

Slide 1 - Zscaler Private Access



Zscaler Private Access

Authentication with SAML – Overview

©2019 Zscaler, Inc. All rights reserved.

Slide notes

Welcome to this training module on Zscaler user authentication with SAML, an important component of the Zscaler Private Access solution.

Slide 2 - Navigating the eLearning Module



Navigating the eLearning Module



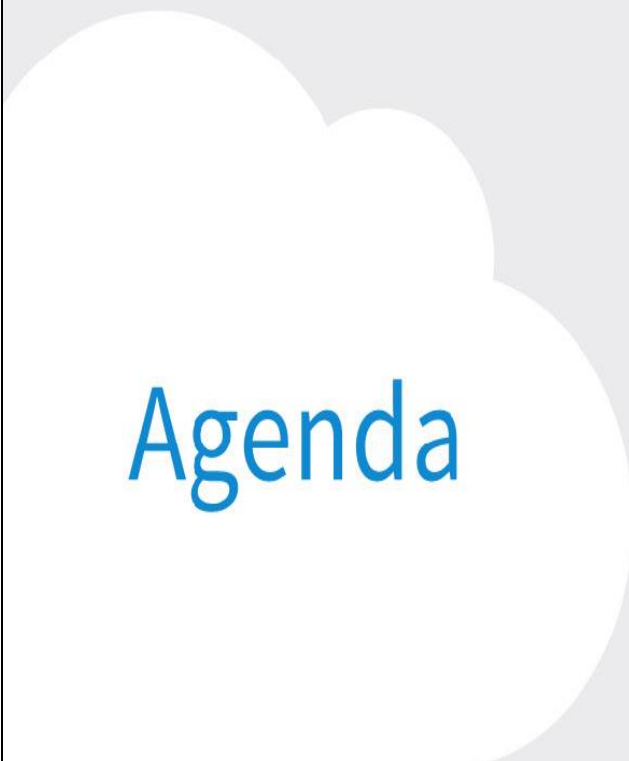

The screenshot displays the Zscaler Cloud Portal dashboard. At the top, there is a navigation bar with links for Dashboard, Analytics, Policy, and Administration. The main content area features several charts and tables, including 'Cloud Application Classes', 'Top URL Categories', 'Top Users', 'Streaming Media Applications', and 'Top Advanced Threats'. Overlaid on the bottom of the dashboard are several blue callout boxes with white text, each pointing to a specific control:

- Exit**: Points to the 'X' button in the top right corner of the dashboard window.
- Previous Slide**: Points to the left arrow button in the video player controls.
- Next Slide**: Points to the right arrow button in the video player controls.
- Play/Pause**: Points to the play/pause button in the video player controls.
- Fast Forward**: Points to the fast forward button in the video player controls.
- Progress Bar**: Points to the progress bar in the video player controls.
- Audio On/Off**: Points to the audio icon in the video player controls.
- Closed Captioning**: Points to the closed captioning icon in the video player controls.

Slide notes

Here is a quick guide to navigating this module. There are various controls for playback including **Play** and **Pause**, **Previous**, **Next** slide and **Fast Forward**. You can also **Mute** the audio or enable **Closed Captioning** which will cause a transcript of the module to be displayed on the screen. Finally, you can click the **X** button at the top to exit.

Slide 3 - Agenda



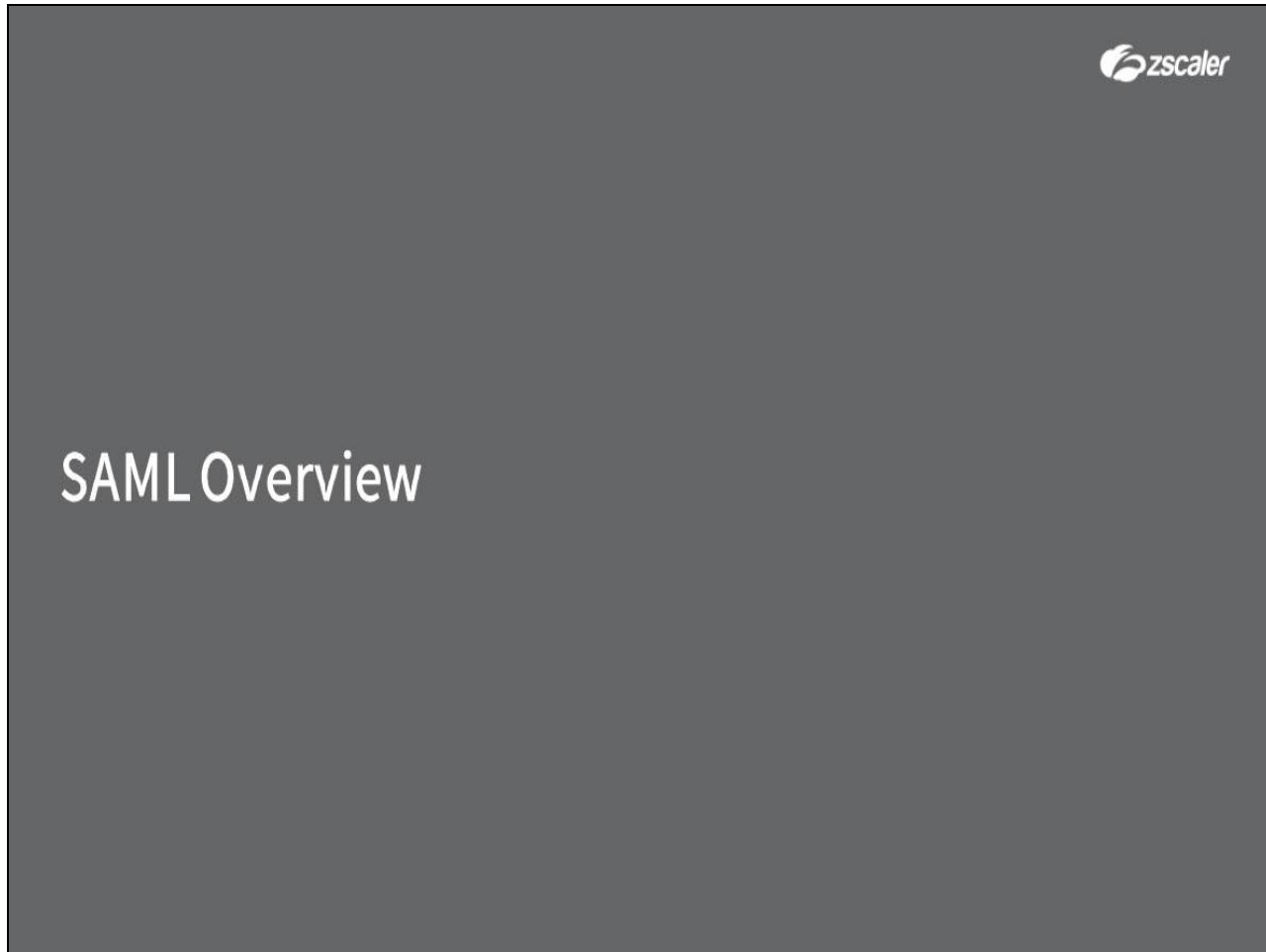
Agenda

- SAML Overview
- SAML User / Administrator Authentication for ZPA
- ZPA Support for Multiple SAML IdPs

Slide notes

In this module, we will first look at SAML in overview; look at the SAML user or administrator authentication process for ZPA; and finally, have a look at ZPA support for multiple SAML Identity Providers (IdPs).


Slide 4 - SAML Overview



Slide notes

In the first section, we will discuss the components of the SAML system, and the available Identity Providers.

Slide 5 - What is SAML



What is SAML

- Security Assertion Markup Language (SAML)
 - Federated Identification Standard for Web Authentication
 - Allows for 'Single Sign-on' (SSO) of users to services
- Components:

Service Provider (SP)

 - Also known as a *Relying party* (RP)
 - Employs the services of an IdP for the identification and authentication of users
 - Zscaler may act as an SP

Slide notes

The Security Assertion Markup Language, or SAML can be used to provide a Single Sign on (SSO) environment for the users of multiple cloud applications. The user signs-in once and can then be automatically signed in to other cloud applications that the user subscribes to, such as Salesforce, or Box, or even Zscaler.

There are three main components of a SAML system, the first of which is the **Service Provider** (or SP - also known in a Microsoft-centric world as a Relying Party (RP)). This is the application that requires users to authenticate before they may gain access to it. Typically, these are your cloud SaaS applications such as SFDC, SAP, or even Zscaler.

Slide 6 - What is SAML



What is SAML

- Security Assertion Markup Language (SAML)
 - Federated Identification Standard for Web Authentication
 - Allows for 'Single Sign-on' (SSO) of users to services
- Components:

Service Provider (SP)	Identity Provider (IdP)
<ul style="list-style-type: none">• Also known as a <i>Relying party</i> (RP)• Employs the services of an IdP for the identification and authentication of users• Zscaler may act as an SP	<ul style="list-style-type: none">• Provides <i>Identifiers</i> and <i>Identity Assertions</i> for users that wish to access a service (IdP examples are: Okta, Ping, AD FS)

Slide notes

The next component is the **Identity Provider** (or IdP for short). This is where the users go (or are sent) to get authenticated in the first place, and an IdP can manage the authentication of users into any application that they have integrated with (giving us the SSO capability). There are many SAML IdPs available, whether cloud-based (such as Okta, or Ping), or on-premise (for example Microsoft AD FS).

Slide 7 - What is SAML



What is SAML

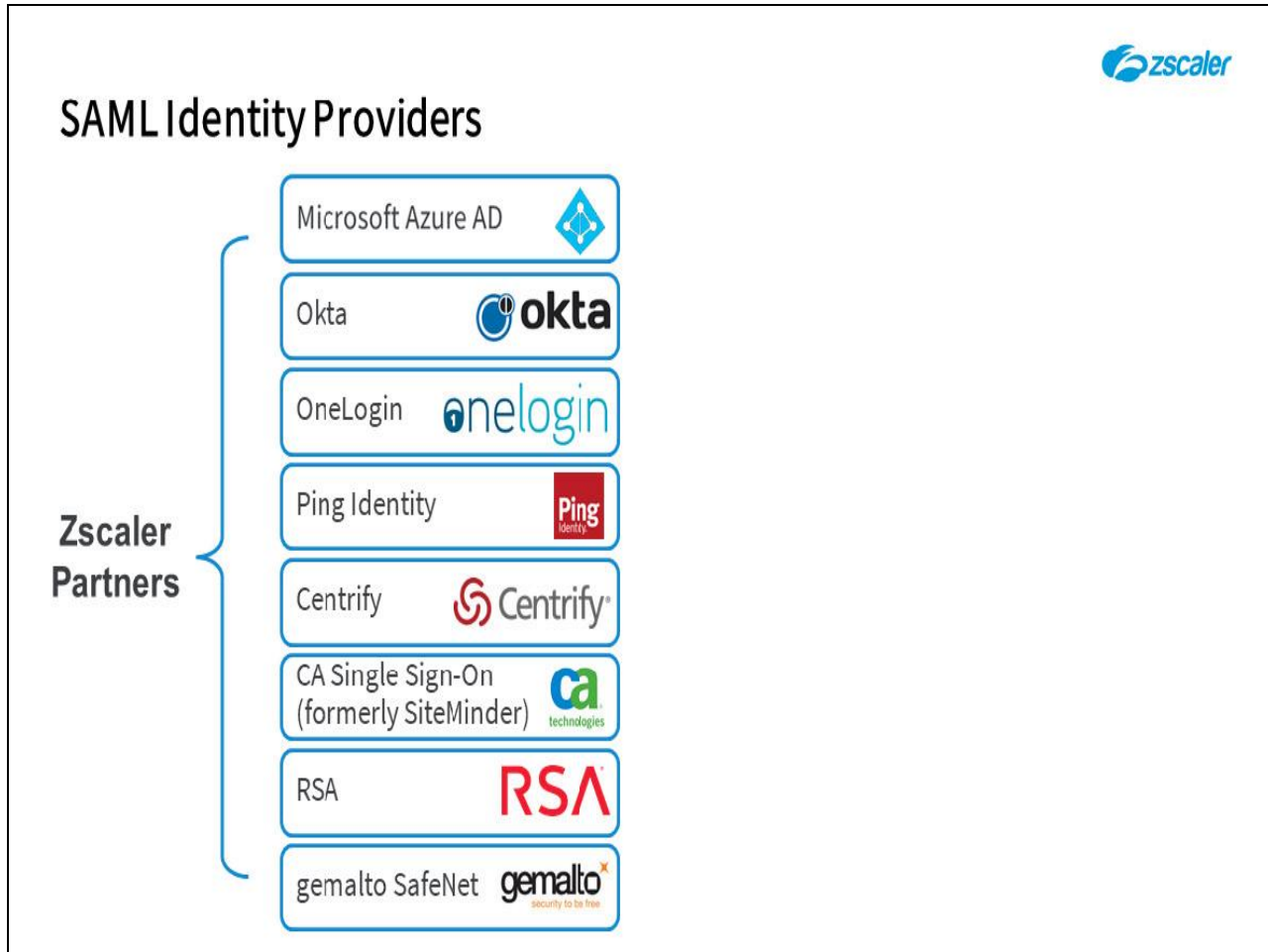
- Security Assertion Markup Language (SAML)
 - Federated Identification Standard for Web Authentication
 - Allows for 'Single Sign-on' (SSO) of users to services
- Components:

Service Provider (SP)	Identity Provider (IdP)	Security Assertions
<ul style="list-style-type: none">• Also known as a <i>Relying party</i> (RP)• Employs the services of an IdP for the identification and authentication of users• Zscaler may act as an SP	<ul style="list-style-type: none">• Provides <i>Identifiers</i> and <i>Identity Assertions</i> for users that wish to access a service (IdP examples are: Okta, Ping, AD FS)	<ul style="list-style-type: none">• Also known as Tokens• Issued to users by IdPs• Presented to SPs / RPs to confirm authentication• Trust based on PKI• Assertions may contain; Authentication, Attribute, or Authorization statements

Slide notes

Finally, there are the **Security Assertions** (also known as **Tokens**) which are given to end users that successfully authenticate to the IdP, as proof that they have authenticated. The tokens are cryptographically secure XML-based containers, with security based on the trust relationship established between the IdP and the SP during setup and integration. They contain the user's authentication status, their identity, and optionally additional authorization attributes with more information about the user, such as department, or group memberships.

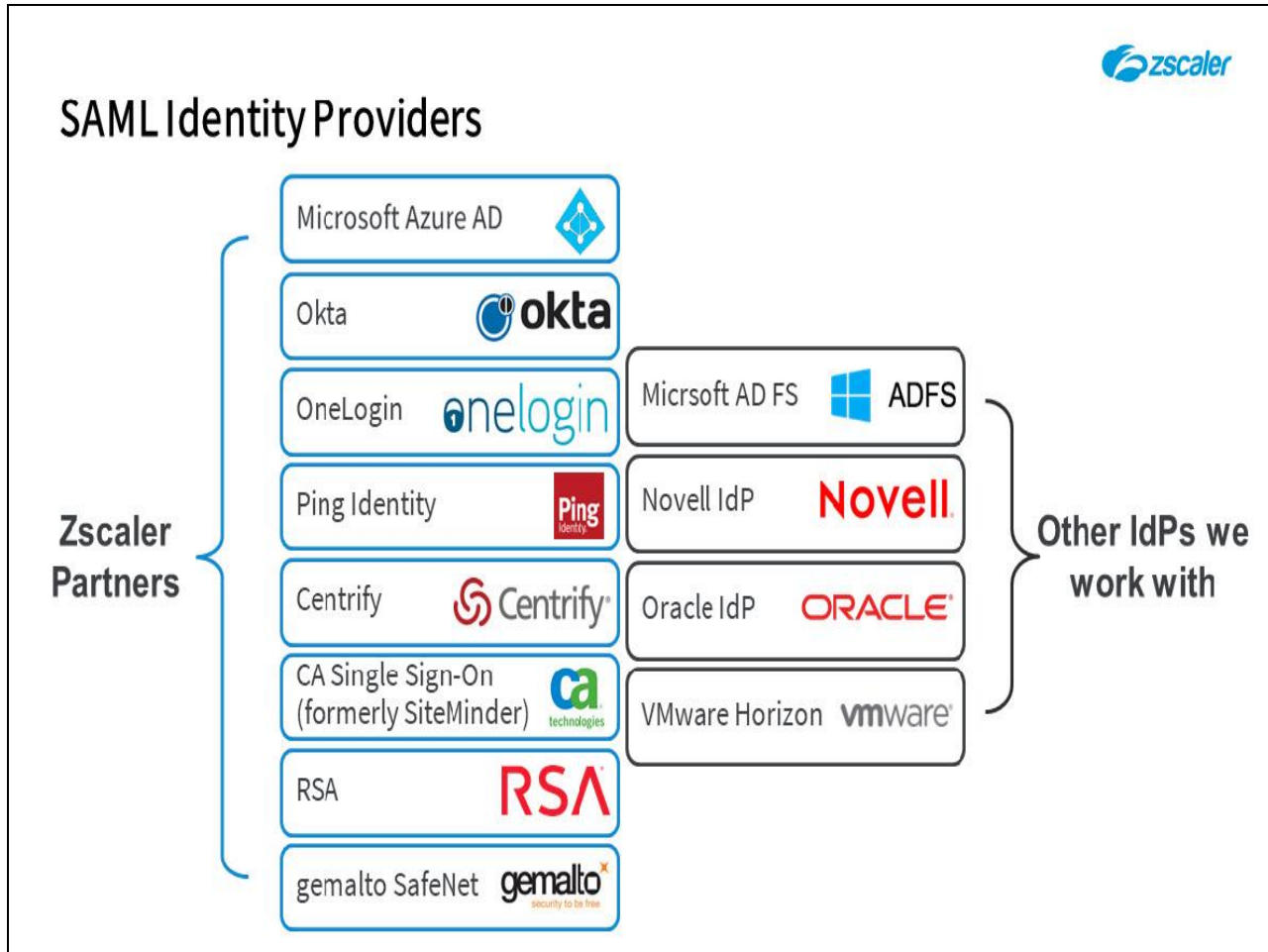
Slide 8 - SAML Identity Providers



Slide notes

SAML is a standards-based protocol so Zscaler integrates with any compliant Identity Provider, such as our authentication partners: Microsoft Azure AD; Okta; OneLogin; Ping Identity; Centrify; CA Single Sign-On (formerly known as SiteMinder); RSA; and the gemalto SafeNet solution.


