

Slide 1 - Zscaler Private Access: Privacy

A blue rectangular slide with a black border. In the top left corner is the Zscaler logo, which consists of a stylized white 'Z' icon followed by the word 'zscaler' in a white, lowercase, sans-serif font. In the center of the slide, the words 'Zscaler Private Access' are written in a large, white, sans-serif font. Below this, the word 'Privacy' is written in a smaller, white, sans-serif font. In the bottom right corner, the text '©2020 Zscaler, Inc. All rights reserved.' is written in a small, white, sans-serif font.

 zscaler

Zscaler Private Access

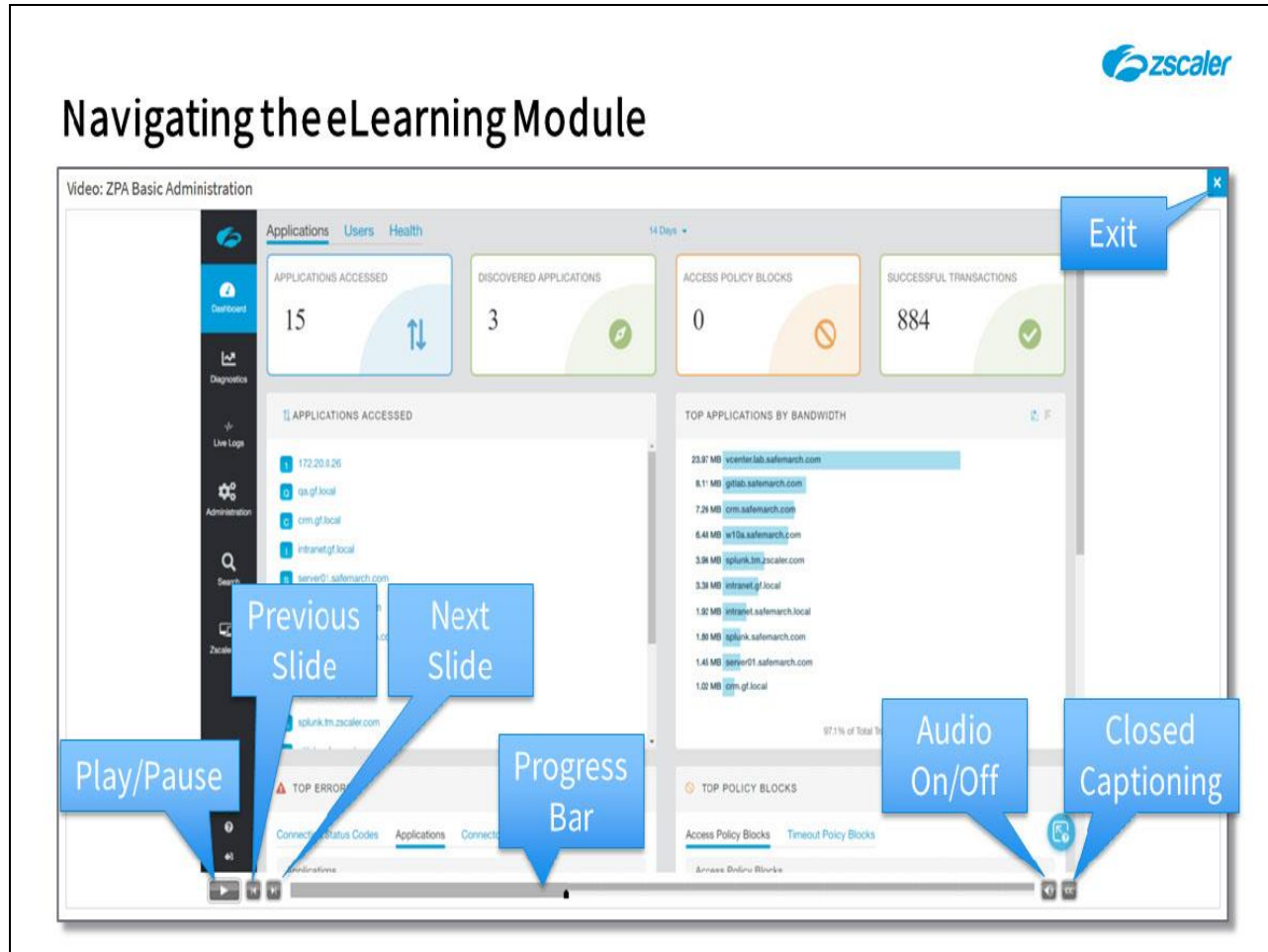
Privacy

©2020 Zscaler, Inc. All rights reserved.

Slide notes

Welcome to this training module on privacy threats and the countermeasures to them employed by the Zscaler Private Access service.

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

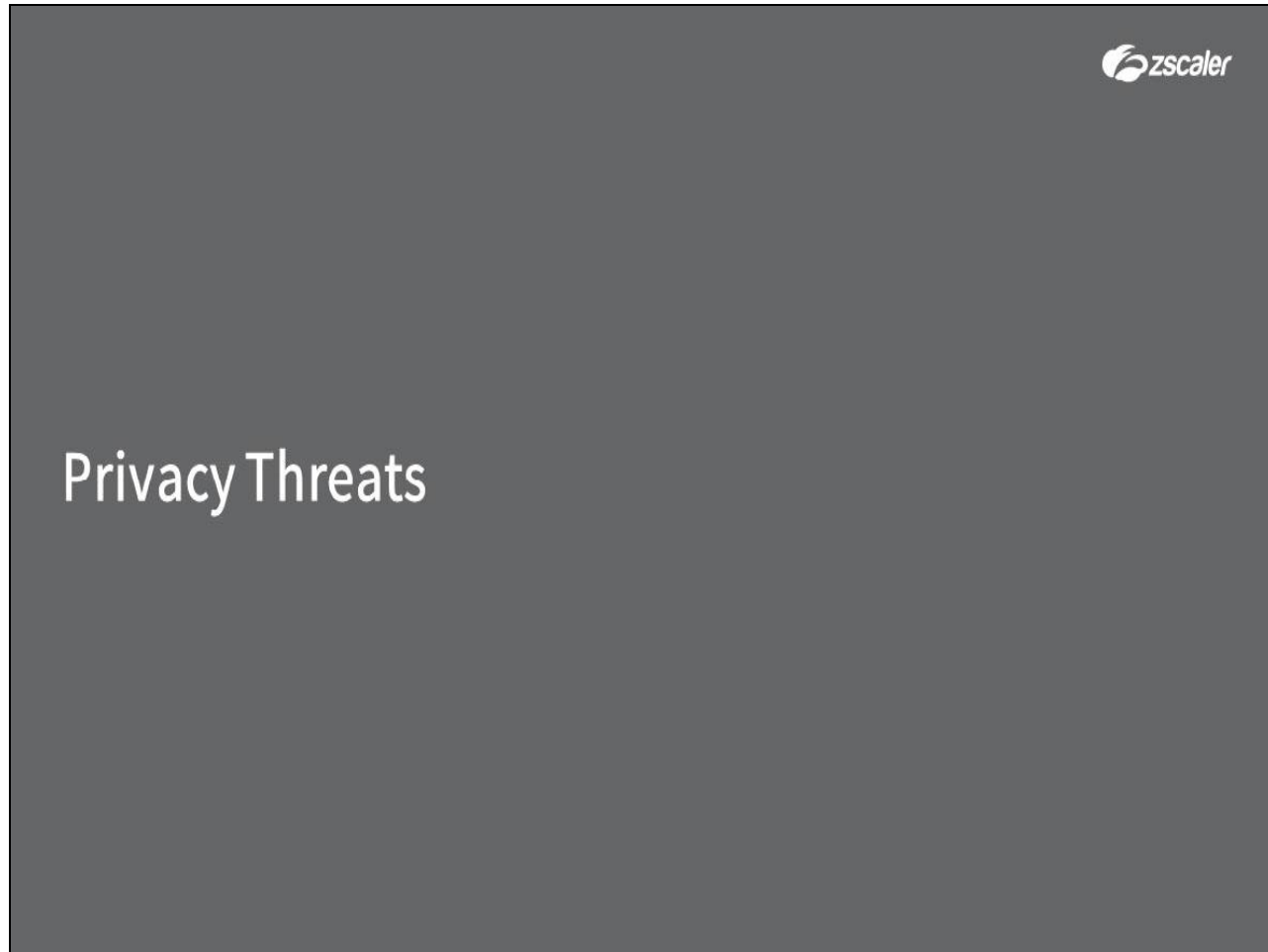
- Privacy Threats to PII
- Privacy of Data in Motion
- Privacy of Data in Use / at Rest

Slide notes

In this module we will we will look at:

- The threats to user Personally Identifiable Information (PII);
- Privacy concerns for data in motion;
- And privacy concerns for data in use and at rest.

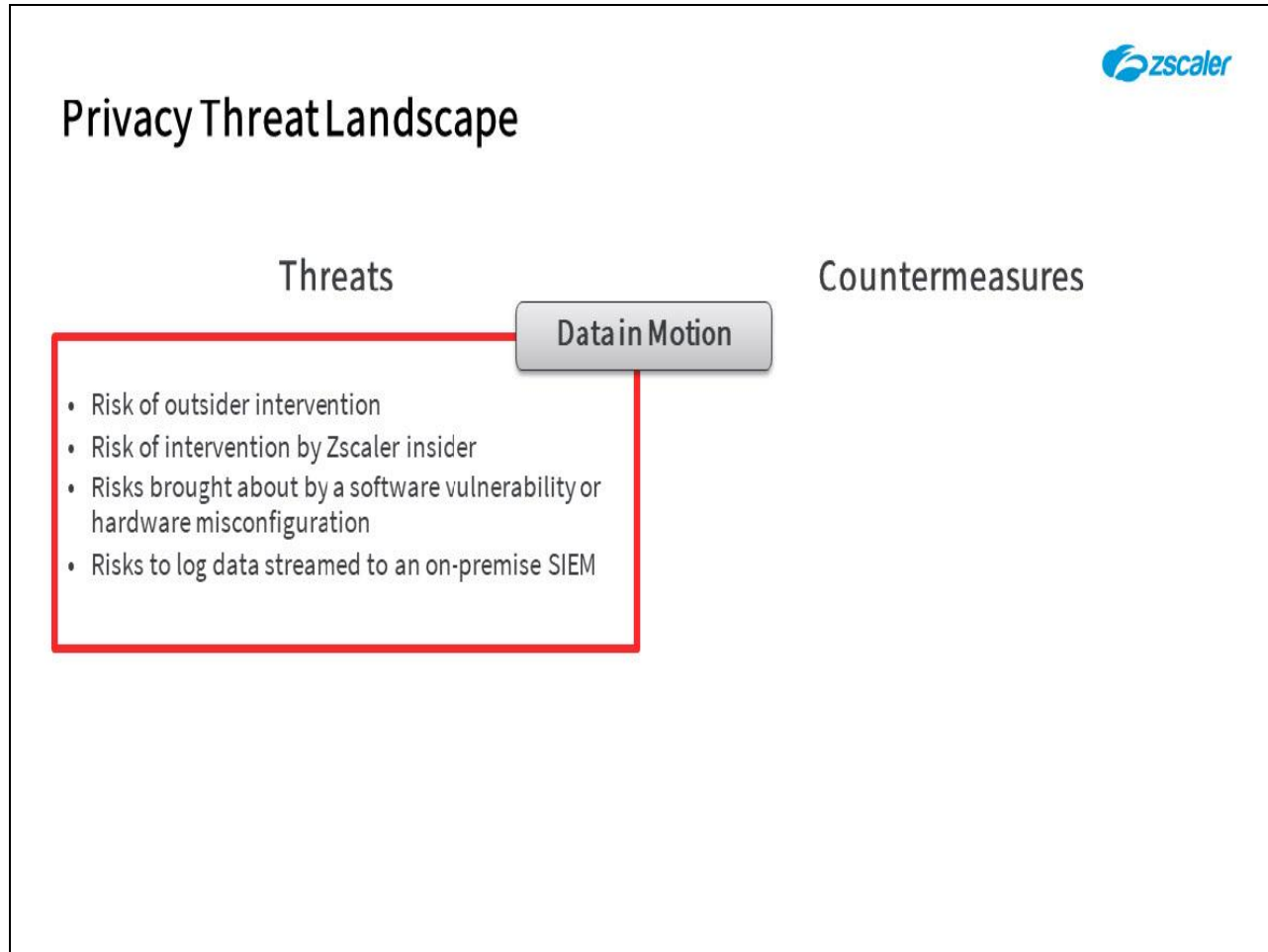
Slide 4 - Privacy Threats



Slide notes

Firstly, let's have a look at some of the potential threats to customer PII in general and at the countermeasures employed by the ZPA solution.

