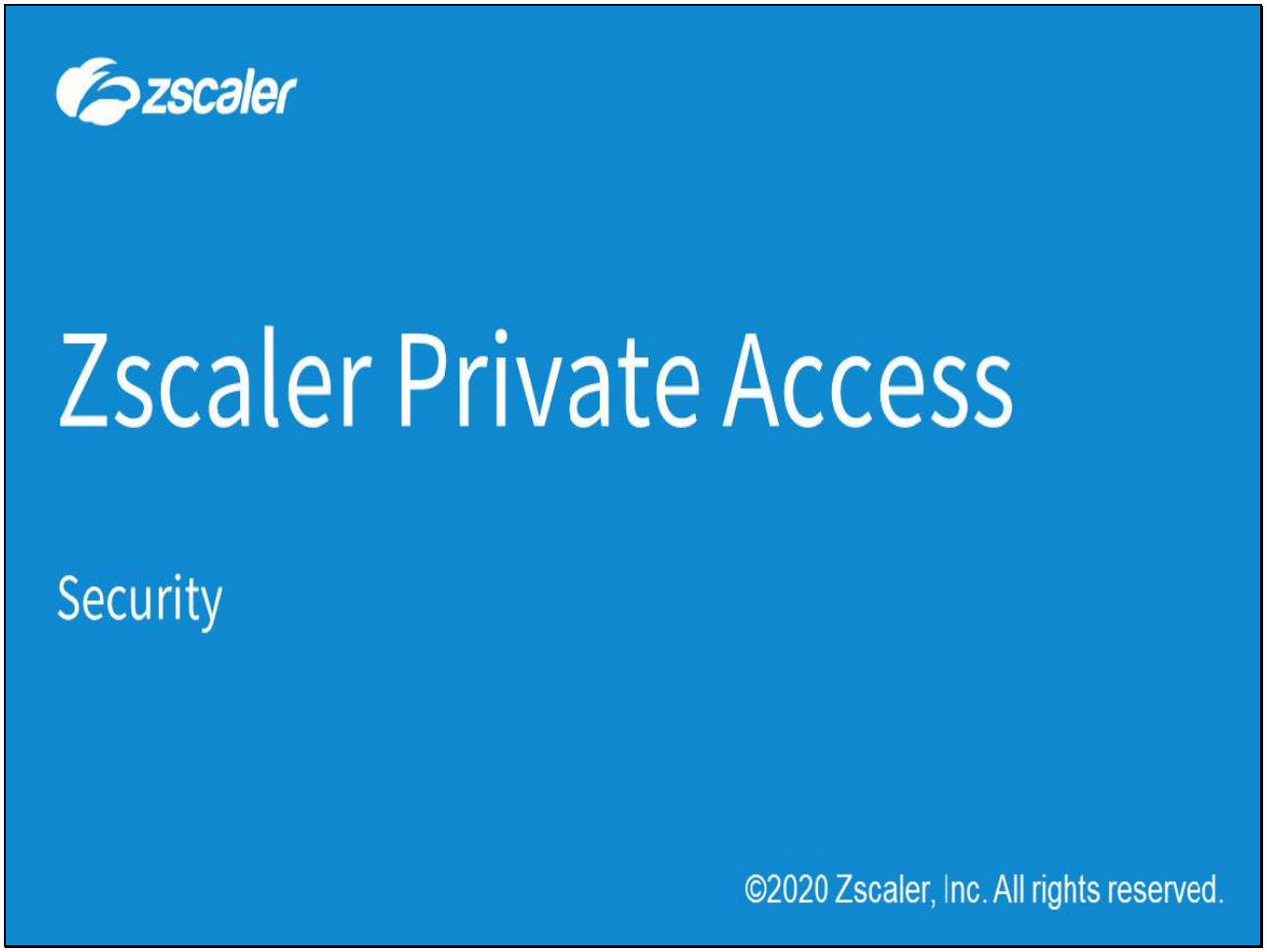
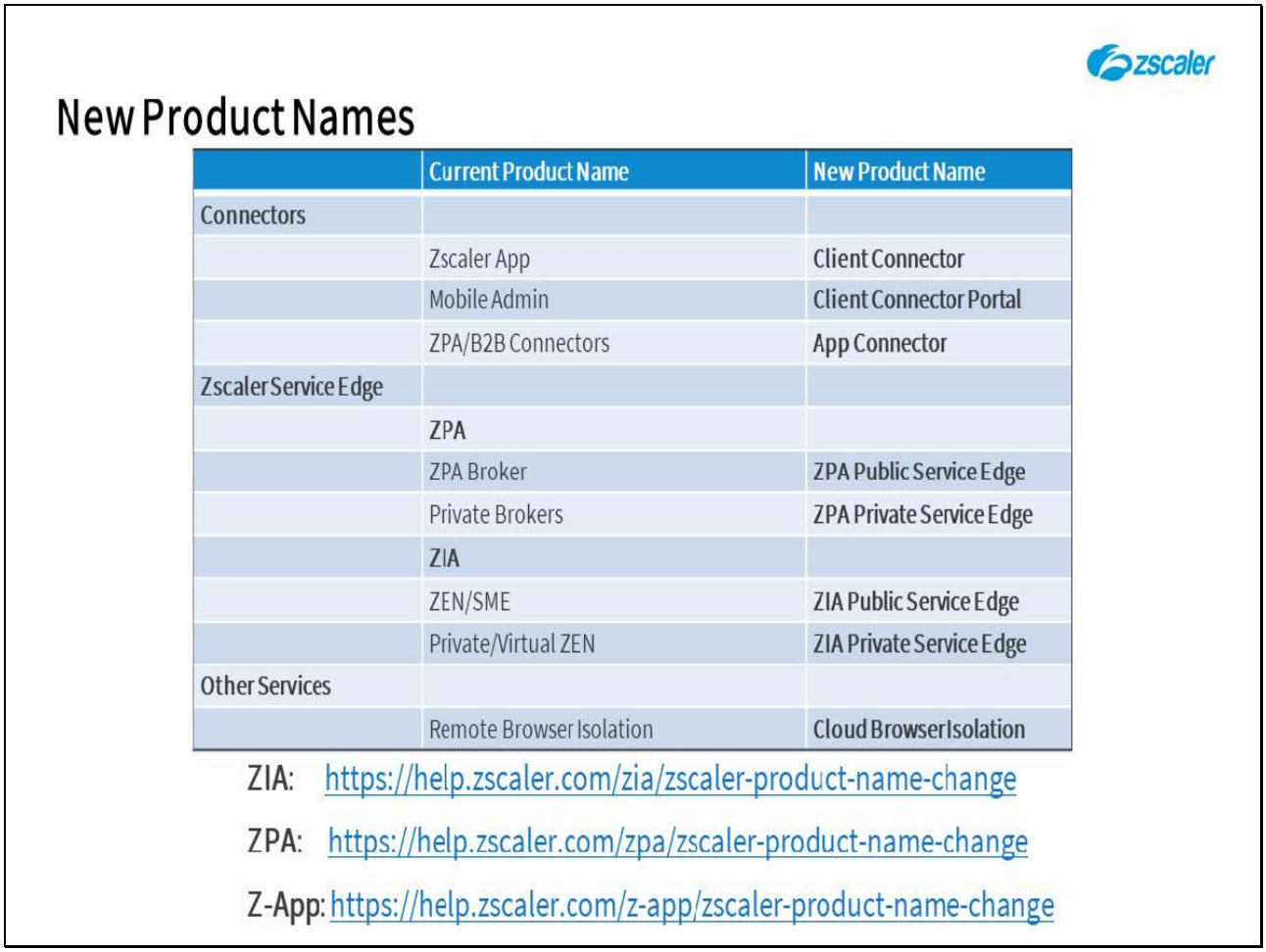
Slide 1 - Zscaler Private Access



Slide notes

Welcome to this training module on Zscaler Private Access security.

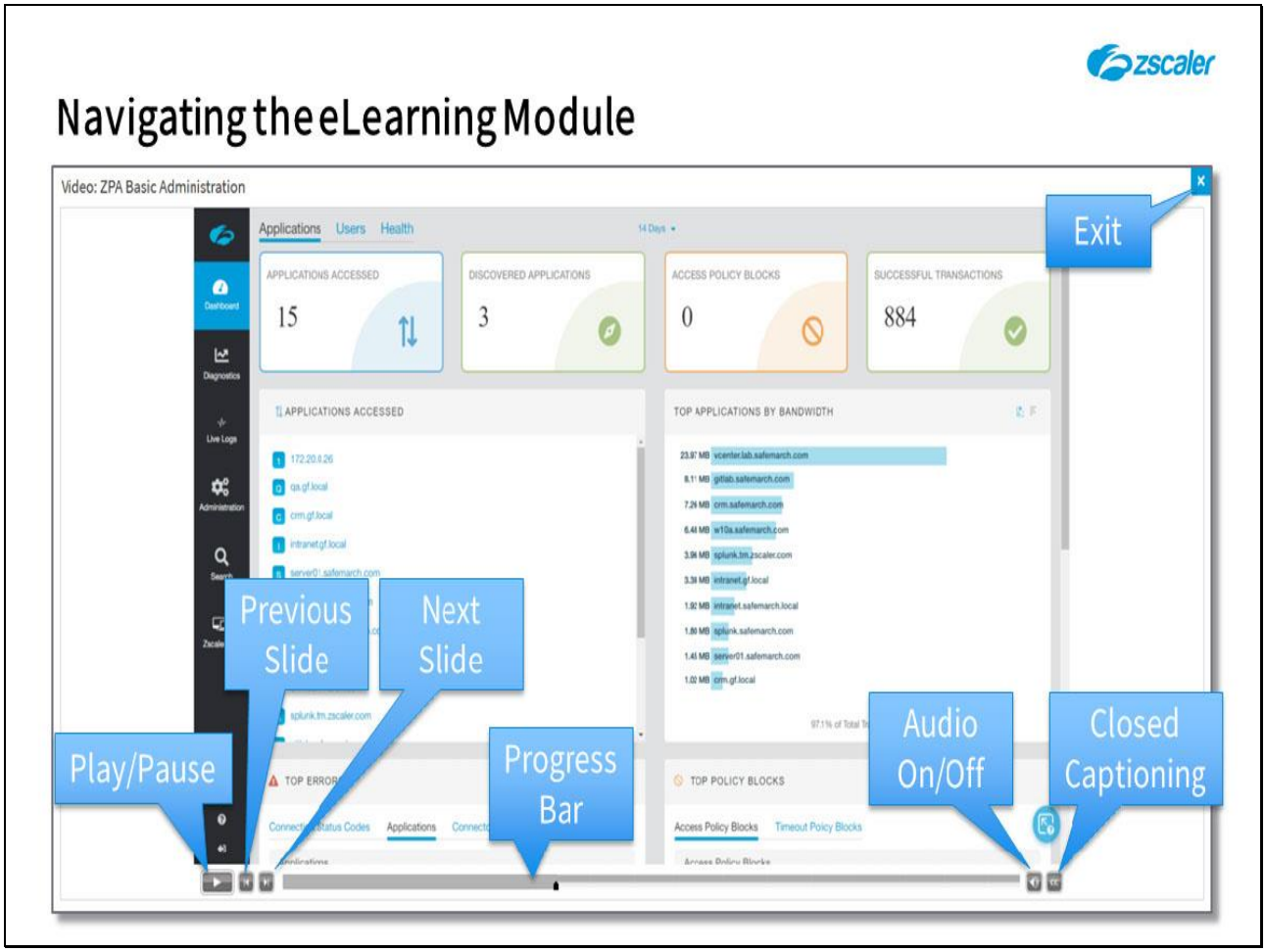
Slide 2 - New Product Names



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 3 - 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 4 - Agenda

Slide notes

In this module we will we will look at:

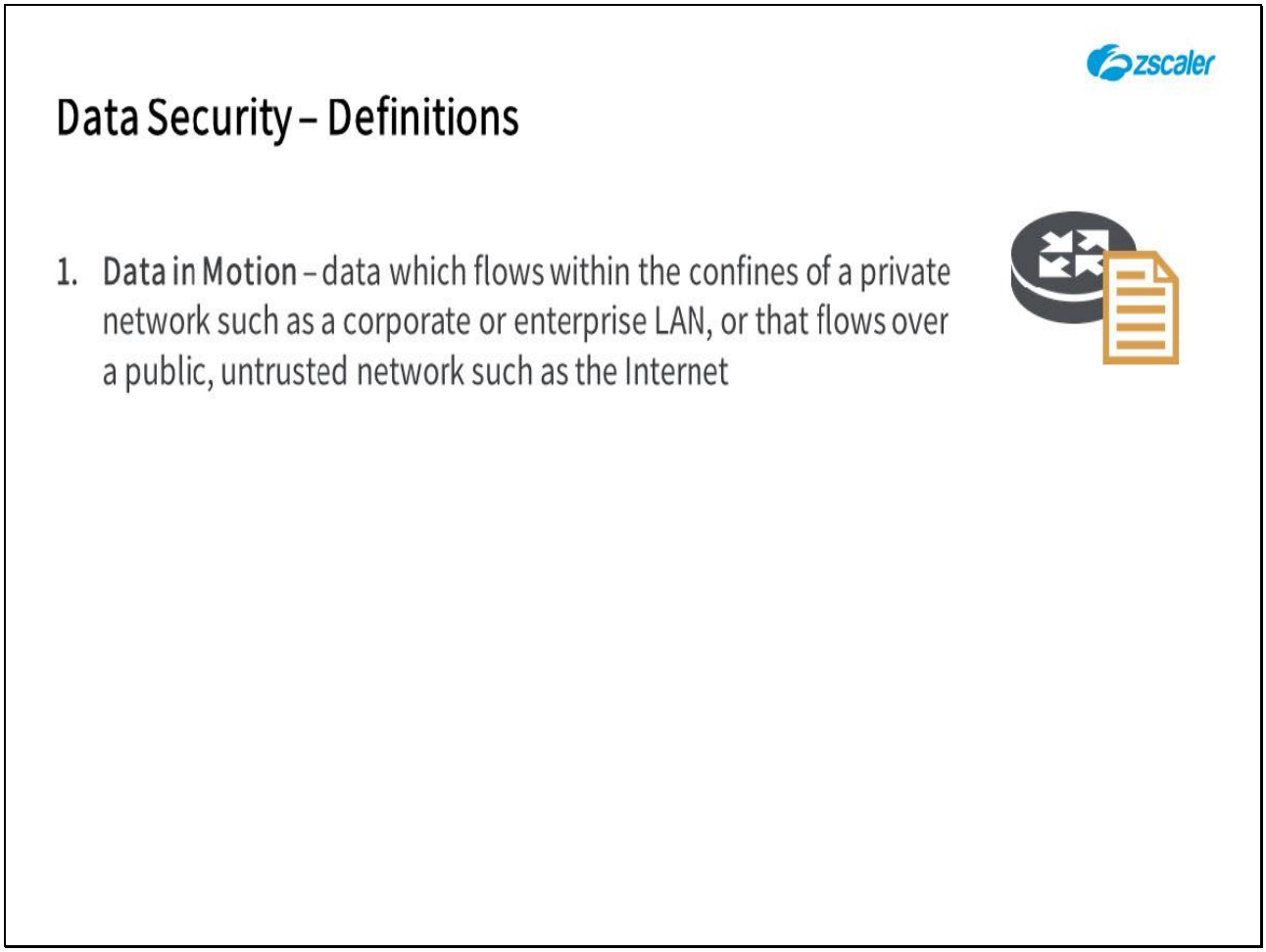
- The components of a comprehensive data security architecture;
- The ZPA user authentication process through the Zscaler Client Connector;
- The App Connector enrollment process;
- The protection of 'data in motion' using ZPA;
- The **Double Encryption** option for applications with 'Bring Your Own Encryption' (BYOE) certificates;
- And at the options for Source IP anchoring using ZPA.

Slide 5 - Data Security Components

Slide notes

Firstly, let’s look in general terms at the components of a comprehensive data security architecture.

Slide 6 - Data Security – Definitions



Slide notes

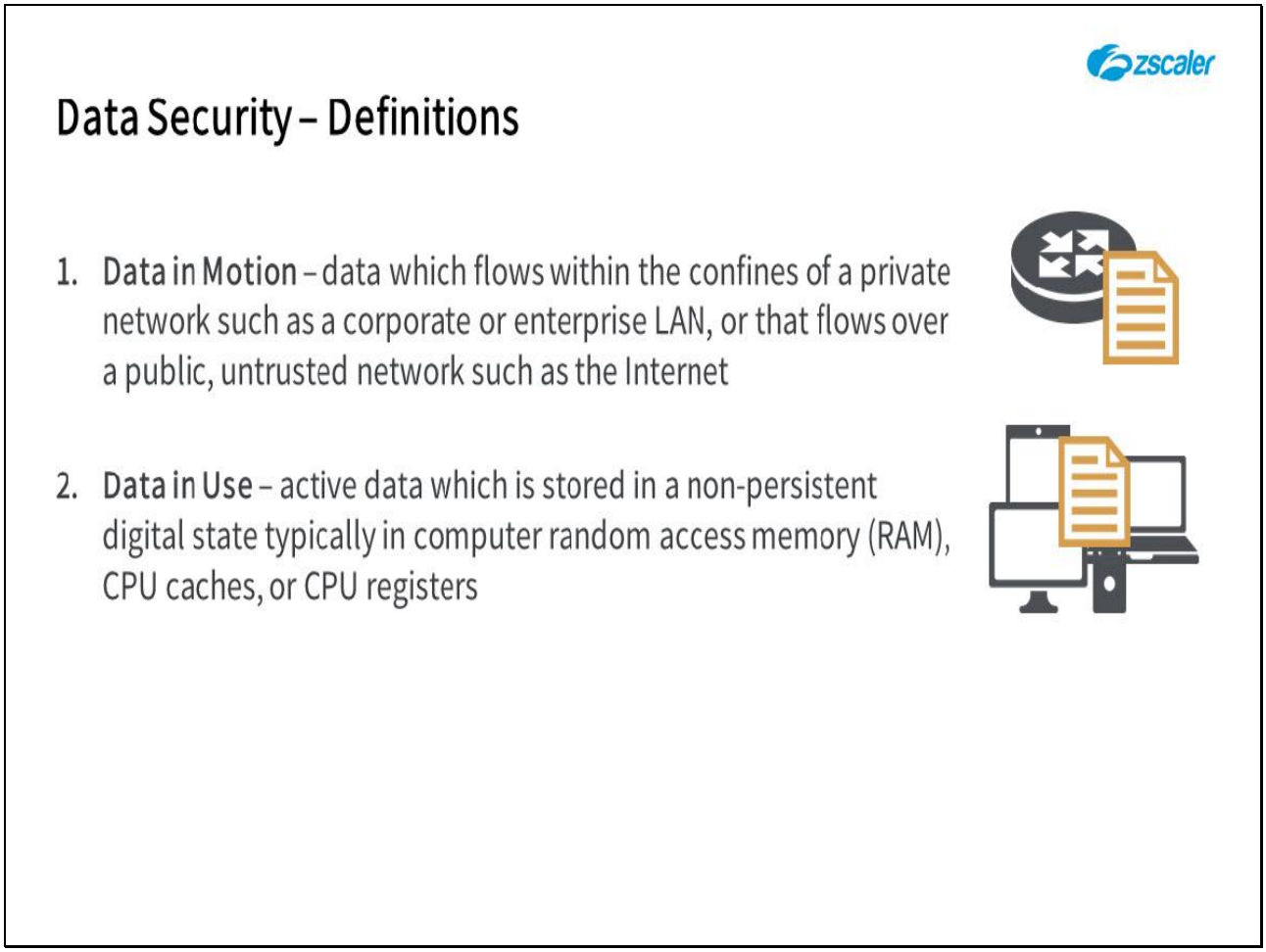
Your corporate data is one of your most valuable resources and every step possible must be taken to protect it from external and internal threats. Your data may comprise highly sensitive information, such as:

- Your own intellectual property (software algorithms or design data);
- The intellectual property of 3rd parties shared under NDA;
- Corporate legal and financial records;
- The personally identifiable information (PII) of your customers and/or employees (possibly including Social Security or Credit Card numbers);
- Passwords, encryption keys and digital certificates (which can give unrestricted access to other data).

The damage that can be caused to your organization through unauthorized access to, manipulation or deletion of this data can be incalculable.

Typically, the problem of securing corporate data is split into three main areas, the first being the protection of **Data in motion** (aka **Data in transit**), which is data that is in the process of being transferred between two or more locations, whether across some network connection or physical data bus. Data may be confined within a trusted private network segment (such as corporate LAN/WAN) or it may transit the untrusted public Internet. **Data in transit** between network nodes is potentially at its most vulnerable and the protection of data while it is in motion is essential.

Slide 7 - Data Security – Definitions



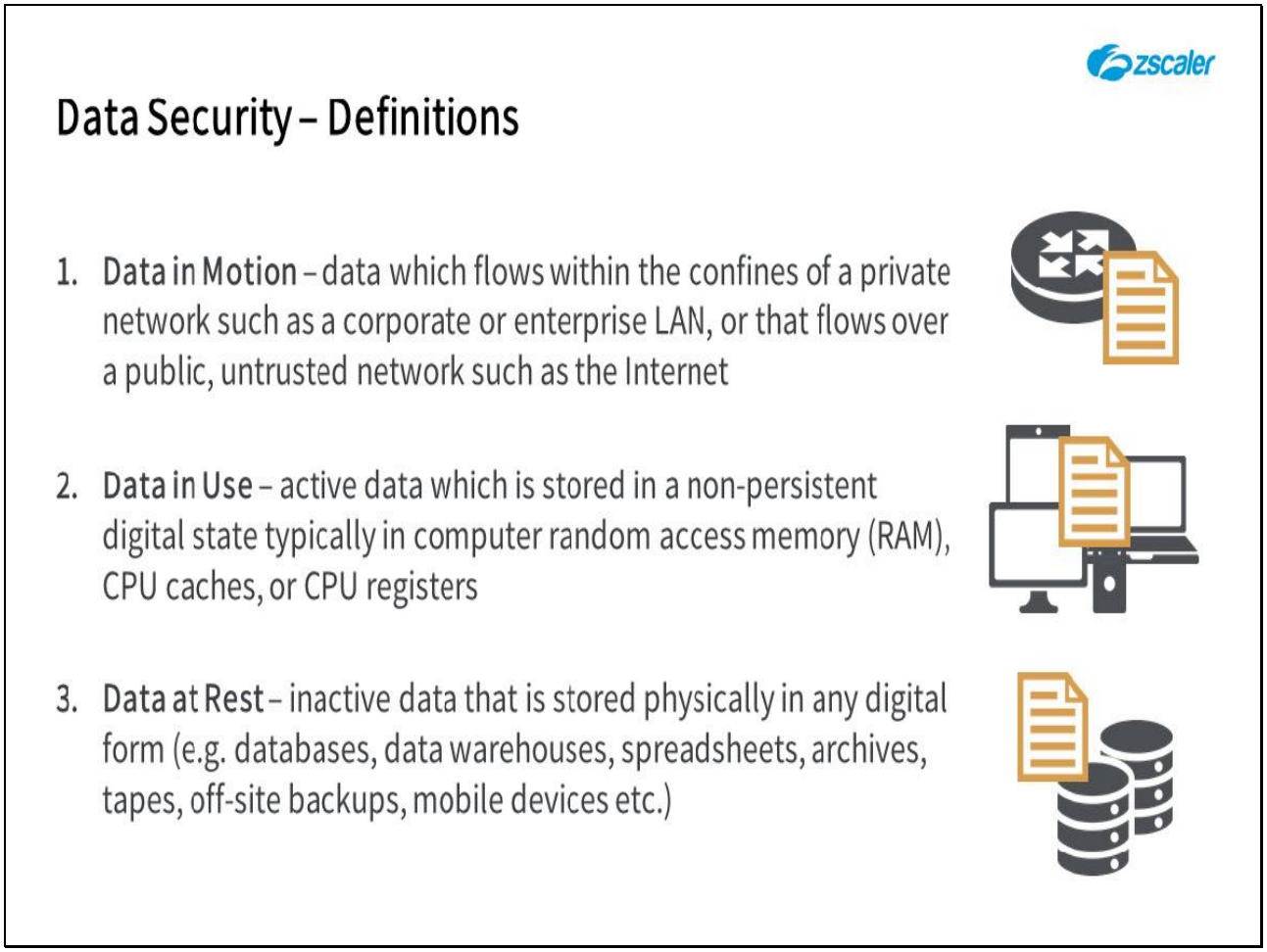
Slide notes

Data in use is considered to be active data stored in some form of non-persistent digital state, typically in computer RAM, CPU caches or CPU registers.

Data in use can contain sensitive data in its own right, such as intellectual property (software algorithms, design data) and personally identifiable information, or it may include data that can give wider access to **Data at rest**, including; digital certificates, encryption keys, or passwords.

Compromising **Data in use** can enable access to encrypted **Data at rest** and **Data in motion**.

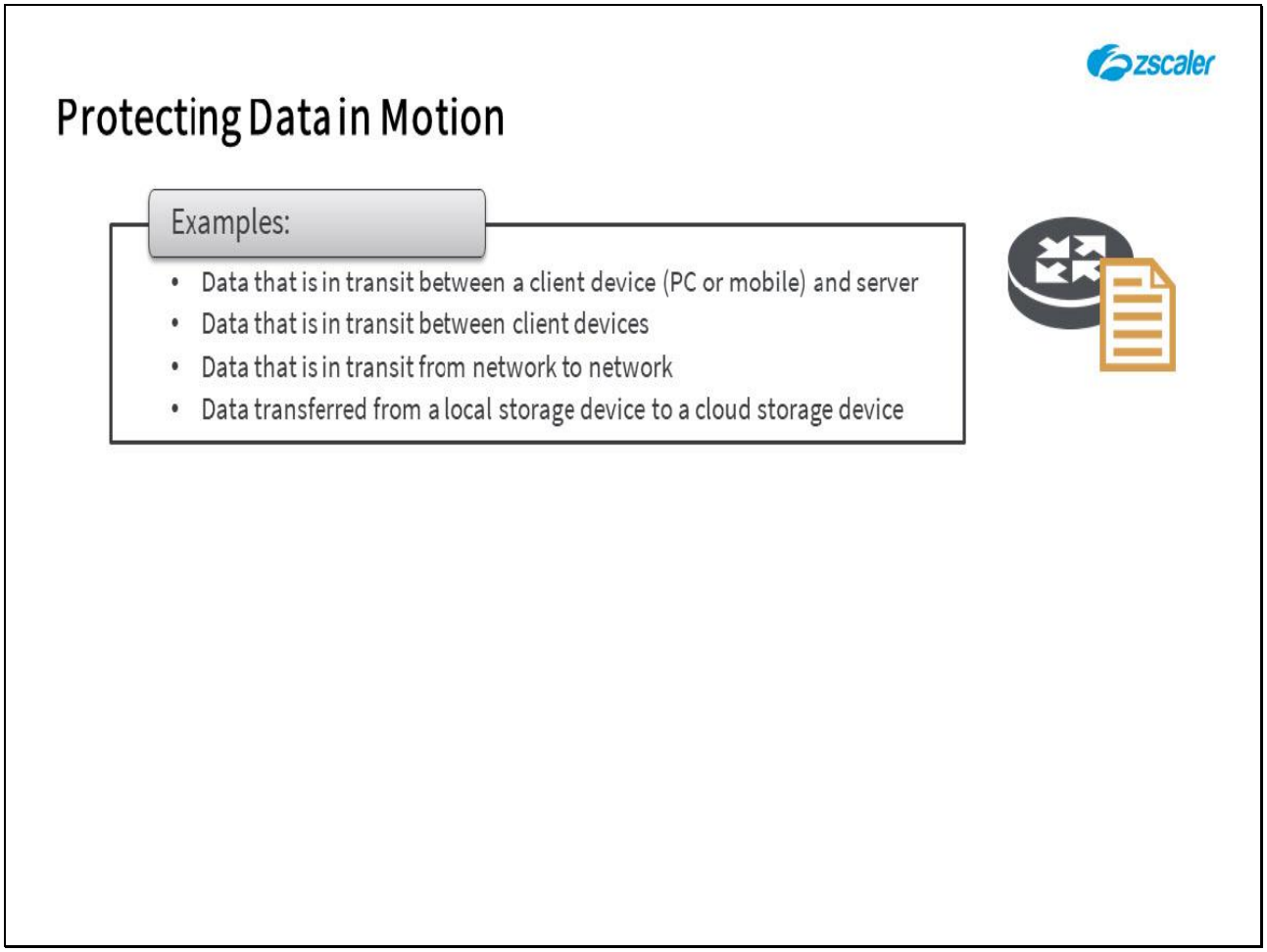
Slide 8 - Data Security – Definitions



Slide notes

Finally, **Data at rest** which is generally considered to be data that is static or inactive in nature, meaning that it is not being continually accessed or changed.

Slide 9 - Protecting Data in Motion

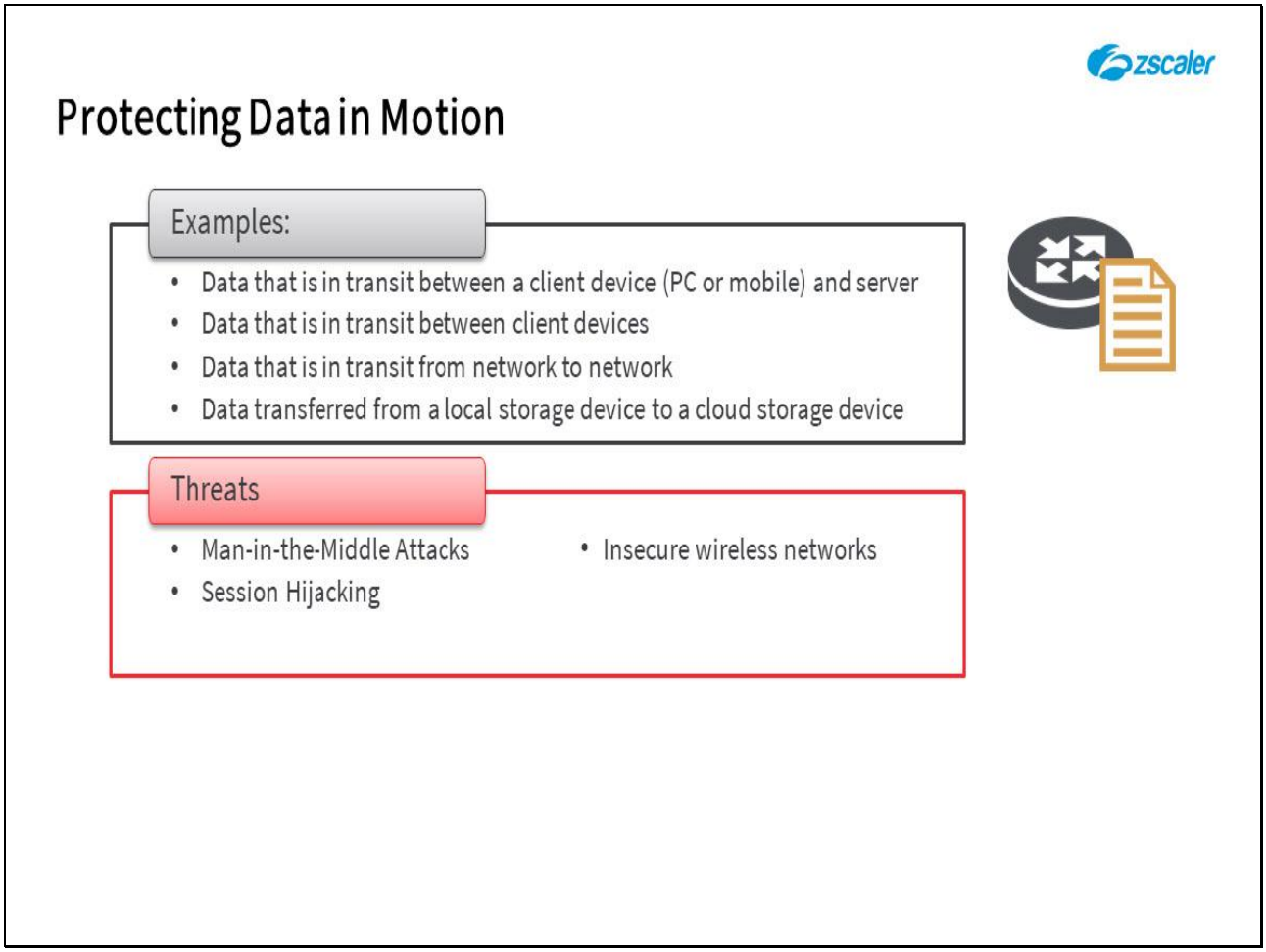


Slide notes

Data in motion can include:

- Data that is in transit between a client device (PC or mobile) and server;
- Data that is in transit between client devices;
- Data that is in transit from network to network;
- And data transferred from a local storage device to a Cloud storage device.

Slide 10 - Protecting Data in Motion

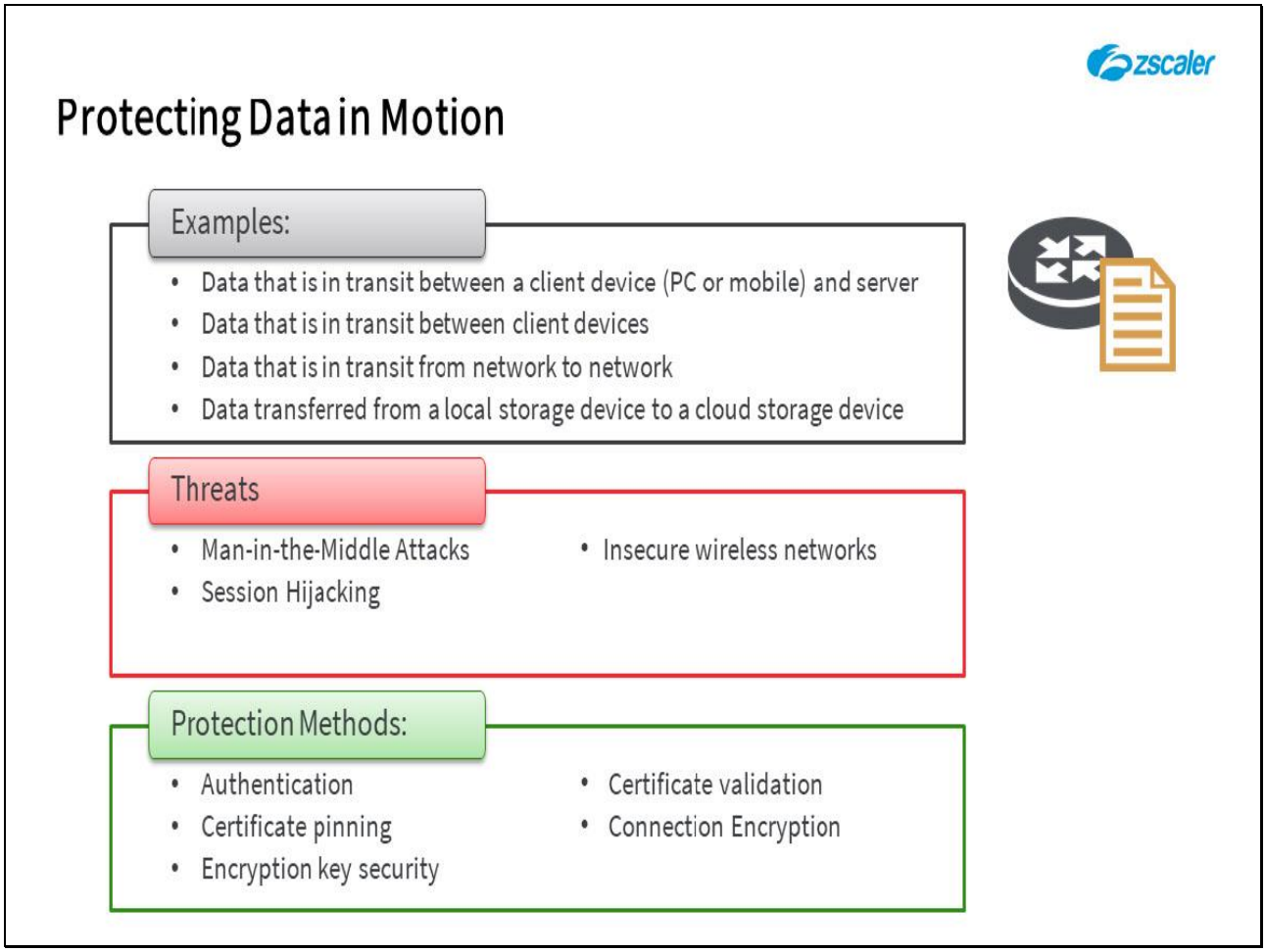


Slide notes

Data can be especially vulnerable to unauthorized interception while it is in transit and may be recovered or even manipulated through some form of 'man-in-the-middle' (MitM) attack or through session hijacking.

Typically, an attacker needs to insert themselves into the data path in order to mount an effective attack, which means that end users are particularly vulnerable when on the road and connecting across insecure public infrastructure.

Slide 11 - Protecting Data in Motion



Slide notes

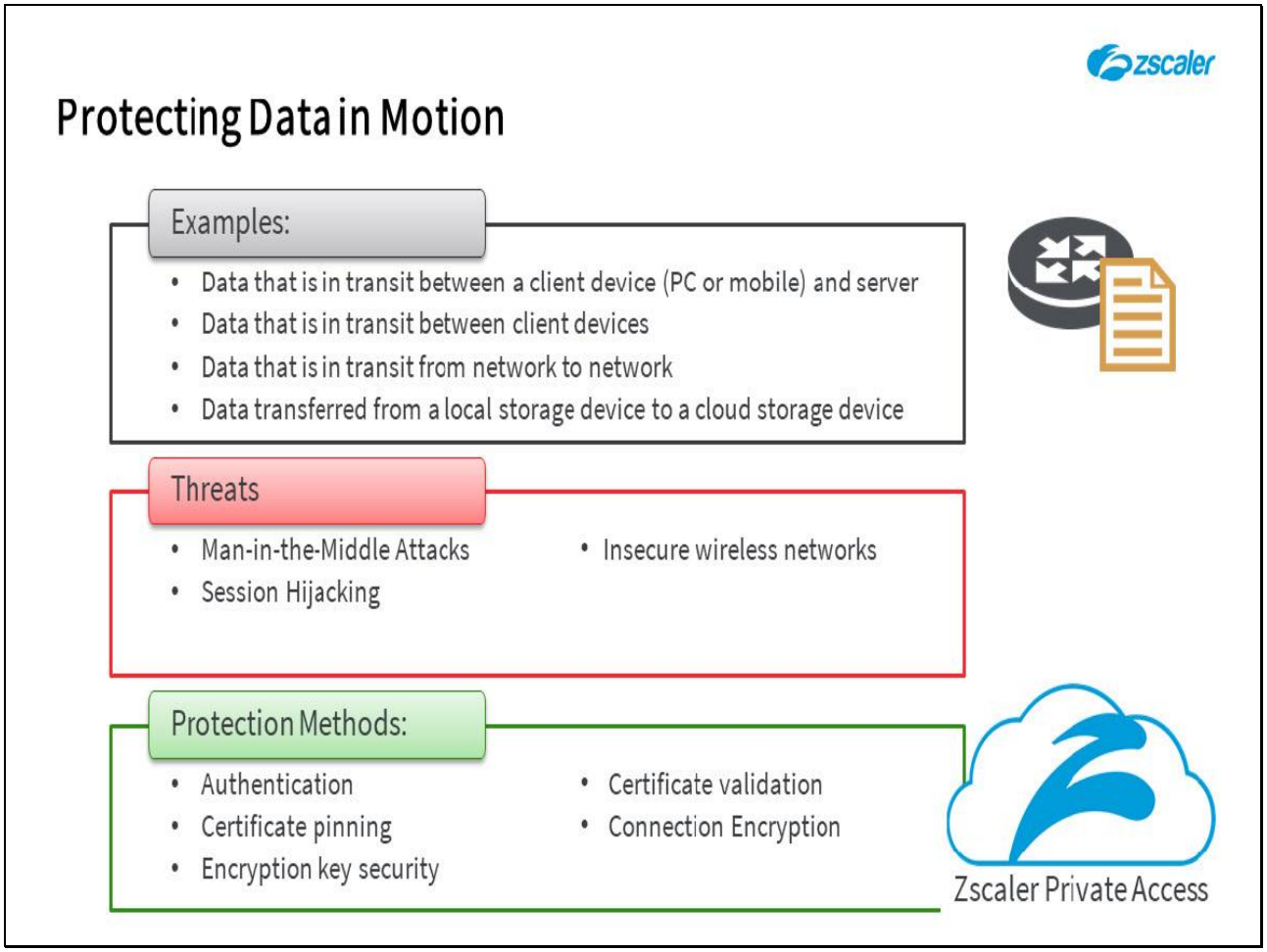
Authentication and encryption are the best tools to protect data while in motion and the IPSec, TLS and SSH standards have been developed to provide the necessary tools to manage this.

The implementation of a robust PKI infrastructure with mutual certificate validation is essential to ensure data is exchanged between trusted end points. Data can subsequently be encrypted end-to-end to ensure protection while in transit.

Certificate pinning may be used to enforce a stricter level of trust and prevent the establishment of a connection if a specific public key is not present during certificate validation.

A PKI infrastructure is only as secure as the keys used to initialize it, so correct key management and rotation is essential to prevent exposure of the private keys that the trust depends upon.