Slide 9 - SAML Identity Providers



Slide notes

Other vendors that we have successfully integrated with include: Microsoft AD FS; the Novell IdP; the Oracle IdP; and the VMware Horizon solution.

Slide 10 - SAML IdP : In the Cloud or on premise?



SAML IdP : In the Cloud or on premise?

In The Cloud

- No servers to own or maintain
- Generally easier to implement
- Minimized downtime
- Generally, no inbound firewall rules required
- Subscription fee (varies by provider)
- AD sync agent must be installed

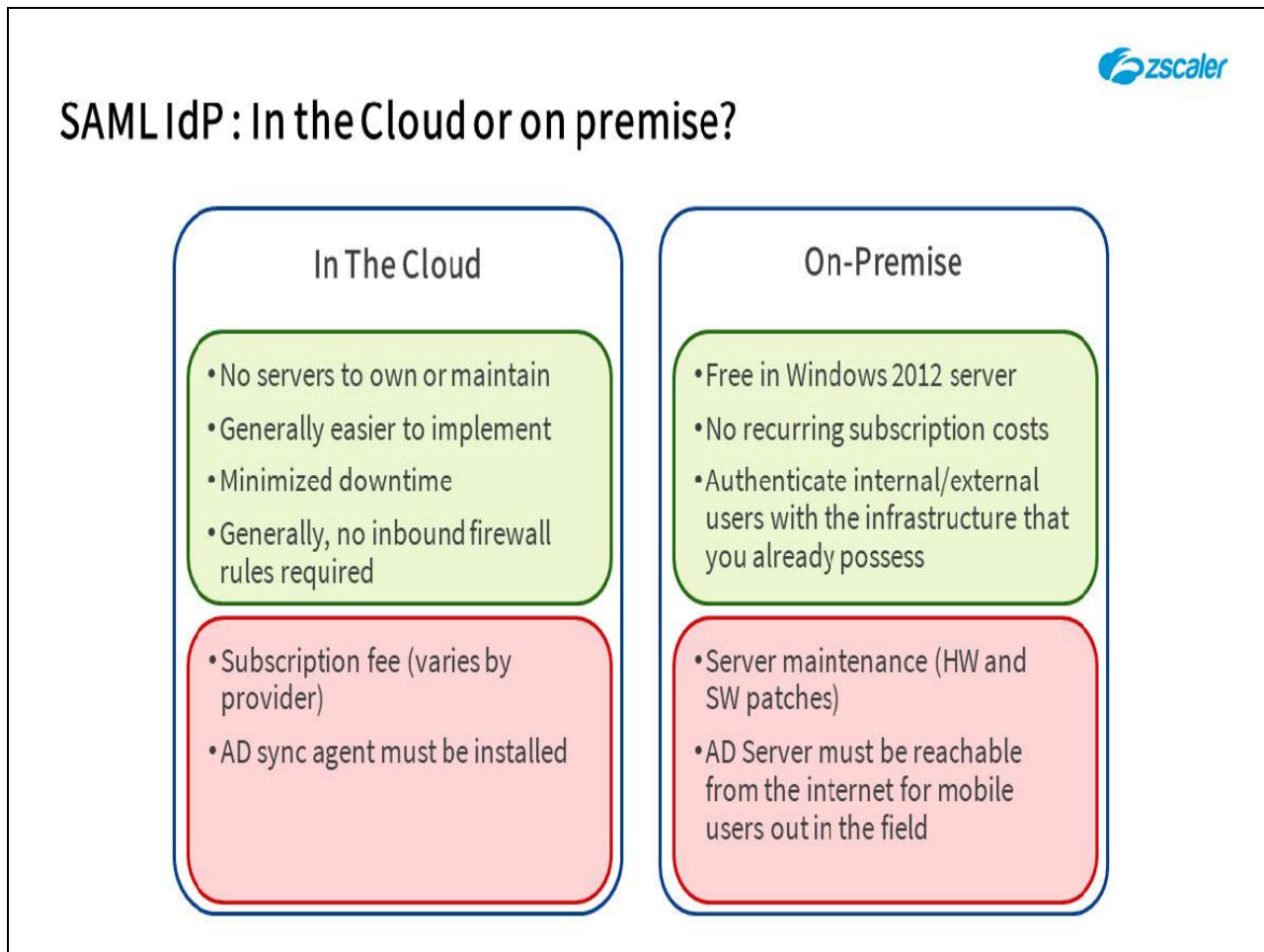
Slide notes

As you have now seen you have multiple options when it comes to choosing your identity provider, one big choice you need to make is whether to use a cloud-based IdP or use an on-premise IdP. Two popular options are: Okta, in the cloud; or Microsoft AD FS on-premise.

Let's take a look at the "Pros" when it comes to using an IdP in the cloud: First, and most obvious, there are no servers to own or maintain; so a Cloud based solution is generally easier to implement; there is minimal downtime as there is no hardware to be maintained and updated; and generally there are no inbound Firewall rules to configure.

Some of the "Cons" for an in the cloud IdP are: That there are subscription fees, which vary by provider; and often times, an Active Directory sync agent must be installed on the Active Directory server to synchronize accounts to the IdP and allow authentication.

Slide 11 - SAML IdP : In the Cloud or on premise?

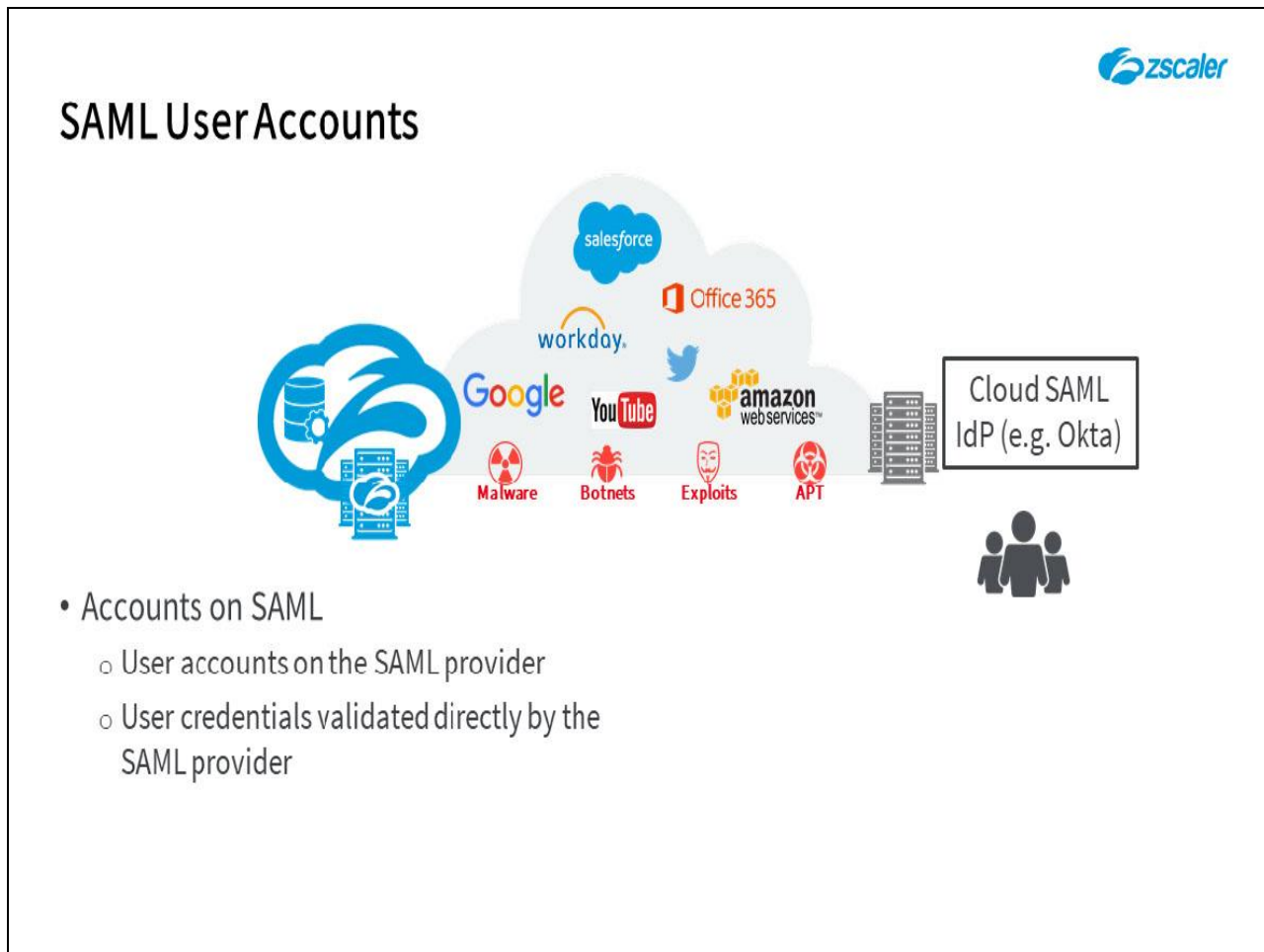


Slide notes

Next, let's take a look at on-premise solutions such as Microsoft AD FS: AD FS is free in Windows server and there are no recurring subscription costs; you can leverage the infrastructure that you already own to authenticate internal, or external users.

Some of the "Cons" of AD FS on-premise are: That there is server maintenance that must be done periodically, both potential hardware and software patches; also, AD must be reachable from the internet for mobile users out in the field which means that an AD FS Proxy is required, and inbound firewall rules must be configured.

Slide 12 - SAML Authentication and Provisioning Options

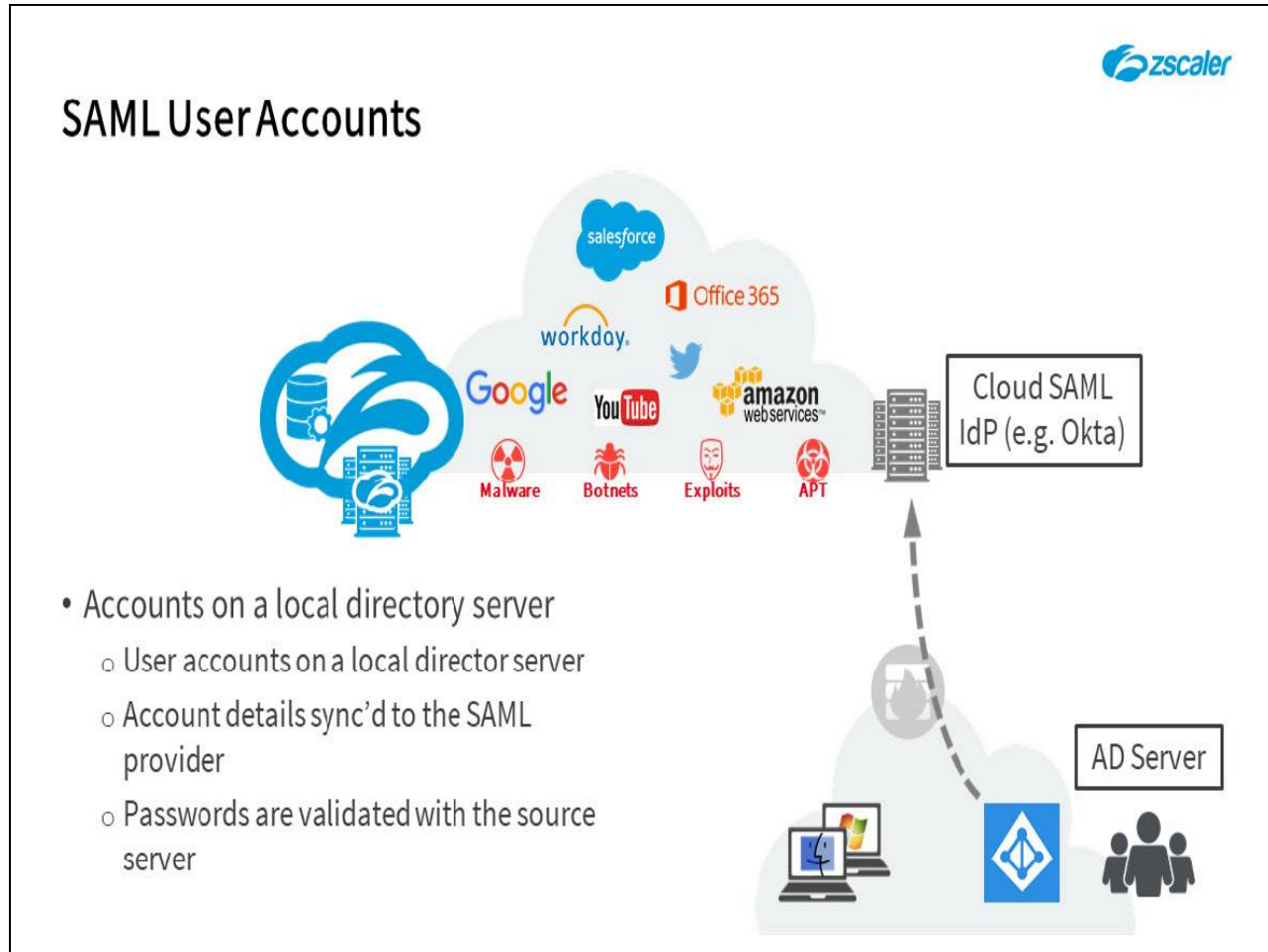


Slide notes

There are two main ways to manage end user accounts with a SAML system. They may exist only on the SAML provider, and users authenticate directly to the IdP using whatever form of credentials are required; simple usernames and passwords, certificate-based, or even multi-factor authentication. Note that the user accounts and whatever attributes you wish to employ must be defined and maintained on the SAML provider directly.

This method is typically NOT deployed in production unless the organization does not have its own authentication scheme such as Active Directory, although it can be useful in Proof of Concept testing.

