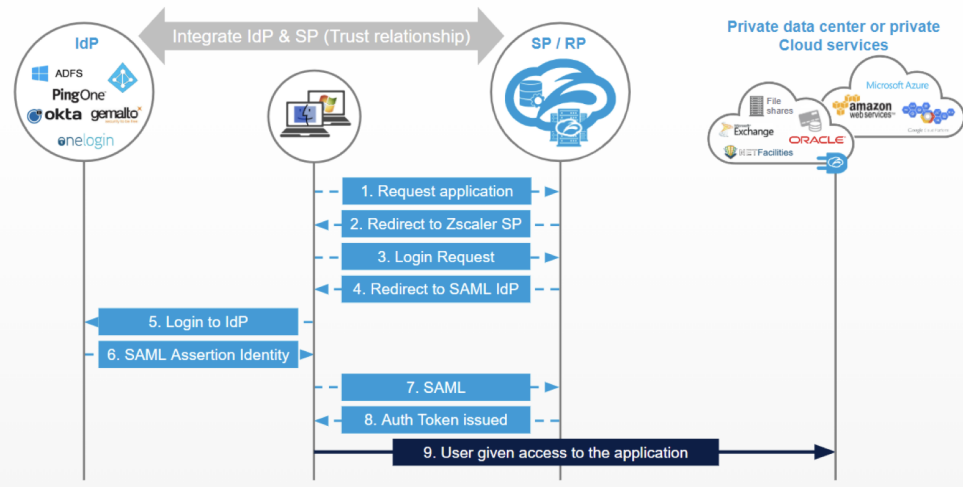
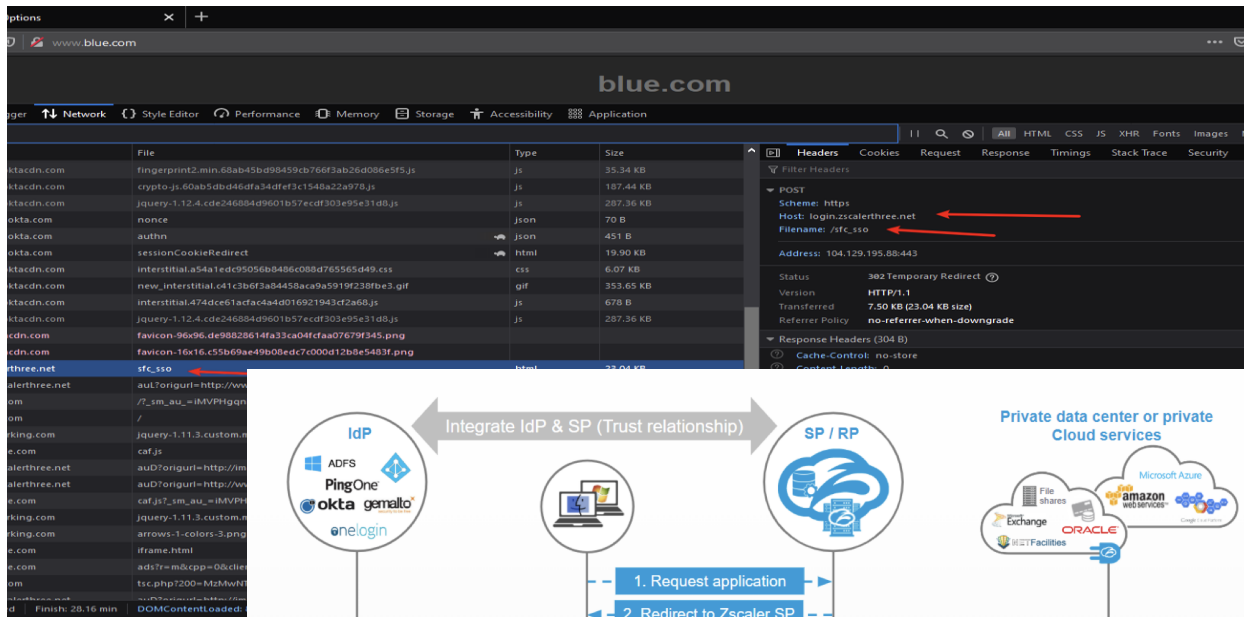
You can use any browser to collect the SAML logs. A browser dedicated (not a Zscaler dedicated) SAML tracer extension can be downloaded with respect to the:

- **Chrome: Home > Extension > SAML Message Decoder**
- **Firefox: Add-ons Manager > SAML Message Decoder**

These tools will help collect the SAML encoded information which can be decoded later with any SAML decoder.

