Protection For Your Business

The Wizuda CFS (Compliant File Share) solution provides users with secure email and file sharing capabilities and has been built with **security and privacy by design**.

Company Background

We have been specialising in secure data transfer since 2001, and pride ourselves in developing software solutions that allow organisations to have full control of their file transfer and data sharing operations, enabling them to operate efficiently, securely, and compliantly. All development and support operations are carried out from our two Irish offices located in Dublin (Wizuda Headquarters) and Limerick.

We are **ISO/IEC 27001 certified** which ensures we meet the international standard on managing information security and assuring our customers of our systematic and best practice approach to managing information security risks. Our ISO 27001 audits are carried out by our accredited partner Certification Europe. We undertake surveillance audits at six-monthly intervals to maintain the certification and the certification is renewed every 3 years, the most recent being in March 2021.

Our Customers

In 2019, we were awarded the Data Transfer contract for An Garda Síochána which includes Wizuda CFS and our automated data transfer solution. Other customers include The Mater Hospital, Crowe, efficienC, Advant Medical, HIQA, Vodafone, Kitman Labs, eShopWorld and Kerry County Council. Our most recent implementation is with Vodafone Oman where our solutions are responsible for transferring and streaming all critical data across their 5G network in real time.

Microsoft Azure

Wizuda is a Microsoft Certified Partner and our senior developers are Microsoft Certified Professionals. For our hosed customers, including HIQA, all data is hosted in Microsoft Azure's Europe North Data Centre which is located Dublin 22.

Security

Network Protection

Azure's secure network also has built-in mechanisms to protect against distributed denial-of-service (DDoS) attacks. Microsoft isolates networks, ensures the confidentiality of data, and actively works to combat against DDoS attacks.

Services Protection

- *Azure Defender for App Services* monitor the requests and responses sent to and from Wizuda's App Services and protects them from a multitude of ever-changing threats.
- *Azure Defender for Storage* detects unusual and potentially harmful attempts to access or exploit Wizuda's Storage Accounts. It utilises the advanced capabilities of security AI and Microsoft Threat Intelligence to provide contextual security alerts and recommendations including protection from suspicious access patterns & activities and attempted malicious content uploads.
- *Azure Defender for SQL* includes functionalities for discovering and mitigating potential database vulnerabilities and detecting anomalous activities that could indicate threats to Wizuda's databases. Advanced threat protection monitors for suspicious database activity and threats such as SQL injection, brute-force attacks, and privilege abuse.

Encryption

- **File Encryption at Rest**
  All files stored in Wizuda's hosted environment are encrypted using the 'Azure Storage Service Encryption for Data at Rest' service, which helps protect your data and meet organisational security and compliance commitments. With this feature, Azure Storage automatically encrypts your data before persisting it to Azure Storage and decrypts the data before retrieval. The handling of encryption, encryption at rest, decryption, and key management in Storage Service Encryption is transparent to users. All data written to Azure Storage is encrypted through AES-256 encryption, one of the strongest block ciphers available.

- **Database Encryption**
  All customer databases stored in Wizuda's CFS hosted environment are encrypted using the 'Azure Transparent Data Encryption for SQL Database and Data Warehouse' service, which helps protect against the threat of malicious activity. It performs real-time encryption and decryption of the database and transaction log files at rest without requiring changes to the application. Transparent data encryption encrypts the storage of an entire database by using a symmetric key called the database encryption key. This database encryption key is protected by the transparent data encryption protector.

- **Additional At Rest Encryption**
  On top of the previously stated Azure encryption; Wizuda uses AES-256 encryption technologies, along with individual database field tamper-proofing to safeguard against malicious activity.

- **Internet Communications**
  All web-based interactions with Wizuda CFS are made using the HTTPS communications protocol, encrypted with the latest TLS technology.

- **Email Communications**
  By default, Wizuda CFS will opportunistically try outbound TLS when attempting to deliver email notifications. This means that if the recipient's email server accepts inbound TLS connections, then the email will be delivered over a TLS end-to-end encrypted connection.

Penetration Testing

Our software development and release processes include regular penetration testing using leading accredited security scanning platforms trusted by companies such as Microsoft, Skype, Adobe, Capita and others, giving us peace of mind that our products are secure and data is not compromised.