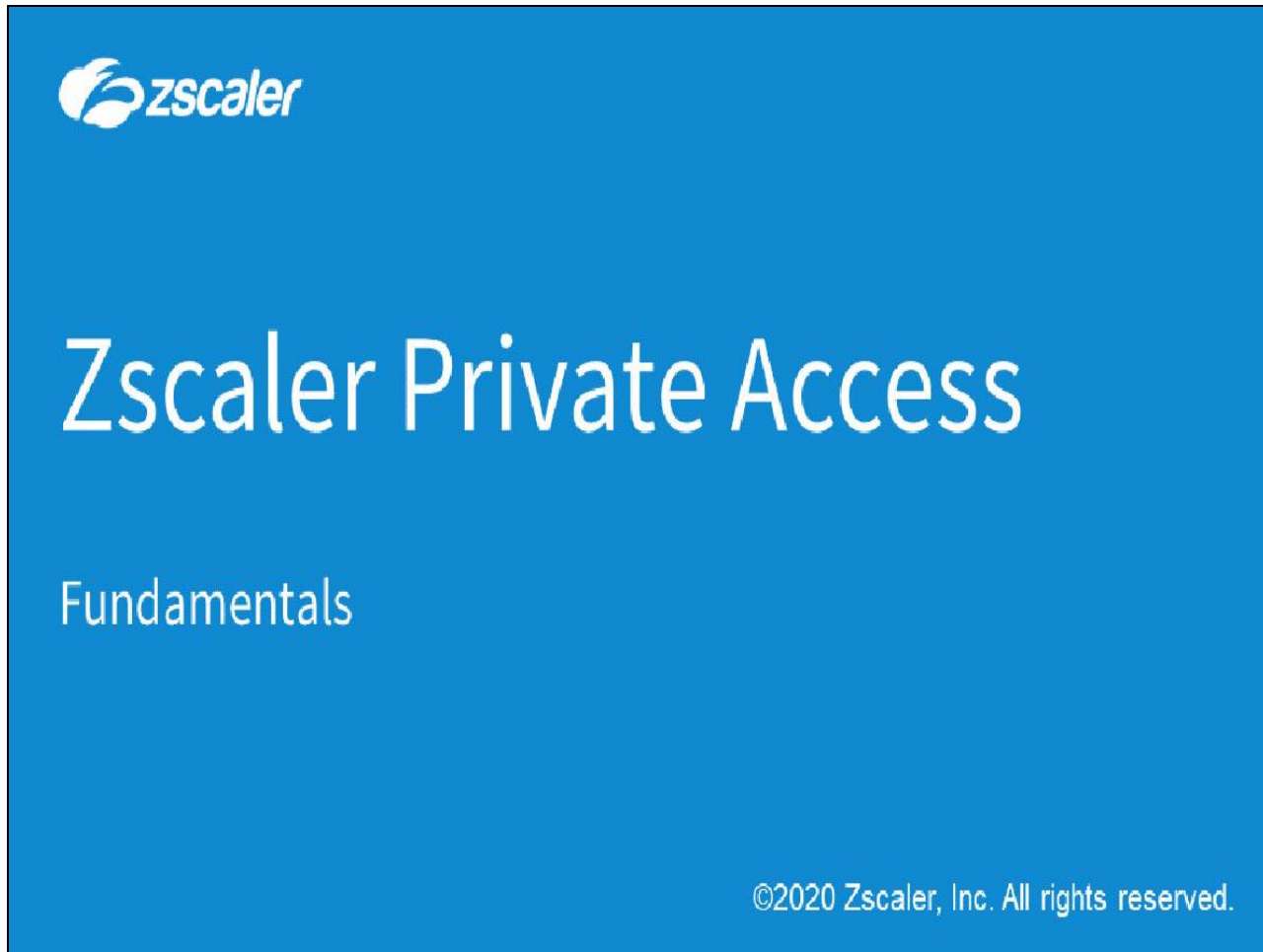



Slide 1a - Zscaler Private Access



Slide notes

Welcome to this training module on Zscaler Private Access fundamentals.

Slide 1b - New Product Names



New Product Names

	Current Product Name	New Product Name
Connectors		
	Zscaler App	Client Connector
	Mobile Admin	Client Connector Portal
	ZPA/B2B Connectors	App Connector
Zscaler Service Edge		
	ZPA	
	ZPA Broker	ZPA Public Service Edge
	Private Brokers	ZPA Private Service Edge
	ZIA	
	ZEN/SME	ZIA Public Service Edge
	Private/Virtual ZEN	ZIA Private Service Edge
Other Services		
	Remote Browser Isolation	Cloud Browser Isolation

ZIA: <https://help.zscaler.com/zia/zscaler-product-name-change>

ZPA: <https://help.zscaler.com/zpa/zscaler-product-name-change>

Z-App: <https://help.zscaler.com/z-app/zscaler-product-name-change>

Slide notes

Before you begin, take a moment and familiarize yourself with the recent changes to Zscaler product names used throughout this course. For example, **Zscaler App** is now called **Client Connector**. A complete reference of old and new product names for ZIA, ZPA and Z-App is available on the Help Portal at the URLs listed here.

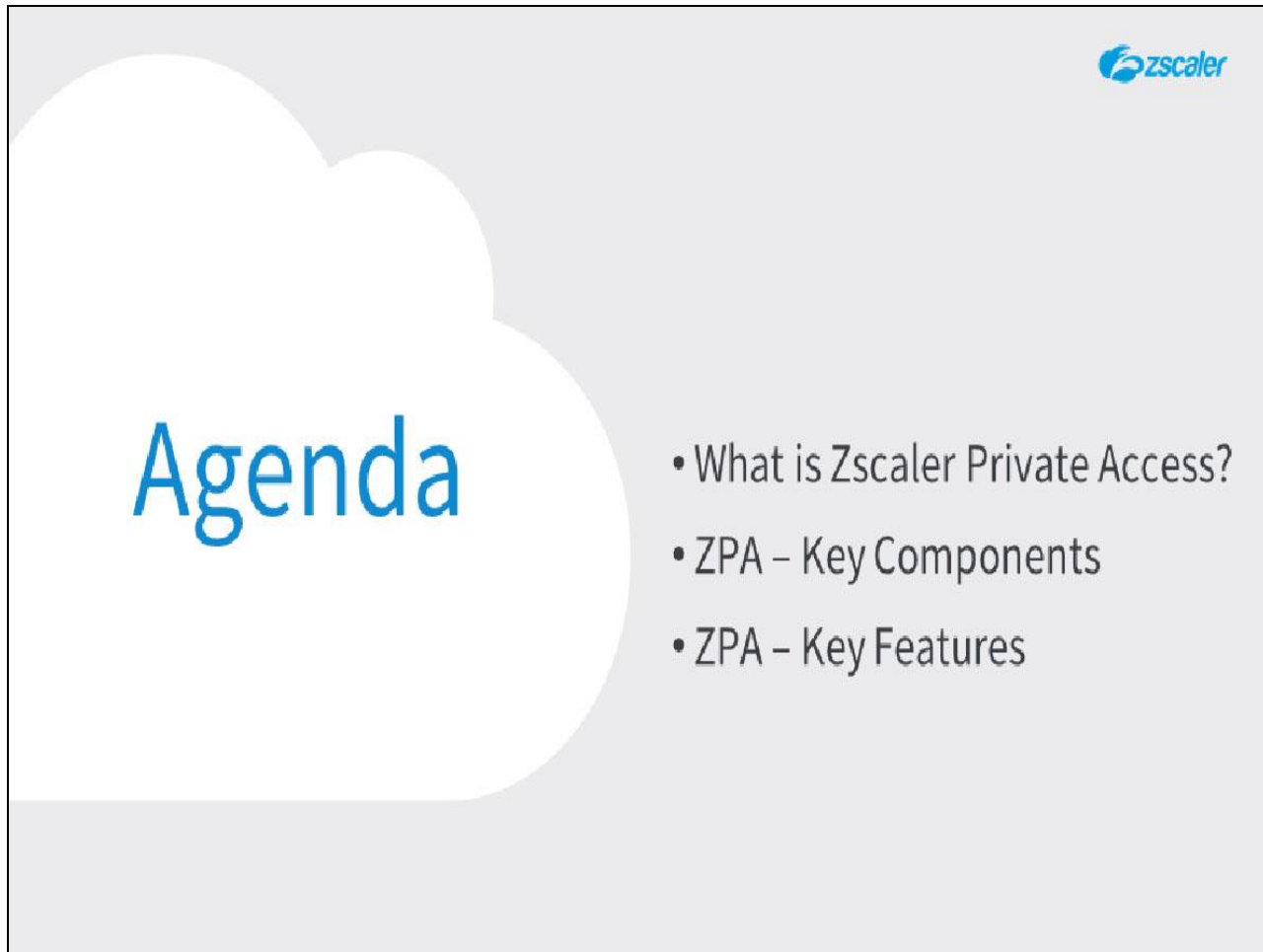

Slide 2 - Navigating the eLearning Module



Slide notes

Here is a quick guide to navigating this module. There are various controls for playback including **Play** and **Pause**, **Previous** and **Next** slide. 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

- What is Zscaler Private Access?
- ZPA – Key Components
- ZPA – Key Features

Slide notes

In this module we will cover the following topics: We will describe in overview what Zscaler Private Access actually is, its design tenets, and use cases; we will have a look at the components of ZPA; and we will have a brief look at some of the key features of the ZPA service.

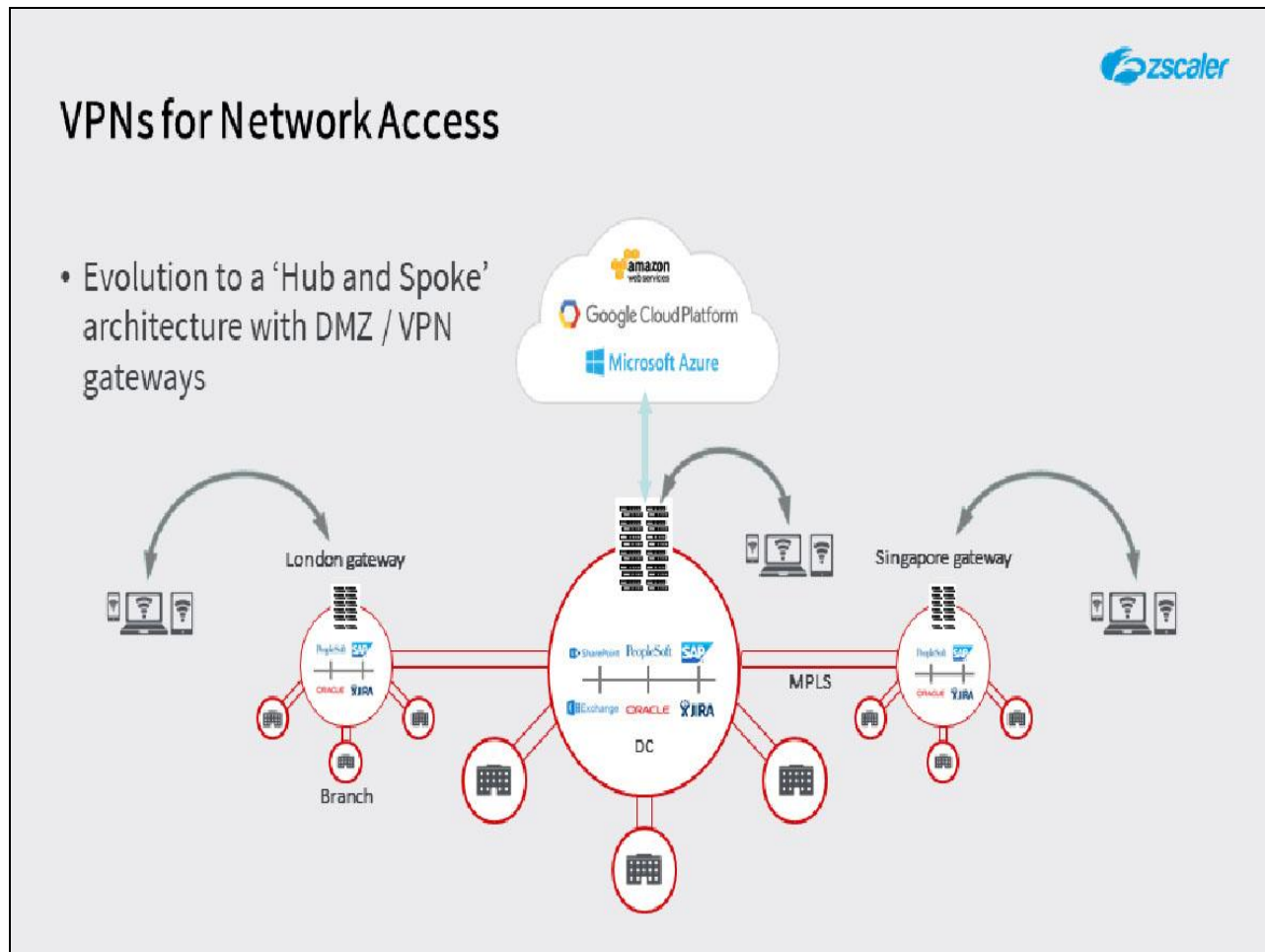
Slide 4 - What is Zscaler Private Access?



Slide notes

The first topic that we will cover is a description in overview of what Zscaler Private Access actually is.

Slide 5 - Active Health Monitoring of Defined Applications

**Slide notes**

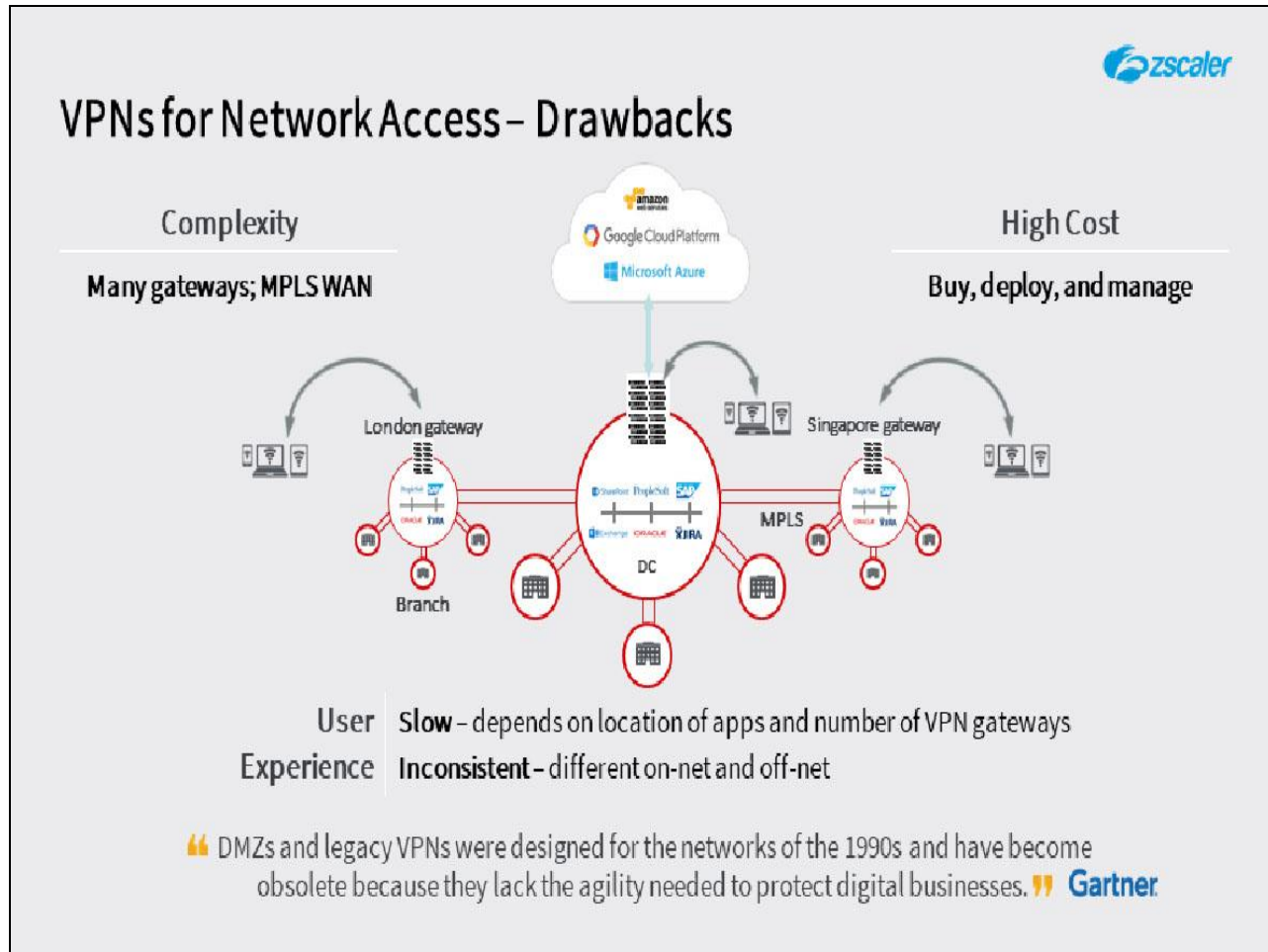
Virtual Private Networks (VPNs) have been the standard method to provide remote access to private applications and assets since users began moving away from a central office with a direct connection to the data center. Remote access VPNs extend the enterprise network perimeter to 'trusted' users, providing them with an 'on-net' experience. As the network perimeter has evolved and use of the cloud becomes increasingly prevalent for business and personal applications, however, certain attributes of remote access VPNs have become drawbacks.

As the network perimeter has evolved and use of the cloud becomes increasingly prevalent for business and personal applications, however, certain attributes of remote access VPNs have become drawbacks.

Remote access VPNs were designed to deliver the user access to a network, and as the enterprise network becomes increasingly mission-critical, it has become increasingly complex. The proliferation of remote access VPNs adds exponentially to this complexity. This is partly because, like any other part of an enterprise network, the remote access VPN must be highly available. This typically leads to multiple regional data centers, each with load balancers and redundant configurations to ensure reliability. Enterprises often must further deploy global load balancers to ensure availability in case of regional disaster, as well as purchase additional user licenses for concurrent use.

This typically leads to multiple regional data centers, each with load balancers and redundant configurations to ensure reliability. Enterprises often must further deploy global load balancers to ensure availability in case of regional disaster, as well as purchase additional user licenses for concurrent use.

Slide 6 - VPNs for Network Access – Drawbacks




Slide notes

The drawbacks of this VPN architecture have become apparent over time:

- The 'Hub and Spoke' architecture is complex, with principal and regional data centers, each with its own stack of security appliances to control access in and out. An MPLS backbone is often used to interconnect these data centers.
- This architecture is expensive to implement and maintain. Every appliance at each location must be purchased, deployed, managed, and maintained up to date.
- The end user experience when accessing resources from remote can be horrible. The VPN gateway that a user connects to may or may not be relatively local, while the resources they need access to could be hosted anywhere within a datacenter, or even in the cloud. This can result in severely sub-optimal routing and significant latency. Plus, the end user experience when off the network is different from when they are on it.