Slide 12 - Protecting Data in Motion

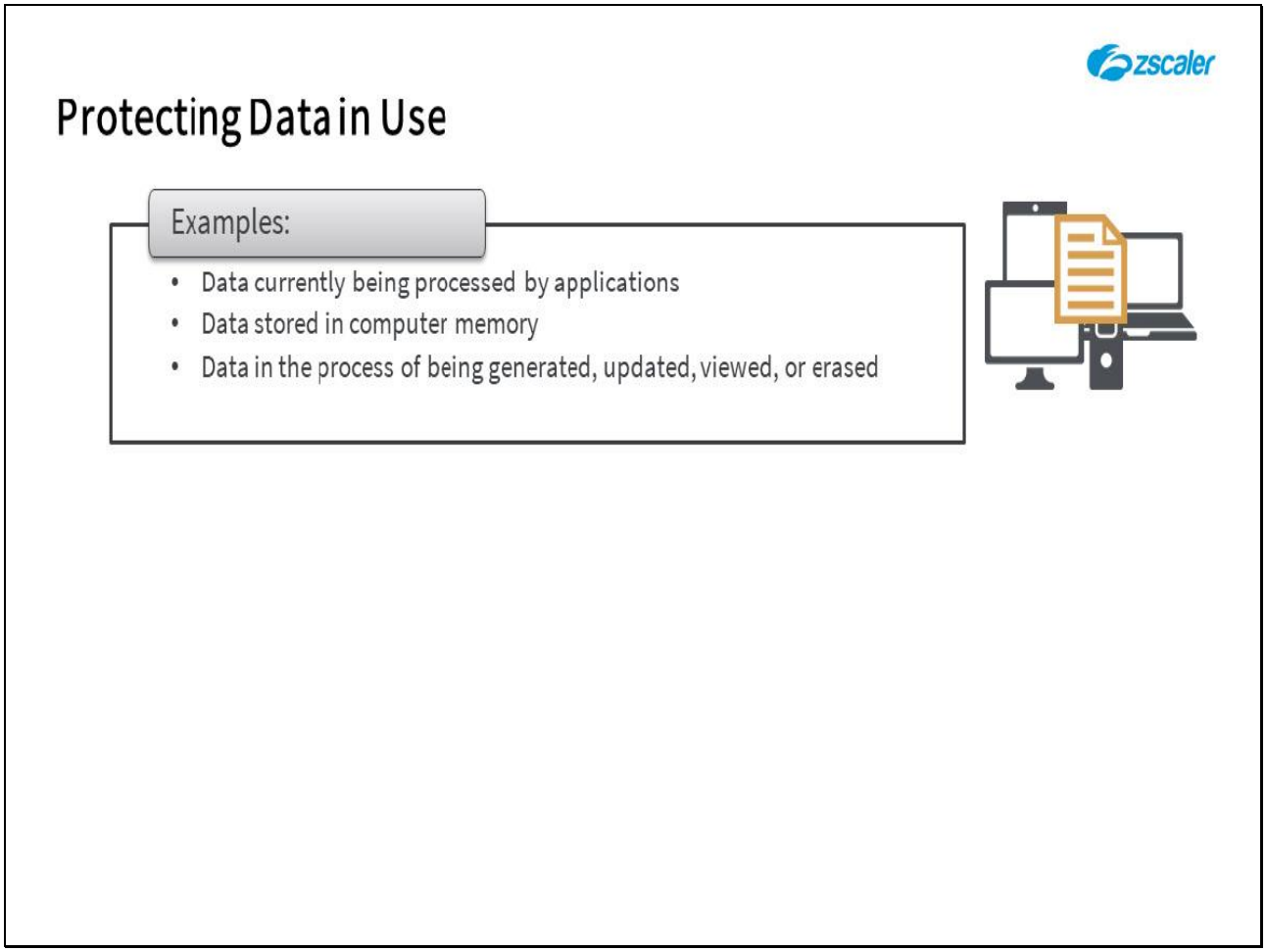


Slide notes

The protection of corporate **Data in motion** is what the Zscaler's Private Access service was developed for and it employs all of these techniques to prevent any exposure of customer data in transit across the Zscaler infrastructure, including any exposure to Zscaler if that is required.

End points are robustly authenticated using industry best practices, connections are only ever established following mutual certificate validation with pinning and connections are always encrypted with the strongest possible ciphers. Industry best practices are always followed for private key security and keys may be revoked at any time.

Slide 13 - Protecting Data in Use

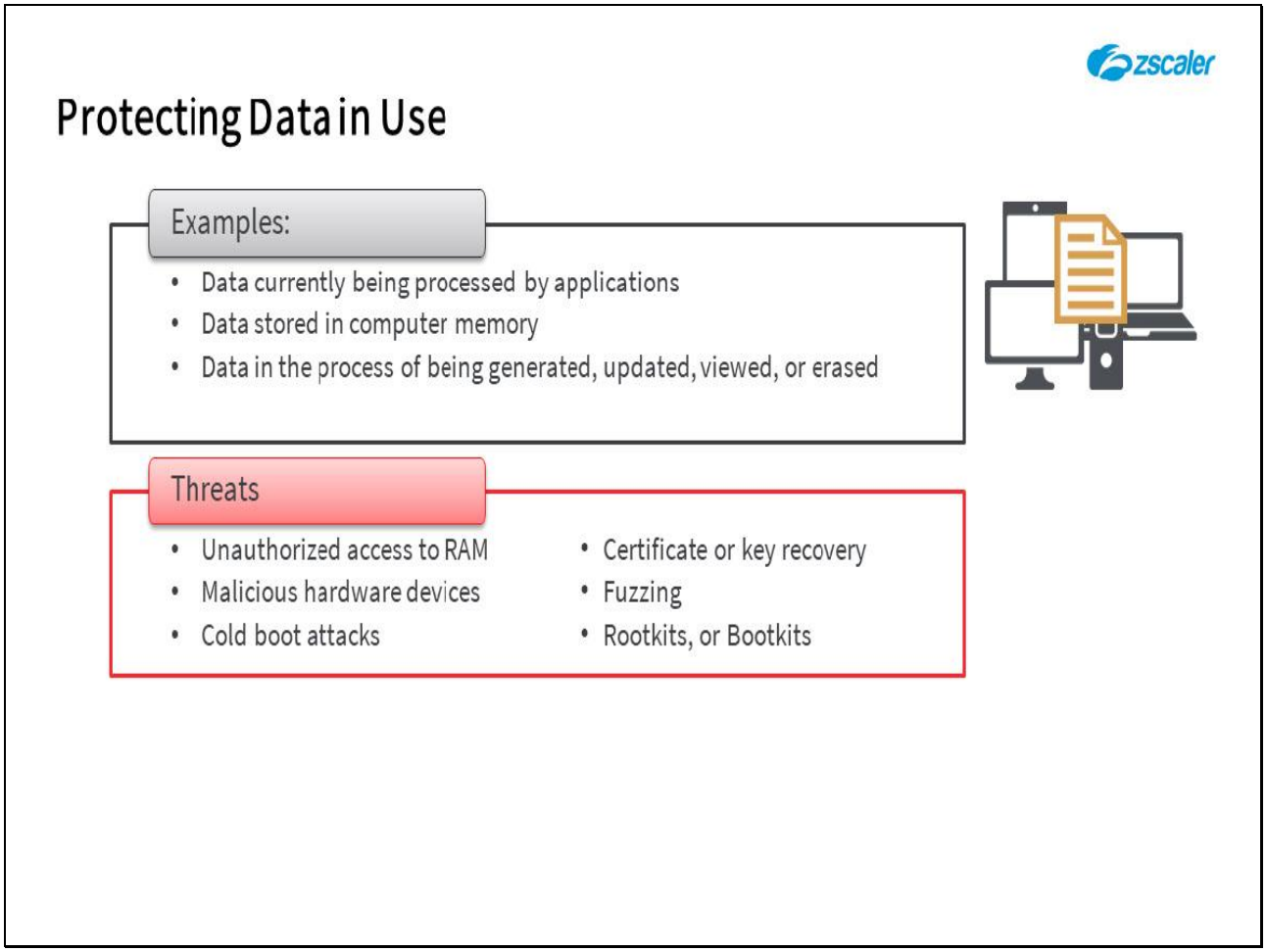


Slide notes

Data in use can include:

- Data currently being processed by applications;
- Data stored in computer memory;
- Or data in the process of being generated, updated, viewed or erased.

Slide 14 - Protecting Data in Use



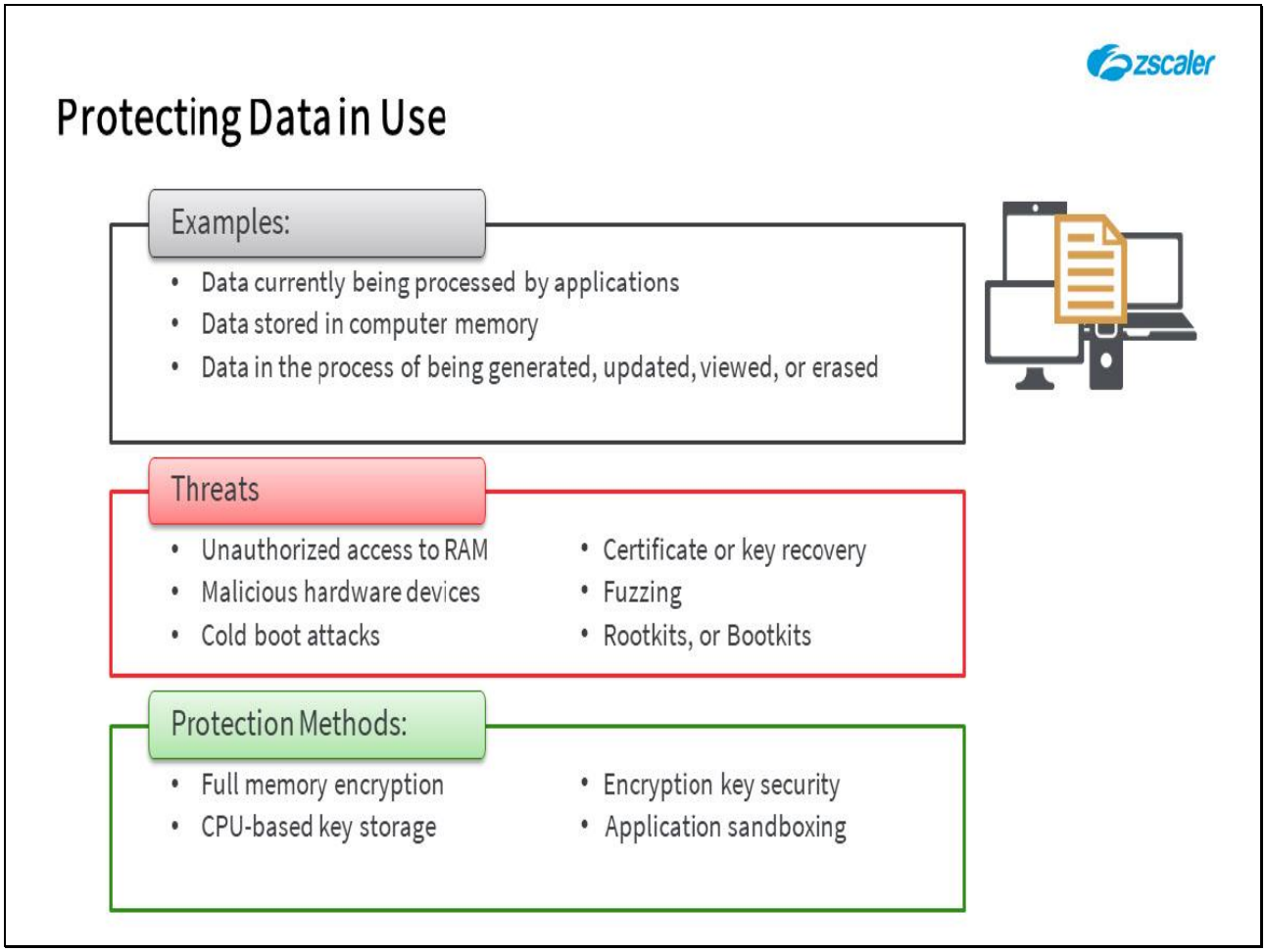
Slide notes

Data in use is in some ways less vulnerable to theft or manipulation, however given physical access to a system, unauthorized access to data in memory is certainly possible.

If a malicious intruder can gain access to the hardware itself to install hardware or some form of 'Root Kit' or 'Boot Kit', then access to data in memory is trivial. If not, there are still remote recovery options such as 'Fuzzing' (sending invalid packets or input to cause a system to crash or expose data) or by triggering a cold boot to gain access during the device restart process.

Significantly, these techniques can also potentially be used to recover certificates or encryption keys that then give access to data elsewhere within the organization (at rest or in motion).

Slide 15 - Protecting Data in Use

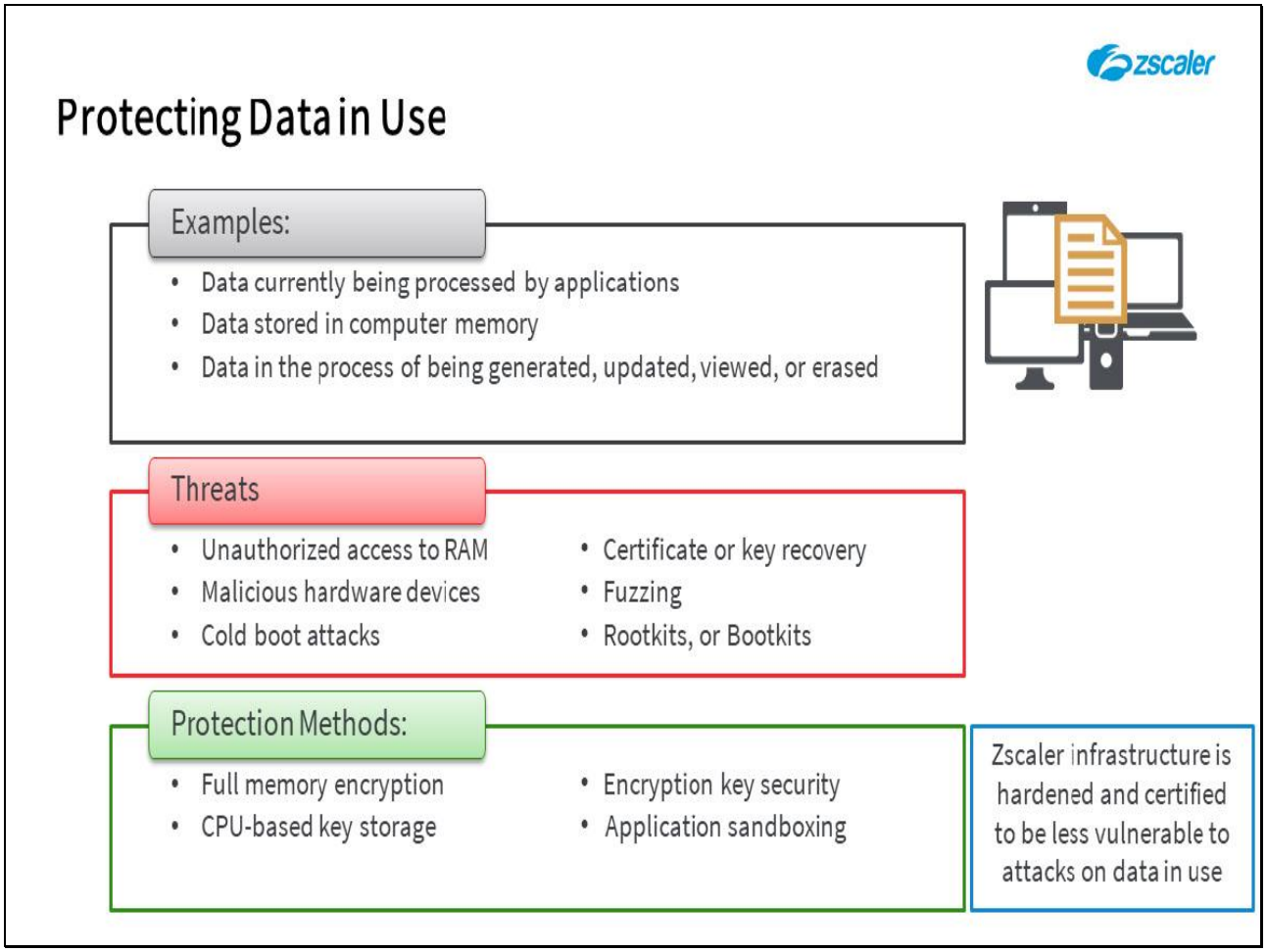


Slide notes

Protective measures for **Data in use** include the option to encrypt memory, although as always you would also need to protect the encryption keys, for which CPU-based key storage may be suitable (such as TRESOR).

A common way to prevent application data leaking used in modern OS's is to sandbox them and restrict the exchange of data between application sandboxes.

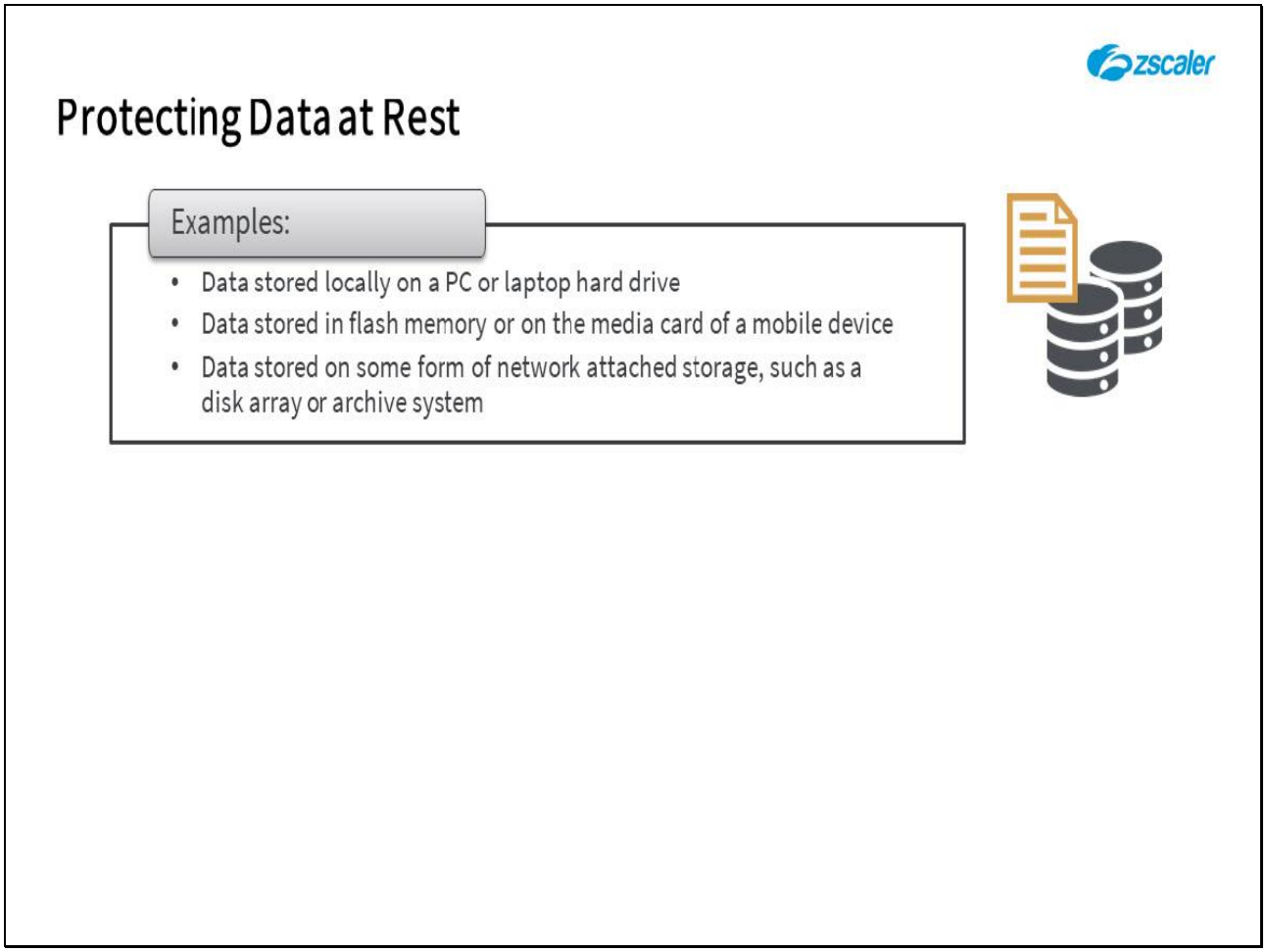
Slide 16 - Protecting Data in Use



Slide notes

All Zscaler infrastructure components are hosted in ISO and SOC 2 certified data centers that restrict unauthorized physical access. Our services undergo regular penetration testing to identify potential vulnerabilities that might expose customer data in use as it transits our infrastructure.

Slide 17 - Protecting Data at Rest

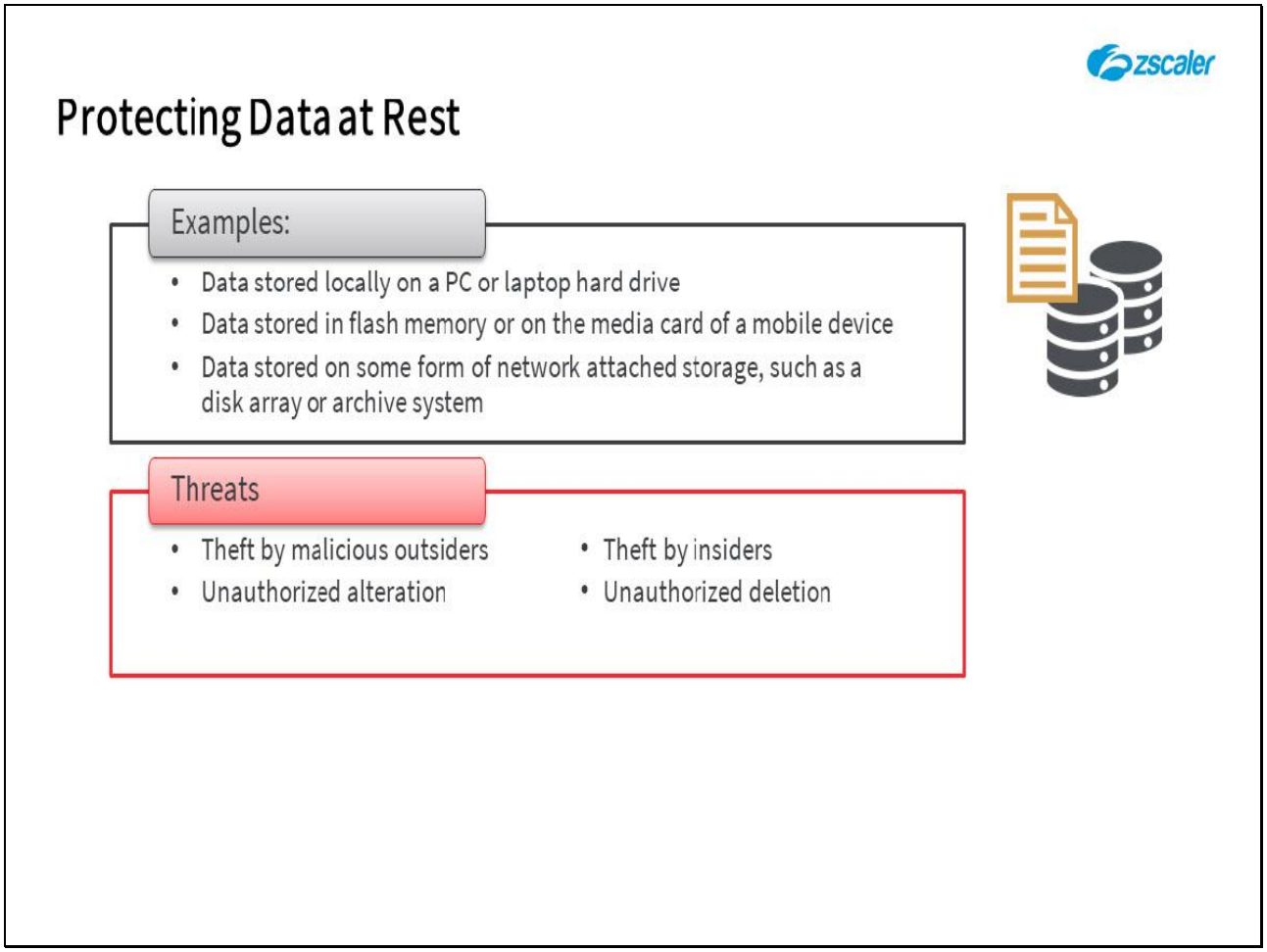


Slide notes

Data at rest can include:

- Data saved to the hard drives of your employee's computers;
- Data stored by servers in databases, spreadsheets or data warehouses;
- Data saved to a network attached storage or archive system;
- Or even data saved on your employee's mobile devices (in flash memory or on media cards).

Slide 18 - Protecting Data at Rest

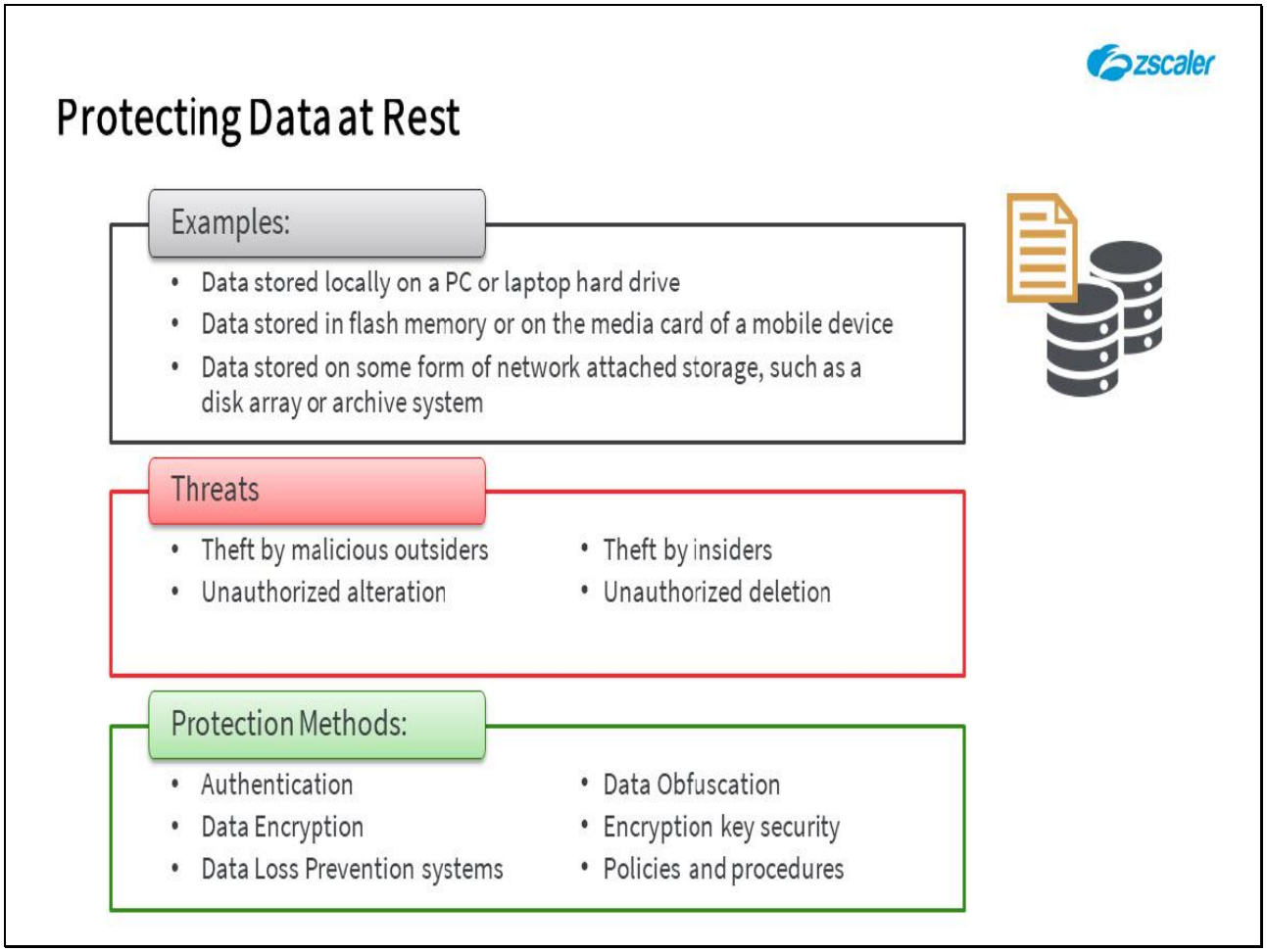


Slide notes

Protecting data while it is at rest is a fundamental IT security task and data must be protected both from external and internal threats.

Data at rest is sometimes considered less vulnerable to unauthorized access than **Data in transit**, although because of its volume it may be a more valuable target than data in motion. **Data at rest** must be protected from theft, alteration or deletion by unauthorized intruders and disgruntled or criminal insiders.

Slide 19 - Protecting Data at Rest



Slide notes

Protecting **Data at rest** requires the prevention of unauthorized access to data stored on a device or network resource through the use of some form of authentication.

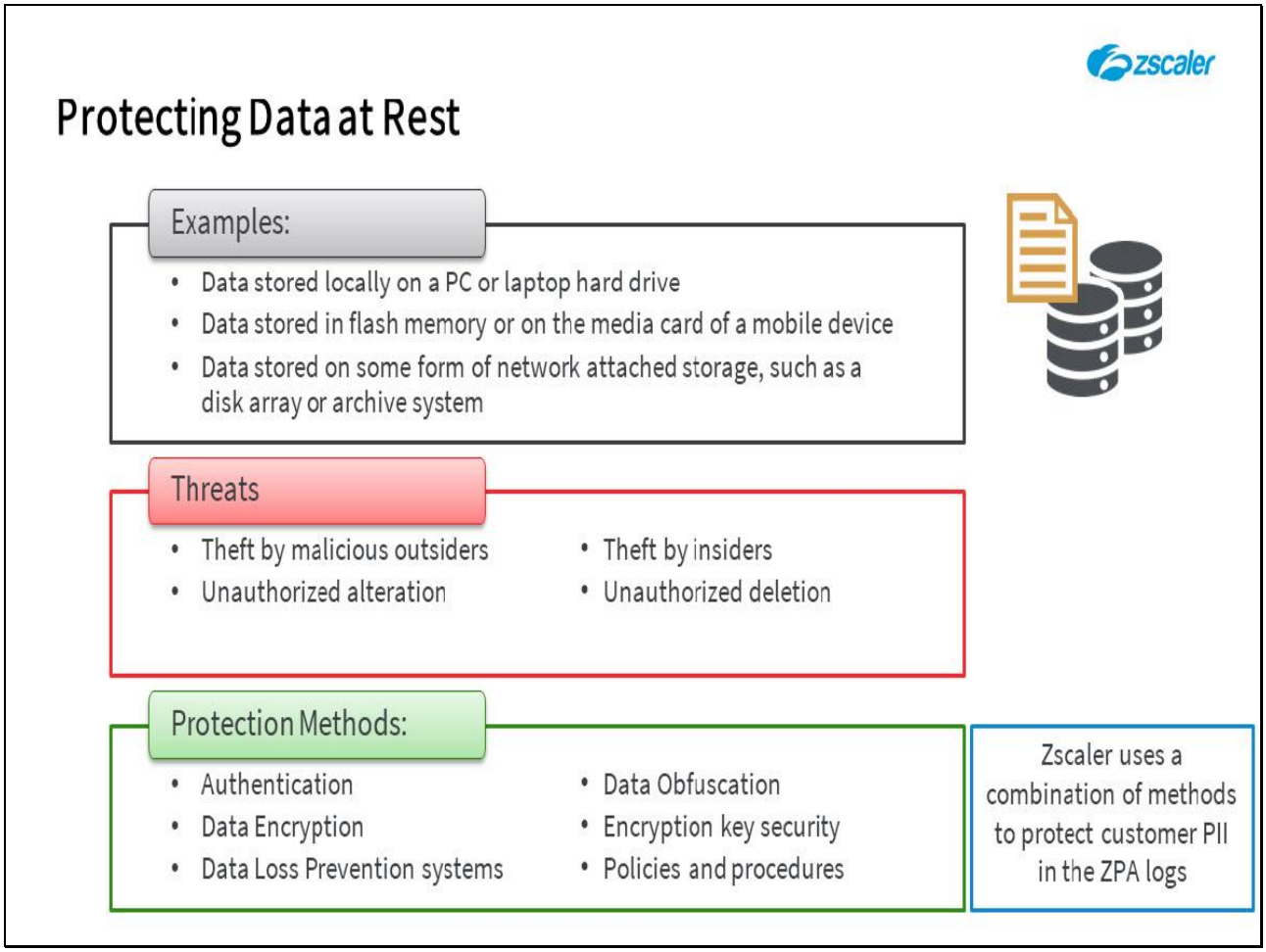
Data written to long term storage may be obfuscated in some way to remove meaningful context, the data is only meaningful when viewed using a particular application or when paired with another data set that provides the necessary context.

Data at rest may also be encrypted, although access to the encryption keys must then also be protected.

Data Loss Prevention systems may be used to actively detect or prevent the unauthorized exfiltration of data from a network or device.

Policies and procedures should be developed, implemented and communicated to ensure the protection of key data resources.

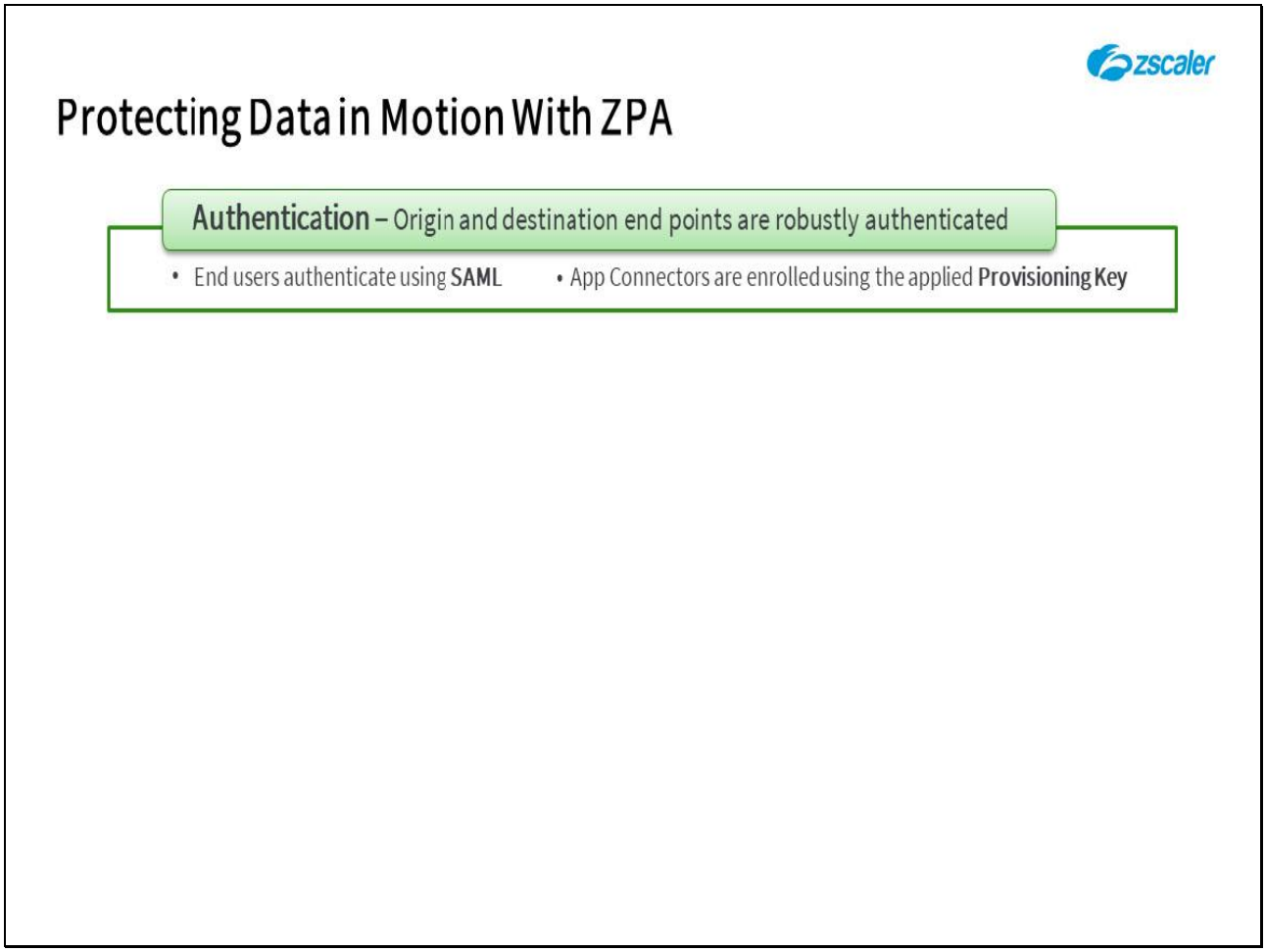
Slide 20 - Protecting Data at Rest



Slide notes

The protection of corporate **Data at rest** is beyond the scope of Zscaler's Private Access service, although Zscaler uses some of these techniques (authentication, obfuscation and encryption) to protect customer PII in any log data stored within the ZPA infrastructure.

Slide 21 - Protecting Data in Motion With ZPA



Slide notes

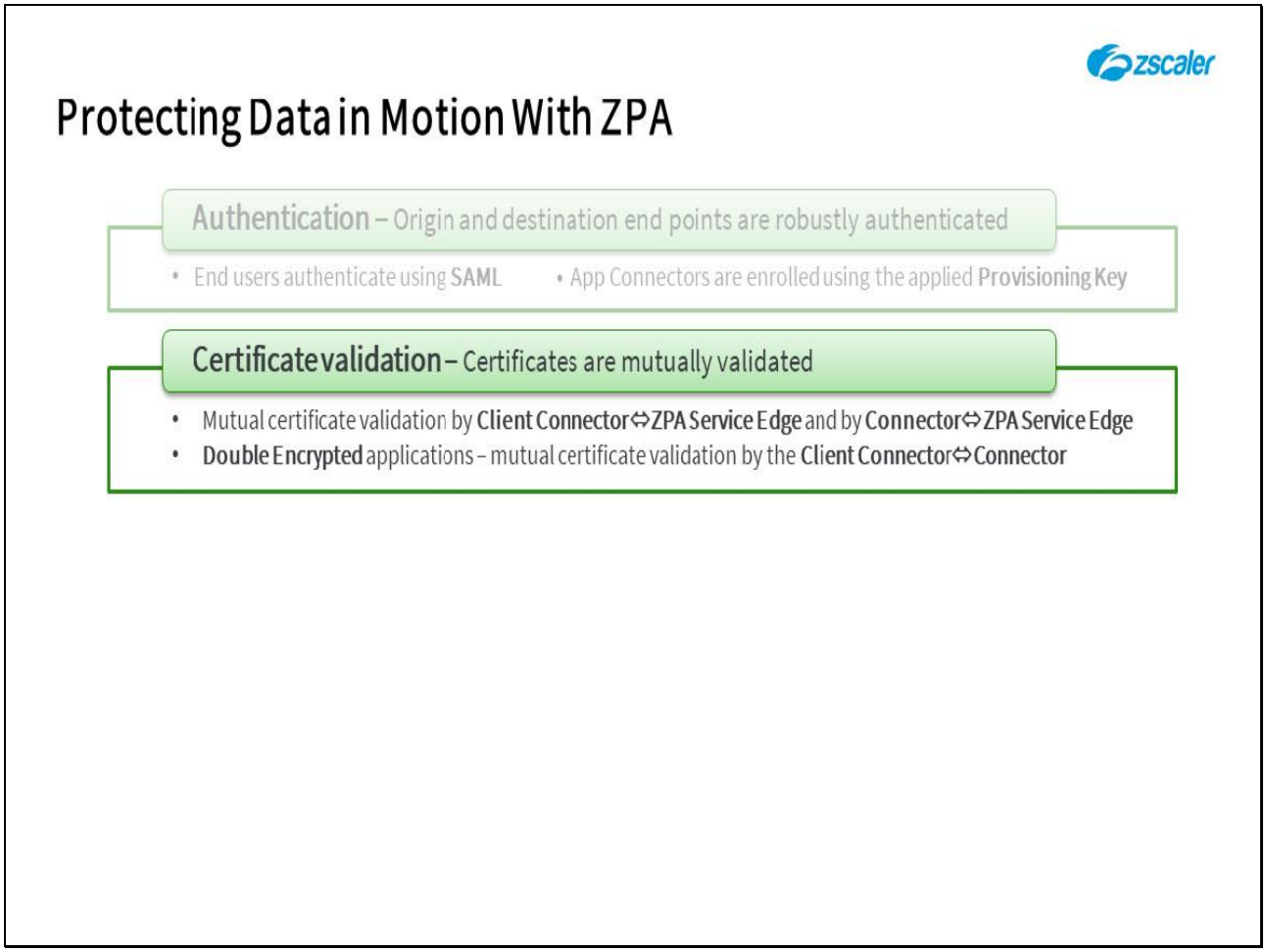
In the first section of this module, we saw a summary of the measures that can be taken to protect data in motion in general terms. Now we will look in detail at the measures used by the ZPA service, the first of which is the robust authentication of end users and the secure provisioning of the App Connectors.

End user authentication is done through the Client Connector using SAML across TLS 1.2 encrypted connections with full certificate validation at each stage. The authentication method to be used is configured on the IdP and may be forms- or certificate-based or include multiple factors. The security assertion is stored securely within the Client Connector and is presented at every application access attempt to authorize access.

The user's authentication can be revoked by an administrator at any time, which results in the revocation of the deployed identity certificates rendering them unusable.

App Connectors are infrastructure components deployed by an administrator and are authenticated and authorized through the installation of a valid **Provisioning Key**. ZPA administrators have full visibility into the enrolled and active App Connectors and can delete their configurations at any time.

