PUBLIC V2.2 Oct 2023

ASITE™

Connecting people and
helping the world
Build Better

Asite Platform
High Level Diagram and Data Flow Diagram

Platform Architecture

ASITE™

Logical Design

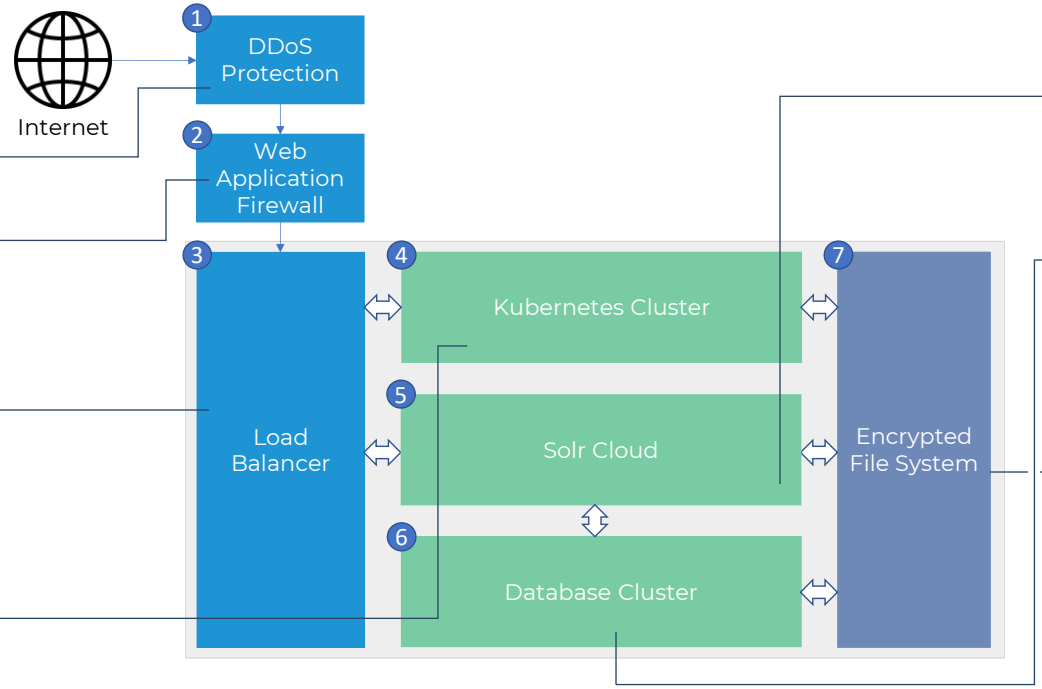
The Asite platform uses a standard architecture in order to reduce complexity, minimise risk and simplify ongoing maintenance and assurance.

1. Distributed Denial of Service Protection (DDoS): Ensures availability of the platform and protects against various denial of service attacks.

2. Azure Web Application Firewall: The first point of contact for a client request - Web Application Firewall and Load Balancer.

3. Load Balancer: Routes requests depending on availability and usage levels. Offloads TLS operations which results in a higher throughput of requests by the web server.

4. Kubernetes Cluster: Hosts multiple instances of application servers, and 1:1 relationship between web servers and application servers



5. Solr Cloud: Searching and indexing is provided by the Apache Solr enterprise search platform.

6. Database Cluster: Most client requests require access to database and/or dedicated file storage, this is dealt with by a clustered Microsoft SQL Server service.

7. Encrypted File System: The application servers process client requests, access resources like file and data base systems and ultimately reply to the client with a response.

