Security Overview

Rohan Berry - 11/07/2017

1. Document Version Control

Version	Date	Author	Comments
1.0	11/07/2017	Rohan Berry	Initial document
1.1	17/08/2017	Rohan Berry	Revisions: SQL 2016 upgrade, clarity

2. Contents

3. Overview

This document details key security related aspects of the Xeppo application and its infrastructure. Infrastructure is managed by our hosting partner Seek Tech and further details are available in an accompanying document.

The Xeppo portal is a publically facing, web-based application, hosted in a highly-available environment. Use of the Xeppo portal is encrypted via SSL as is communication between Xeppo source system Connectors and the central warehouse.

4. Application Security

Application

The Xeppo application is secured through username and password. Issuing of logins is managed by Xeppo users with the Practice Admin role, along with the ability to reset passwords. Users can also reset their password by issuing a temporary login to their registered email address, then entering a new password upon first login.

Two-factor authentication and Single Sign-on (SSO) options have been reviewed but are not currently available within Xeppo.

Data

Xeppo's back-end infrastructure is built on Microsoft SQL 2016 Enterprise where we have implemented "Row Level Security" (RLS) to secure data between tenants. Through this implementation we secure data access at a per-record level within the database rather than within the data access layer in the application. This ensures that no unauthorised access between practices is possible.

Data is encrypted at rest using Transparent Data Encryption (TDE) allowing the application to function as normal, but with all client data encrypted on the physical storage and in backups.

Note that Xeppo does not hold sensitive data such as credit card numbers or bank details. Client TFNs are hashed within Xeppo so cannot be read in plain text. Hashed TFN values are used within the matching process only and is not displayed in the interface.

Data Transfer

For on-premises connectors such as APS and MYOB, all communication of data to the Xeppo warehouse is encrypted via SSL. Connectors that retrieve data from cloud based sources reside within Xeppo's secure environment.

5. Backup

Database and Application backups are managed by our hosting partner through snapshots of virtual servers. Backups are performed nightly and synchronised to an additional data centre as well as an offsite backup. These are secured through physical security of the data storage locations as detailed in the attached Seek Tech security document and are retained for 31 days.

Data is encrypted at rest using Transparent Data Encryption (TDE) allowing the application to function as normal, but with all client data encrypted on the physical storage and in backups.

6. Disaster Recovery

In the event of total failure of the primary data centre, Xeppo will be restored within 8 – 16 hours, with a maximum loss of data of one business day. As the majority of data within Xeppo is obtained from source systems, a refresh of this data can occur post recovery, restricting actual data loss to only data entered directly in Xeppo within the last business day (e.g. Tags, System Configuration, Apps data such as Opportunities or Activities, etc.).

Further detail on recovery scenarios and procedures can be found in the Seek Tech security document.

7. Vulnerability Scans

Monthly vulnerability scans are performed on both the Application and the Infrastructure layers using the Qualys suite of security products.

Application scans test using both authenticated and non-authenticated access to determine any existing vulnerabilities at the application level.

Infrastructure scans are attested by the scan provider to a level of PCI compliance. Summary of this attested result can be provided upon request.

Internal testing is also executed prior to each deployment of the application using Unit Testing & Functional Testing within the development team and User Acceptance Testing (UAT) by Distributors, Directors and Key Stakeholders.

8. Compliance Audit

Upon request, a third party Infrastructure audit may be completed with the requestor paying for all reasonable costs. Further information relating to this is available within the Seek Tech security document.

Further discussion will be required between the Client and Xeppo in order to potentially provide application audits.

9. Data Access

Xeppo developers require access to client data in order to perform their regular duties including testing, maintenance and support. Access to the hosting infrastructure is restricted to the development team as well as the required persons as detailed in Seek Tech's security policy.

Data access at the application level is made available to support staff from the Xeppo Distributors where required. All actions through the Xeppo portal are audited.

Xeppo developers are required to provide a valid National Police Certificate before commencing employment.

10. Risk Management

In order to further reduce risk in relation to compromising security, the following measures are in place for Xeppo staff with client data access.

- All application development is performed in a remote, password secured development environment within the data centre, ensuring that RDP credentials must be used in order to gain access, even when a local machine may be compromised.
- Local machines are password secured.
- Encrypted local drives ensure that loss or theft of machines would not compromise any locally stored data, though through policy, no data is to be stored on local machines.
- Clean desk & computer locking policy to ensure no data can be physically accessed unless authorised.
- Secure premises with key-card authorisation required.

11. Supporting Documents

The following supporting documents provide additional, specific information. Please contact support@xeppo.com.au if you have any further queries.

