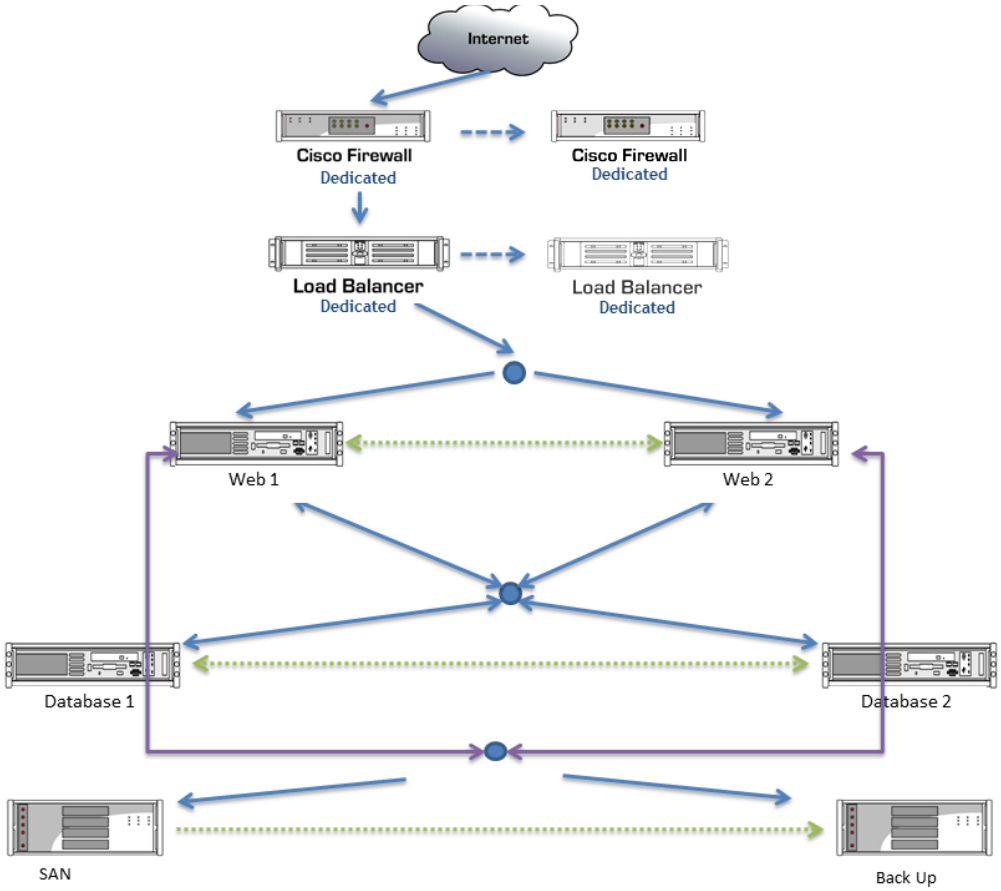
Security & Data Centre Information

EVOLVE is a fully hosted service solution, and as such clients do not require any additional hardware or software[1] in order to use or manage the service. It is scripted in Microsoft Active Server Pages, is hosted on the Microsoft Windows Server 2012 R2 platform and stores dynamic data within a clustered SQL database environment.

eduFOCUS' server infrastructure is housed in one of the UK's leading data centres which benefits from:

- ✓ UK Data Centre
- ✓ Daily server back-up
- ✓ Dedicated fail-over load-balanced servers
- ✓ Managed Cisco firewall protection
- ✓ Independently wired (powered) server racks
- ✓ Uninterrupted power supply
- ✓ No "single point failure" infrastructure
- ✓ Intelligent traffic routing and re-routing
- ✓ Sophisticated environmental monitoring to ensure optimum server performance
- ✓ CCTV monitoring, motion detection, 24/7/365 security guards and an advanced access control system
- ✓ Sophisticated VESDA fire detection system with CO2 and Halon gas fire suppression systems

Infrastructure Overview:



[1] other than a web browser and internet connection

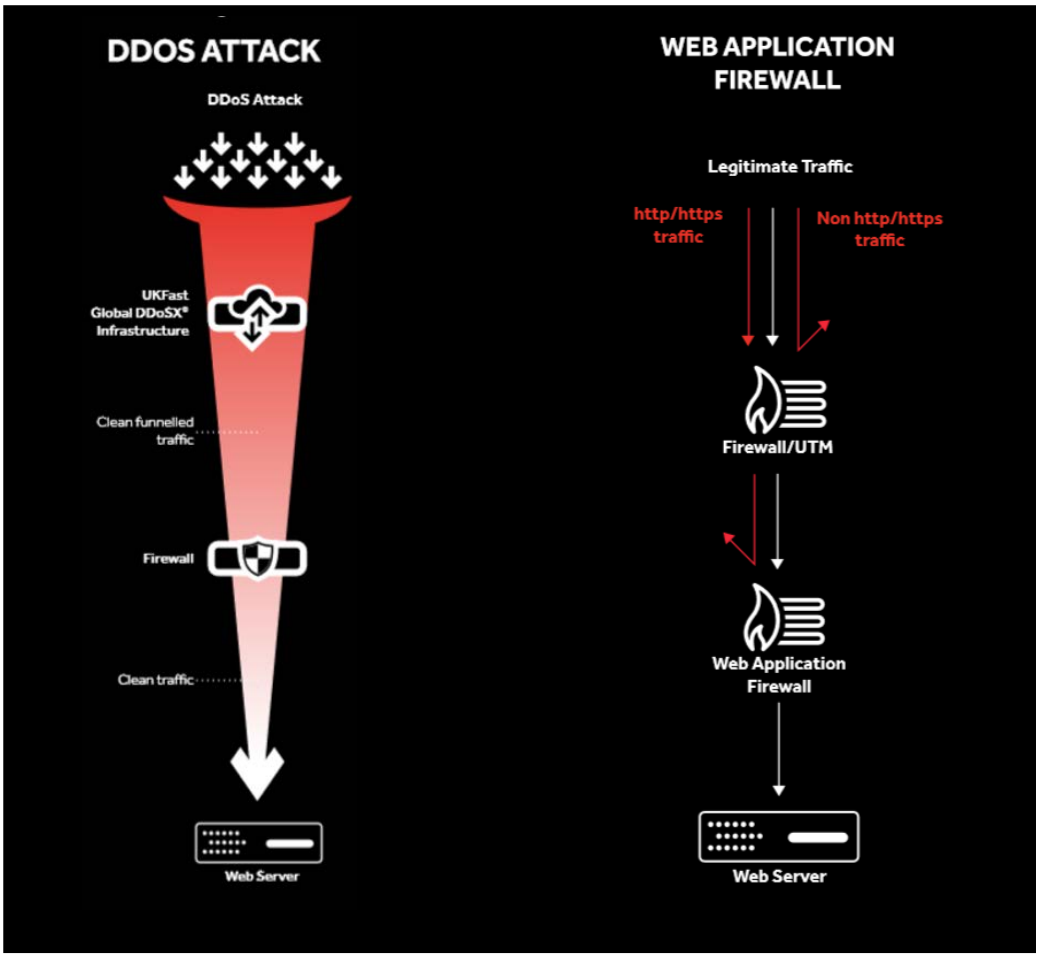
Additional Security Features*

1. **DDoS 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.

2. **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.

3. **Proactive Threat Monitoring** on each server detects host-based intrusion attempts, provides file integrity monitoring and vulnerability scans.

4. **Threat Response** ensures that a dedicated team of security specialists are on hand to respond and mitigate threats.



*Additional data protection features to be implemented March 2018

Who is responsible for what?

The Licensee is the **Data Controller.** A Data Controller is defined as the person/organisation who (either alone, or jointly, or in common with others) decides how and why any personal information is to be processed.

This therefore means that it is the Licensee that decides which information is collected, stored and processed. The Licensee decides:

- who can access the system and therefore which users are permitted to view what information (by setting their account type)
- to turn on the Visit Register and/or the Accompanying Staff modules
- to add custom questions to gather additional information
- to require/request files to be attached to visit forms
- etc.

As such, the Licensee is responsible for ensuring that appropriate data is stored and processed and that access to such data is restricted appropriately.

What about eduFOCUS Ltd?

eduFOCUS are registered with the Information Commissioner's Office and utilise a wide range of security measures in line with the recommendations provided by ICO (Information Commissioner's Office - http://www.ico.org.uk/

These security measures include advanced firewalls, enterprise-level virus protection on all servers, SSL encryption for all communication between our servers and users, regular data backup, username/password/PIN to access control, failed log-in attempt logging, automatic suspicious activity detection and logging etc.

Data Centre Key Features

- No single point of failure connection to internet including 2 x direct fibre links to the hub of the internet (Telehouse) with dark fibre redundancy
- Data stored within the UK
- Accreditations – ISO27001:2013, ISO9001:2008, ISO14001:2015, ISO 27018:2014, Cyber Essentials, G-Cloud 9, PAS2060, PCI DSS Compliance
- Certified Level 3 engineers manning the support desk
- 24/7/365 UK based support – round the clock HQ & on-site DC engineers
- 3 rings policy + 15 min rapid response + 1hr hardware replacement guarantee
- Secure site access and control 24/7
- Internal CCTV monitoring
- UPS and diesel generator system ensures continuous power supply to all equipment (seven-day independent run time in the event of mains failure)
- Sophisticated VESDA fire detection system with CO2 and Halon gas fire suppression systems
- Intelligent backup – secure, effortless full state system backups
- Proactive uptime monitoring – continuous monitoring with engineer & client alerts
- Award winning – ISPA Best Hosting Provider 4 consecutive years, ISPA Best Business Customer Service winner, ISPA Best CSR winner
- High grade bandwidth, optimised for web acceleration
- 100% network uptime guarantee
- UPS systems, standby diesel generators and high-density infrastructures in excess of 15kW per rack ensure power supply is resilient and uninterrupted
- Data centres have an average PUE of 1.3

Data Centre Physical Security

1. Access to the data centre is restricted to authorised personnel who hold Photo ID security passes.
2. On arrival at the data centre, all visitors MUST sign in.
3. 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).
4. Key fobs have different levels of access. The levels only allow access to pre-arranged areas within the data centre.
5. Within each server room, racks of servers are secured within large cages. Each cage has an unique 4-digit code in order to gain access.
6. Visits to the data centre for non-authorised personnel must be arranged with data centre staff at least 24 hours in advance.
7. Clients taken on data centre tours must bring and show a valid form of photographic ID.
8. Because of security protocol, access will be denied to anyone attempting to gain entry without a valid form of photographic ID.
9. In addition, an authorised photo ID holder must accompany visitors at all times during their visit.
10. Visitors must wear visitor passes at all times during the data centre visit.