Slide 22 - Protecting Data in Motion With ZPA

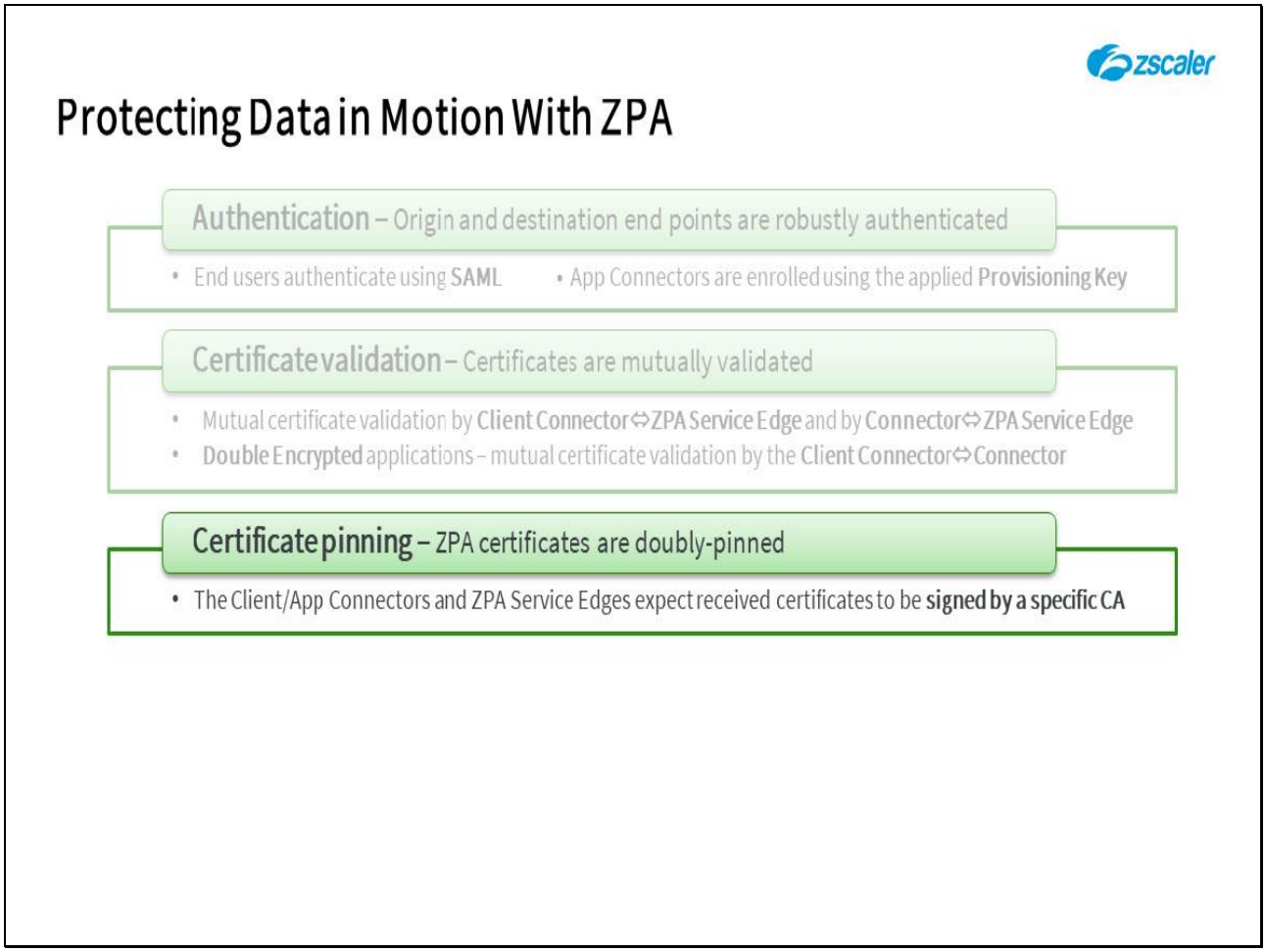


Slide notes

The next security measure to protect end user data passing through the ZPA infrastructure, is the use of TLS 1.2 encrypted connections with full certificate validation. The Z Tunnel connections from the Client and App Connectors are both mutually validated, with each end point possessing the appropriate Root CA certificate to verify the received server certificates.

For a **Double Encrypted** application using the Bring Your Own Encryption (BYOE) model, the Client Connector and the destination App Connector are able to validate each other's certificates.

Slide 23 - Protecting Data in Motion With ZPA

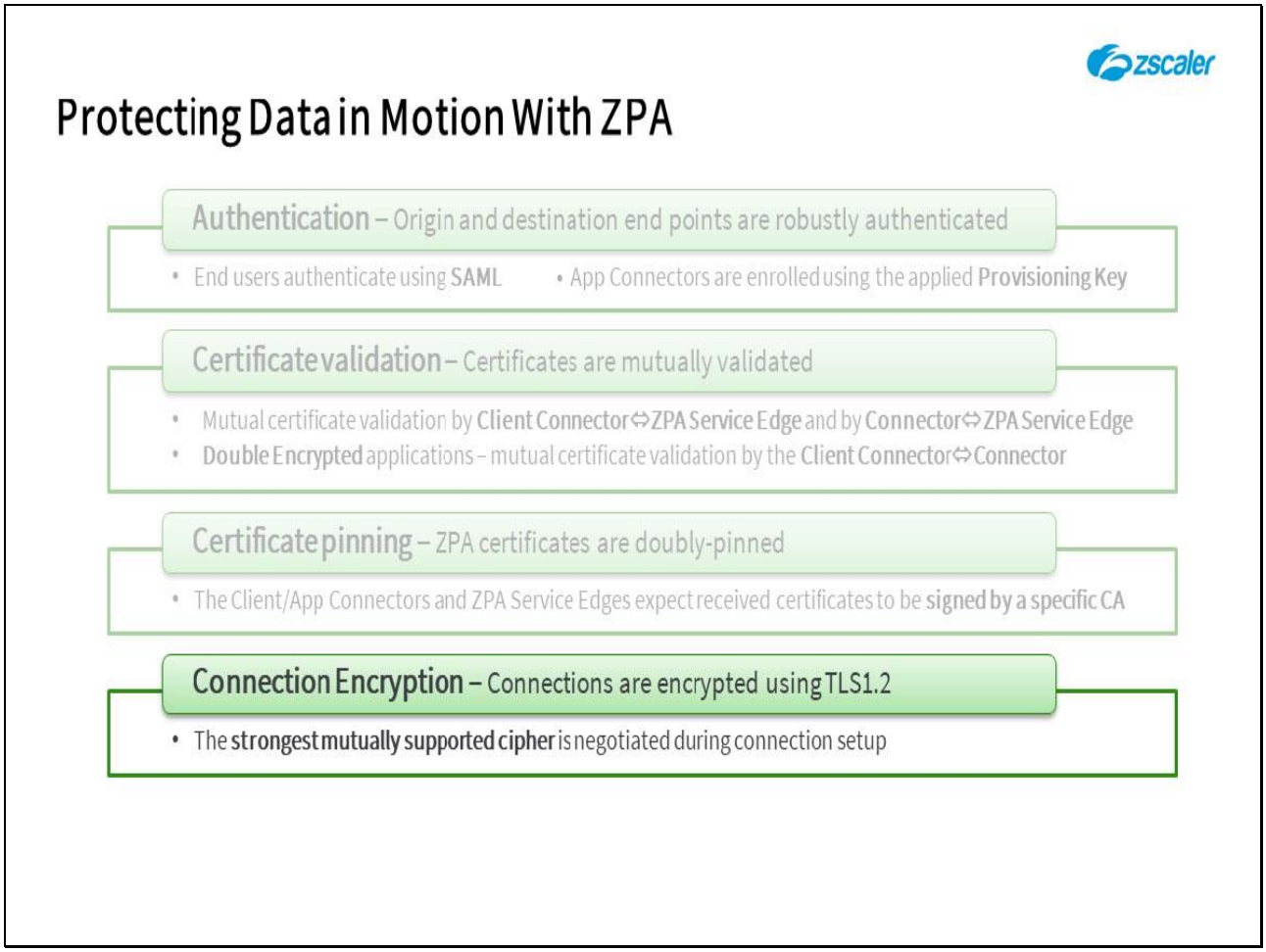


Slide notes

In addition to the certificate validation on these connections, specific certificates are expected by each of the end points, so they are in effect doubly-pinned. Both the Client and App Connectors expect and require, the received server certificate from the ZPA Service Edge to be signed by Zscaler, plus the ZPA Service Edges expect the identity certificates from the end points to be signed by the appropriate CA in use by the customer.

Mutual validation and certificate pinning are also used for **Double Encrypted** application connections between the Client Connector and the destination App Connector.

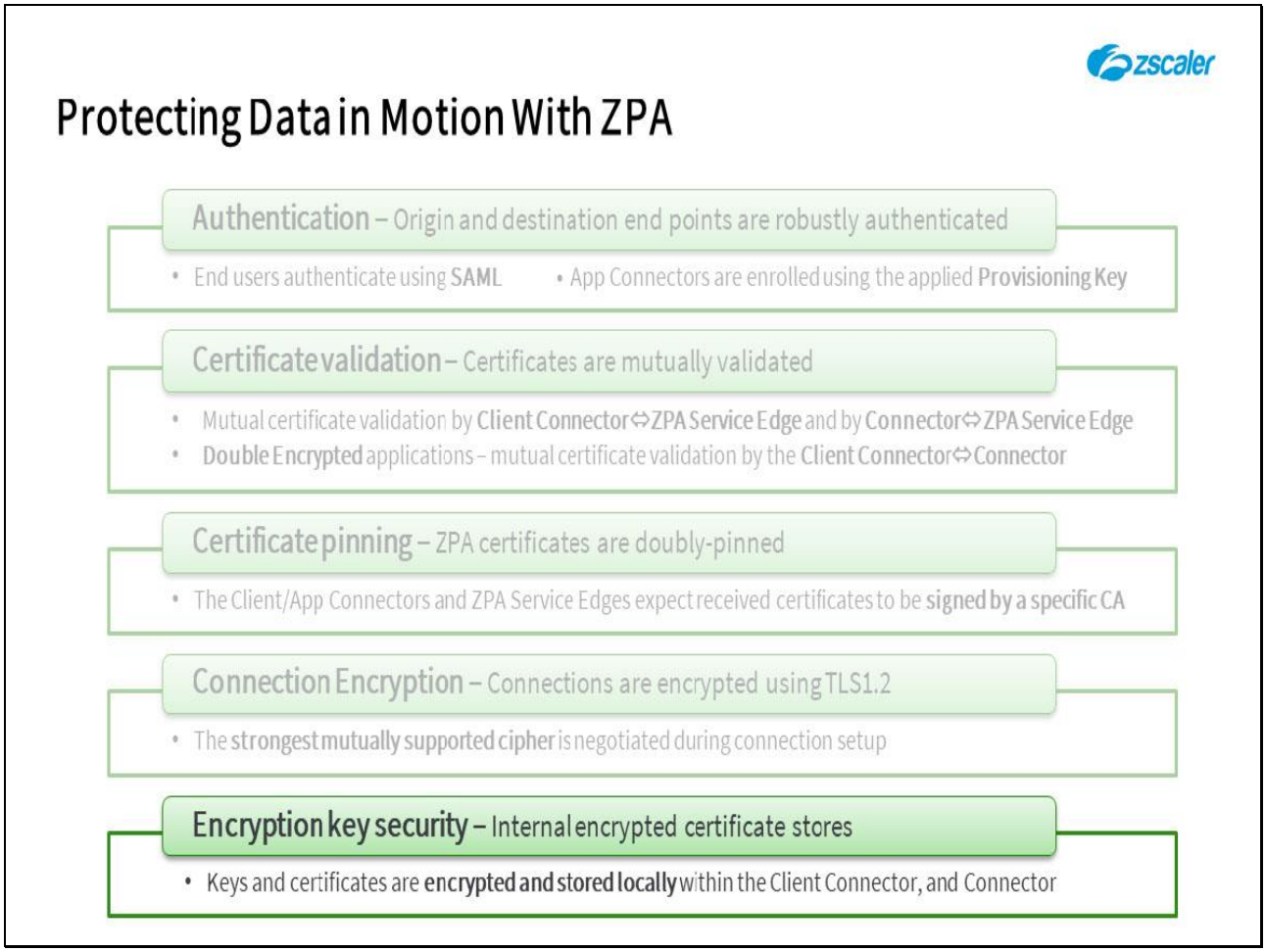
Slide 24 - Protecting Data in Motion With ZPA



Slide notes

On all of these connections, the strongest mutually supported cipher between the parties is used, so the encryption method used will always be the strongest available.

Slide 25 - Protecting Data in Motion With ZPA



Slide notes

The keys and certificates used to establish the ZPA service connections are all securely managed according to industry best practices. Both the Client and App Connectors generate their own public/private key pairs, with the private keys being encrypted and stored locally, they are never shared with any other network entity.

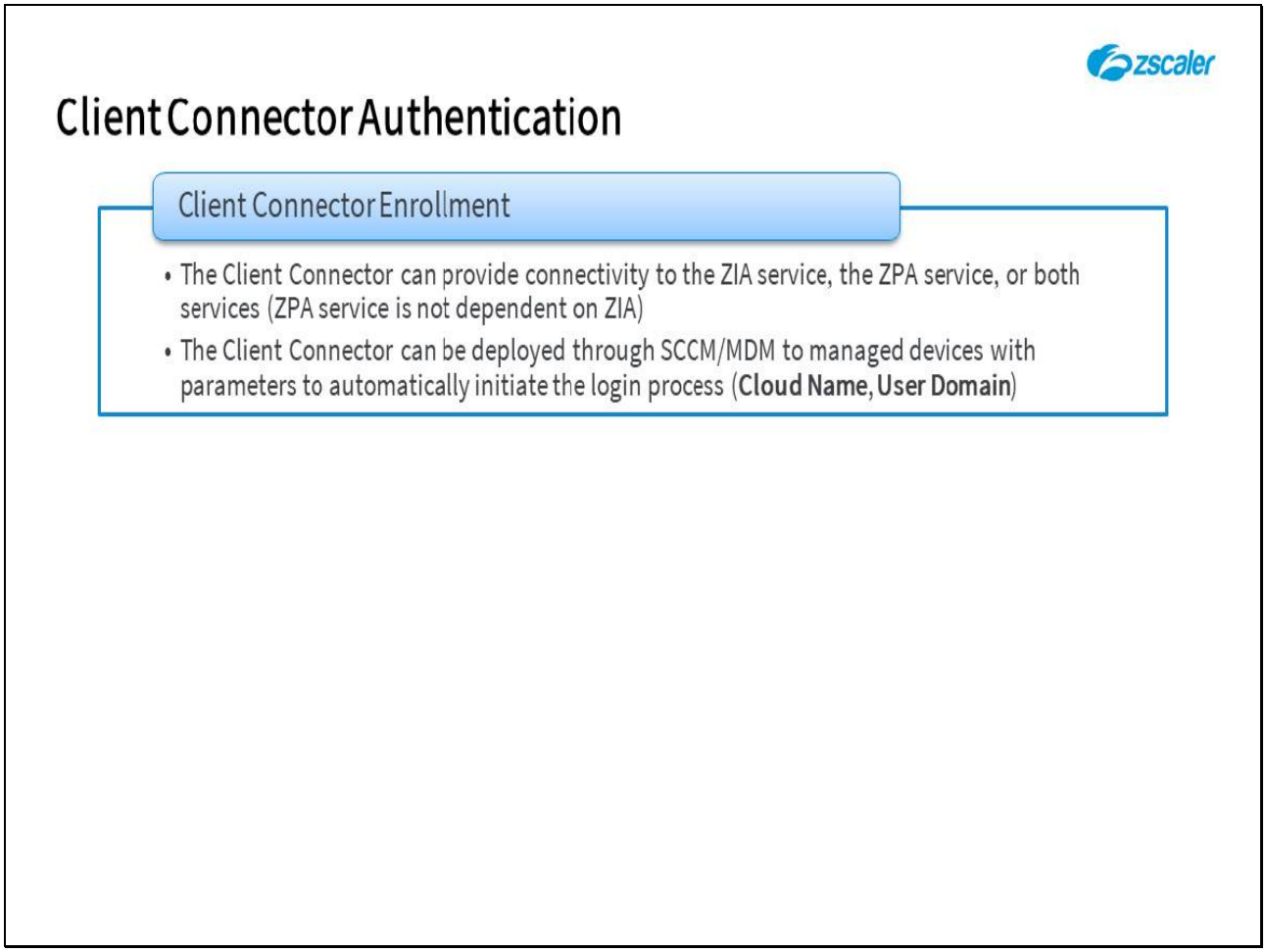
Any of the issued certificates can be revoked as necessary by a ZPA administrator, which will immediately unenroll the entity in question (Client or App Connector).

Slide 26 - ZPA User Authentication

Slide notes

Let’s now have a look at how ZPA user authentication and enrollment works.

Slide 27 - Zscaler App Authentication

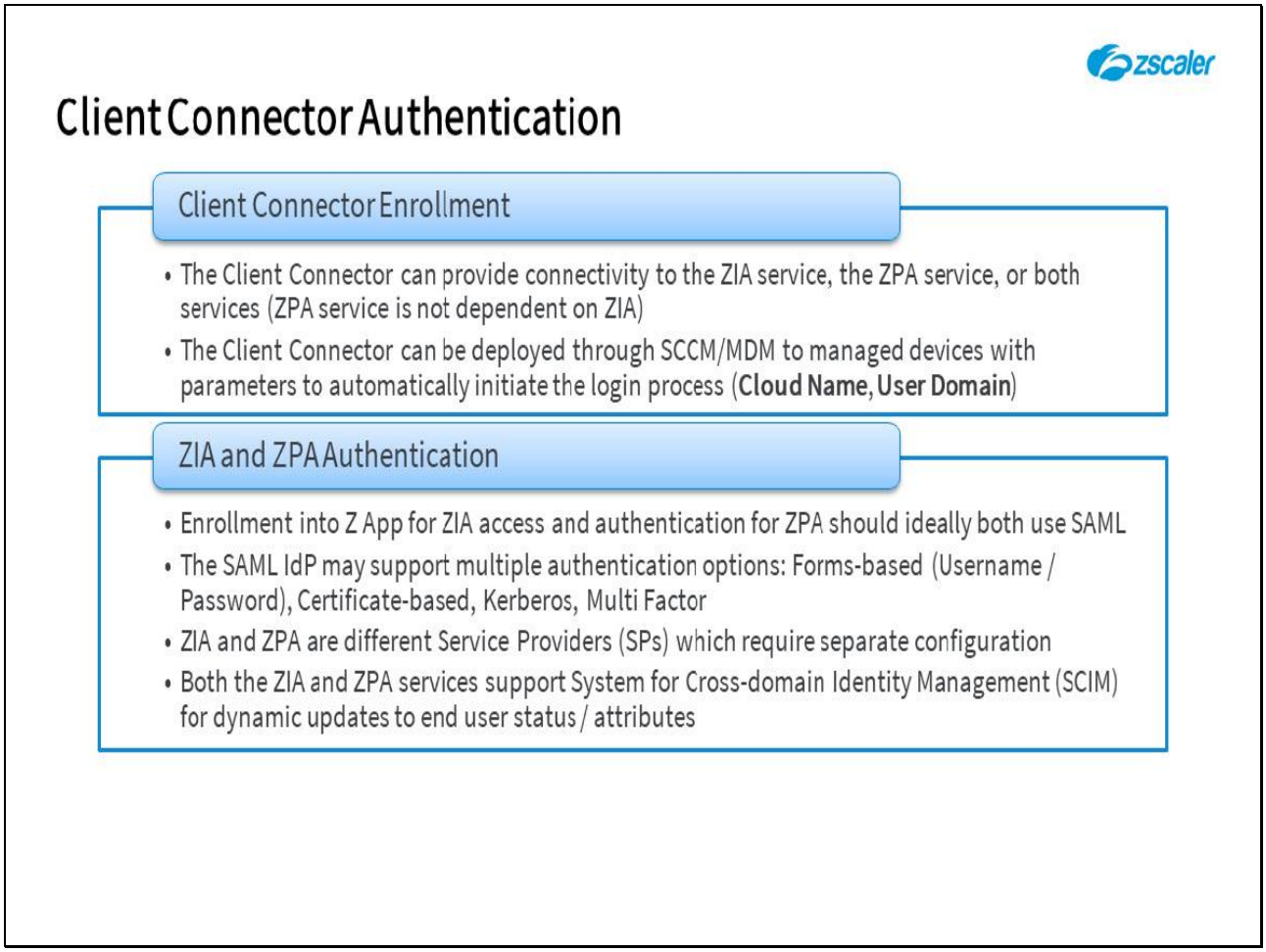


Slide notes

The Zscaler Client Connector is end point agent software for PCs and mobiles that can be used to securely connect to the Internet using the ZIA service, or to private resources using the ZPA service. It is not necessary to have a ZIA enrollment for ZPA to be provisioned, although from a Software Defined Perimeter perspective it provides better security if you do so. ZIA may use some other form of authentication or a different SAML IdP, although this would then require your end users to login through the Zscaler Client Connector twice.

The Client Connector can be installed remotely to PCs using AD or SCCM and to mobiles using your preferred MDM platform. Parameters are available to make the installation as automated as possible and to hide some of the initial authentication steps from the end users (the **--CloudName** and **--userDomain** install parameters).

Slide 28 - Zscaler App Authentication



Slide notes

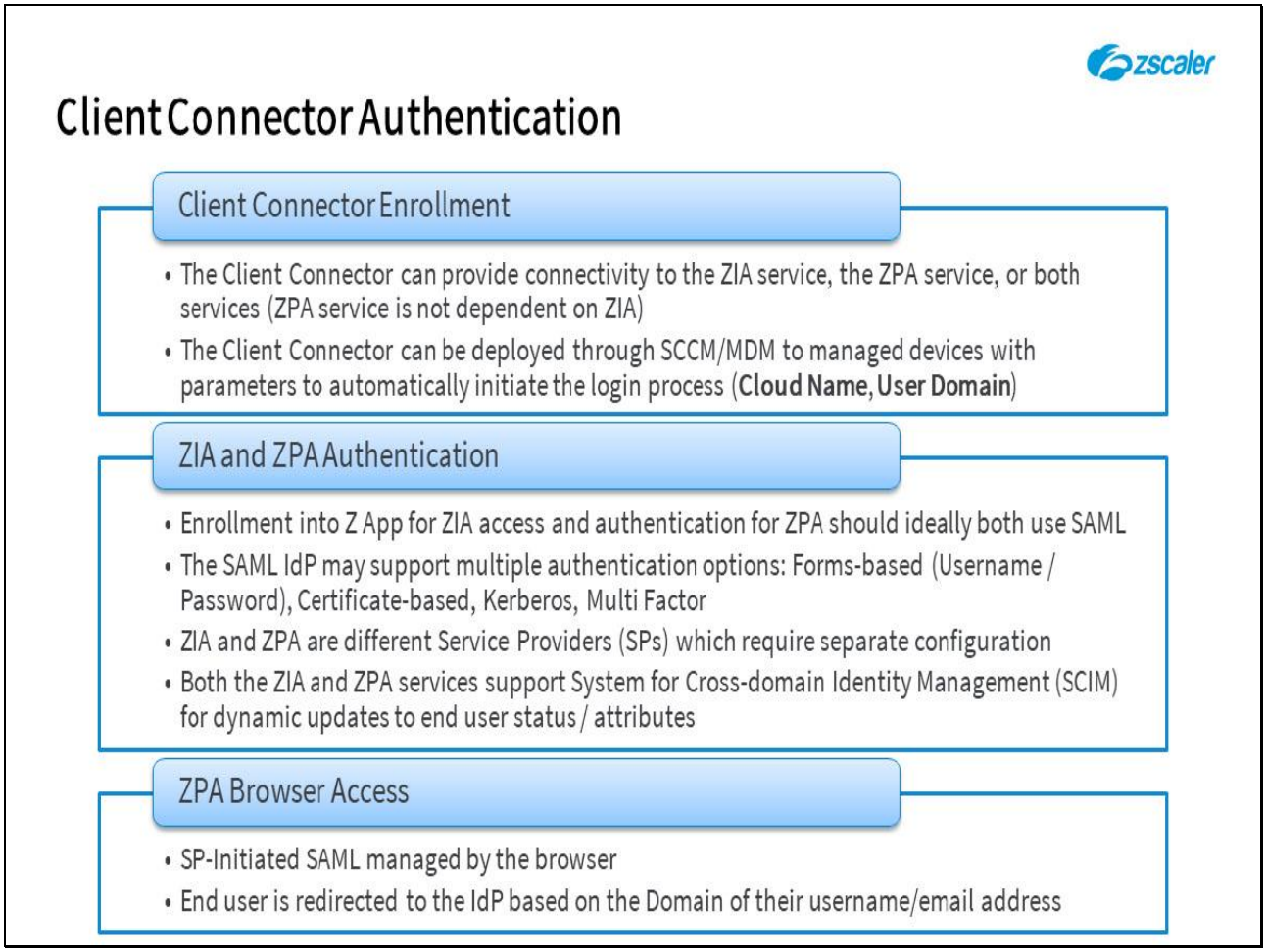
Enrollment into the Client Connector for ZIA service (if it is used) and authentication to the ZPA service, should ideally both be done using SAML and the Cloud-based or on-premise IdP of your choice. The end user authentication methods available depend entirely on the capabilities of the IdP you chose and can include:

- Forms-based authentication (Username/Password);
- Certificate-based authentication;
- Kerberos;
- Or even multi factor authentication (MFA).

Note that in your SAML IdP, ZIA and ZPA are considered to be different SPs and require separate configurations.

Both the ZIA and ZPA service support System for Cross-domain Identity Management (SCIM), which allows the dynamic, on-the-fly updates of end user status (adds or deletions), or to their authorization attributes (moves and changes).

Slide 29 - Zscaler App Authentication

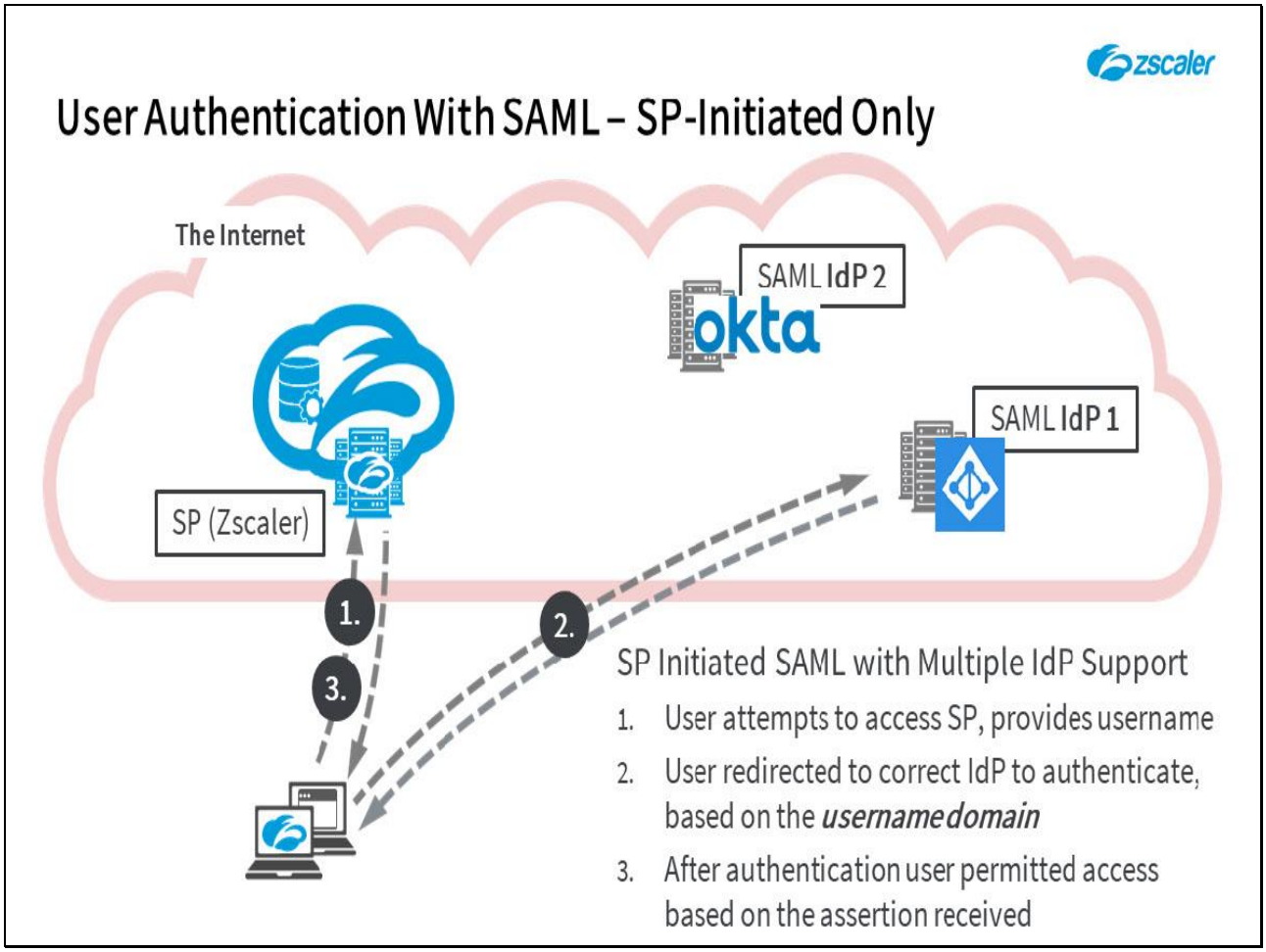


Slide notes

With the ZPA service, end users may also authenticate in a browser to access private, web-based resources. In this case authentication is managed as vanilla SP-initiated SAML managed by the end user's browser directly; the Client Connector agent is not required.

As with the Client Connector, the end user will be re-directed to the correct IdP based on the domain/realm of their email address. The SAML assertion received on a successful authentication is stored and managed by the browser that initiated the authentication.

Slide 30 - User Authentication With SAML – SP Initiated Only

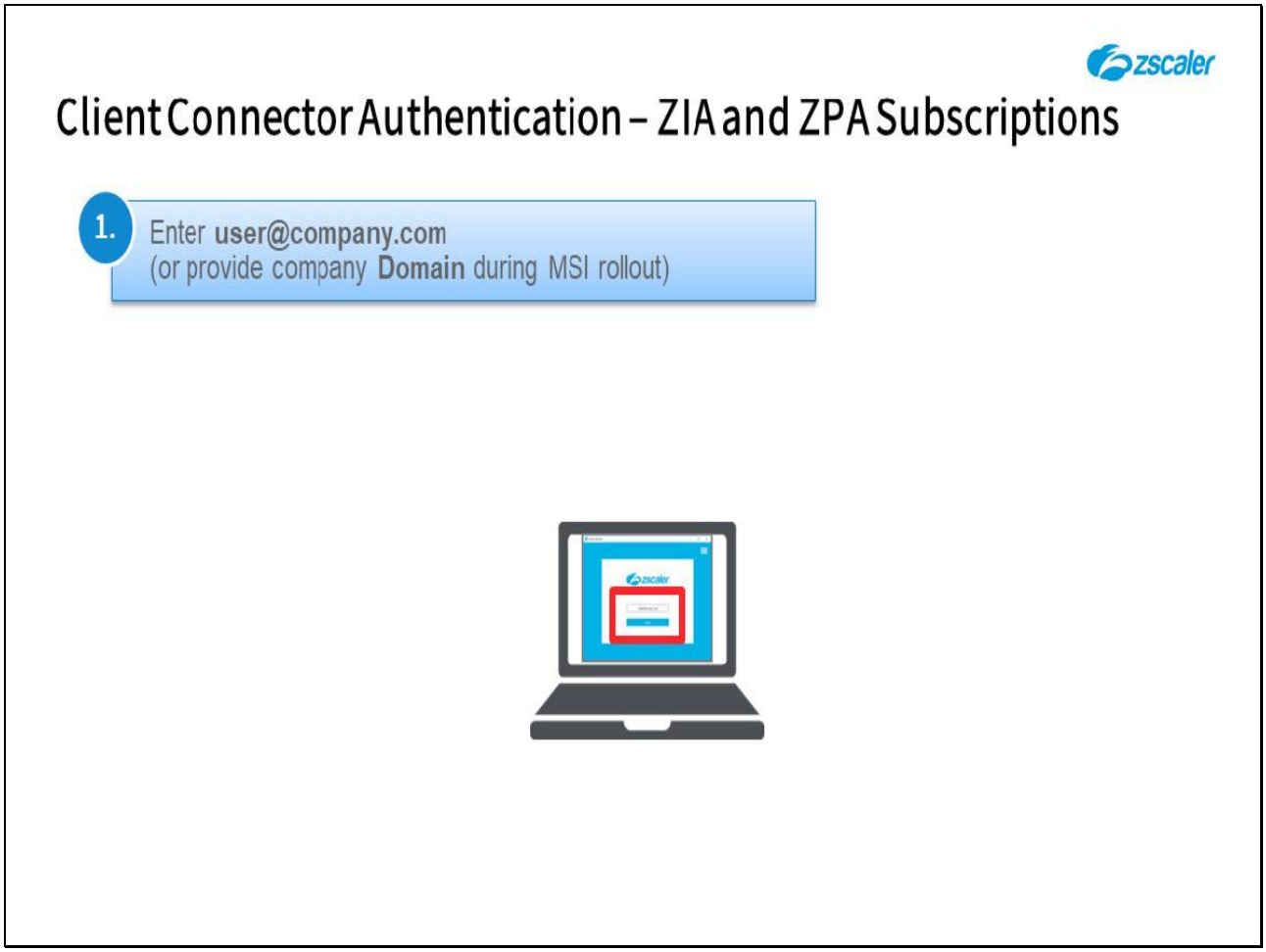


Slide notes

As discussed in the ZCCA-PA content, SAML is required for end user authentication to the ZPA service, through the Zscaler Client Connector or in a browser.

The only SAML mode supported for end user authentication is SP-initiated SAML. With the Multiple IdP capability, the user (or Client Connector Installer) must provide domain information at enrollment, to allow the ZPA service to identify the correct IdP to use to authenticate the user.

Slide 31 - Zscaler App Authentication



Slide notes

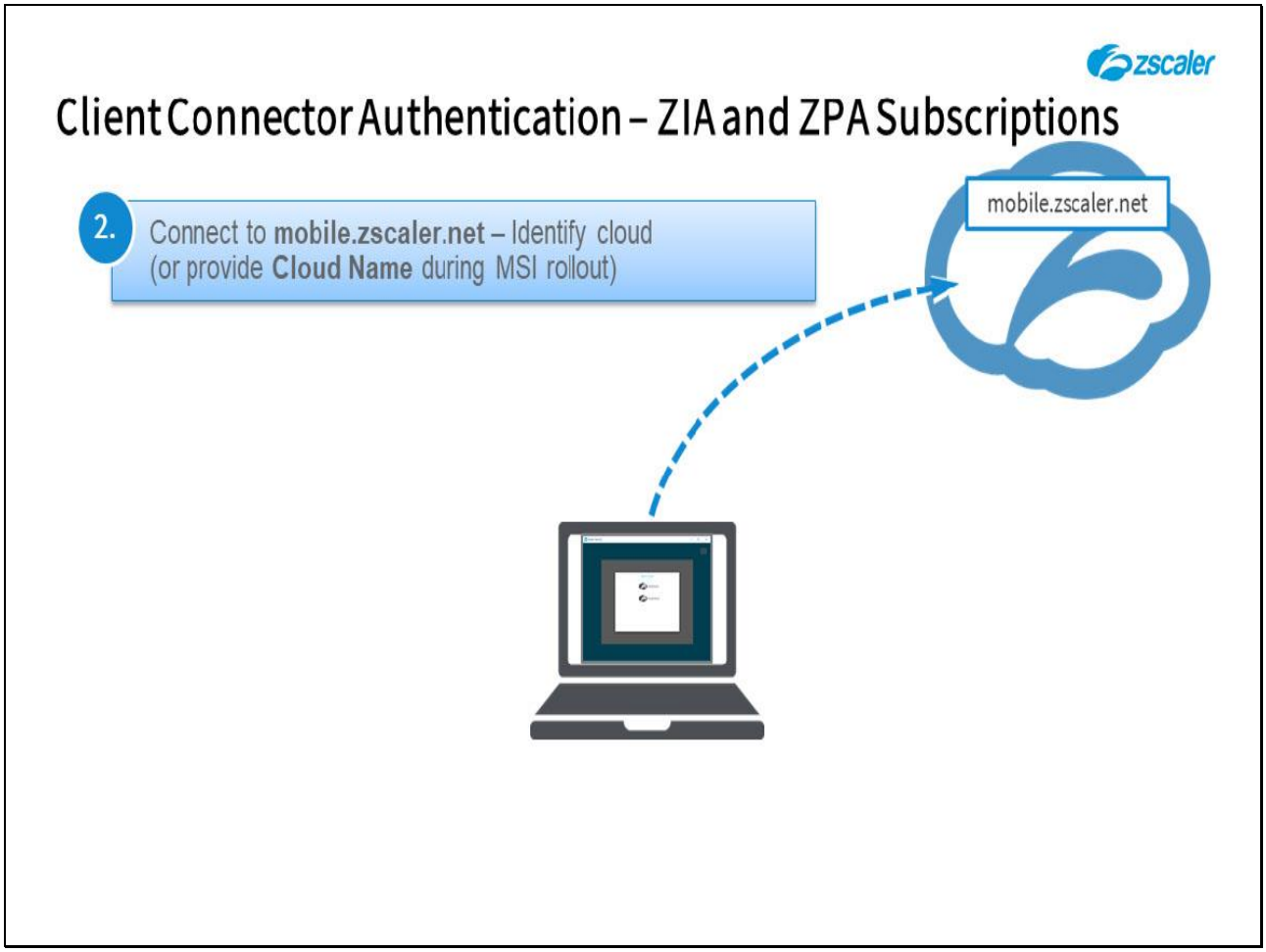
Let's step through the process for an end user authentication in the Zscaler Client Connector for a subscription to both the ZIA and ZPA services.

1. The process begins with a prompt for the user's ID in email format.

   Note that the realm portion of the email address provided must match either the organization's **Primary Authentication Domain** or one of the **Secondary Authentication Domains**.

   Also note that it is possible to populate the company's domain during installation of the Client Connector, at which point the end user will be immediately re-directed to the associated IdP for authentication.

Slide 32 - Zscaler App Authentication



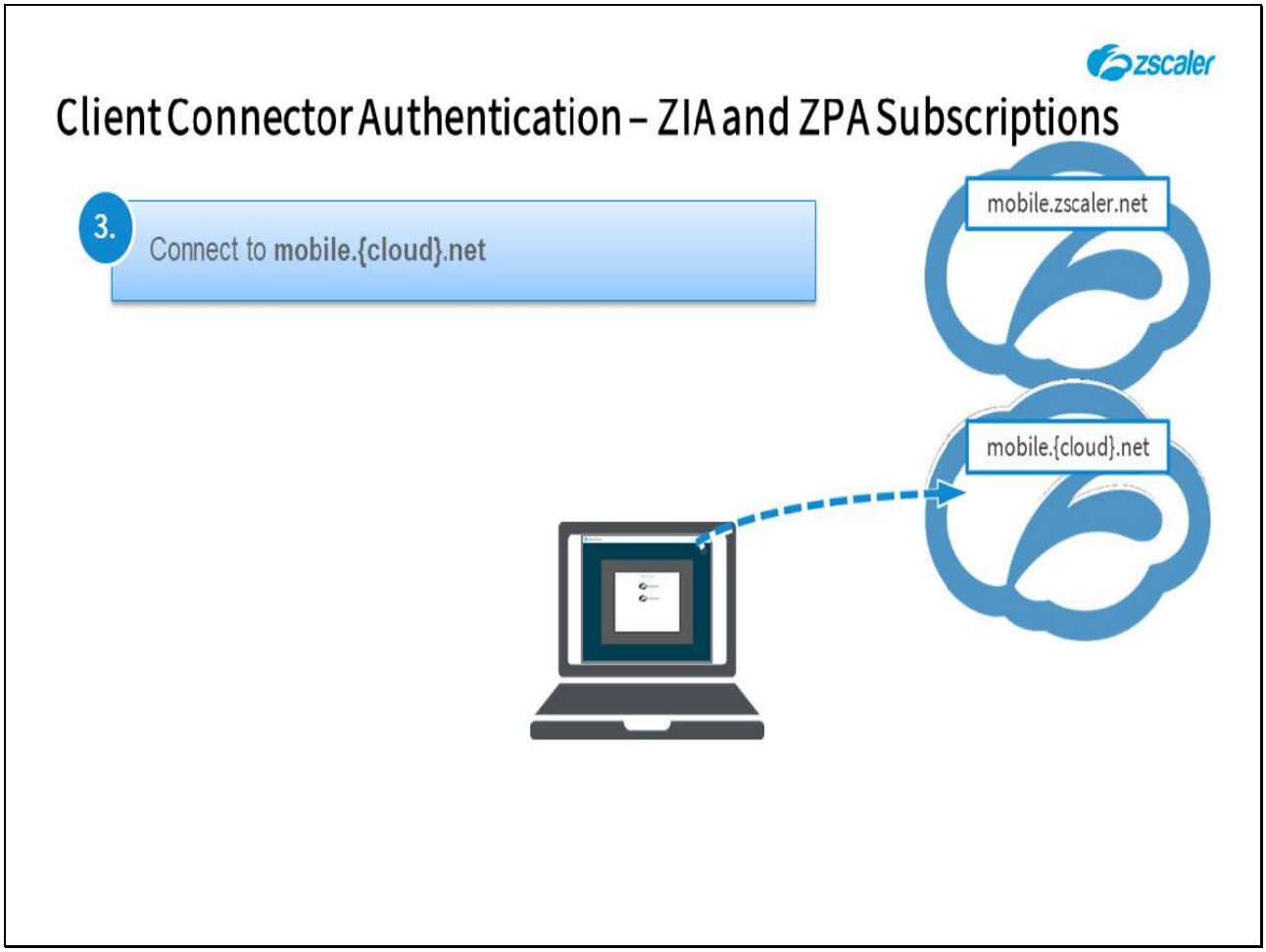
Slide notes

2. One of the first things that the Client Connector needs to do is to identify the Zscaler Cloud that the organization is provisioned on for mobile access, if the end user's domain is associated with multiple Clouds, they will be prompted to select the Cloud for this enrollment.

   Alternatively, the Cloud name may also be provided as an installation parameter to save the end users seeing this prompt.

   The first connection that the Client Connector establishes is to the **mobile.zscaler.net** Cloud.