Gartner have said, "DMZs and legacy VPNs were designed for the networks of the 1990s and have become obsolete because they lack the agility needed to protect digital businesses."

Slide 7 - Active Health Monitoring of Defined Applications



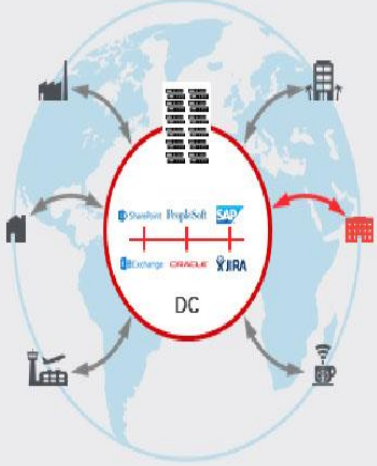
VPNs for Network Access – Security Threats



**Broader attack surface =
Higher risk**

- App access requires a user to be on the network; corporate network extends to every location of a VPN user. This broadens the attack surface, exposing apps to attacks
- Once on your network, a user can laterally scan other resources and exploit their vulnerabilities

**Over-exposed =
Vulnerable**

- VPNs are exposed to the Internet – a DDoS target, potential service disruption
- Attackers will target any exposed surface, discover vulnerabilities, and attack them



 Attackers who discover services often find vulnerabilities in applications and in APIs that bypass firewalls and intrusion prevention systems (IPS). Attackers will target services, users of the services, or both.  **Gartner**

Slide notes

Some of the known issues and vulnerabilities of remote access VPNs are:

- The VPN gateway is typically installed on the DMZ subnet of the corporate firewall and must listen for inbound connections from the remote users or sites. This means that ports and protocols must be opened at the external firewall.
- Once connected, a remote node receives an IP address on the destination network, which it can use as a bridgehead to move laterally on the internal network and potentially access any application or data that can be reached on that network.

As services and applications move to the cloud, this can result in sub-optimal data routing, as the remote access VPN connection to corporate must then be 'tromboned' back out to the cloud.


Known remote access VPN attack vectors include:

- Man-in-the-Middle attacks (MitM), particularly from public hotspots; shared devices giving unauthorized access;

- Unrestricted access to 3rd parties, such as contractors or service vendors;
- DoS/DDoS against the VPN gateways themselves; SSL VPNs may also be subject to Browser vulnerabilities.

To quote Gartner again, “Attackers who discover services often find vulnerabilities in applications and in (APIs) that bypass firewalls and intrusion prevention systems (IPS). Attackers will target services, users of the services, or both.”

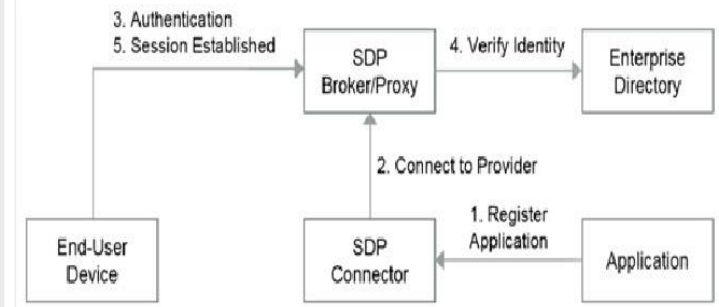
Slide 8 - Gartner: 'Zero Trust Network Access' (ZTNA) Architecture



Gartner: 'Zero Trust Network Access' (ZTNA) Architecture

- Apps are invisible to the Internet
 - No visibility = no DDoS exposure
- 'Just in time' and 'Just enough'
 - Application access only rather than network access
 - Policy-based application access
 - Native app segmentation
- Secure access
 - End-to-end encryption
 - Posture-based access
 - Client-based and clientless access

Conceptual Model of Service-Initiated ZTNA



Source: Gartner (April 2019)
ID: 396774

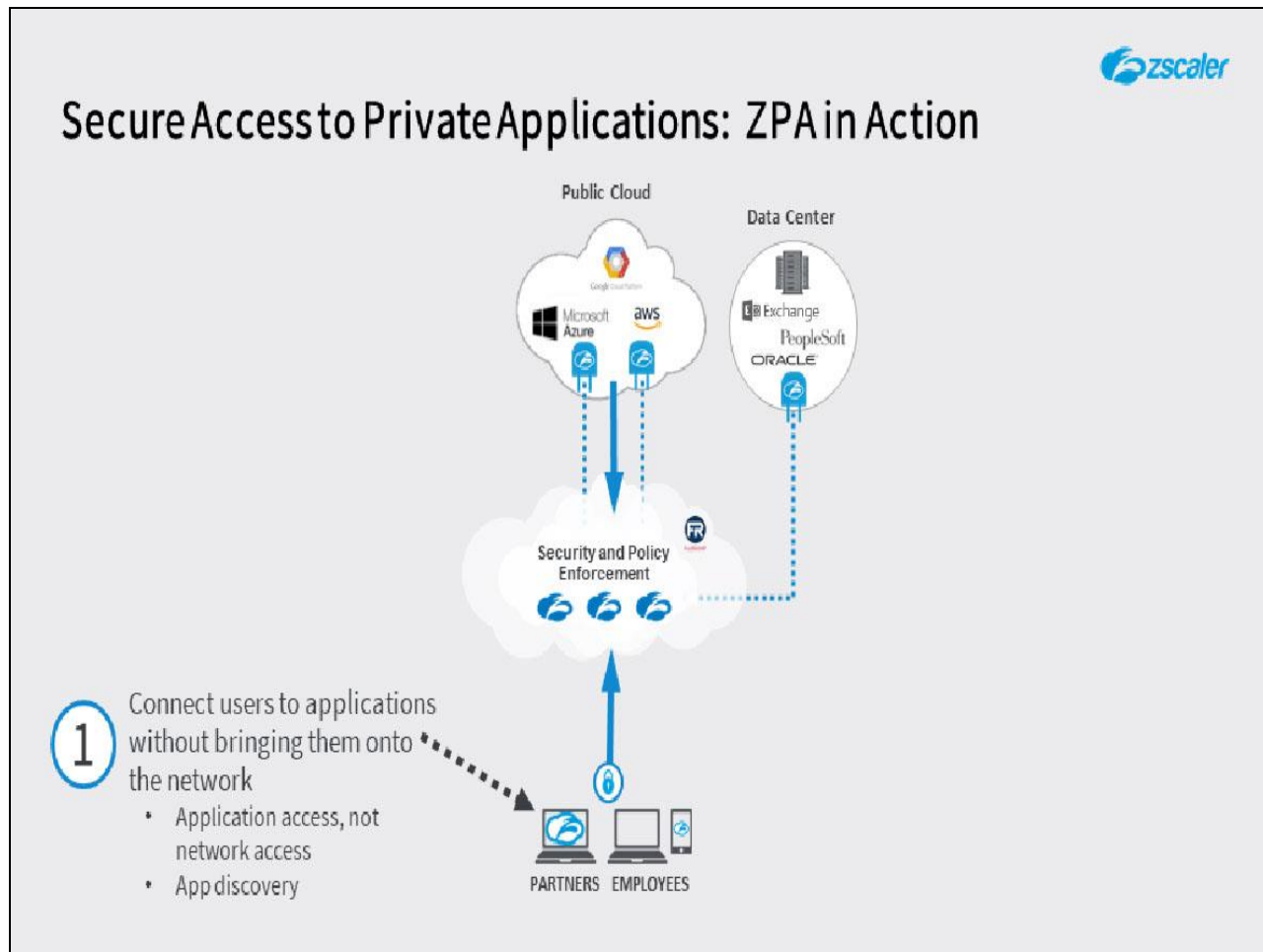
Slide notes

Gartner define 'Zero trust network access' as a replacement for traditional technologies, which require companies to extend excessive trust to employees and partners to connect and collaborate. Key attributes of a ZTNA system include:

- Removing applications and services from direct visibility on the public internet - if applications cannot be seen, they cannot be targeted for denial of service or other types of attack;
- Enabling precision ('just in time' and 'just enough') access for named users to specific applications and only after an assessment of the identity, device health and context has been made;
- Enabling application access independent of the user's physical location or the device's IP address (except where this is a requirement - e.g. for specific areas of the world);
- Application access policies need to be based on user, device and application 'identities';
- Granting access only to the specific application and not to the underlying network, as this limits the need for excessive access to all ports and protocols, or all applications, some of which the user may not be entitled to;

- Providing end-to-end encryption of network communications is of course a fundamental requirement;
- And providing a consistent user experience for accessing applications - clientless or via a ZTNA client regardless of user's location.

Slide 9 - Secure Access to Private Applications: ZPA in Action



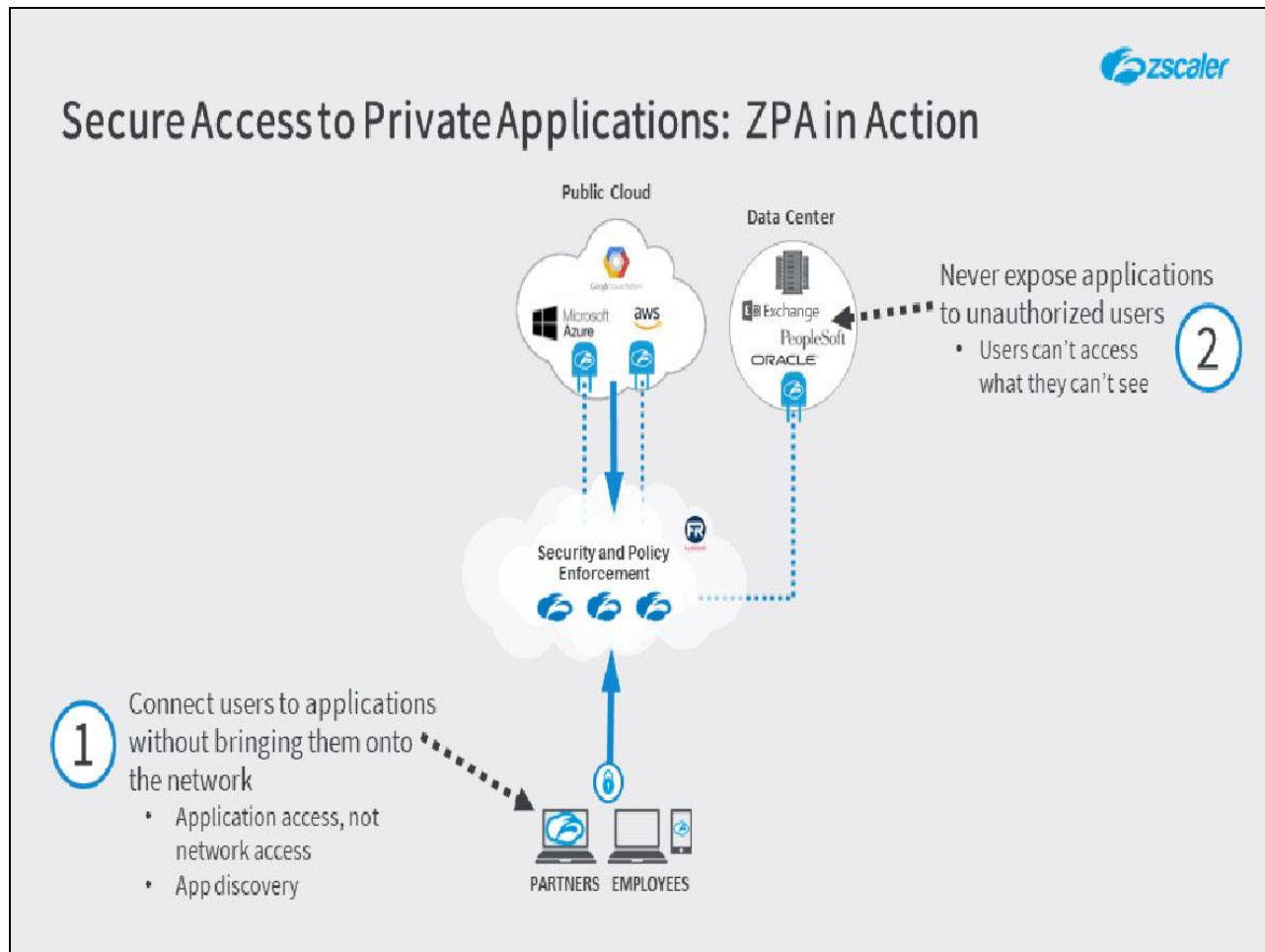
Slide notes

Zscaler Private Access has been built with four key security tenets in mind to achieve a true ZTNA infrastructure:

- **Tenet 1:** 'Connect users to applications without bringing them onto the network' - with ZPA, end users are never placed onto the private network, they are simply granted access to a specific application based on the applicable policy rules.

The goal has always been to connect users to applications without having to bring them onto the network. Application access shouldn't require network access, and access policies should be application-centric, rather than ACLs based on network IP addresses. If remote users are not brought onto your network, then it isn't extended to thousands of locations, which helps to minimize the attack surface, and provides better security.

Slide 10 - Secure Access to Private Applications: ZPA in Action

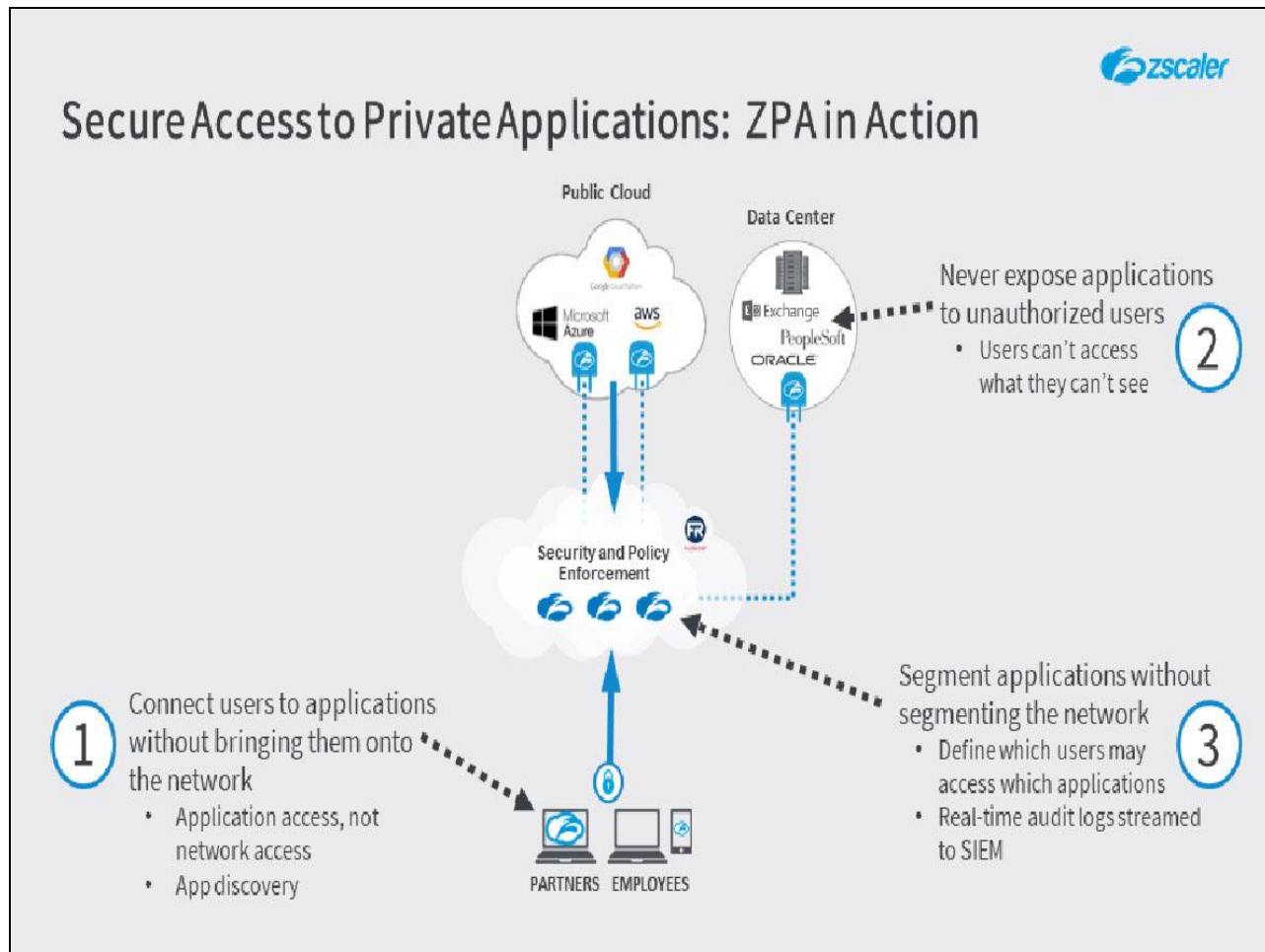


Slide notes

- **Tenet 2:** 'Never expose applications to unauthorized users' ZPA does not advertise the availability of applications; they are invisible to users other than legitimate and authenticated end users.

We never want to expose applications to unauthorized users. Application access should happen only after authentication succeeds and policy is applied, so unauthorized users cannot discover or exploit internal applications. Eliminating inbound connections and public IP addresses creates an enterprise darknet, where applications are invisible to the external and unauthorized users.