Slide 13 - SAML Authentication and Provisioning Options

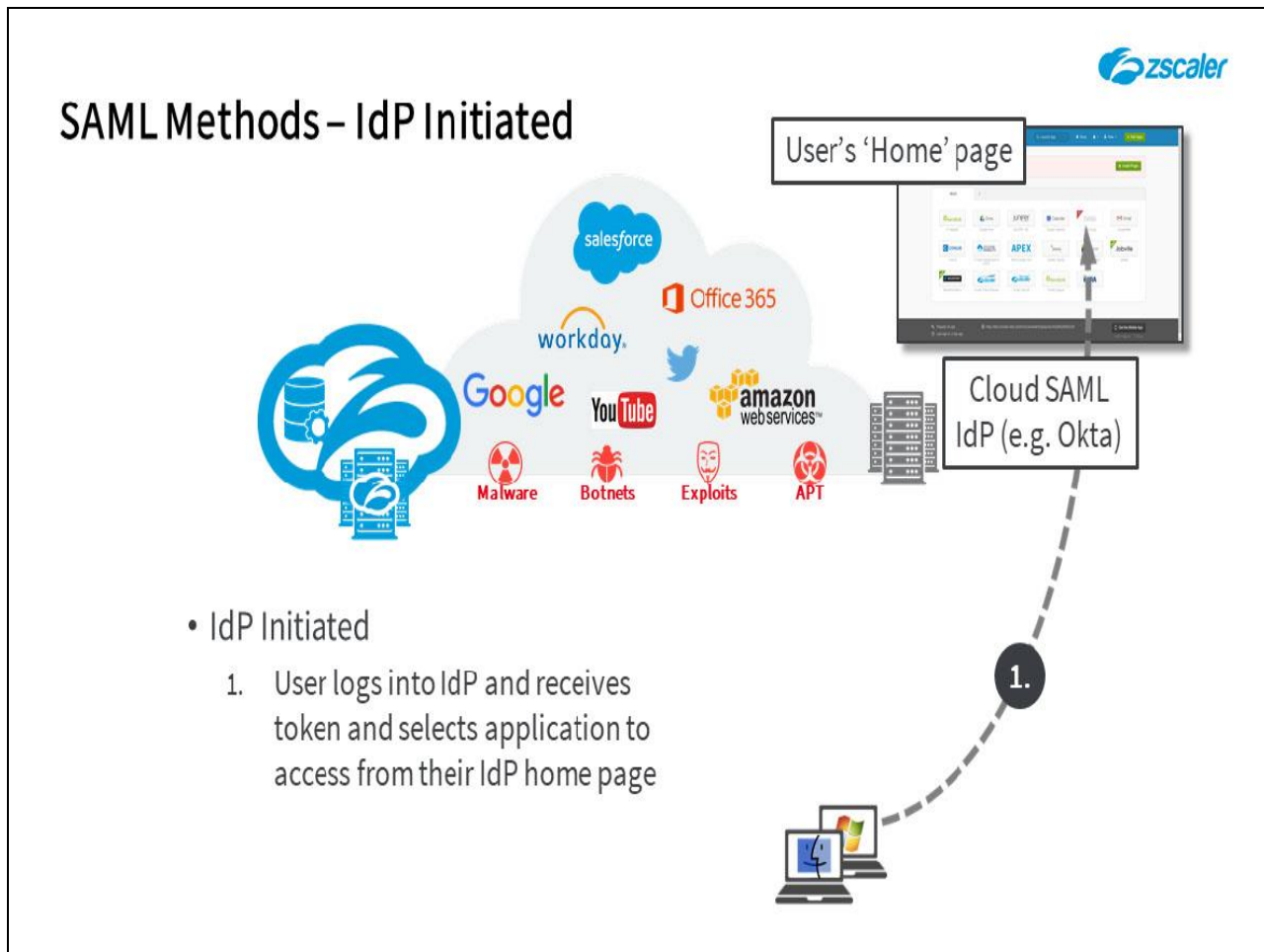


Slide notes

Alternatively (and more commonly), many SAML providers give you the option to synchronize user accounts from an existing directory server, such as Microsoft AD. Typically, this is done on a secure persistent, outbound TCP connection from an agent installed on the AD server. This method saves you the need to separately create accounts on the SAML provider, although you do need to set up the synchronization process and decide what subset of the user attributes you need to sync.

It may also be possible to validate passwords with the source directory server, down the persistent TCP connection, so that user account passwords are never shared with your SAML provider. Multi-factor authentication is also an option with this model.

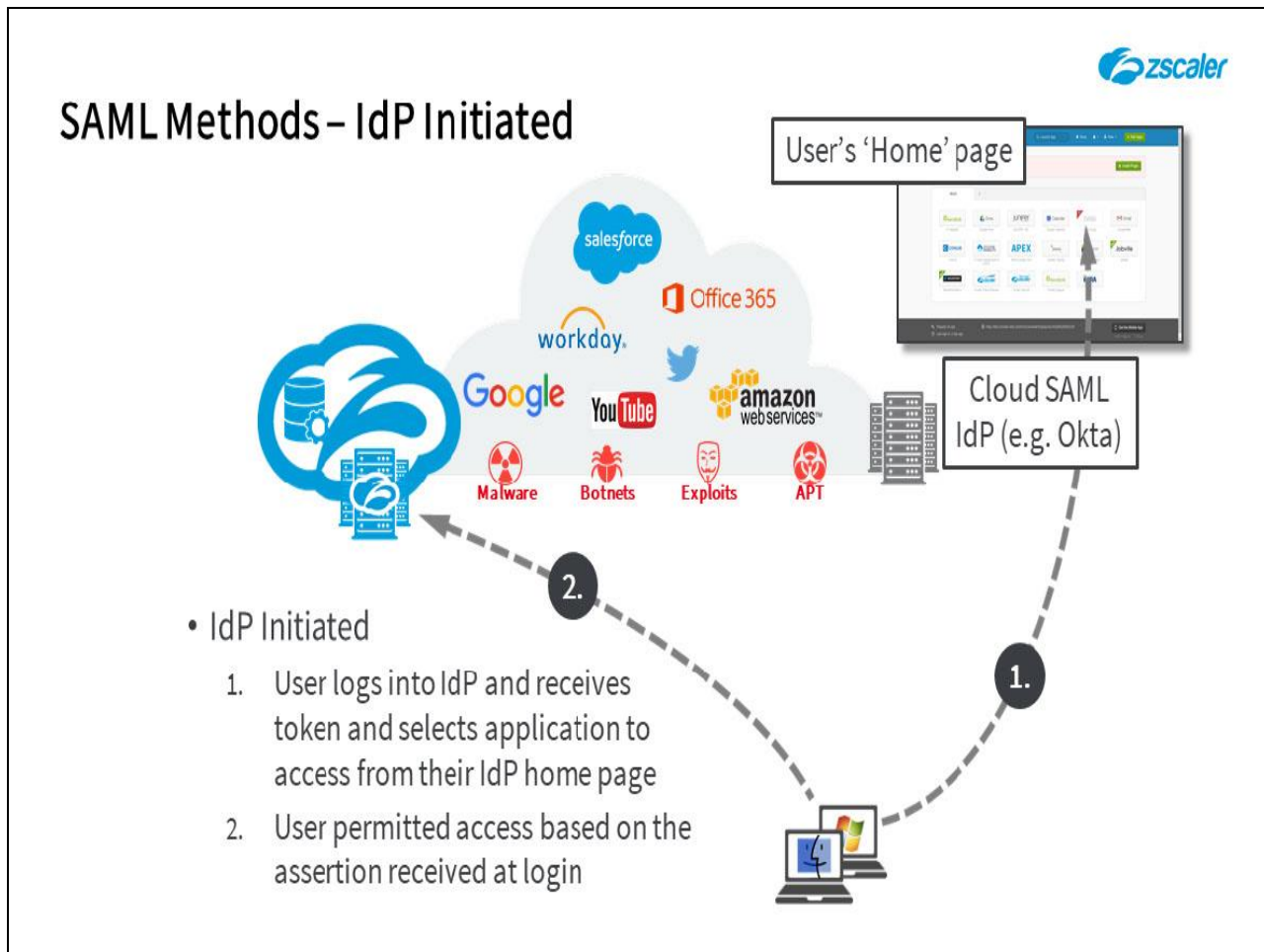
Slide 14 - SAML Methods – IdP Initiated



Slide notes

There are also two main ways for a user to authenticate using SAML, the first method being what is called **IdP Initiated** SAML. With this method, the end user first logs into the IdP itself, at which point they are authenticated and receive their **Token**. Authentication may simply be forms-based (username/password), may be certificate-based, or even multi-factor. After login the end user is typically taken to a Home page on the IdP that lists all of the applications (Service Providers) that are available to them for SSO.

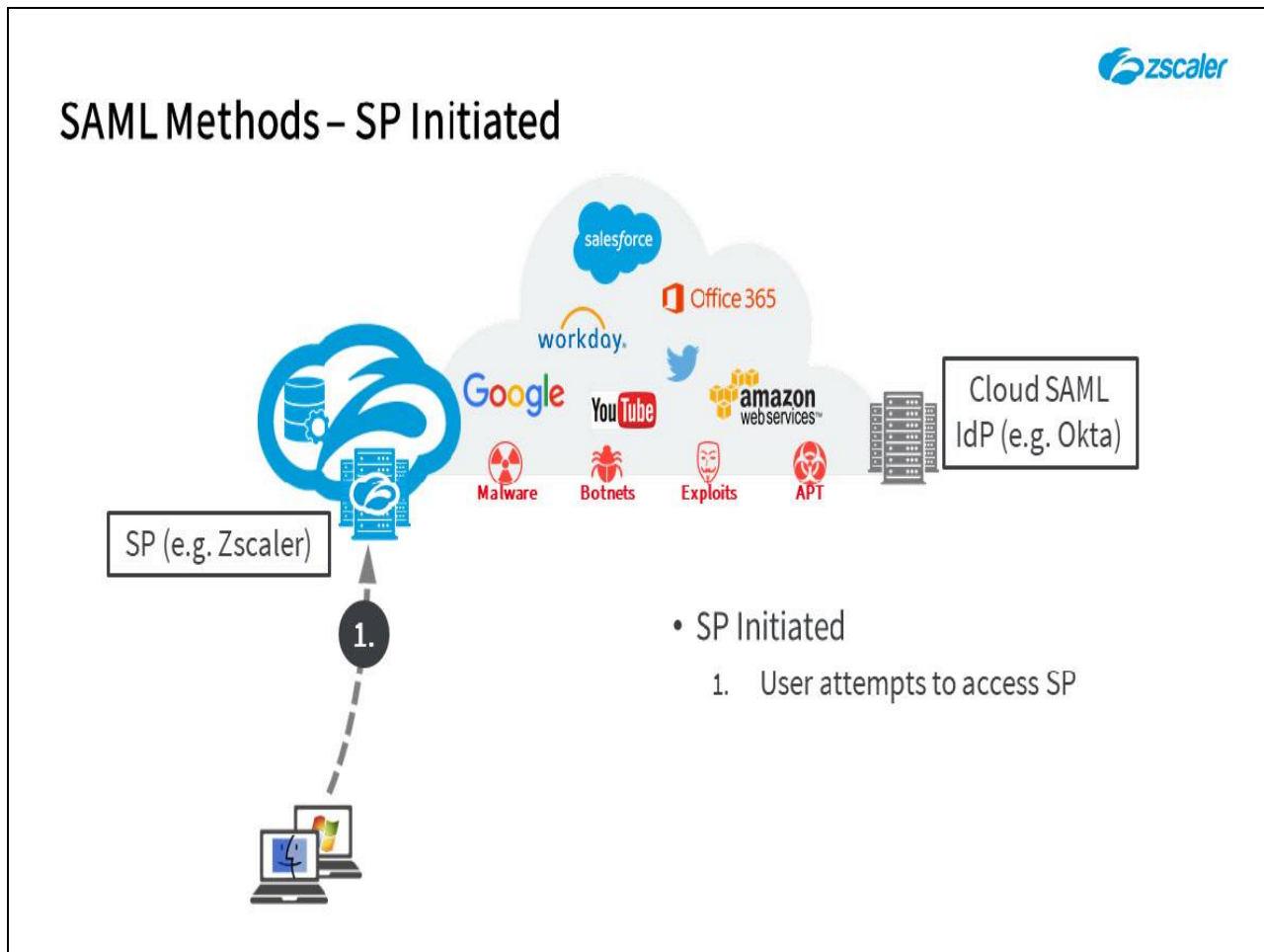
Slide 15 - SAML Methods – IdP Initiated



Slide notes

When the user clicks on one of the applications on their IdP home page, they are redirected to that Service Provider, and they are immediately given access based on the **Token** that they received when logging in to the IdP.

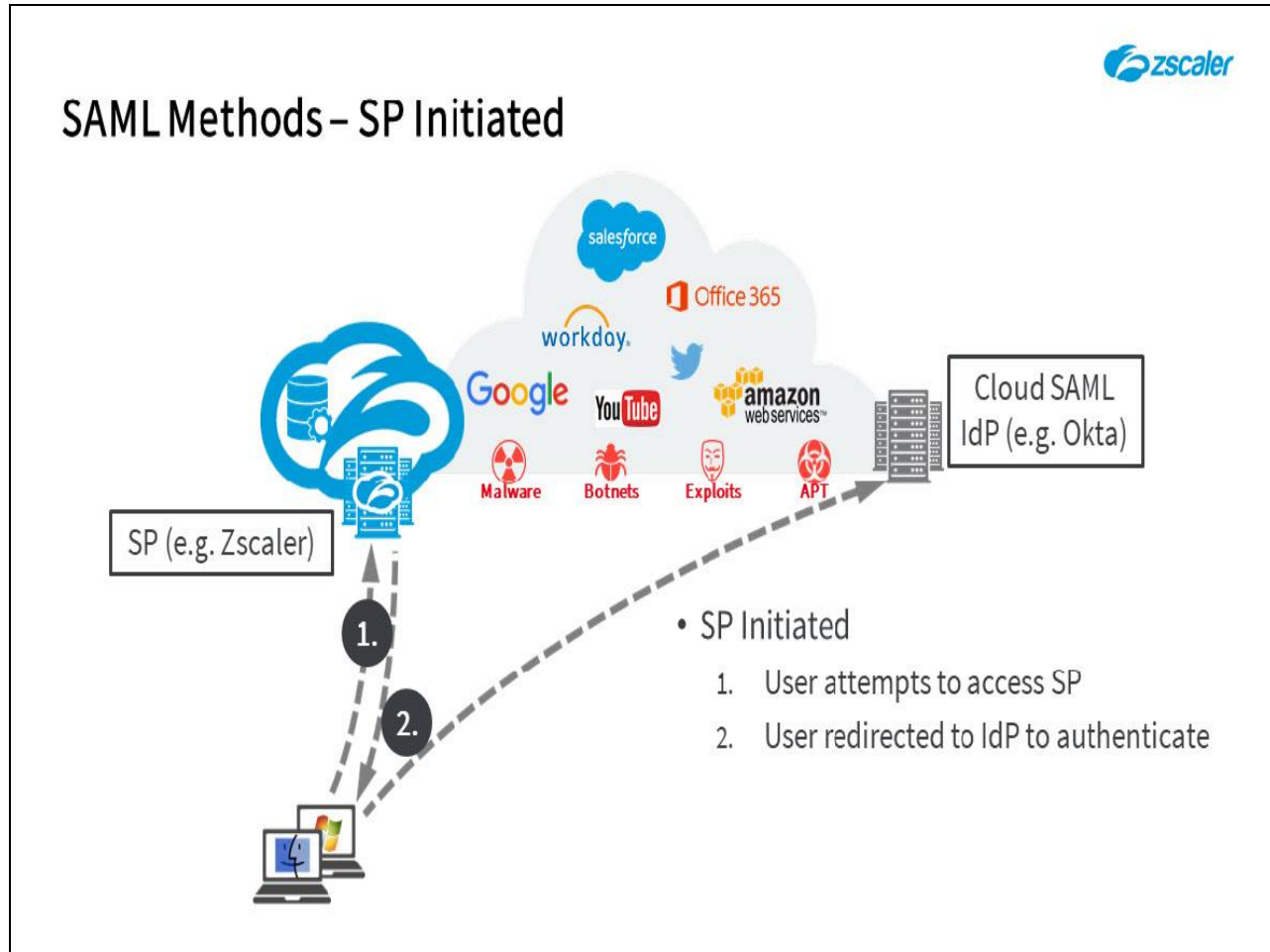
Slide 16 - SAML Methods – SP Initiated



Slide notes

The other, and more common method for user authentication with SAML, is known as the **SP initiated** SAML. With this method, the end user goes direct to the Service Provider and requests access. If they already have a **Token** from a valid IdP, all well and good, and they will be given access immediately. If they don't yet have a **token**, the SP will push back and redirect them to the IdP to be authenticated.

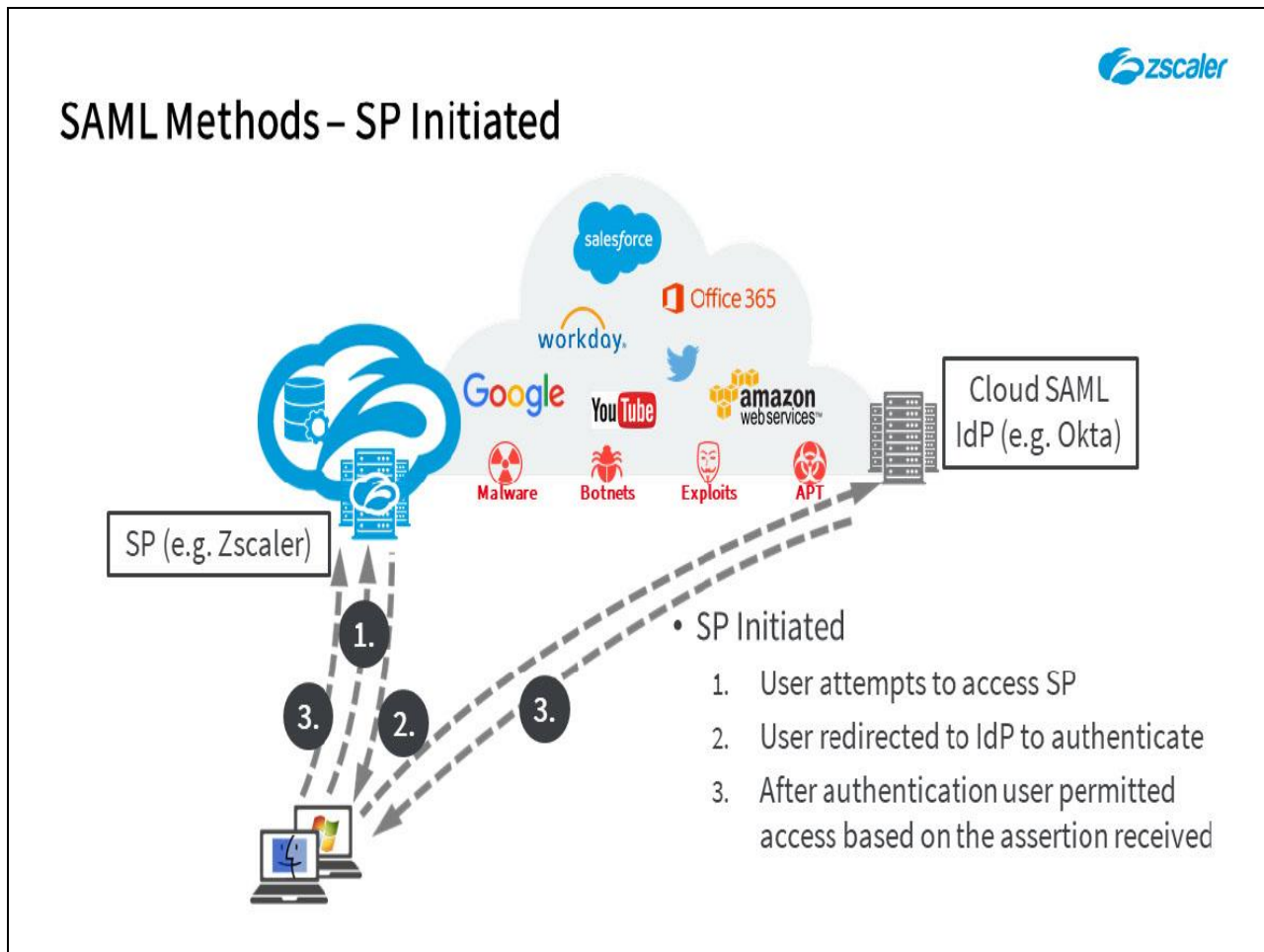
Slide 17 - SAML Methods – SP Initiated



Slide notes

The end user's browser will go to the IdP for authentication using the specified method; forms-based, certificate-based, multi-factor, or whatever is defined on the IdP. If authentication can be done transparently (e.g. using a certificate) the user may not even know that this is happening. Alternatively, at this point they will be presented with an IdP login page so that they can authenticate. After a successful authentication the end user receives a **SAML Assertion (Token)**.

