

Network Architecture

The solution is provided as a hosted service run from the TeleWare secure data centre. This enables us to ensure the platform architecture is both resilient and secure and is provided with disaster recovery capabilities. Traffic is passed through the core router using secure network connections, for example, VLANs or VPNs, and is subject to security controls, such as, intrusion detection and rate limiting.

Support for Distributed Architecture and Multi-site Networks	The hosted approach removes the requirement for any call recording-specific hardware on-site. This enables us to deliver the call recording service to distributed architecture and multi-site networks with common capabilities, irrespective of location or the hardware installed on the site.
Flexible and Scalable	<p>Each customer has a designated secure tenancy within the hosted data centres. The hosted platform architecture has been designed to provide scalability. Providing this solution as a hosted application ensures that, as new offices or users come online, there are no issues of size limitation imposed by the system.</p> <p>Many multi-site organisations will have both IP and traditional TDM-based telephone architectures in place across their network. By using a centralised hosted solution, TeleWare is able to support both new and traditional architectures with identical capabilities and user interfaces.</p>
Disaster Recovery (DR)	Two fully independent and remotely sited hosted platforms support the call recording facility. In the event that a total loss of the primary data centre is experienced, then the calls will automatically be re-routed into the back-up data centre. All important information, including user IDs, passwords and call recordings are mirrored in real-time from the primary file server to the secondary file server. In the event of a disaster, the secondary system will be up-to-date so the latest recordings will be accessible.

Intelligent Communications

Call Recording within Wealth Management Institutions



The FSA Regulations

The Financial Services Authority (FSA) legislation introduced in March 2009 requires that some UK financial institutions record and store telephone conversations and electronic communications relating to client orders. For financial institutions looking to introduce new systems to meet this new legislation, there are considerations for security and a resilient authentication system. Encryption has to meet the FSA requirements, both on the platform and while transmitted, and the archiving system needs to be secure and easy to use.

This can be an opportunity to extend the system to cover the increasing number of mobile workers who need to make and receive calls on a mobile phone. It's also an opportunity to meet the requirements of the growing number of employees making lifestyle choices for flexible working by introducing a recording system with the flexibility to use any handset - home, desk phone, or mobile.

There are additional priorities relating to the system infrastructure such as the need to ensure the solution is based on a secure solution architecture offering high resilience and reliability levels.

The FSA regulations have been introduced in line with an EU review and are part of the FSA's efforts to combat market abuse. Particularly insider dealing and market manipulation. Firms involving client orders for the equity, bond and derivatives markets have to retain these files for six months. Electronic communication includes e-mail, instant messaging and fax.

The FSA rules take effect from March 2009 for companies who are undertaking the following activities:

- Receiving client orders
- Executing client orders
- Arranging for client orders to be executed
- Carrying out transactions on behalf of the firm or another person in the firm's group and which are part of the firm's trading activities or the trading activities of another person in the firm's group
- Executing orders that result from decisions by the firm to deal on behalf of its client
- Placing orders with other entities for execution that result from decisions by the firm to deal on behalf of a client.

For those firms affected, there is a transitional period of one year to give firms enough time to prepare and implement the necessary system changes.

Encryption and Authentication Delivering a Secure Service

Two Factor Authentication

Each user will be required to be authenticated through a CRYPTO Card session, as well as through the secure login details associated with the TeleWare Hosted Voice account. These technologies form the two factor authentication. Failed authentication by either will prohibit access.

Unique Encryption Keys

The TeleWare Runtime provides a unique capability and strength, which is the ability to use the Runtime to apply encryption during the recording process. This solution avoids the limitations of using an encrypted file server, where the same encryption key is used for all recording files on the server. Customers are provided with software to generate their own unique 2048 bit RSA signing and encryption keys. The system ensures that no-one else with access to the platform can decrypt a customer's recordings.

Call Recording Storage

As additional security against hacking, no unencrypted data is stored, even on a temporary basis. All recordings are written and processed in real-time to the file server.

Support for Mobile and Flexible Workers

The services can be delivered for inbound and outbound calls made from any designated phone irrespective of the network. This could be a mobile phone, a home phone or a desk phone. This enables the system to seamlessly support the growing number of workers who use their mobile phone in preference to their desk phone, and the increasing number of home workers without requiring any special equipment at the home premise.

Reporting

Standard Log and Call reports are available from within the call recording web application. Bespoke reports can also be created on request.

The intelligent Call Recording Service

intelligent Call Recording records and stores all inbound and outbound calls automatically. Calls can then be retrieved using the service's web interface.

Inbound Call Recording

Each user who wishes to record inbound calls is allocated an intelligent Number DDI (Direct Dial Inbound); any calls made to this DDI will be automatically recorded and the recording will be securely stored on the call recording hosted platform.

Outbound Call Recording

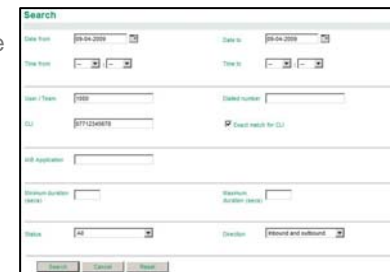
A single DDI allows users to enter an ID and a PIN then to securely make an outbound call.

Call Recording Access

Access to the stored call recordings is through a secure web interface housed on the platform. The web application utilises Secure HTTP as well as IP address filtering and two factor authentication.

Call Recording Searches

Searches for call recordings can be filtered based on key search criteria. Once the call recording is identified the user selects a telephone number from a restricted list to be used to listen to the playback of the selected recording.



Call Recording Retrieval

Recordings can be downloaded using the call recording web application. All downloads are in encrypted form and download is over a secure HTTP connection. Software is provided to decrypt the recordings after they are downloaded. The decryption uses the customer's own unique key; this ensures that the recordings are never transited in unencrypted form and can only be decrypted by the customer who owns them.