Slide 11 - Secure Access to Private Applications: ZPA in Action

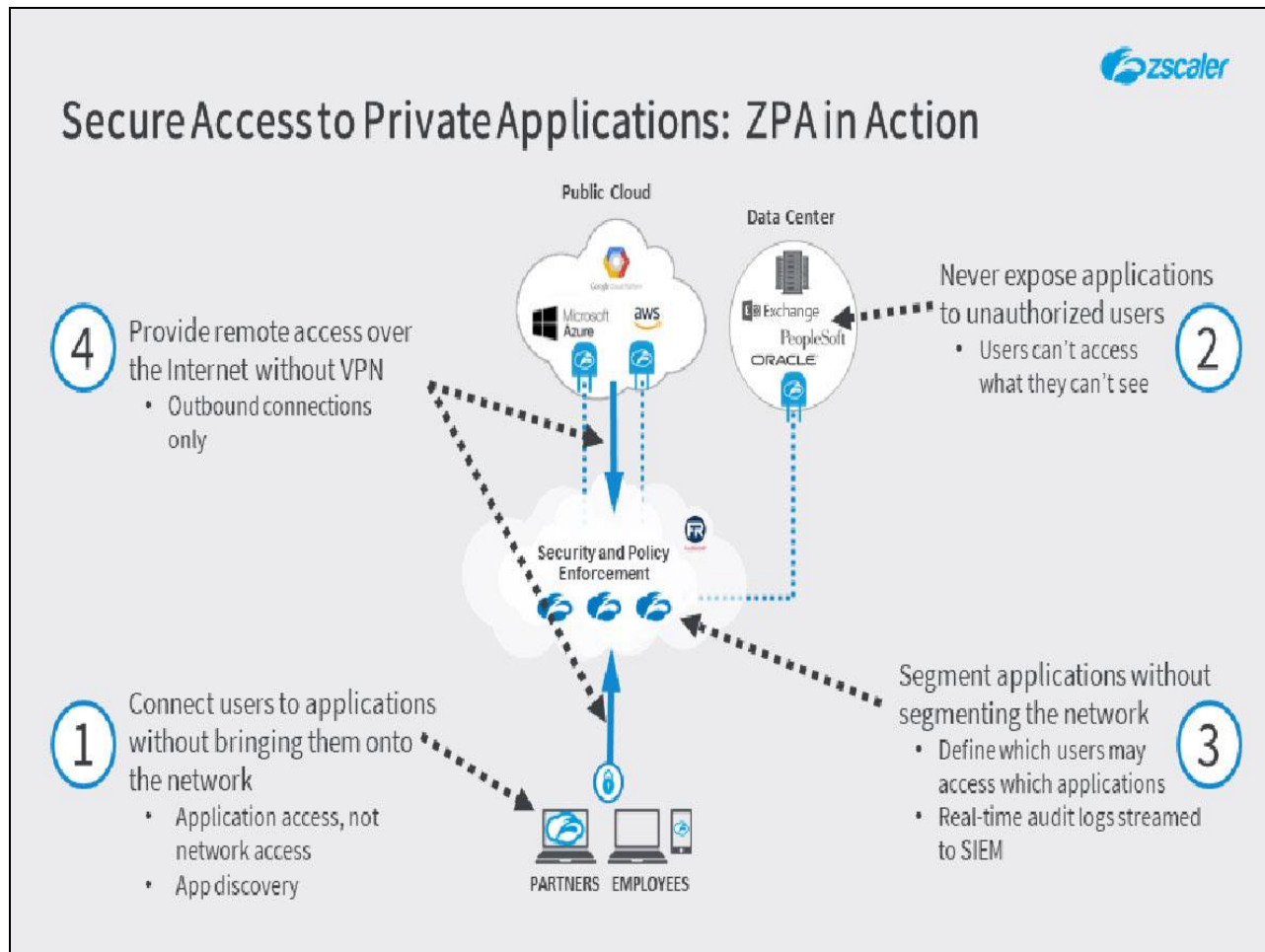


Slide notes

- Tenet 3:** 'Segment applications without segmenting the network' ZPA controls access to applications based on who the users are, what access they are entitled to, and the posture status of their end device.

We wanted to segment applications without having to segment the network. Each user connection is to a specific application, through a per-session micro-tunnel. Moving from a network-to-network connection, to a user-to-application connection, eliminates any possibility of lateral movement on the secure connection.

Slide 12 - Secure Access to Private Applications: ZPA in Action



Slide notes


- Tenet 4:** 'Provide remote access over the Internet without VPN' ZPA allows you to securely tunnel across the Internet to access the private applications you need, without the need to open network-level access. ZPA also allows the double encryption of data transferred between an end device and the application, for complete security and privacy.

We wanted to provide remote access over the Internet without the need for any form of remote access VPN connection. Both end points to a connection establish dynamic, outbound TLS tunnels, and Zscaler brokers the secure end-to-end user connection so that the traffic remains completely private. Data is encrypted end-to-end, plus for additional security, customers can use their own client and server certificates for double encryption.

Slide 13 - Four Main Enterprise Use Cases



Four Main Enterprise Use Cases



Business Customers

- Minimize exposure of apps
- Simplify identity management
- Browser access and user portal
- Improve visibility into activity

Slide notes

Common ZPA use cases include:

- Enabling truly secure partner, vendor or B2B access to specific applications only. ZPA end user authentication and access policy rules can control exactly who gets access to which applications, which prevents any possibility of unauthorized access.

Slide 14 - Four Main Enterprise Use Cases




Four Main Enterprise Use Cases

Business Customers	M&A
	
<ul style="list-style-type: none">• Minimize exposure of apps• Simplify identity management• Browser access and user portal• Improve visibility into activity	<ul style="list-style-type: none">• Simplify IT integration during M&A• Reduce cost of infrastructure• Standardize security for entities• Supports multiple trusted networks




Slide notes

- Quickly and securely allow (or block) access to applications on merger, acquisition, or divestiture. ZPA allows you to provide named users access to named applications without any need to merge, or route between networks.

Slide 15 - Four Main Enterprise Use Cases




Four Main Enterprise Use Cases

Business Customers	M&A	VPN alternative
		
<ul style="list-style-type: none">• Minimize exposure of apps• Simplify identity management• Browser access and user portal• Improve visibility into activity	<ul style="list-style-type: none">• Simplify IT integration during M&A• Reduce cost of infrastructure• Standardize security for entities• Supports multiple trusted networks	<ul style="list-style-type: none">• Remove inbound VPN gateway• Users never placed on-net• App segmentation by default• Prevent inbound connections





Slide notes

- As a remote access VPN replacement technology for employee access to internal applications. With ZPA you can give users access to specific applications. Users are never brought onto the network, and applications are never exposed to the Internet, all without the need to deploy any hardware.

Slide 16 - Four Main Enterprise Use Cases



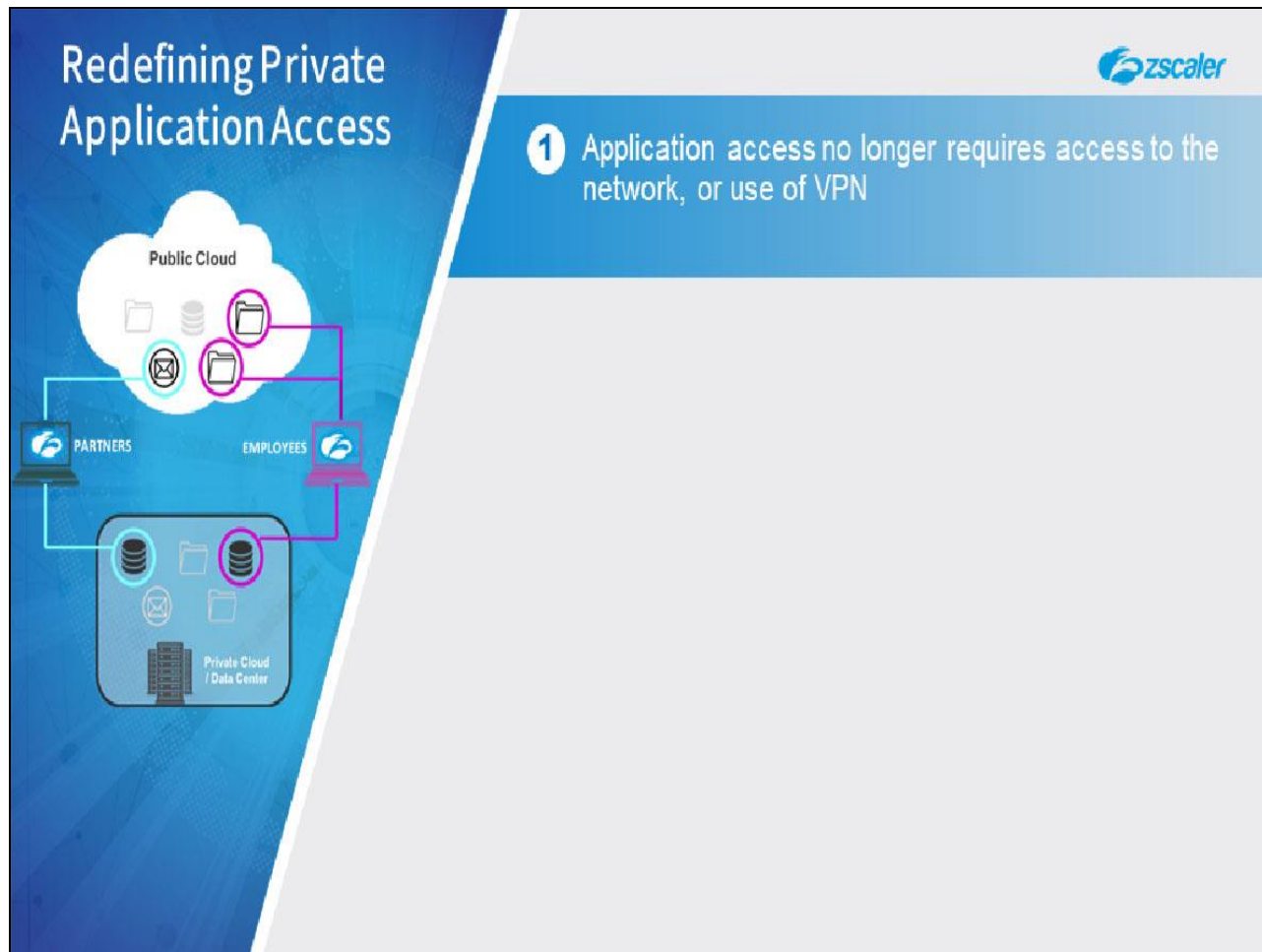
Four Main Enterprise Use Cases

Business Customers	M&A	VPN alternative	Multi-cloud access
			
<ul style="list-style-type: none">• Minimize exposure of apps• Simplify identity management• Browser access and user portal• Improve visibility into activity	<ul style="list-style-type: none">• Simplify IT integration during M&A• Reduce cost of infrastructure• Standardize security for entities• Supports multiple trusted networks	<ul style="list-style-type: none">• Remove inbound VPN gateway• Users never placed on-net• App segmentation by default• Prevent inbound connections	<ul style="list-style-type: none">• Avoid IaaS lock-in• Seamless hybrid cloud access• Improved user experience• Streamline adoption of IaaS

Slide notes

- To facilitate a migration to cloud-based applications. With ZPA you can transition to cloud seamlessly by deploying Connectors adjacent to your cloud applications. The end user experience is identical to accessing on-premise applications; no remote access VPN connectivity is required, and no new infrastructure.

Slide 17 - Redefining Private Application Access



Slide notes

All-in-all ZPA meets the majority of Gartner's criteria for consideration as a Zero trust Network access solution and completely redefines the private application access model. For a start, users no longer need network access in order to use an application, with ZPA they do not need to know where the application is hosted, they do not even know it's IP address!

Slide 18 - Redefining Private Application Access

Redefining Private Application Access

Public Cloud

Private Cloud / Data Center

PARTNERS

EMPLOYEES

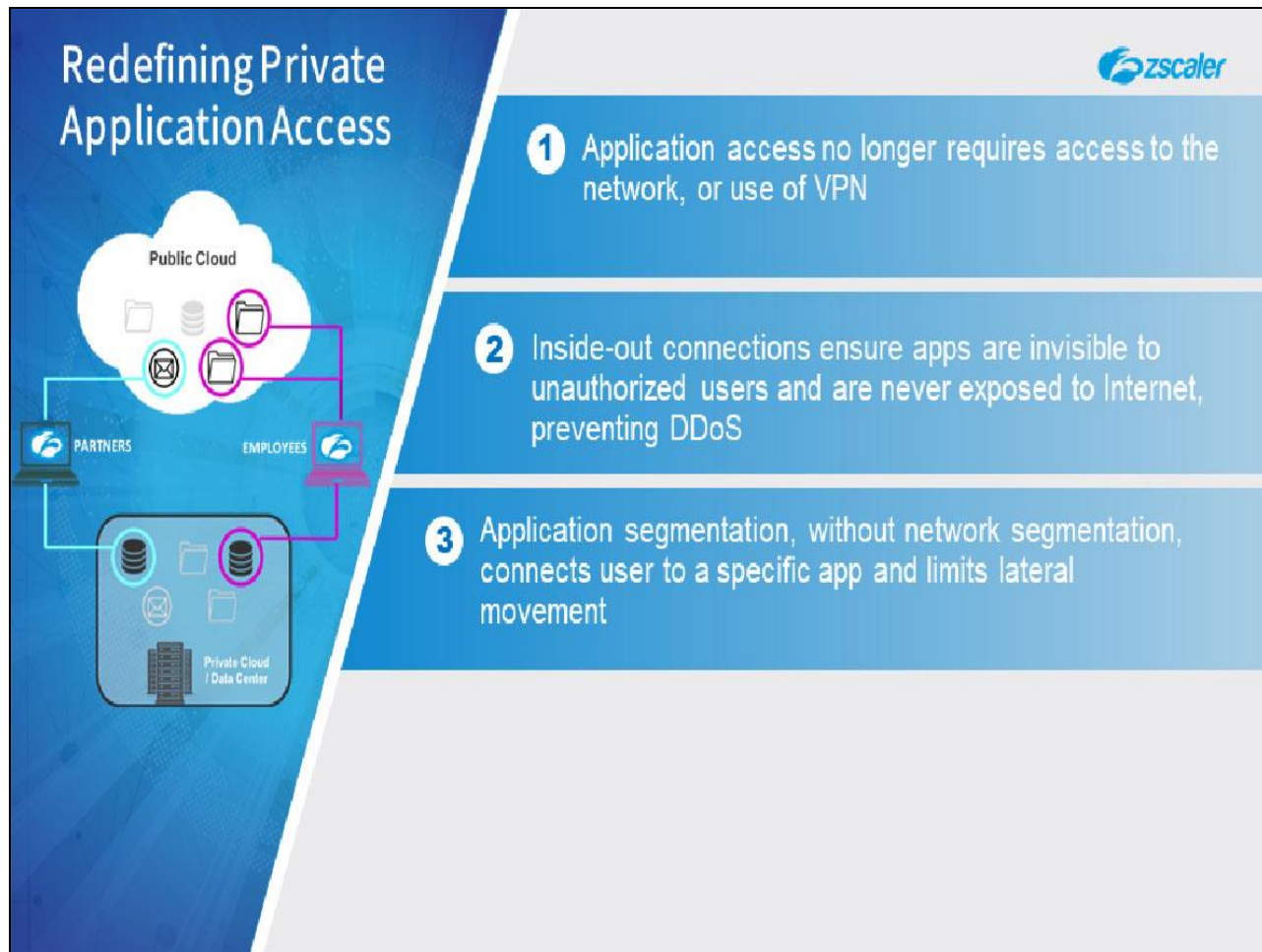
zscaler

- 1 Application access no longer requires access to the network, or use of VPN
- 2 Inside-out connections ensure apps are invisible to unauthorized users and are never exposed to Internet, preventing DDoS

Slide notes

The 'Inside-out' communication model of ZPA allows the data center to 'go dark', there is no longer any need to advertise the applications publicly. No inbound connections are required, removing the main vector for DDoS attacks against traditional VPN appliances.

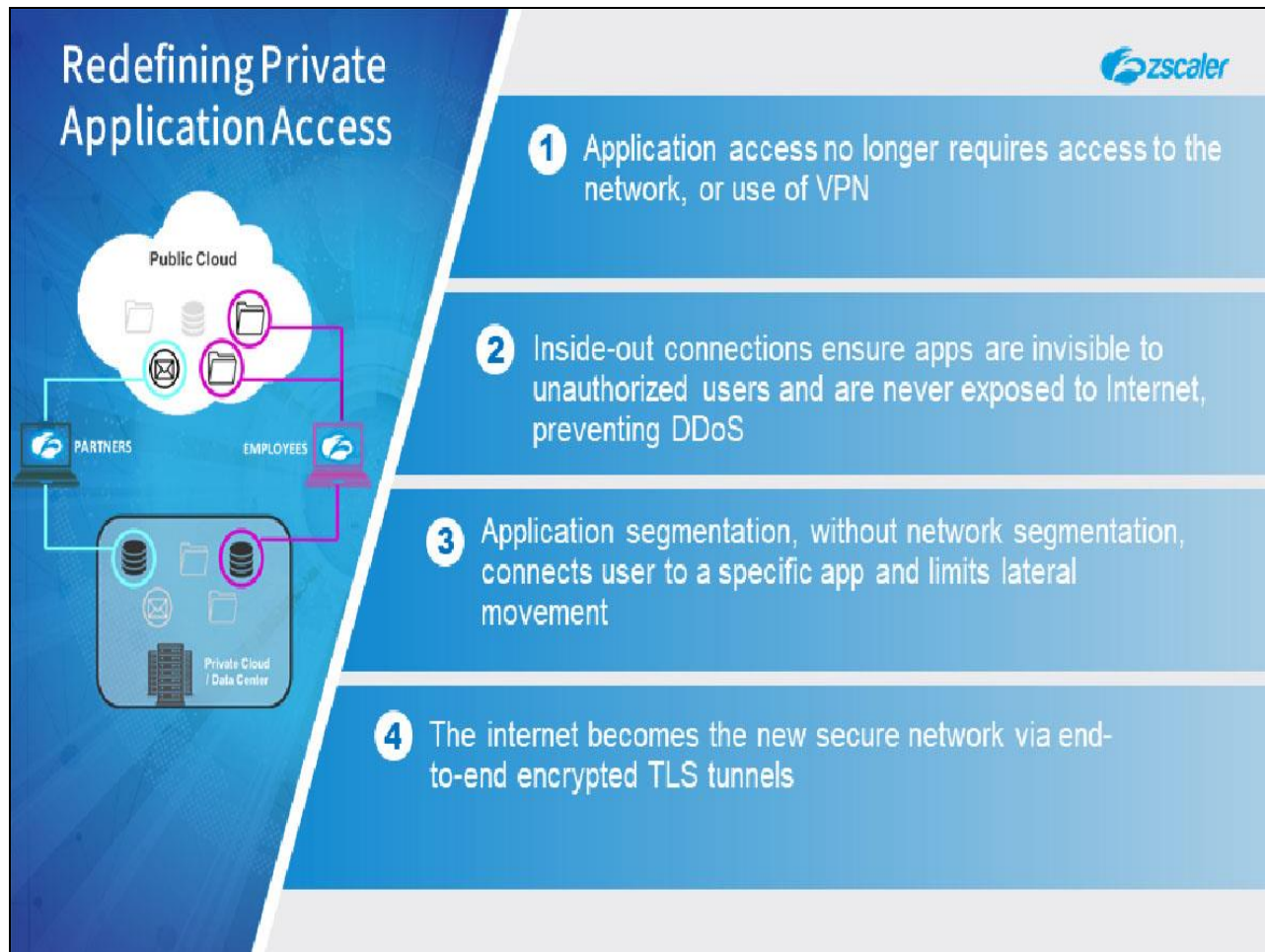
Slide 19 - Redefining Private Application Access



Slide notes

As the user is never placed onto the destination network by ZPA, there is absolutely no possibility of remote network discovery through probing, or lateral movement to exploit vulnerabilities in adjacent servers or other hosts.