- Xeppo Data Breach Policy
- Xeppo Privacy Policy
- Seek Tech Security Policy
- Seek Tech Privacy Policy
- Colocity - Data Centre Capabilities

12. Appendix A - Architectural Diagrams

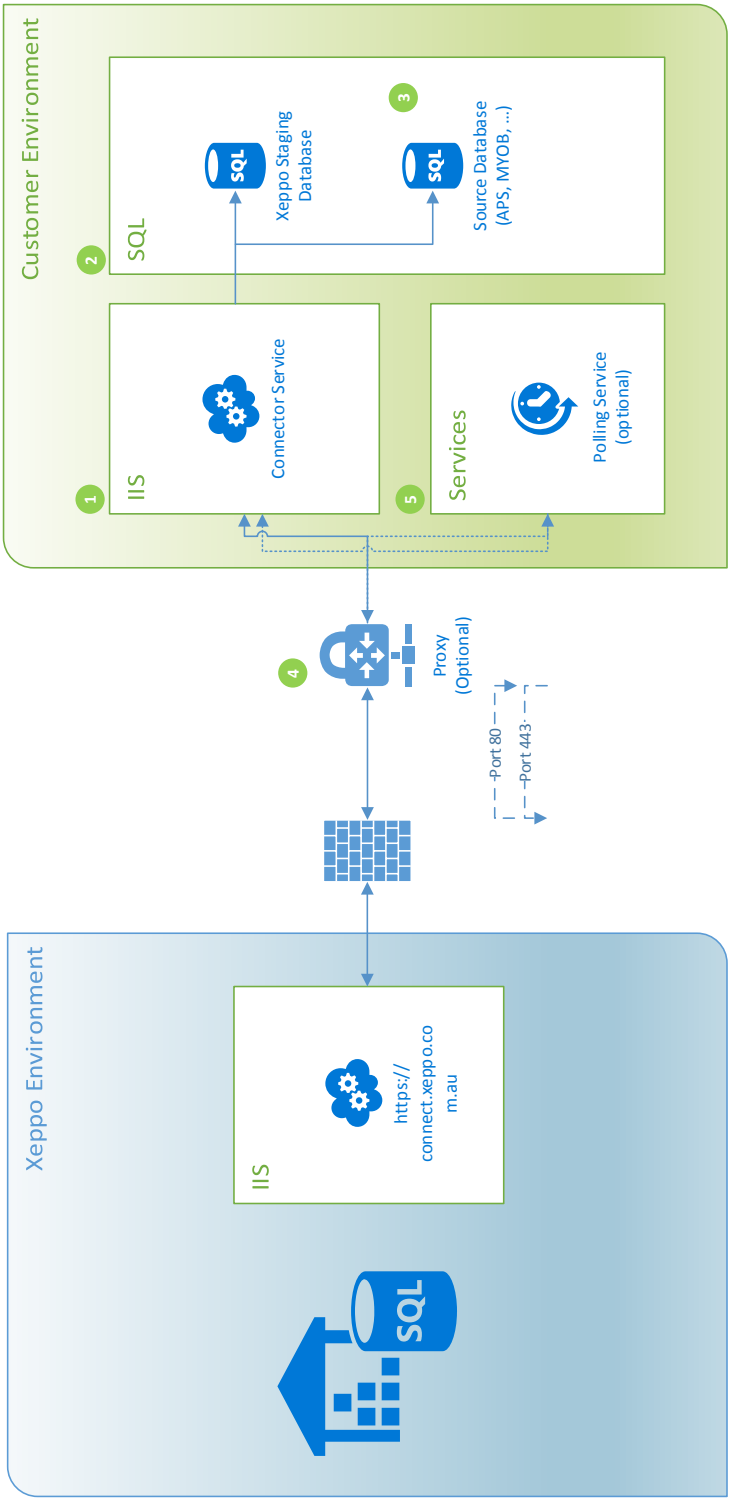