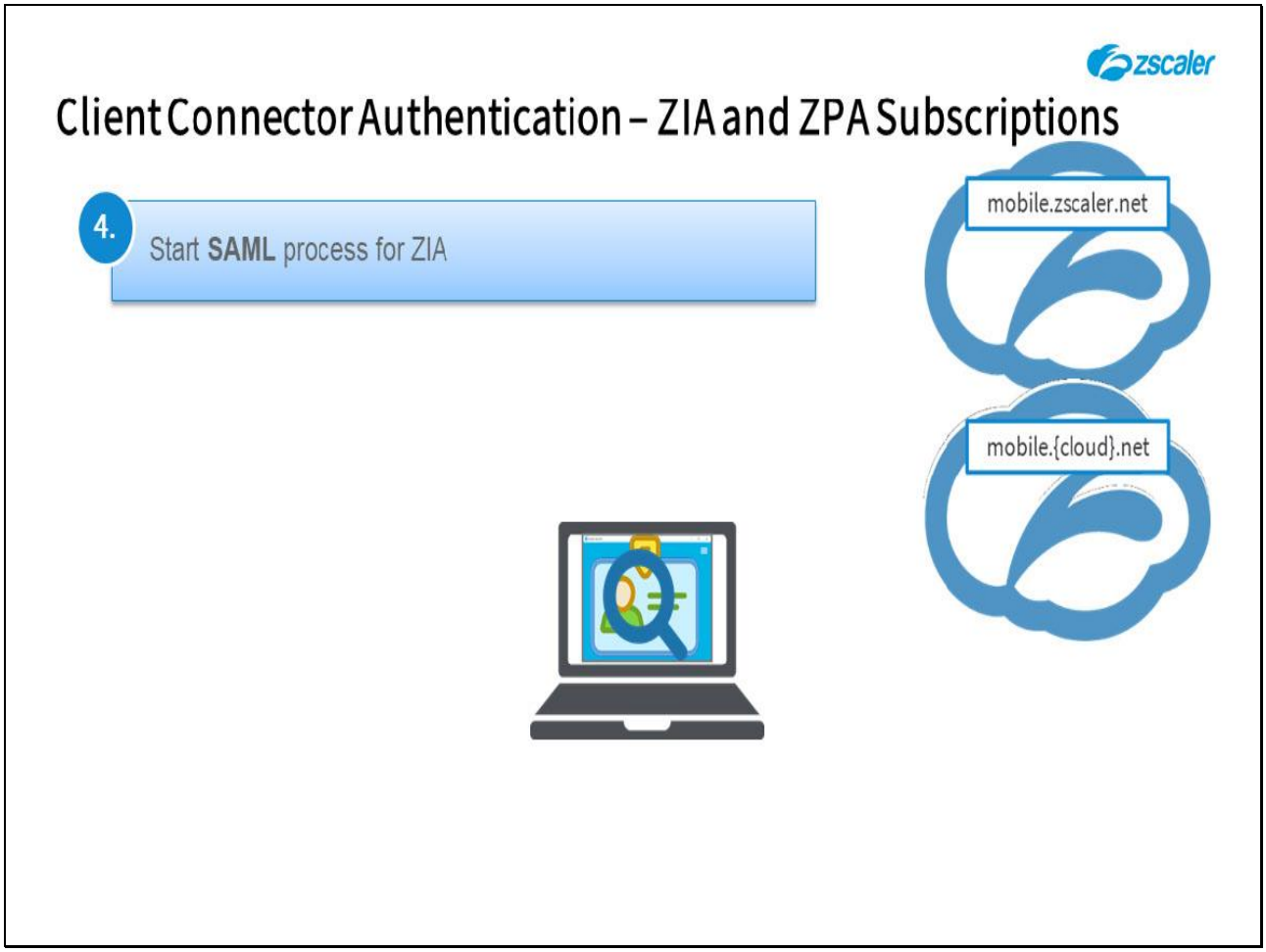
Slide 33 - Zscaler App Authentication



Slide notes

3. Having identified the correct Cloud, the Client Connector will connect to it.

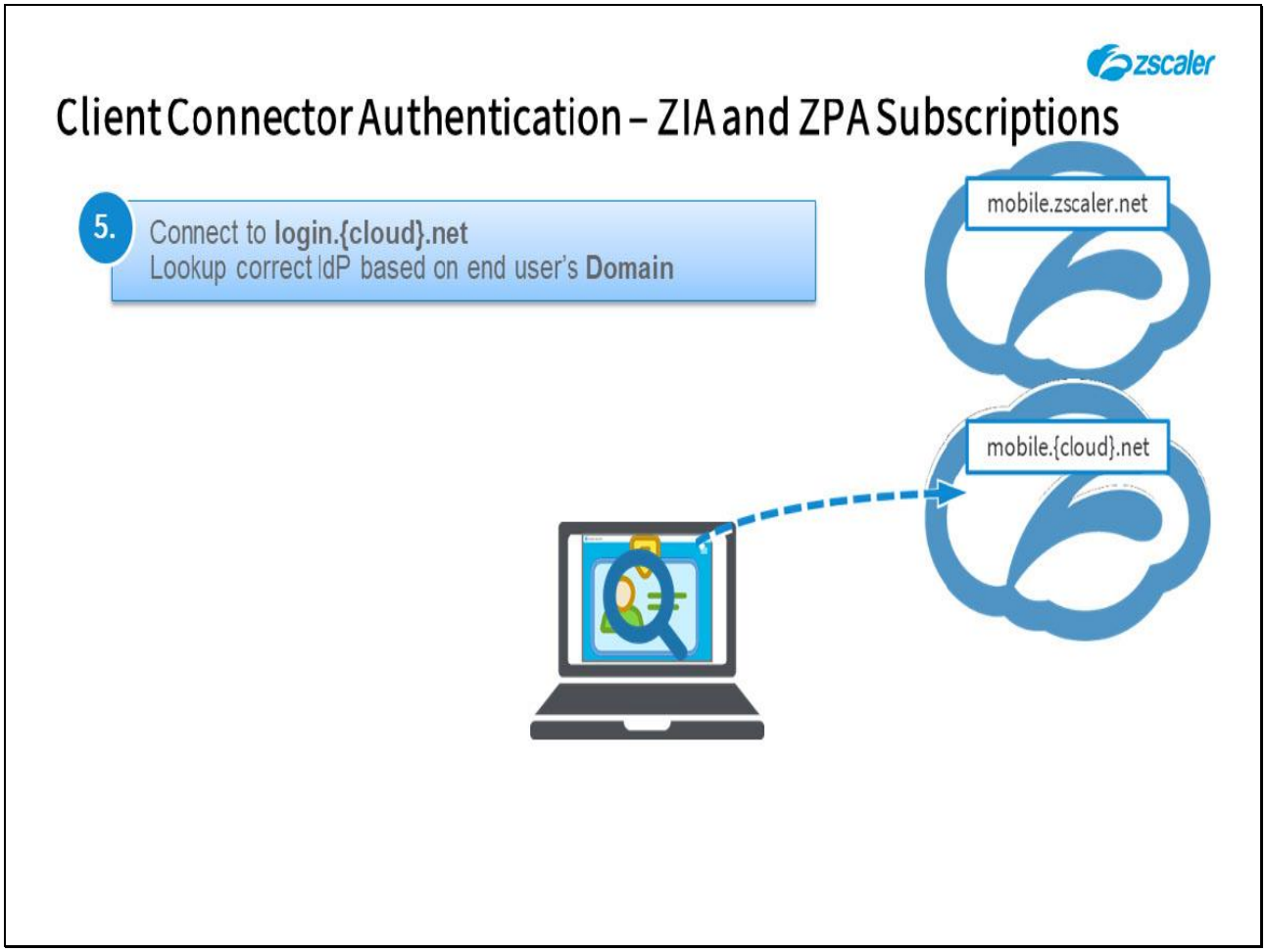
Slide 34 - Zscaler App Authentication



Slide notes

4. The next step is to initialize the SAML authentication process for ZIA (if required).

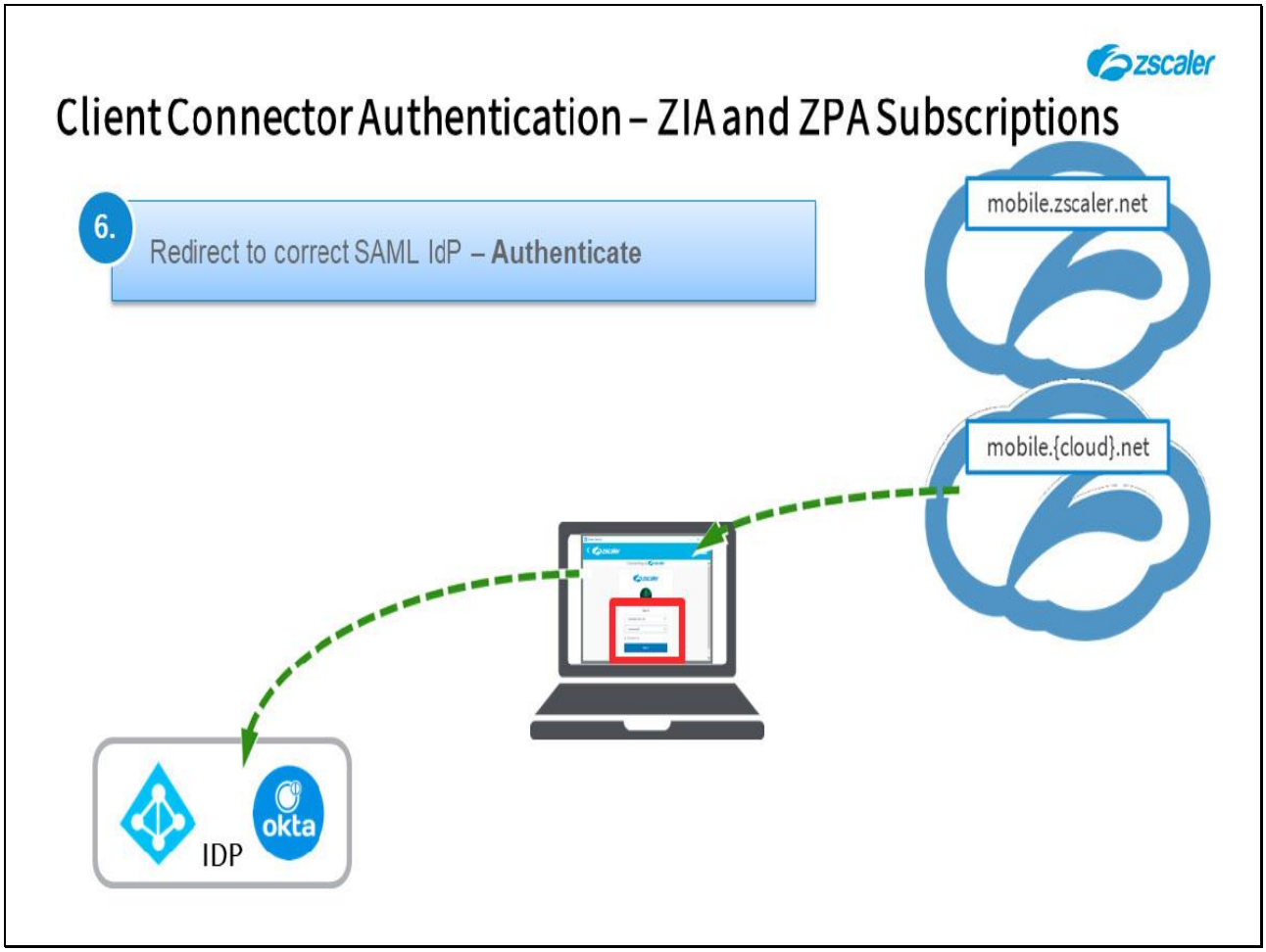
Slide 35 - Zscaler App Authentication



Slide notes

5. The Client Connector will connect to the relevant mobile Cloud, which triggers the SP-initiated SAML authentication process.

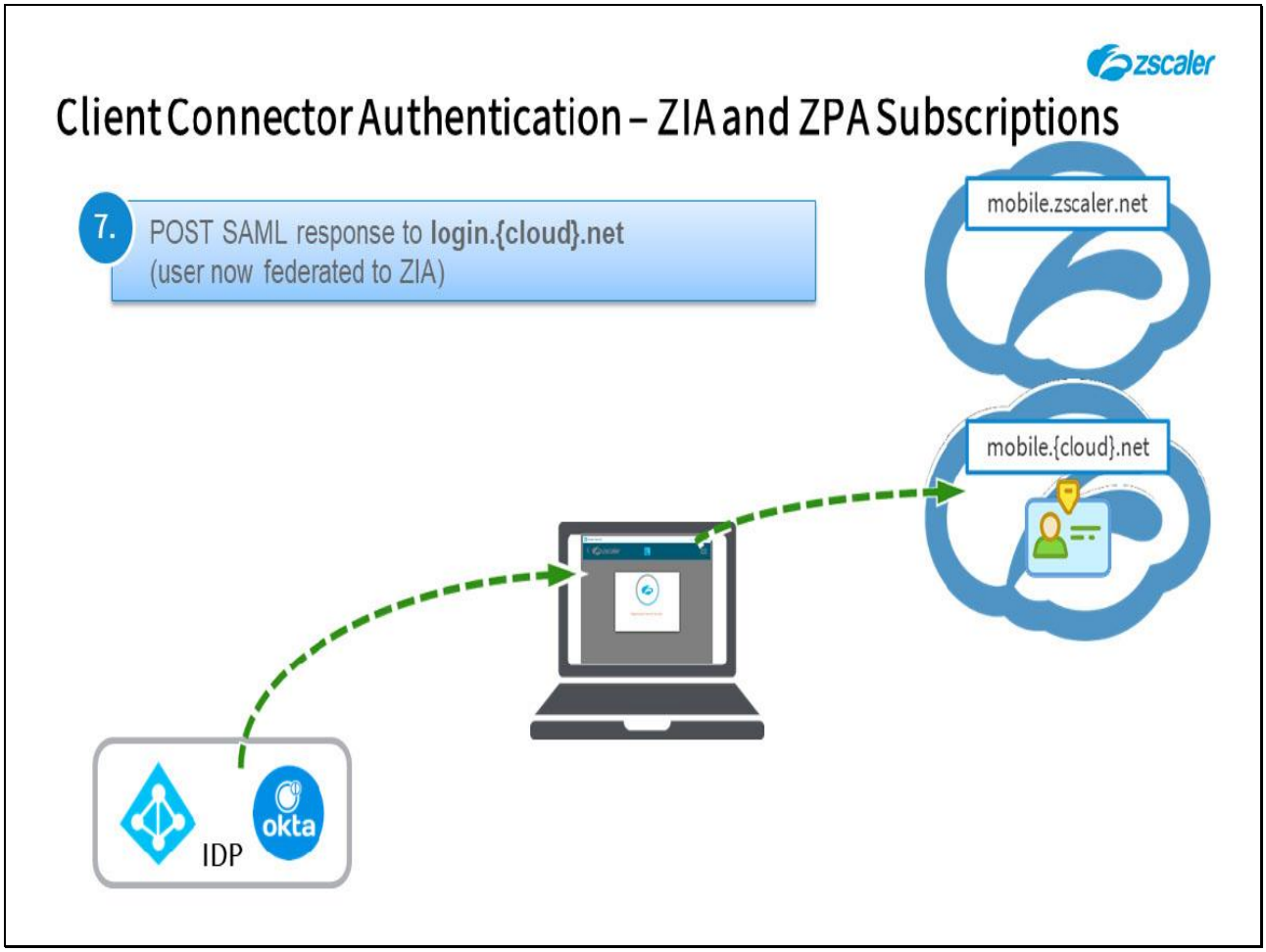
Slide 36 - Zscaler App Authentication



Slide notes

6. The Cloud will redirect the Client Connector to the configured SAML IdP for ZIA authentication. The user will be prompted for whatever credentials are required by that IdP.

Slide 37 - Zscaler App Authentication

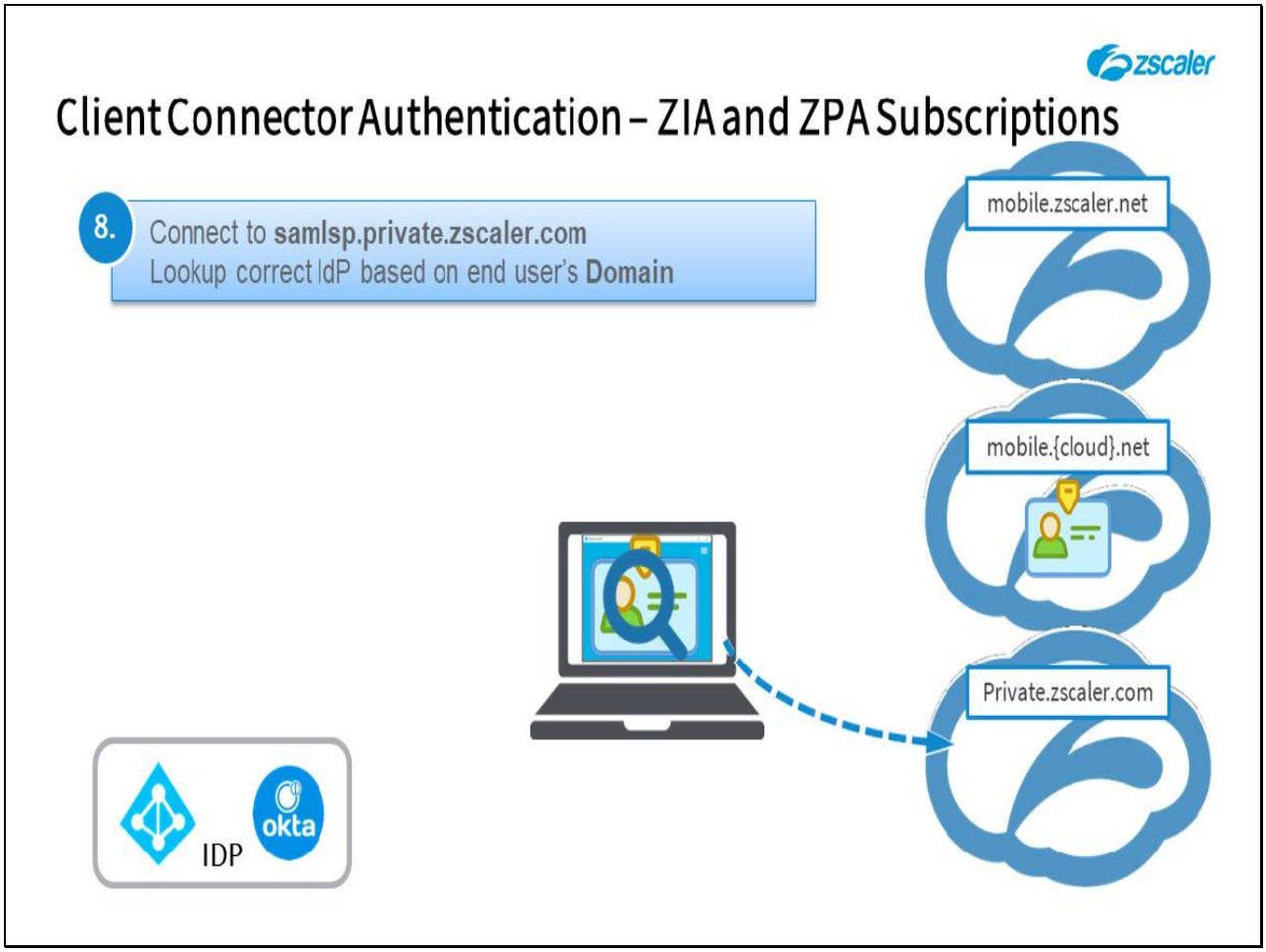


Slide notes

7. If the user authenticates successfully at the IdP, the Client Connector will receive the SAML security assertion as a POST response, which it then forwards to the mobile Cloud. The user is now authenticated and federated to the ZIA service.

   If SAML Auto-Provisioning is enabled, the user's identity and any assigned authorization attributes are added to the ZIA user database for future reference.

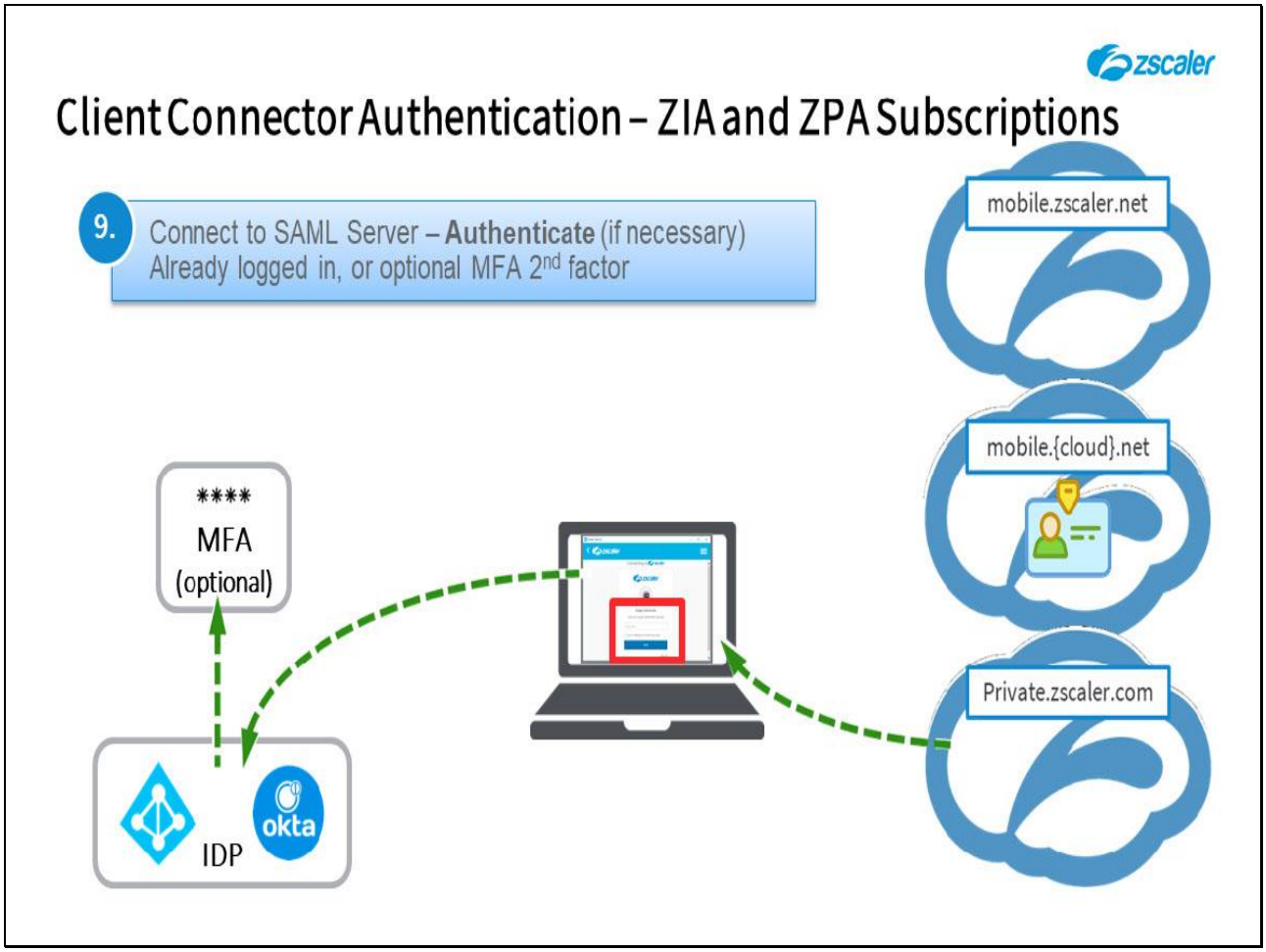
Slide 38 - Zscaler App Authentication



Slide notes

8. The Client Connector will now initiate SAML authentication for the ZPA service and will connect to the ZPA Cloud.

Slide 39 - Zscaler App Authentication

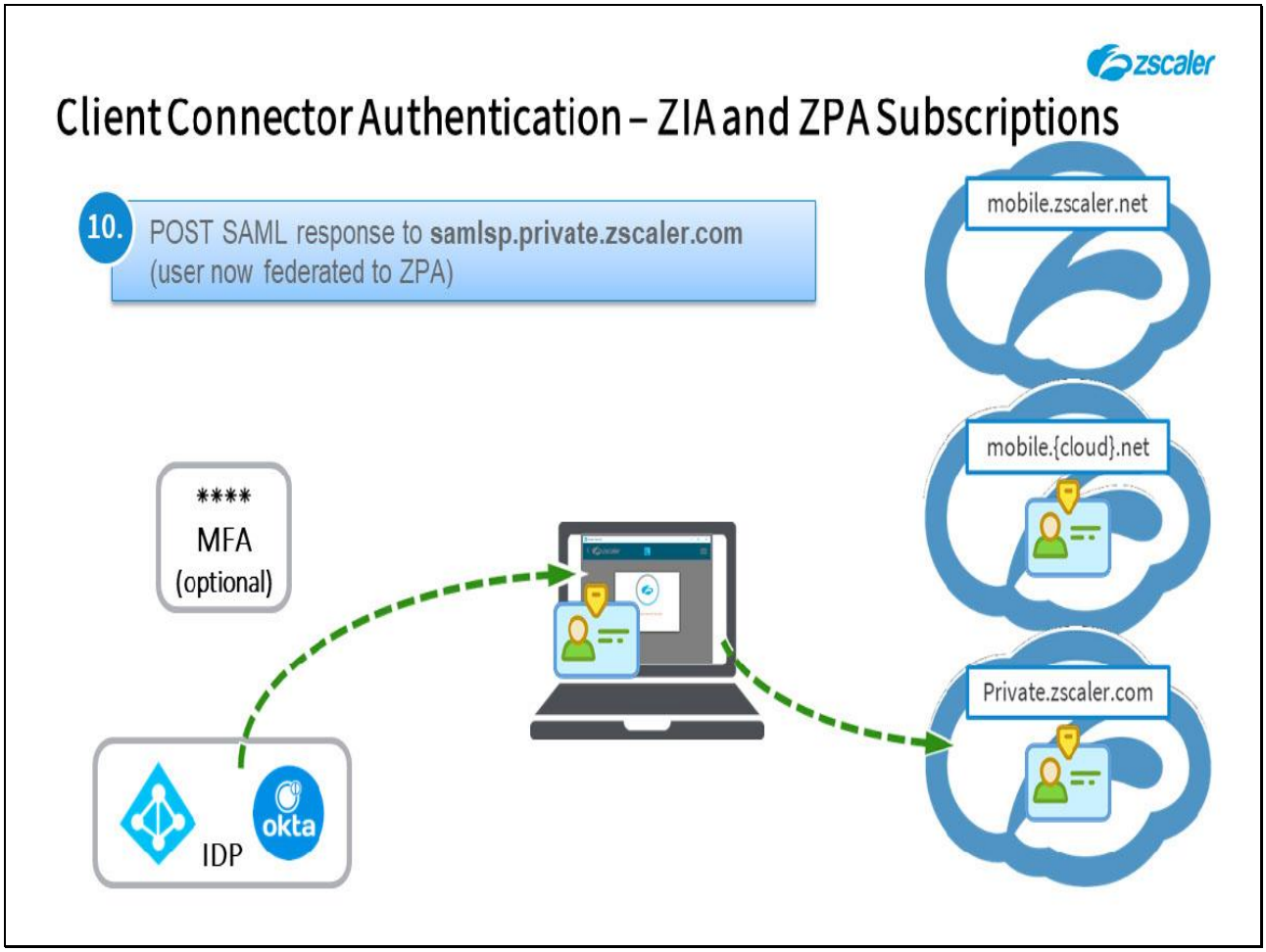


Slide notes

9. Once again, the Client Connector will be redirected to the associated SAML IdP to authenticate. If this is the same IdP as for ZIA the user is already logged in, if this is some other IdP the user will be prompted to authenticate again.

   If ZPA is configured for multi-factor authentication, the user will be prompted to complete the second factor.

Slide 40 - Zscaler App Authentication

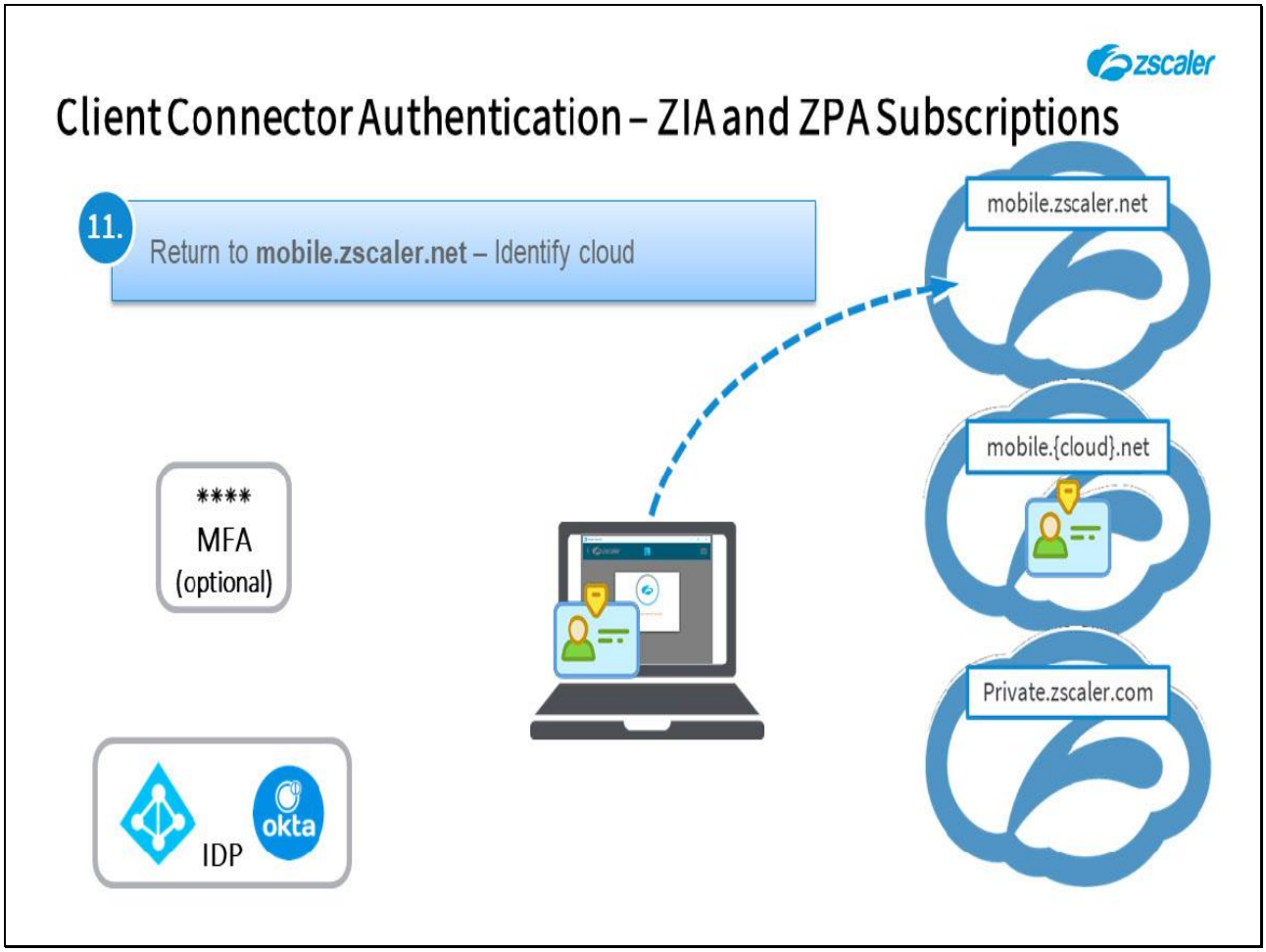


Slide notes

10. On successful authentication, the IdP returns the SAML security assertion to the Client Connector as a POST response, which the Client Connector forwards to the ZPA Cloud. The user is now authenticated and federated to the ZPA service as well.

    Note that the ZPA service does not store the user's details and authorization attributes (as with the ZIA service). The Zscaler Client Connector encrypts and stores the SAML assertion and its attributes (**NameID**, **memberOf**, etc.) and it presents the assertion to the Cloud on every ZPA application access attempt.

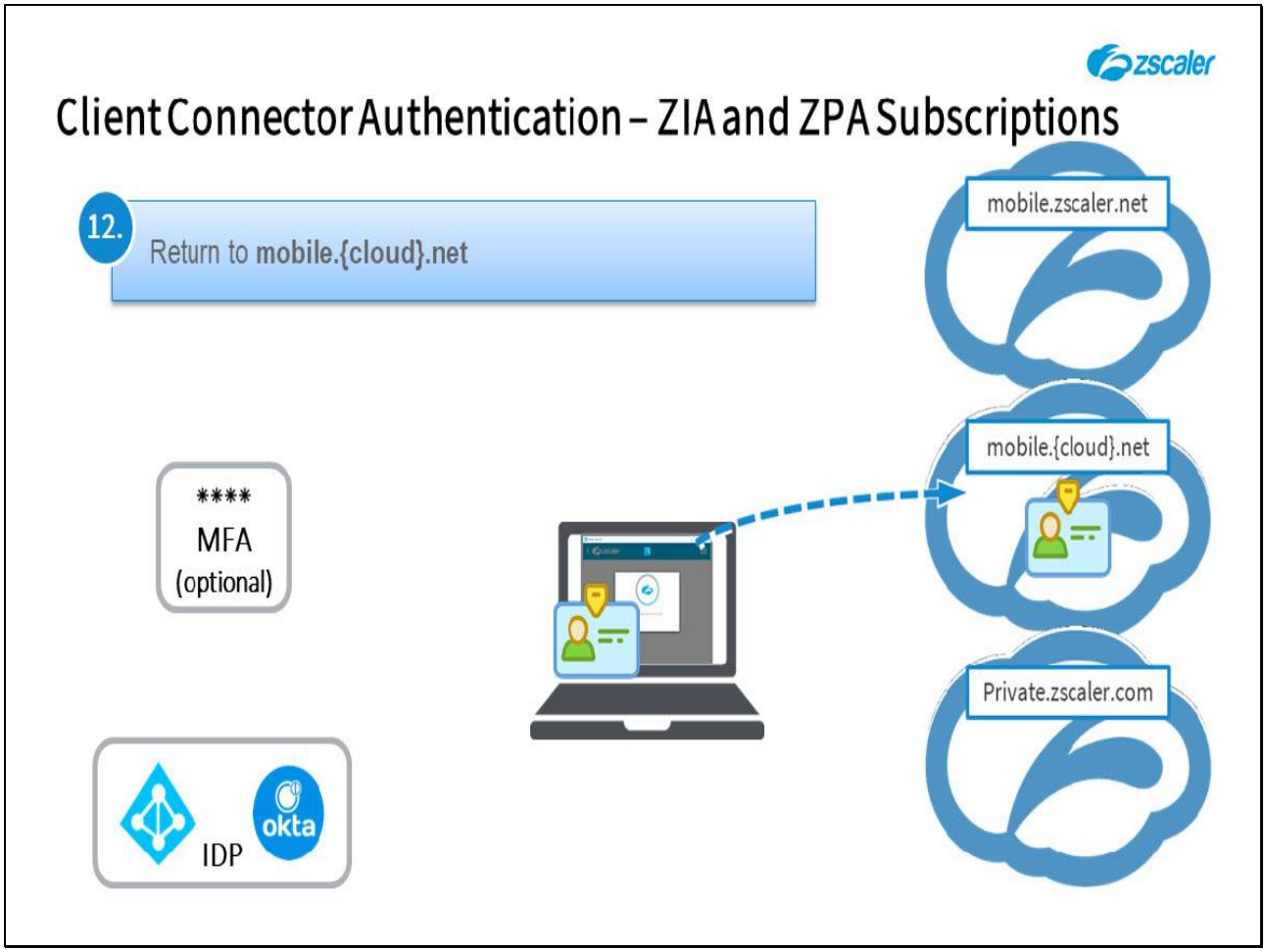
Slide 41 - Zscaler App Authentication



Slide notes

11. The Client Connector then returns to the **mobile.zscaler.net** Cloud.

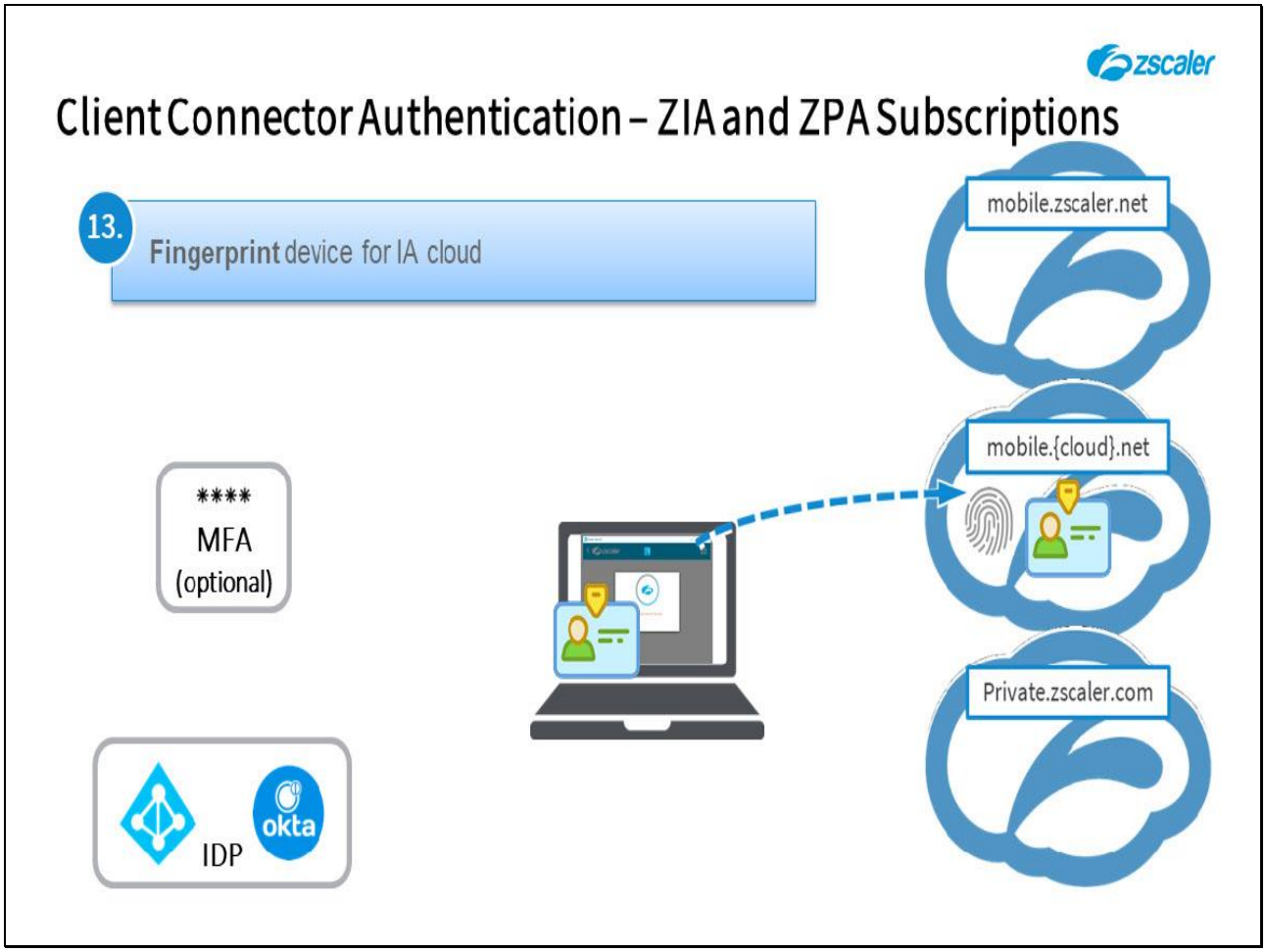
Slide 42 - Zscaler App Authentication



Slide notes

12. Then connects back to the correct mobile Cloud for the organization, to complete the enrollment process.

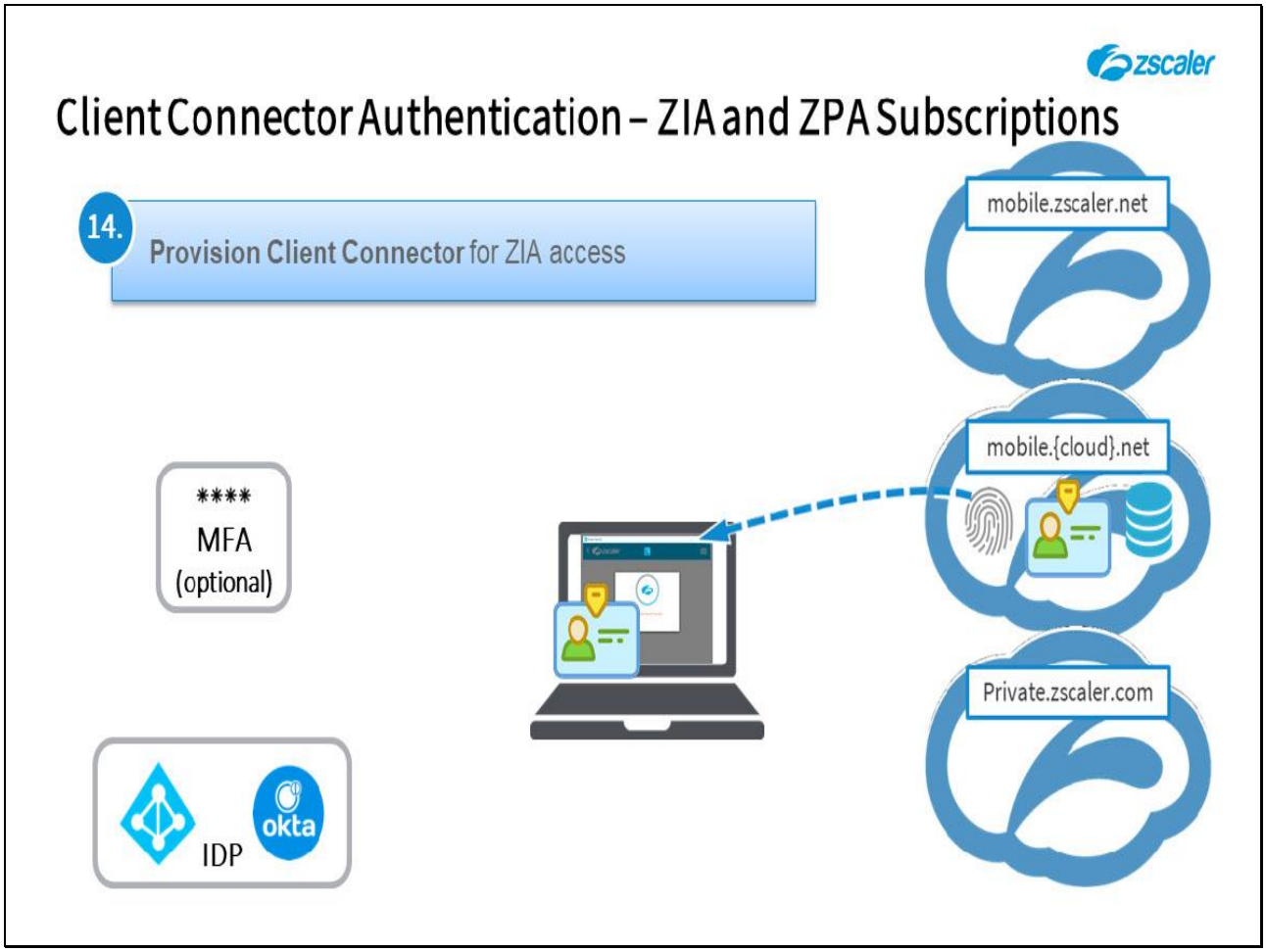
Slide 43 - Zscaler App Authentication



Slide notes

13. The device is fingerprinted to the IA Cloud, to prevent cloning, …

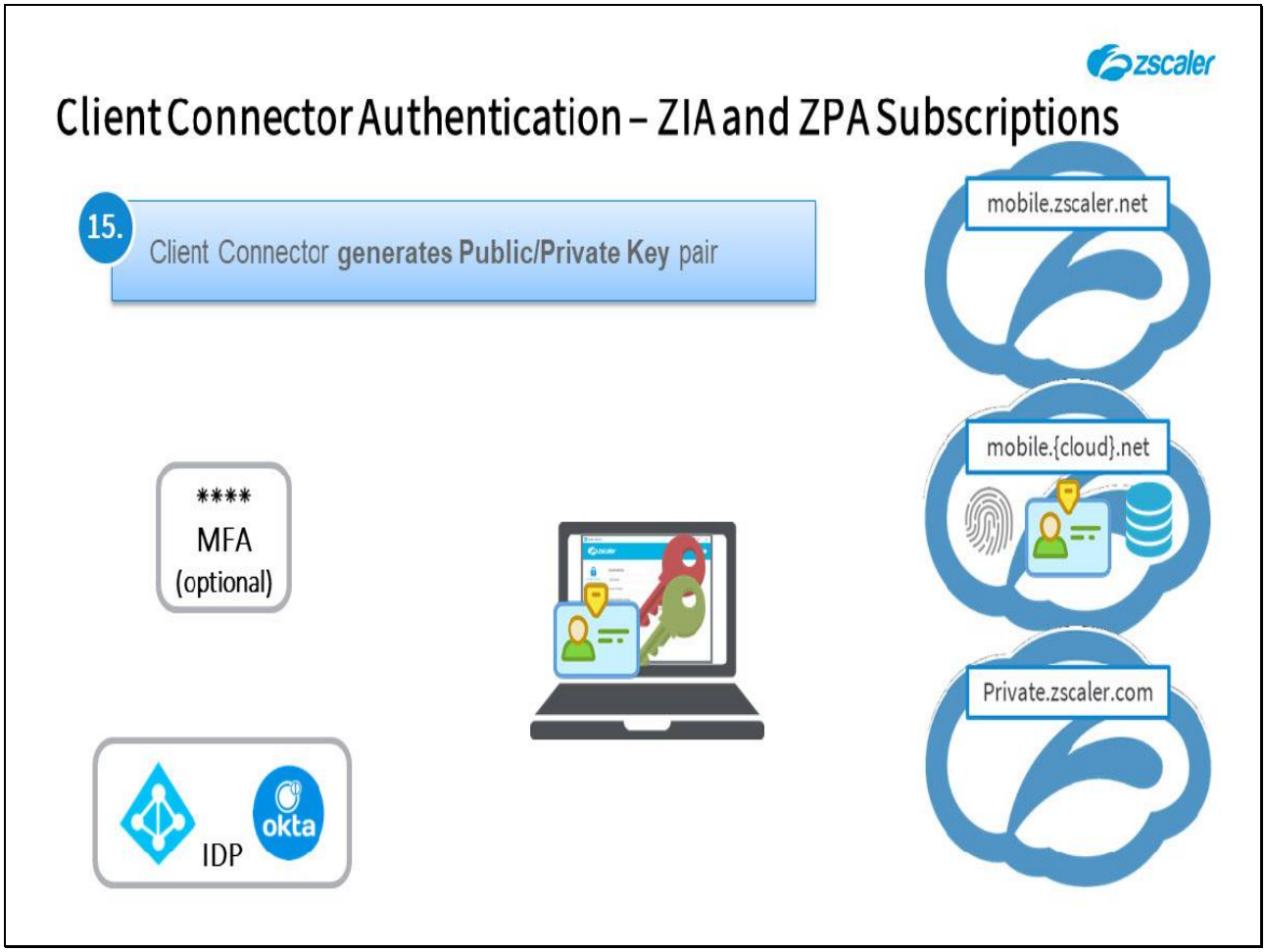
Slide 44 - Zscaler App Authentication



Slide notes

14. …and provisioned for IA connectivity (**App Profile**, **Forwarding Profile** and other configurations).