Slide 5 - Privacy Threat Landscape

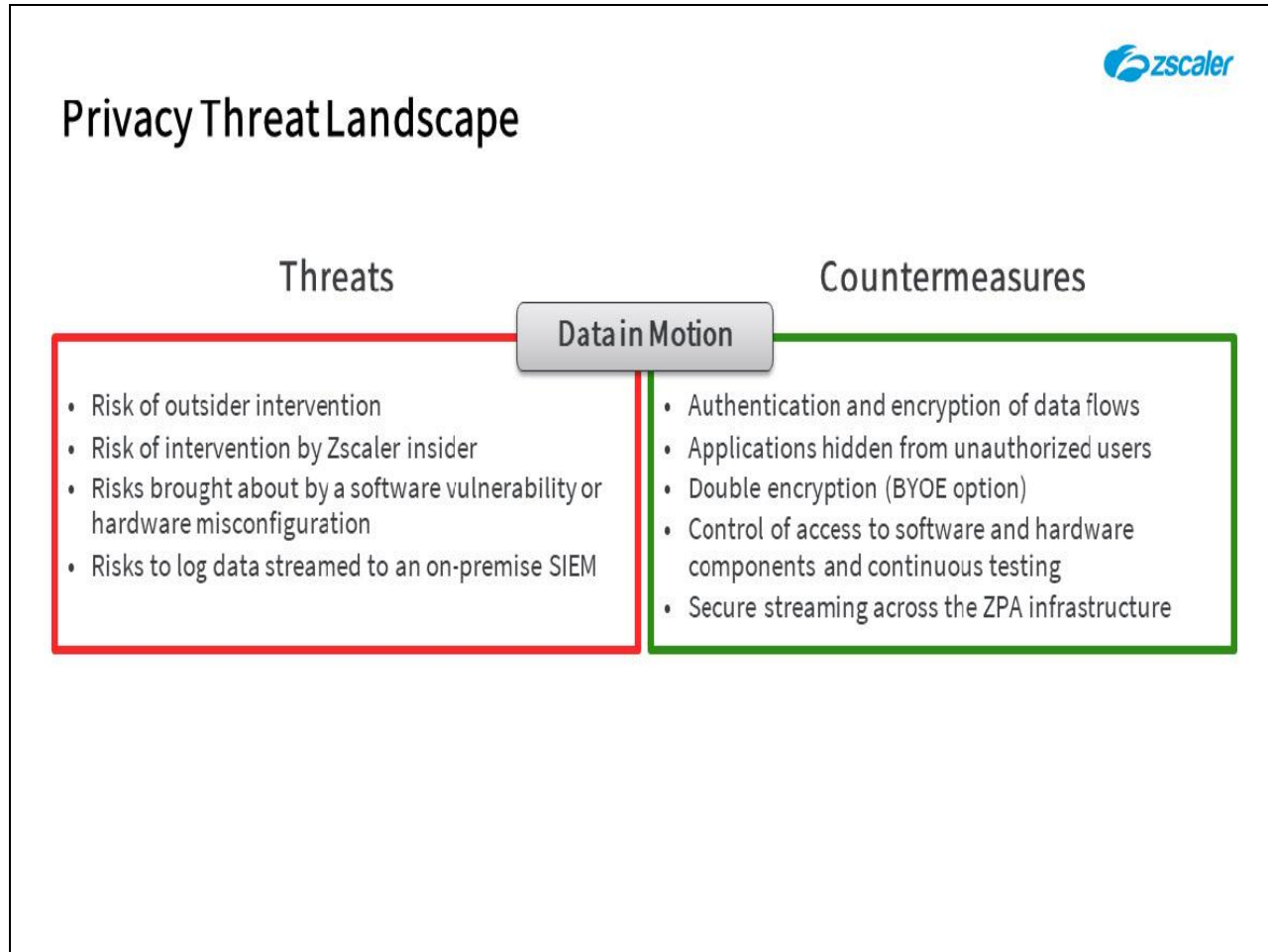


Slide notes

In overview, there are four main areas that have the potential to expose customer PII from data in motion:

- The threat of outsider intervention;
- The threat of an intervention by a Zscaler insider;
- Potential data exposure due to an undetected software or hardware vulnerability or through a misconfiguration;
- And the risk of exposure of customer PII in logs streamed to an on-premise, or cloud-based SIEM.

Slide 6 - Privacy Threat Landscape

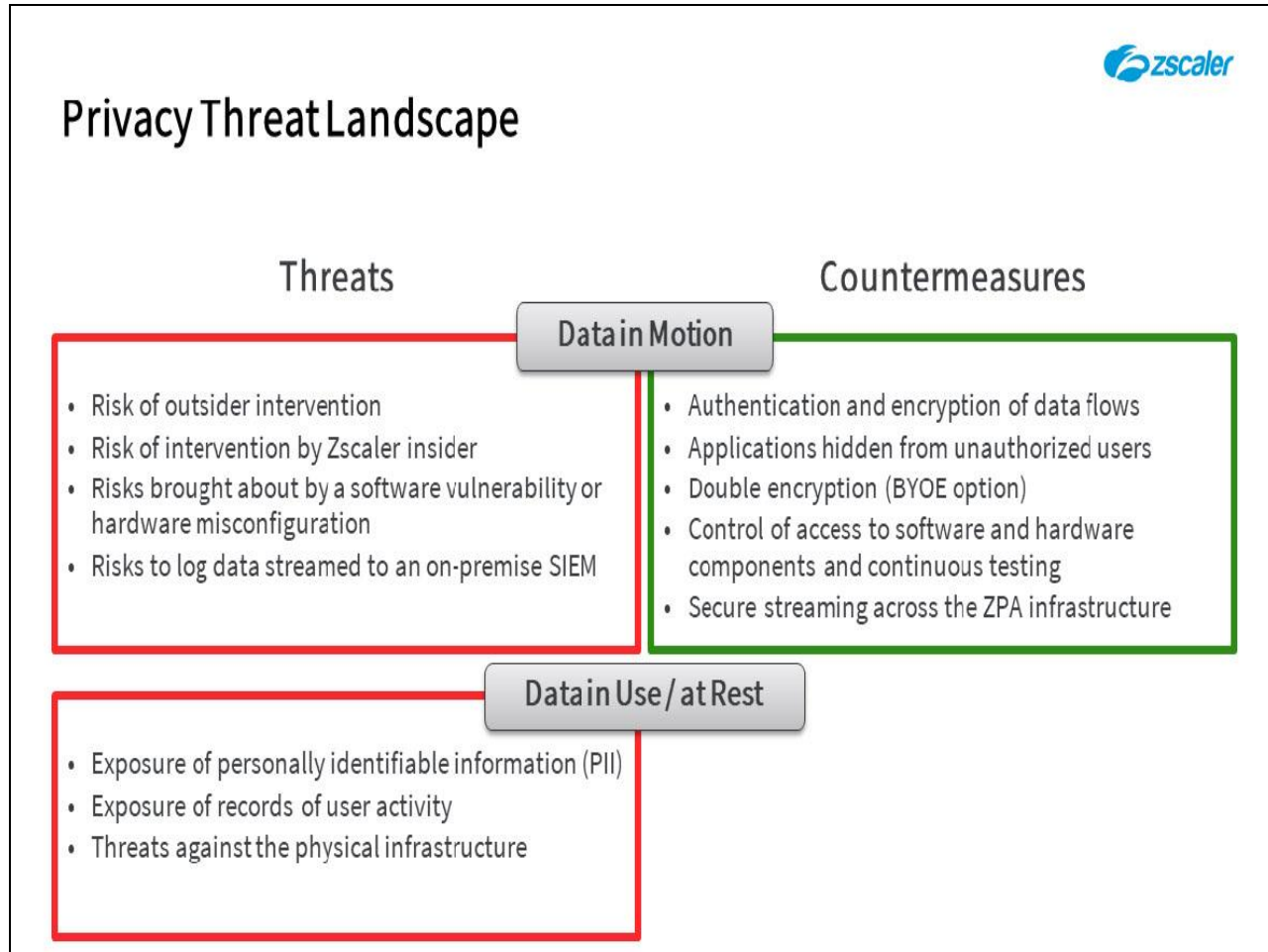


Slide notes

ZPA countermeasures to the threats against data in motion include:

- Robust end user authentication prior to the establishment of any ZPA connection and the encryption of all data transferred;
- The ZPA system architecture, by its very nature, ensures that private applications are not visible, discoverable, or accessible to unauthorized users;
- With the **Double Encryption** provided by the 'Bring Your Own Encryption' (BYOE) model, customer data is simply not accessible to any Zscaler employee;
- Zscaler SW and HW is continuously tested for vulnerabilities, including testing by independent third parties;
- Plus, the ZPA Log Streaming Service (LSS) employs the ZPA infrastructure itself, so all of the protective measures to safeguard customer data in motion are also applied to LSS data streams.

Slide 7 - Privacy Threat Landscape

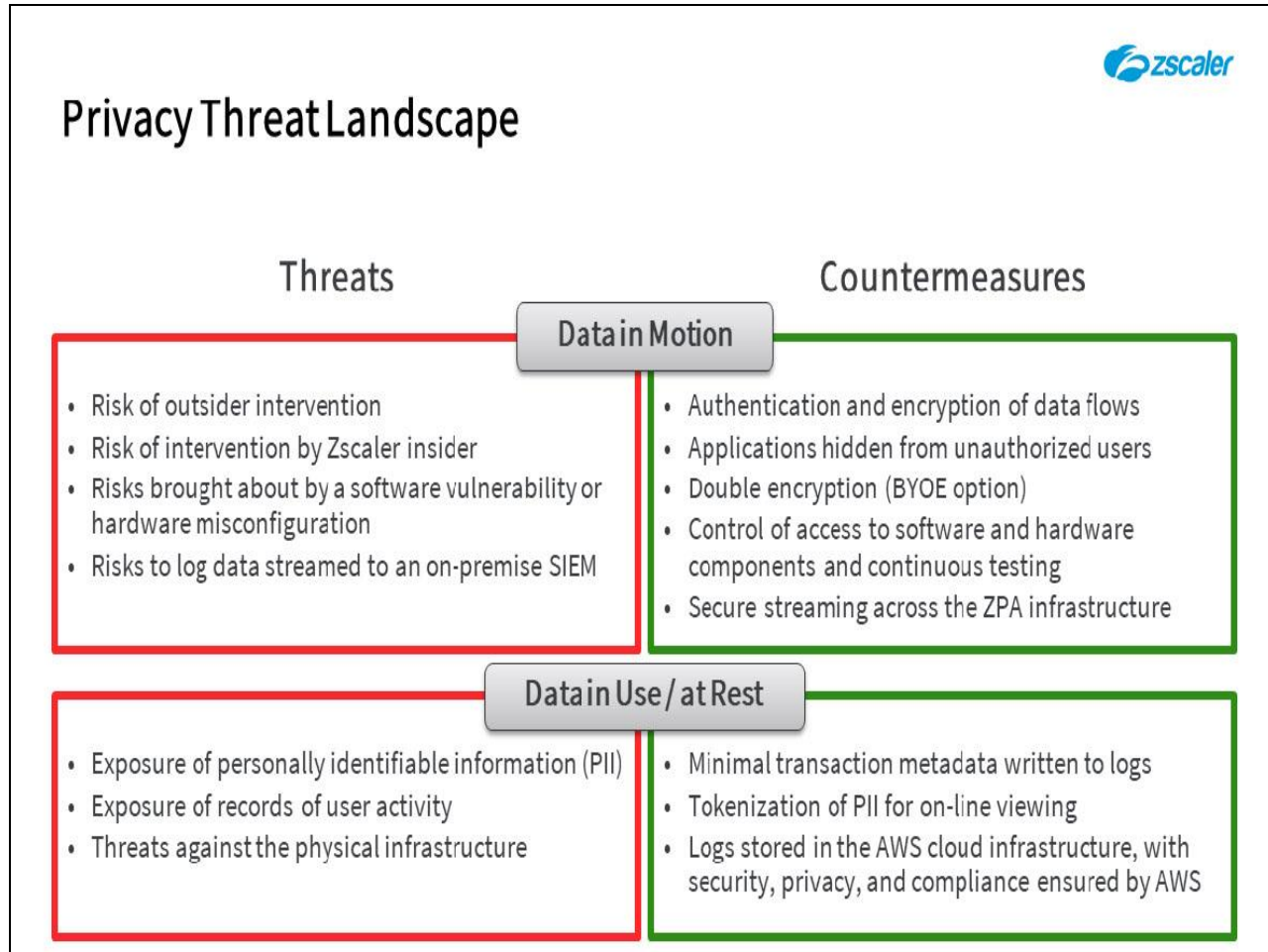


Slide notes

For the ZPA service, threats to data in use and data at rest are primarily threats against the logging infrastructure and include:

- The potential exposure of records of user activity;
- The threat of exposure of end user PII in the stored logs;
- And threats against the physical infrastructure where the logs are stored.

Slide 8 - Privacy Threat Landscape

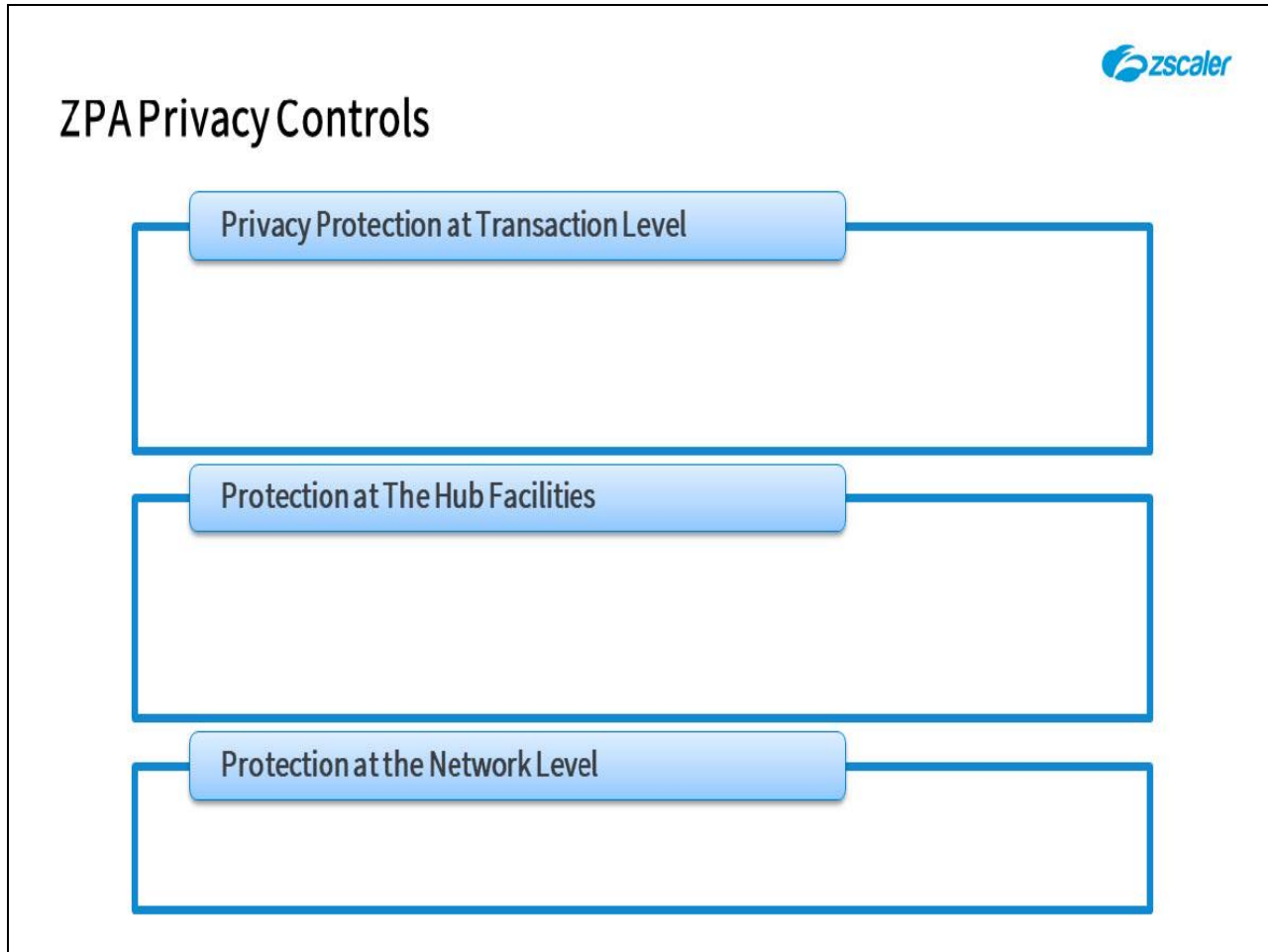


Slide notes

The ZPA countermeasures to these risks are:

- Firstly, that only minimal metadata is ever written to the logs, such as; **username, company name, application name** and **data quantities**;
- Any PII data written to the logs (such as **usernames** and **company names**) is tokenized and only interpretable when viewed from within the Zscaler admin portal, making it of little value to an unauthorized outsider;
- The logs are stored in the Amazon Web Services infrastructure, which means that security, privacy and compliance are all guaranteed by Amazon.

