



## Technical & Security Overview

### Data Centre - Key Features

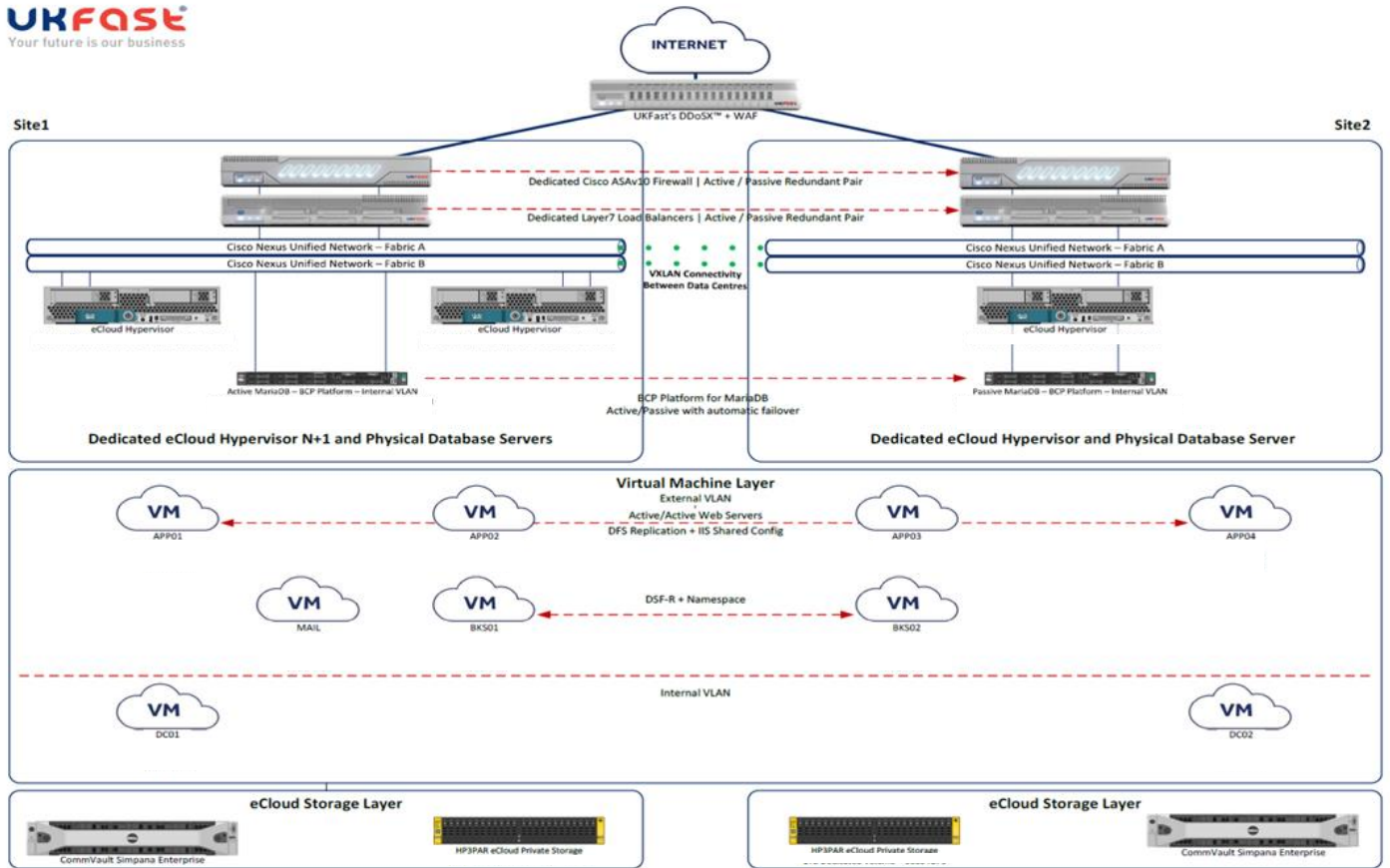
- ISO–Certified tier 3 data centres located at ANS Group Data Centre, Manchester, UK.
- Accreditations – SO27001:2013, ISO9001:2008, ISO14001:2015, ISO 27018:2014, Cyber Essentials, G-Cloud 9, PAS2060, PCI DSS Compliance.
- 24/7/365 UK based support – round the clock HQ & on-site DC engineers.
- 15 min rapid response + 1hr hardware replacement guarantee.
- Redundant high-capacity power supplies, scalable for future expansion to ensure continuous operation.
- UPS and diesel generator system ensures continuous power supply to all equipment capable of supporting the site indefinitely in the event of mains failure.
- DX chillers, in N+1 configuration, for each data hall and external units that cool the refrigerant and pass through the Computer Room Air Conditioner (CRAC) unit.
- Sophisticated VESDA fire detection system linked to and monitored continually from ANS network operations centre.
- Enterprise-grade backup and recovery with Commvault.
- Award winning:  
ANS Group winner of the 'Microsoft Business Applications 2021/2022 Inner Circle awards'.  
ANS Group won 'Best DevOps Services Company' at the 'DevOps Excellence Awards 2020'.  
ANS Group named 'Microsoft Partner of the Year Finalist 2021'.
- 99.99% network uptime guarantee.
- 100% Carbon neutral with a PUE of less than 1.3 at full design load.