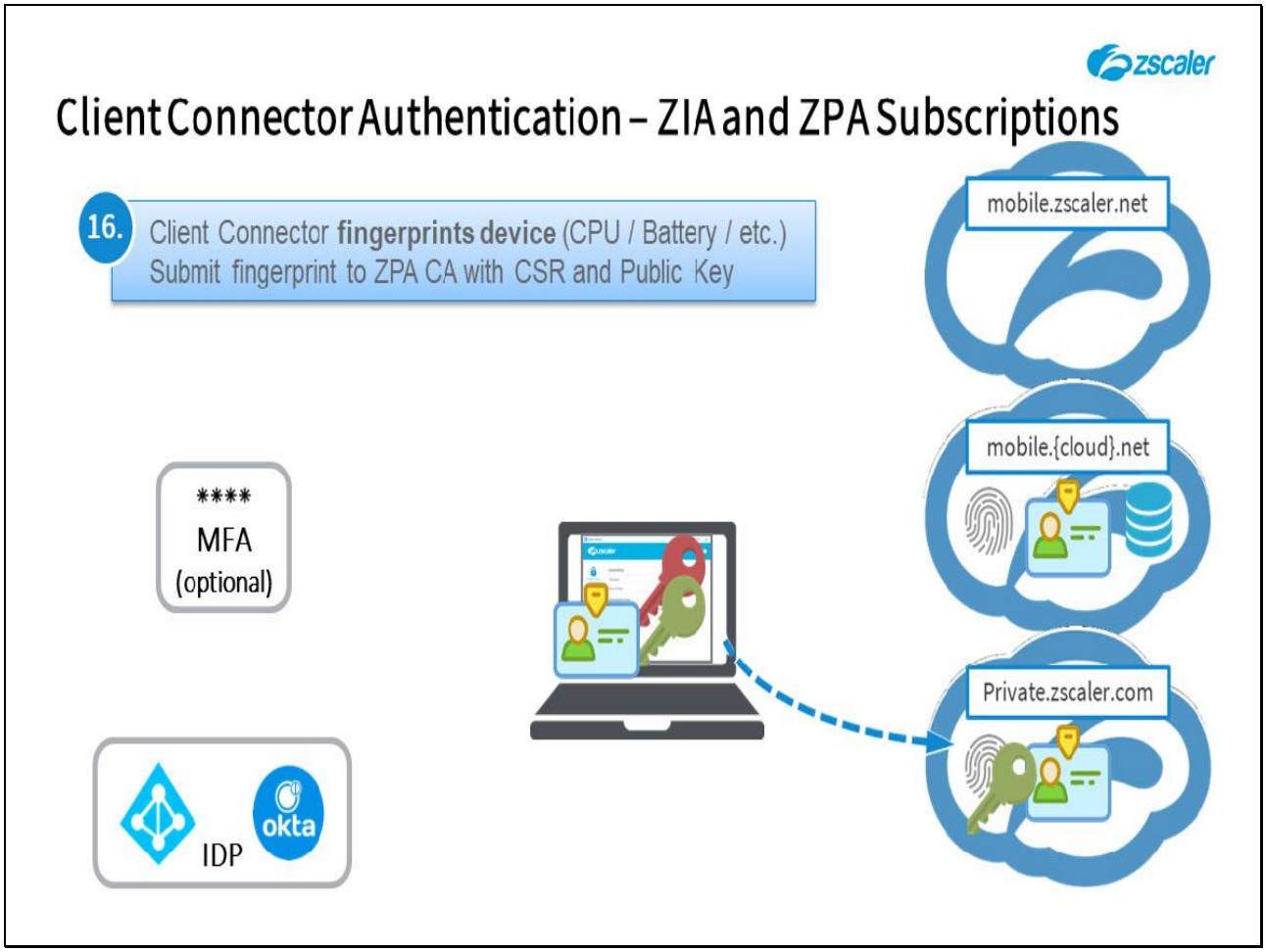
Slide 45 - Zscaler App Authentication



Slide notes

15. The Client Connector then generates its own public/private key pair, which are encrypted and stored within the Client Connector itself.

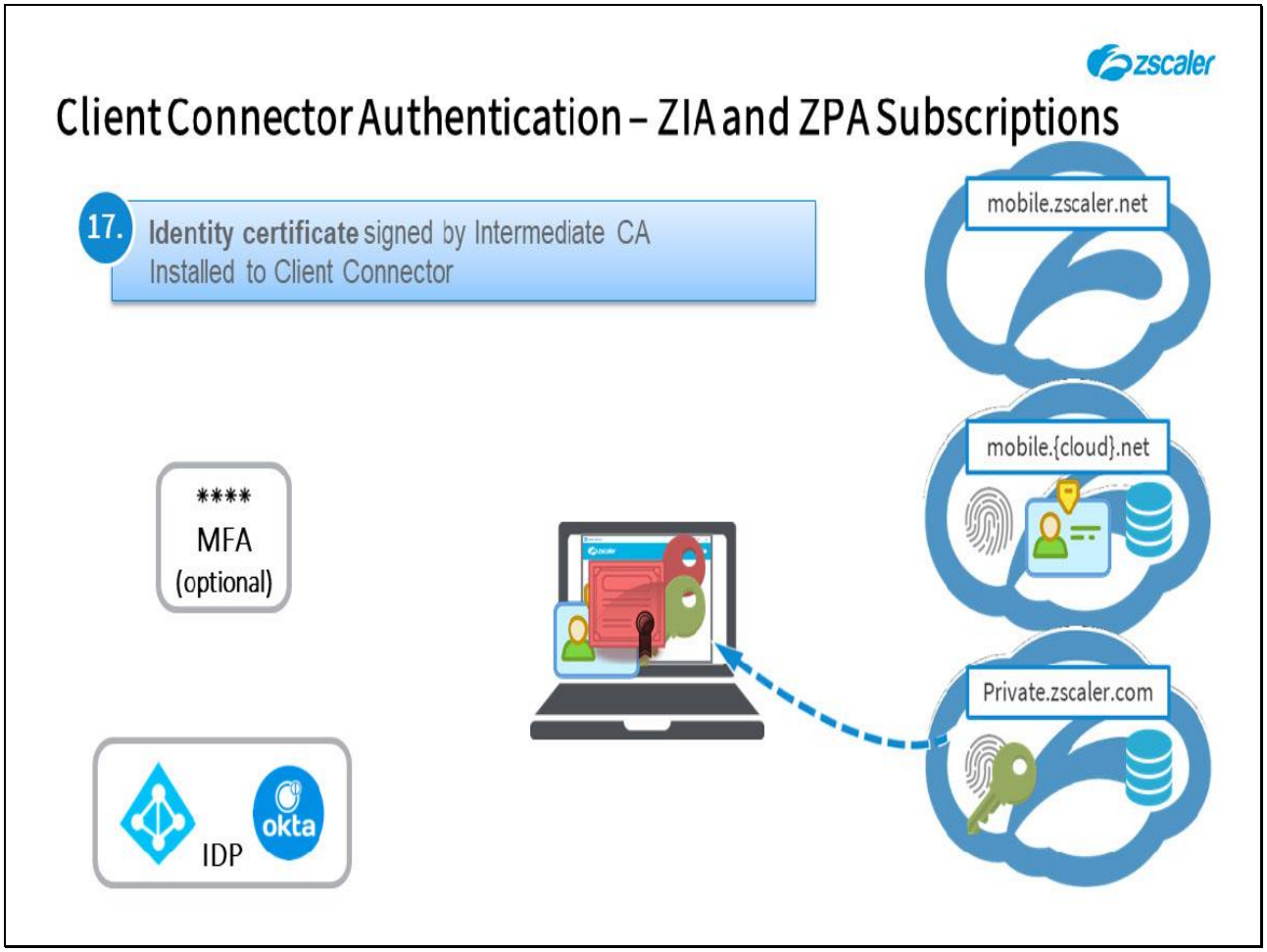
Slide 46 - Zscaler App Authentication



Slide notes

16. The Client Connector fingerprints the device, then submits the fingerprint and a certificate signing request (CSR) containing its public key, to the ZPA Central Authority.

Slide 47 - Zscaler App Authentication



Slide notes

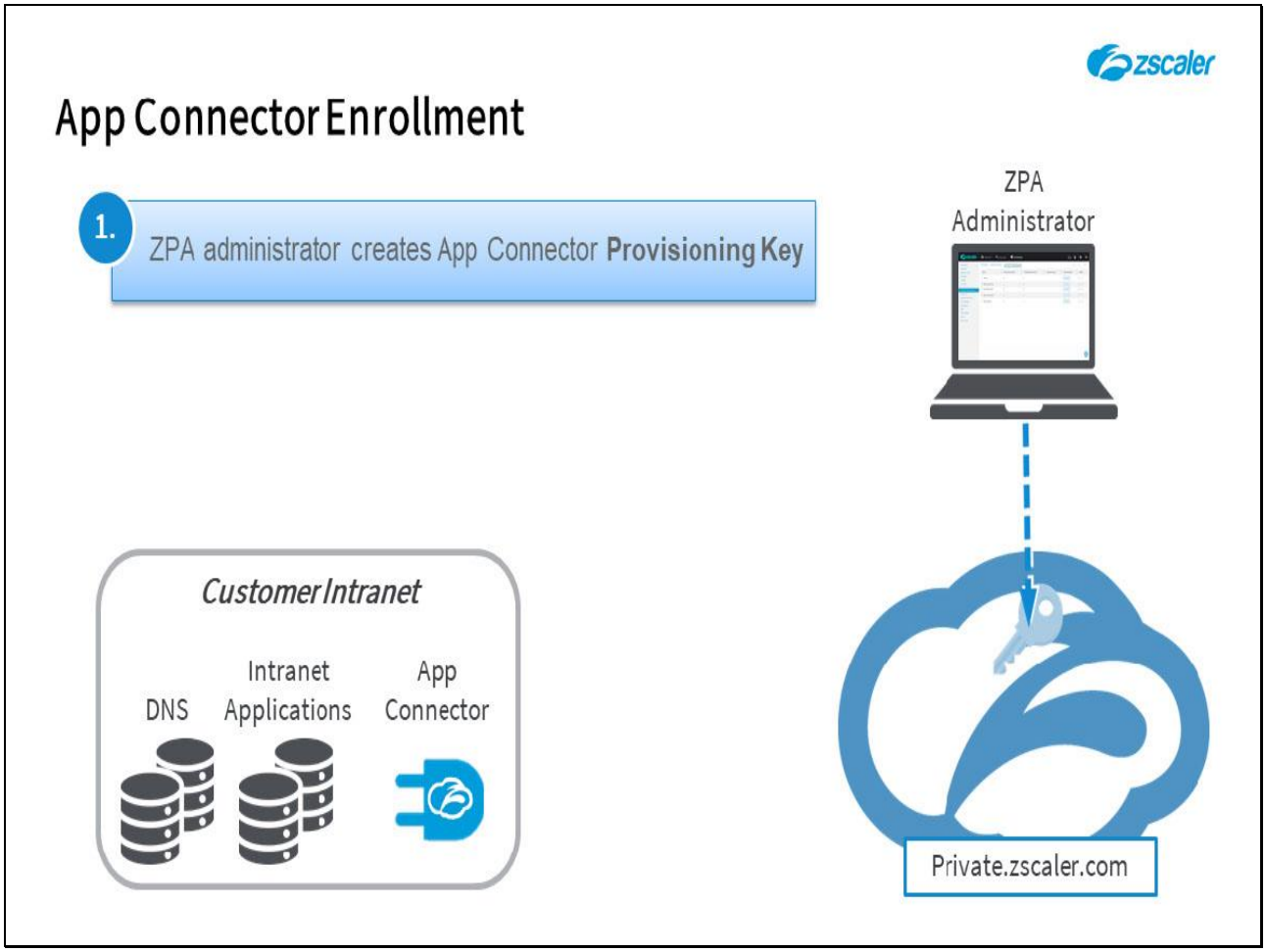
17. The CSR is signed by the appropriate organization's Subsidiary CA and the identity certificate is returned to the Client Connector. It is securely stored in a private certificate store within the Client Connector and used to authenticate Z Tunnels from the Client Connector to the ZPA infrastructure on every application connection attempt.

Slide 48 - ZEN Connector Enrollment

Slide notes

Now let’s have a look at how App Connector enrollment is achieved.

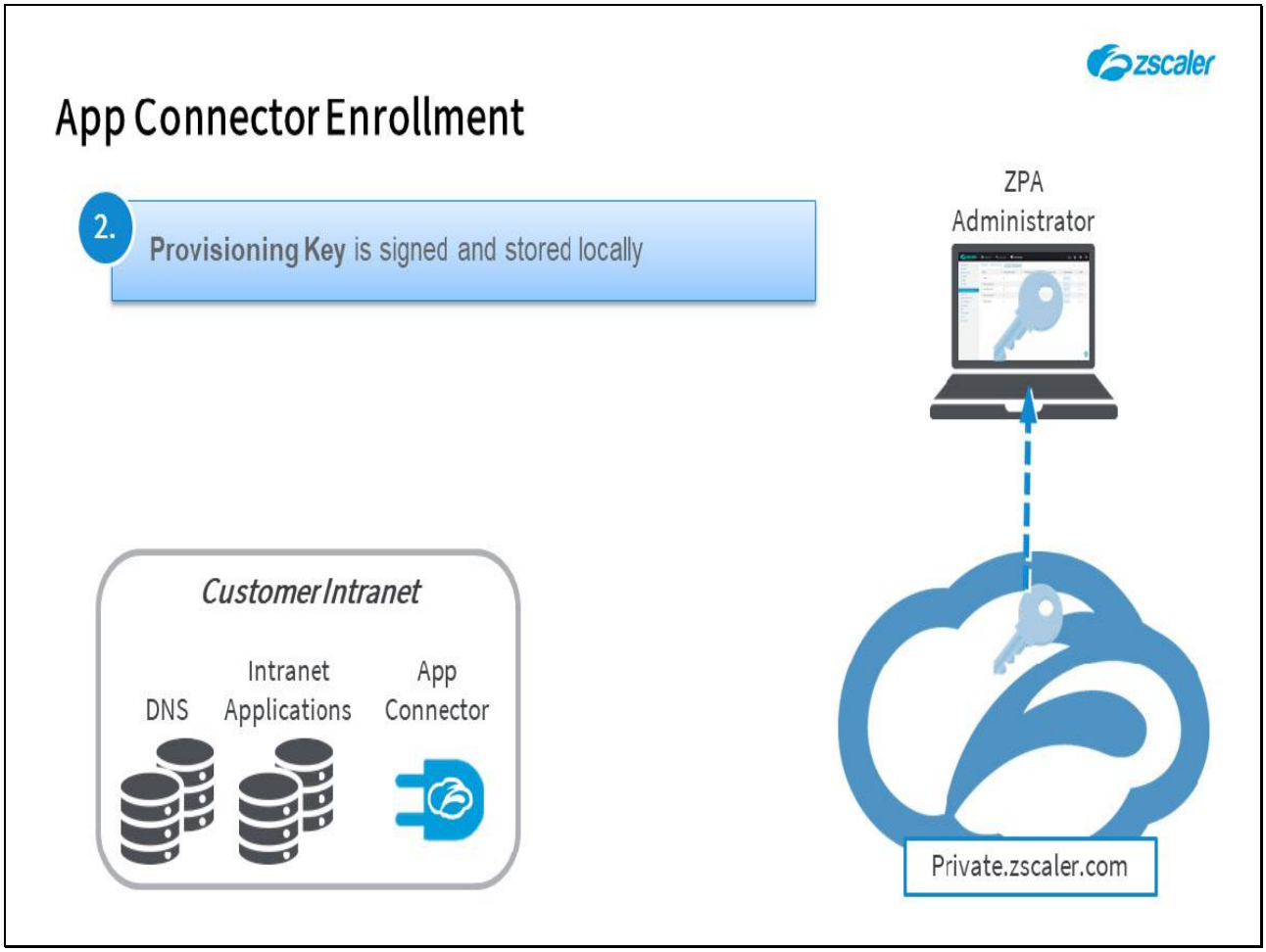
Slide 49 - ZEN Connector Enrollment



Slide notes

1. The first step in the process to enroll an App Connector, is for the ZPA administrator to generate an App Connector **Provisioning Key** at the ZPA Admin Portal.

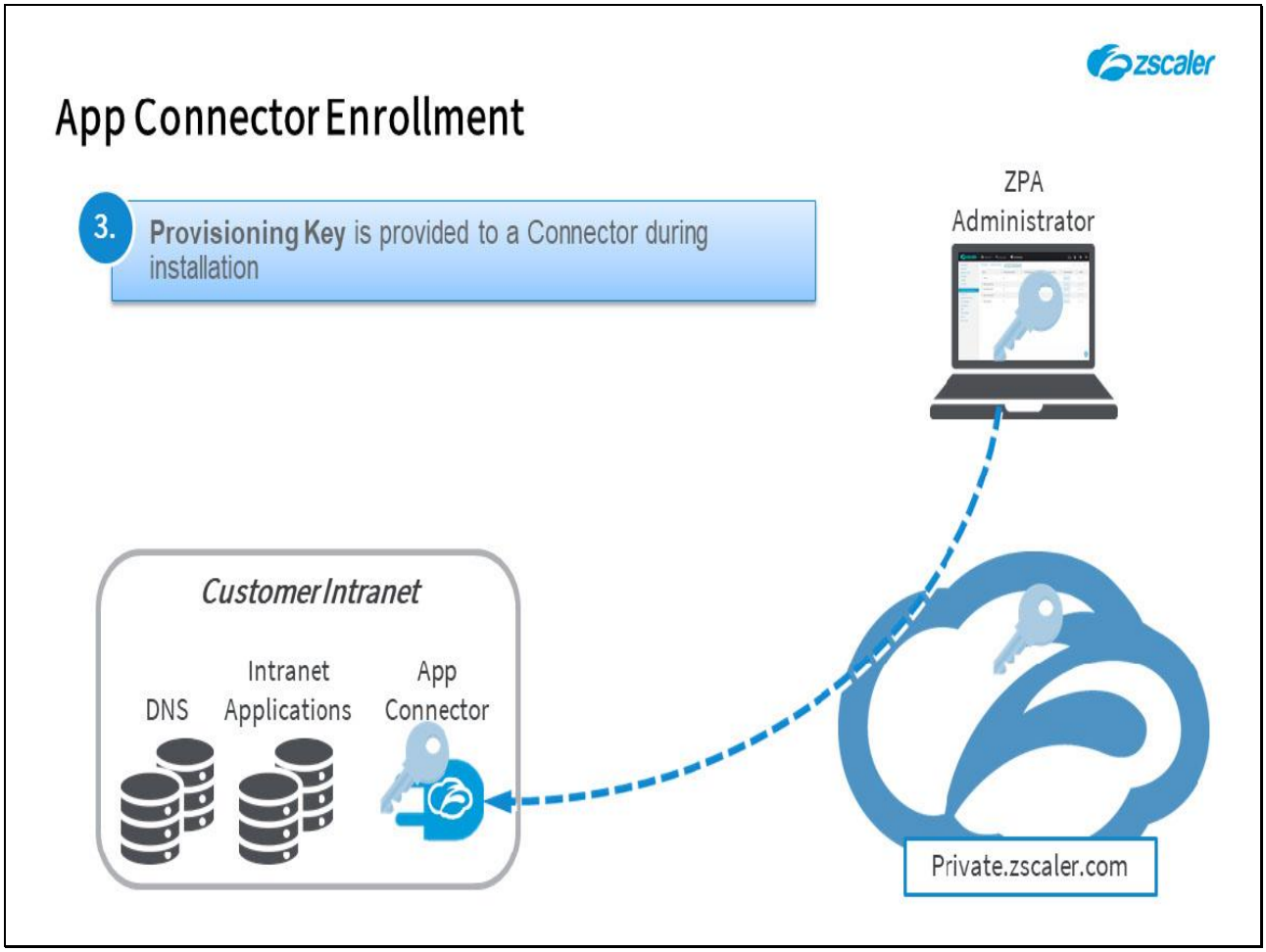
Slide 50 - ZEN Connector Enrollment



Slide notes

2. The **Provisioning Key** is signed by the appropriate Subsidiary CA and is stored locally by the administrator.

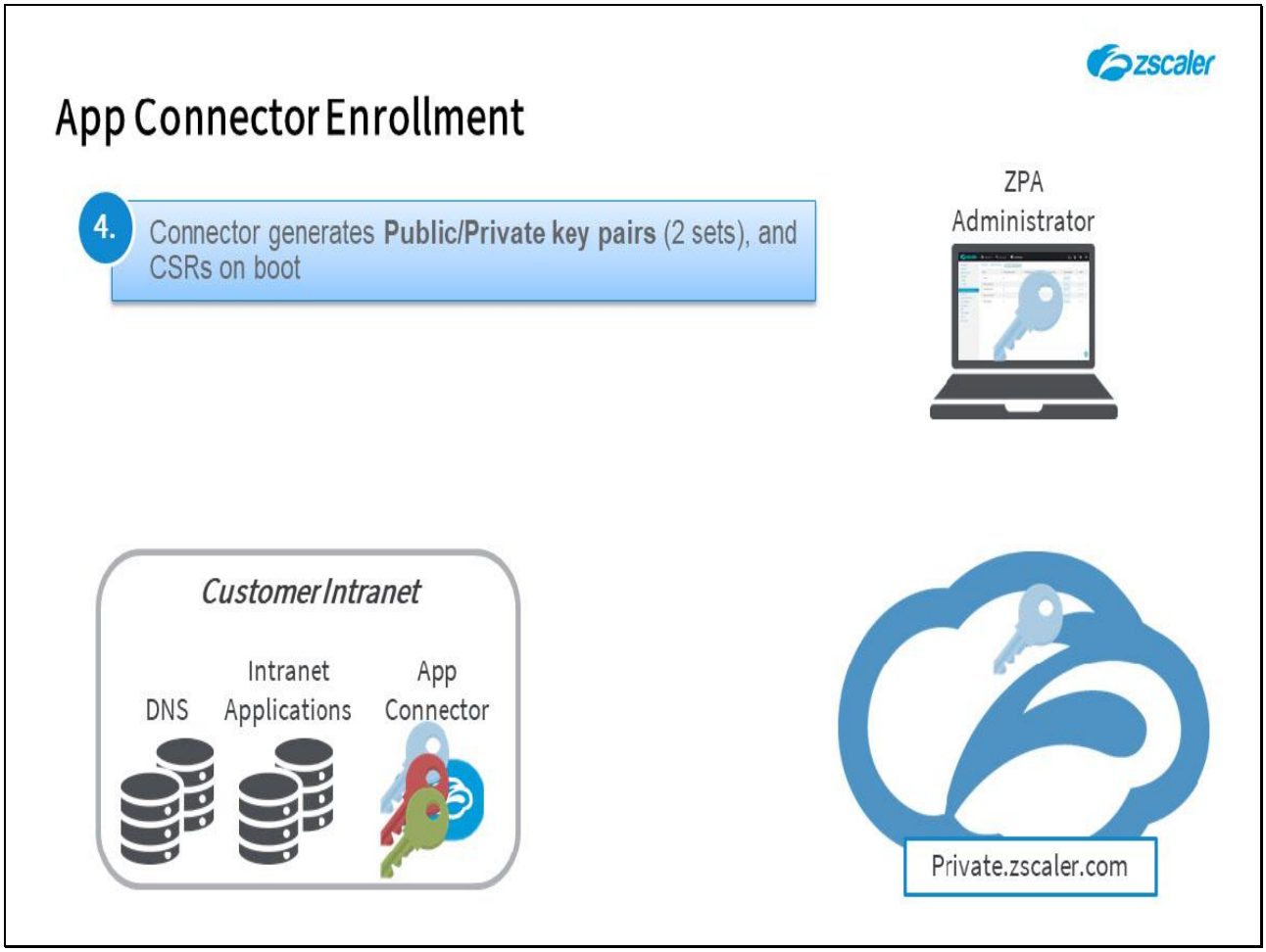
Slide 51 - ZEN Connector Enrollment



Slide notes

3. When installing the App Connector, the **Provisioning Key** is installed to it.

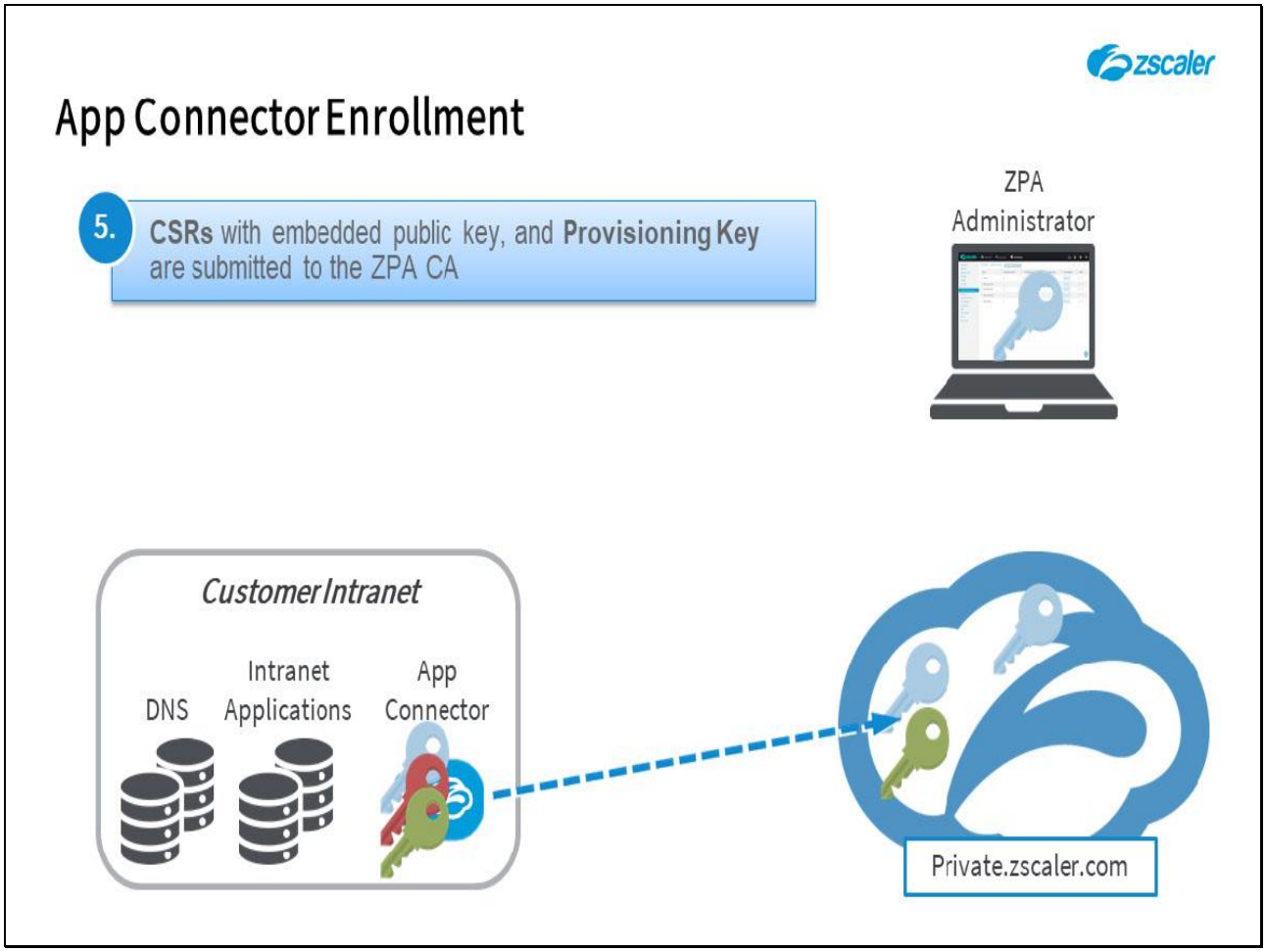
Slide 52 - ZEN Connector Enrollment



Slide notes

4. On first time boot, the App Connector generates:
    - Its own public/private key pairs (one for the identity certificate and one for the server certificate);
    - A certificate signing request for an identity certificate;
    - And a CSR for a server certificate.

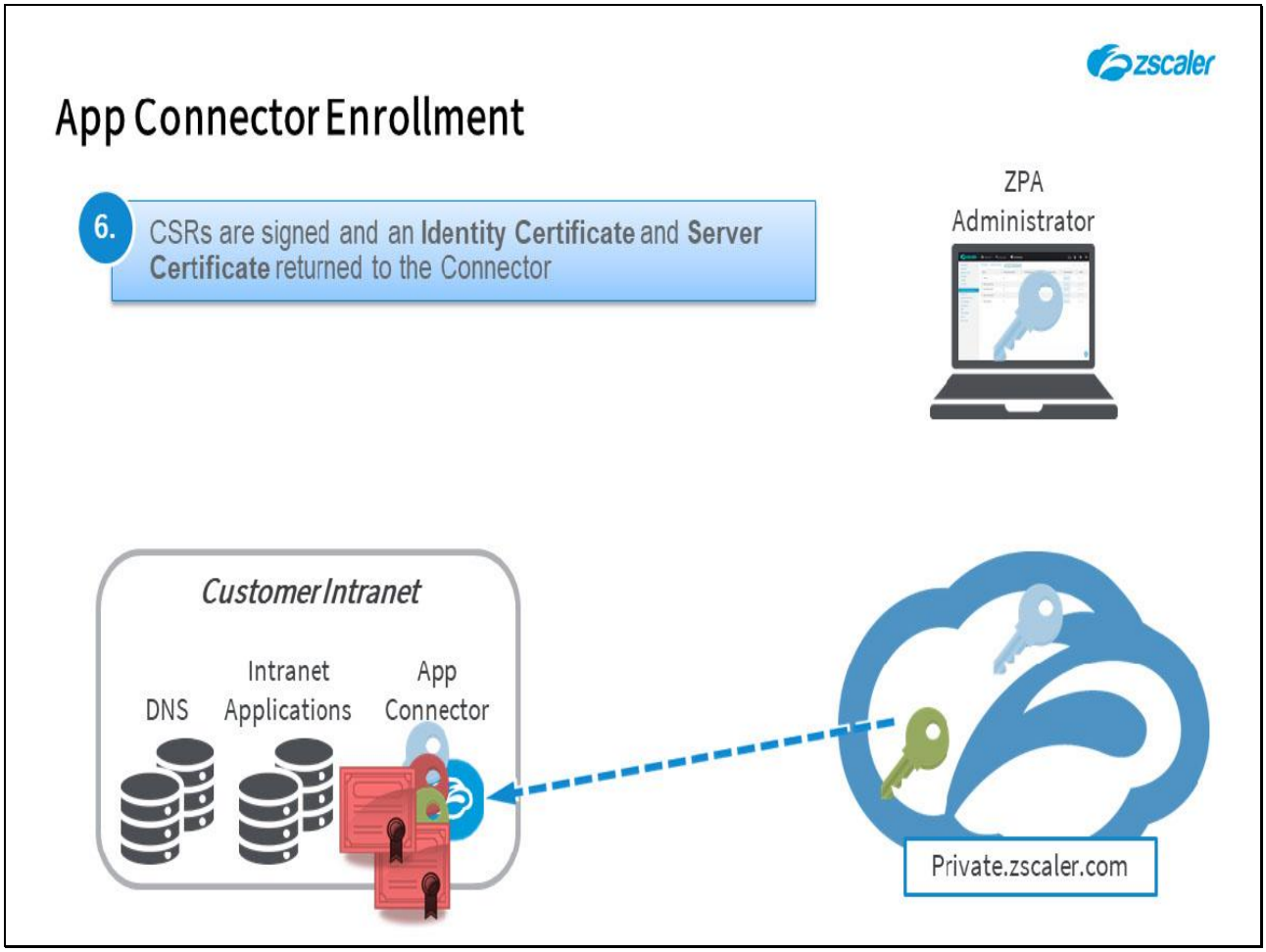
Slide 53 - ZEN Connector Enrollment



Slide notes

5. The CSRs with embedded public keys and the **Provisioning Key** (for validation) are all submitted to the ZPA CA on a secure connection.

Slide 54 - ZEN Connector Enrollment



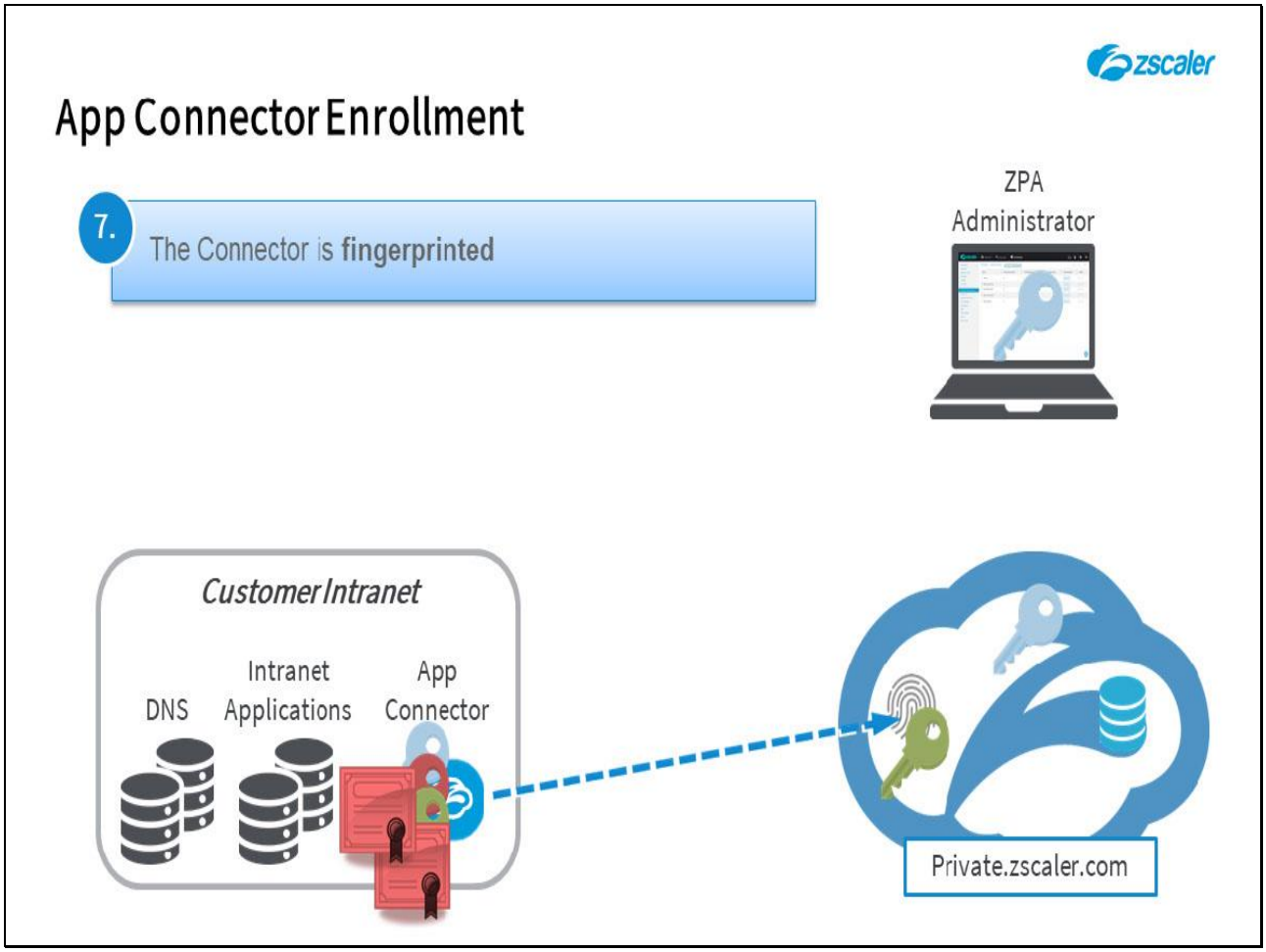
Slide notes

6. The CSRs are signed by the appropriate Subsidiary CA and returned to the App Connector.

   The identity certificate is used to authenticate Z Tunnel connections initiated by the App Connector to the ZPA infrastructure.

   The server certificate is used to establish the end-to-end TLS connections required for **Double Encrypted** applications.

