

# BUSBYTE

## UNHACKABLE DATA TRANSFER



### PROBLEM

Do you face challenges in retrieving data from on-site or remote, hard-to-reach locations without compromising asset security or exposing systems to potential cyber threats?

Is ensuring end-to-end data security a critical requirement for your operations?

Our solution provides a secure, reliable method for retrieving data from remote systems without increasing the attack surface.



### SOLUTION

We utilise a combination of air-gapped architecture and a strict read-only methodology to securely retrieve data from a wide range of industrial systems.

BusByte technology operates across two distinct security layers:

First layer applies to data collection and enforces a strict read-only policy, including support for serial communication protocols such as Modbus.

Second layer enhances data transfer security when TCP/IP-based collection is used, ensuring the system remains fully isolated and virtually impervious to external attacks.



## COMMUNICATION EXAMPLE

BMS Systems



Industrial Controllers

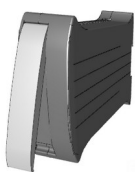


Meters, Sensors



BusByte data collection

Data Collector



BusByte data transfer

Data Sender



Cloud Servers



Client Access



## DETAILS

We collect data from existing systems securely and push pre IoT systems providing IoT connectivity.

Data transfer can be carried out over wireless or wired connections, depending on the deployment requirements.

The data collector and data sender unit is locked down OS on encrypted storage so your data are protected end to end.

All communication between data collectors and our servers is TLS/SSL encrypted.



## CONTACT

mail@dbr.co.uk  
+44 1268 442888