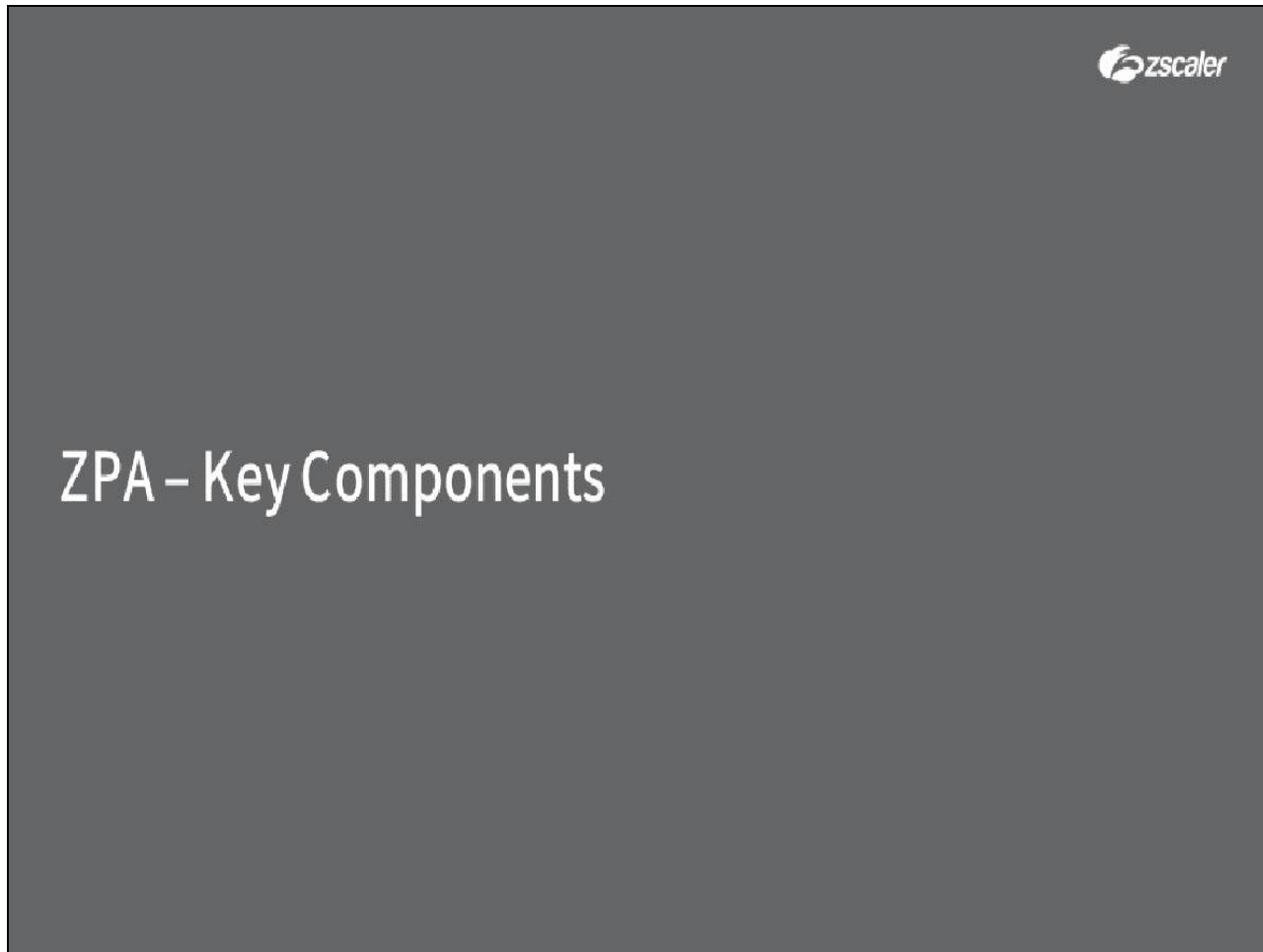
Slide 20 - Redefining Private Application Access



Slide notes

As a result, ZPA is the enabler that allows the Internet to be used as the new Corporate network, providing secure access to internal applications from mobile devices or direct from the Branch Office. Robust authentication of end users, granular access policy controls and end-to-end encryption all contribute to allow this network transition.


Slide 21 - ZPA Components










Slide notes

The next topic we will cover are the components of the Zscaler Private Access solution.

Slide 22 - ZPA Components



ZPA – Key Components

- **ZPA Central Authority (ZPA-CA)** – Multi-tenant, globally distributed, policy engine for provisioning policies and enabling connection requests
- **ZPA-ZENs** – Zscaler’s global traffic brokers enable the connection of users to Connectors for access to specific applications
- **Zscaler App (Z App)** – Enables a client to use ZPA and also delivers Zscaler’s award-winning cloud security services for Internet traffic.
- **App Connectors** – Lightweight virtual machines that enable connections to your applications across the ZPA cloud
- **ZPA Tunnels (Z Tunnels)** – Encrypted TLS 1.2 tunnels to the Zscaler Cloud
- **Microtunnels** – end-to-end data connection to private applications
- **Logging and Analytics Cluster and LSS** – correlates analytics information sent by the ZPA-ZENs. Log Streaming Service sends log data to your local SIEM

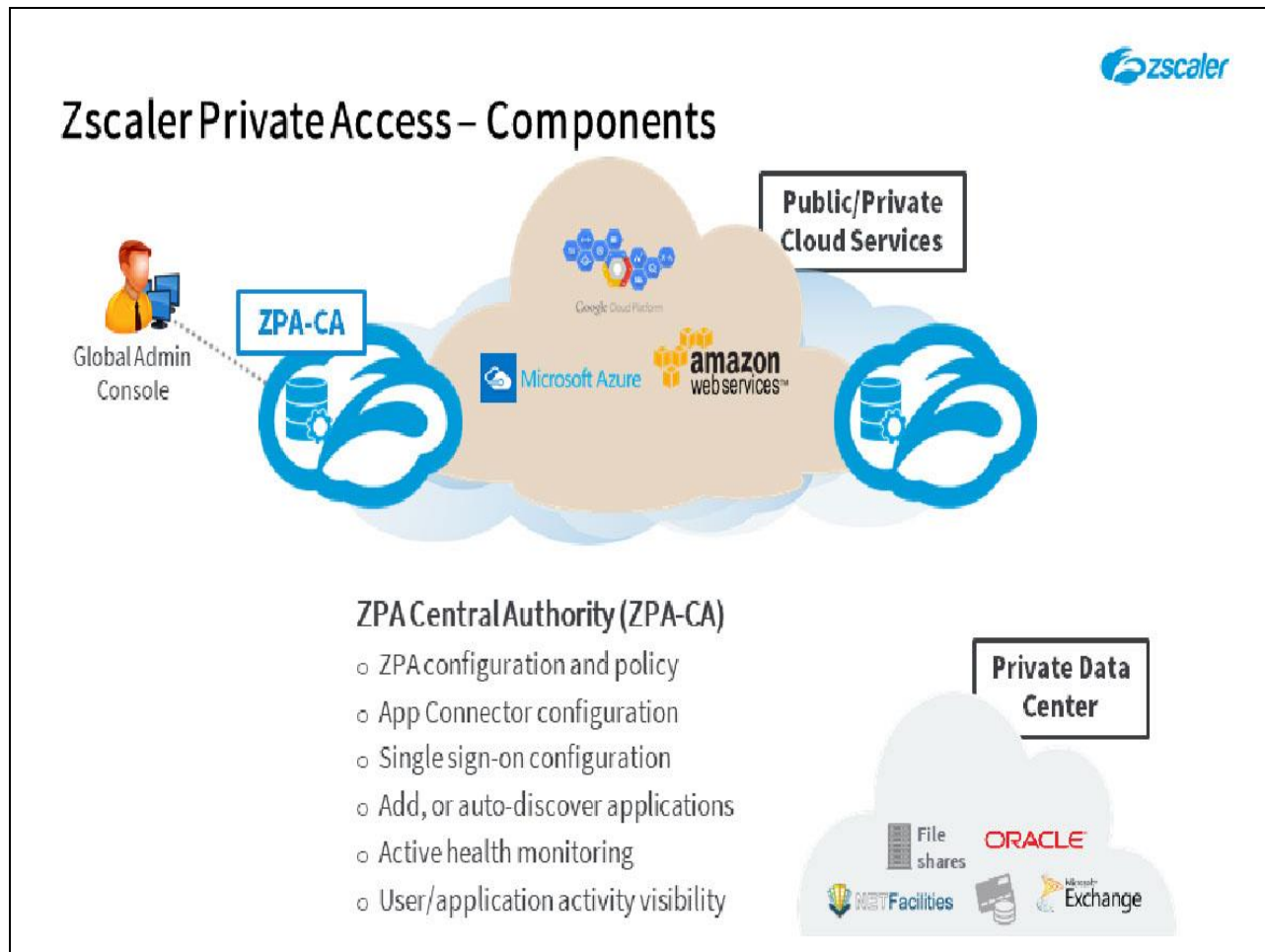
Slide notes

Zscaler Private Access is a service deployed on a completely separate cloud from the Zscaler Internet Access service, and some of the key components of the system are listed here. We will look at each in more detail in the following slides.

- The ZPA Central Authority (ZPA-CA) - is a multi-tenant, globally distributed policy engine for provisioning policies and enabling connection requests, providing full visibility into user activity and application access. Note this is a different engine from the regular Zscaler Internet Access CA.
- ZPA-ZENs - are globally available Zscaler Enforcement Nodes that act as brokers to enable the connection of users to Connectors for access to specific applications. Note that the ZPA-ZENs are distinct from standard ZENs used for Internet access. ZPA-ZENS are hosted in a combination of Zscaler in-house Data Centers, in AWS and in Azure to provide optimum coverage World-wide.
- The Zscaler App (Z App) - is a lightweight client available for the most popular end user platforms that can be configured to access ZPA applications. It can also be used to provide Zscaler’s award-winning cloud security services for Internet traffic. With Z App installed, authenticated and authorized end users can be given access to private TCP or UDP client/server applications regardless of port.

- App Connectors (Connectors) - these are lightweight RPMs or virtual machines (VMs) installed on the destination network, that establish an 'inside-out' connection from the private applications to the Zscaler cloud.
- ZPA Tunnels (Z Tunnels) - are fully encrypted TLS tunnels to the Zscaler cloud from both the Zscaler App, and from a Connector. These tunnels are mutually validated and doubly-pinned, so are immune to Man-in-the-middle attacks.
- Microtunnels - are end-to-end byte stream connections, identified by unique source and destination tags, that are used for user access to a specific application. Optionally Microtunnels may also be encrypted using Customer-derived keys (the Double Encryption option).
- And a Logging and Analytics Cluster and Log Streaming Service (LSS) - this component correlates analytics information sent by the ZPA-ZENs. The optional Log Streaming Service (LSS) allows you to stream log data to your SIEM through a chosen set of Connectors.

Slide 23 - Zscaler Private Access – Components



Slide notes

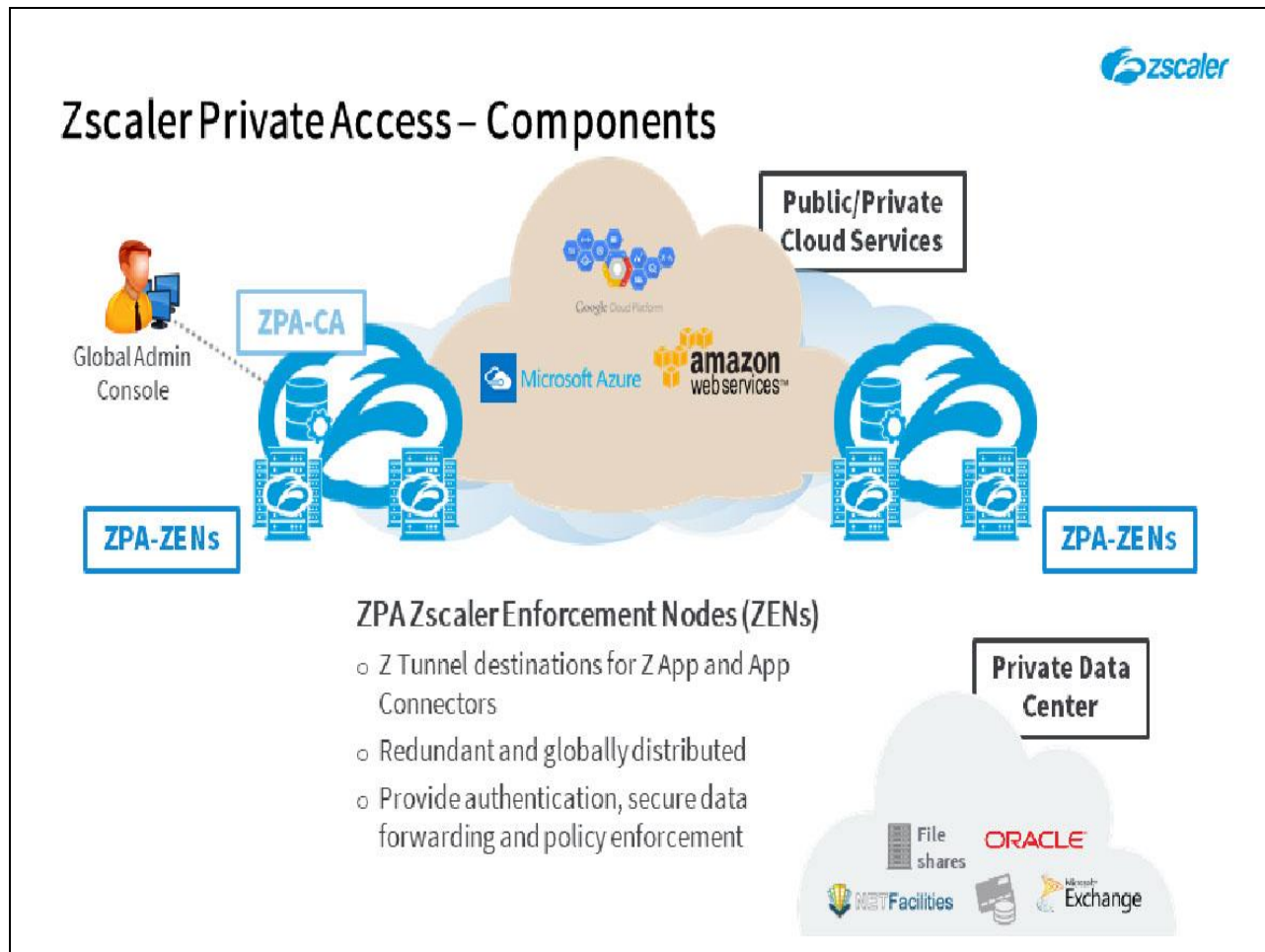
The ZPA Central Authority (CA) is the brains behind the ZPA system. It is a redundant, distributed, multi-tenant engine that is implemented within the ZPA cloud. It allows:

- The configuration of the environment;
- The establishment of policies for application access;
- It offers detailed visibility into user activity and application access;
- And it provides the Connectors with their configurations.

One or more SAML IdPs to be used for user and/or administrator authentication must be configured on the CA, and customer-signed enrollment certificates (if required) may be loaded to it. The CA lists all discovered applications and can be configured to target policies for specific applications (identified by hostname/IP address and port ranges).

The servers hosting the applications can be added manually or be dynamically discovered (recommended), and policy configurations are available to control exactly who gets access to what. As applications are discovered, the CA also monitors reachability and health, so that clients are always connected to the best possible instance of an application.

Slide 24 - Zscaler Private Access – Components

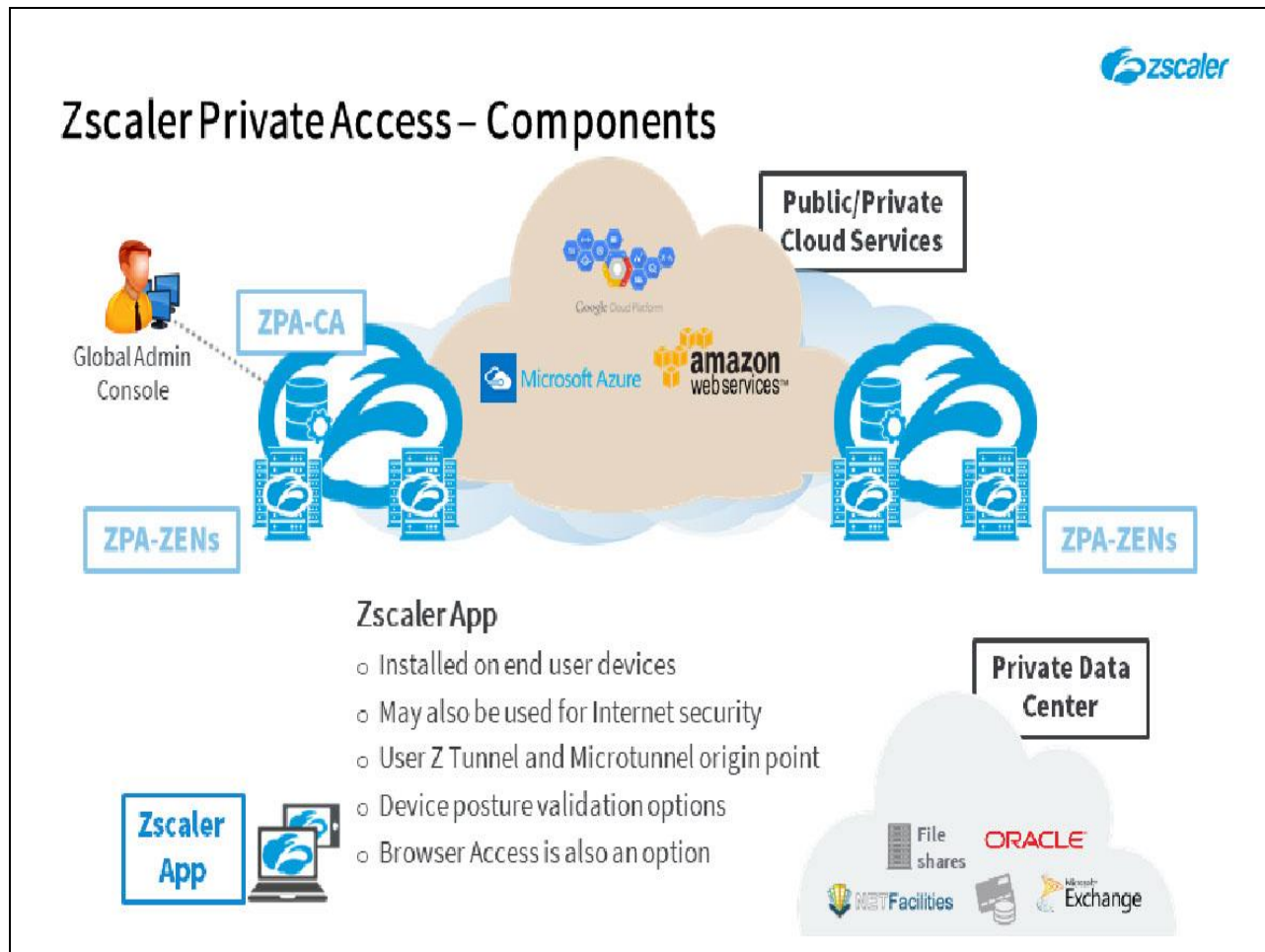


Slide notes

ZPA-ZENs, hosted within the ZPA Cloud, are the central contact points between the end user devices and the customer hosted components; they can be thought of as the data forwarding component of the system. The ZPA-ZENs are the Z Tunnel destinations for both the Zscaler App users, and the Connectors and they 'broker' the end-to-end connections needed by the end users.