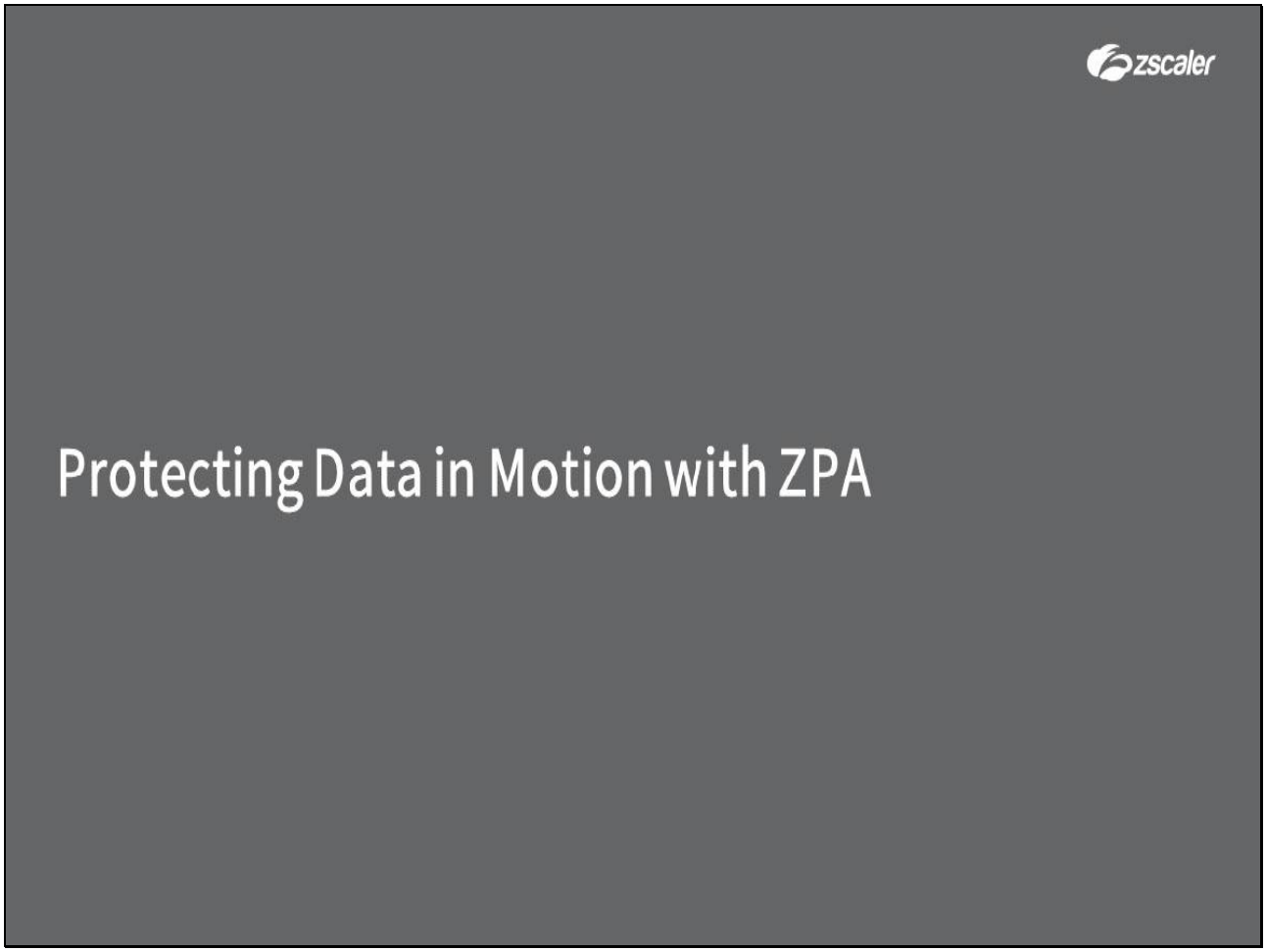
Slide 55 - ZEN Connector Enrollment



Slide notes

7. Finally, the App Connector is fingerprinted to prevent cloning.

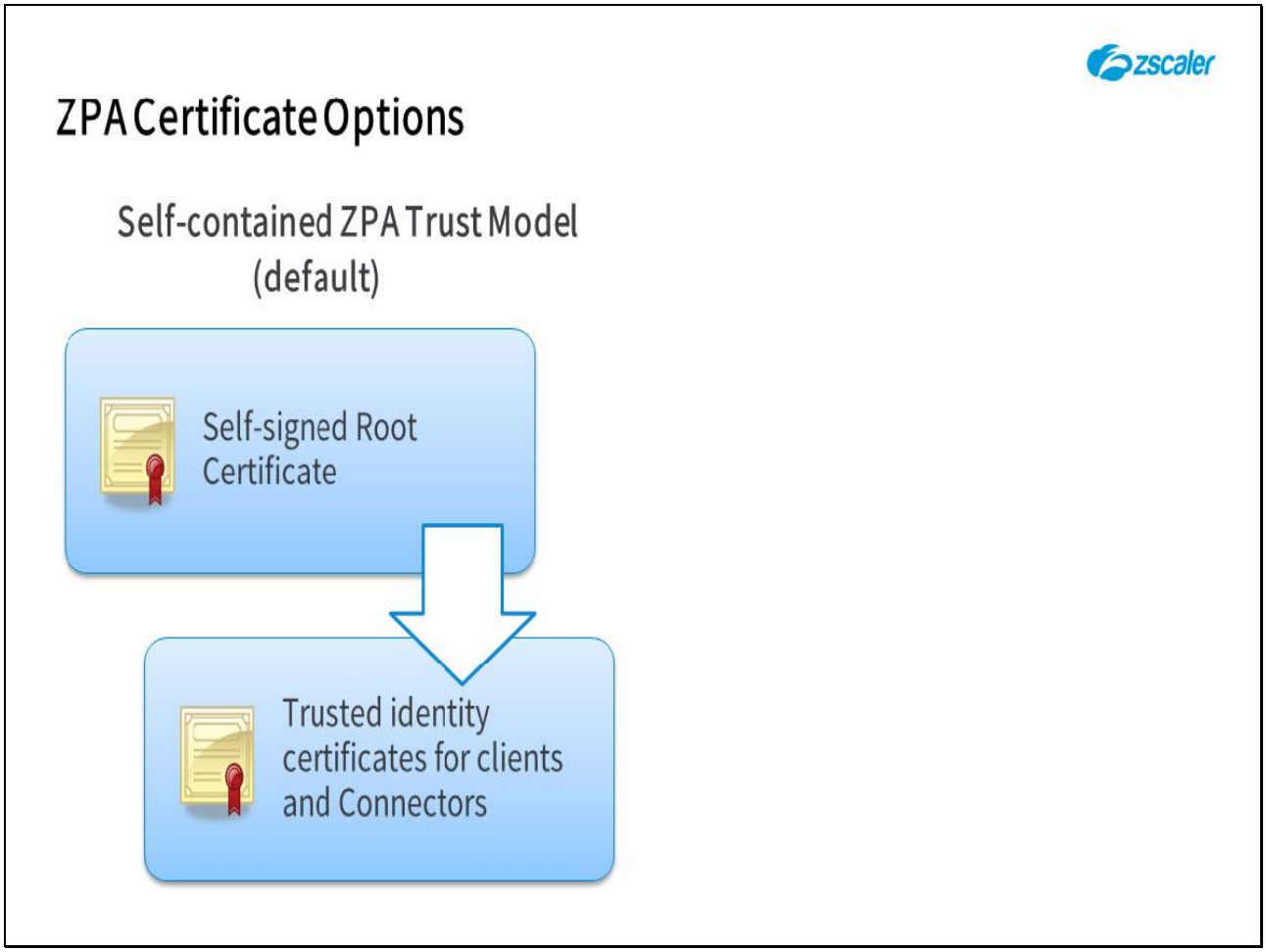
Slide 56 - Protecting Data in Motion with ZPA



Slide notes

The next topic we will cover is how ZPA is used to protect data in motion.

Slide 57 - ZPA Certificate Options



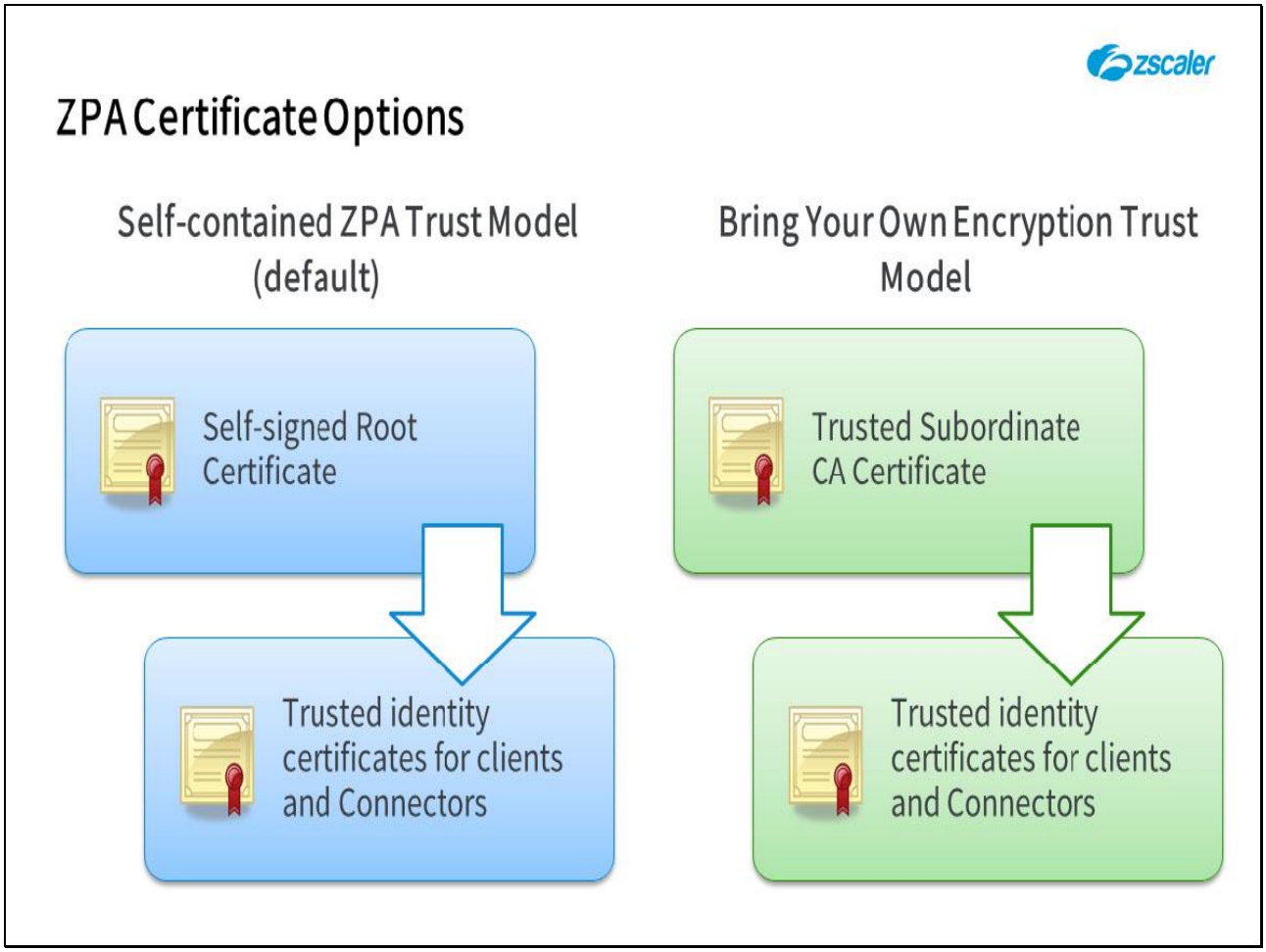
Slide notes

Let's talk about the trust model options for ZPA, of which there are two:

1. Firstly, you have the option within the ZPA Admin Portal to generate a new self-signed root certificate for your ZPA instance and subsequently generate the identity certificates required by both the Client and App Connectors for authentication based upon it. Essentially you create a new stand-alone and self-contained certificate authority just to deploy the identity certificates to your ZPA infrastructure, that are then used for authenticating the Z Tunnel connections.

   Note that a self-signed root certificate and subsidiary CAs for Client and App Connectors are provided by default on any new ZPA instance.

Slide 58 - ZPA Certificate Options



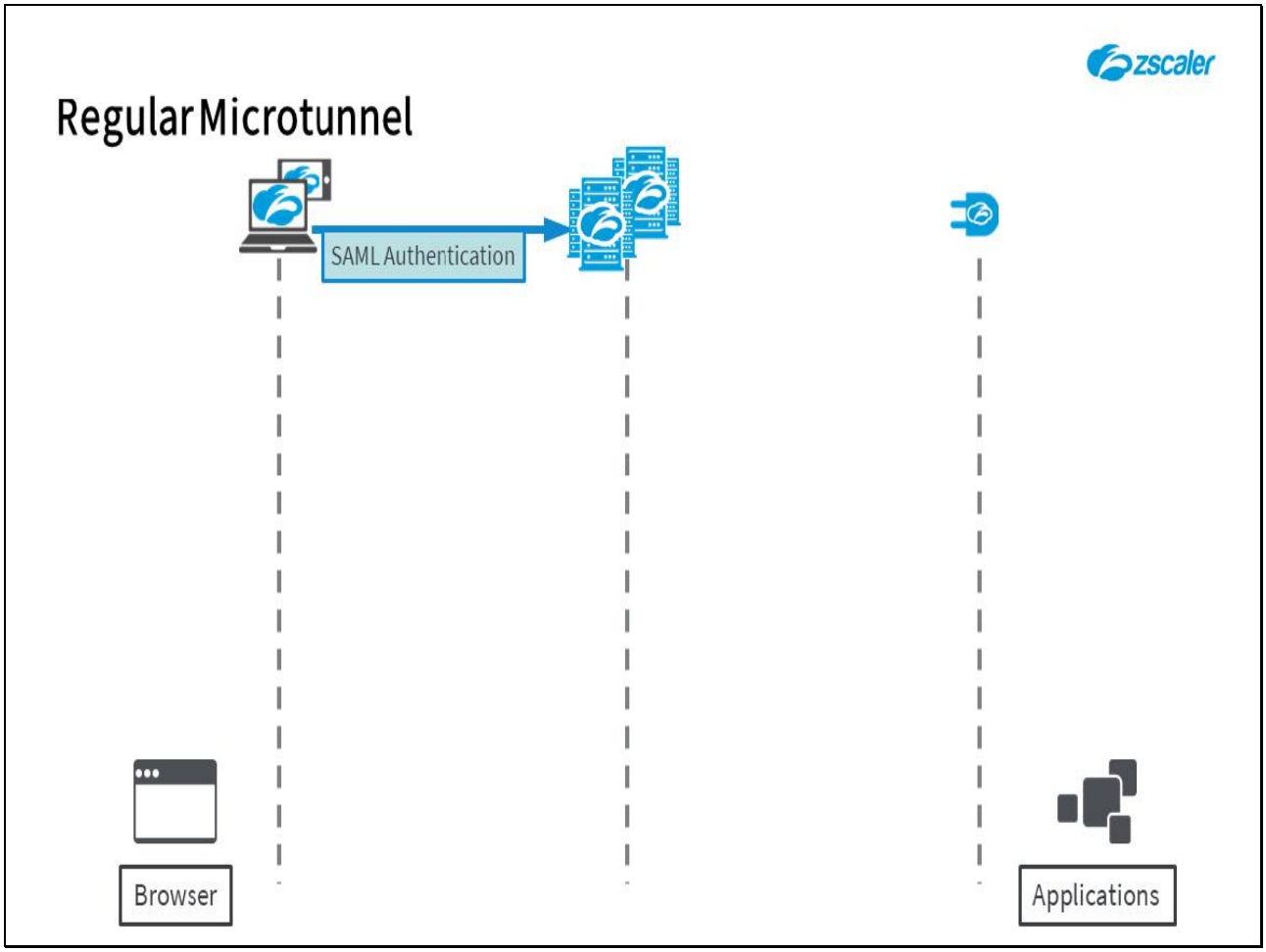
Slide notes

2. Your other option is to request a certificate for ZPA from your preferred external private CA, that then allows ZPA to act as a subordinate CA. This will most likely be an enterprise private root CA that is under your management control. Note that public CAs are not suitable for this use case, as certificates purchased do not support the signing of subordinate certificates.

   The identity certificates for Client and App Connectors can then be generated from this trusted subordinate CA, providing a trust chain all the way back to the external trusted root CA. Note that this option requires you to load all the intermediate certificates in the trust chain.

   All certificates that are part of the ZPA system, including all customer-operated systems, have private keys that never leave the physical device in which they were generated.

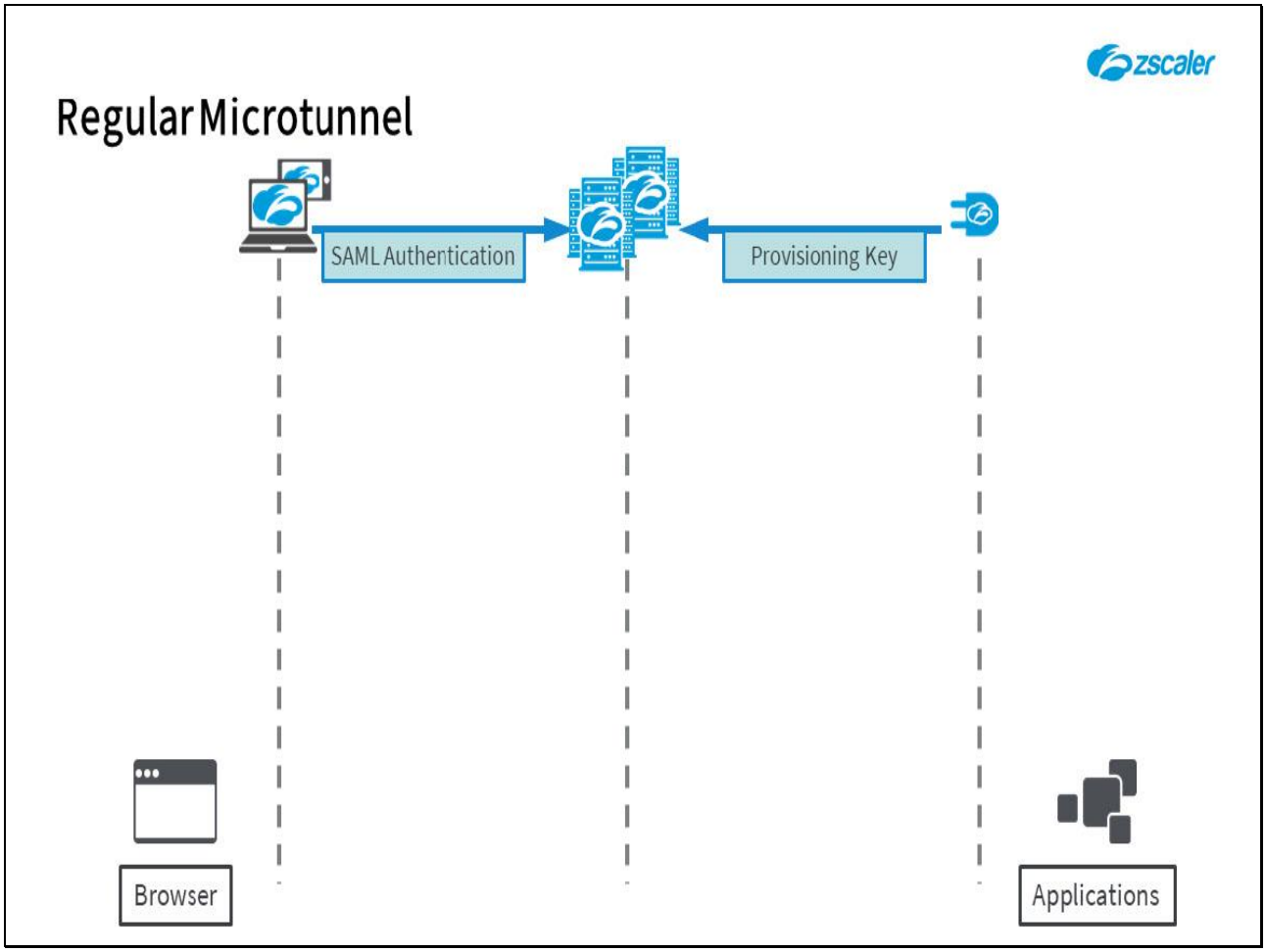
Slide 59 - Regular Microtunnel



Slide notes

The first requirement for any ZPA connectivity is to authenticate the end points, as described earlier. End users must authenticate using SAML against the specified IdP, using the required method.

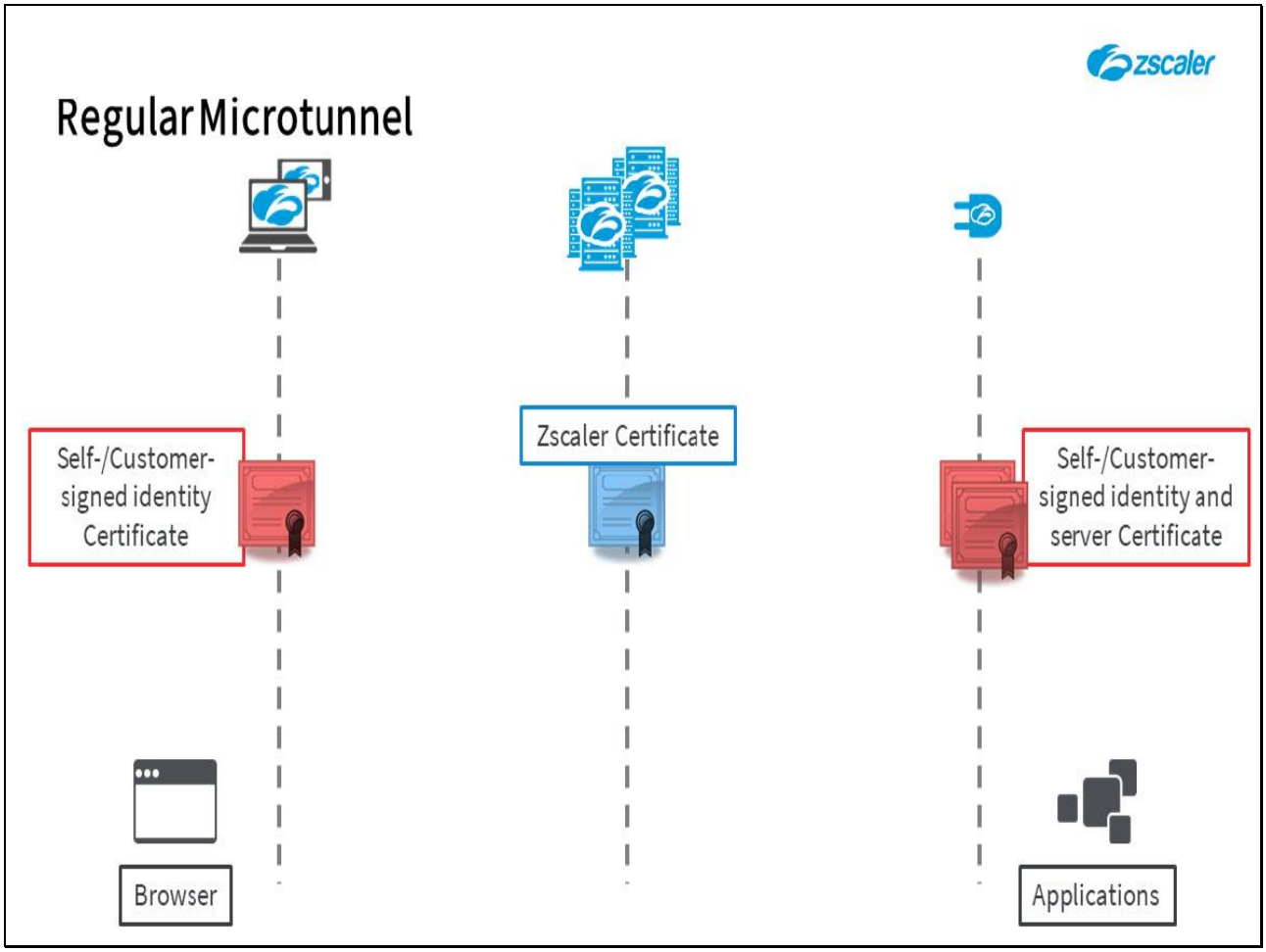
Slide 60 - Regular Microtunnel



Slide notes

App Connectors are enrolled using a **Provisioning Key** deployed to them on activation by an administrator.

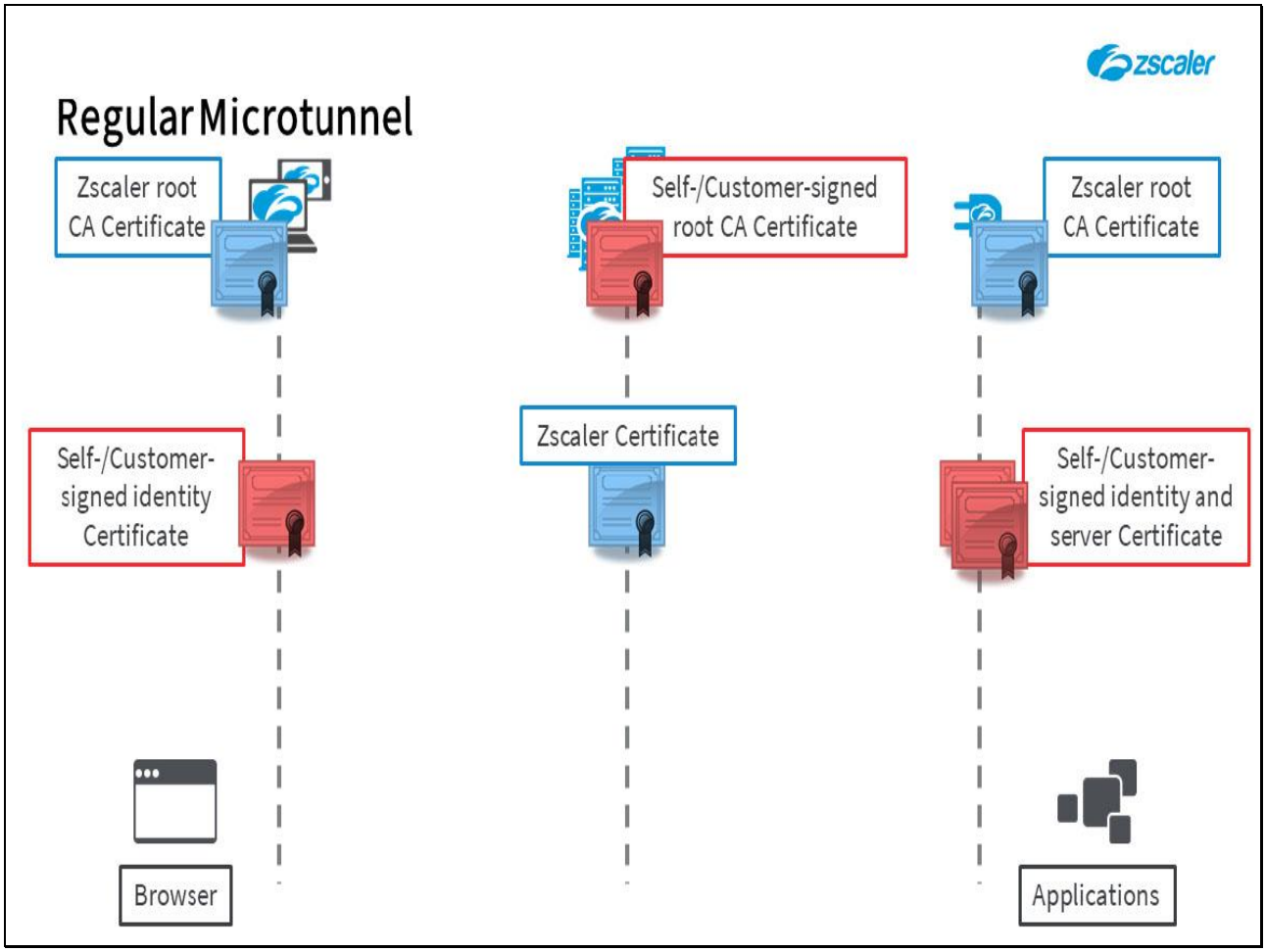
Slide 61 - Regular Microtunnel



Slide notes

Z Tunnels are built using certificates deployed from the ZPA Admin Portal. The ZPA Service Edges use a Zscaler-signed certificate, while the end points (Client and App Connectors) may receive either a self-signed or customer-signed certificate, depending on customer preference.

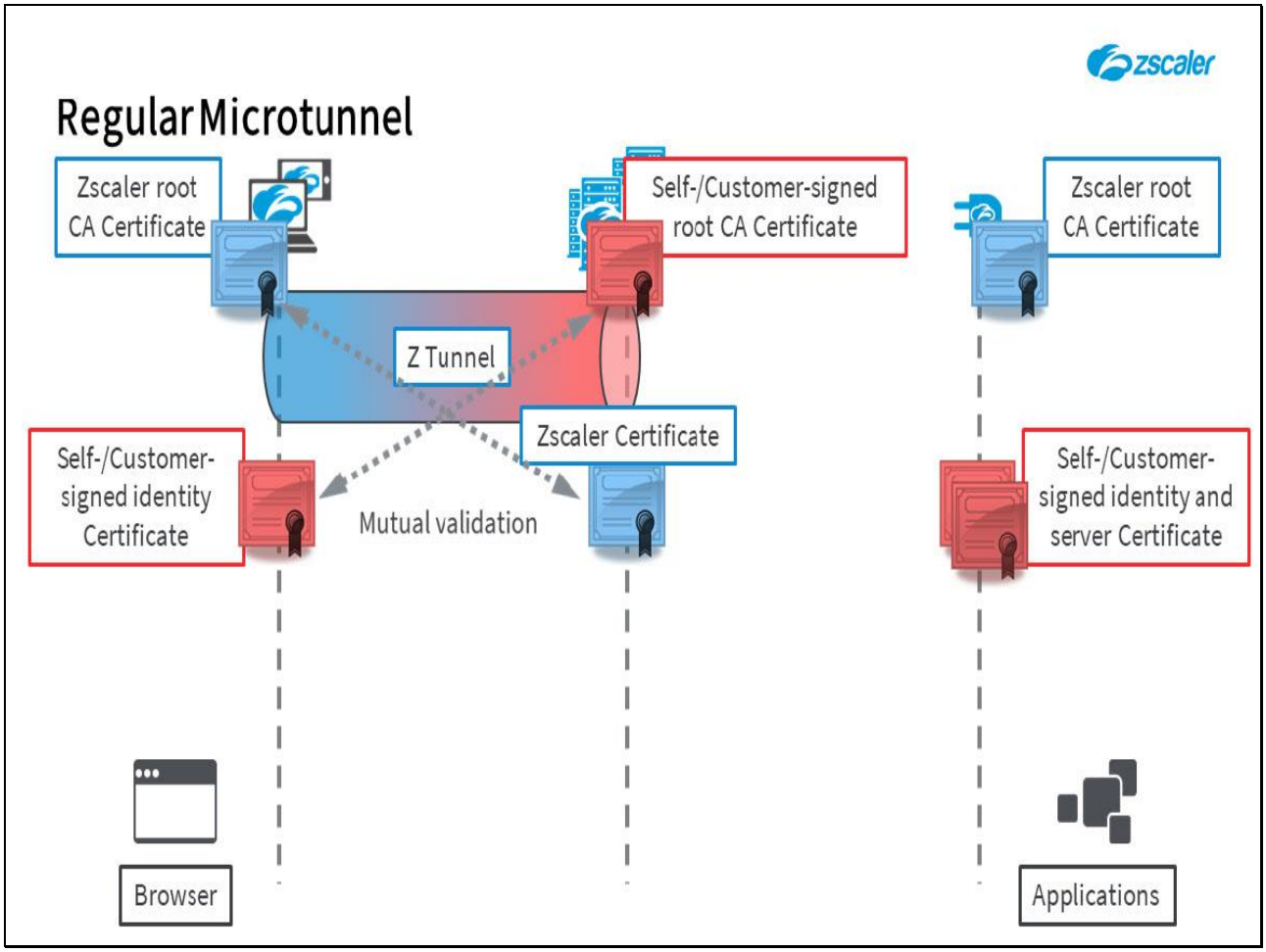
Slide 62 - Regular Microtunnel



Slide notes

Each component is provided with the appropriate Root CA certificate, to allow them to establish trust on each of the connections. The Client and App Connectors receive the Zscaler Root CA certificate and ZPA Service Edges the appropriate CA certificate used by the customer, which may be self- or customer-signed.

Slide 63 - Regular Microtunnel

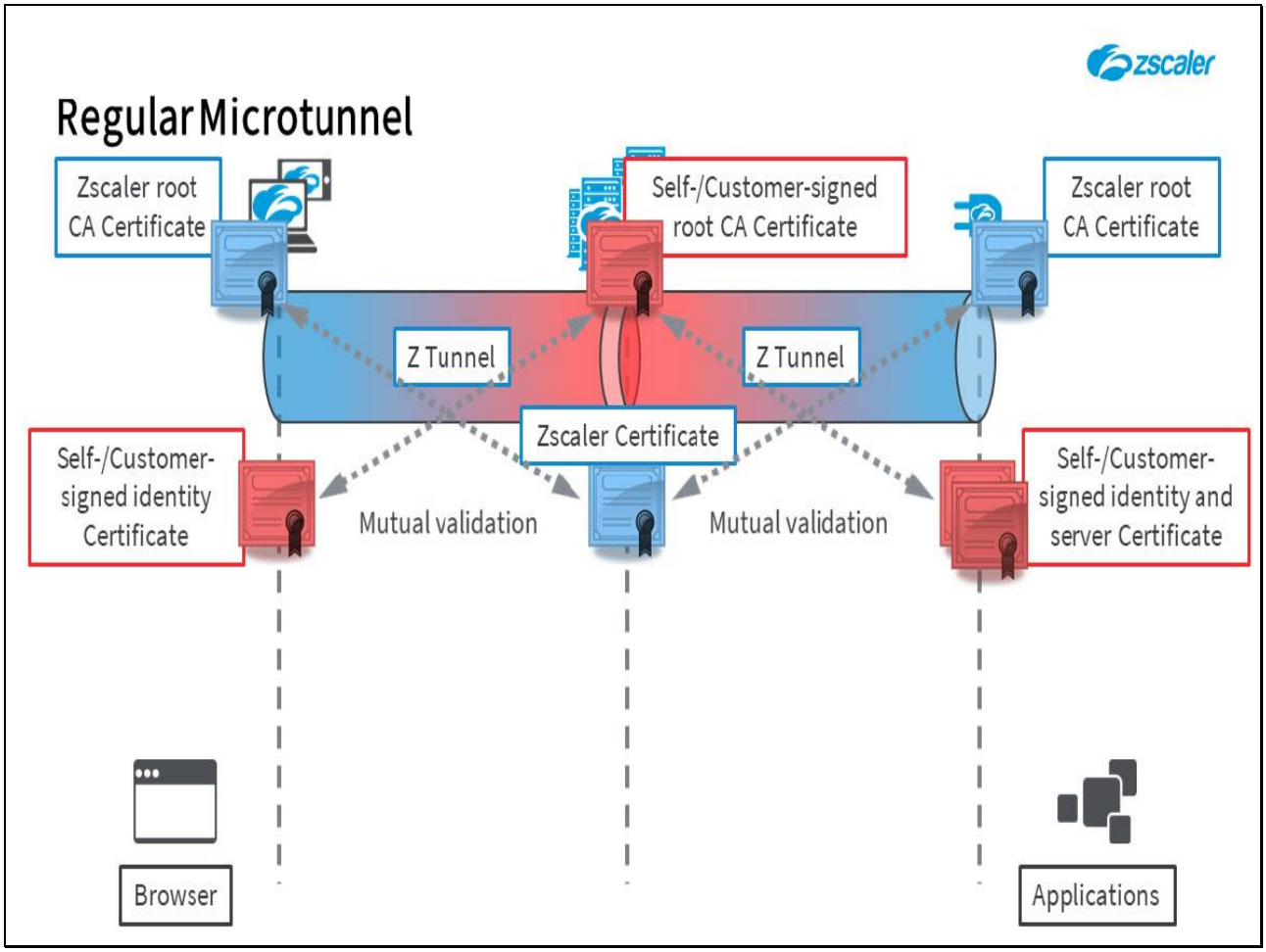


Slide notes

Z Tunnels are established and mutually validated using the deployed certificates. For the Client Connector the tunnel is established in the outbound direction to the nominated ZPA Service Edge using the standard TLS 1.2 tunnel setup negotiation on port 443. As the Client Connector possesses the Zscaler root CA certificate, it can validate the server certificate it receives from the Service Edge during tunnel establishment.

Similarly, as the customer has previously created or installed a root CA certificate through the ZPA-CA, the Zscaler infrastructure can validate the identity certificate presented by the Client Connector.

Slide 64 - Regular Microtunnel

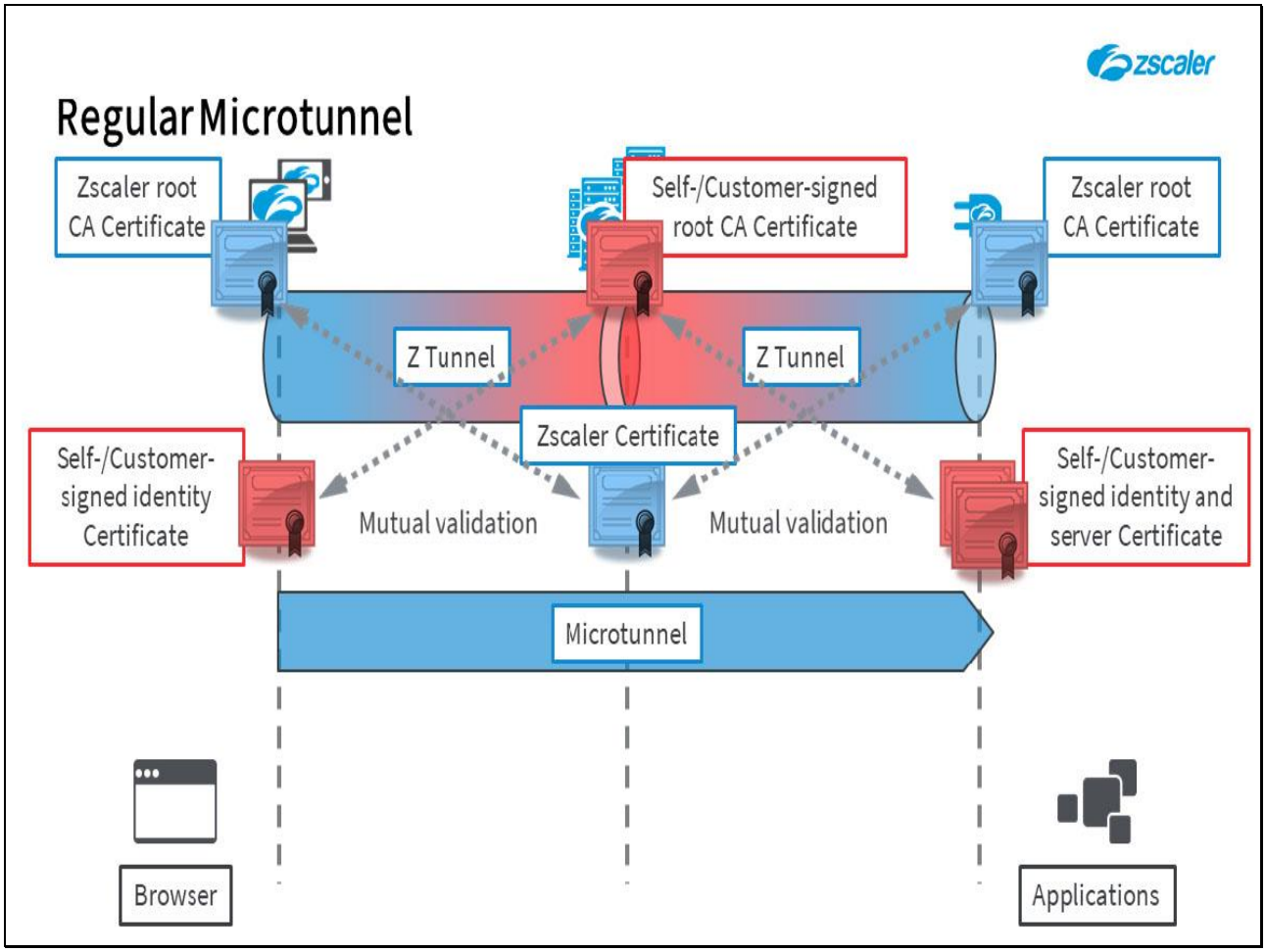


Slide notes

The Z Tunnel from the App Connectors is established in the exact same way, as an outbound connection from the App Connector to the nominated ZPA Service Edge. Once again mutual certificate validation is done, with the App Connector presenting the identity certificate it received during enrollment.

These tunnels are encrypted using the strongest cipher that is mutually supported by the Client and App Connector hosts at one end and the ZPA Service Edges at the other.

Slide 65 - Regular Microtunnel

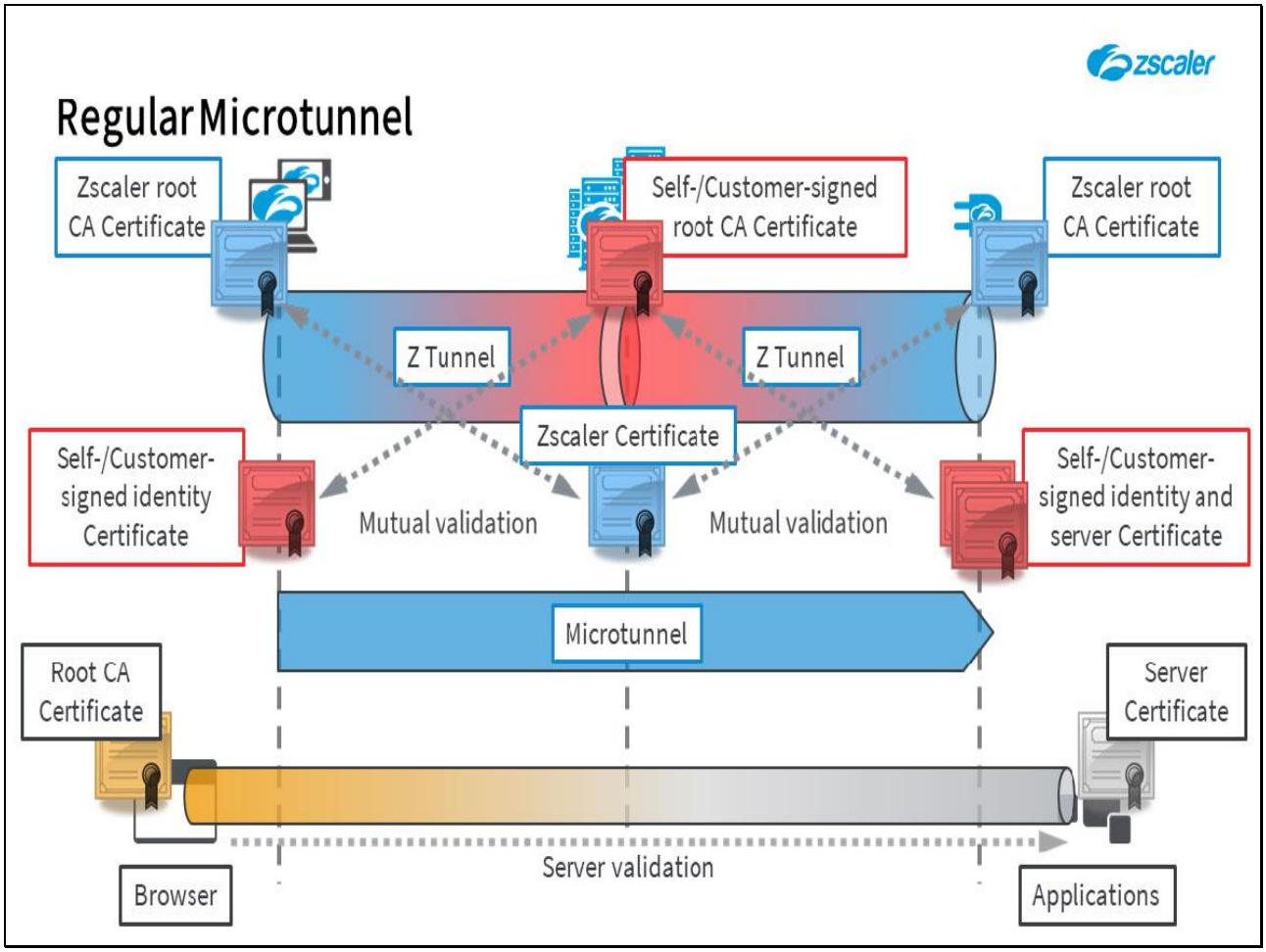


Slide notes

Once the Z Tunnels are in place, traffic can be sent from the Client Connector to the App Connector based on the labels that they previously generated, to provide the end-to-end Microtunnel. Remember, Microtunnels are user and application specific, a Microtunnel cannot be used by any other user, nor can it be used to connect to an application other than the one originally requested by the user.