### Data Centre - Physical Security

- Secure site access and 24hr NSOI-accredited security patrol.
- Common ports on servers are disabled in order to restrict access.
- Staffed 24/7/365 by SIA accredited ANS staff.
- Internal and external CCTV.
- 2.8m secure fencing and razor wire perimeter fence.
- Access to the data centre is restricted to authorised personnel who hold Photo ID security passes.
- On arrival at the data centre, all visitors MUST sign in.
- Photo ID security passes are handed to a member of data centre staff who exchanges them for a key fob to access the relevant server room(s).
- Key fobs have different levels of access. The levels only allow access to pre-arranged areas within the data centre.
- Within each server room, racks of servers are secured within large cages.
- Each cage has a unique 4-digit code in order to gain access.
- Visits to the data centre for non-authorised personnel must be arranged with data centre staff at least 24 hours in advance.
- Clients taken on data centre tours must bring and show a valid form of photographic ID.
- Because of security protocol, access will be denied to anyone attempting to gain entry without a valid form of photographic ID.
- In addition, an authorised photo ID holder must always accompany visitors during their visit.
- Visitors must wear visitor passes at all times during the data centre visit.

## EVOLVE Infrastructure Overview

eduFOCUS' server infrastructure is housed across multiple sites at one of the UK's leading data centres. EVOLVE is a fully hosted service solution and clients do not require any additional hardware or software<sup>1</sup> in order to use or manage the service. It is scripted in Microsoft Active Server Pages, is hosted on the Microsoft Windows Server 2019 Datacentre platform and stores dynamic data within a clustered SQL database environment.



<sup>1</sup> other than a web browser and internet connection

## EVOLVE Infrastructure Details

- ✓ **DDoSX security feature** sits in front of firewalls to block any DDoS attacks, including the most common 'volumetric flood' attacks, before they even reach our network infrastructure.
- ✓ **Web Application Firewalls (WAFs)** proactively protects the application layer against attempted fraud or data theft and will block any suspicious activity. WAFs automatically inspect every web request for cross-site scripting, SQL injection, path traversal and hundreds of other types of attacks and safeguards against application layer attacks and mitigates inbound and outbound traffic for all web applications.
- ✓ EVOLVE infrastructure is hosted across **multiple sites** and benefits from **full redundant pair configuration** to maximise availability.
- ✓ The network is protected by **ASAv10 Cisco firewalls** configured as a redundant pair.
- ✓ Access to application servers is managed by **Dedicated Level 7 Load-Balancers** to maximise system availability and response times.
- ✓ All data is **encrypted in transit** using TLS 1.2.
- ✓ Data is stored in **clustered and encrypted MariaDB** environment (AES-256) to maximise availability and security.
- ✓ Incremental hourly and full daily CommVault **database backups**.
- ✓ Documents uploaded by users are stored in **high availability encrypted SAN** (AES-256).
- ✓ **SAN and server backups** performed by CommVault
- ✓ **Proactive Threat Monitoring** on each server detects host-based intrusion attempts, provides file integrity monitoring and vulnerability scans.
- ✓ **Threat Response** ensures that a dedicated team of security specialists are on hand to respond and mitigate threats.

