CONNEXONE
CASE STUDY
CLOUD INTEGRATION

ANY PROTOCOL DATA WHERE

CONNEXITE

INDEX

INTRODUCTION **3**

SOLUTION OVERVIEW **4**

SOLUTION COMPONENTS **5**

APPLICATION **5**

SECURE DATA TRANSFER TO PUBLIC CLOUD AND REMOTE REPOSITORIES

In high-security environments, unidirectional data flow is critical to prevent unauthorized access or tampering. Connexone **hardware-based data diode** enables **secure one-way data transmission**, while allowing the receiving side to **connect to cloud services or remote networks over VPN**.

This architecture combines **air-gapped data security** with **remote accessibility and integration**, ensuring operational efficiency without compromising security.

Organizations managing sensitive environments such as defense networks, industrial control systems (ICS), SCADA networks, and critical infrastructure, face conflicting demands of, **isolating critical networks** from the internet or corporate IT for security also p**roviding operational visibility** and transferring critical logs, metrics, and telemetry to external monitoring or cloud analytics platforms.

This presents a dilemma of directing connections, open up vectors for attacks and leading full isolation to blind spots and manual inefficiencies.

CHALLENGE

Isolating critical infrastructure while providing operational visibility to keep business flows running while maintaining high security standards.

SOLUTION

Connexone Data Diode allows **unidirectional data flow** from a transmitter (TX) side—connected to the protected network—towards a receiver (RX) side to further transfer data to a cloud server such as AWS and Azure or any SOC using encrypted tunnels

OUTCOME

End to end protected data flow from data generating end point to the remote repository, with minimal network configuration and no security breaches.

SOLUTION OVERVIEW

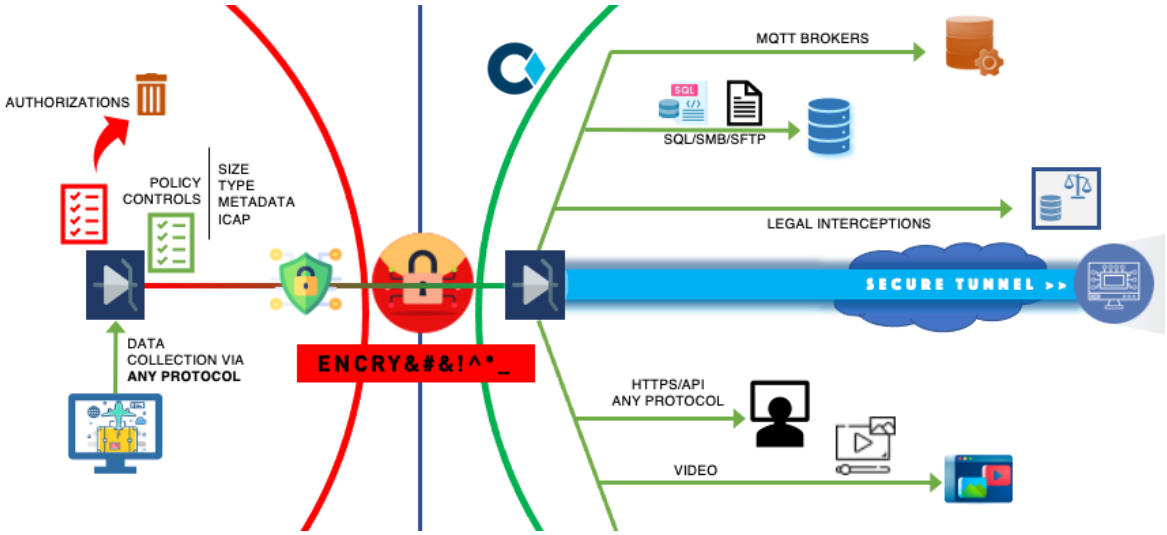
Connexite solution introduces a secure and efficient method for transferring data from isolated or critical networks to external systems using a hardware-based data diode. ConnexONE enforces strict one-way communication, allowing information to flow only from the transmitter (TX) side—connected to sensitive networks such as SCADA, ICS, or OT—toward the receiver (RX) side. This physical separation ensures that no external commands or data can ever be injected back into the protected environment, eliminating common attack vectors like remote code execution or malware propagation.

On the receiving side, the RX unit is designed to act as a secure intermediary, equipped with the ability to process incoming data and establish outbound VPN connections. It supports protocols such as IPSEC, WireGuard or OpenVPN to securely tunnel the received data to cloud-based platforms or centralized monitoring systems. This allows organizations to maintain real-time situational awareness, log aggregation, or threat detection without compromising the security of the source network.

The combined architecture provides the best of both worlds: air-gapped protection for the source environment and modern connectivity on the destination side. Whether the end goal is sensitive information sharing, secure telemetry upload, SIEM integration, or regulatory compliance reporting, this setup allows data to be safely exported without ever opening a return channel—bridging the gap between operational isolation and cloud-native intelligence.

Solution Components

All ConnexOne hardware pairs are capable to transfer data from secure zone to any cloud or remote environment



Application

ConnexONE enables secure transfer of any data over any protocol to be carried out to a controlled less secure zone. This is the usual operation of a ConnexONE data diode and works on any environment. In cases where the data from critical infrastructure should be delivered outside the organization network, to any sort of remote destination, ConnexONE receiving unit, VPN tunnelling feature steps in and create a secure channel from receiving device to any VPN concentrator running in public clouds such as Amazon AWS, Microsoft Azure, Google or Digital Ocean.

Modern tunneling protocols such as IPSEC, OpenVPN and Wireguard is supported by ConnexONE, allowing easy and quick integration.

Here are the steps to deliver critical data to remote targets:

- **Data Collection**: ConnexONE TX gathers files, logs, OT data, CSV/JSON outputs, or packet captures.
- **Unidirectional Transfer**: Data is serialized and sent over a unidirectional channel to RX.
- **RX Decryption & Queueing**: ConnexONE RX buffers or optionally sanitizes incoming data.
- **VPN Tunnel Establishment**: ConnexONE RX establishes a VPN tunnel (e.g., WireGuard, OpenVPN) to a trusted external receiver.
- **Data Upload**: Data is uploaded to cloud storage, analytics platforms, or incident detection systems.

DISCOVER CONNEXITE SOLUTIONS

connexite.co.uk

CONNEXITE LTD
284 CHASE ROAD A BLOCK 2ND FLOOR
LONDON UNITED KINGDOM N14 6HF

contact@connexite.co.uk