Slide 9 - ZPA Privacy Controls

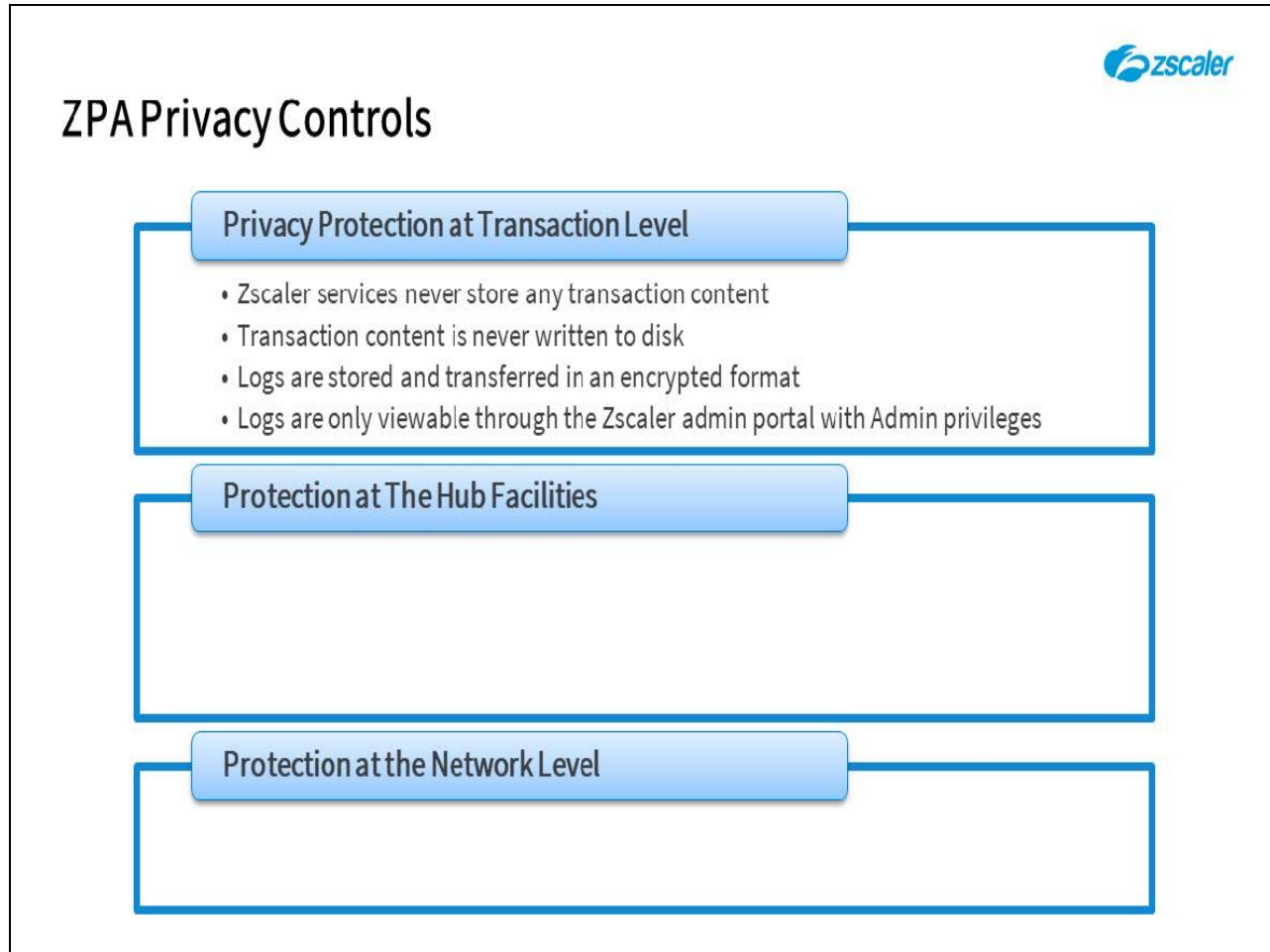


Slide notes

To summarize the ZPA privacy protection controls another way, we provide protections at three levels:

- At the Transaction level;
- The Hub Facilities level;
- And at the Network level.

Slide 10 - ZPA Privacy Controls

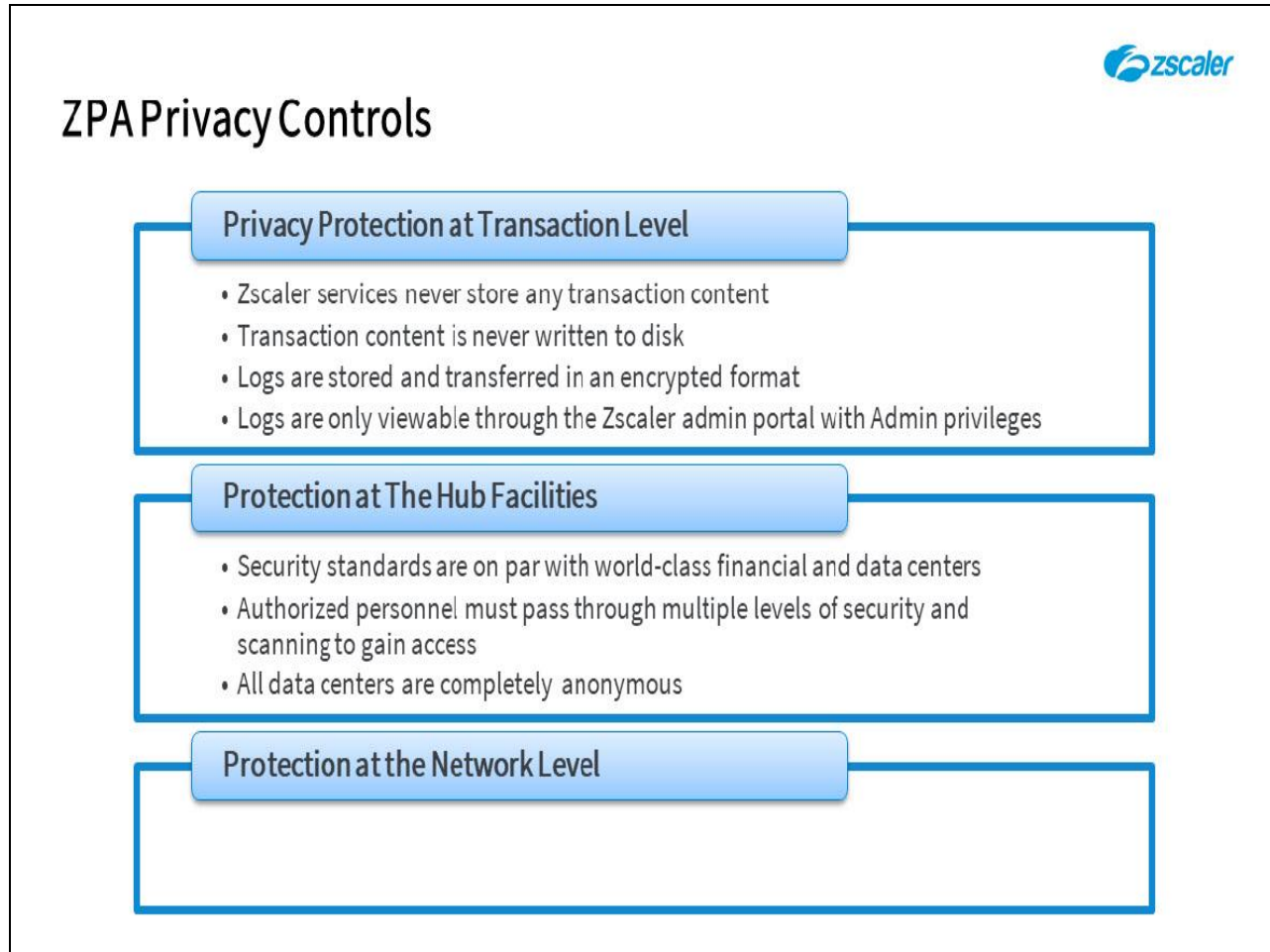


Slide notes

At the transaction level:

- The ZPA service never stores any actual transaction content, it only ever stores tokenized metadata;
- Transaction content is never written to disk, it is only ever processed in memory to forward it to the destination end-points and is immediately 'forgotten';
- Logs are always stored and transferred in an encrypted format;
- Logs can only be viewed and interpreted through the Zscaler admin portal, by a user with admin privileges.

Slide 11 - ZPA Privacy Controls

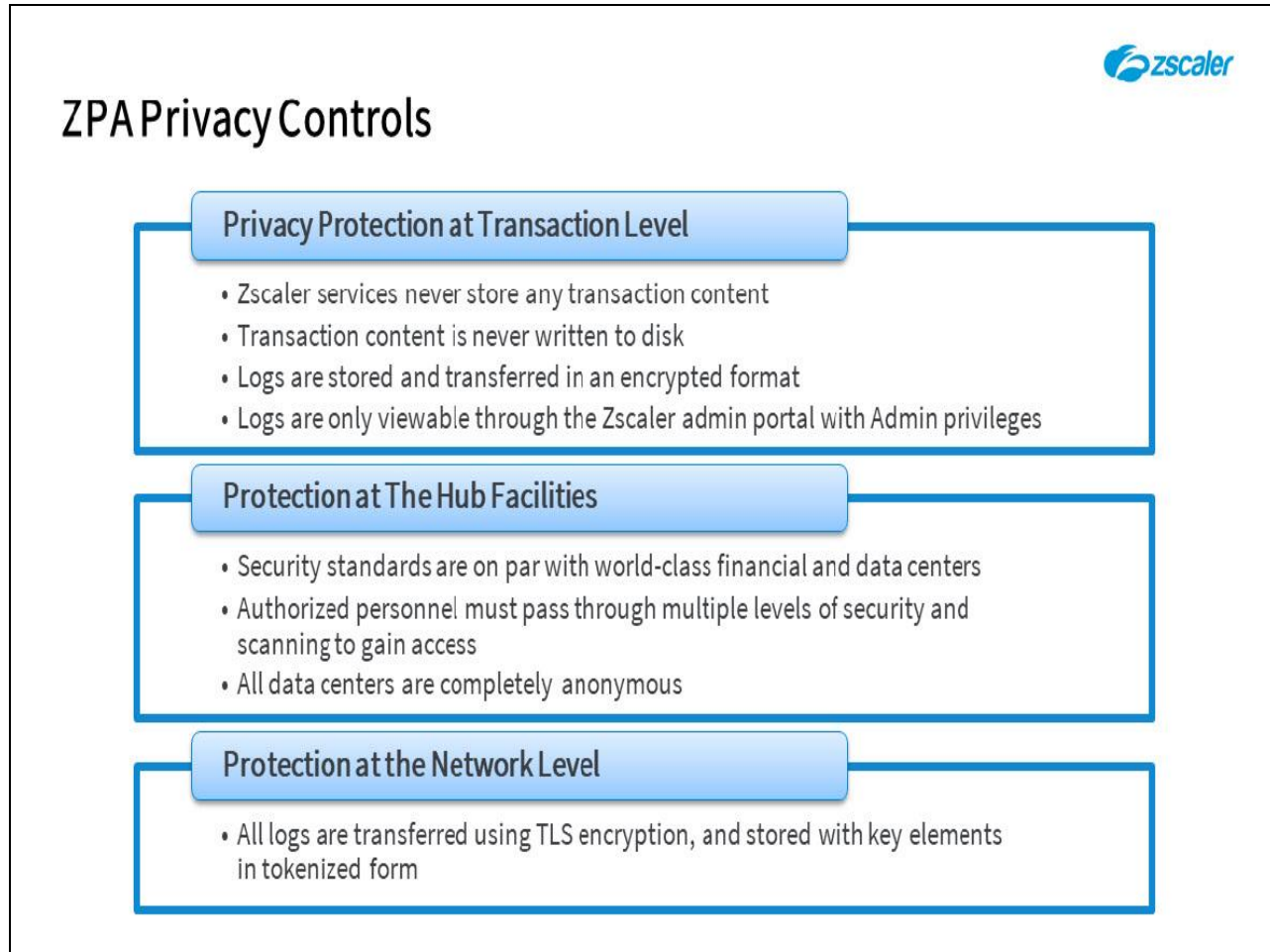


Slide notes

At the Hub Facilities level:

- The security standards of the AWS data centers are on par with those of World-class financial institutions;
- Physical access to the infrastructure is only possible for authorized personnel, who must pass through multiple levels of security and scanning to gain access;
- Plus, all of the data centers are completely anonymous.