Reference Architecture

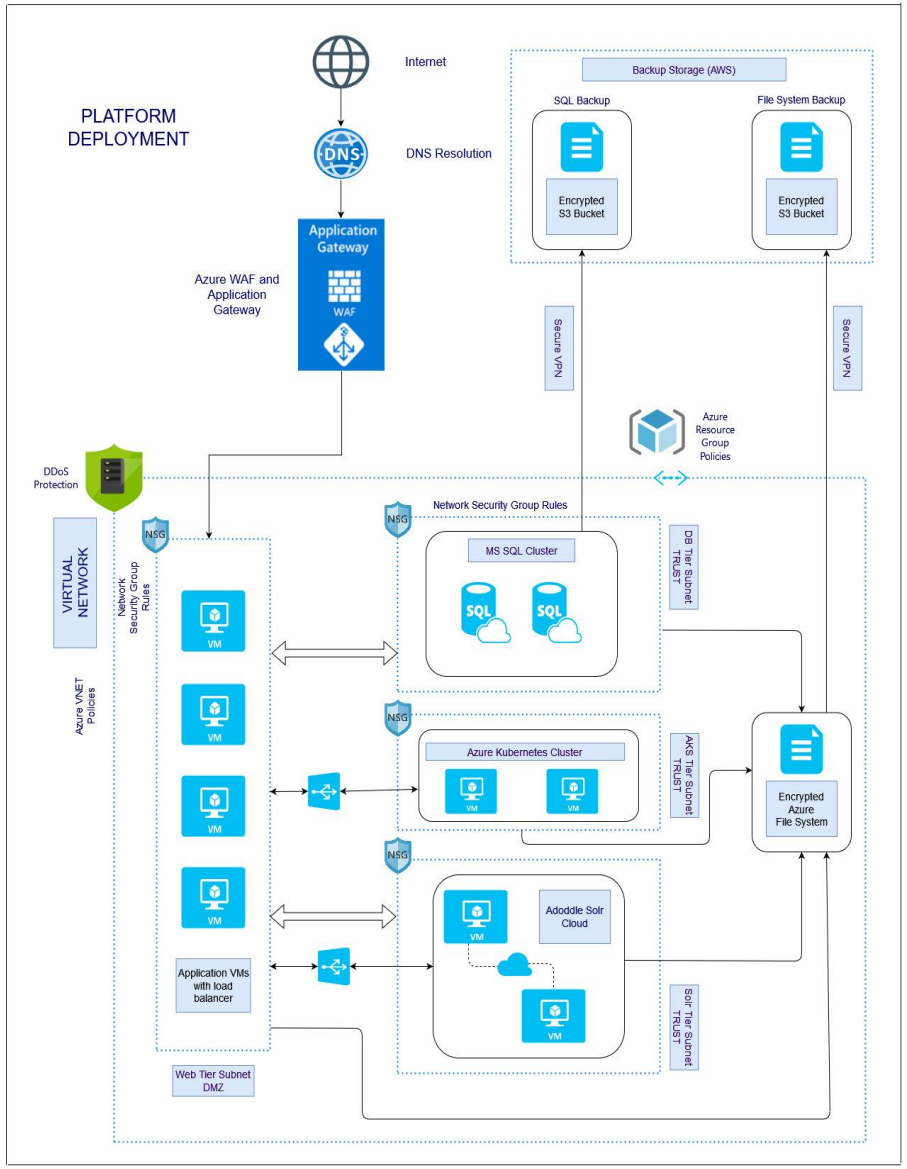
The “Reference Architecture” describes the technical design by which an Asite platform instance is built and maintained.

This diagram shows the Asite solution as hosted for UK clients in the Microsoft Azure (UK South) data centre, the AWS (EU-West-2) and its connectivity to end users.

Currently Asite have datacentres in

USA, Canada, UK, Netherlands, UAE, KSA, Hong-Kong and Australia

All countries have at least two datacentres and redundancy to other two in a different cloud provider.