ZPA-ZENs are hosted in Zscaler in-house DCs, in AWS and in Azure to provide a globally distributed, redundant access infrastructure. They also provide authentication, secure data forwarding and policy enforcement services.

Slide 25 - Zscaler Private Access – Components



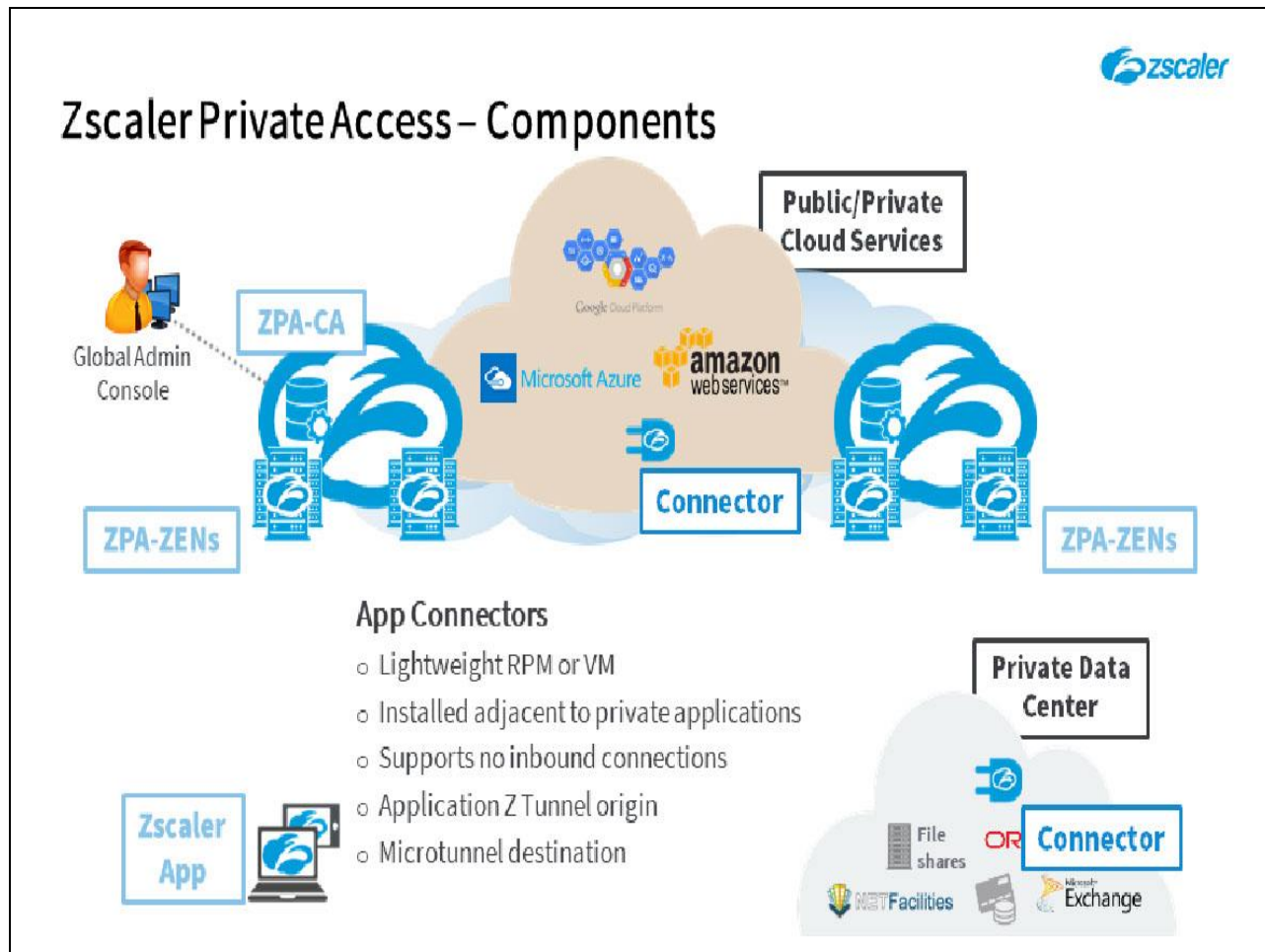
Slide notes

Deployed by the customer, the Zscaler App sits on end-user devices and enables the user to request access to applications. It may be used just for ZPA access to applications, or it can also be configured to protect Internet bound traffic by forwarding it to the Zscaler Internet Access Cloud. When connecting to ZPA applications, the browser (or other SW agent) on the end user's device will believe that it is talking direct to the application on a synthetic IP address assigned for the application by Z App.

The Zscaler App is the origin point for the user's encrypted Z Tunnels, and the end-to-end Microtunnels required to connect the user to private resources. Posture profiles can be defined to ensure that access is only permitted to your private applications if the host device complies to specified posture requirements.

Note that the Zscaler App is not required for ZPA access, as that can also be achieved for web applications from a standard browser using a Browser Access (BA) configuration. However, Z App is required to allow client device posture-checking, trusted network configuration validation and to provide multi-protocol access to private applications.

Slide 26 - Zscaler Private Access – Components



Slide notes

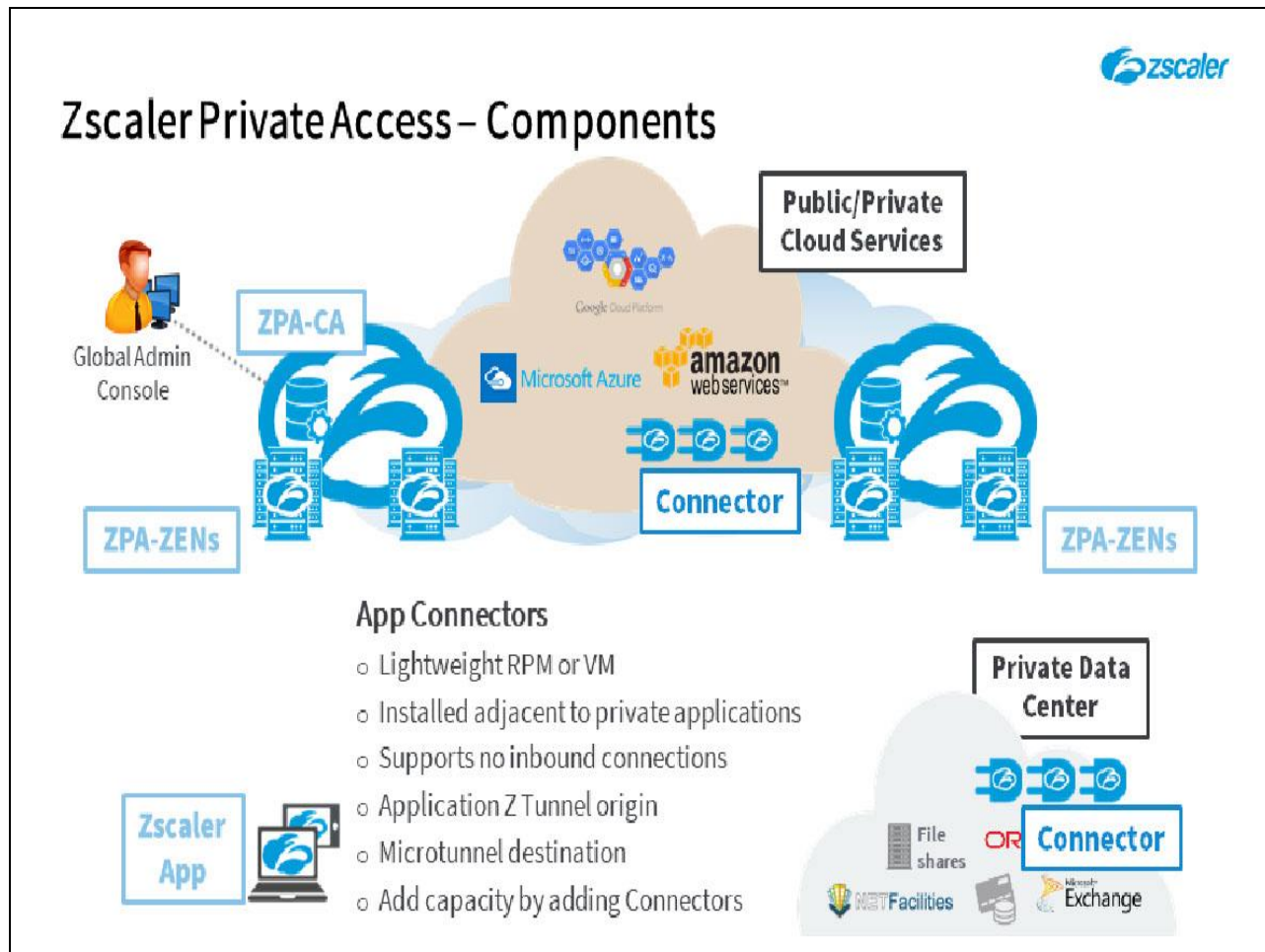
Also deployed by the customer, the App Connector is the only component of the ZPA solution that is connected to the customer's internal network, adjacent to the applications that need to be accessible. It is available as a lightweight virtual machine for a number of popular hypervisor solutions, or as a Remote Package Manager (RPM) for deployment on Linux.

Connectors must be able to DNS resolve the applications to be made available over ZPA and subsequently establish a connection to them. The applications will believe that they are talking solely to the Connector and are unaware of the tunneling used to connect with the end user's device.

A Connector is a lightweight software module that boots extremely fast and is intended to sit adjacent to the private applications that you need to provide remote access to, typically on the same subnet. Connectors neither support, nor require any inbound connections. They are the origin point for the application Z Tunnels, and destination for the end-to-end Microtunnels.

A provisioning key, signed by the appropriate ZPA subsidiary CA, is required to enroll a Connector after which it receives its configuration and certificates from the ZPA-CA. They may be updated or restarted from the CA as required.

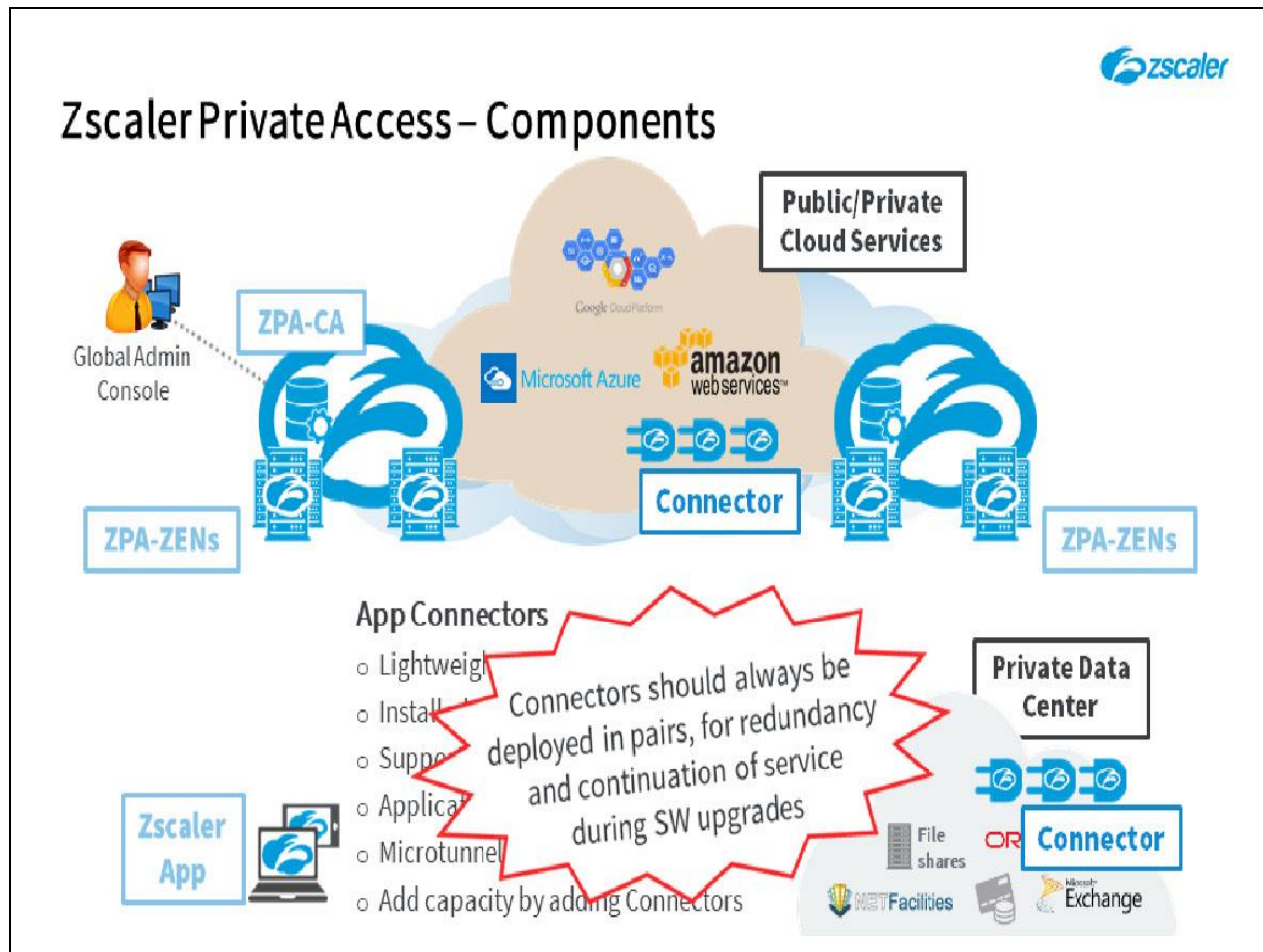
Slide 27 - Zscaler Private Access – Components



Slide notes

A single Connector supports up to 500Mbps of throughput and to add access capacity for your private applications, you simply need to add more Connectors. They scale horizontally without any need for clustering or load-balancing; the ZPA-CA automatically distributes user sessions across the available Connectors to ensure an optimum user experience.

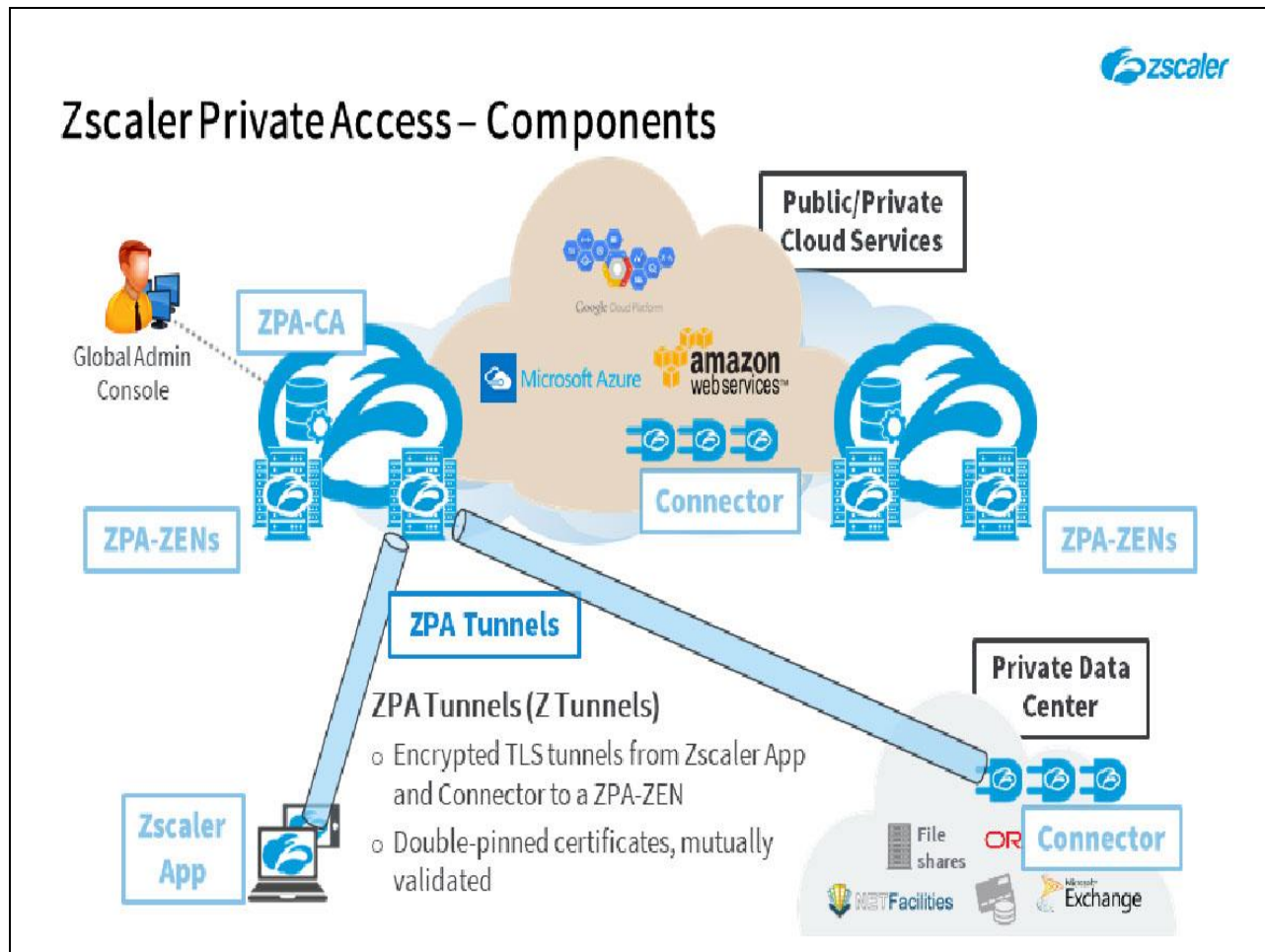
Slide 28 - Zscaler Private Access – Components



Slide notes

Note that Zscaler recommends that Connectors always be deployed in pairs, for redundancy and to ensure continuous availability during the weekly Connector software upgrades.