Slide 12 - ZPA Privacy Controls

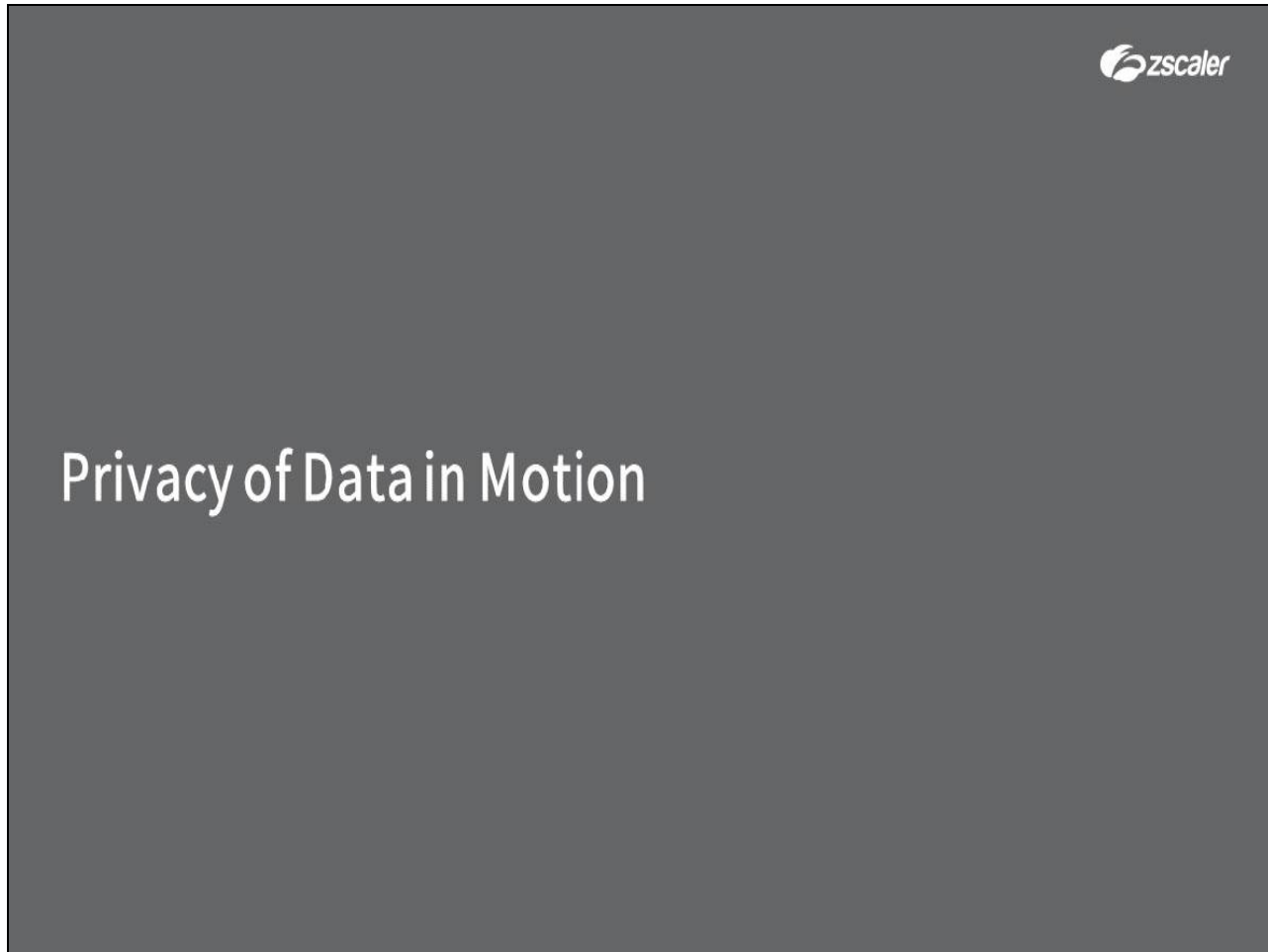


Slide notes

At the Network level:

- Logs are only ever transferred in an encrypted form using TLS 1.2 and the strongest encryption cipher that is mutually supported by the end points;
- In addition, the logs are tokenized to further obfuscate any PII that might otherwise be accessible.

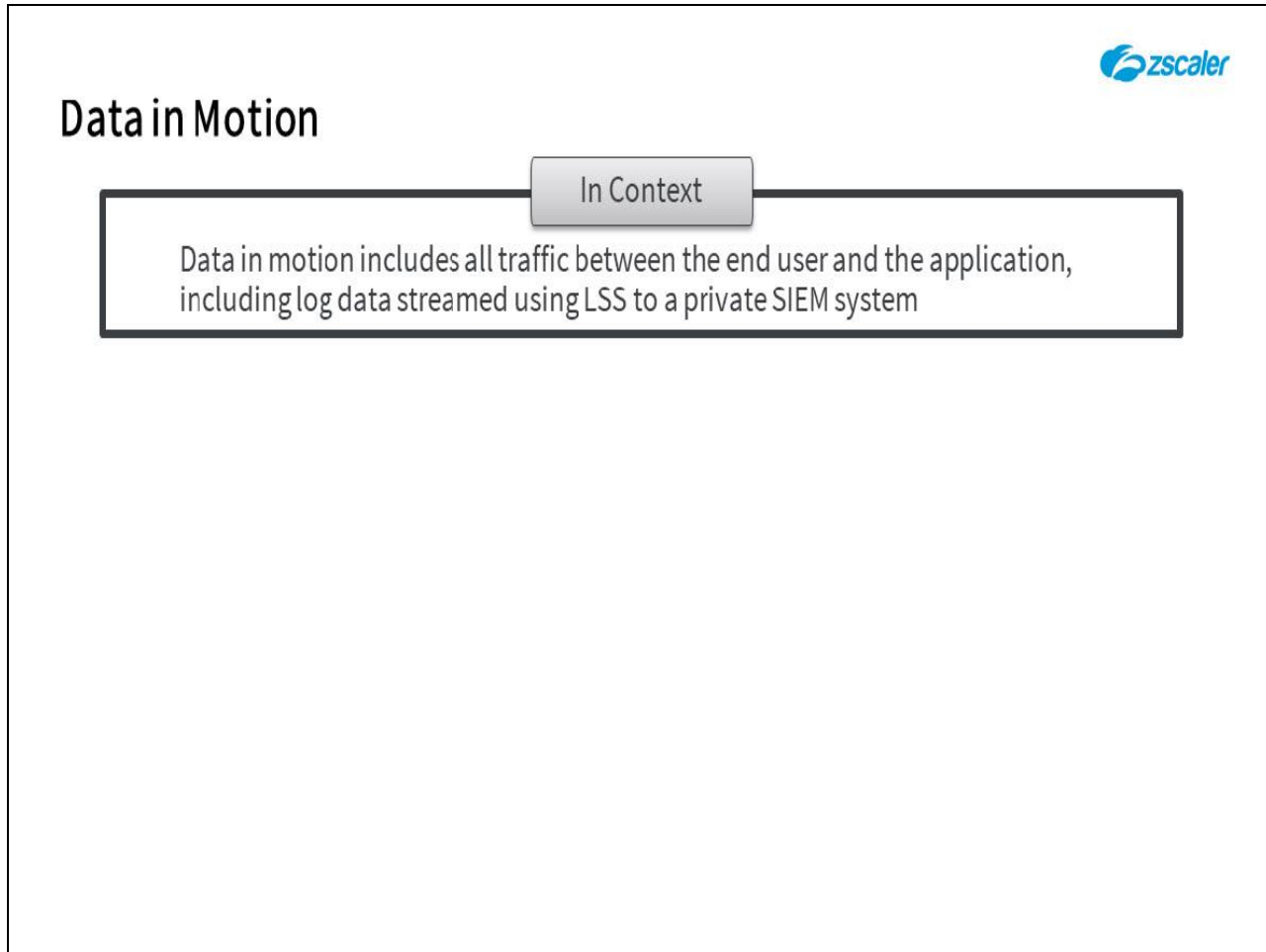
Slide 13 - Privacy of Data in Motion



Slide notes

Let's now have a look in more detail at the privacy of data in motion through the ZPA infrastructure.

Slide 14 - Data in Motion

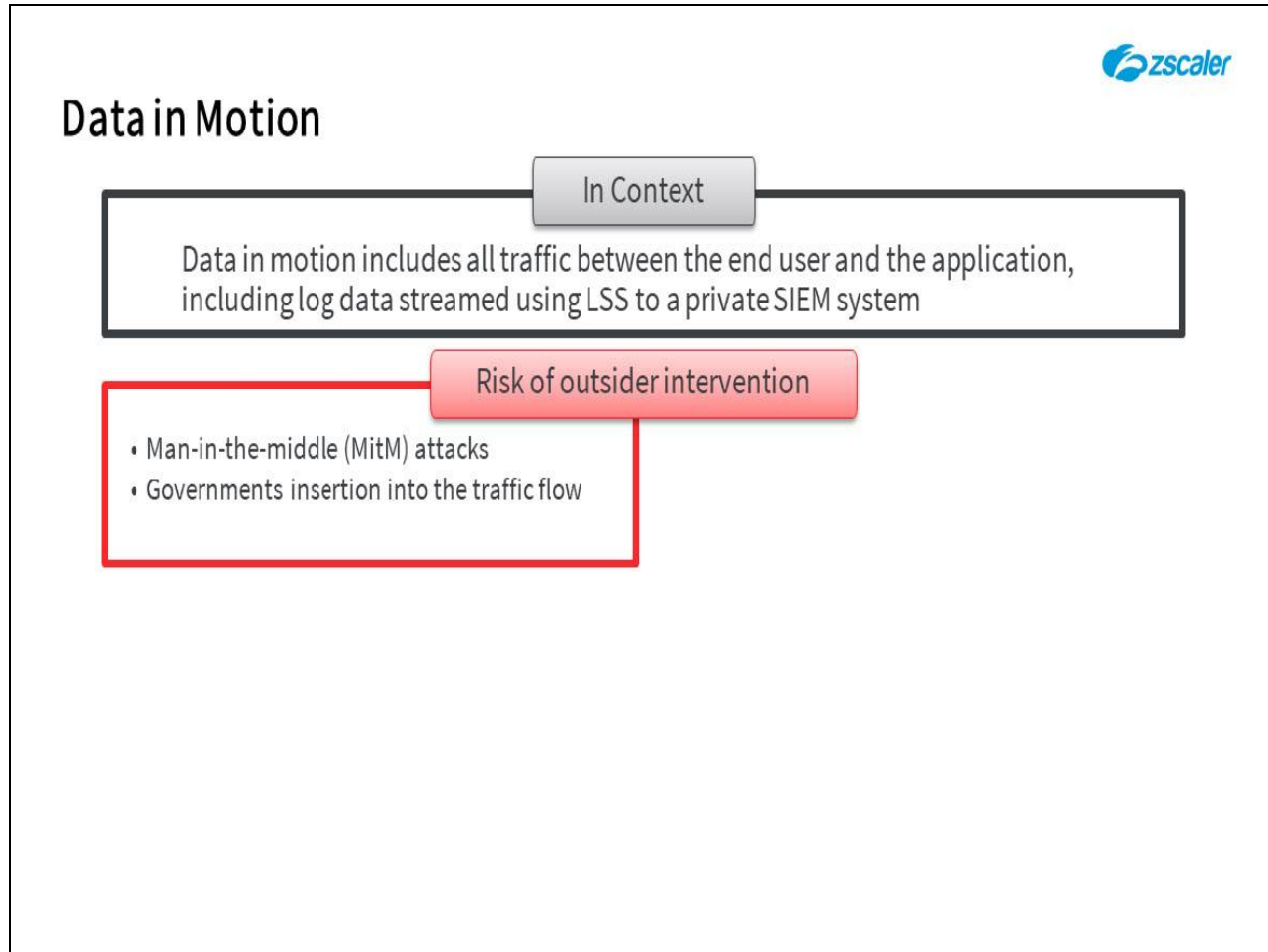


The diagram is titled "Data in Motion" in the top left corner. In the top right corner, there is a Zscaler logo. A horizontal line spans the width of the diagram, with a gray box labeled "In Context" centered on it. Below this line is a large rectangular box containing the text: "Data in motion includes all traffic between the end user and the application, including log data streamed using LSS to a private SIEM system".

Slide notes

Just to specify the context here, we are looking specifically at data in transit across the ZPA infrastructure, whether end user data transferred to or from a private application, or ZPA log data streamed to a SIEM hosted on-premise, or in a private cloud.

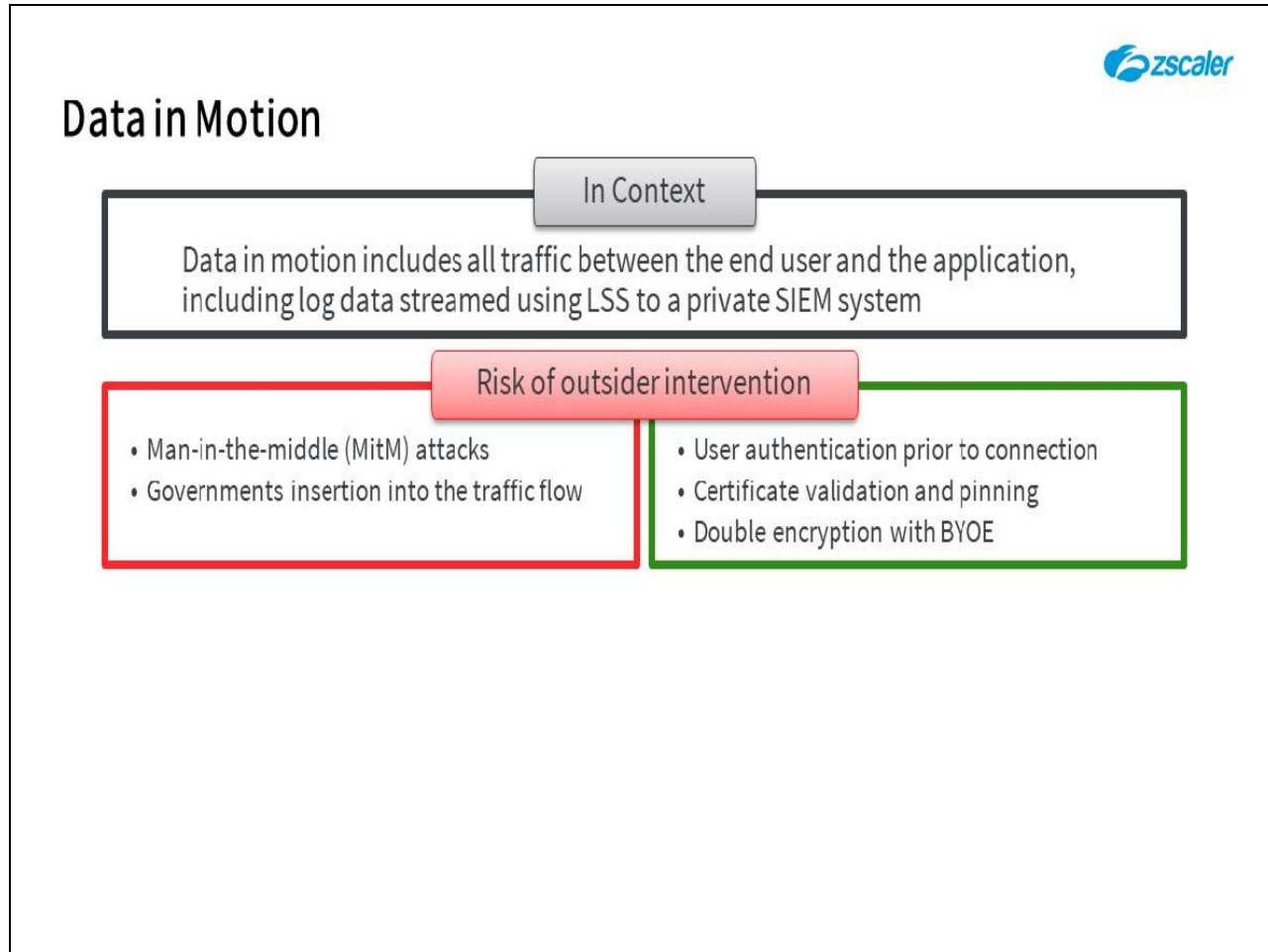
Slide 15 - Data in Motion



Slide notes

Threats from outsiders include potential man-in-the-middle attacks (MitM) mounted by someone with the ability to insert themselves at a key location along the data path, or interception by some government entity that is able to legally insert themselves into the data path.