Slide 18 - SAML Methods – SP Initiated

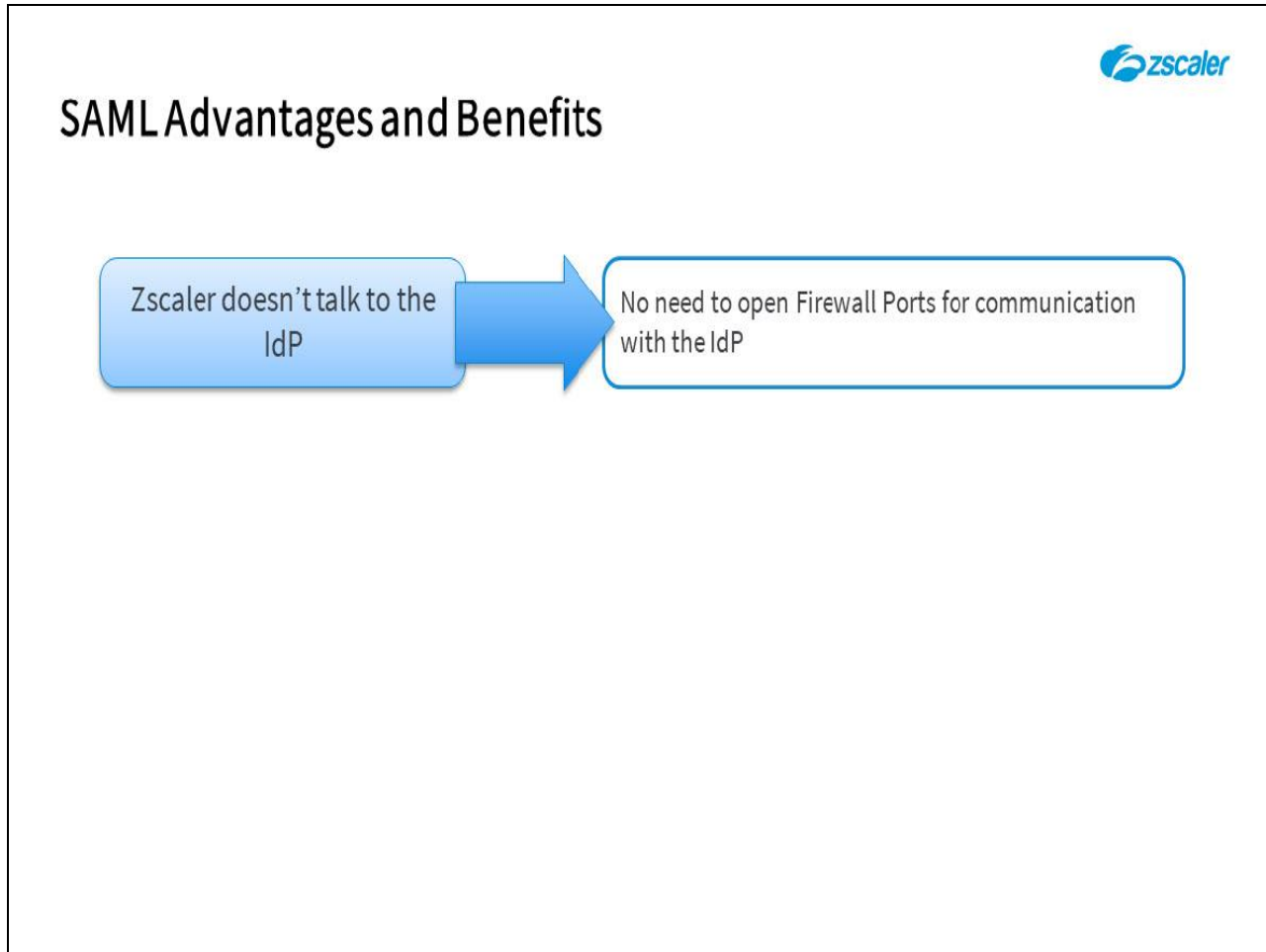


Slide notes

The user is then redirected back to Service Provider they originally tried, and they are immediately given access based on the **Token** that they received from the IdP.

This **Token** is also good for any other SP that has been integrated with this particular IdP.

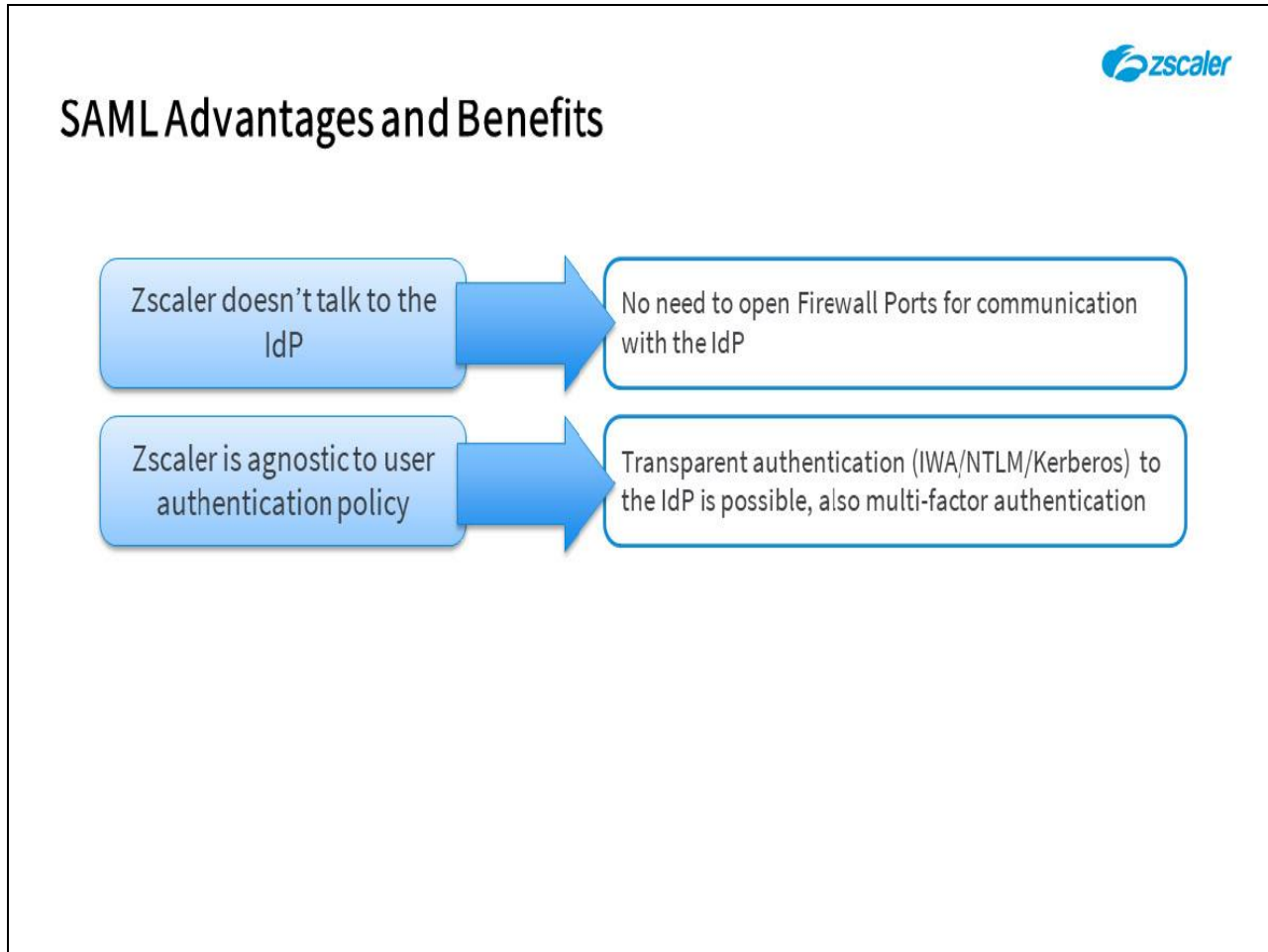
Slide 19 - SAML Advantages and Benefits



Slide notes

Advantages and benefits of a SAML implementation are: firstly, as you will see when we discuss the authentication flow, Zscaler does not communicate with either the IdP or Active Directory so there is no need to open Firewall ports to Allow Zscaler to reach internal resources.

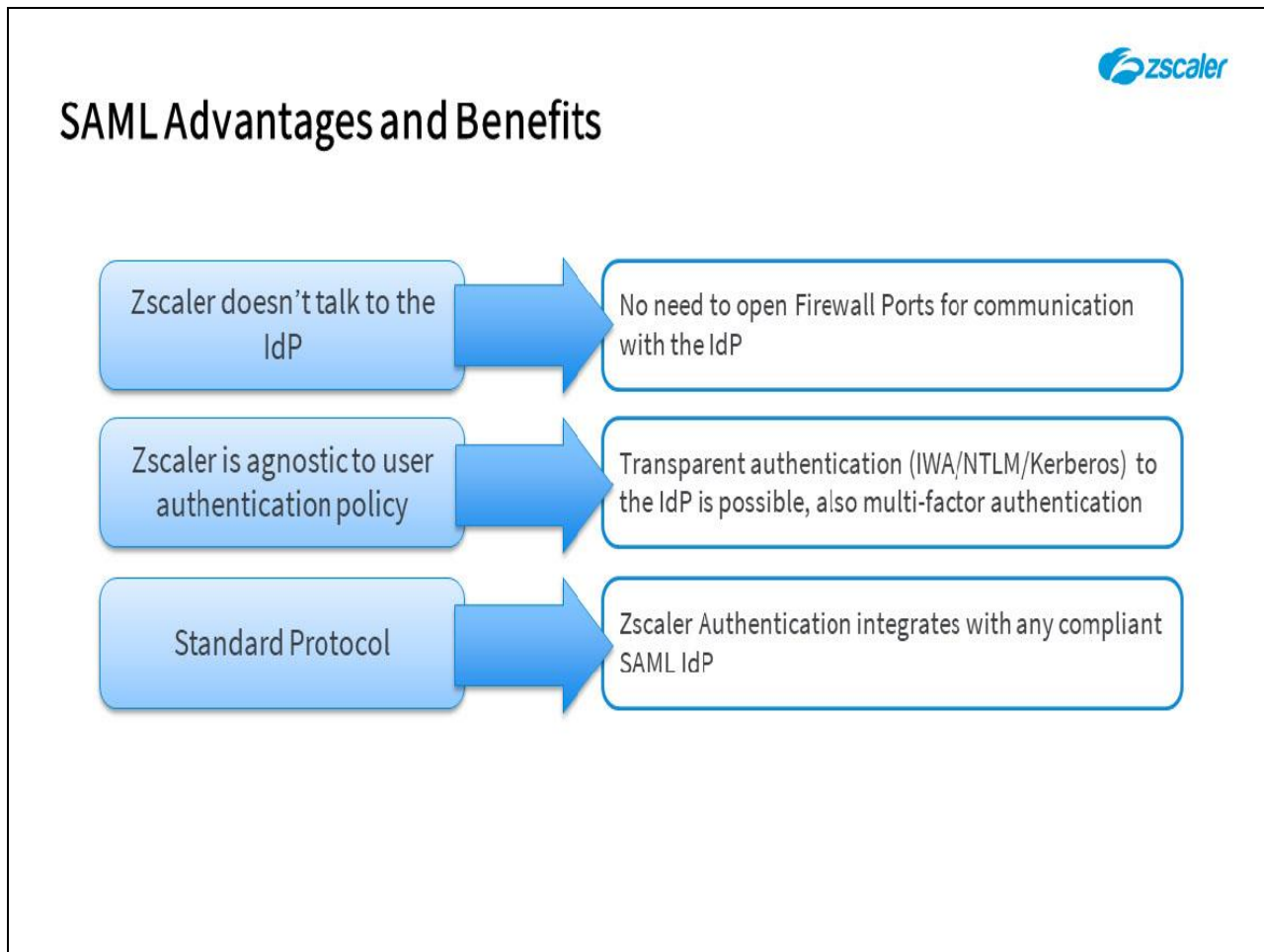
Slide 20 - SAML Advantages and Benefits



Slide notes

SAML can provide for true single-sign on for end users in a Windows environment, once the user authenticates to the PC desktop they can be automatically logged into the IdP in the background, which then authenticates them into Cloud applications. Multi-factor authentication is also a possibility.

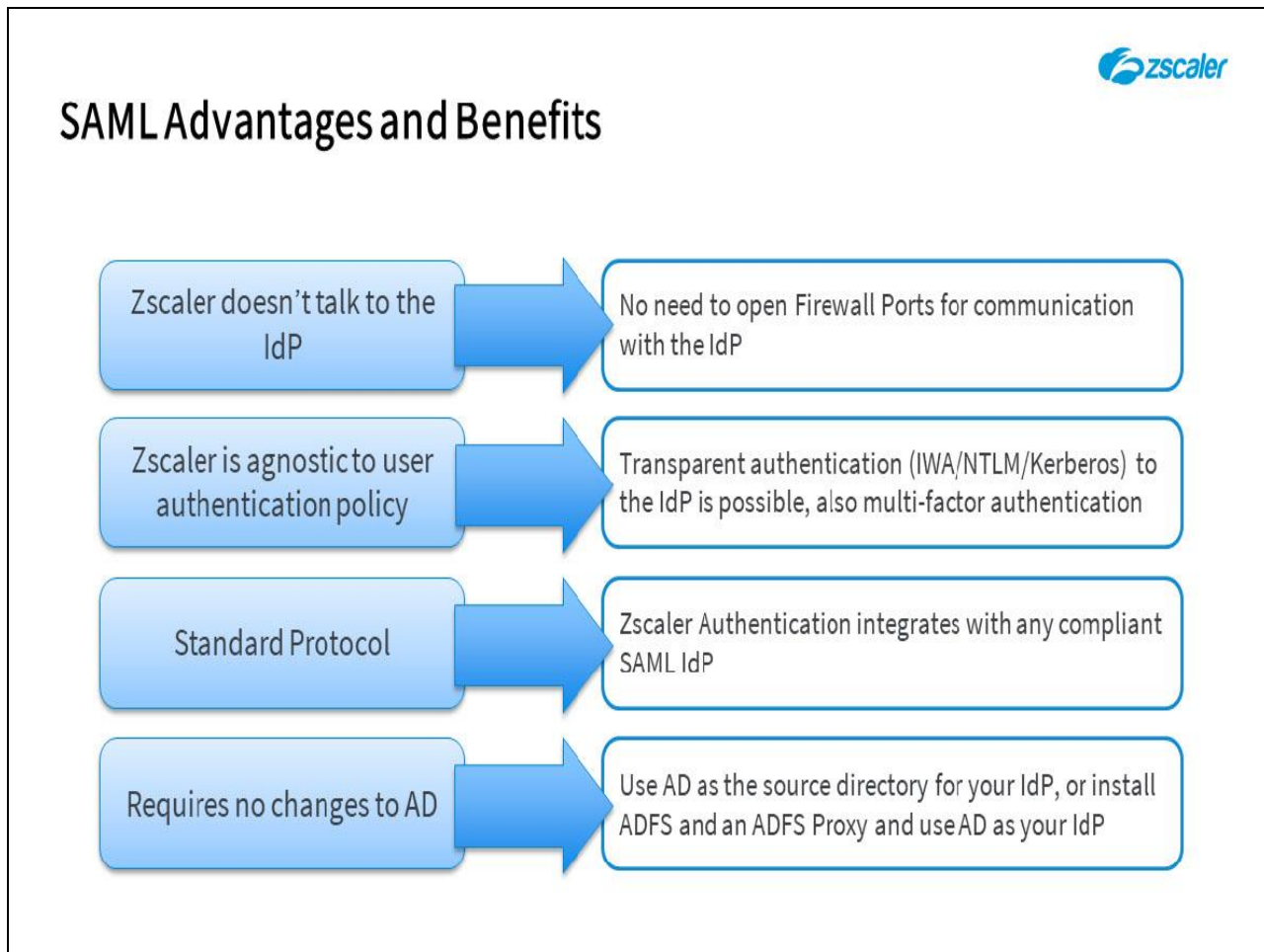
Slide 21 - SAML Advantages and Benefits



Slide notes

SAML is a standards-based protocol so Zscaler integrates with any compliant IdP.