Slide 29 - Zscaler Private Access – Components



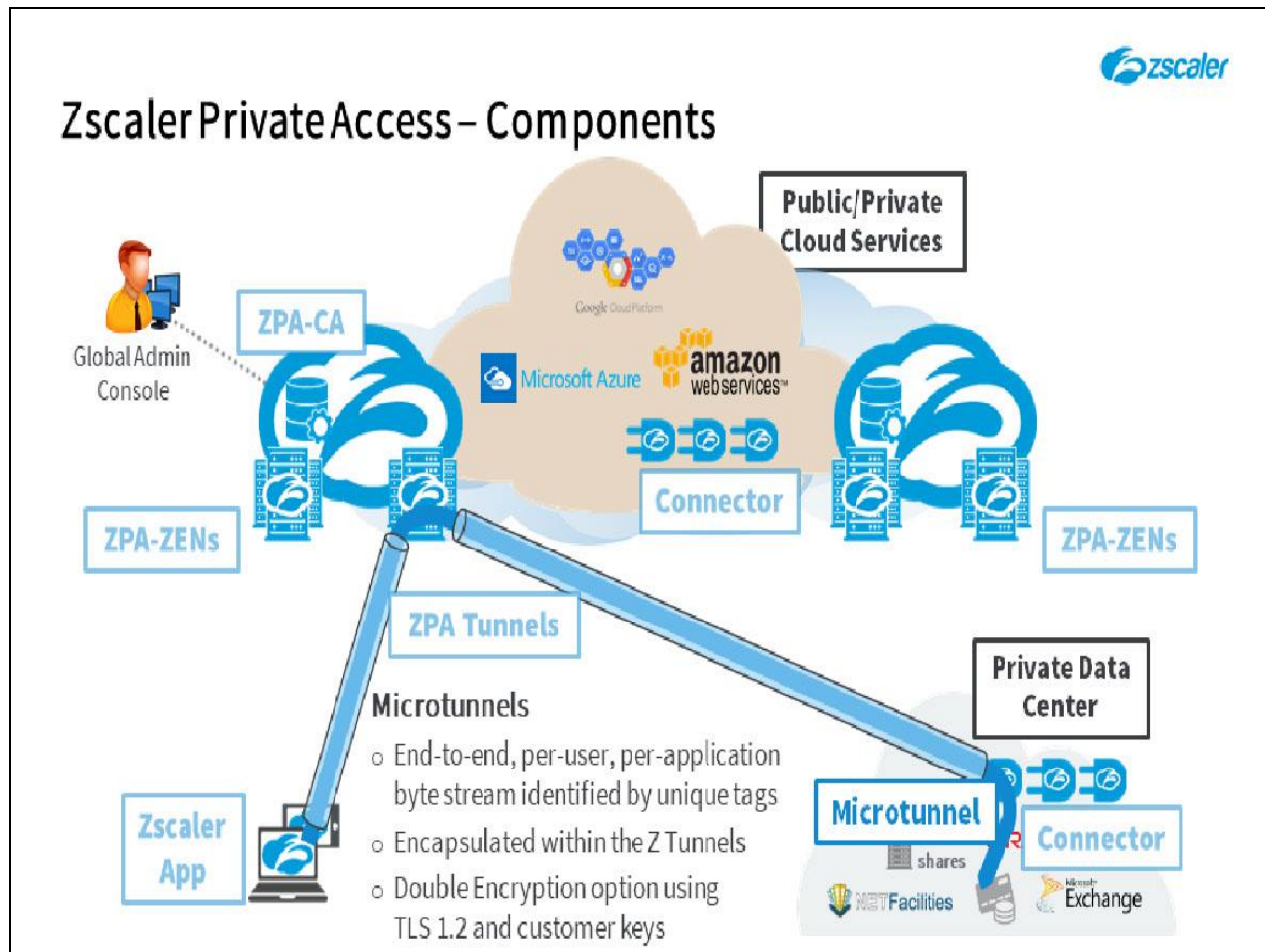
Slide notes

ZPA Tunnels (Z Tunnels) are encrypted TLS tunnels on port 443 that are established outbound by both the Zscaler App and the selected Connector, to the nominated ZPA-ZEN for the connection. Both the Connector and the Zscaler App may open multiple Z Tunnels to the ZPA infrastructure, depending on the locations of the applications requested, and the users requesting them.

These tunnels are double-pinned with mutual certificate validation, so are immune to Man-in-the-Middle attacks. If you use outbound Firewall rules, contact Zscaler for the IPs that must be allowed for these connections.

The authentication of the Z Tunnels from the Zscaler App is inherently multi-factor, as they are validated using the SAML assertion, user identity certificate, and a hardware fingerprint; for the Connector Z Tunnel an identity certificate and hardware fingerprint are used for validation. TLS 1.2 is used to establish these tunnels, with the strongest encryption cipher that is mutually supported by the Zscaler App and Connector hosts, and the ZPA-ZENs.

Slide 30 - Zscaler Private Access – Components



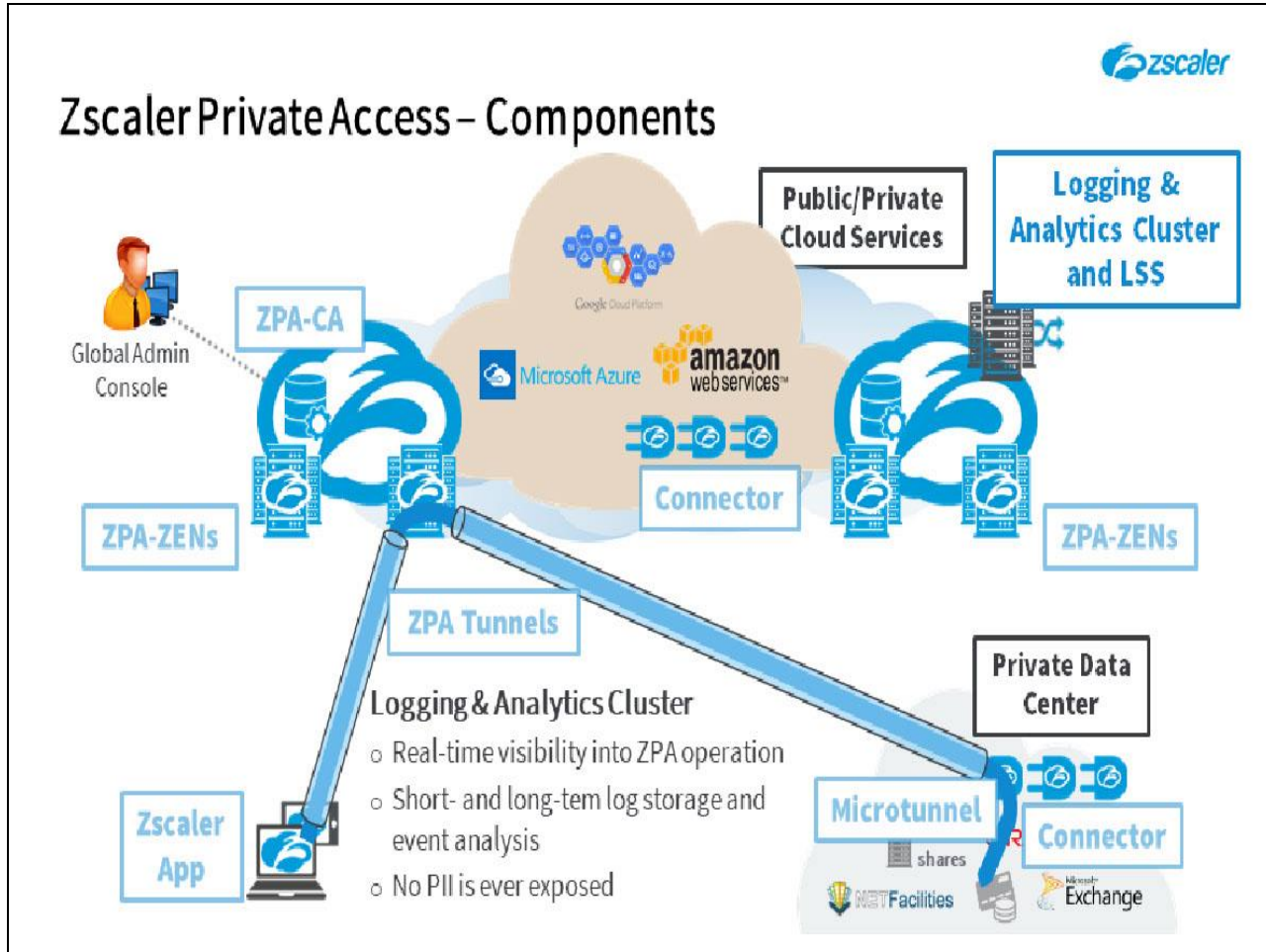
Slide notes

Microtunnels consist of the data byte stream from the client application (Browser or software) that is transported within the Z Tunnels to provide end-to-end connectivity between the client-side agent on the end user's device and the private application (in the datacenter or cloud). Microtunnels are established on a per-user, per-application basis, and cannot be shared.

They are addressed using unique IDs allocated dynamically when the connection is first established. The addressing of data into the Microtunnels is somewhat similar to the 'Label Switched Path' of an MPLS network, with Microtunnel IDs being generated on-the-fly by the Zscaler App, and the Connector as required, and the ZPA ZEN switching traffic into the Microtunnels as necessary (based on the IDs) to provide application connectivity.

Optionally, an additional encrypted TLS tunnel can be established within the Microtunnel, encrypted using the strongest cipher that is mutually supported by the Zscaler App and Connector hosts. Keys can be provided by the customer, which means that Zscaler has no possibility of intercepting, or reading data within the tunnel at the ZPA ZEN. This results in the double-encryption of traffic between the Zscaler App and Connector.

Slide 31 - Zscaler Private Access – Components



Slide notes

The Logging and Analytics Cluster provides real-time visibility into the operation of ZPA by analyzing events reported, primarily by the ZPA-ZENs. Information includes:

- Primary tunnel logs (which consist of authentication logs for the Connectors and the Zscaler App end stations);
- As well as Microtunnel logs (which consist of transaction data).

These logs are sent to both the Log Cluster and, if so configured, to your SIEM through the Log Streaming Service (LSS). The ZPA Log Clusters and LSS provide real-time analytics and status, as well as short and long-term log storage.

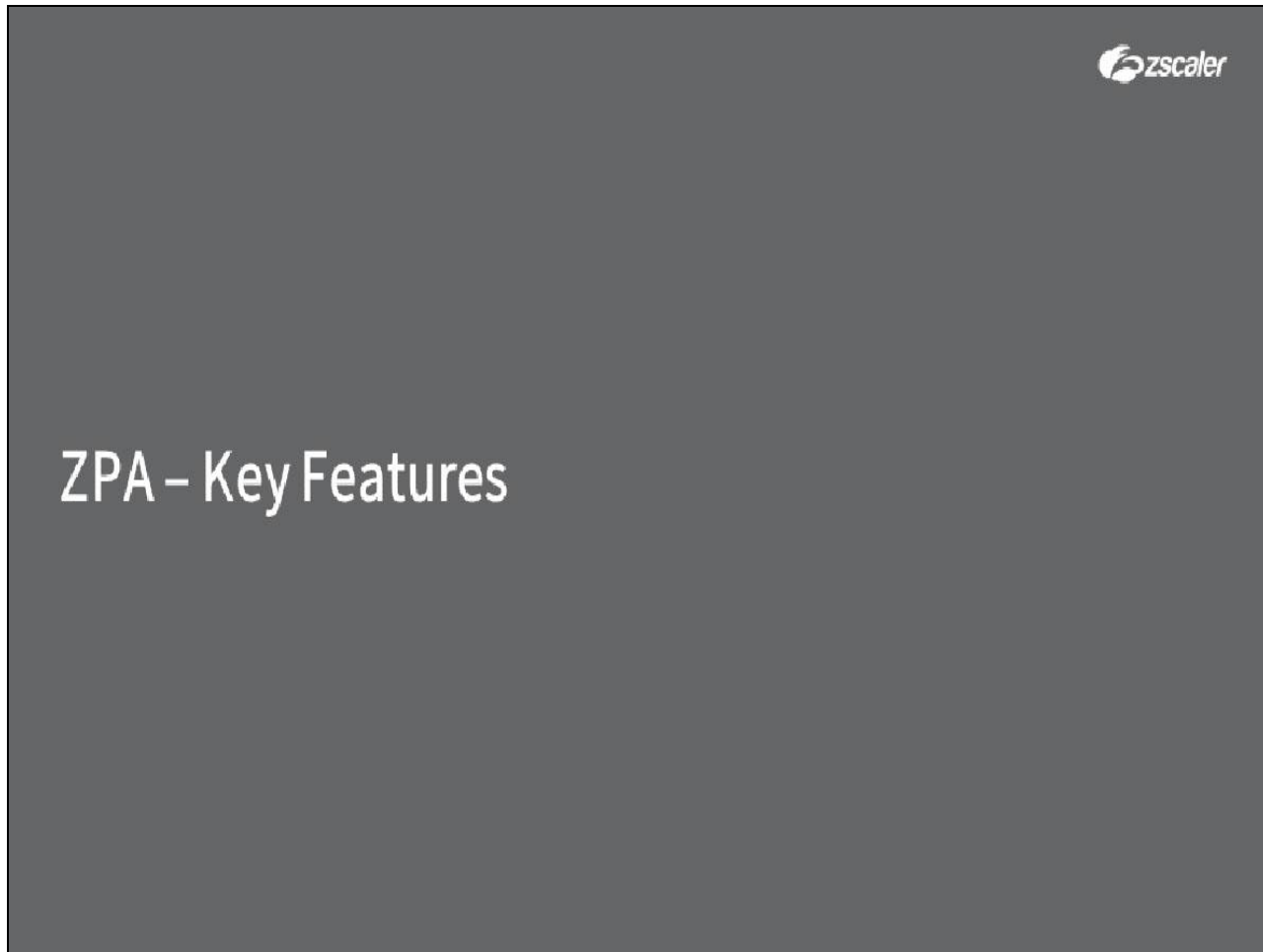
No personally identifiable information (PII) is included in any logs created by ZPA, as security and privacy are the central tenets upon which the solution has been built. The material is never stored on any type of persistent media until it arrives at the Log Cluster. The information can also be obfuscated, based on the customer's preferences.

It is important to note that data at rest in the Log Cluster consists of abstracted IDs and is not useful in any way on its own; this information must be combined with additional information housed elsewhere to derive anything meaningful. Should this data ever be combined, ZPA does not retain any record of the traffic.

The log streaming service (LSS) allows you to automatically stream user activity, user authentication connector and Browser Access logs to your SIEM. You can then view them at leisure within your SIEM to analyze, identify and remediate as needed. LSS provides a better understanding of the information coming from the ZPA service, by allowing you to create log receivers that can receive information about Connectors and users.

LSS utilizes ZPA to stream the logs, and therefore requires a Connector adjacent to your SIEM. LSS initiates a log stream through a ZPA ZEN which forwards it to a log receiver (your SIEM) through the appropriate Connector.

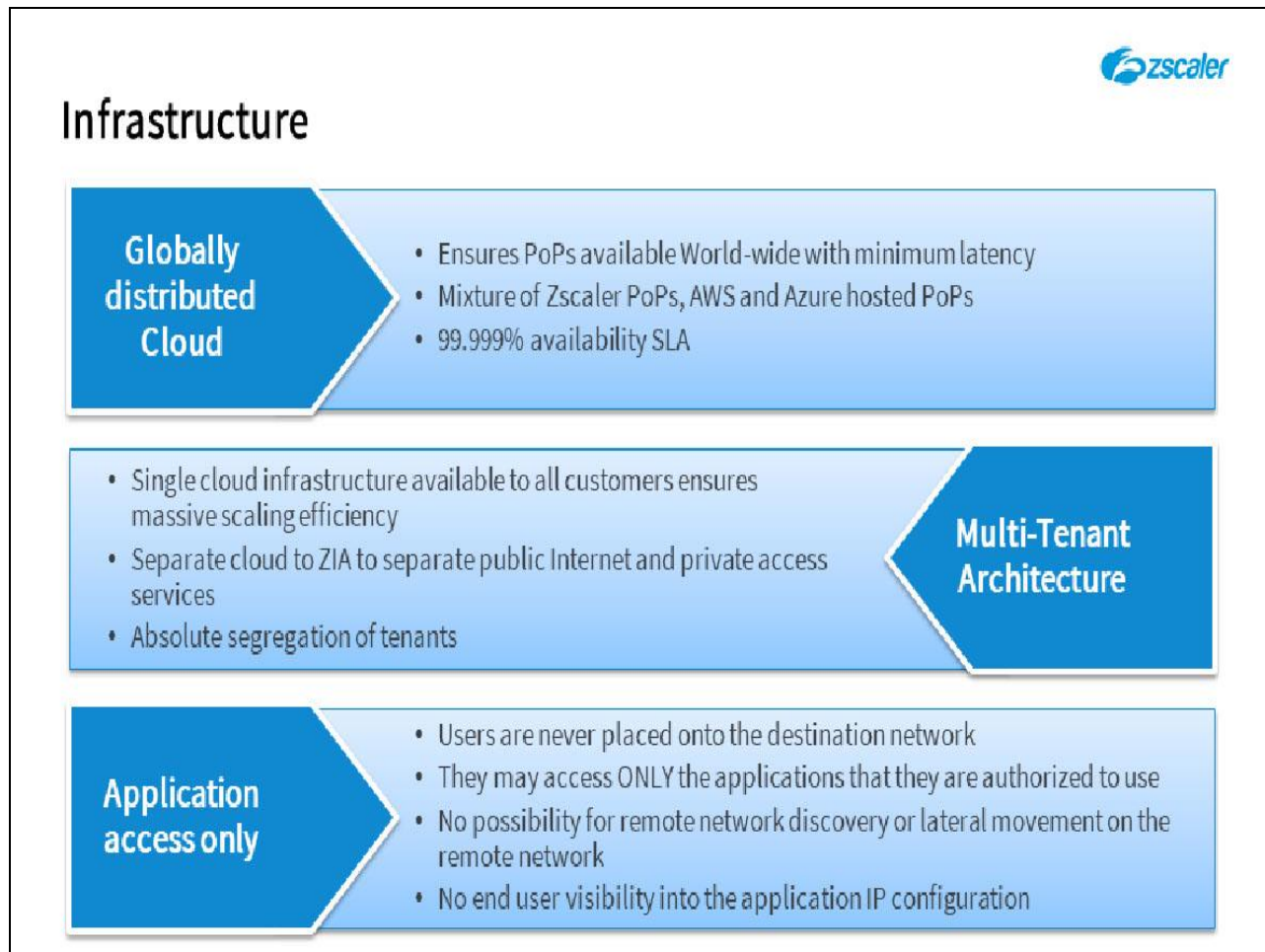
Slide 32 - ZPA – Key Features



Slide notes

The final topic we will cover is a list of some of the principal features of the Zscaler Private Access solution. Note, review the specifics of each item in your own time, there may be Quiz questions on the list of features, but not on their details.