Figure 1- Client side Connector Architecture

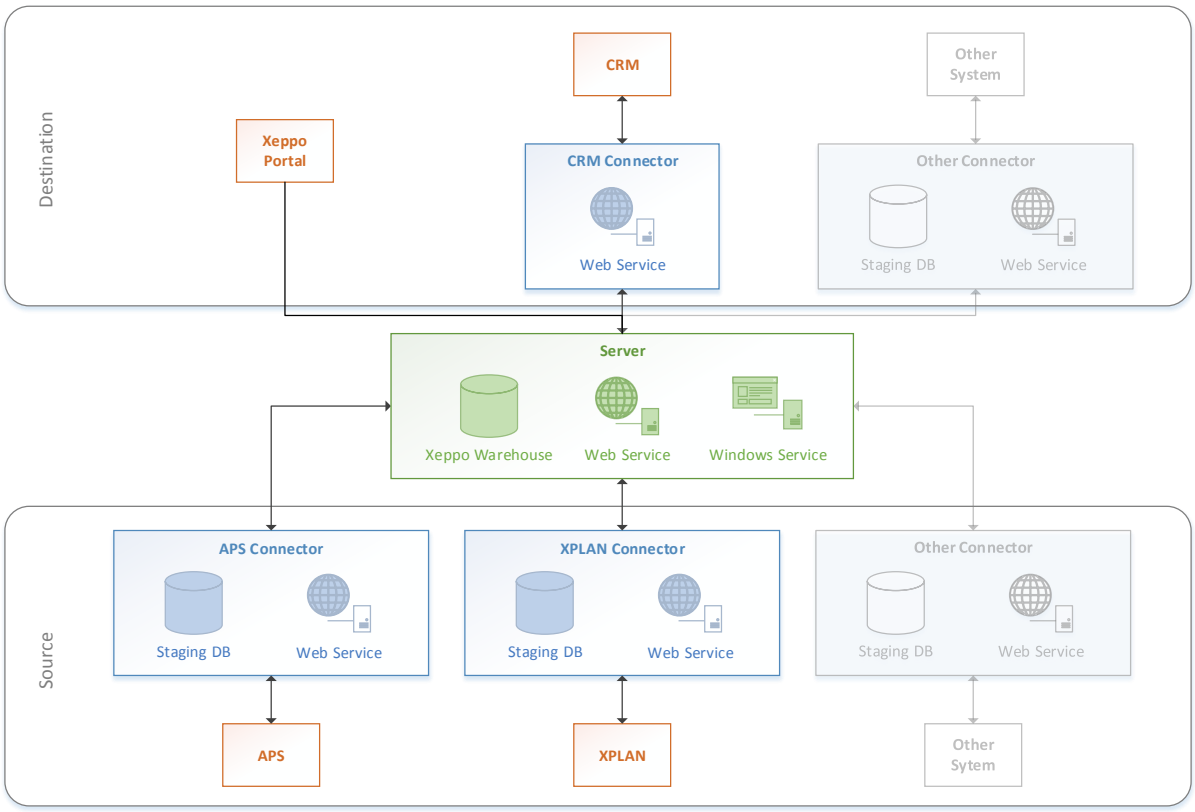

Figure 2- High-level Architecture

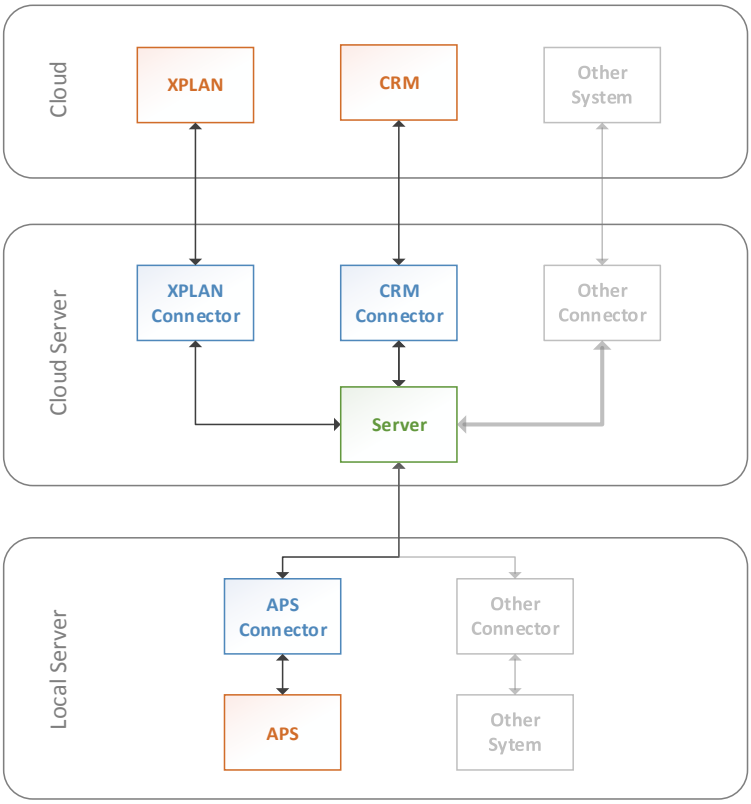

Figure 3 - High-level Architecture - Location