Slide 16 - Data in Motion



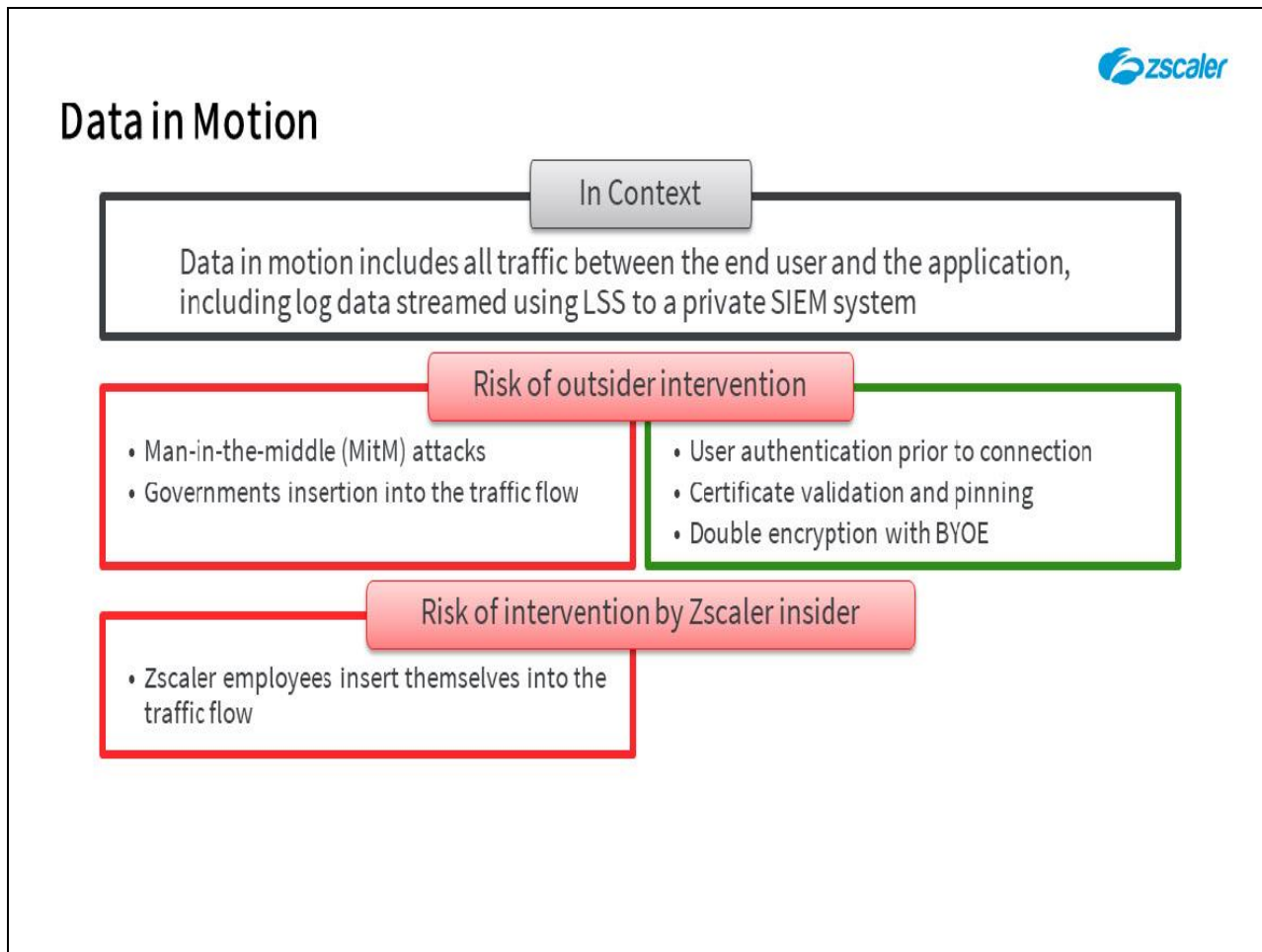
Slide notes

Firstly, most MitM attacks occur at user authentication, when the secure connection is first established, however with Zscaler Private Access, the user is authenticated (within the Zscaler App or in a browser) before any data access requests are processed. All communication between the Zscaler App and the Zscaler cloud uses doubly-pinned certificates generated for this purpose and no connections can be established if certificate validation fails at any point.

Subsequently, data is encrypted at least once and with the **Double Encryption** option may then be encrypted again using keys that are never shared with Zscaler (the BYOE option). The 'legal', government outsider intervention can be mitigated entirely when ZPA is configured in **Double Encrypted** mode with BYOE.

Because of the way ZPA is designed, even if an outsider could insert themselves into the data path, their very presence would prevent any connection from ever being established (due to the mutual certificate validation and pinning), if they are 'sniffing' in some passive mode attack, all they would see is encrypted, or doubly-encrypted traffic. The attacker has no way to reach the applications themselves, as they are not advertised publicly and are not accessible using conventional IP routing. Applications effectively become invisible, or 'dark'.

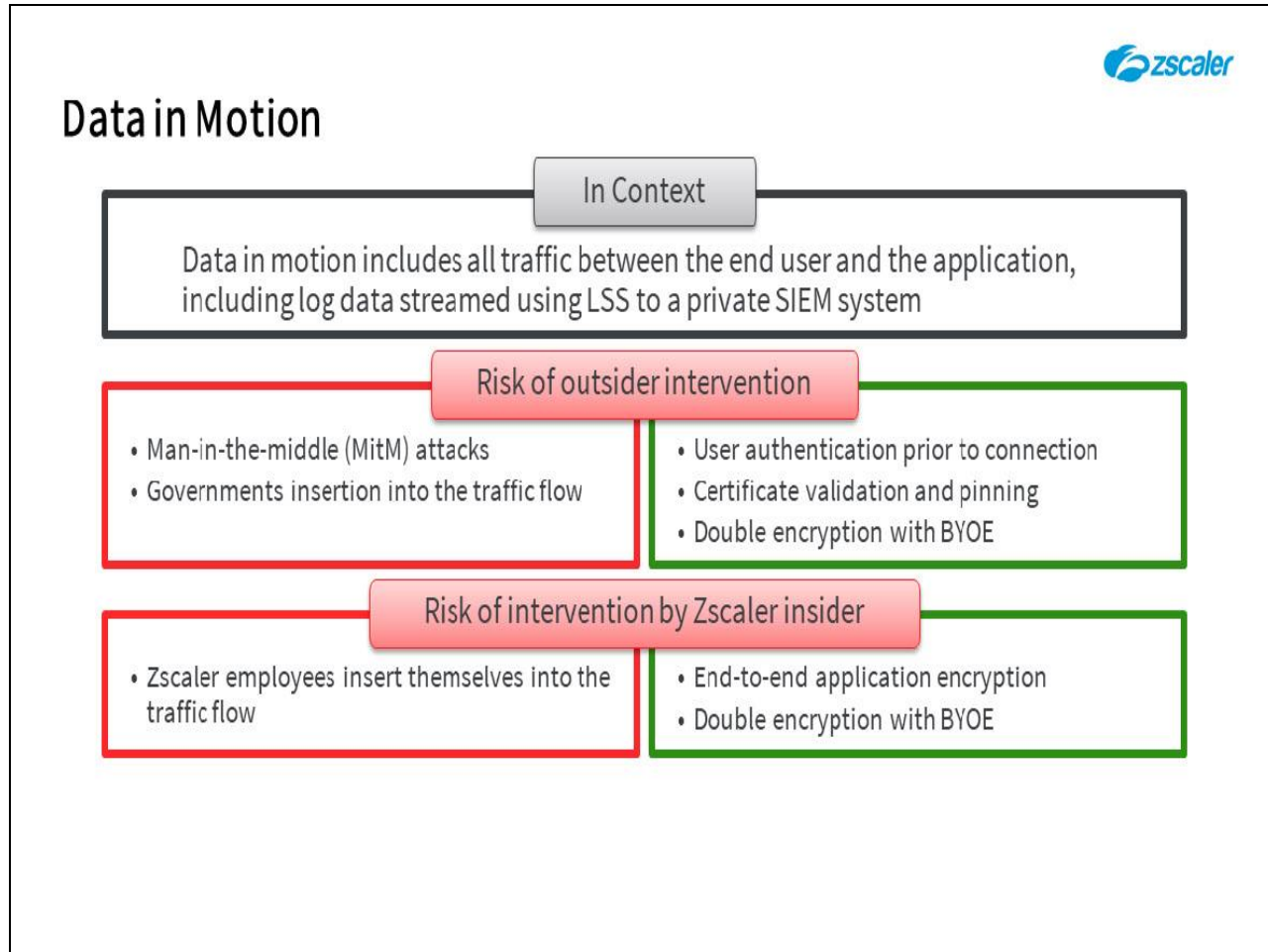
Slide 17 - Data in Motion



Slide notes

For the (hypothetical) threat where a Zscaler employee could insert themselves into the traffic flow, ...

Slide 18 - Data in Motion



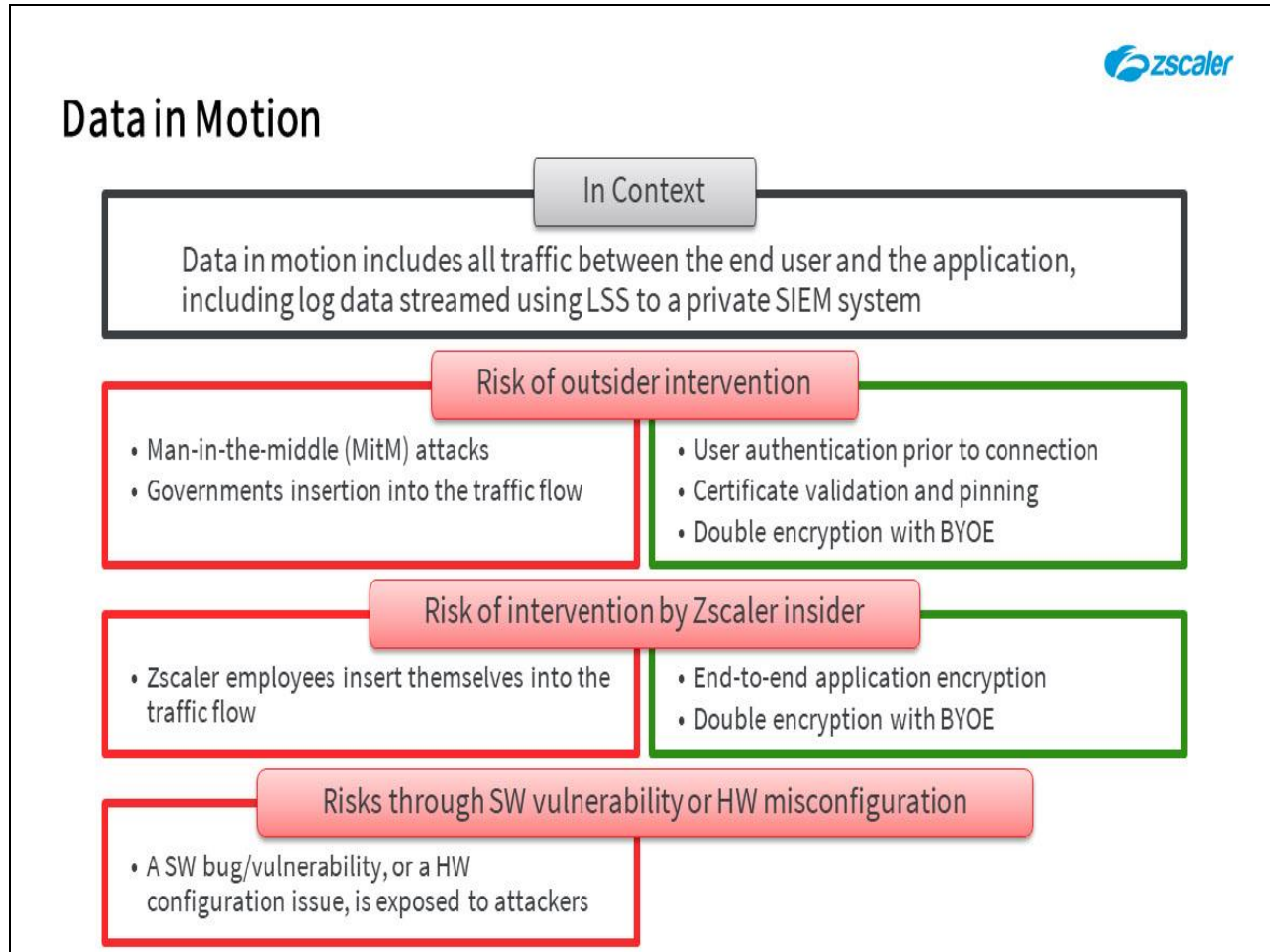
Slide notes

...this threat is mitigated completely, both by the use of end-to-end application level encryption (such as HTTPS) and by the ZPA **Double Encryption** option with BYOE.

If an application is built to be secure in the first place, using HTTPS or TLS, the encryption is established end-to-end through the ZPA tunnels before any data flows. Zscaler has no access to the certificates or keys used for this encryption, so has no ability whatsoever to decrypt and view any data sent.

With ZPA **Double Encryption** mode, traffic is encrypted in the Microtunnel end-to-end using the customer's own public key infrastructure and while the Zscaler cloud facilitates the key exchange, the Zscaler infrastructure itself does not have any visibility whatsoever into the transactions. In this mode, communications occur within a TLS-encrypted tunnel and application requests flow in an interior TLS-encrypted Microtunnel. In addition, the double encryption mode tunnels from the client to the App Connector are also client and server pinned.