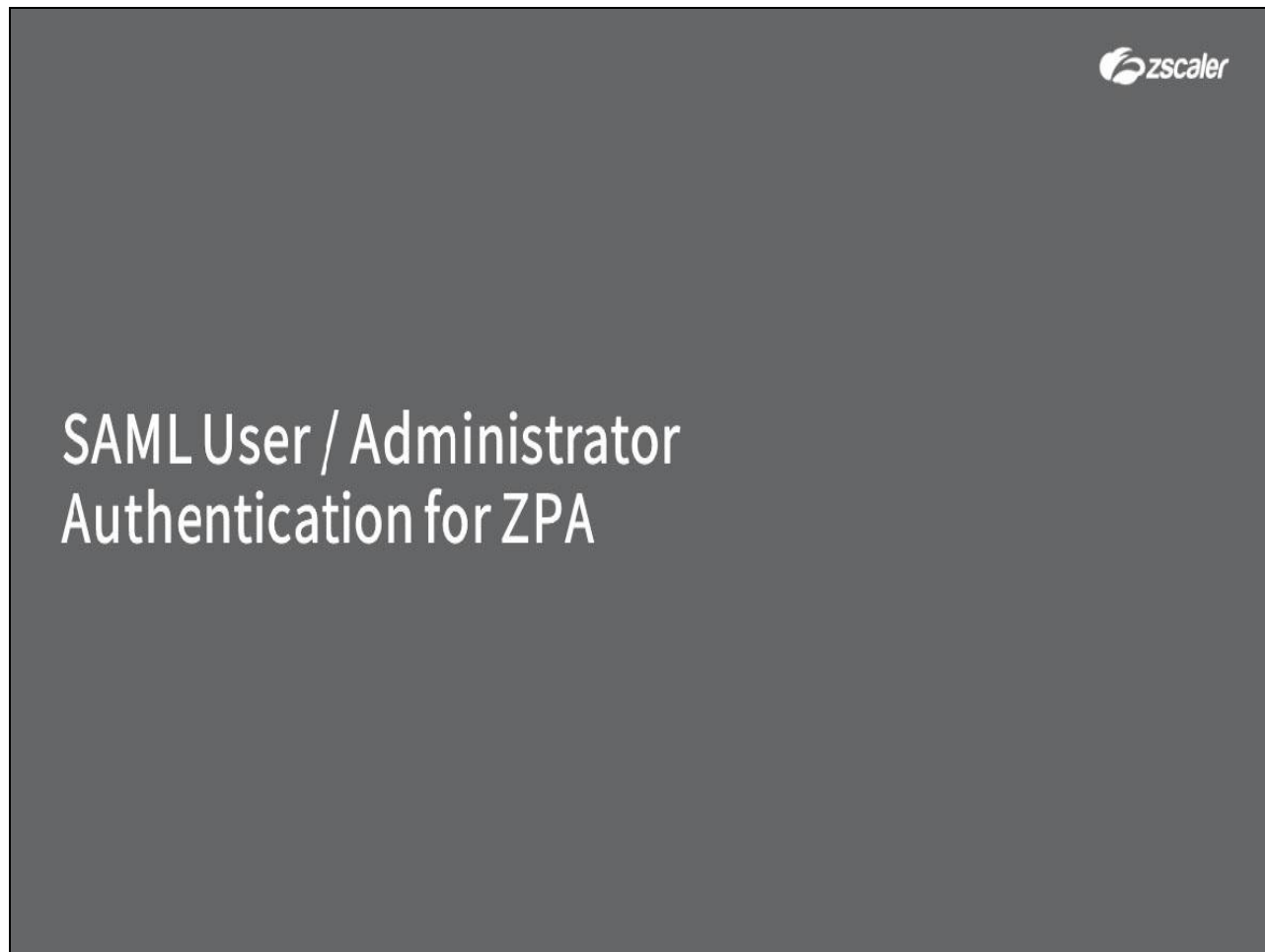
Slide 22 - SAML Advantages and Benefits



Slide notes

A SAML implementation does not mean that you need to throw away your existing AD configuration however. You can simply sync user accounts to your chosen IdP for those users that need to authenticate from external locations but continue to use AD for your internal users. Alternatively, leverage your AD deployment for end user SSO internally and externally by enabling AD Federated Services (AD FS), and optionally installing an AD FS proxy.

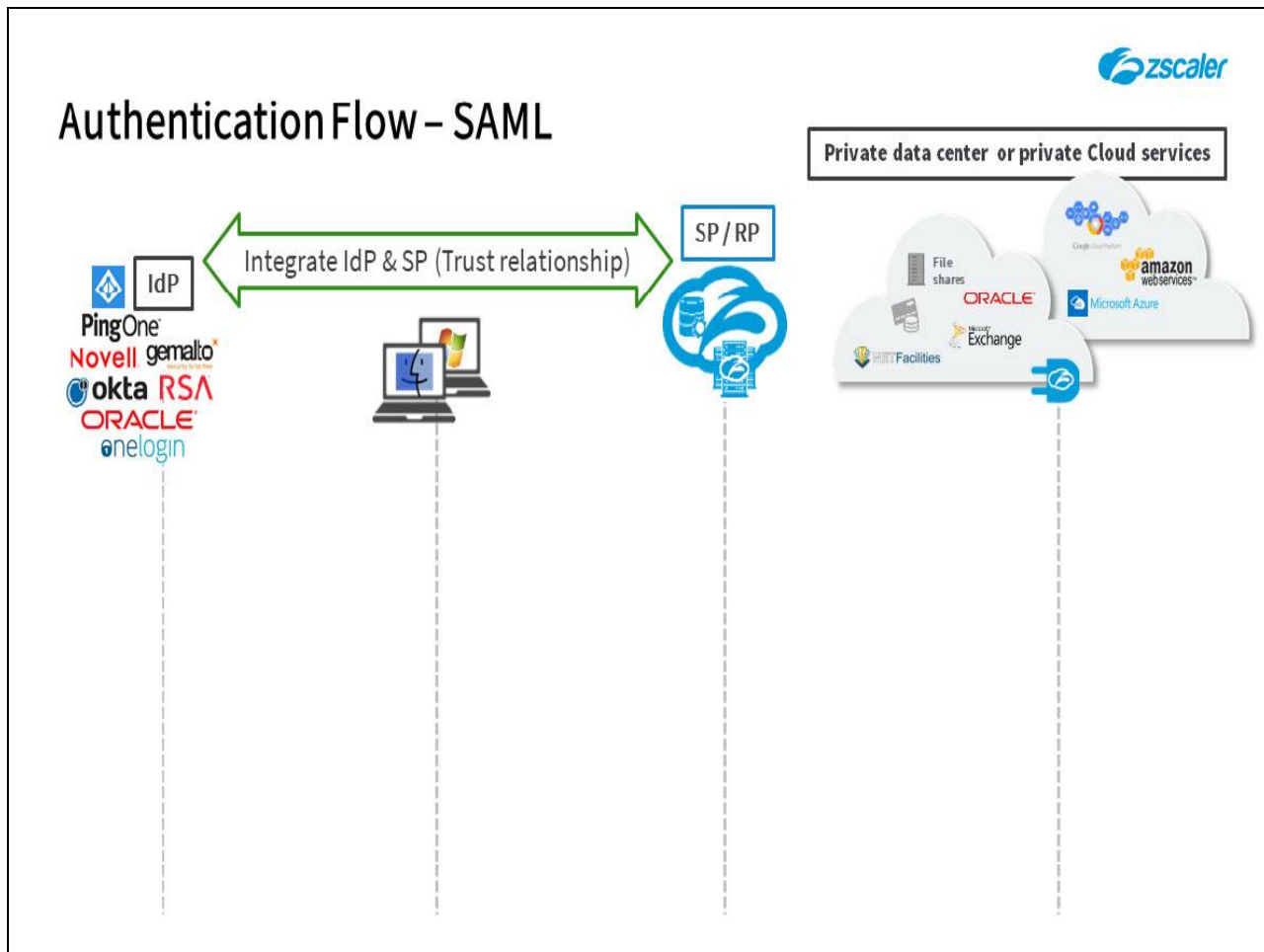
Slide 23 - SAML User Authentication



Slide notes

In the next section, we will look at the authentication process when using SAML.

Slide 24 - Authentication Flow – SAML

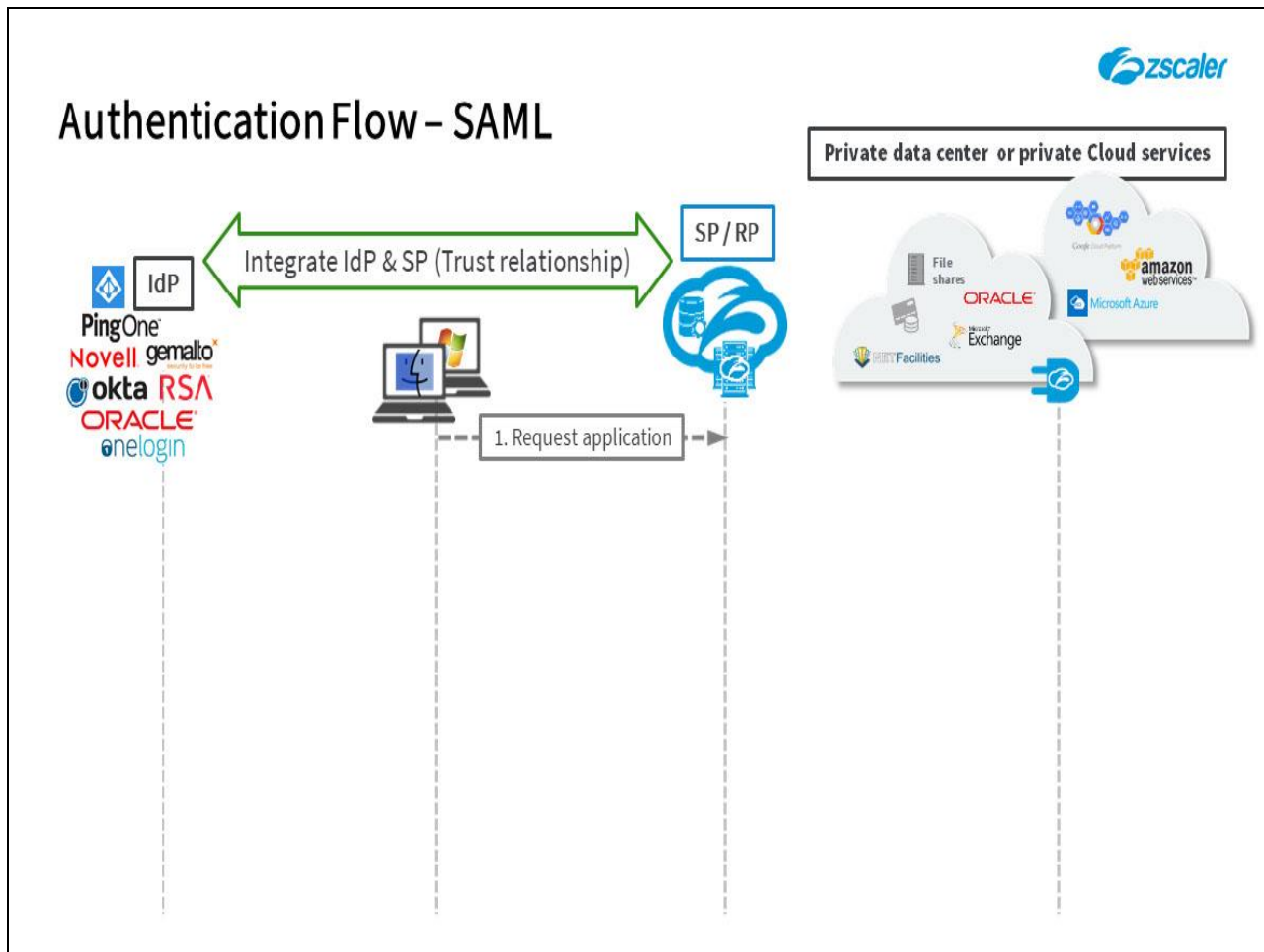


Slide notes

Let's take a high-level look at the SAML authentication process for a ZPA user that wishes to access private applications through Zscaler.

Before any end-user authentication can happen, the SAML IdP and Service Provider (Zscaler) must be configured to know about one another, and to establish the trust relationship that is a requirement for SAML authentication to work.

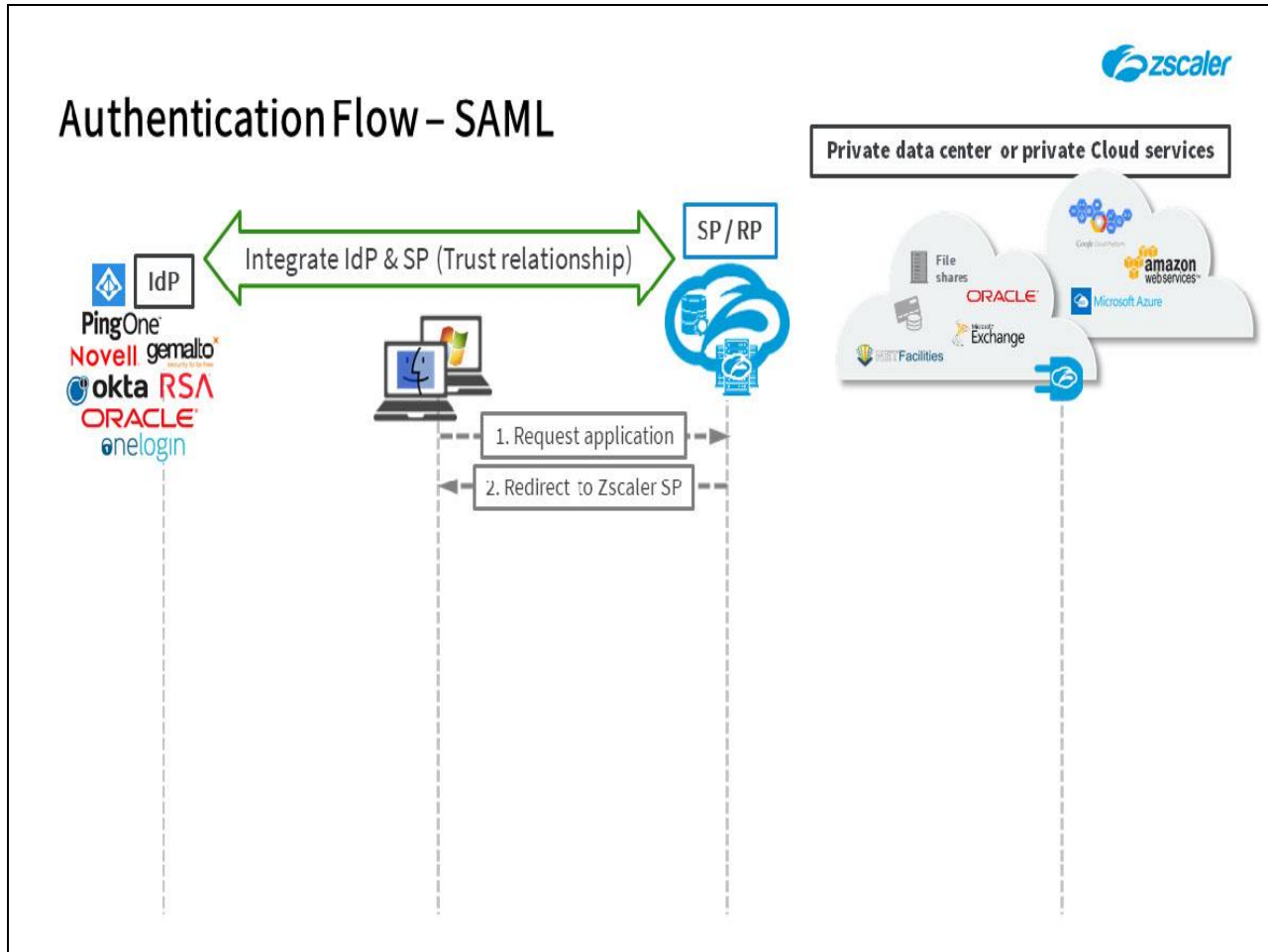
Slide 25 - Authentication Flow – SAML



Slide notes

1. A private access user simply wants to access a private application so initiates a request for the application, which is sent by the Zscaler App or redirected by the browser to the local ZPA-ZEN.

