



# Security

## WHITE PAPER

---

This white paper covers the security controls of Eightwire. This document is intended for a security audience who will have experience with information security, privacy, and technology.

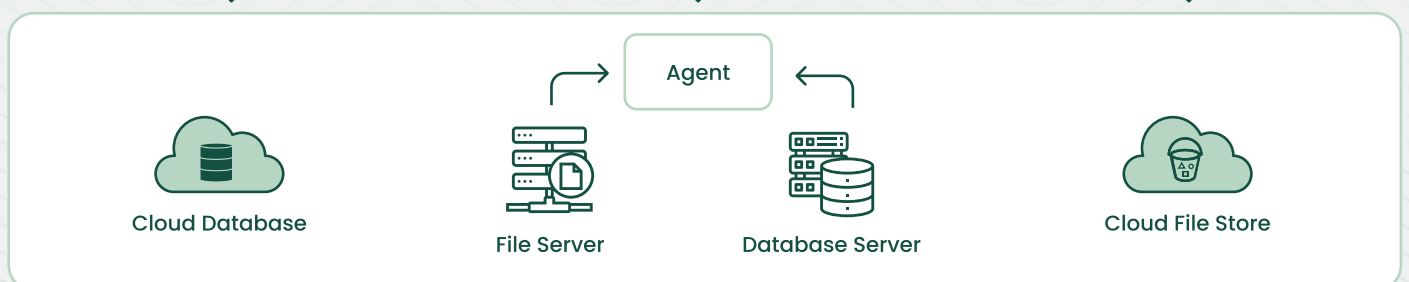
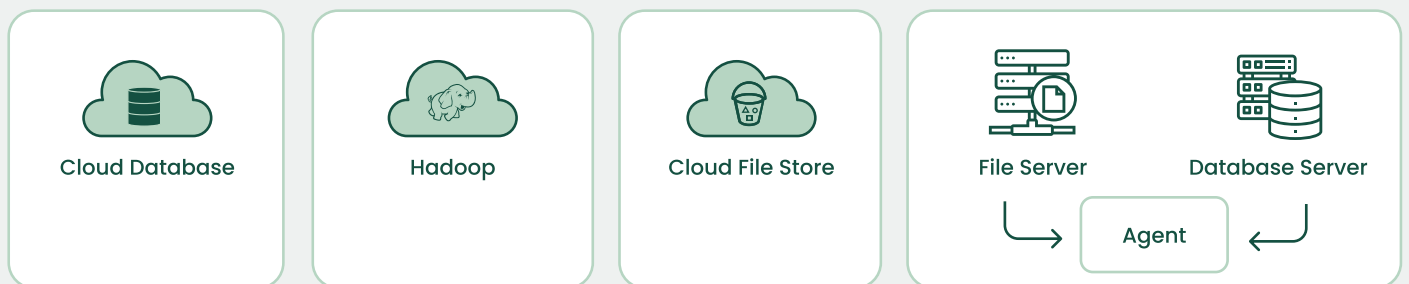
# Overview

Eightwire is a data sharing platform that automates the secure sharing of information between enterprises. This is accomplished through automating the many business and technology steps needed to share data across network boundaries.

Eightwire delivers secure data exchange for governments and multinational organisations. To deliver this function, Eightwire is built with overlapping levels of security for users, encryption, and transport. The diagram below shows how Eightwire's application links together on premises and cloud hosted data stores.



## PARTNERS



## ENTERPRISE

# Application Control

---

## Database

The Eightwire Agent makes use of ODBC and native communication protocols when communicating with databases. The agent relies on existing drivers on the server it is running on and does not provide any native functionality to support these protocols or drivers. The user provides a connection string through the Eightwire website, which is passed to the Agent to make a connection to the database. All encryption is the result of the connection between the database driver and the user's database. If your driver natively supports encryption then your connection is encrypted, if it needs to be enabled then you should do this in the connection string. No data has entered your network as part of this link between a database and an agent, provided the database is within your network.

## File System

For file-based data stores, the agent will either load a file into memory from a drive, or write a file to a drive from memory. The security of this data as it travels between the agent and the file system is dependent on the file systems' own encryption and security practices. Again, no data has travelled outside of your network to achieve this.

## Security Context on Microsoft Windows

When an agent is installed on a Microsoft Windows computer it will run as a service under the NT AUTHORITY/SYSTEM account by default. You can configure which account it runs under in the installation of the Agent. You should ensure that the account used has enough access to the data stores to do the job and nothing more. This account should also have the right to access the internet over port 443 (HTTPS). By managing these access permissions you can dictate the abilities for the agent.

# Application Control

---

## Agent to Eightwire Encryption

When an agent receives data from a data store on your network, whether it is data from a file or database, it compresses it, opens a TLS tunnel, and sends it over the internet to Eight Wire servers. When it receives data from the Eight Wire server the same process happens in reverse.

All communication over the internet happens using the industry standard HTTPS protocol and encryption over TCP port 443. Our encryption certificate uses SHA2/RSA (2048 bit) encryption.

All communication between agent and server is encrypted and obscure – aside from the data itself, it does not contain references to accounts or users and cannot be tracked back to individual customers using any information contained in the metadata included in the data transfer.