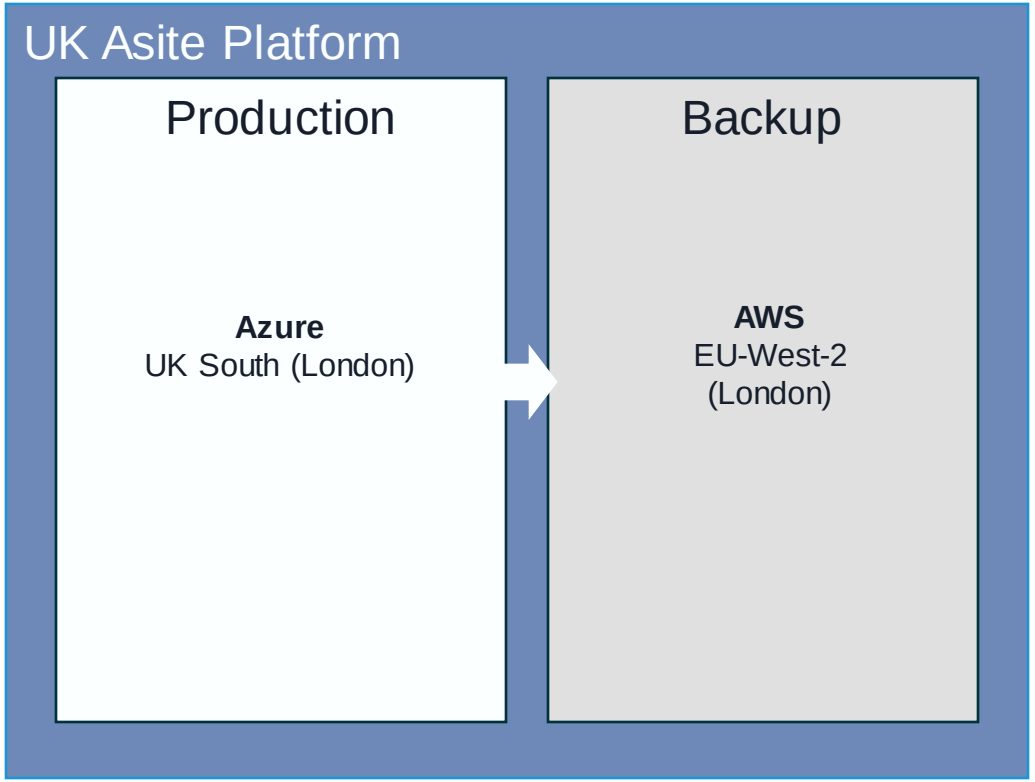
Transfer of data between Production and Backup is fully encrypted.

Data at rest is encrypted using Azure “Encrypted File System”, and AWS “Encrypted S3 Bucket”.

Implementation Architecture – Data Sovereighnity

The implementation architecture describes the specific technical configuration for the production instance of the Asite Platform, Asite guarantees the data hosting in the country of choice.

The UK Asite Platform instance is wholly hosted within the UK, with no data leaving the UK.