Note that under these circumstances, the Microtunnel is not separately encrypted and in principal Zscaler could view and scan traffic as it transits the ZPA Service Edge (although this is not done currently).

Slide 66 - Regular Microtunnel

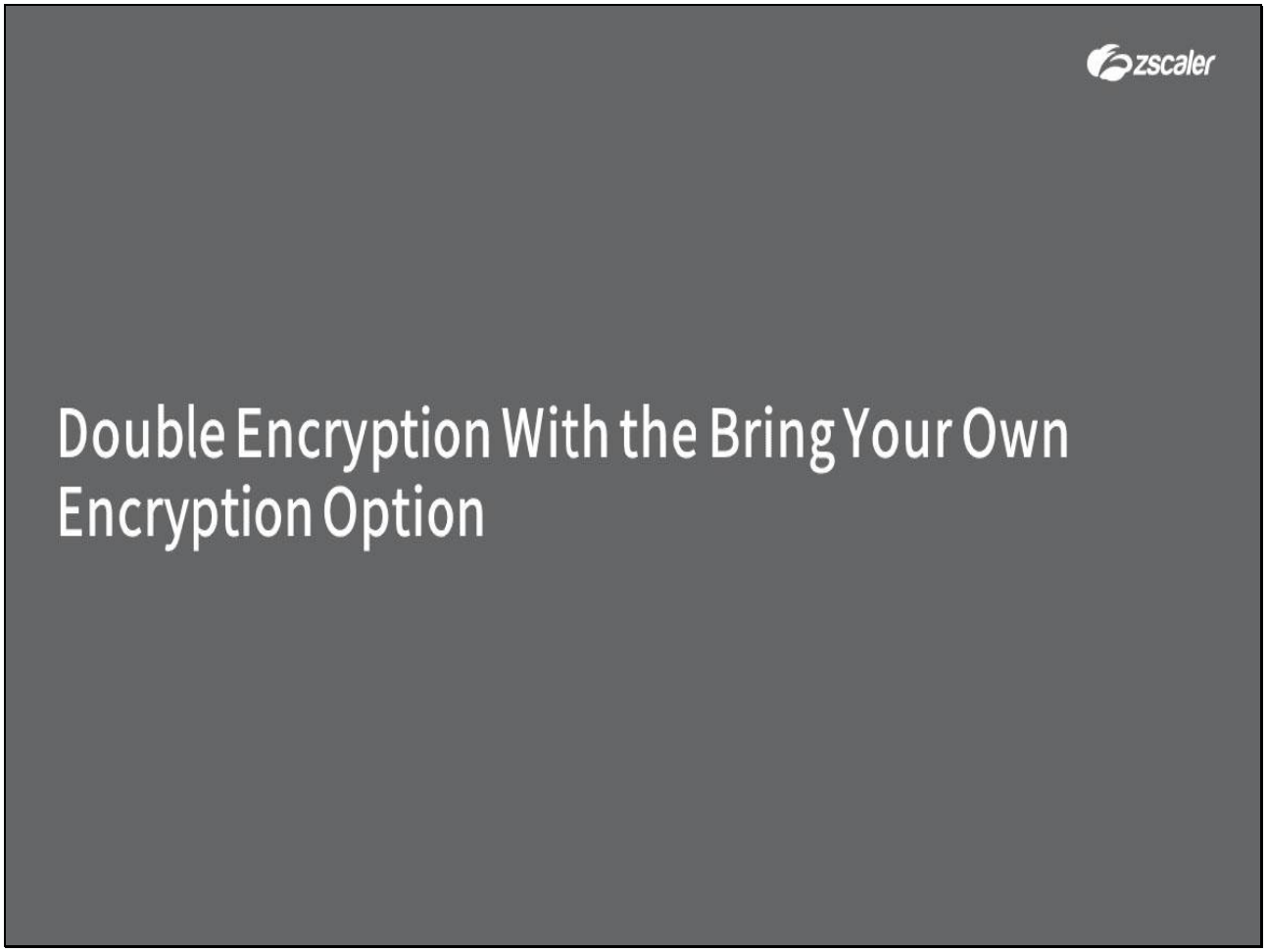


Slide notes

In addition to the layers of encryption provided by Zscaler, if the applications themselves use HTTPS then TLS encryption is established end-to-end within the Microtunnels based on the server certificate, which can be validated at the client by the appropriate Root CA certificate.

With such end-to-end encryption in place, Zscaler has no visibility into any data transferred between the client and application.

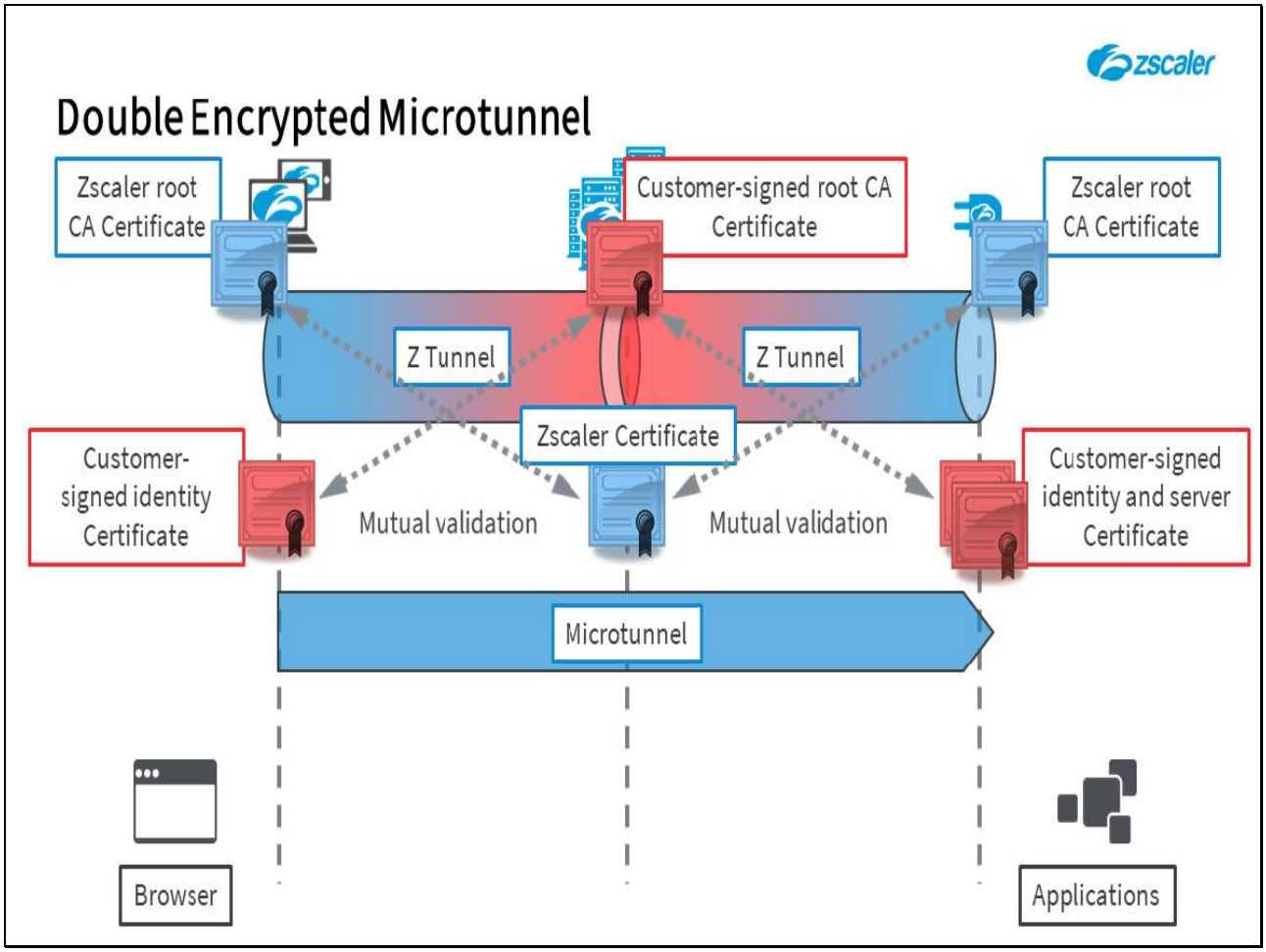
Slide 67 - ZPA Bring Your Own Encryption Option



Slide notes

Next, let’s have a look at the **Double Encryption** option for applications, using BYOE certificates.

Slide 68 - Double Encrypted Microtunnel

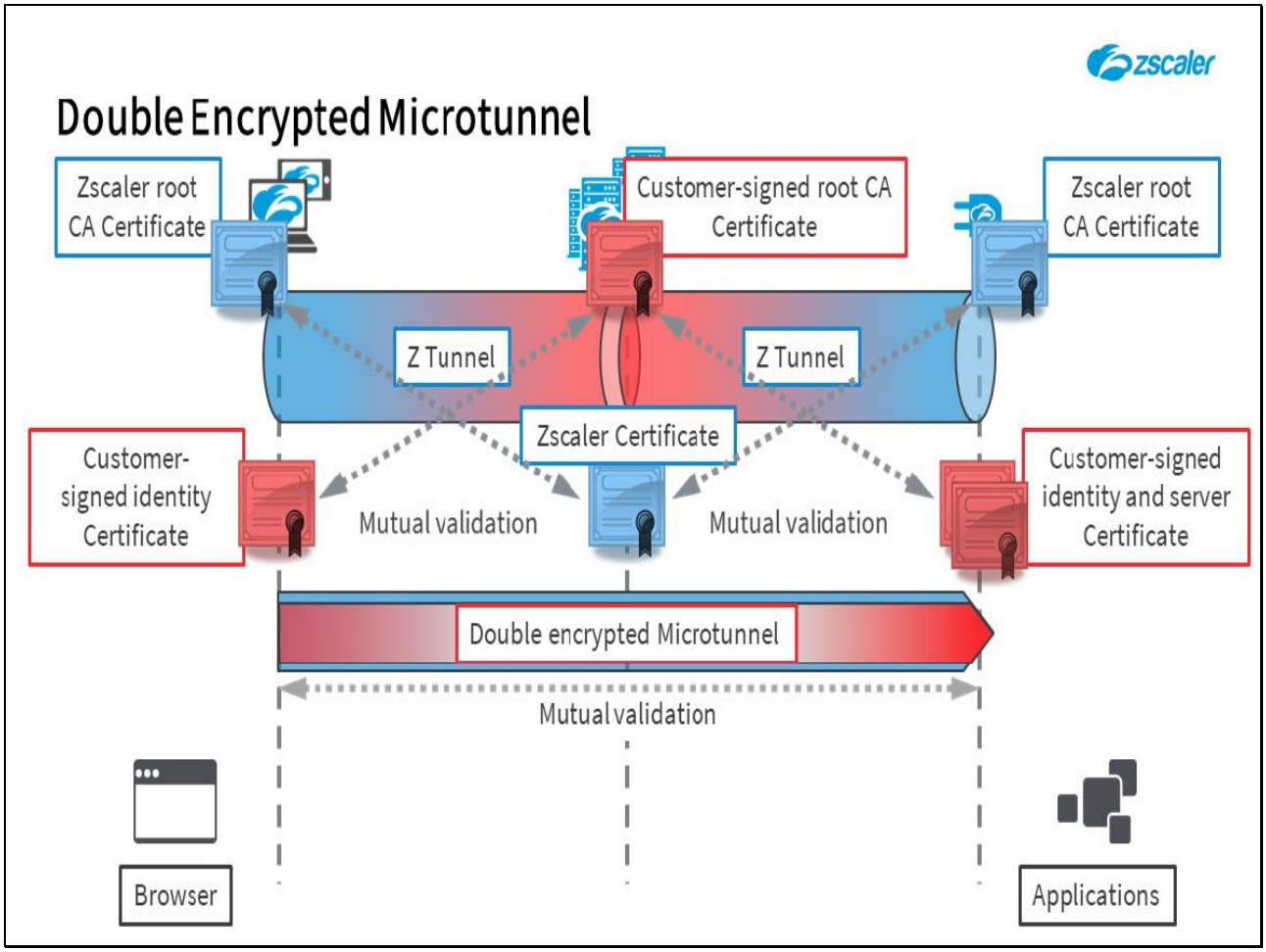


Slide notes

For those customers who do not want to expose their internal traffic and data even to Zscaler, it is possible to enable **Double Encryption** for application connections. With **Double Encryption** enabled, Z Tunnels are established in the exact same way, although in this case the certificates used should be provided by the customer from a trusted external CA. Note that, while it would be possible to enable double encryption using self-signed certificates, this provides no additional privacy.

The end-to-end Microtunnels are established as before, …

Slide 69 - Double Encrypted Microtunnel

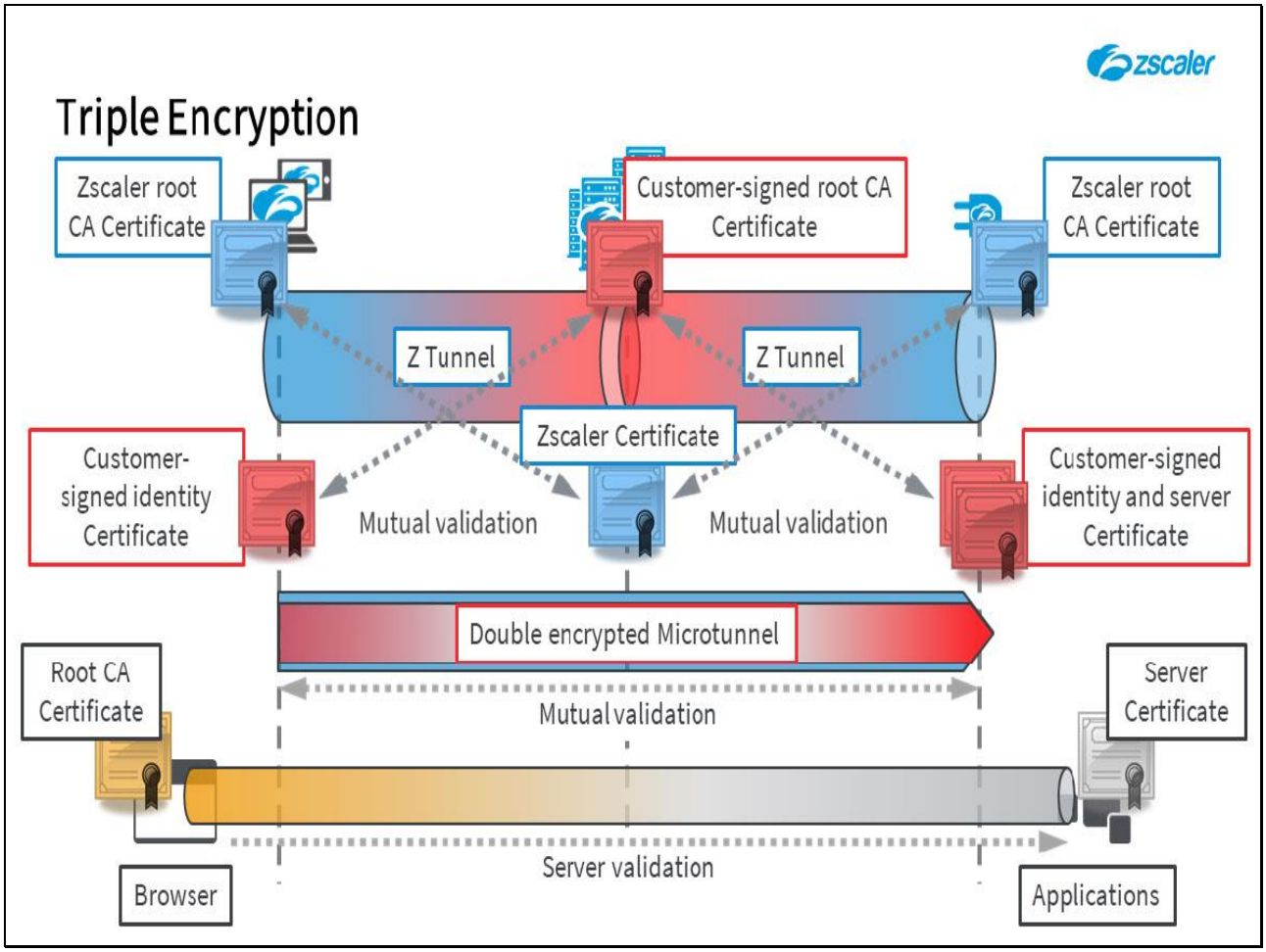


Slide notes

…but then instead of application traffic being sent as an unencrypted byte stream, the traffic is sent in an additional end-to-end TLS tunnel, which is established between the Client and App Connectors based on the customer-signed server certificate provisioned to the App Connector on enrollment and the customer-signed identity certificate provided to the Client Connector.

As this is an end-to-end tunnel, there is now no possibility for the Service Edge to intercept or inspect the private traffic that it processes. As with Z Tunnels, the Microtunnels are encrypted using the strongest cipher that is mutually supported by the Client and App Connector hosts.

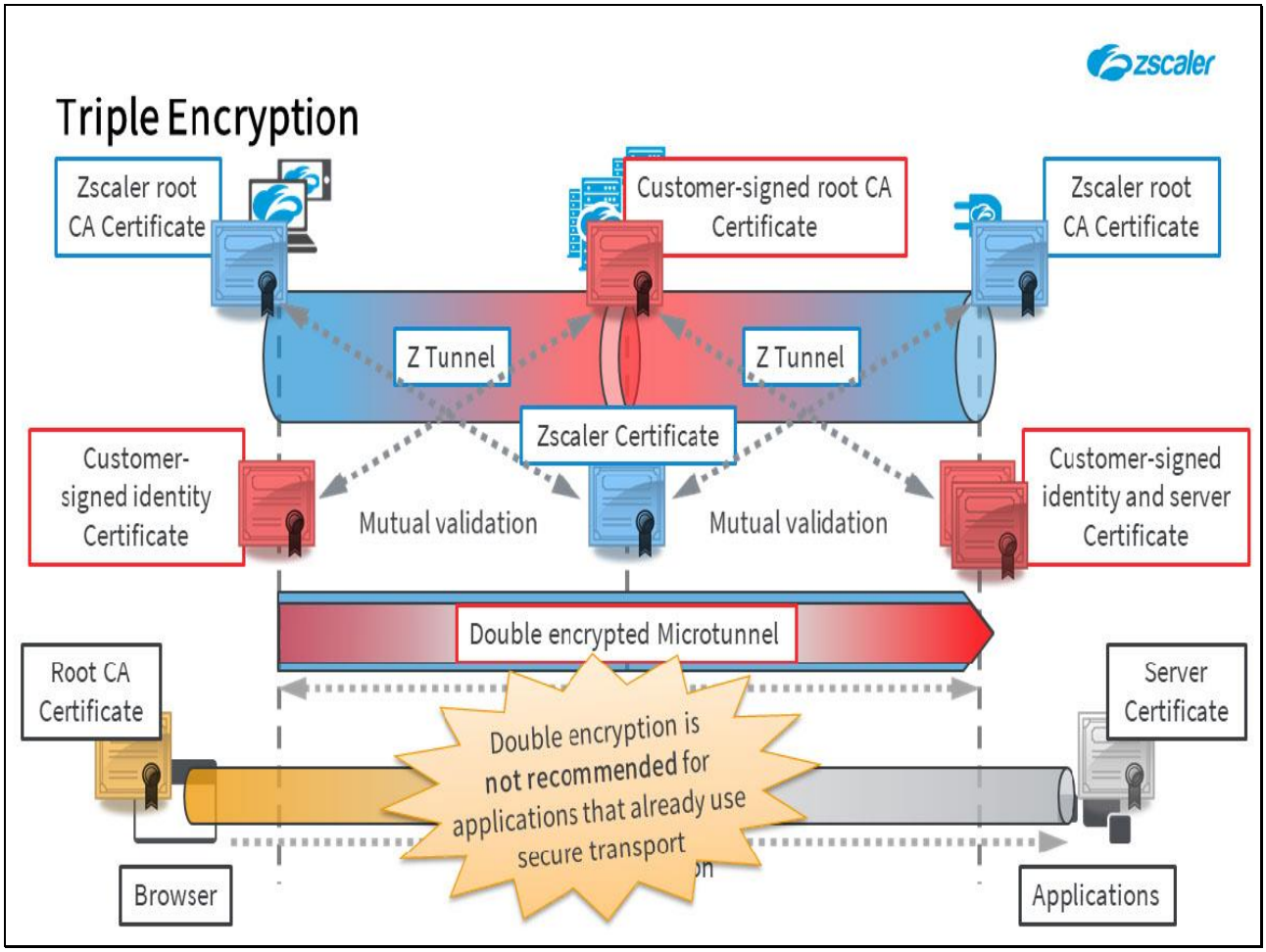
Slide 70 - Triple Encryption



Slide notes

As before, if the applications themselves use HTTPS then TLS encryption is established end-to-end within the Microtunnels. If the BYOE model is used, with **Double Encrypted** Microtunnels, this will mean that data is ***triple*** encrypted as it passes across the ZPA infrastructure, with no opportunity whatsoever for Zscaler to intercept or otherwise access application data.

Slide 71 - Triple Encryption



Slide notes

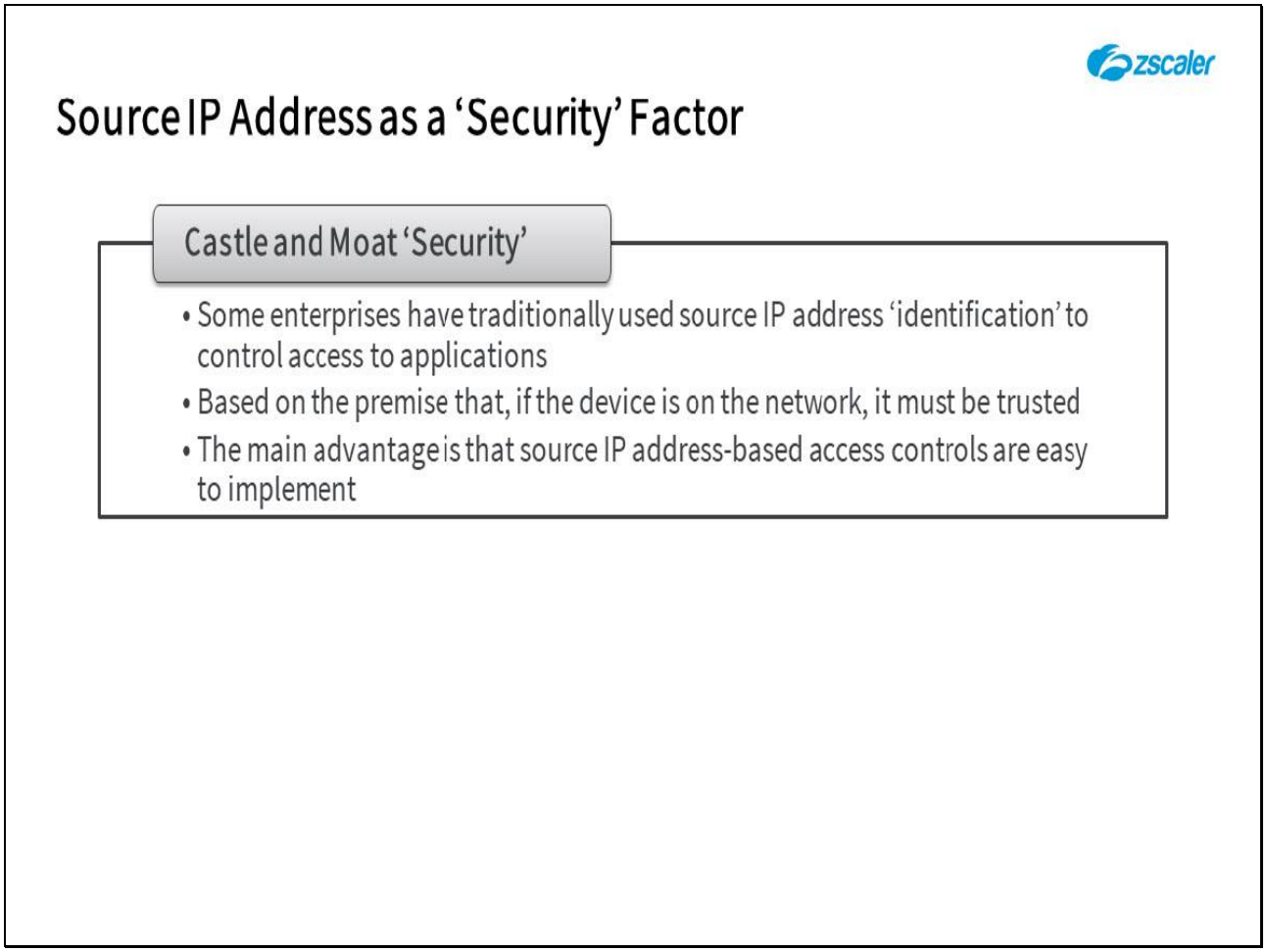
Note that **Double Encryption** is not recommended for traffic that is encrypted by default, such as secure web traffic over TLS between a web browser and an internal web application. For applications that already use encrypted transport between the client and server, **Double Encryption** adds overhead without providing any additional privacy.

Slide 72 - Source IP Anchoring With ZPA

Slide notes

Finally, let’s have a look at some ZPA options for managing source IP address anchoring requirements.

Slide 73 - Source IP Address as a 'Security' Factor

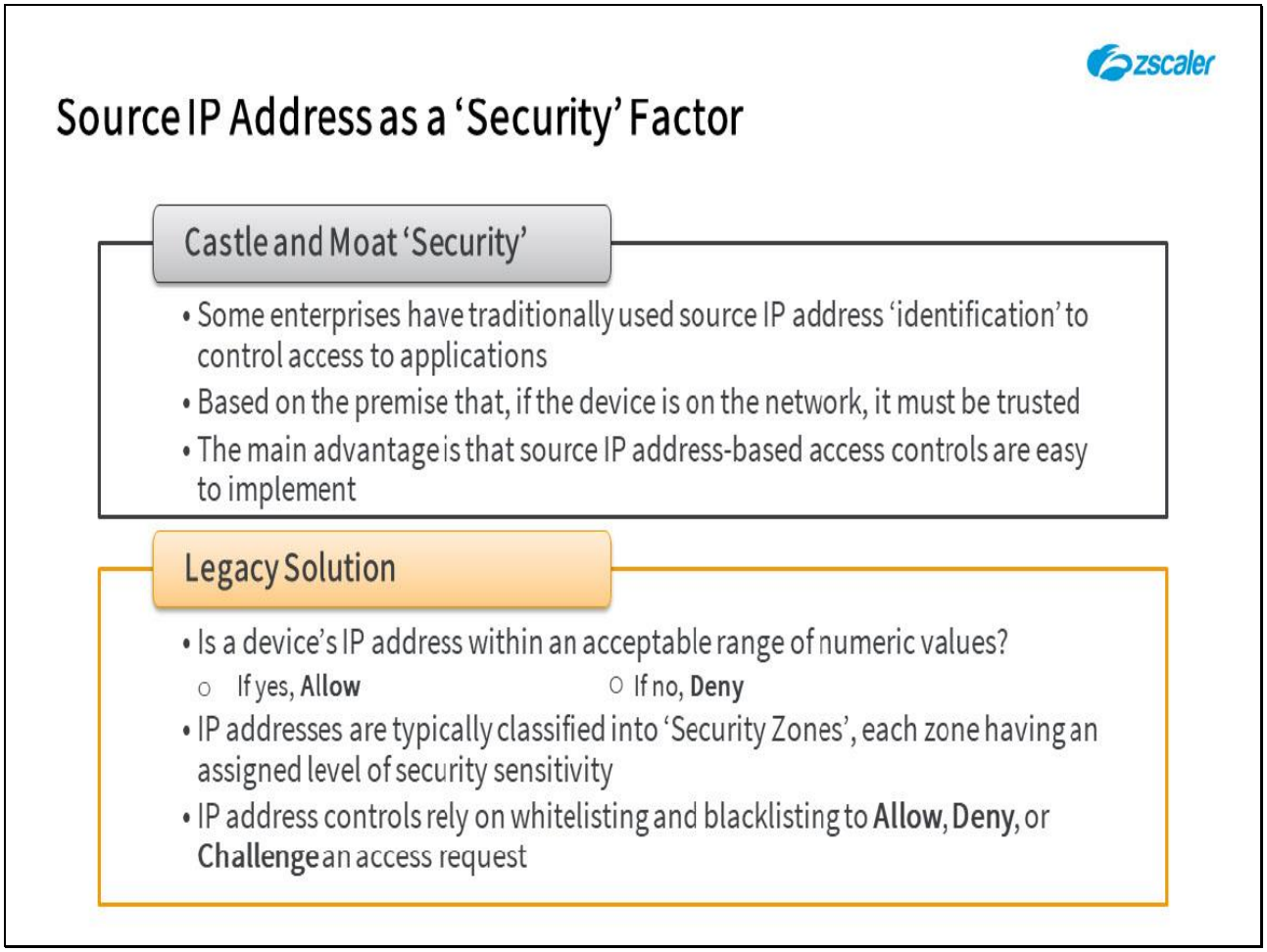


Slide notes

Many enterprises employ source IP address identification to control access to applications. Restricting access to applications or resources based on IP address is a control concept from an era when users and applications both sat within a perimeter defense. If the IP address of the host device seeking access to the application or resource over the corporate network is from within the corporate range, then the device must be trusted and therefore permitted access. The main advantage of this mechanism is in its simplicity to implement.

However, when those organizations adopt SaaS applications, migrate internal applications out of data centers and support remote work, source IP address identification becomes less effective as a means to secure access to corporate resources.

Slide 74 - Source IP Address as a 'Security' Factor



Slide notes

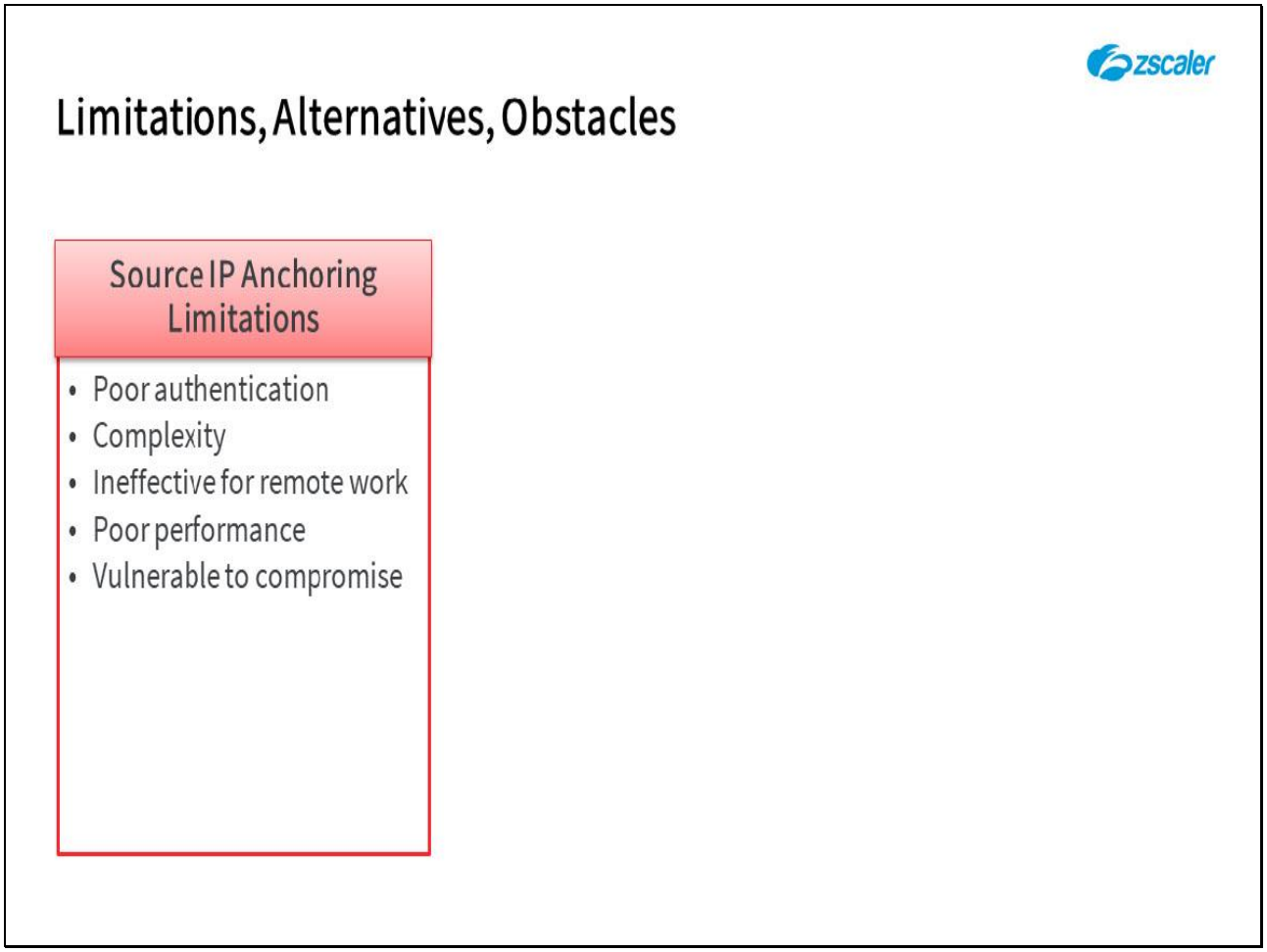
Using source IP as a security factor, the access decision is pretty binary:

- Is this device's IP address within an acceptable range of numeric values?
    - If yes, then allow them to connect.
    - If no, the originating host machine is blocked.

In such an enterprise environment, IP addresses may be classified into so-called 'Security Zones' in which each zone has an assigned level of security sensitivity. An enterprise device can then access resources based on the privileges afforded to its particular zone. A zone range may be discontinuous, and some host devices might be assigned to a default security zone (if the interface is not already explicitly associated with an existing security zone).

IP address controls may then rely on whitelisting and blacklisting. To allow access, an application or service compares the source IP address of the inquiring device to an approved list of numbers (to see if it is within an authorized security zone), also known as a 'whitelist' and based on the result of the comparison, allows, denies, or in more sophisticated implementations may challenge the access request. If challenged, the host device may have to provide additional authorization details. If the host device fails the challenge, its address can be automatically blacklisted. Alternatively, IT security may restrict access to a specific URL or IP address range by actively managing the white-/blacklist.

Slide 75 - Limitations, Alternatives, Obstacles



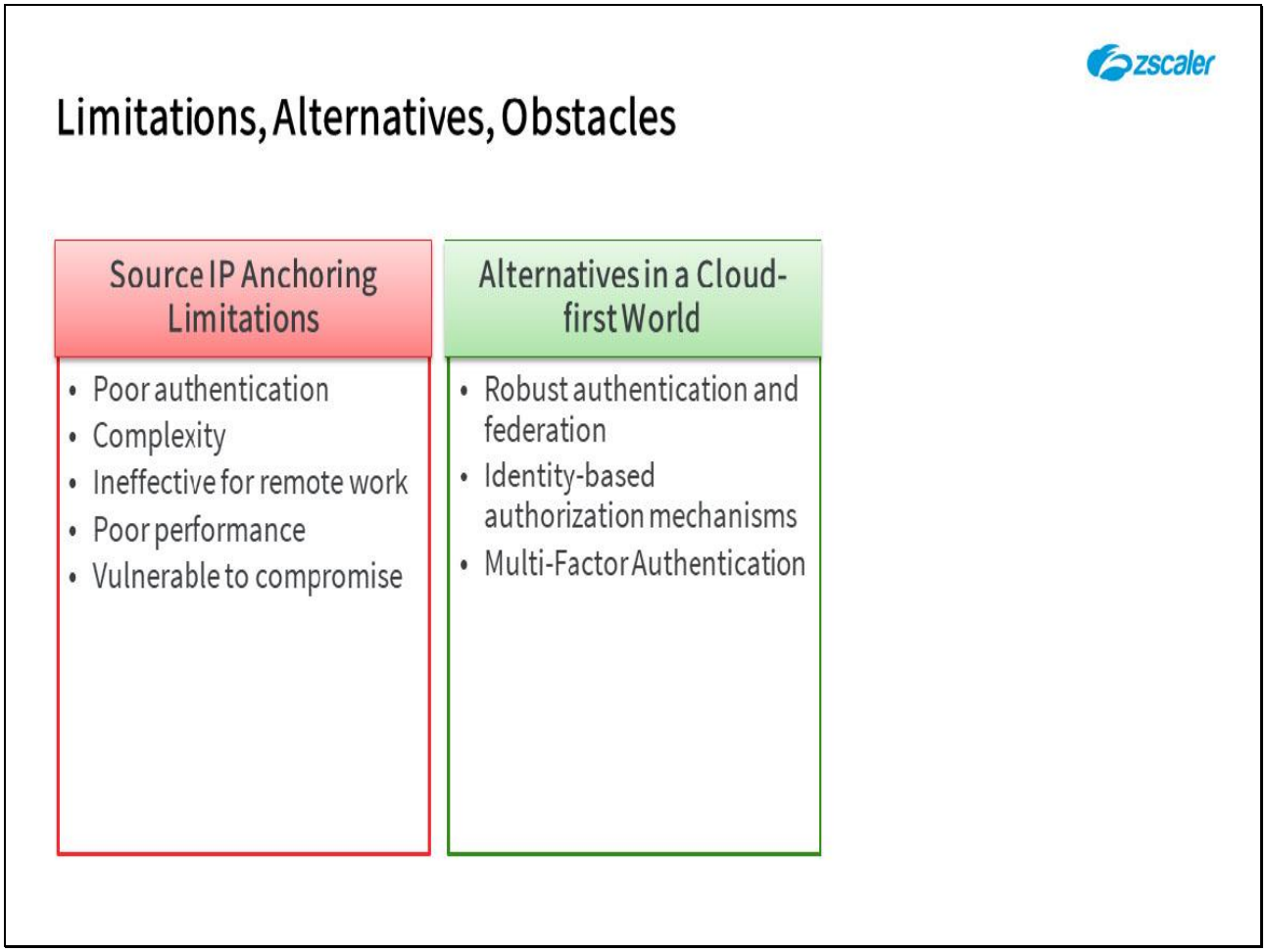
Slide notes

Source IP address identification, by itself, is no longer a reliable nor enforceable security control for governing access to enterprise resources. When it comes to securing the new enterprise way of work, source IP address-based access controls have limitations:

- **Poor authentication** - As an identity mechanism, IP address controls recognize a device, not the device's user (this prevents the application applying least-privilege permissions, a key component of Zero-Trust policies), if any device within an authorized security zone is compromised, everything accessible to that device is vulnerable to attack;
- **Complexity** - IP address management is exceedingly complicated and improperly configured IP ranges can inadvertently lock out access to admin sites; Ineffective for remote work - When used for geo-restriction (e.g., specific ranges assigned based on geography), source IP address controls fail when users access resources from new, 'out-of-geo' locations;
- **Poor performance** - Source IP restrictions force users to VPN in from remote work locations just so they can egress to the Internet via a known IP, this backhauling adds latency;

- Vulnerable to compromise - IP addresses can be easily spoofed, one common attack-vector scenario - An open (or weak WEP encryption based) Wi-Fi network in an allowed address space can easily be exploited to hijack connections and gain access.

Slide 76 - Limitations, Alternatives, Obstacles

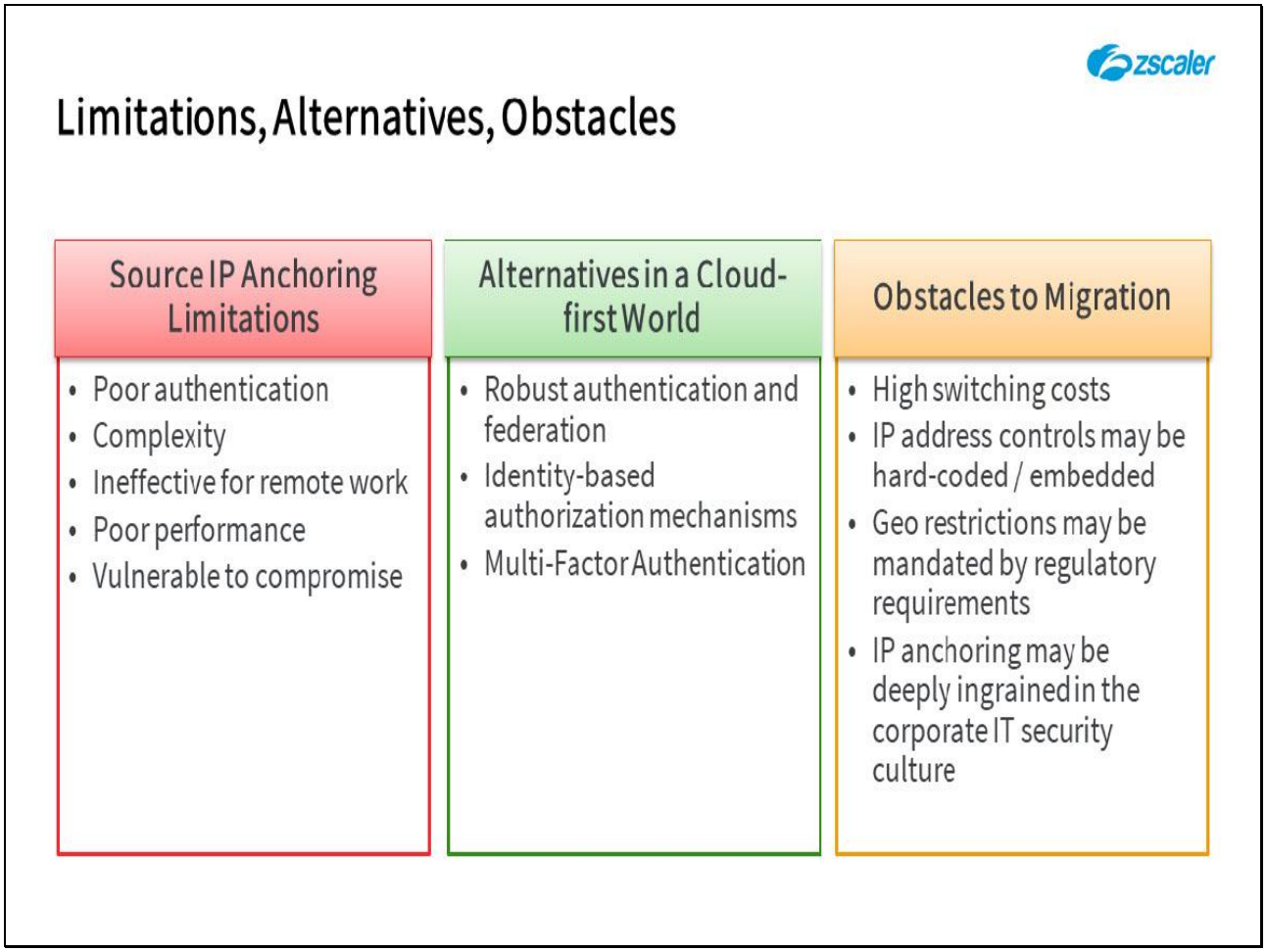


Slide notes

In a Cloud-first world there are better options available to provide robust authentication of end users based on a variety of factors, or even multiple factors. Zscaler recommends that you:

- Deploy enterprise SAML capabilities for SaaS access, this is a valuable step toward migrating from device authentication to user validation;
- Add MFA for all application access, coupled with SAML, MFA provides an essential security layer for the new way of work, enabling SaaS application access to users anywhere and anytime.