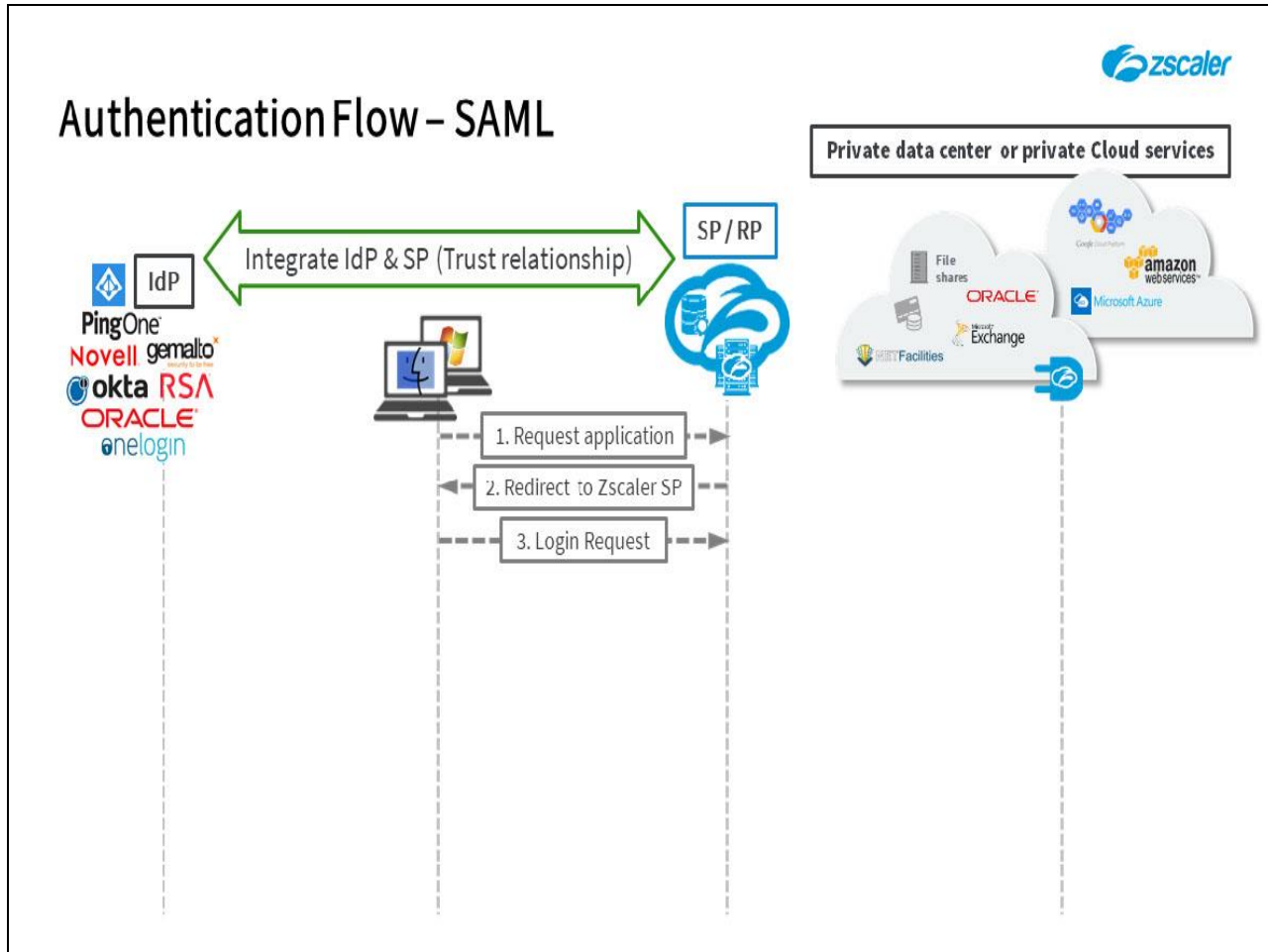
Slide 26 - Authentication Flow – SAML



Slide notes

2. The user is redirected by the ZPA-ZEN to the ZPA Central Authority, to check the user name.

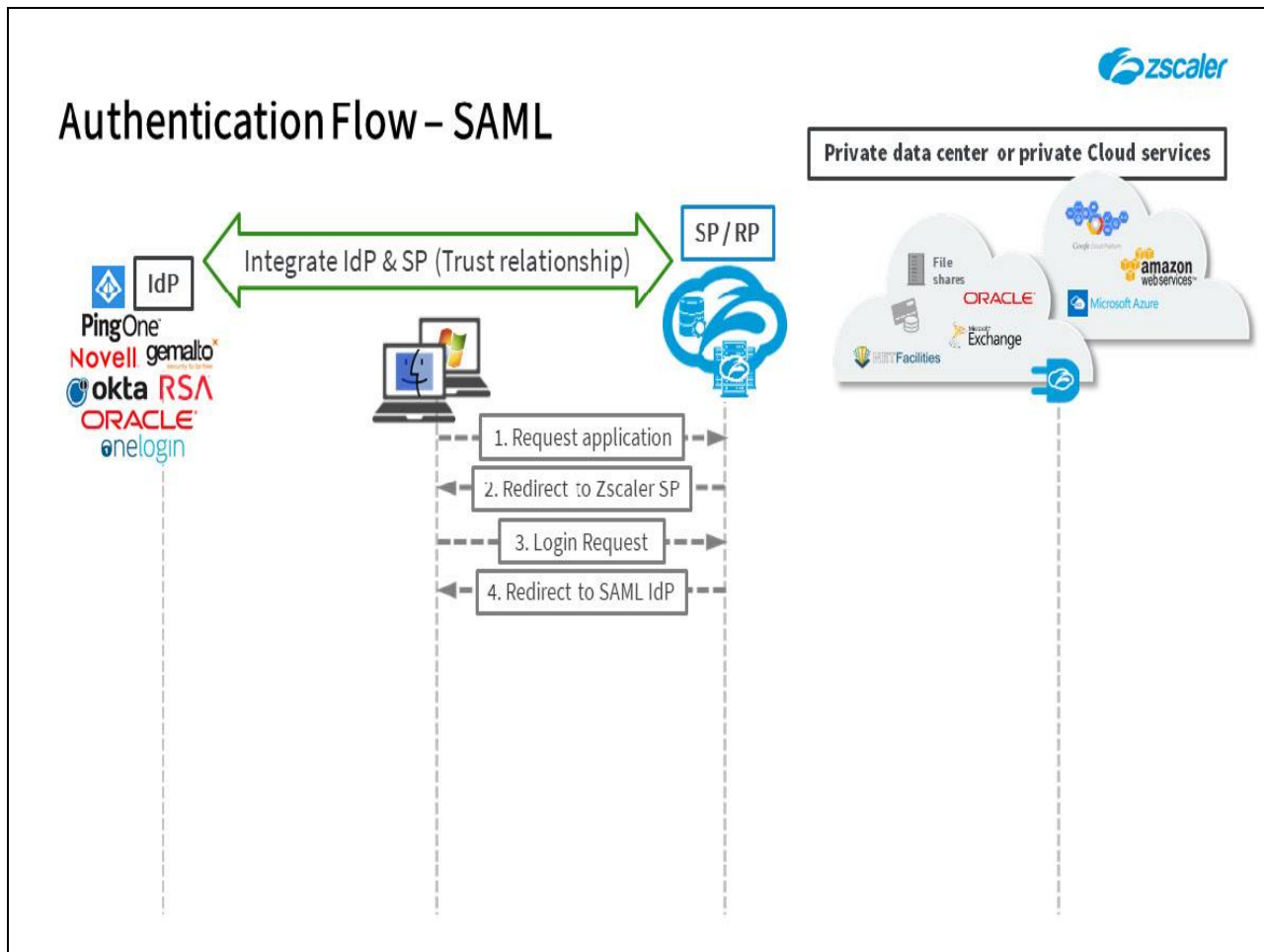
Slide 27 - Authentication Flow – SAML



Slide notes

3. The Zscaler App, or the user in the browser, sends their username to the CA...

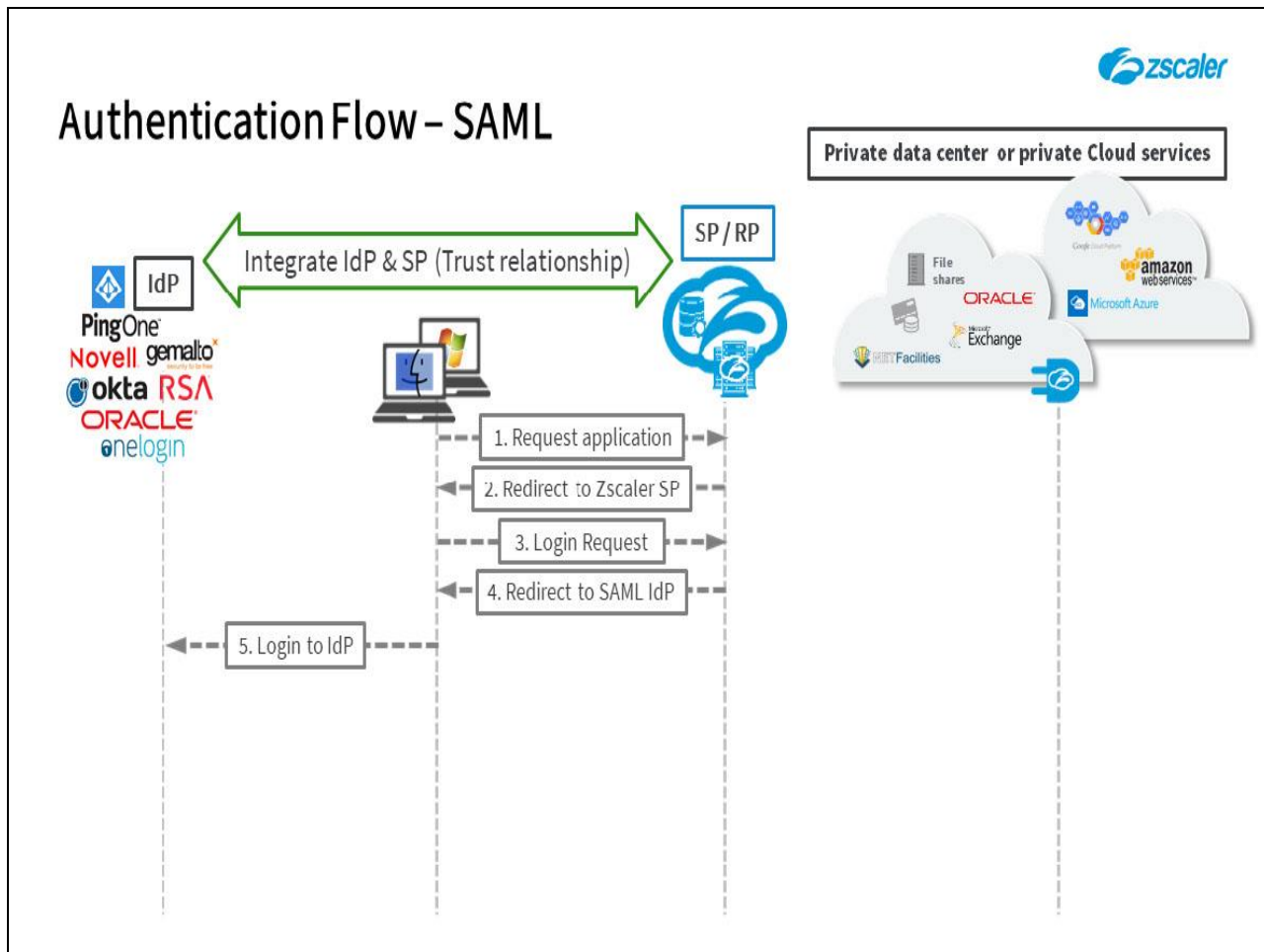
Slide 28 - Authentication Flow – SAML



Slide notes

4. ...and based on the **Realm** of the username, is redirected with an authentication request to the SAML IdP configured for the organization on the CA.

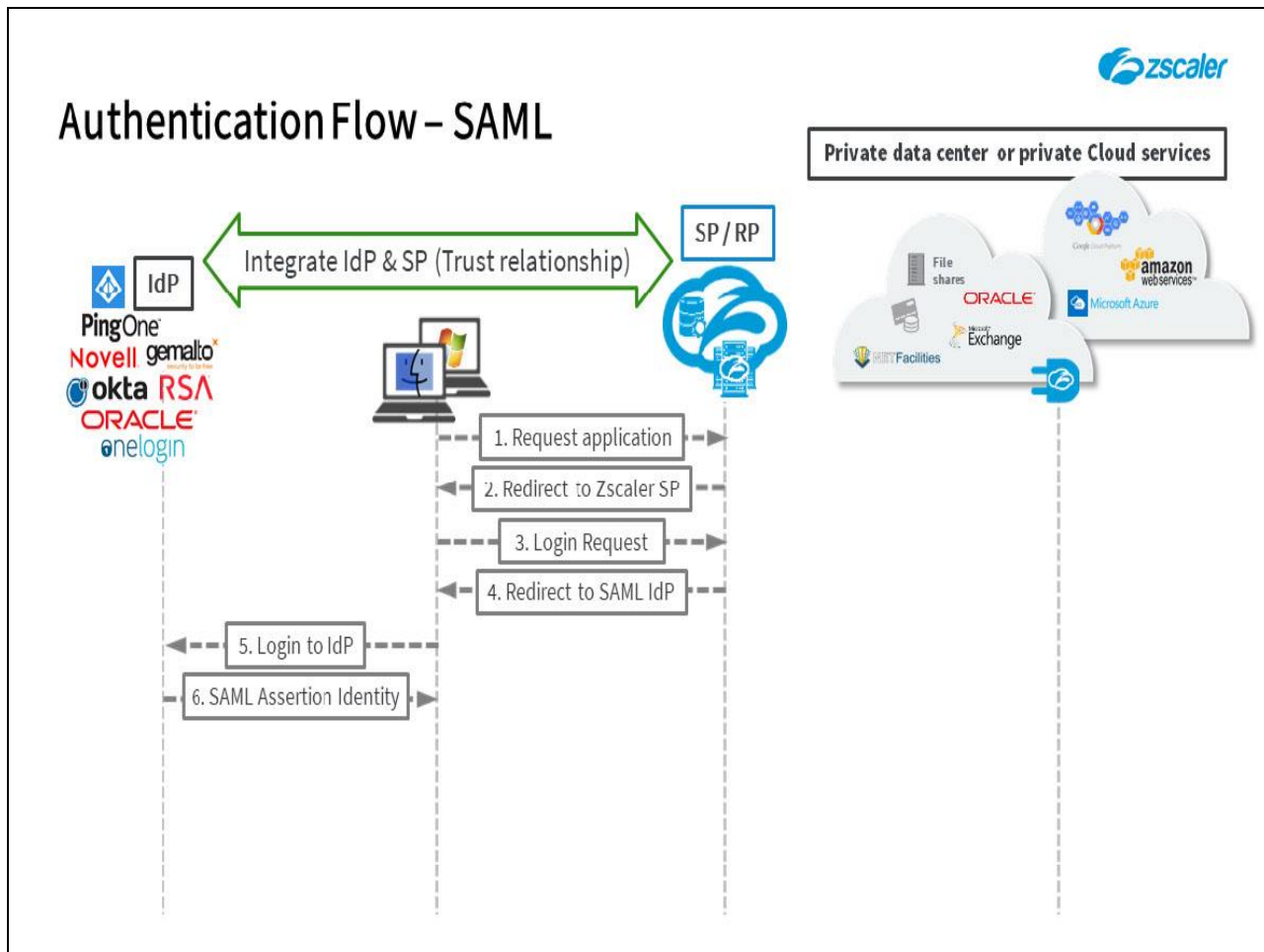
Slide 29 - Authentication Flow – SAML



Slide notes

5. The user submits the appropriate credentials to the IdP for verification, either from an internal database, or by consulting an external directory server such as Active Directory.