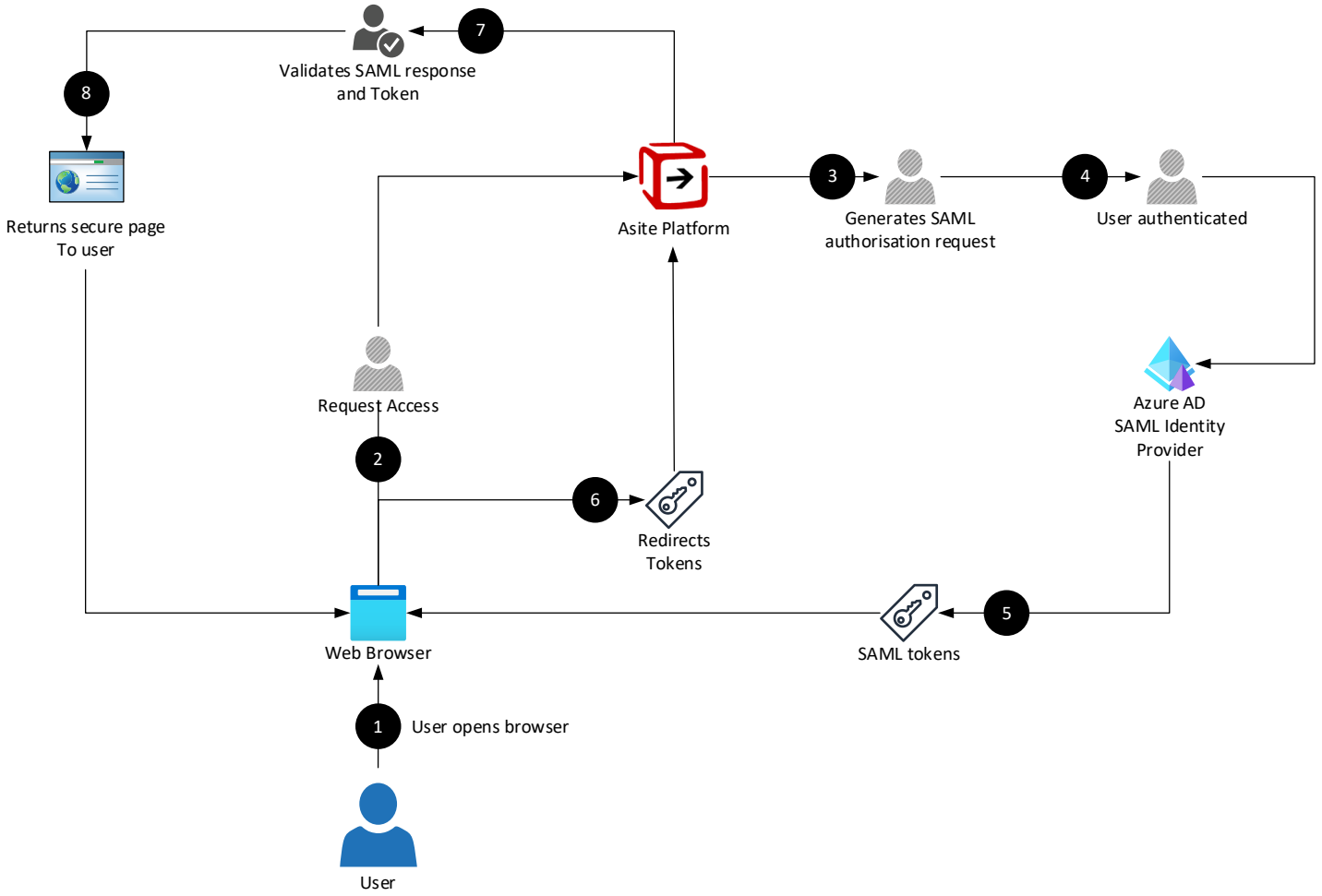


Production (Azure):
The production environment uses Microsoft Azure services:
- The IaaS platform demonstrates significant resilience as detailed in Microsoft's response to Principle 2: Asset Protection and Resilience of the NCSC 14 Cloud Security Principles.
- Additionally, multiple redundant server instances are configured, and filesystem and SQL Server backups have been enabled and configured in Azure.

Backup (AWS):
Backup facility for the Asite platform is hosted on the Amazon Web Services (AWS) S3 Cloud Solution, which aligns to the NCSC 14 Cloud Security Principles.
- Data is transferred via a 256-bit AES encrypted VPN connection and data at rest is stored in encrypted format on the AWS S3 Cloud, which uses Server-Side Encryption with Customer-Provide Keys to encrypt data stored-at-rest.
- AWS support is located within the EEA to ensure compliance with GDPR principles.

Authentication

Client Identity – Logical Architecture



The Asite SaaS Platform supports SSO via SAML v2.

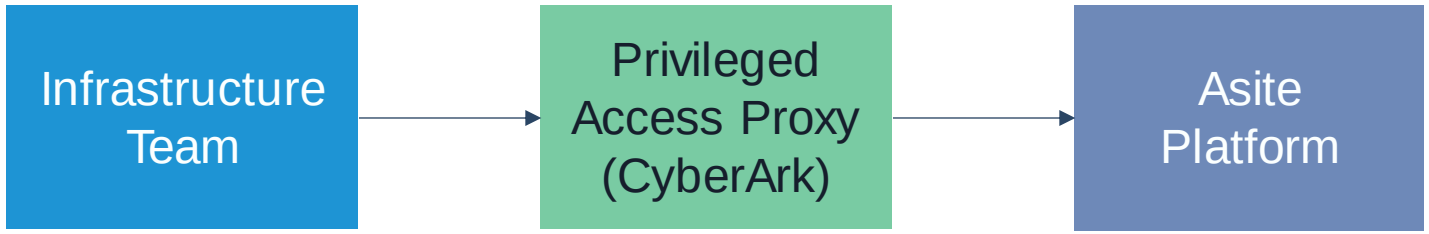
Integration provides the following benefits:

- Control of who has access to the Asite platform via your identity service.
- Users can be automatically signed-in to the Asite Platform (Single Sign-On) with existing accounts.
- Central management of accounts using existing client processes.