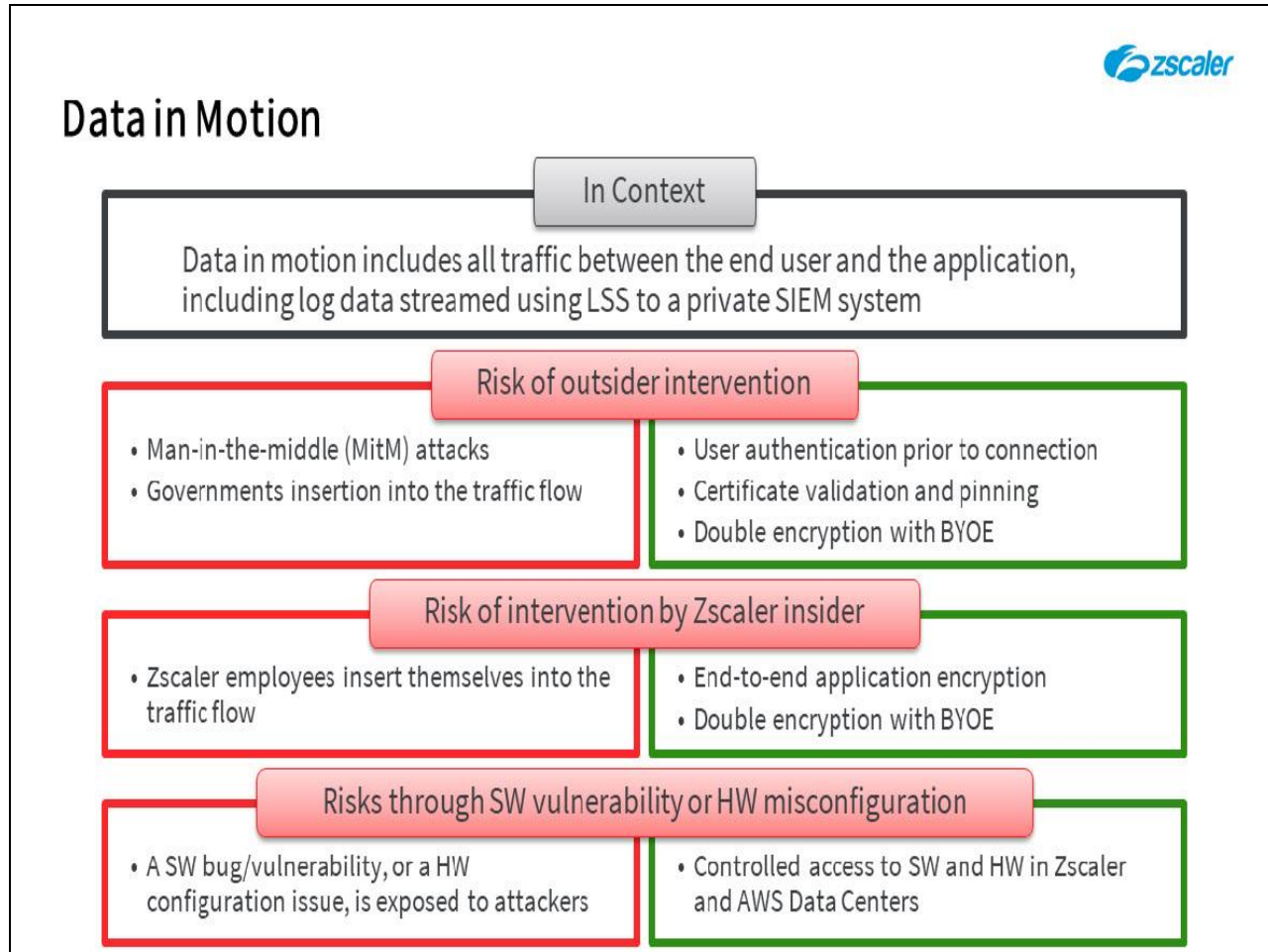
Slide 19 - Data in Motion



Slide notes

Lastly, the threat from some as yet unidentified SW vulnerability, or HW misconfiguration, ...

Slide 20 - Data in Motion

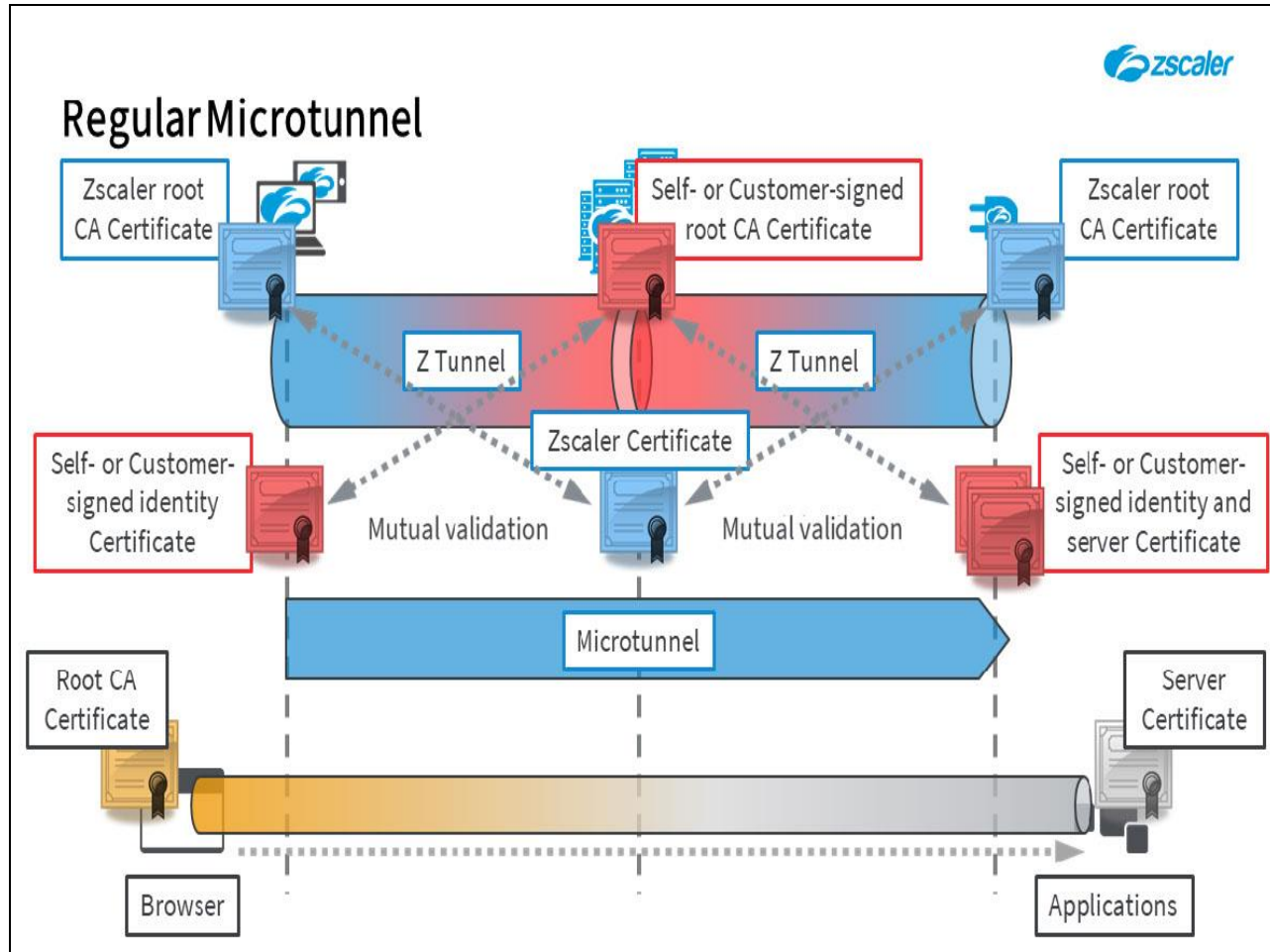


Slide notes

...this threat occurs when a software bug/vulnerability, or a hardware configuration issue is exposed to attackers. Because ZPA is a service, not an appliance or infrastructure component, an attacker's access to the hardware or software involved in the connection is greatly reduced.

Zscaler is completely dedicated to maintaining the security of all components of the ZPA and Cloud Security Platform. Plus, as every component of the Zscaler solution is interconnected, any changes to correct a vulnerability or misconfiguration can be made in close to real time. Another benefit in working with Zscaler is our focus on Internet security, delivering not only the ZPA service, but also the expertise behind it.

Slide 21 - Regular Microtunnel

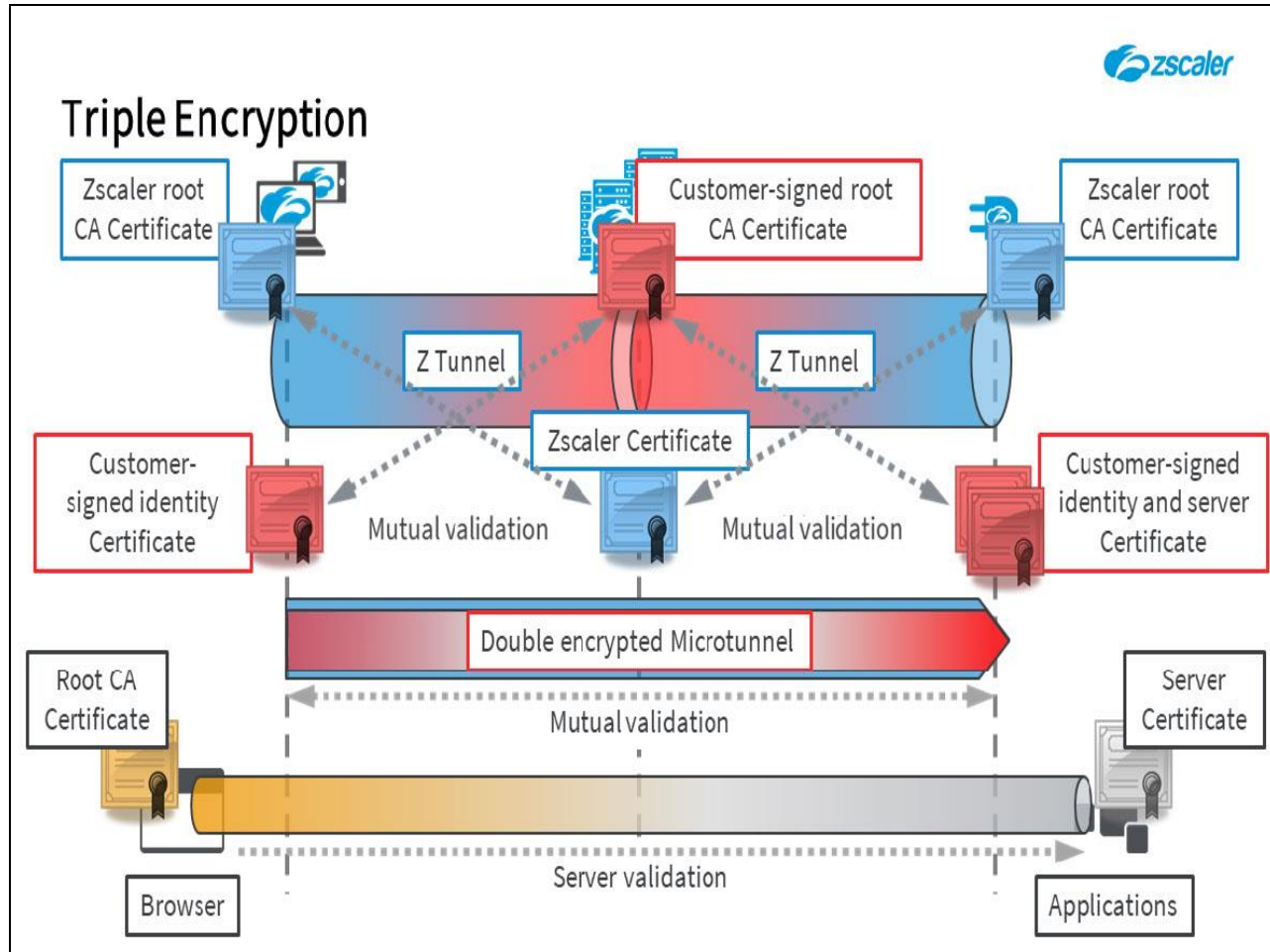


Slide notes

As a reminder, all application access is initiated by the end user through the Zscaler App or in a browser, they are only able to access applications that are made available by the ZPA infrastructure. Application access can only be achieved if (and only if) the encrypted Z Tunnels can be established to the Service Edge nodes without intervention.

Data is subsequently transferred within the Microtunnel established between the Zscaler App (or BA Exporter for **Browser Access** users) and appropriate App Connector. In addition, end-to-end encryption across the Zscaler infrastructure may be applied if the application is anyway configured for TLS.