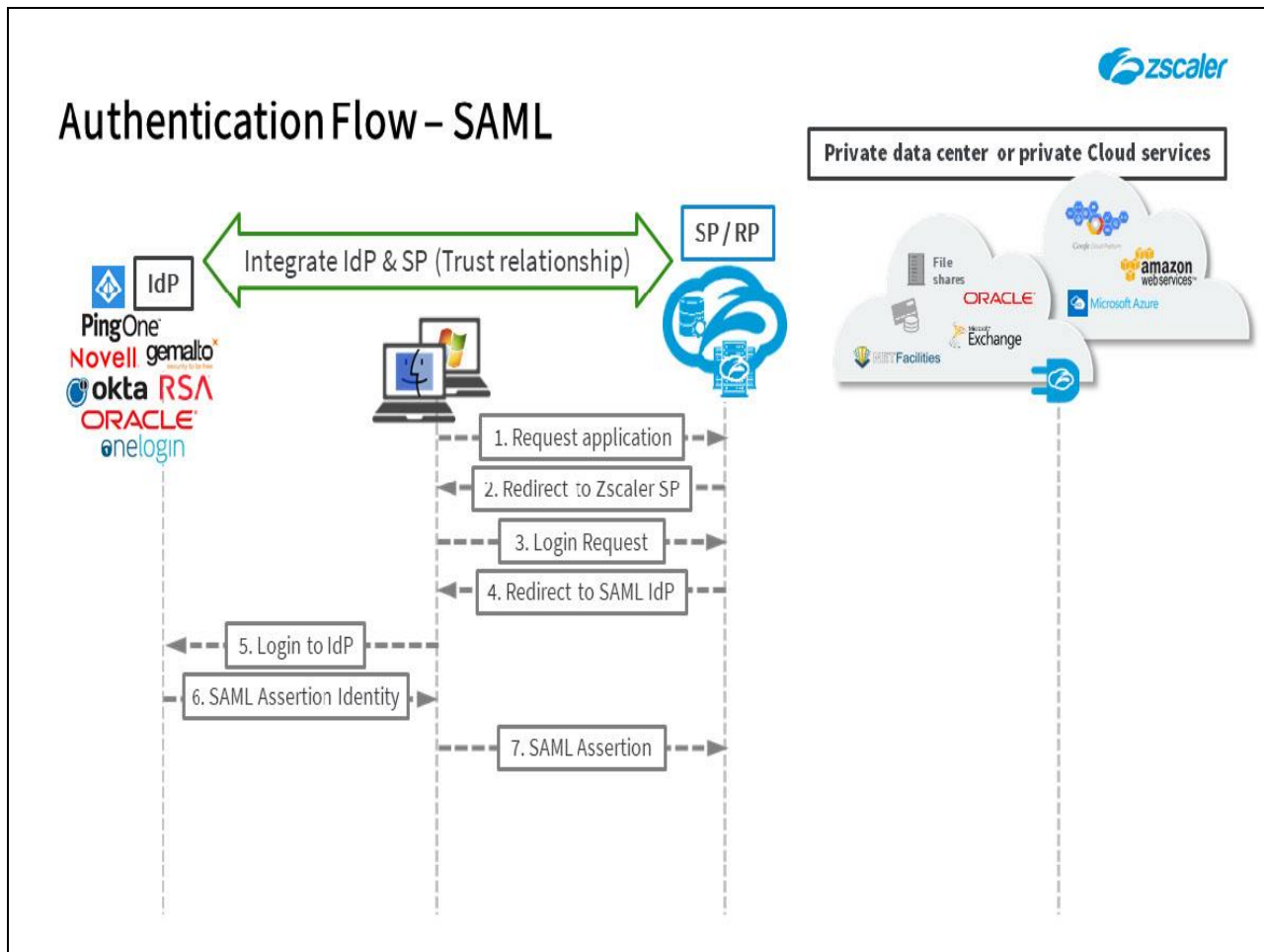
Slide 30 - Authentication Flow – SAML



Slide notes

6. The IdP responds back to the Zscaler App or browser with the signed **SAML Assertion (Token)** confirming successful authentication, the user identity, and optionally containing authorization attributes.

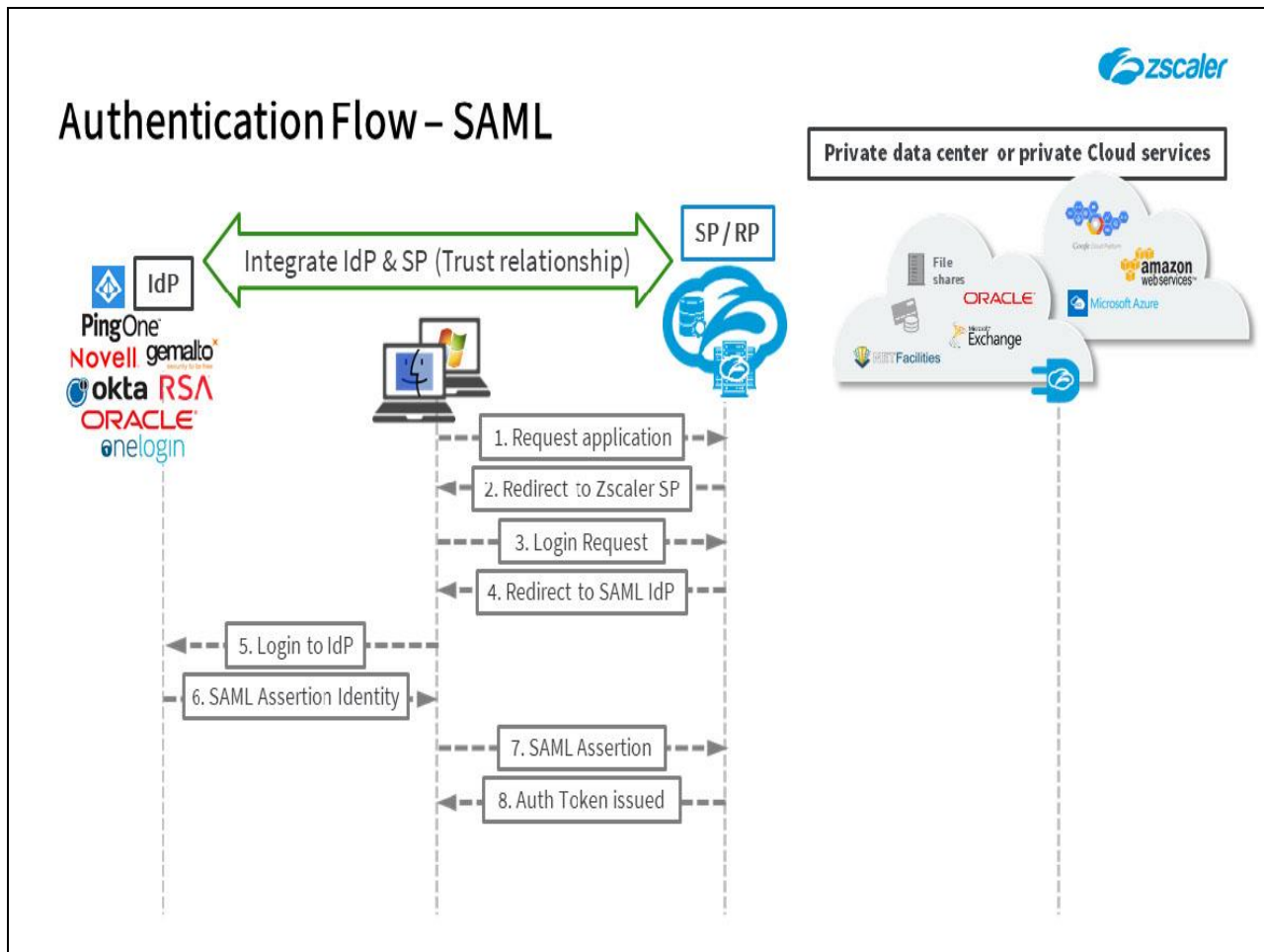
Slide 31 - Authentication Flow – SAML



Slide notes

7. The Zscaler App or browser now sends the **SAML Assertion** to the ZPA-CA as proof of authentication. As there is a trust relationship between Zscaler and the IdP, we can validate the **Token** and verify that the user has actually authenticated successfully.

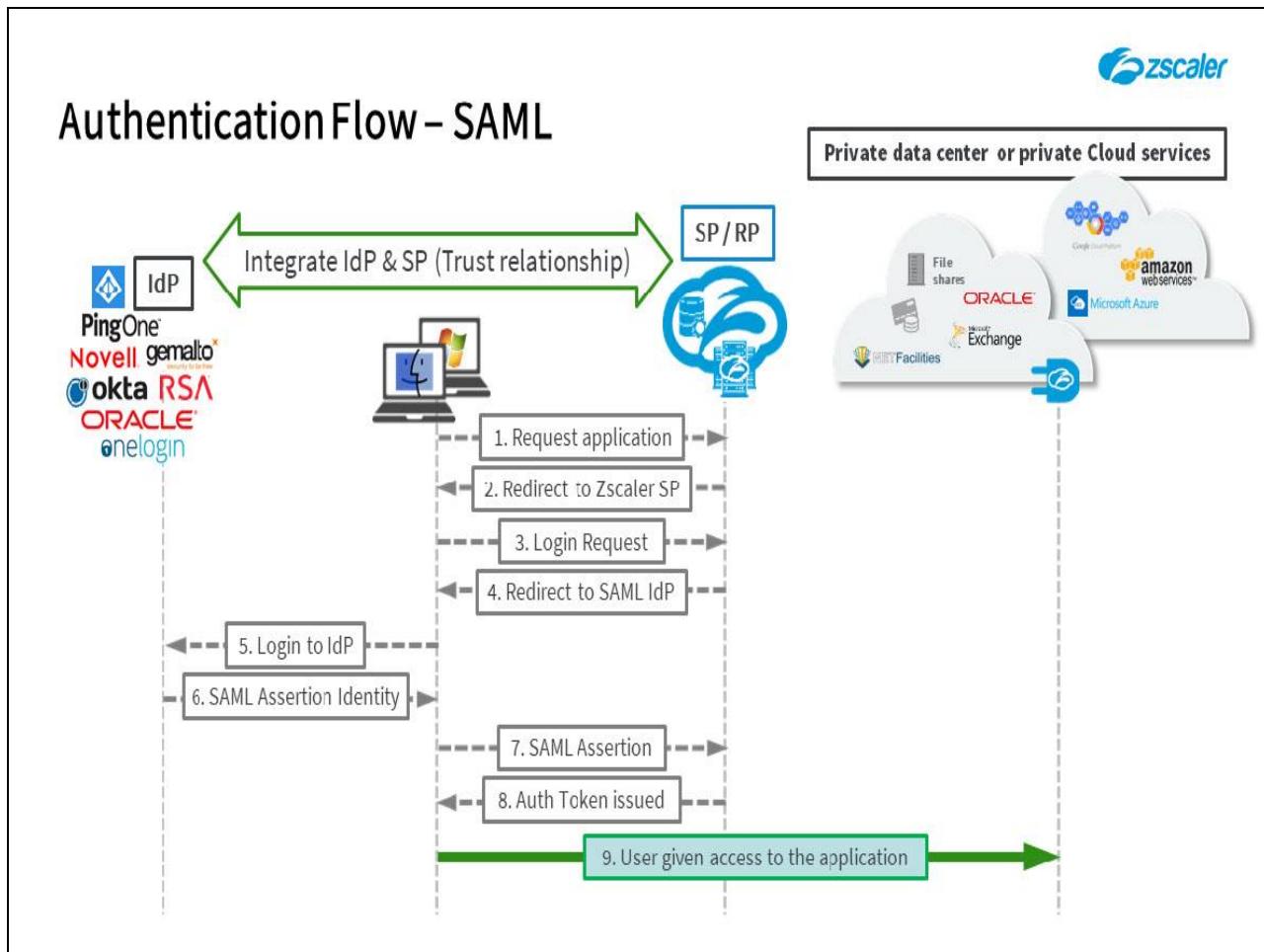
Slide 32 - Authentication Flow – SAML



Slide notes

8. Zscaler then sends an **Authentication Token** to the Zscaler App or browser.

Slide 33 - Authentication Flow – SAML



Slide notes

9. Finally, the user is granted or denied access to the requested private application based on the access policies applied to them.

Slide 34 - Zscaler Support for SAML



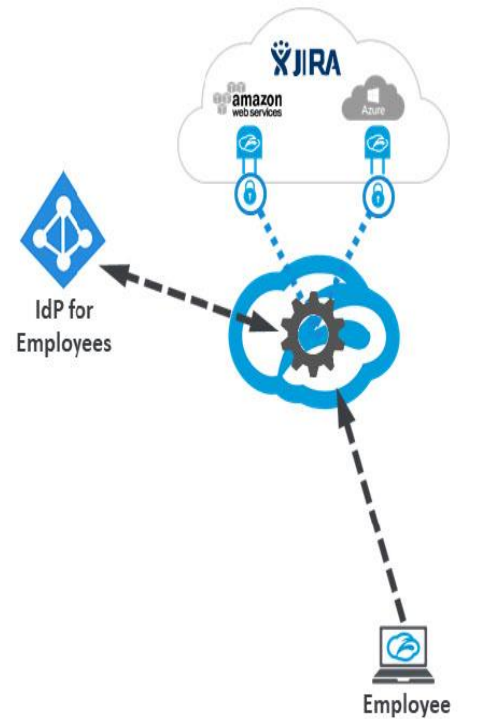
Slide notes

The final topic is a look at the support for multiple SAML IdPs for user and administrator authentication into the ZPA service.

Slide 35 - Support for Multiple SAML IdPs

Support for Multiple SAML IdPs

- What is the Multiple IdP (MIdP) Feature?
 - Multiple IdPs can be added to a ZPA account for user or admin SSO



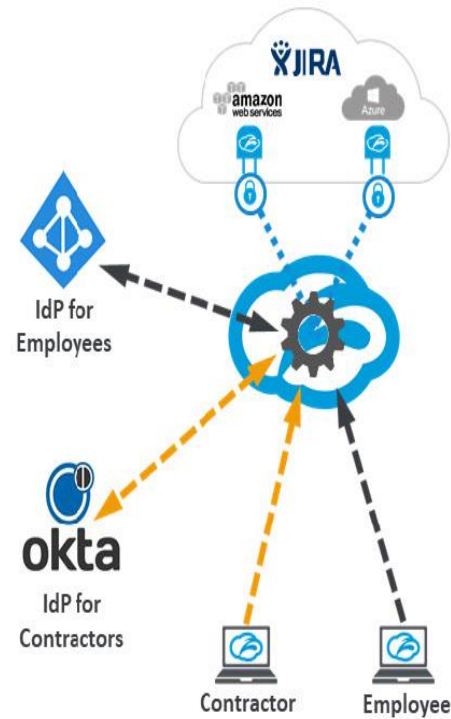
Slide notes

The ZPA service supports integration with multiple SAML IdPs simultaneously, allowing you to control access for your corporate users on one IdP, ...

Slide 36 - Support for Multiple SAML IdPs

Support for Multiple SAML IdPs

- What is the Multiple IdP (MIdP) Feature?
 - Multiple IdPs can be added to a ZPA account for user or admin SSO



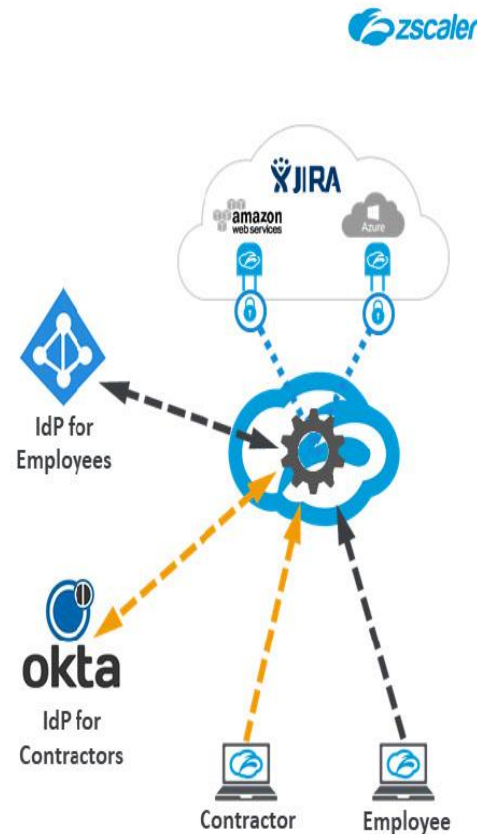
Slide notes

...while controlling access for 3rd party contractors or consultants with accounts on some other IdP.

Slide 37 - Support for Multiple SAML IdPs

Support for Multiple SAML IdPs

- What is the Multiple IdP (MIdP) Feature?
 - Multiple IdPs can be added to a ZPA account for user or admin SSO
- Why is MIdP needed?
 - Avoid identity infrastructure integration complexity during M & A / Divestitures
 - Simplify partner life-cycle management in enterprise IdP
 - Allow Business Units to share identity across ZPA tenants but preserve administrative independence
 - Enable partners to configure the same IdP in the ZPA tenants of multiple customers



Slide notes

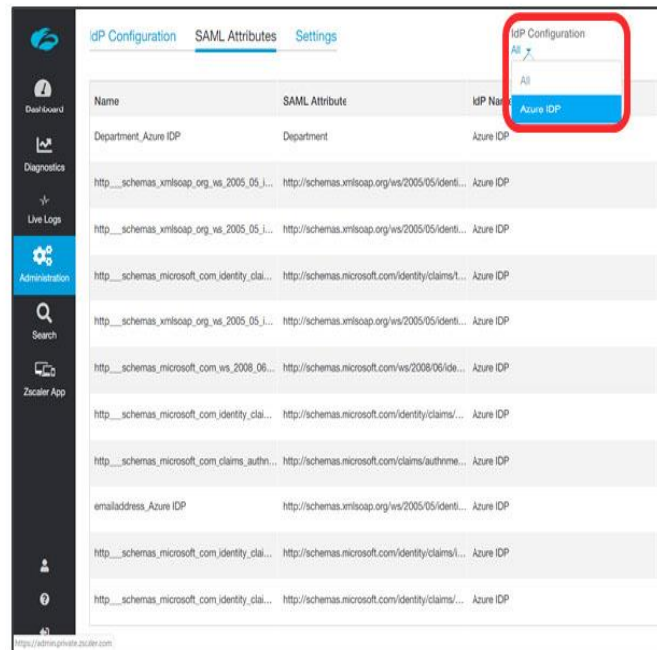
Support for multiple SAML IdPs is crucial for the service to provide the authentication flexibility required in M&A or divestiture scenarios, or when you wish to give access to a subset of your private applications to 3rd party contractors or consultants. MIdP support prevents you having to integrate the entire directory structure from the two sides of a merger or acquisition and can simplify partner life-cycle management.

