IXUP Secure Collaboration Platform

Technical Description

Version 1.1

29 May 2019

Contents

1. Introduction

The IXUP Secure Collaboration Platform (ISCP) is a cloud deployed enterprise software solution for inter and intra organisation data collaboration. The Platform provides a secure working environment, enabling matching of data across data silos to gain previously unattainable insights.

2. Overview

The IXUP environment supports two deployment models – Software as a Service (SaaS) or Platform as a Service (PaaS). The SaaS deployment model frees the user of any infrastructure setup and management responsibilities and is ideal for most situations. The PaaS deployment model provides all the same features as the SaaS model, but additionally includes extra flexibility in networking options as well as a dedicated environment for organisations that require it. This paper provides an overview of the platform seen in Figure 1. The specific model appropriate to your requirements may vary.

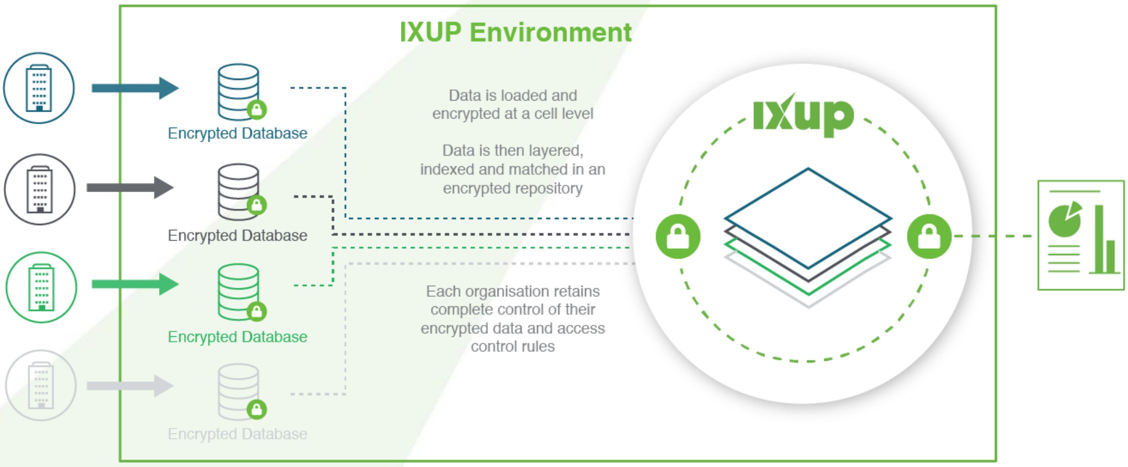

IXUP Environment
Encrypted Database
Encrypted Database
Encrypted Database
Encrypted Database
Data is loaded and encrypted at a cell level
Data is then layered, indexed and matched in an encrypted repository
Each organisation retains complete control of their encrypted data and access control rules
ixup

Figure 1

3. Key Features

The IXUP Secure Collaboration Platform (ISCP) includes a number of key features including:

- Data is always encrypted – at rest, in-flight and in-use.
- Industrial strength AES256 encryption as standard.
- Homomorphic Encryption support for arithmetic operations on encrypted data.
- Geographic matching with support for ABS SA1 codes.
- Support for common file formats as well as SQL Server and ODATA.
- Exact and Fuzzy match capability for encrypted datasets.
- Integration with popular visualisation and BI tools including Microsoft Power BI and Tableau.
- Intuitive data design workflow environment via the Collaboration Canvas.
- Support for data warehouses including Azure Data Warehouse, AWS Redshift, Snowflake and blob storage from Azure, AWS and Google.
- Comprehensive governance and auditing capability built in.

The IXUP Secure Collaboration Platform is comprised of several key elements, all deployed in the cloud for scale, elasticity, efficiency and cost effectiveness. These key elements are depicted in Figure 2 and are further explored in this paper.