Support Architecture

Infrastructure Support : Information Access and Segregation

Access to the Asite platform is controlled by “Privileged Access Proxy” (CyberArk). This ensures access to the platform is carefully protected, controlled and audited.



Principles

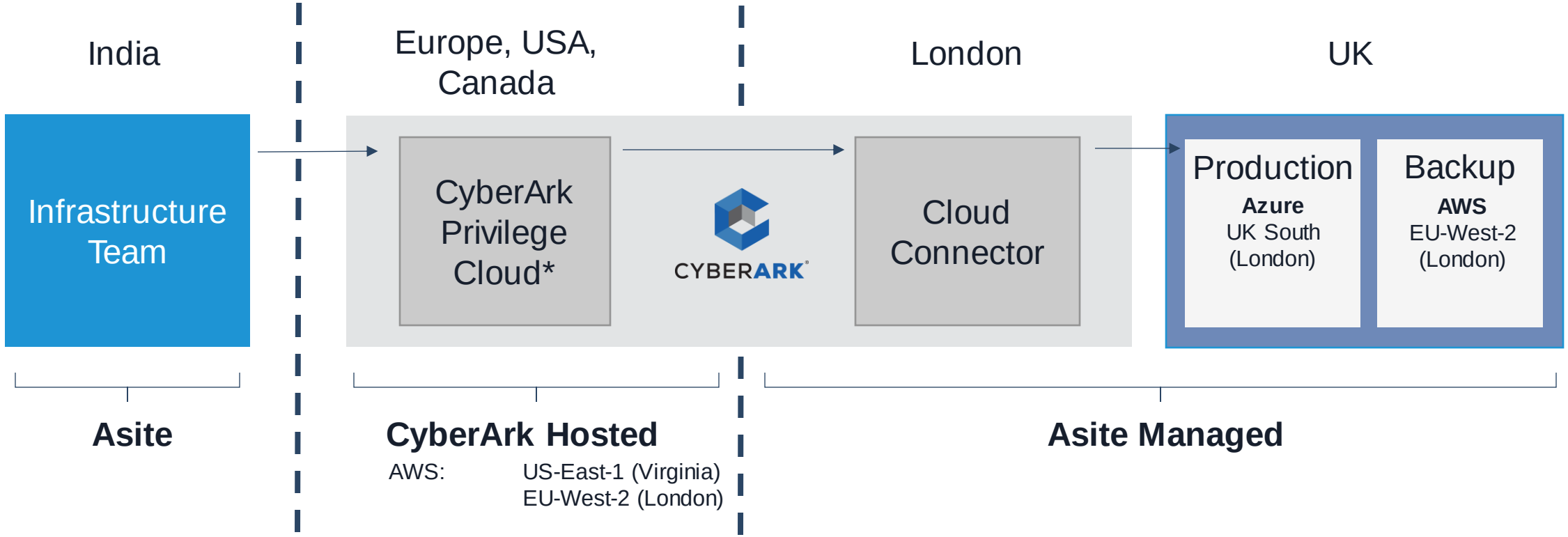
1. All admin access to servers is via Privileged Access Proxy (CyberArk) service
2. No user has direct access to servers (see above)
3. All access have several layers of authentication, all using 2FA/MFA
4. All access and activity is recorded, auditable and audited.

Asite data security includes certification for documents up to UK MoD *Official Sensitive* as per Asite UK MoD DART certification

Ministry of Defence

Infrastructure Support : Geographic Locations

Access to the Asite platform is controlled by “Privileged Access Proxy” (CyberArk). This ensures access to the platform is carefully protected, controlled and audited.