After collecting the headers: You can look for the POST requests against the **login.<cloudname>.net** and/or **samlsp.private.zscaler.com** URL





From the same request, you can fetch the SAML code and that can be decoded with any SAML decoder.

The information can be collected by using the URL <https://samisp.private.zscaler.com/auth/v2/login?domain=<domain>&ssotype=test> on the browser after putting the domain information, **This will show the logs in plaintext format.**

## Zscaler Customer Support Services



Provides expertise & tools to help our customers get deployment recommendations and efficiently solve technical issues



Help our customers to derive maximum value from their Zscaler investment while minimizing the operational costs and recurring problems

### Getting the help you need

Zscaler has built multiple support offerings tailored to each organization's unique requirements and needs. The table below provides an overview of capabilities, deliverables, and SLAs:

	Standard	Premium	Premium Plus	Premium Plus 16	Premium Plus 24
<b>Access</b>					
Business Hours Access (8/5)	✓	✓	✓	✓	✓
Access (24/7/365)		✓	✓	✓	✓
Phone / Web Portal / Admin UI	✓	✓	✓	✓	✓
Online Training, User Guides, Articles, etc.	✓	✓	✓	✓	✓
Support Engineers	Level 1 (pool)	Level 2 (pool) 24x7	Level 2 (pool) 24x7	Level 2 (pool) 24x7	Level 2 (pool) 24x7
<b>Technical Account Manager</b>					
TAM Engagement (weekly, monthly, quarterly)			✓	✓	✓
TAM (Shared TAM or Dedicated TAM based on the SKU)			8x5 (Local business hours)	16x5 (2 time zones)	24x5 (3 time zones)
<b>Service Level Objectives</b>					
P1 Response	2 hours	30 mins	15 mins	15 mins	15 mins
P2 Response	4 hours	1 hour	30 mins	30 mins	30 mins
P3 Response	12 hours	3 hours	2 hours	2 hours	2 hours
P4 Response	48 hours	4 hours	4 hours	4 hours	4 hours

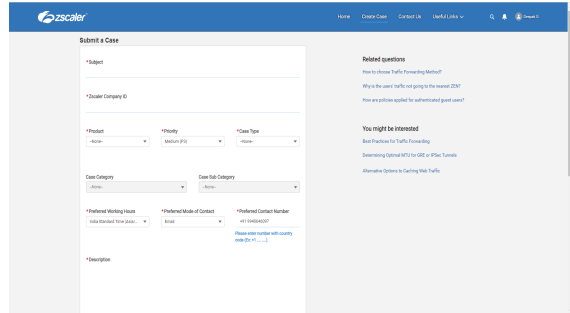
Premium Support is a paid upgrade from our default embedded Standard Support with the license purchase. Premium Support subscription customers meeting certain criteria qualify for the elevated Premium Plus services, with the assignment of a Technical Account Manager (TAM) supplemented by Zscaler's senior support engineers for an enhanced support experience



Assisted Service

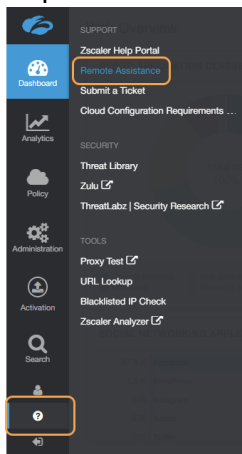
## Submitting a support ticket via the admin console:

- Fastest way to submit a ticket
- Login to the admin console and submit a case
- Provide a “Preferred Contact Time Zone” to enable the support team to call you when you are available



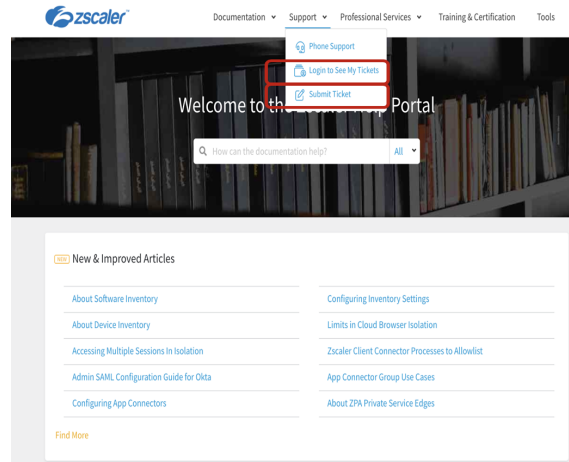
## Remote Assistance

- Enabling remote assistance in READ ONLY mode enables our support team to review your configuration and assist you efficiently
- Logs can be anonymized to ensure privacy requirements are met



## Submitting a support ticket via the web form:

For customers who do not have access to the Zscaler console, tickets can be submitted via a web form.