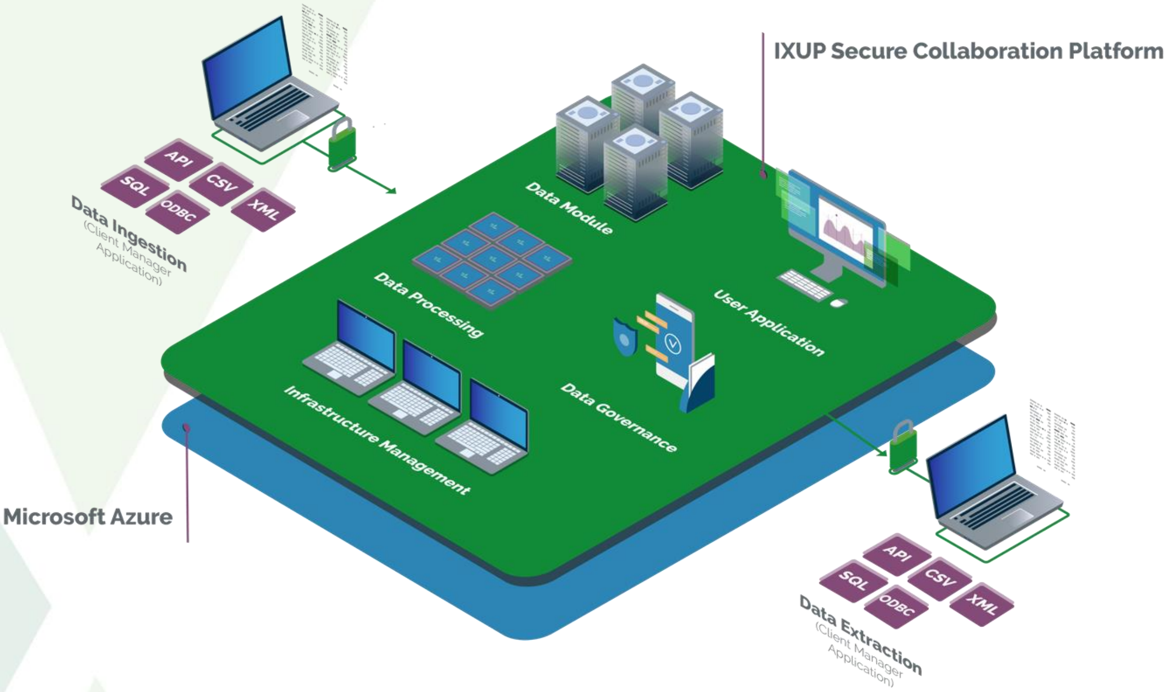


Figure 2

4. IXUP Secure Collaboration Platform

The IXUP Secure Collaboration Platform (ISCP) is the collection of applications, databases, infrastructure, orchestration, governance and process that together create a secure data collaboration environment.

4.1 User Application

The User Application is the main user interface to the platform and is delivered as a Web Application. All major administrative and user functions for the platform are supported directly within the User Application, with the notable exception of the Data Ingestion and Data Extraction processes, which are managed via the IXUP Client Manager Application.

4.2 Data Governance

Data Governance within the platform provides a secure audit capability, platform encryption key management, and data authorisation. The Data Governance module is exposed to the platform administrators and relevant/authorised users via the User Application.

4.3 Data Module

The Data Module is the core component of the platform responsible for managing data uploads, data storage, data movement, transactional relational databases and relational database warehouses.

Each collaborator and collaboration are assigned their own unique area with the Data Module to ensure no data is accessible to unauthorised party(ies) and the owner of each element of data is clear and always known.

The Data Module scales to meet the specific requirements of each collaborator and collaboration.

4.4 Data Processing

The Data Processing component of the platform is responsible for data matching, encryption management, logic execution and private set intersection.

The Data Processing module has been built using native cloud services to take full advantage of the computational power of the cloud.

4.5 Infrastructure Management

The ISCP includes an integrated infrastructure management component. The infrastructure management component provides easy to use and intuitive capability to;

- Specify roles and permissions, create, update and delete users, manage user permissions for underlying Azure services, including databases, database warehouses and Workspaces
- Managing;
  - Collaborations
  - Collaborators
  - Interface branding
- Tracking and reporting on user and project activities
- Create templatised Virtual Machine and database profiles for users, enabling integrated cost control and oversight
- Resource collections enabling the management of large numbers of resources (databases, database warehouses and Workspaces) and set auto shutdown / resume plans.
- Scale Azure resources as required without requiring knowledge of the Azure administrative consoles.

4.6 Data Ingestion

Data Ingestion is the process name used to load any instance of the ISCP with data. Data ingested into the platform is encrypted at source leveraging the IXUP Client Manager application. The IXUP Client Manager Application securely encrypts data at the cell/block level prior to transferring data into the IXUP platform for eventual usage in a defined collaboration. The Data Ingestion process supports several file formats as well as reading directly from SQL Server databases.

To further support the rapid ingestion and manipulation of data, the platform also supports integrated staging environments and rapidly deployable Workspaces where relevant/authorised users can leverage tools such as SQL Management Studio, R-Studio and scripting languages.

The platform provides an integrated error handling process to detect and handle data ingestion failures.

4.7 Data Extraction

Data Extraction is the process of removing data from the ISCP. Results of a given collaboration can be extracted from the platform; however, all extracted data will be encrypted in compliance with the stated IXUP principles. A data owner will always be able to leverage their secure encryption key to reveal their own data, and a data owner may request matching data from another collaborator via the system.