Slide 22 - Triple Encryption

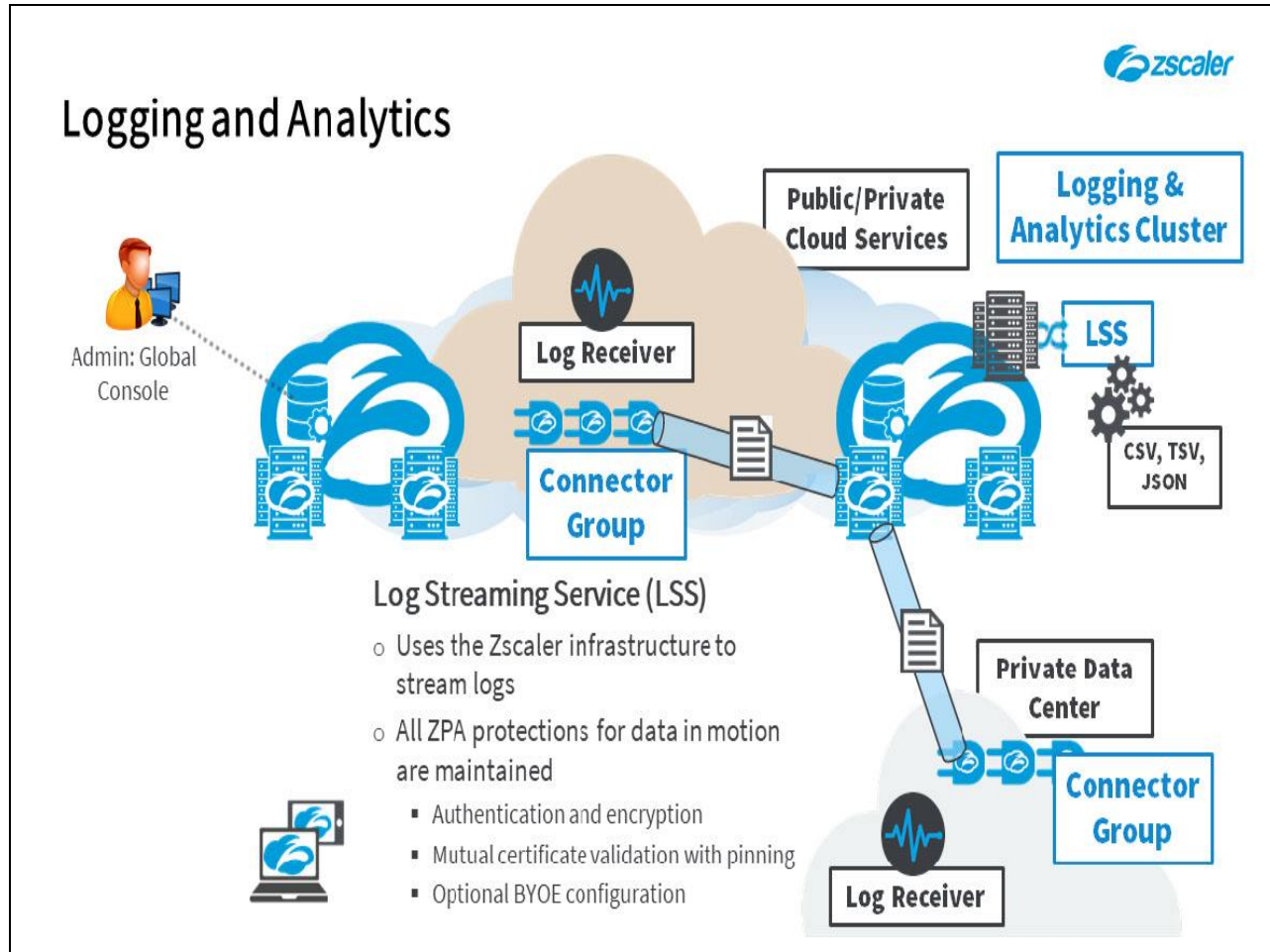


Slide notes

With the BYOE capability and the **Double Encryption** option, data within the internal Microtunnel can also be encrypted using customer keys that Zscaler has no access to. This makes the data transfer completely private from Zscaler, or any government entity that may 'legally' insert themselves on the data path.

Remember, if the application also uses L7 encryption, then this results in the triple encryption of data on this link!
...which is not recommended for performance reasons.

Slide 23 - Logging and Analytics

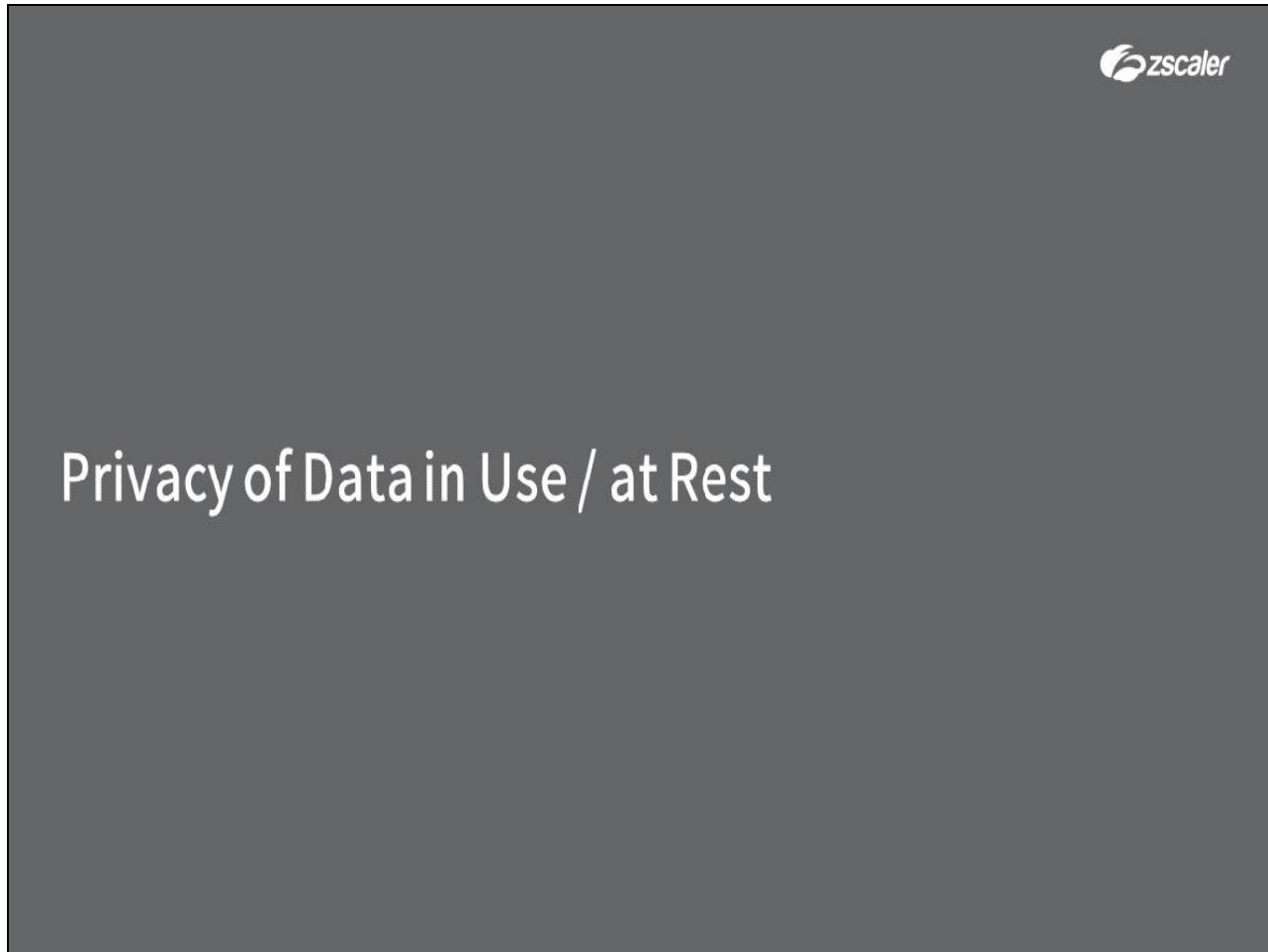


Slide notes

As the ZPA **Log Streaming Service (LSS)** makes use of the App Connector infrastructure for the delivery of logs to your SIEM, all of the ZPA protections for data in motion also apply to this log data.

Note that these streamed logs consist only of metadata, however so that it may be interpreted at your SIEM, the data is not tokenized to obfuscate **company names**, or **usernames**. You will need to ensure the safety and privacy of this log data once it has been received locally by your SIEM.


Slide 24 - Privacy of Data in Use / at Rest



Slide notes

Finally, let's have a look the threats to data in use on the ZPA infrastructure and to data at rest.

Slide 25 - Data at Rest



Data at Rest

In Context

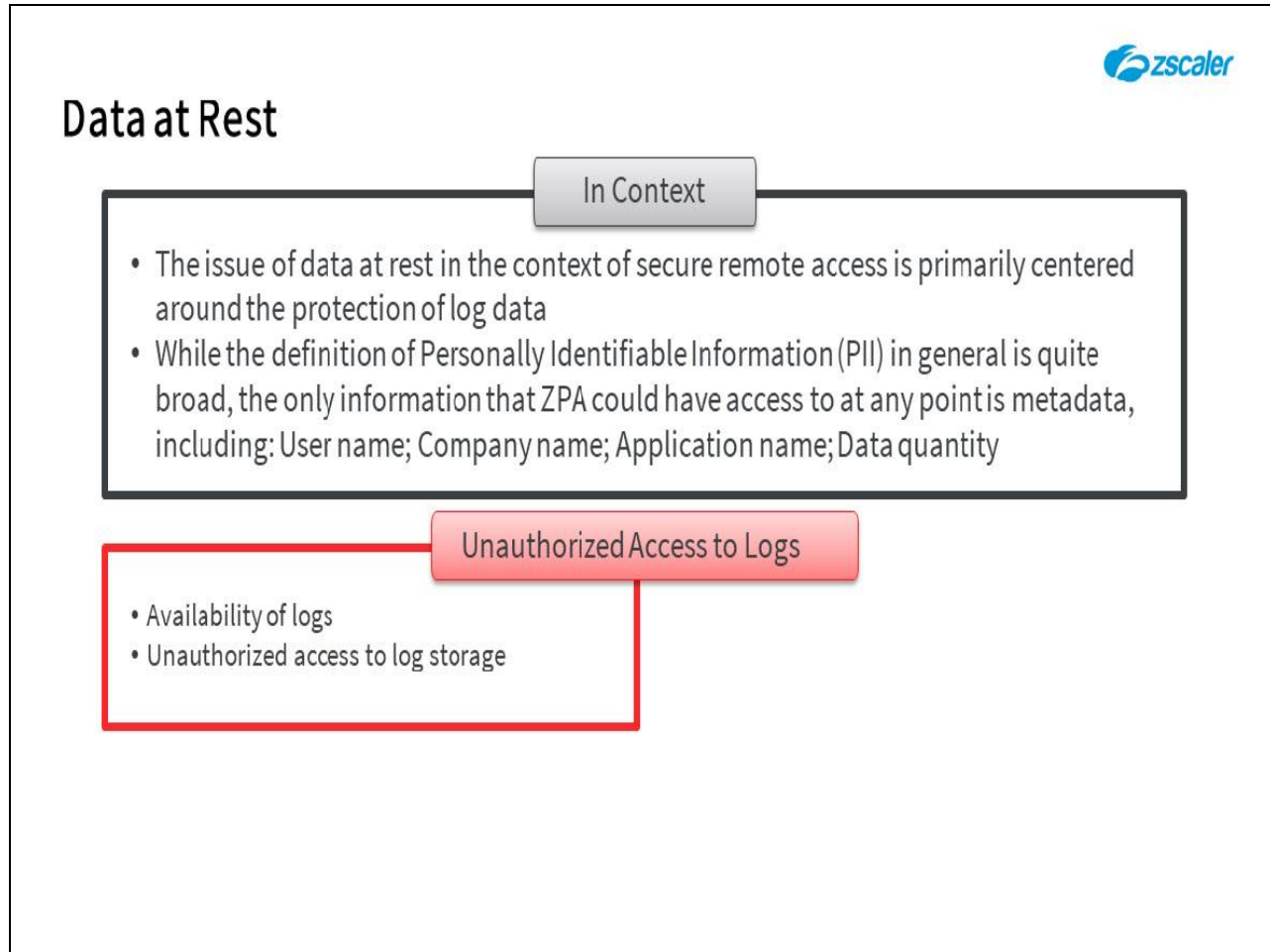
- The issue of data at rest in the context of secure remote access is primarily centered around the protection of log data
- While the definition of Personally Identifiable Information (PII) in general is quite broad, the only information that ZPA could have access to at any point is metadata, including: User name; Company name; Application name; Data quantity

Slide notes

When discussing data in use, or data at rest in the context of the ZPA service, we are really talking about the privacy of data logged by the system, as application data is only ever transported by the service for end-to-end delivery (with all the privacy measures discussed in the previous section).

Protecting PII is vital for any organization in order to maintain public trust, protect reputation and protect against legal liability. While the definition of PII in general is quite broad, the only information that ZPA could have access to at any point is metadata from the logs, including; **usernames, company names, application names** and **data quantities**.

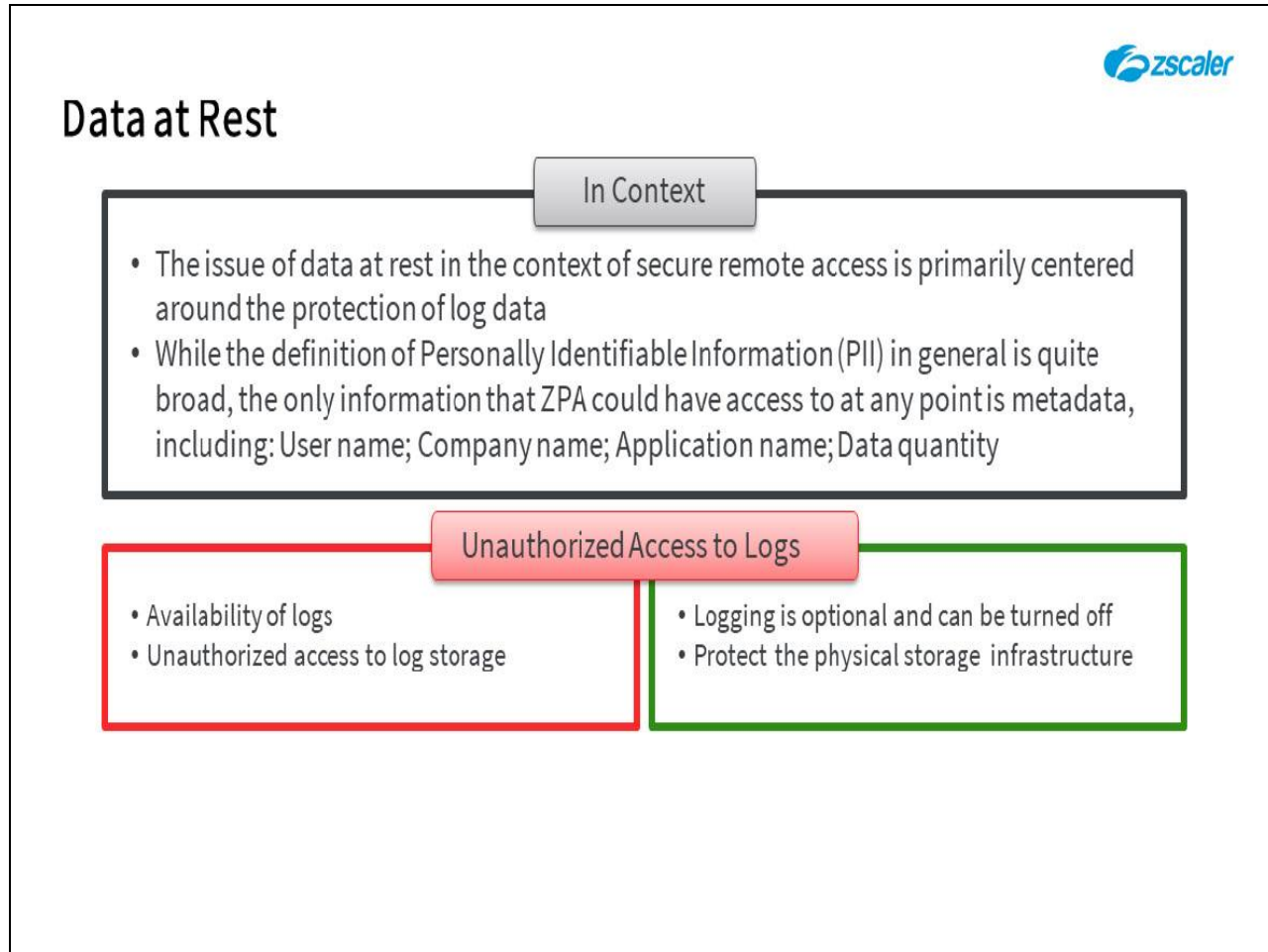
Slide 26 - Data at Rest



Slide notes

Privacy concerns in this context center on unauthorized access to that log data, or unauthorized access to the log storage infrastructure. Even if logging is disabled, in theory at least limited insights could be still be derived in the absence of actual transaction logs by examining a users' activity logs. The assets that were accessed by a user and from what device/location, could theoretically be used to plan an attack on the user, the location, or even the device.