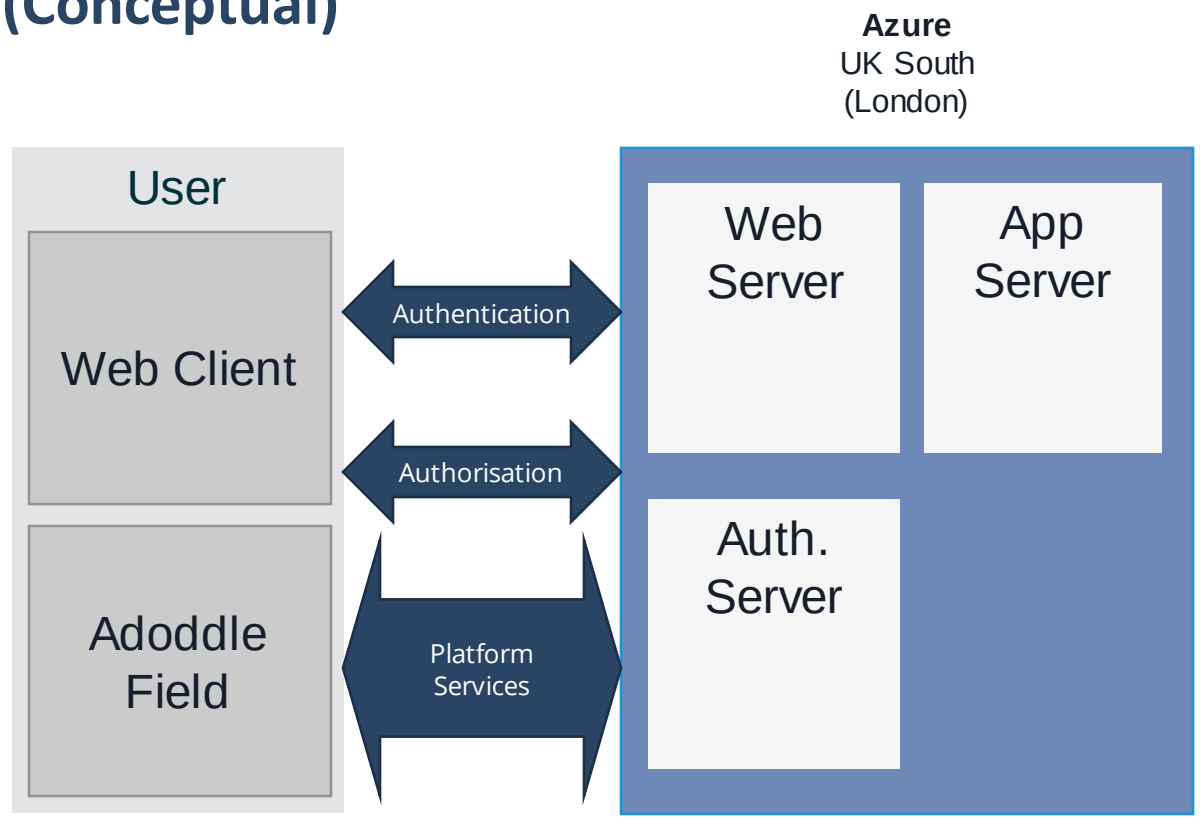
*CyberArk Privileged Cloud is configured and maintained by Asite security team, with the platform hosted by CyberArk

Appendix

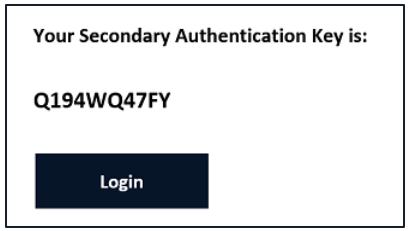
ASITE™

Thank you

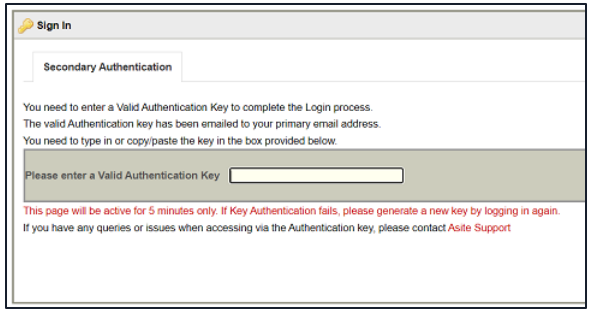
Asite Identity - Authentication Architecture (Conceptual)



1. The user inputs their login credentials to access the platform.
2. After successful authentication, the user receives an email with a secret code to their registered email address.



3. The user inputs the secret code.



4. This allows the user to successfully log into the Asite platform and access permitted data and functionality.

Asite Identity - Authentication (MFA) Sequence Diagram