## ZIA - Submit Ticket

**US Government Customers (FedRAMP):** For US customer support, please use the Zscaler Help Portal for Government at <https://help.zscaler.gov.net>

Product \*  
ZIA

Case Type \*  
-- Select --

Subject \*  
Enter subject

Priority \*  
Medium (P3)

Zscaler Company ID \*  
Enter organization

Description \*  
Write here... 5000 remaining

First Name \*  
Enter first name

Last Name \*  
Enter last name

Email Address \*  
abc@company.com

Preferred Contact Phone Number \*  
+ 081234 56789

Collaborator (CC) List  
Separate multiple email addresses with a semi-colon

Preferred Working Hours \*  
-- Select --

Preferred Mode of Communication \*  
-- Select --

By requesting support, you authorize Zscaler's support personnel to access your customer logs, only if required, for the limited purposes of responding to and troubleshooting this support request.

**Submit**

Ticket submissions from the ZIA Admin Portal provides a better response time and SLA compliance because it gives Zscaler additional information about your account. This form should be used only if you cannot reach the ZIA Admin Portal.

## Phone Support

To get live access to one of our support engineers, you can directly call our phone support.

## Zscaler Support Services: Components of Zscaler Support Ticket

Component	Description
Issue Subject	Provide a summary of the problem with the main symptom and scope. This is a free-text field; it should be as concise as possible but give a complete indication of the nature of the problem
Description	Provide a detailed description of the problem. This is a free-text field that allows you to fully explain what the nature of the problem is, what its symptoms are, where and when the problem occurs, what process you suspect is at fault, and what steps you have taken to identify the problem or what corrective actions you have taken with no success
Ticket Type	Select from the available types: "Problem," "Question," "Categorization," or "Provisioning."
Ticket Priority	Select from the available priorities: "Urgent," "High," "Medium," or "Low."

## Zscaler Support Ticket- General Information Gathering

Information to be gathered to move the support ticket forward:

Information to be gathered:	Issue type:
Traffic Forwarding Method	Which traffic forwarding method is used (IPsec Tunnel (VPN); GRE Tunnel; PAC over IPsec; PAC over GRE; PAC Only; Proxy Chaining; Private or Virtual Service Edge; Explicit Proxy; Zscaler Client Connector)?
Zscaler Cloud	Which Zscaler Cloud(s) are experiencing the issue?
Zscaler Data Centers Used	Which Zscaler data centers are used (the ZIA Public Service Edge from the ip.zscaler.com output)?."
Problem / Incidents Period	When did the problem start? When did it stop? Is it ongoing?
Issue Scope	What is the scope (intermittent or always; all or some data centers; all or some sites; all or some users; all or some end-user website destinations) of the issue?
Trigger Event	What seems to have triggered this event?
Work-Around	Is there a work-around? Has it been applied?
Supporting Resources	Are there proxy text screenshots, Zscaler Analyzer outputs, or server/firewall/router or Zscaler Client logs?

## Zscaler Support Services: Zscaler Support Ticket- General Information Gathering: Support Resources

Information to be gathered as per issue type so the support engineer can investigate.

Information to be gathered:	Issue type:
Application URLs, client/server IPs	Connectivity and performance issues.
Header traces	When the website is not loading properly.
Zscaler client connector logs	When ZCC is failing to connect to a Service Edge (Connection error) or Captive portal detection or firewall error.
Packet Captures	When we are not able to connect to Service edge or particular application is not loading.
ZMTR	When we observe the latency in the network.
Speedtest.zscaler.com	When we observe the latency in the network and want to check the network speed.
Web-insights	To check the response code for a particular URL and if the SSL inspection is performed or not.
ip.zscaler.com	When the website/application is not loading.

You explored the three self help portals as a place to start on your troubleshooting journey, and you discovered the process and tools Zscaler recommends that you utilize.

Later, should you proceed with EDU-202: Zscaler for Users – Advanced, you will be presented with common troubleshooting scenarios for a wide range of scenarios along with how to localize, isolate, and diagnose the problem.