Slide 33 - Infrastructure

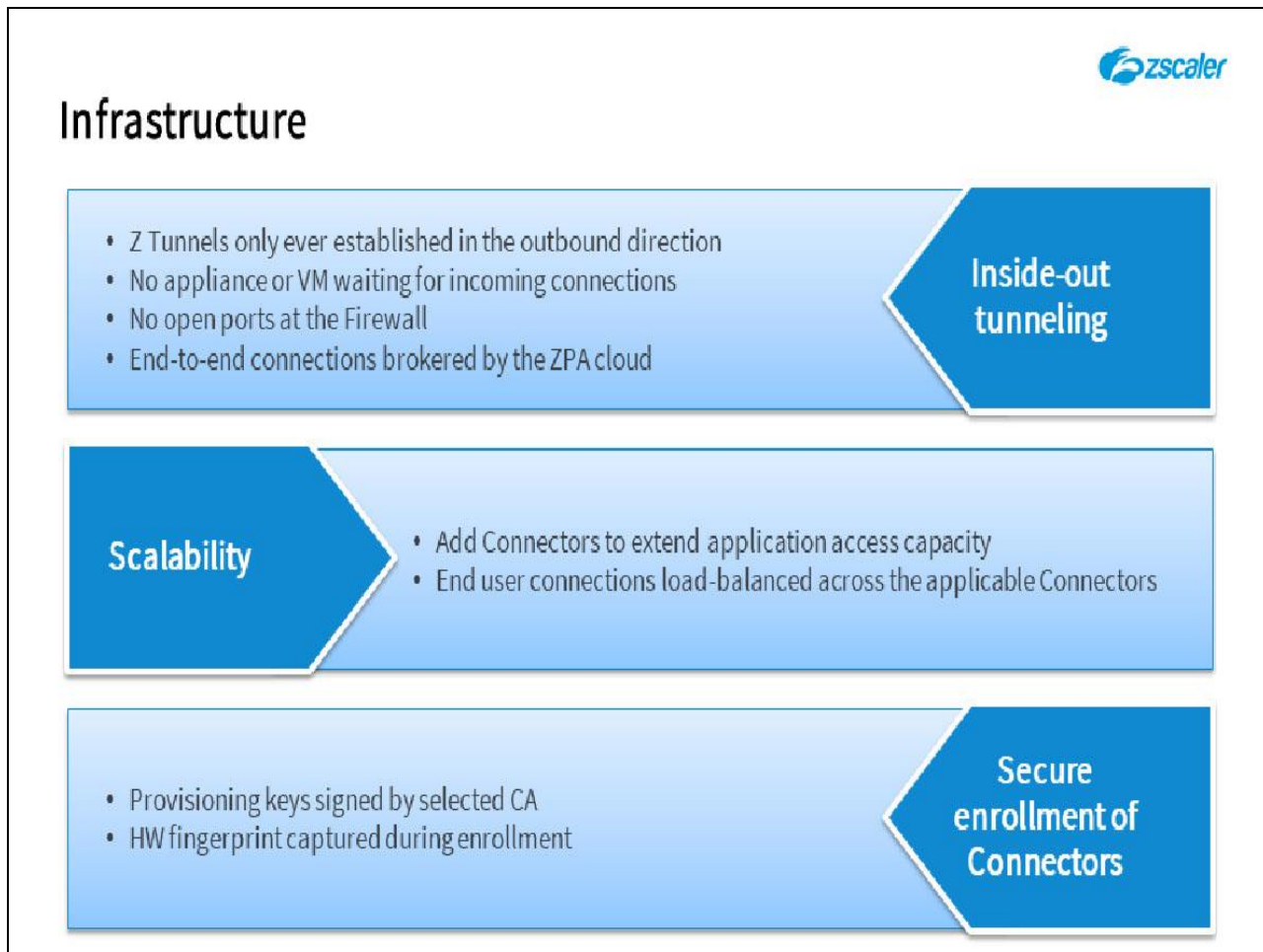


Slide notes

In terms of the infrastructure provided by the ZPA service, here are some of the most important features of the solution:

- ZPA provides a globally distributed cloud service;
- It is a multi-tenant infrastructure;
- ZPA provides end user access to named applications only, it does NOT provide access to the destination network in any way;

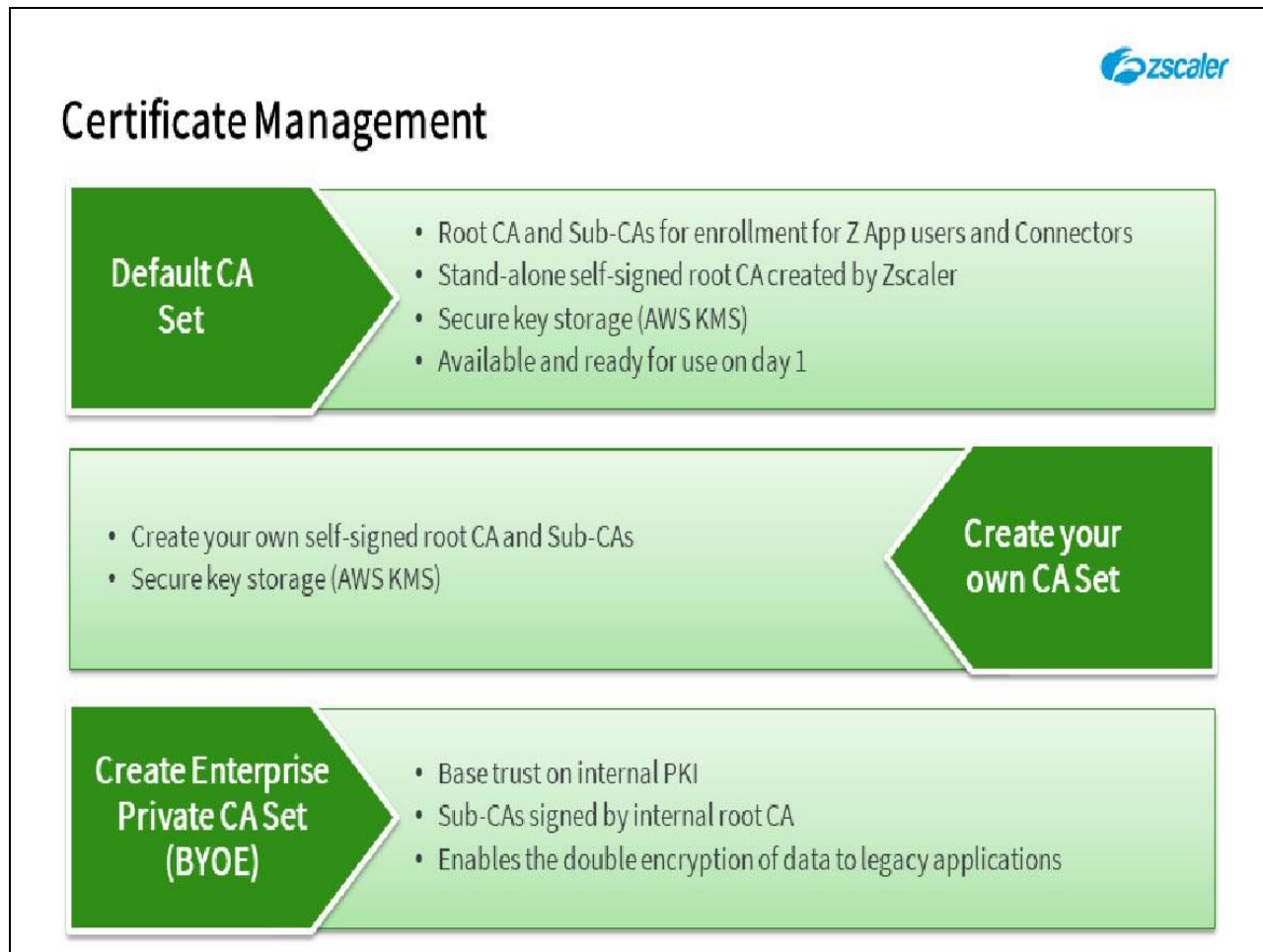
Slide 34 - Infrastructure



Slide notes

- ZPA provides an 'inside-out' tunneling model, where the encrypted TLS tunnels are only ever established in the outbound direction;
- The ZPA cloud is highly scalable;
- And ensures the secure enrollment of the infrastructure components (Connectors) that are installed on the customer's network.

Slide 35 - Certificate Management

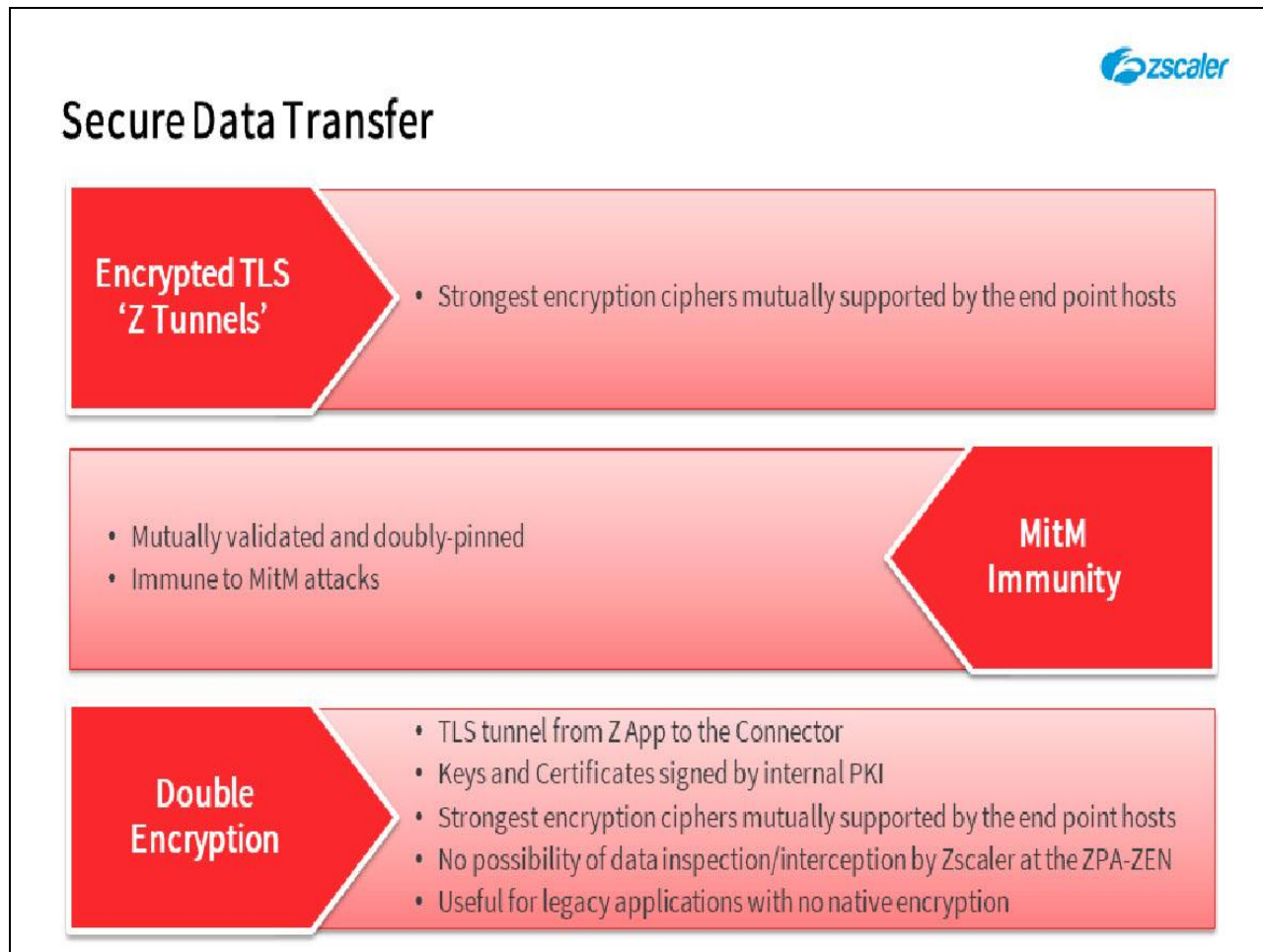


Slide notes

In the certificate management area:

- ZPA provides a default set of certificates for device enrollment and the establishment of TLS tunnels on subscription to the service;
- Alternatively, customers can generate their own self-signed certificate authorities;
- Or even upload certificates signed by an internal enterprise private CA.

Slide 36 - Secure Data Transfer

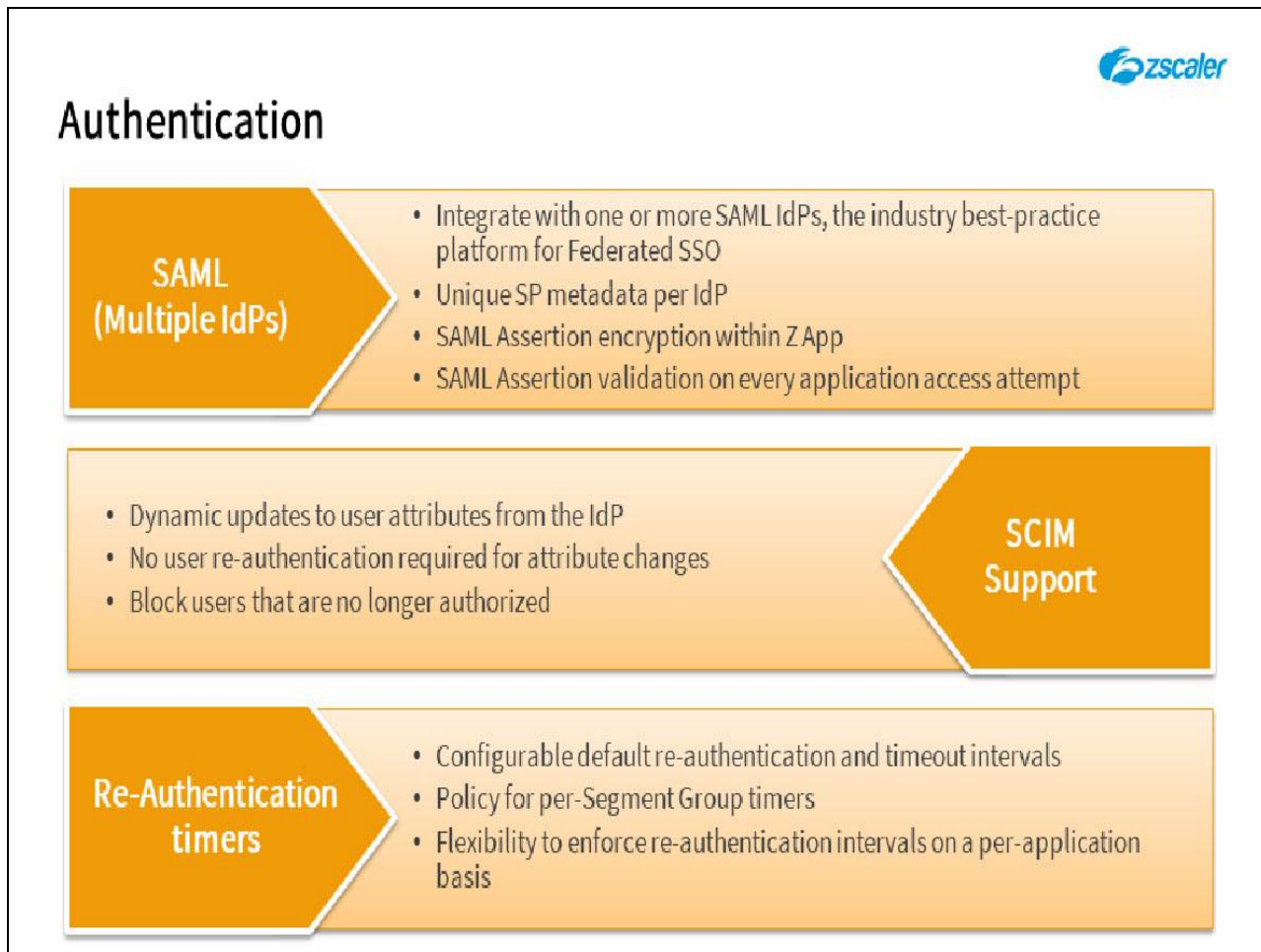


Slide notes

For the secure transmission of application data:

- ZPA tunnels used for data transfer are encrypted with the strongest mutually supported cipher;
- Are immune to Man-in-the-middle attacks;
- A 'Double Encryption' option is available to ensure end-to-end security for data transferred to/from legacy, unencrypted applications.

Slide 37 - Authentication

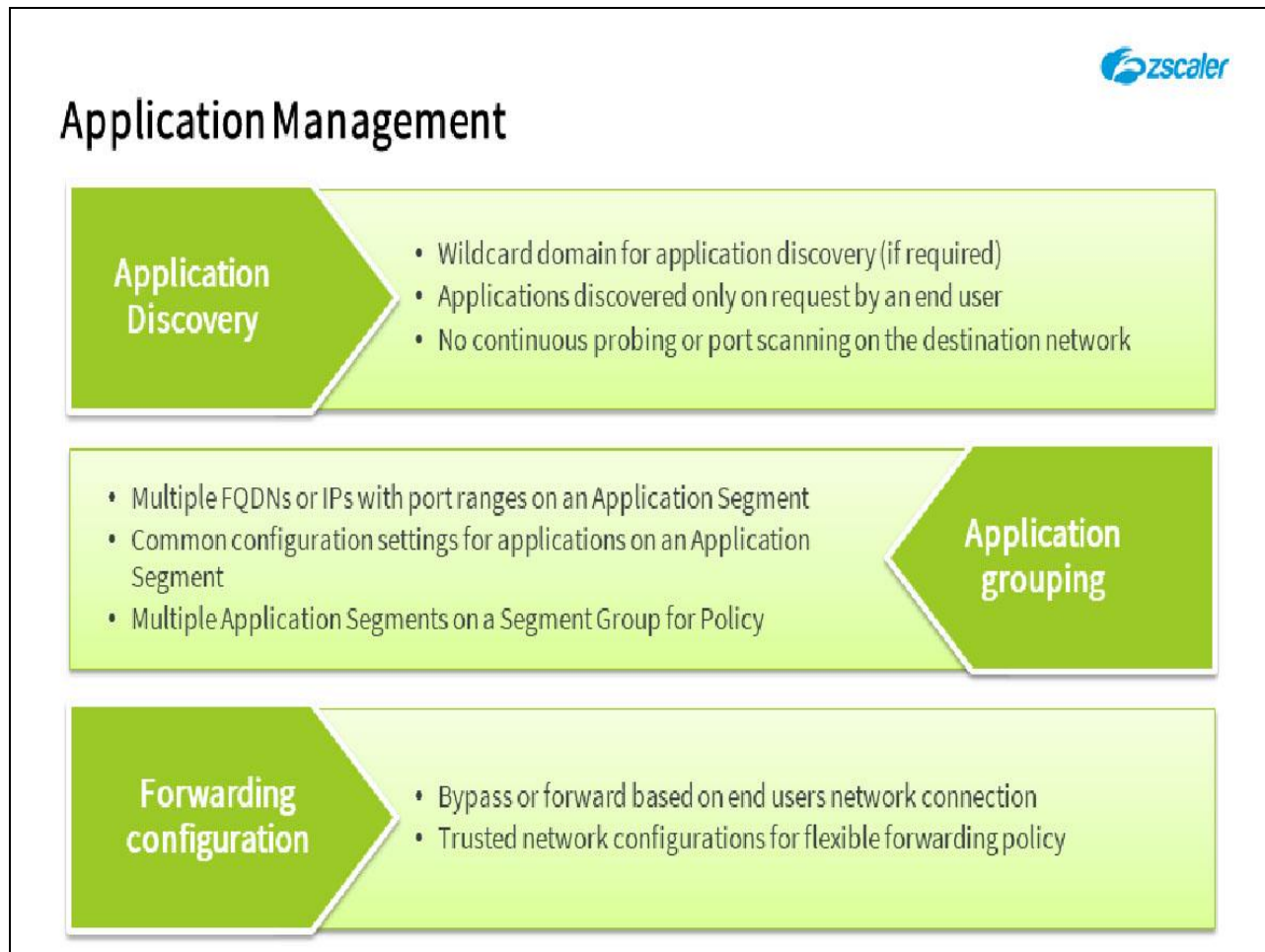


Slide notes

In the area of authentication:

- ZPA supports integration with multiple SAML Identity Providers (IdPs);
- The service supports the dynamic management of user accounts using the System for Cross-domain Identity Management (SCIM);
- Plus, ZPA provides configurable per-application re-authentication timers.