The MIdP functionality gives business units (BU) the independence to manage user access for themselves, yet still collaborate seamlessly with BUs on the same ZPA tenant or (as IdP configurations can be shared) on some other ZPA tenant. The ability to share IdPs across ZPA tenants gives our service provider partners the ability to re-use the one IdP for multiple tenants where necessary.

Slide 38 - MIdP Additional Features

MIdP Features

- IdP Configuration
 - The same IdP can be configured in more than one ZPA tenant
 - SAML attributes from multiple IDPs can be used in Access Policy
 - SAML attributes can be filtered per-IdP



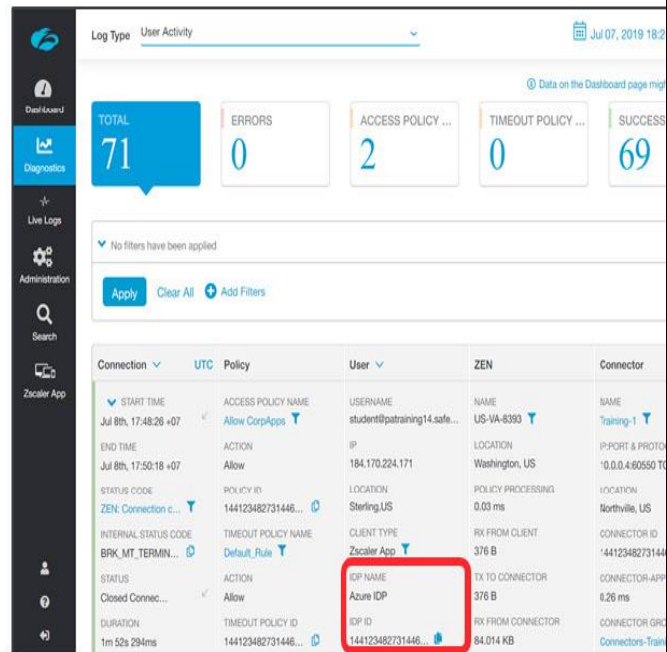
Slide notes

Some features of the MIdP capability include: The ability to use the same IdP configuration on more than one ZPA tenant, allowing the users of either organization to authenticate against the same IdP; If multiple IdPs are added at the ZPA Admin Portal, the **SAML Attributes** imported from any of them can be used in an **Access Policy** to control access to applications; plus you can filter the **SAML Attributes** list in the ZPA Admin Portal to see only the attributes from a selected IdP.

Slide 39 - MIdP Additional Features

MIdP Features

- IdP Configuration
 - The same IdP can be configured in more than one ZPA tenant
 - SAML attributes from multiple IDPs can be used in Access Policy
 - SAML attributes can be filtered per-IdP
- Diagnostics
 - Admin UI Diagnostics will display the IdP used for authentication



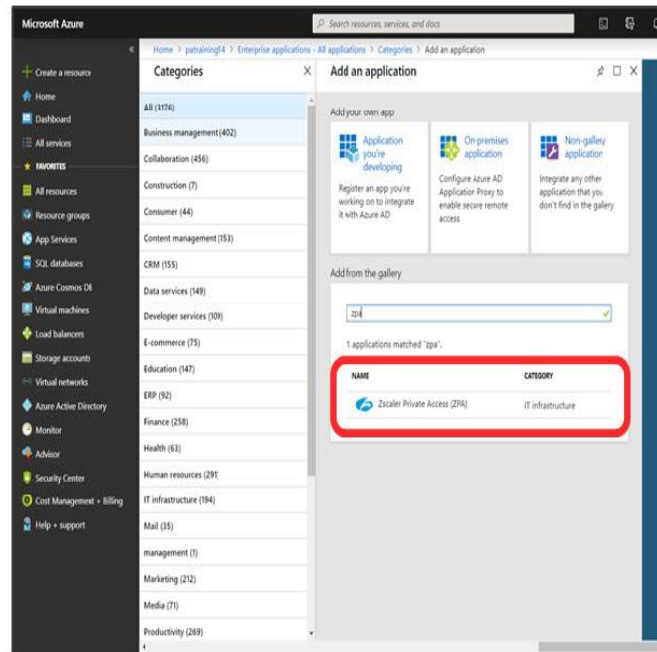
Slide notes

When troubleshooting user authentication issues, the ZPA **Diagnostics** entries log the IdP used to authenticate a user.

Slide 40 - MIdP Additional Features

MIdP Features


- IdP Configuration
 - The same IdP can be configured in more than one ZPA tenant
 - SAML attributes from multiple IDPs can be used in Access Policy
 - SAML attributes can be filtered per-IdP
- Diagnostics
 - Admin UI Diagnostics will display the IdP used for authentication
- Third Party Integrations
 - Microsoft enhancement allows multiple ZPA Apps for user SSO in Azure AD



Slide notes

In addition, Microsoft have enhanced their Azure AD solution, to support the adding of multiple ZPA instances as **Enterprise Applications** for SAML authentication.

Slide 41 - MIdP Domain Name Matching



MIdP Domain Name Matching


- User/ Administrator Authentication
 - The username realm must match either:
 - Primary Authentication Domain (required)** {
 - Primary domain(s) for your organization
 - Additional Authentication Domains (optional)** {
 - Other domains owned by your organization, but not configured as the primary domains

Slide notes

When users authenticate against a SAML IdP, the domain they authenticate against must match either the **Primary Authentication Domain** for your organization, or one of the domains specified as **Additional Authentication Domains**.

The domain names configured for an organization are used for two main purposes, the first and most important being to identify the correct organization for end user authentication. The **Realm** portion of the usernames provided by end users when authenticating through the Zscaler App or in a browser, must match either the **Primary Authentication Domain**, or one of the **Additional Authentication Domains** configured for your organization.

Slide 42 - MIdP Domain Name Matching



MIdP Domain Name Matching


- User/ Administrator Authentication
 - The username realm must match either:
 - Primary Authentication Domain (required)**
 - Primary domain(s) for your organization
 - Additional Authentication Domains (optional)**
 - Other domains owned by your organization, but not configured as the primary domains

Note: Additional authentication domains must be added to enable the Multiple IdP (MIdP) feature, these can only be added by Zscaler Support.

Slide notes

Note that if you plan to use the Multiple IdP feature, then **Additional Authentication Domains** are required. Also note that these additional domains can only be added or modified by contacting Zscaler Support.

Slide 43 - MIdP Domain Name Matching



MIdP Domain Name Matching

- User / Administrator Authentication
 - The username realm must match either:
 - Primary Authentication Domain (required)**
 - Primary domain(s) for your organization
 - Additional Authentication Domains (optional)**
 - Other domains owned by your organization, but not configured as the primary domains
- Application Configuration
 - Applications should be configured to use domains in use within your organization
 - For applications added or accessed using a “short name” domain suffixes can be added:
 - DNS Search Domains (optional)**
 - Added as suffixes to application or host names (mapped drives, printers, etc.) when necessary to create FQDNs
 - Subset of the domains owned by your organization

Slide notes

When you add Applications in the ZPA Admin Portal, the domains you specify for them should match domains in use within your organization. If your users access applications using short names rather than FQDNs (e.g. **filer1** rather than **filer1.safemarch.com**), then **DNS Search Domains** must also be provided on the **Administration > APPLICATION MANAGEMENT > Application Segments** page.

These are DNS search domain suffixes that ZPA uses for your organization, which are applied to application short names when necessary to create FQDNs, for example for; mapped drives, printers, server host names, and so on. The search domains added should be a subset of the domains owned by your organization, although they may not necessarily match your organization's authentication domains. Very often the authentication domains and the application domains will overlap.

Slide 44 - MIdP Configuration

MIdP Configuration

- Domain Mappings
 - An IdP must be associated with at least one Authentication Domain and may be associated with several
 - An Authentication Domain can only be used for a single IdP configuration

The screenshot shows the 'Add IdP Configuration' window in the Zscaler interface. The 'IdP Information' tab is selected. The 'Name' field contains 'Okta'. Under 'Single Sign-On', the 'User' option is chosen. The 'Domains' section is highlighted with a red box, showing a list of domains. The domain 'emea.pattraining.safemarch.com' is selected (highlighted in blue), and 'emea.pattraining.safemarch.com' is also checked with a blue checkmark. Other domains listed are 'anz.pattraining.safemarch.com', 'apac.pattraining.safemarch.com', and 'us.pattraining.safemarch.com'. At the bottom, there are 'Done', 'Select All', and 'Clear Selection' buttons.

Slide notes

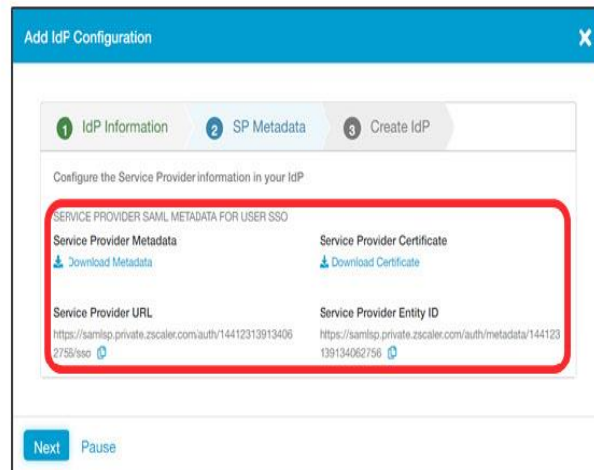
When adding more than one IdP, each must be associated with an **Authentication Domain** and may be associated to more than one. To achieve this, you will need to contact Zscaler tech support to add the **Additional Authentication Domains** that you will need.

However, it is important to note that any one **Authentication Domain** can only be associated to a single IdP configuration. Any Domains that you select here will be unavailable for use on another IdP configuration.

Slide 45 - MIdP Configuration

MIdP Configuration

- Domain Mappings
 - An IdP must be associated with at least one Authentication Domain and may be associated with several
 - An Authentication Domain can only be used for a single IdP configuration
- SP Metadata
 - The Add IdP Configuration wizard creates unique SP metadata for every IdP added
 - The SP metadata, certificate and URLs for an IdP can be downloaded from within the Add IdP Configuration wizard, or from the 'paused' IdP configuration



Slide notes

An important concept to grasp with the MIdP feature, is that the ZPA SP metadata is unique per-SAML IdP added. When you add a new IdP to the ZPA Admin Portal, the first thing we do is generate new SP metadata that can only be used with that specific IdP.

The metadata you need in order to configure the IdP, is generated as you work through the **Add IdP Configuration** wizard in the ZPA Admin Portal. The **Service Provider Metadata** and the **Service Provider Certificate** can both be downloaded when you get to step 2 of the wizard, or you can **Pause** the addition of the IdP (which saves it to the Admin Portal in an incomplete state) and access the metadata and certificate from the paused configuration.

If the IdP does not support the import of SP metadata, we also provide both the SP **URL** and **Entity ID**, so that you can copy/paste this data across to the Admin Portal for the IdP.

Slide 46 - ZPA Admin SSO

ZPAAdmin SSO

- Admin sign on can also be done using SAML
 - Add one or more IdPs just for admin SSO
 - Use the same Authentication Domain as for User SSO
 - Or user a completely different Domain
 - Administrators have the option to use SSO at login
 - Option to require SAML SSO for administrators in the **Company** profile
 - Administrator must be able to reach the IdP



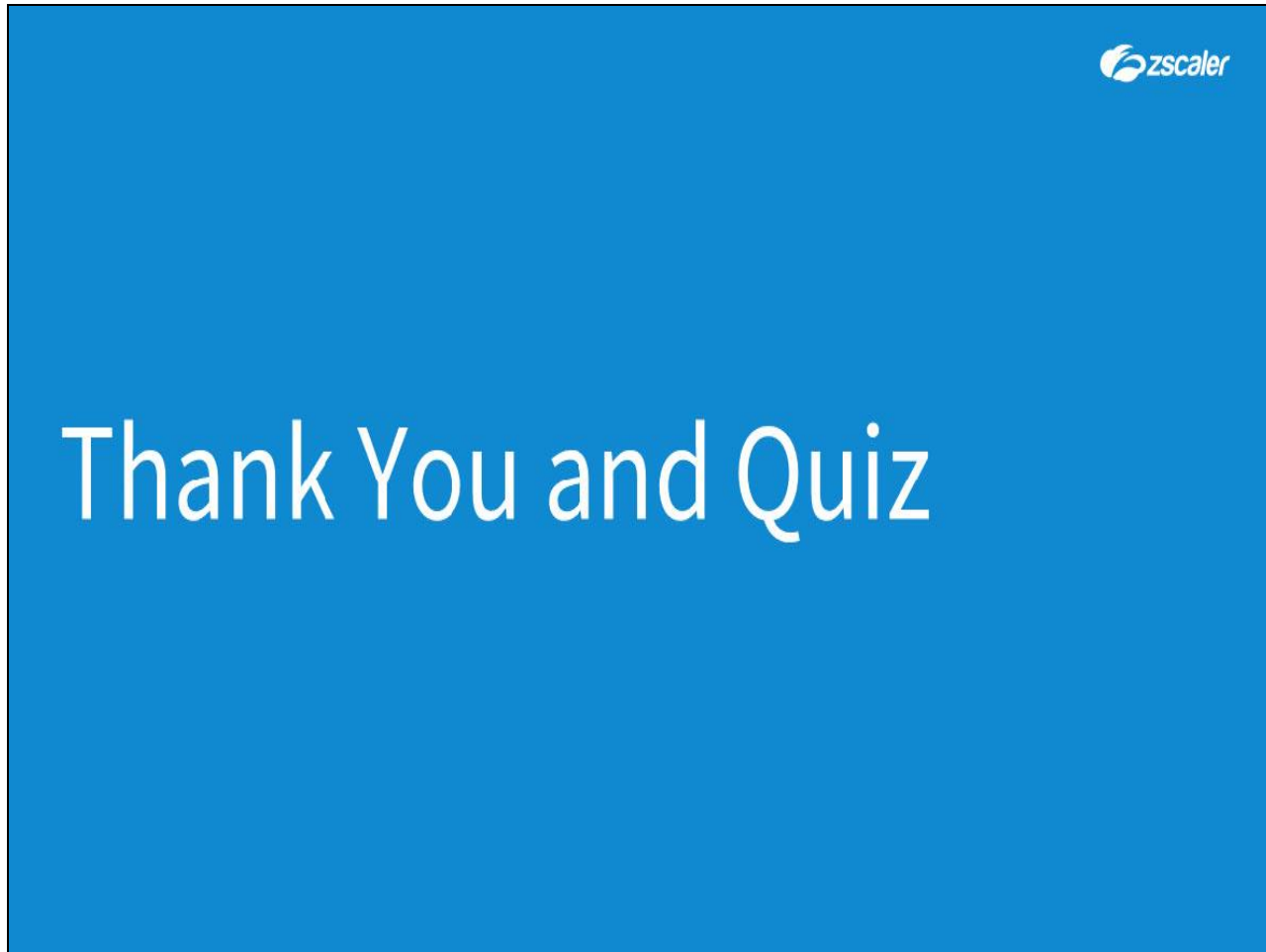
The screenshot shows the Zscaler ZPA Admin SSO login interface. At the top is the Zscaler logo. Below it are input fields for 'Username' and 'Password'. A checkbox labeled 'Single Sign On Using IdP' is highlighted with a red rectangular box. Below this checkbox is another checkbox labeled 'Remember Me' and a link for 'Two Factor Authentication'. Further down is a 'Language' dropdown menu currently set to 'English'. At the bottom is a blue 'Sign in' button.

Slide notes

It is possible to use SAML SSO for administrators as well, it can even be made a requirement for administrator access. You will need to add one (or more) IdPs just for **Admin** SSO, you may specify one of the same **Authentication Domains** as used for **User** SSO, or a completely different domain if you prefer.

When logging in to the ZPA Admin Portal admins have the option (or may be required) to use SAML. There is a setting in the **Company** profile to require admin authentication using SAML. When signing in to the admin portal using SAML, the IdP must of course be reachable from the administrator's current location.

Slide 47 - Thank You and Quiz



Slide notes

This completes the SAML module. We hope this module has been useful to you and thank you for your time.

What will follow is a short quiz to test your knowledge of the material presented in this module. You may retake the quiz as many times as necessary to pass.