Slide 27 - Data at Rest



Slide notes

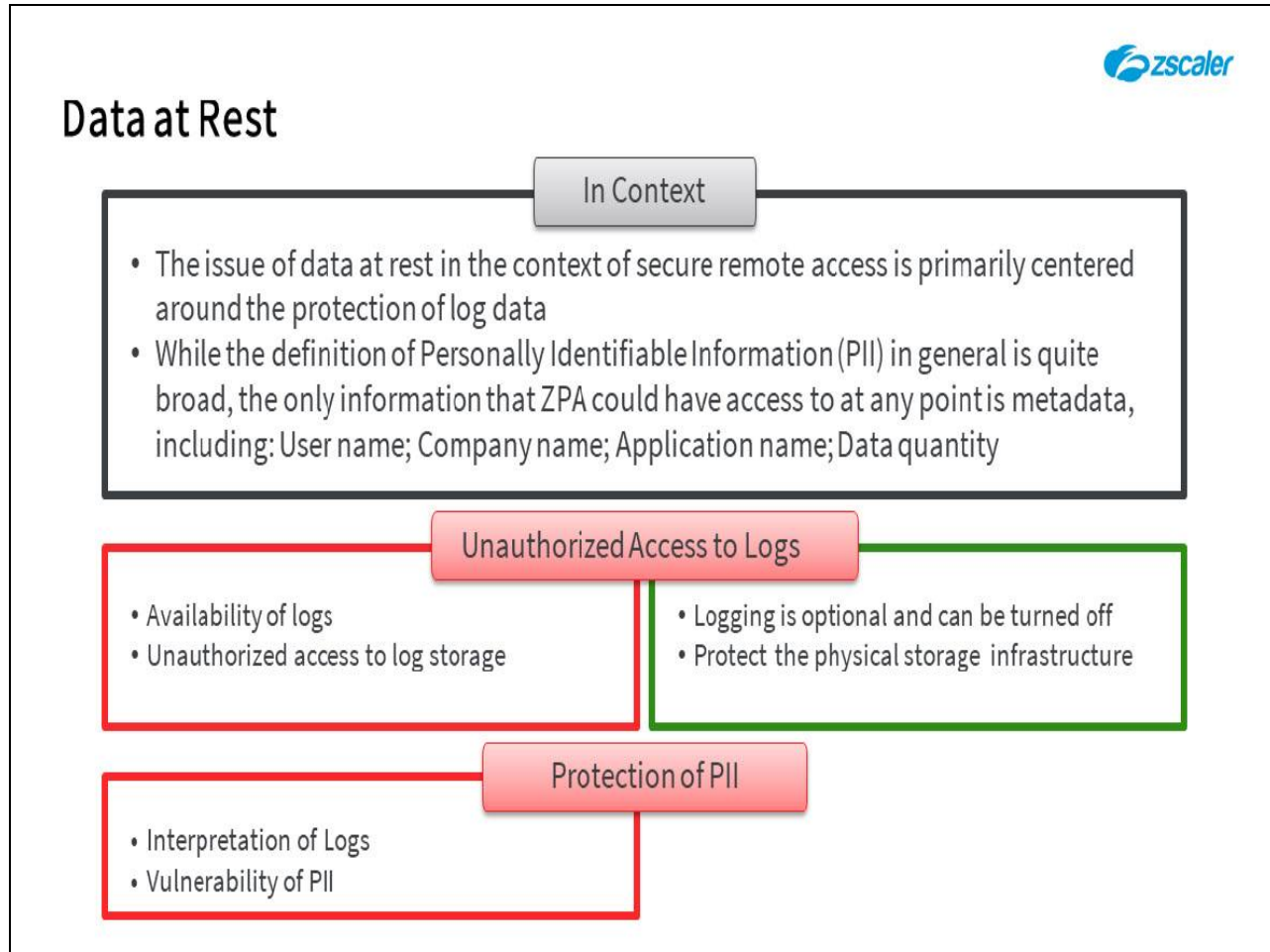
The first thing to understand with the ZPA service, is that customers have the ability to disable logging completely, should they choose to do so. Because ZPA provides only authenticated-user-to-named-application access and all traffic is internal to the customer, logging can be disabled without impacting the service in any way.

The Zscaler infrastructure that houses log data is located in AWS and subject to all the security, privacy and compliance safeguards provided by AWS to its millions of users, including:

- **Data privacy** - Complete information about AWS protections for data privacy, including where data is stored and how AWS complies with new EU privacy strictures, can be found here: <https://aws.amazon.com/compliance/data-privacy-faq/>.
- **Data security** - Details of AWS security measures, including a map of resources to ensure geo-locationing, is available here: <https://aws.amazon.com/security/>.
- **Regulatory compliance** - For a look at how AWS enables strict regulatory compliance, as well as links to the AWS stance on specific certifications/attestation; laws/regulations and privacy mandates; and alignments/frameworks, click here: <https://aws.amazon.com/compliance/>.

In addition, although the ZPA Service Edge nodes are responsible for generating some of the log data, they never store logs, they only ever process them in memory. While the Service Edges are located around the globe, they are always hosted in industry standard, secure and certified data centers. Unauthorized access to the ZPA hardware in these data centers to mount some form of physical attack to recover log data is extremely unlikely.

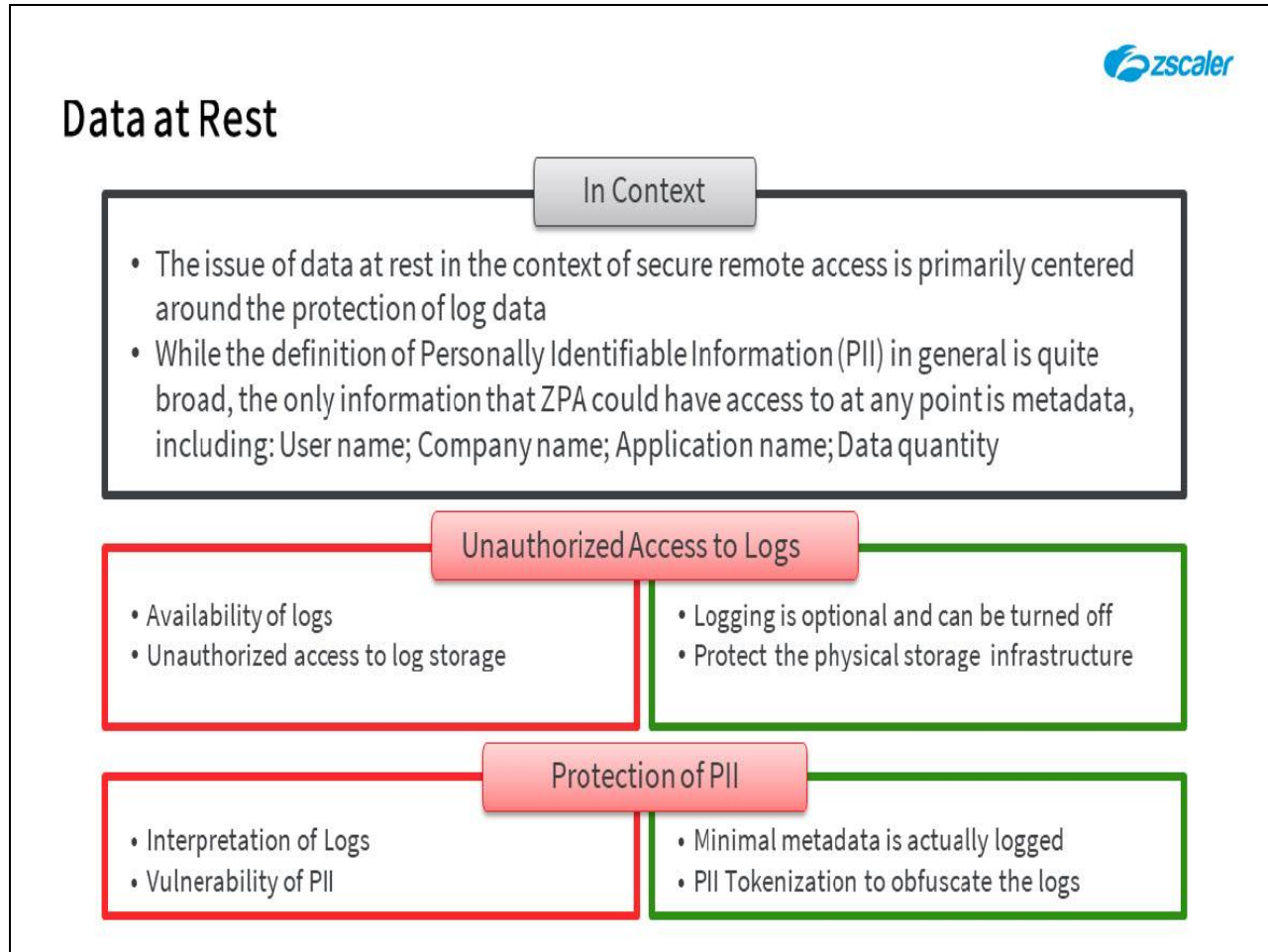
Slide 28 - Data at Rest



Slide notes

Should somebody gain unauthorized access to the logs, they would still need to be able to interpret them in order to exploit the PII that they may contain.

Slide 29 - Data at Rest



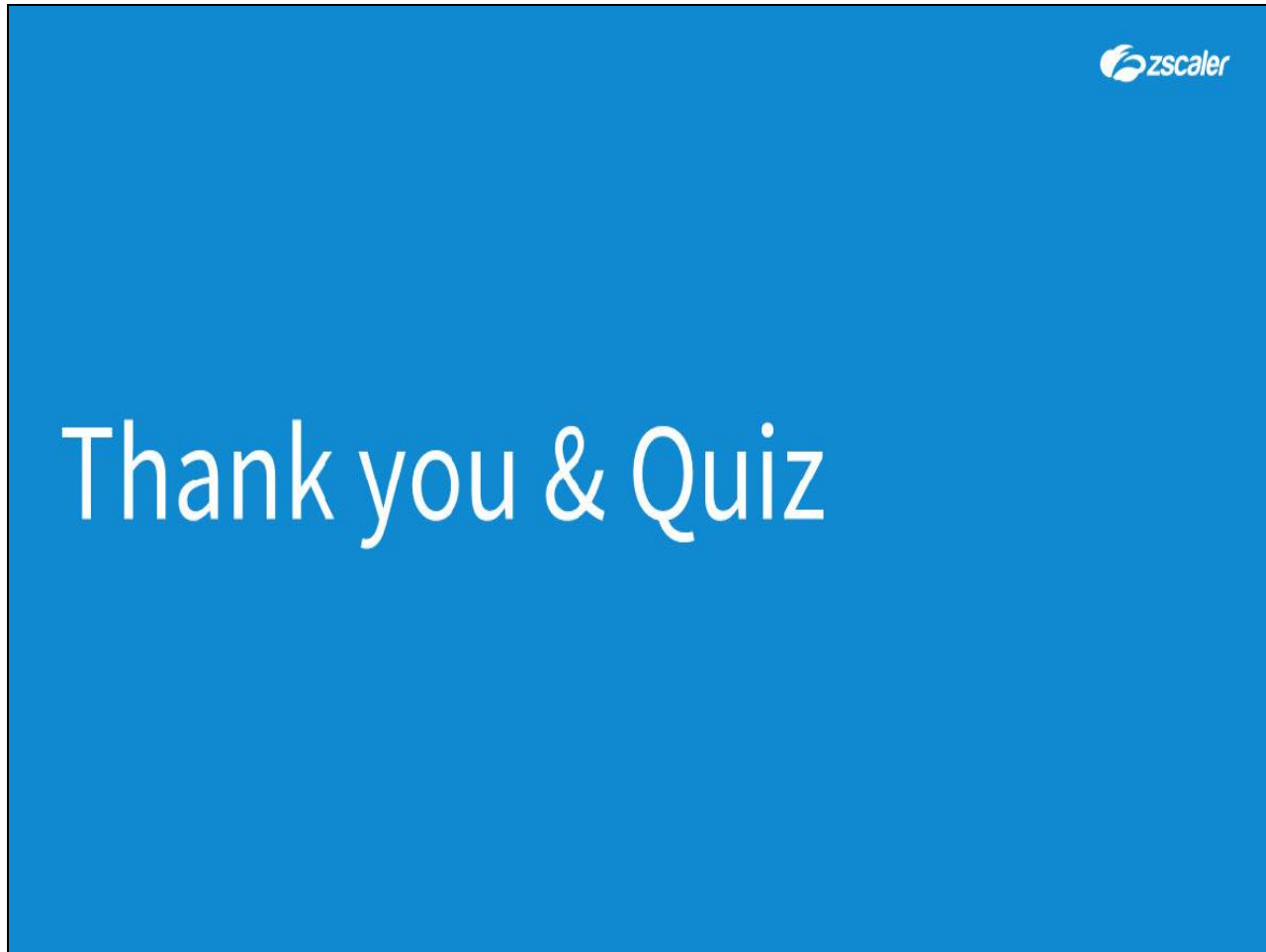
Slide notes

It is important to understand that even when ZPA is enabled to do 'full' logging, key elements of the recorded metadata are tokenized. This ensures that even in the case of records being obtained by attackers, they are of no practical use. Because ZPA is designed to keep the transaction itself completely private and the ZPA infrastructure never inspects the data payload, the only information available to Zscaler is the quantity of data transferred.

ZPA logs therefore, contain data about the nature of the transaction, but no information about the contents of the transaction at all. All entries are in the form of abstract identifiers and contain no PII.

If the customer prefers to have no information written, regardless of security measures or location of records, ZPA can be configured to stream the metadata highlighted above to the customer in real time.

Slide 30 - 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.