The agent periodically calls out to Eight Wire servers, never the other way around. There is usually no need to make any changes to existing firewalls and certainly no need to allow in-bound communications. Instructions sent to the agent initiating an upload or download are likewise encrypted and obscure. The nature of this one-way communication makes it impossible to directly attack an agent from outside the firewall by connecting to it as there is usually no way to make a direct connection.

The agent supports the use of a standard proxy server and can be configured to use one if required.

Customer data is encrypted in transit and at rest using Perfect Forward Secrecy with two separate chains of trust. Eightwire staff cannot decrypt or intercept data flowing through the platform.

## Eightwire to Cloud Providers

The Eightwire Agent makes use of ODBC and native communication protocols when communicating with databases. The agent relies on existing drivers on the server it is running on and does not provide any native functionality to support these protocols or drivers. The user provides a connection string through the Eightwire website, which is passed to the Agent to make a connection to the database. All encryption is the result of the connection between the database driver and the user's database. If your driver natively supports encryption then your connection is encrypted, if it needs to be enabled then you should do this in the connection string. No data has entered your network as part of this link between a database and an agent, provided the database is within your network.

# Application Control

---

## File System

For file-based data stores, the agent will either load a file into memory from a drive, or write a file to a drive from memory. The security of this data as it travels between the agent and the file system is dependent on the file systems' own encryption and security practices. Again, no data has travelled outside of your network to achieve this.

## Security Context on Microsoft Windows

When an agent is installed on a Microsoft Windows computer it will run as a service under the NT AUTHORITY/SYSTEM account by default. You can configure which account it runs under in the installation of the Agent. You should ensure that the account used has enough access to the data stores to do the job and nothing more. This account should also have the right to access the internet over port 443 (HTTPS). By managing these access permissions you can dictate the abilities for the agent.

## Eightwire to Cloud Providers

When Eightwire receives data from a cloud provider it is treated with the same security protocols as described above. When Eightwire sends data to a cloud provider we make use of that provider's own security mechanisms. For example, when we connect to SQL Azure, we use the security implicit in the SQL Native Client, likewise we use HTTPS when communicating with the Cloudbant API. For more information about the security available from each provider please visit their websites. If you are not sure, contact us at [support@eight-wire.com](mailto:support@eight-wire.com).

## Mutually Assured Authentication

Authentication between the agent and Eightwire servers relies on mutually verified certificates when creating an encrypted channel. Man-in-the-middle and SSL intercepts will immediately stop the transmission of data between the agent and Eightwire.

# Application Control

---

## Data Retention

When Eightwire servers receive information from an agent or other source, it is stored only as long as we are processing the data. When a process completes, all data is immediately deleted permanently. These servers are not backed up and the memory space is overwritten after data processing completes, so deleted data is truly gone.

# Corporate Controls

---

## External Security Assessments

Every year, Eightwire undertakes an external review of its security infrastructure and processes. These reviews examine any new features that are being released for security considerations and available controls. Any recommendations are carried out before the next quarterly review.

## Infrastructure-as-a-Service

Eightwire's policy is to use infrastructure-as-a-service where possible. Data is stored in an encrypted and secured database on cloud servers behind multiple layers of firewall and datacentre physical protection. No other information is stored with the data other than an obscure single-use GUID relating to metadata stored in a different part of the system. Eightwire ensures that all data is encrypted in memory before it is transmitted internally or stored in any internal database.

All sensitive information such as user passwords, file paths and connection strings are encrypted. This information is held on a separate network from the data processing servers.

# User Controls

---

## Role Based Access Control

All Eightwire users are managed through role based access control. Specific roles are restricted to carry out specific tasks and users cannot inherit multiple roles to prevent accidental privilege escalation. Roles are set for individual users within each project and cannot span projects or escalate to an account level.

## Two Factor Authentication

All customer logins are verified by two-factor authentication. In order to login, a customer must provide a valid username, password, and code that is texted to their mobile phone.

## Data Sovereignty

Many of Eightwire's customers have specific data sovereignty requirements. Eightwire's hybrid cloud allows customers to restrict the servers that physically handle data to certain countries or data centers. This can be implemented on individual data feeds if needed.

## Data Sharing Workflow

Eightwire allows completely separate entities to share information held in back end systems. In order to create a data share, the data provider has complete control over the data to be shared and destination. When a data provider shares their data, they enter a valid Eightwire customer email address to receive the data. The data provider is also issued with a single-use PIN that the receiver must enter to access the data share.

The user receiving data from an external party is provided with minimal information about the data providers systems. They are simply given a list of data objects (tables or files) to pull from.

# User Controls

---

## Data Leakage Prevention

Numerous user controls are in place to prevent the inadvertent sharing or leaking of data between Eightwire accounts. These include data entity tagging so PII tags will trigger strict contractual controls, 2-factor validation required before a cross-account share is completed, and specific.

## User Behaviour Auditing

Every action that a user makes to data feeds is recorded by Eightwire and held forever. Logs that are less than 3 months old can be queried through the website, older logs can be requested from Eightwire when needed. Audit logs include before and after state changes so all actions can be accessed quickly as required.

## Agent Authentication

All agents must be authenticated by an administrator using a randomly-generated one-time key generated by the Eightwire platform. The one-time key must be applied to the Agent running on the user's infrastructure to ensure that the end-to-end data flow is fully authenticated.