Slide 38 - Application Management




Slide notes

In the area of application management:

- ZPA allows the on-demand discovery of applications, without the need for continuous probing or port scanning on the destination network;
- Applications can be logical grouped at several levels;
- There are flexible forwarding configuration options, based on the network that an end user is connected to;

Slide 39 - Application Management



Application Management

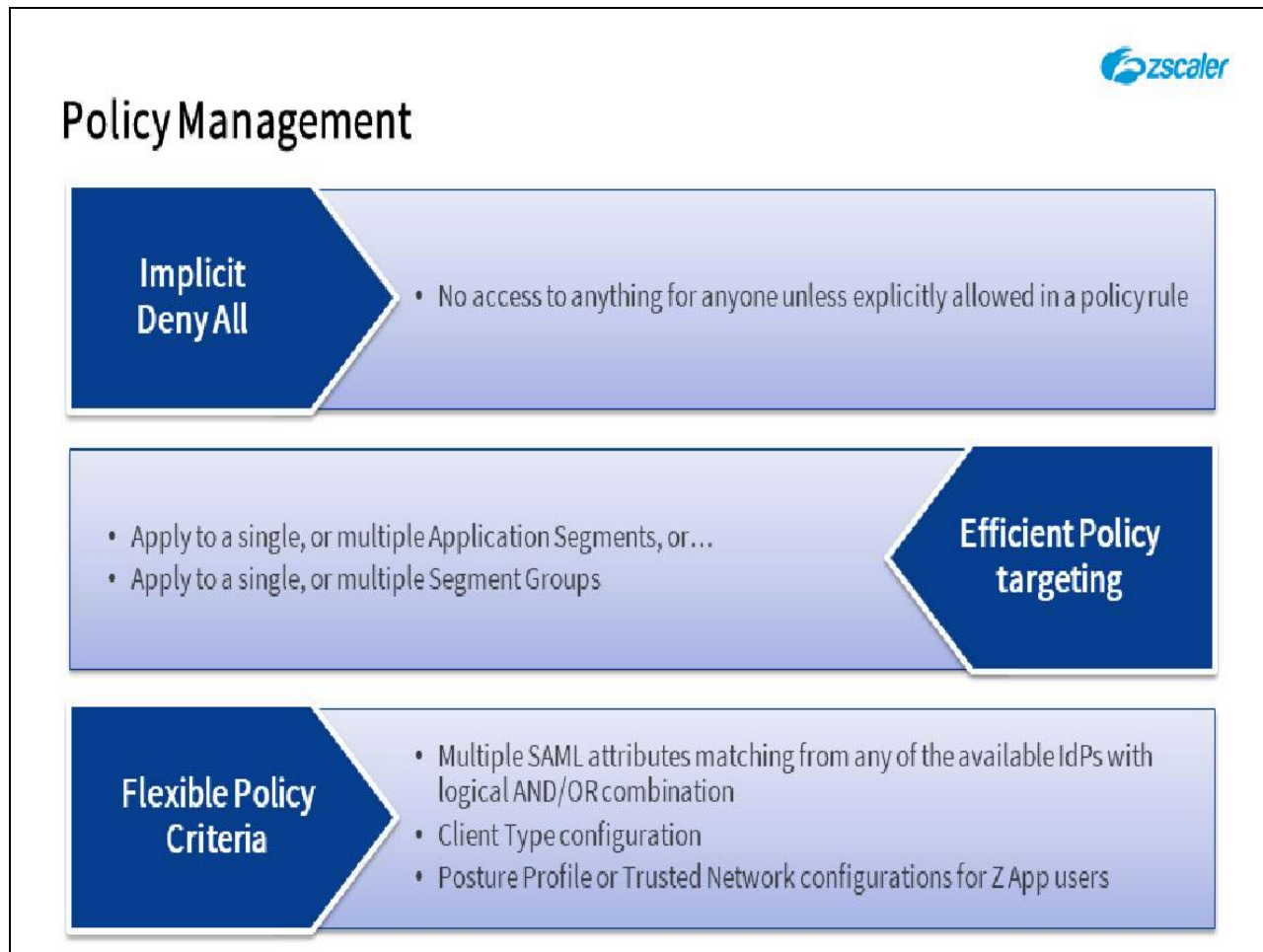
- Flexible mapping of Application Segments to Connector Groups
- Control what applications can be 'seen' and accessed
- Automatic best path selection
- Load balancing across applicable Connectors

Application Path Selection

Slide notes

- Plus, the service is always seeking to find the optimum path to an application instance for the end user.

Slide 40 - Policy Management



Slide notes

In terms of the access policy configuration options:

- The ZPA service will never grant anybody access to anything, unless there is an explicit allow policy;
- The policy rules may be targeted against individual applications, or logical groups of applications;
- There are multiple criteria available to refine the targeting of policy to particular users, groups of users, posture statuses or trusted network settings;

Slide 41 - Policy Management



Policy Management

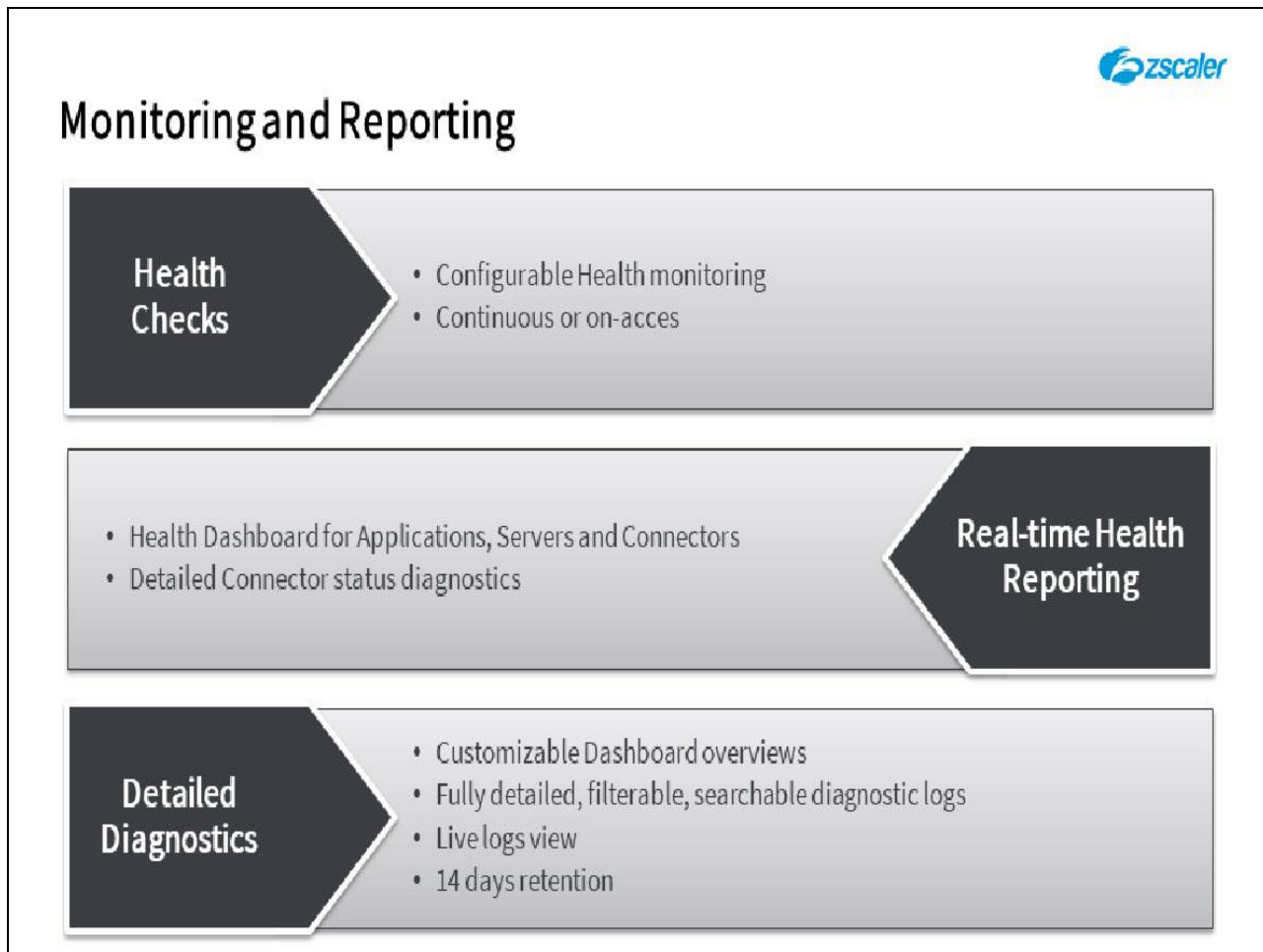
- Z App Posture Profile matching with logical AND/OR combination
- Z App Trusted Network matching with logical AND/OR combination

Logical Criteria Matching

Slide notes

- Plus, there are flexible, logical combination options for the available matching criteria.

Slide 42 - Monitoring and Reporting



Slide notes

In the area of monitoring and reporting:

- The service provides configurable infrastructure health checking;
- With real-time system-wide health reporting;
- Detailed diagnostics are available with a drill down capability;

Slide 43 - Monitoring and Reporting



The slide features the Zscaler logo in the top right corner. The main title 'Monitoring and Reporting' is positioned on the left. Below it, a light gray box contains a bulleted list of features, with a dark gray arrow pointing to the right containing the text 'Log Streaming Service (LSS)'. Below this, a dark gray arrow points to the left containing the text 'Executive Insights', which then points to a light gray box containing a bulleted list of features.

Monitoring and Reporting

- Customizable log streams to multiple destinations
- For longer term retention
- Utilize the ZPA infrastructure, ideally with dedicated Connectors

Log Streaming Service (LSS)

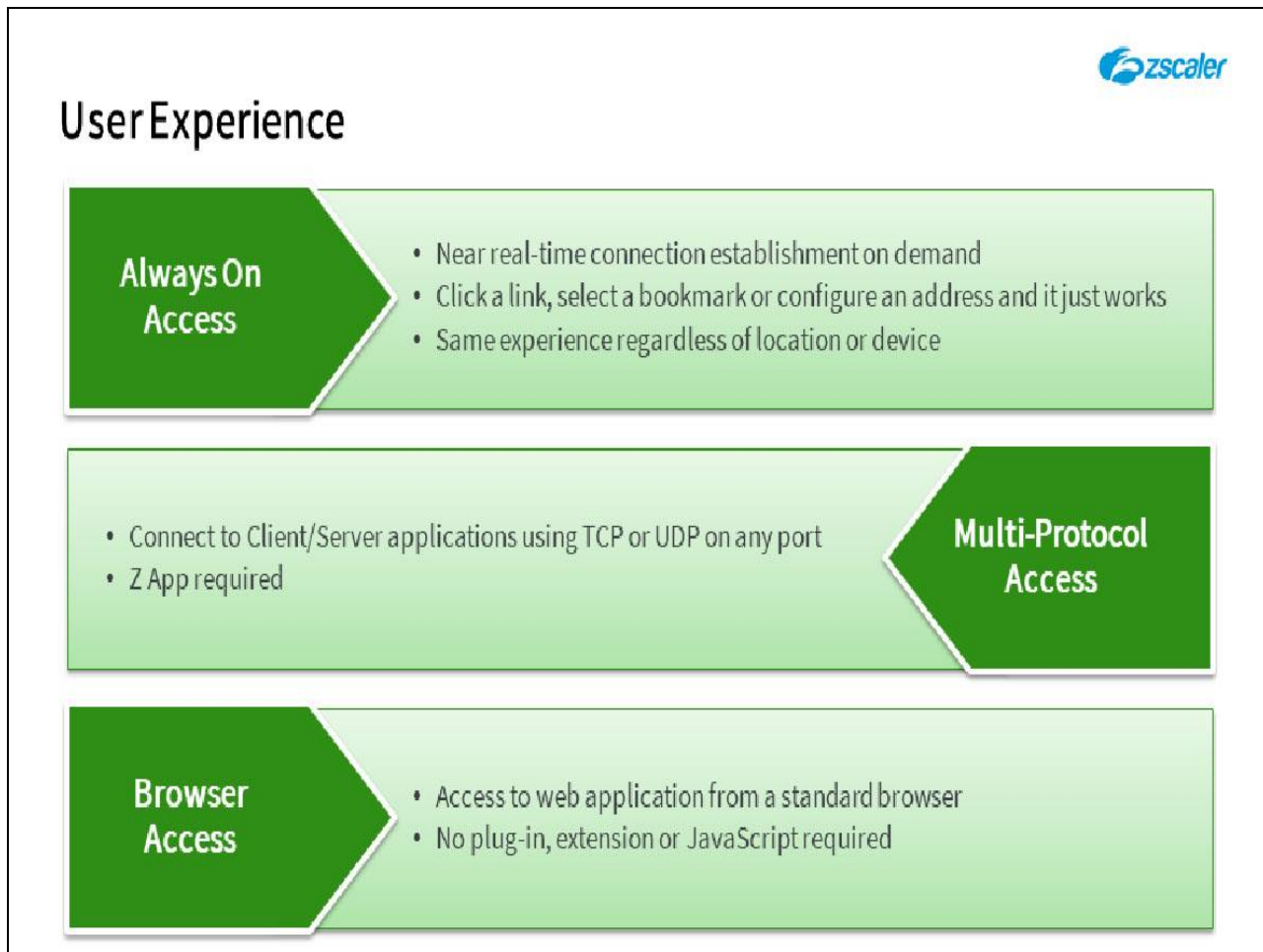
Executive Insights

- Summarized reports to provide platform performance highlights

Slide notes

- Logs are retained for 14 days, plus there is a log streaming service, to allow longer term retention;
- There is also the option to generate and send to targeted individuals a high-level 'Executive Insights' report.

Slide 44 - User Experience




Slide notes

From the end user perspective:

- The service is effectively 'always-on', all they need do is click on a link or bookmark to open the application;
- Connection to any TCP/UDP client/server application is fully supported with the Zscaler App, regardless of port;
- Plus, browser-based access is also available, for the situations where Z App is not suitable;

Slide 45 - User Experience



User Experience

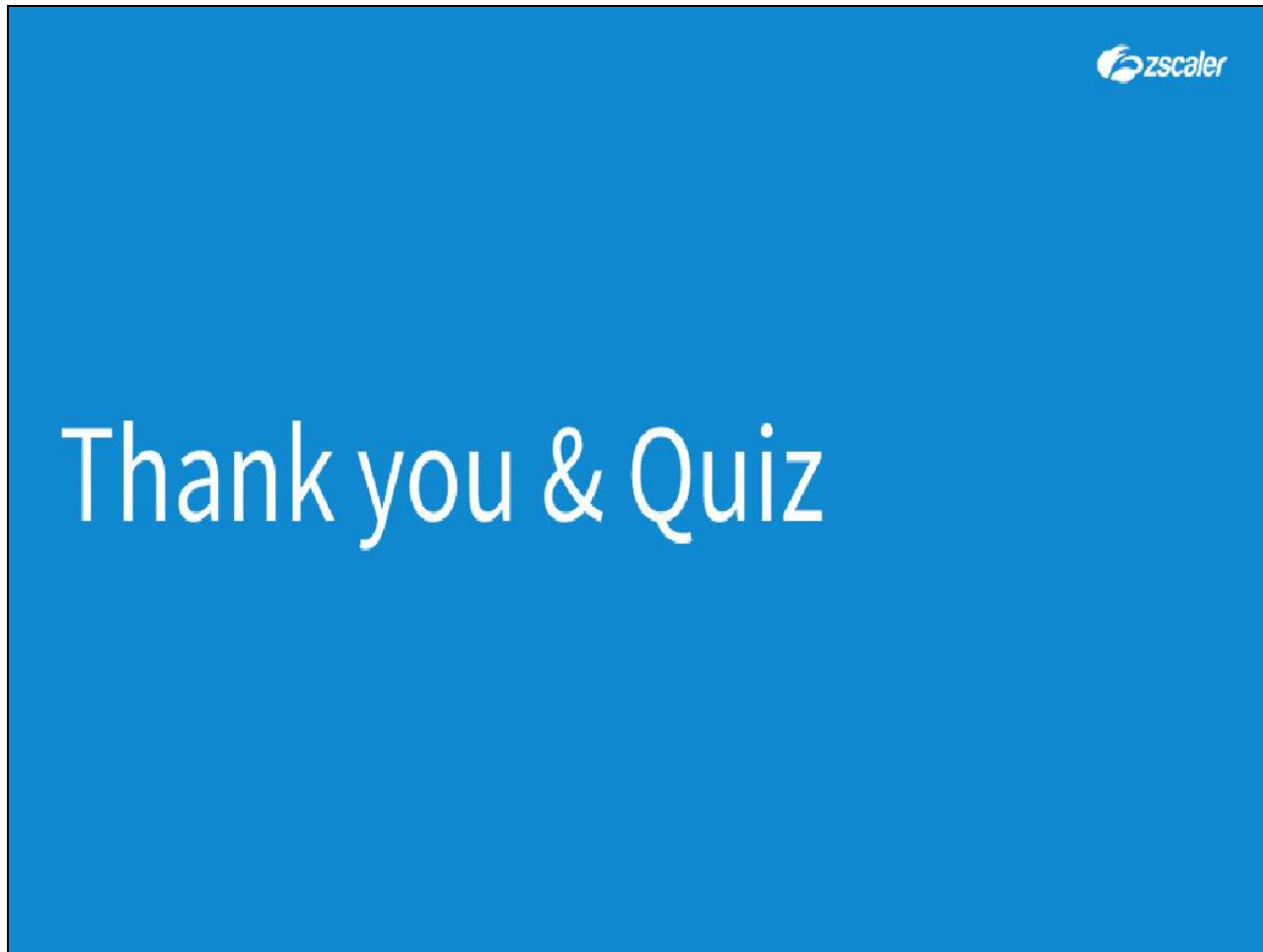
- Customizable End User Portal to catalog the available applications
- Categorize applications by client requirements (BA or Z App)
- Acceptable User Policy prior to access

Application Visibility

Slide notes

- Where necessary a customizable end-user portal can be created to advertise the availability of private applications.

Slide 46 - Thank you & Quiz



Slide notes

Thank you for following this Zscaler training module, we hope this module has been useful to you and thank you for your time.

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