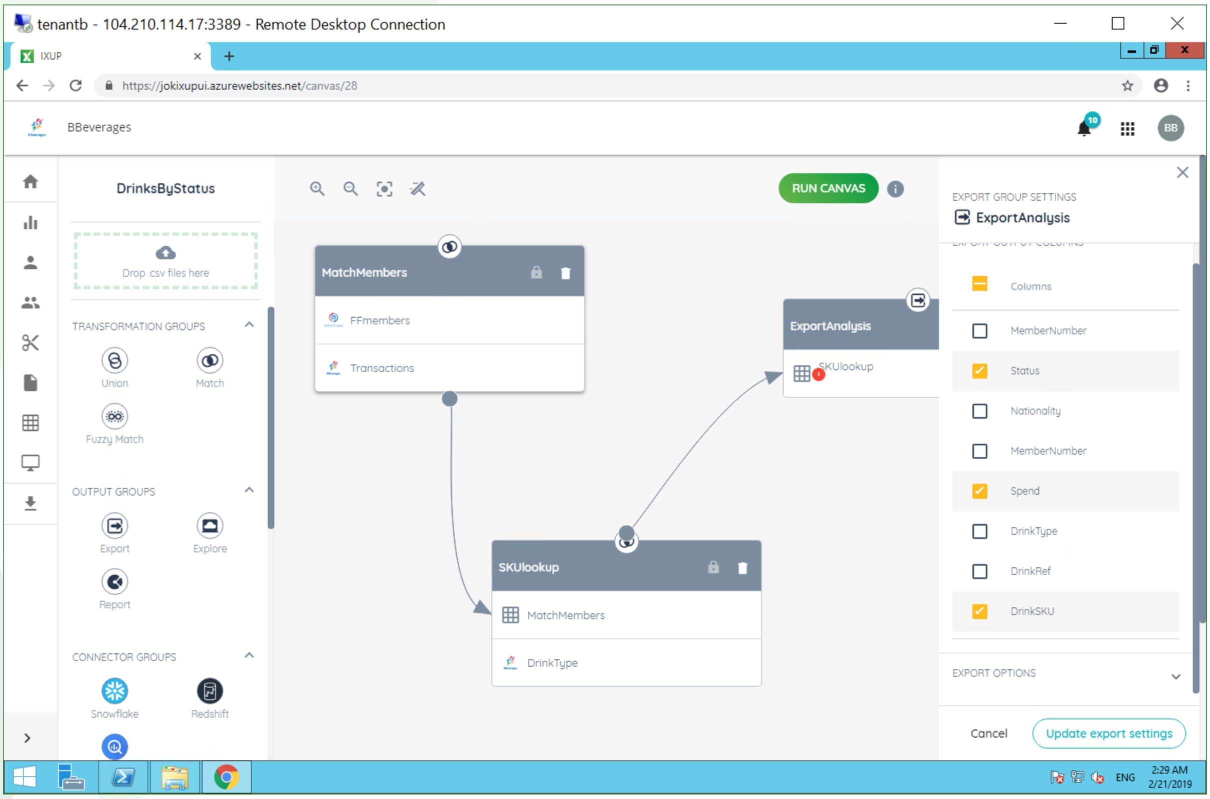
The ISCP provides data in standard formats further allowing customer choice for data visualisation, analytics or reprocessing. The Platform provides native percentage match insights for fully encrypted data sets in the event collaborations are Private. Where matching data is approved for collaboration, the Platform will orchestrate the encryption key process.

5. Technologies Employed

The IXUP Secure Collaboration Platform (ISCP) is a highly available and scalable platform leveraging the latest design patterns for next generation architectures like microservices and serverless compute. High security and full auditing of all operations is a central pillar of the platform.

The platform is deployed in and architected to leverage Microsoft Azure. Microsoft Azure is a public cloud environment that provides highly elastic and scalable compute, storage and networking services around the world. The IXUP Platform can be deployed in all Azure Regions for compliance with local jurisdictions and data sovereignty requirements. Multi-cloud environments are supported as are hybrid-clouds where VNET-VNET peering or VNET-VLAN connectivity is available. Irrespective of whether the data is routed over the public internet, site-to-site VPNs or dedicated lines like MPLS or metro-Ethernet, all data is encrypted before transit and routed via SSL connections from the client application to the platform.

The platform has been developed with modern technologies that facilitate an easy to use graphical design surface (called the Canvas) simplifying adoption. Users simply drag operations from the palette onto the Canvas, configure and wire them together (see Figure 3).



