Application security, load testing and threat protection

Introduction

This article will cover all application security, data encryption and threat protection elements of Xoralia. Any further information required can be requested from support@xoralia.com.

Application Security

The Xoralia application infrastructure has been built with security at the forefront. All Azure services that are utilised are protected by both Azure Application Gateway Web Application Firewalls and Azure Virtual Networks. This ensures that only valid, secure traffic is passed on to Xoralia web apps and APIs.

Within the application itself, we have utilised the following technologies / techniques:

- Azure SQL Auditing
- Microsoft Defender for Cloud
- Azure Transparent Data Encryption
- Azure Key Vault

All staff working across the Xoralia platform are running Windows 10 or later compliant devices and using company-managed antivirus, malware and firewall systems. Content Formula staff are background checked prior to joining the team.

Data encrypted at rest and in transit

All data stored on Xoralia servers is encrypted at rest using Azure Transparent Data Encryption. All data in transit is sent over HTTPS connections only. HTTPS is enforced on all web apps and APIs.

Under load testing and scalability

Xoralia has been tested under high loads (>5000 active users) and has passed all tests as expected.

The Xoralia application architecture allows us to proactively monitor and instantaneously scale the application on demand should it be needed. In the event of high load on 1 service, the application monitoring will automatically scale that service until normal operations are realised.