Slide 77 - Limitations, Alternatives, Obstacles



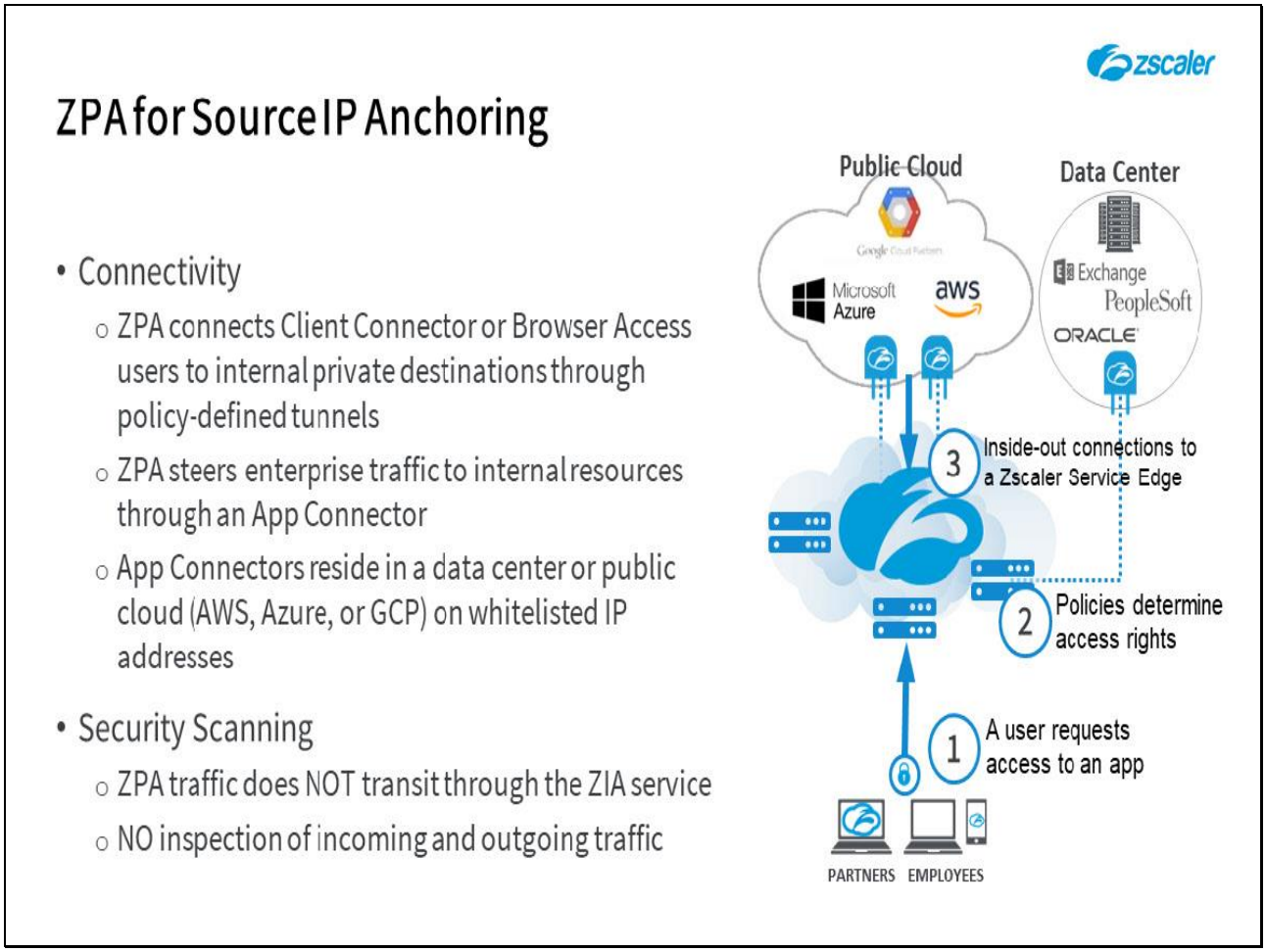
Slide notes

Unfortunately, source IP address controls remain firmly entrenched in many organizations, as moving beyond source-IP address controls as an exclusive means of securing access isn't trivial and such efforts can incur switching costs.

For some organizations, the path from IP address-only to MFA with inline proxy security also carries high switching costs. IP address controls may be hard-coded in legacy applications, embedded in internal websites as geo restrictions, mandated by regulatory requirements, or simply deeply ingrained in the corporate IT security culture.

Ideally, you should establish a migration plan for applications that still require source IP address validation, in the short term, deploy Zscaler and apply the solution considerations presented here, in the long term, consider refactoring or recoding to reduce dependence on source IP address-based access controls.

Slide 78 - ZPA for Source IP Anchoring



Slide notes

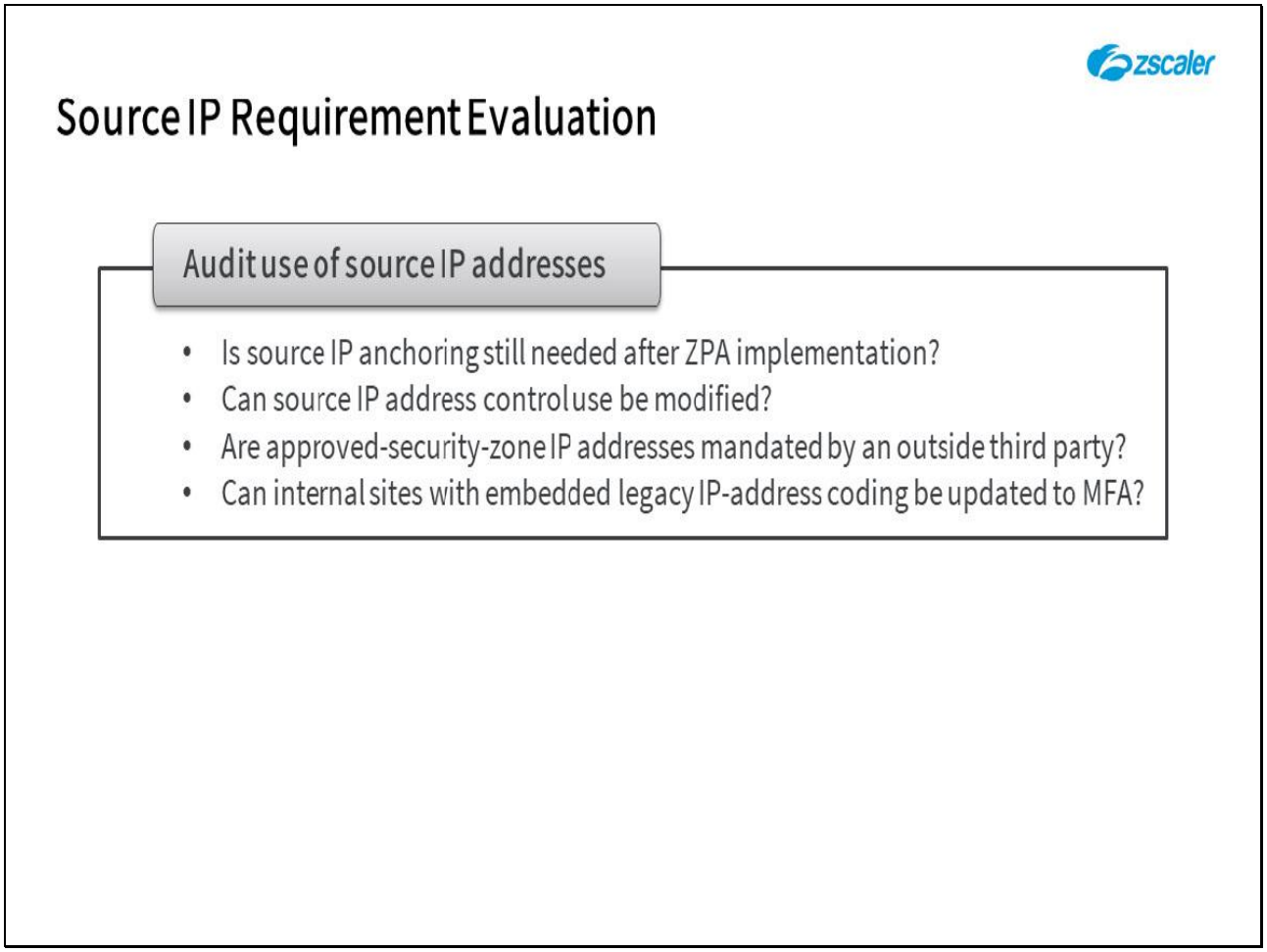
ZPA connects users to internal private destinations through policy-defined tunnels between Client Connector or Browser Access users and App Connectors installed adjacent to the internal applications to be enabled. ZPA steers enterprise traffic to internal resources, as the connection does not egress through ZIA, but instead routes to an App Connector, from where it connects to the appropriate internal resource.

Since the App Connectors reside in a customer's own data center or public Cloud (say, AWS, Azure, or GCP) the destination resource (e.g., internal application or content server) sees the user's IP address as being the internal (whitelisted) address of the App Connector. ZPA does require the Client Connector agent as an endpoint control for non-web applications, it also allows Browser Access without any kind of agent for internal web applications.

ZPA plus source IP-address controls is an option for securing user access to trusted applications that do not require security inspection, but only if you are willing to accept potential exposure to broader internet-egress risks in the absence of ZIA security scanning.

When considering a ZPA-only approach for source-IP preservation, customers should be comfortable with the security implications of not scanning Cloud application traffic with ZIA.

Slide 79 - Source IP Requirement Evaluation

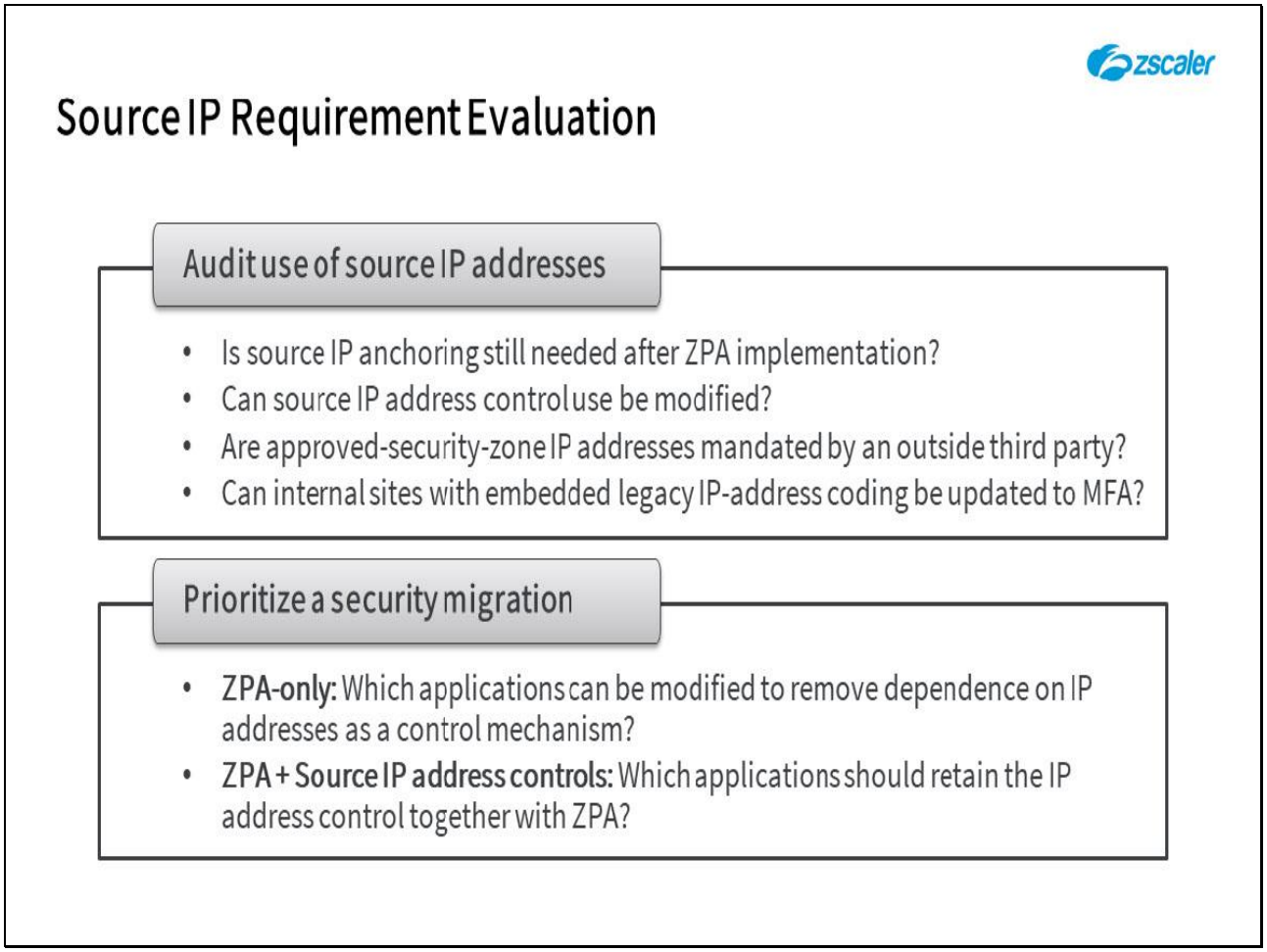


Slide notes

When evaluating the implementation of ZPA for an application that currently requires source IP address anchoring, there are a number of aspects to consider. You will need to audit the use of source IP addresses to allow/restrict access to internal and external resources:

- Is it possible for the source IP address control requirement be modified?
- If so, what's the scope of those modifications (on a case-by-case basis)?
- Are approved-security-zone IP addresses mandated by an outside third party (like a government regulator using IP addresses to determine in-geo access)?
- Can internal sites with embedded legacy IP-address coding be updated to more modern (and dynamic) authentication mechanisms like MFA?

Slide 80 - Source IP Requirement Evaluation

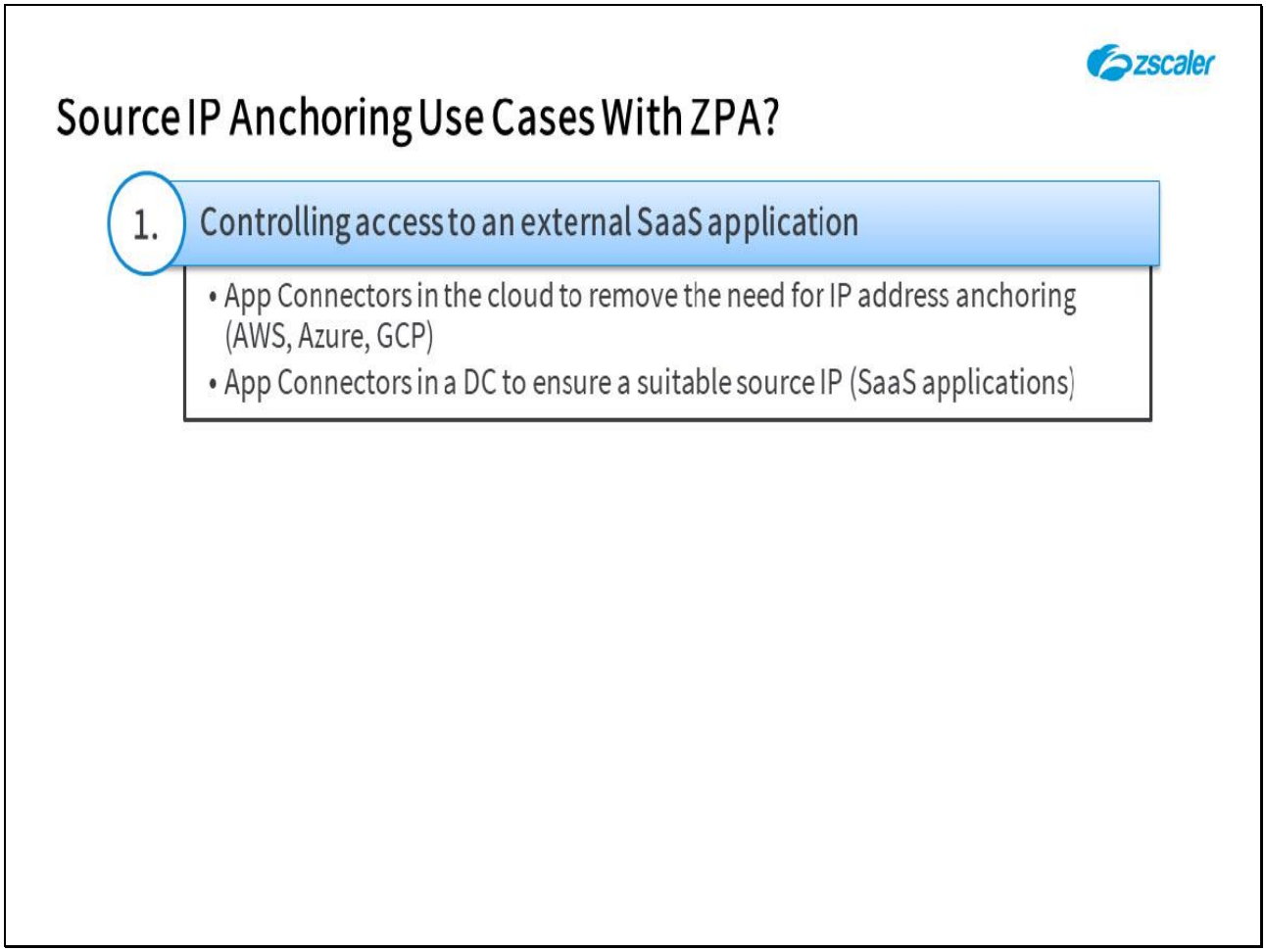


Slide notes

Based on your assessment findings, prioritize a security migration. Options include:

- ZPA-only - which enterprise operations can be modified to remove dependence on IP addresses as a control mechanism?
- Or, ZPA plus source IP address controls - which enterprise operations should retain the IP address control in conjunction with ZPA?

Slide 81 - Source IP Anchoring Use Cases With ZPA?



Slide notes

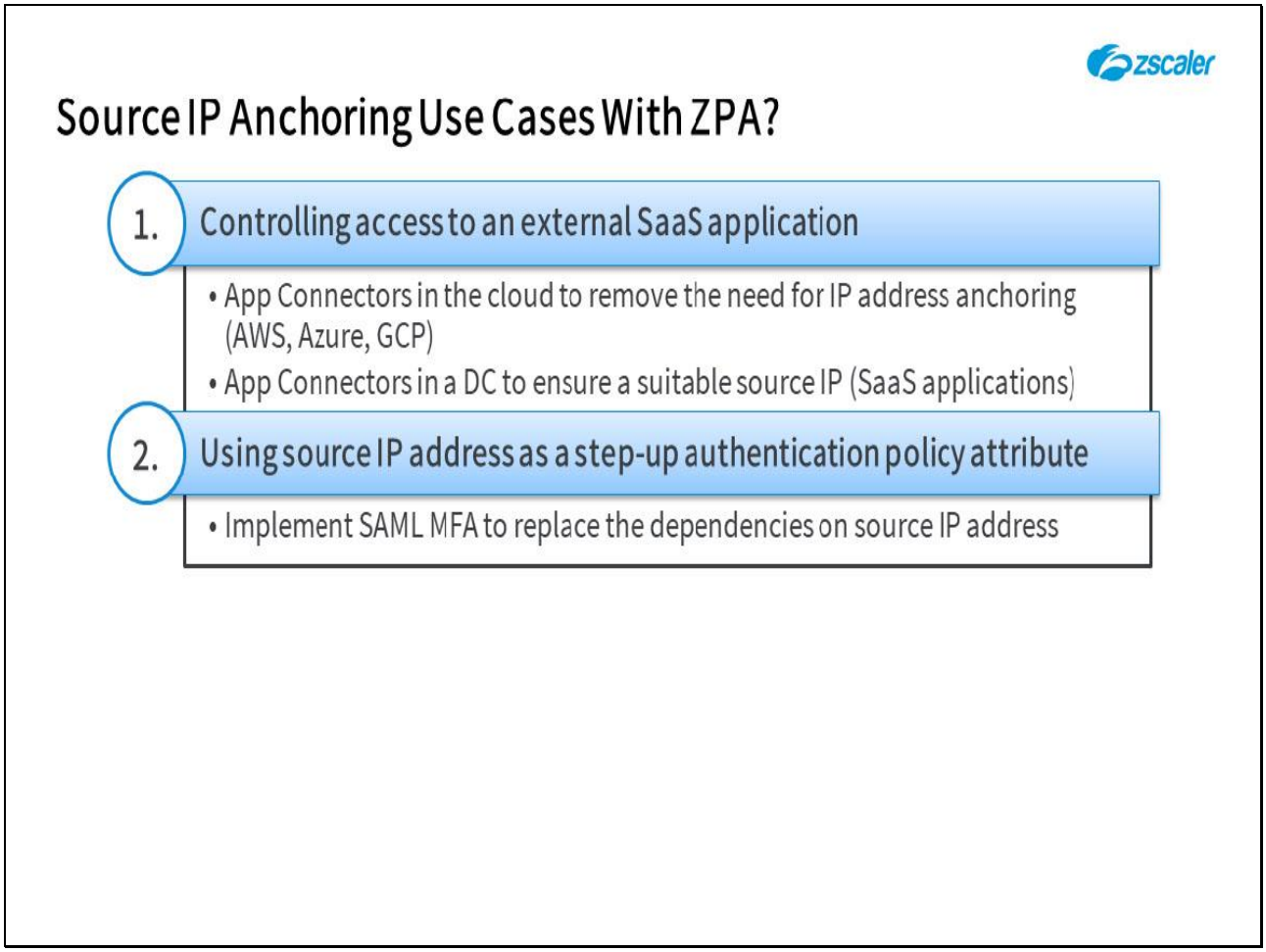
Many applications (including SaaS applications surprisingly) continue to use IP address as an authorization criterion for access to an application server. This method may be employed in enterprise environments as a supplemental access mechanism for applications (often ones that carry legacy IP-address-based access-control code) that have been migrated from a protected data center to the Cloud or Internet.

ZPA anyway requires robust authentication using SAML, so adding MFA to provide a more modern security approach would be relatively trivial. If source IP anchoring is a hard requirement, there are a couple of options with ZPA to enable it, depending on the applications in question.

For the main Cloud computing platforms (such as Azure, AWS or GCP), it is trivial to install an App Connector on an appropriate Resource Group or virtual LAN to ensure that any user connecting through it uses a local, whitelisted IP address.

For SaaS application vendors (such as SFDC, ServiceNow or Workday), it may also be possible to configure end user connections to transit an App Connector located in a Data Center, so that the source IP address is from a whitelisted range. Although, note that this can lead to the sort of sub-optimal routing (tromboning) that ZPA is explicitly designed to avoid.

Slide 82 - Source IP Anchoring Use Cases With ZPA?



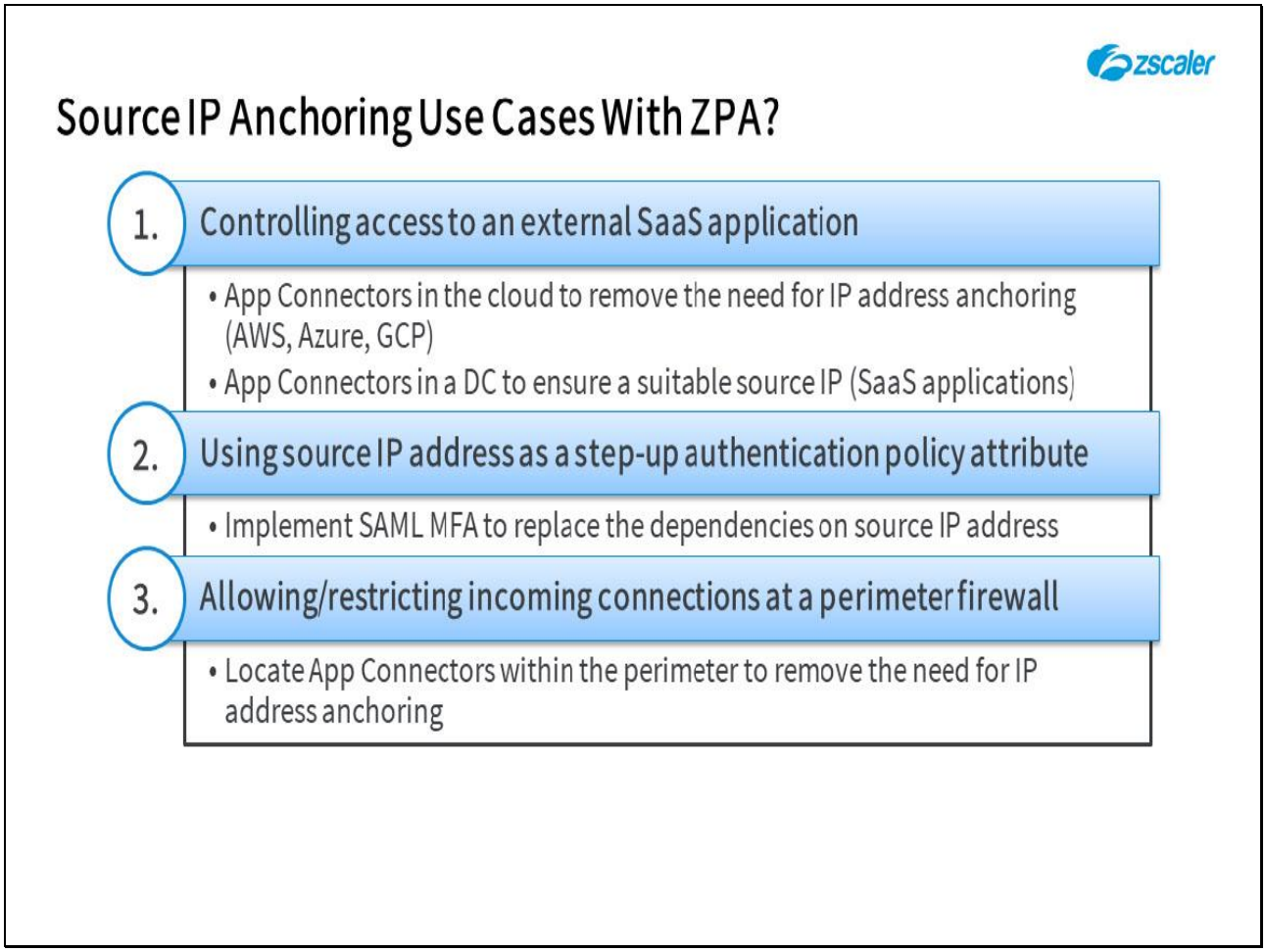
Slide notes

Source IP address can be used as a decision criterion to escalate authentication challenges. For example, in an enterprise environment that uses source IP address for whitelisting (as in use case #1 above), an incoming device connection would be allowed based on a single factor of authentication (the IP address number itself) if the source IP address is within an acceptable range.

But if there are situations where an outside-the-range IP-addressed device might need access, then the IP-address check becomes a challenge. If the source device's IP address is not within allowable range, then a second factor (or more) of authentication (either a one-time password or RSA key entry) is required.

As this use case is the same as use case #1, plus an additional authentication challenge to allow for unrecognized IP address access, the ZPA deployment options described on the previous slide are also applicable here. Any additional second-factor authentication validation required for a user that reaches the application from an unknown IP address, is outside the scope of the ZPA deployment.

Slide 83 - Source IP Anchoring Use Cases With ZPA?



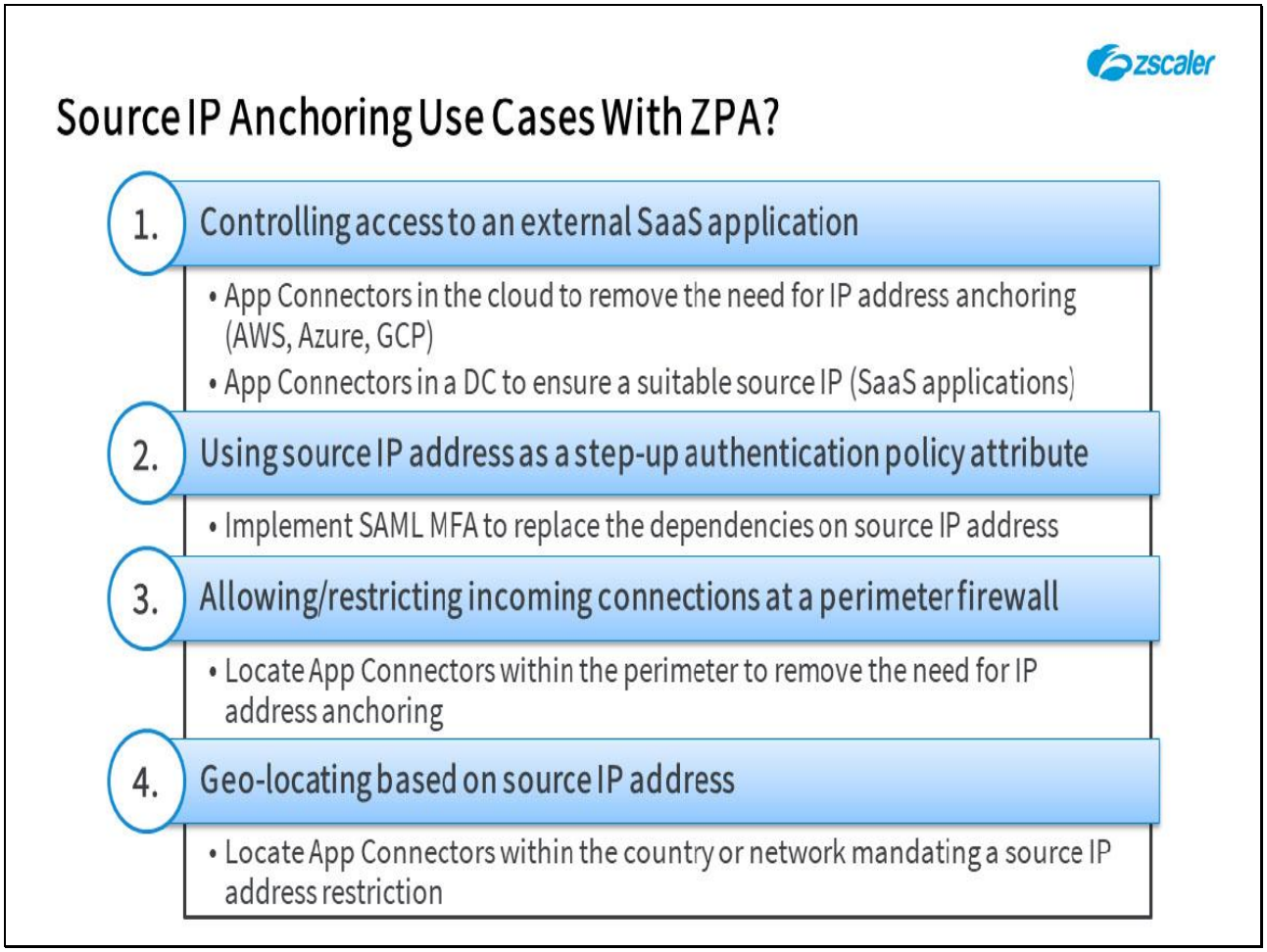
Slide notes

Some enterprises, when migrating applications or data from internal networks or data centers to public IaaS Clouds, seek to restrict access to the virtual networks that host the relocated applications.

In this model, IT essentially extends a perimeter firewall around a virtual network, virtualizing a castle-and-moat-secured network (with all its known security limitations) in the Cloud. Inbound access is allowed through a VPN (with access to the VPN granted based on source IP address, of course) or based on whitelisted IP addresses within a select range (configured in the virtualized firewall rule set).

A ZPA App Connector on the network protected by the Firewall, will of course allow seamless access to applications from an internal IP address.

Slide 84 - Source IP Anchoring Use Cases With ZPA?



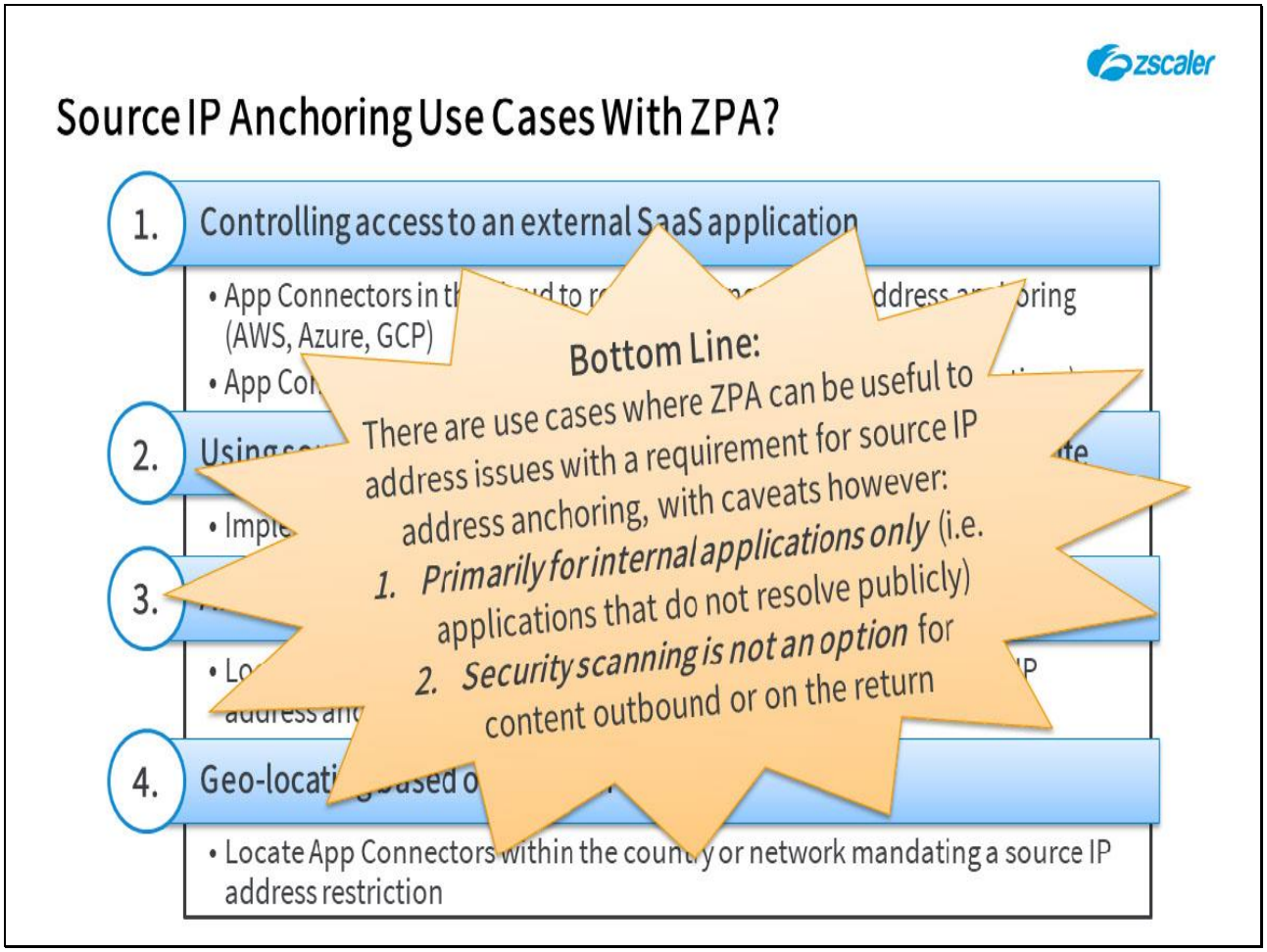
Slide notes

Some websites present dynamic content based on IP-address geo-location. Others, including many media services and government sites, use source IP address identification to restrict access to content (e.g. the Indian Tax Authority's site for submitting tax returns). Unfortunately for the sites that rely on it, IP-address-based geo-location isn't particularly accurate anymore:

- 'Anycasting' can obfuscate device pinpointing - When an IP address prefix is simultaneously announced from multiple locations, it is said to be 'anycast' a connectivity optimization technique commonly used by CDNs, DDoS mitigation services, and DNS providers to route traffic to its destination in the fewest network hops. But that prefix can appear to be in multiple locations at once (depending on vantage point), making the source device nearly impossible to accurately geo-locate.
- Mobile devices are, well, mobile - Users working remotely may move and stay connected. When device locations move over a relatively short period of time (e.g., taking the train from one city to another), it's hard for destination sites/content servers to definitively associate an IP address to a specific place.
- Subscription data services route traffic through their own gateways - Many service carriers (think mobile device providers) use centralized gateways as onramps to the public internet. That misdirection can easily confuse destination sites into thinking source device access is coming from the location in which the gateway resides.

For services such as these, it may be necessary to deploy a ZPA App Connector Group on a network with a ‘legal’ IP address range, and ensure end users employ that Group when necessary. This would ensure that their apparent source IP, is actually within the country’s IP range.

Slide 85 - Source IP Anchoring Use Cases With ZPA?

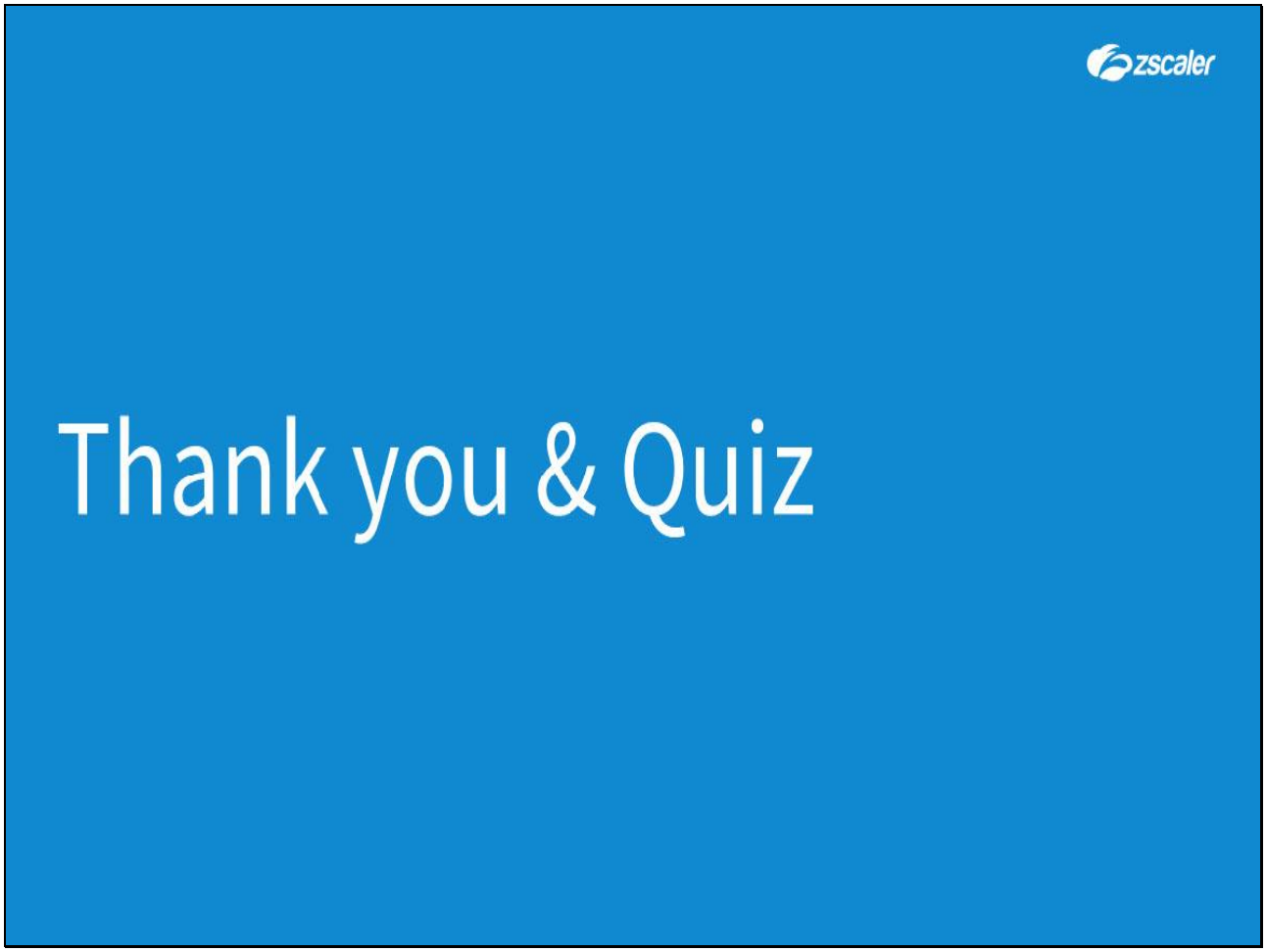


Slide notes

The Bottom Line: There are use cases where ZPA can be useful to address issues with a requirement for source IP address anchoring, primarily where an App Connector can be installed on the 'legal' IP address space, to make it appear as though that is where the end user is connected. There are some caveats however:

- ZPA is primarily intended for access to internal applications (i.e. applications that do not resolve on the public Internet). There may be situations where it is expedient to define a public application in ZPA, especially for those geo-restricted applications, however this should only be done under exceptional circumstances and should by no means be considered as a general solution.
- ZIA security scanning of data sent over ZPA is not an option, either for the outbound connections or return traffic. If security scanning is considered essential, then the source IP anchoring options offered by the ZIA service should be considered.

Slide 86 - 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.