EXPORT GROUP SETTINGS

ExportAnalysis

- ☐ Columns
- ☐ MemberNumber
- ☑ Status
- ☐ Nationality
- ☐ MemberNumber
- ☑ Spend
- ☐ DrinkType
- ☐ DrinkRef
- ☑ DrinkSKU

EXPORT OPTIONS

Cancel | Update export settings

Figure 3

Integration with popular BI tools (like Tableau and PowerBI) is provided as is support for industry standard protocols like ODATA, as well as data warehouse solutions from major vendors like AWS, Microsoft and Google (see Figure 4).

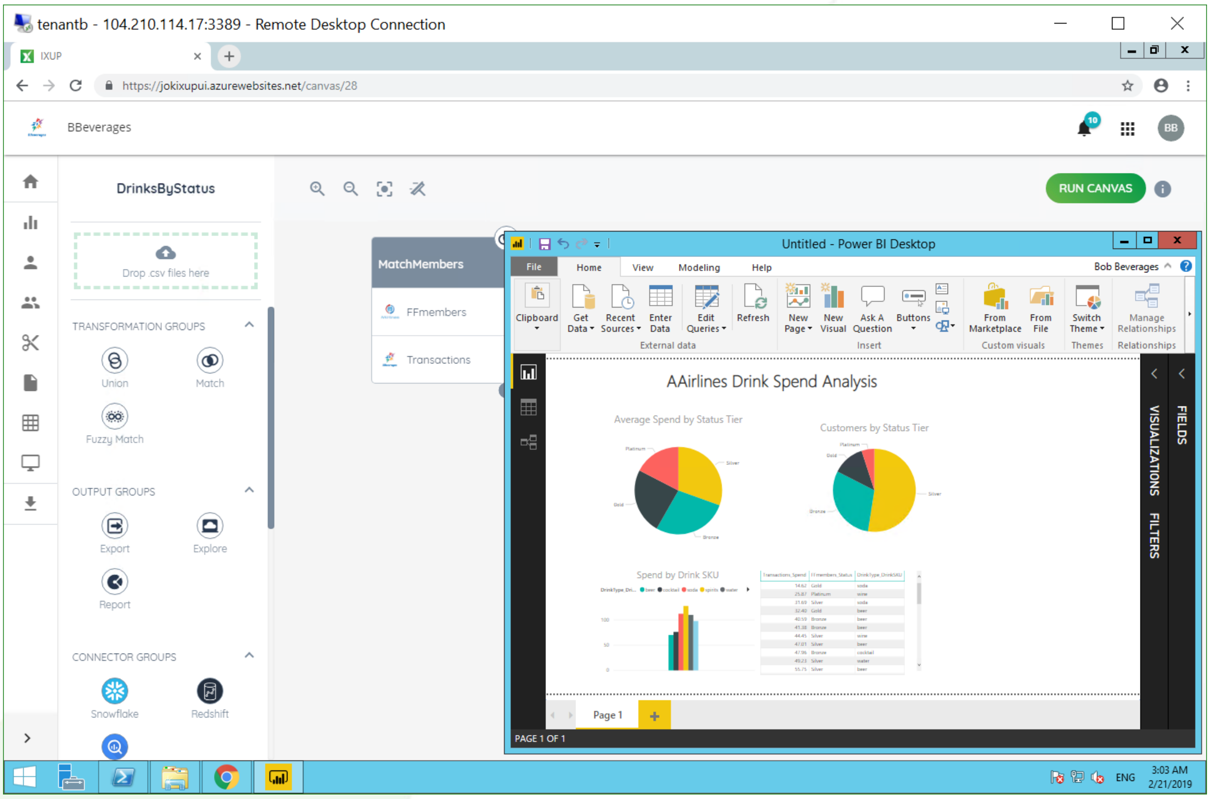


Figure 4

Summary

Like anything of value, data needs protecting. That’s why ensuring the security of your data analytics is paramount. The IXUP platform enables you to protect your organisation, to uphold the rights and privacy of the people whose data you use and to operate compliantly within legislative frameworks.

ABOUT IXUP

IXUP Limited (pronounced 'eyes up') is a listed technology company (ASX: IXU) that secures data analytics and delivers insights within a governance framework. The platform encrypts and connects data from multiple sources, solving the problems of data loss and misuse by enabling data owners to remain in complete control of their data. IXUP was listed in 2017.

FOR FURTHER DISCUSSION, PLEASE CONTACT:

Peter Leihn
Chief Executive Officer
peter.leihn@ixup.com

+61 2 8206 8888

IXUP | Secure your data analytics