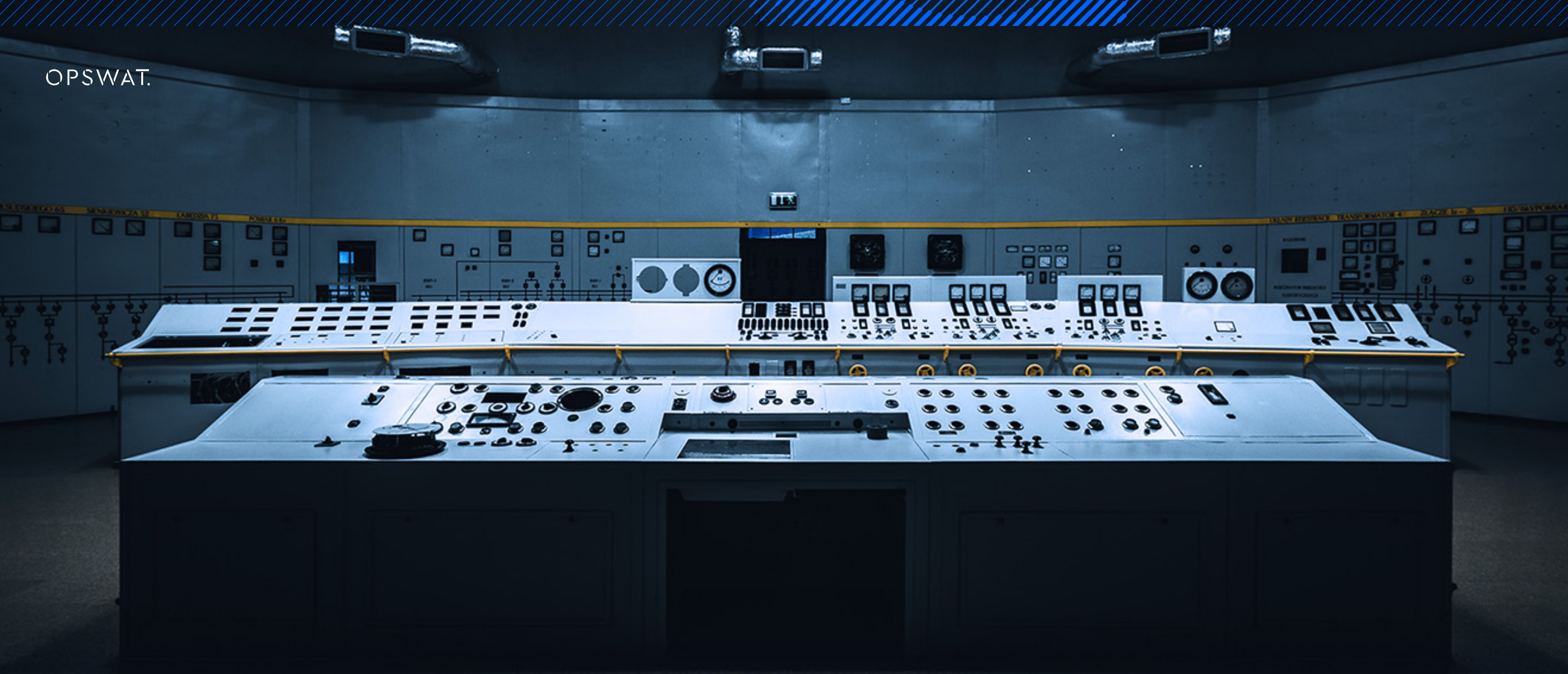
OPSWAT.

METADEFENDER

NetWall™ Series

Next-Level Data Diode and
Security Gateway Solutions
Powering Risk-Free
IT-OT Communications

Protecting the World's Critical Infrastructure



CHALLENGE

Protecting Your Critical Network in the Converging World of IT and OT

The once-clear distinction between IT (information technology) and OT (operational technology) systems, processes, and people is becoming blurred. Conventional air gaps between OT and IT network segments have eroded due to increased corporate demand for connectivity and data analytics from industrial environments.

This increased demand for connectivity exposes industrial assets to targeted cyberattacks because firewalls and next-generation firewalls are inherently bi-directional. They rely on software-based policies and are prone to misconfiguration that threat actors can exploit.

MetaDefender Optical Diode™ (Fend) and Security Gateways provide access to real-time OT data and enable secure data transfer to OT environments without compromising the security and integrity of your critical production systems.

OPSWAT.

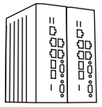
METADEFENDER

NetWall Series

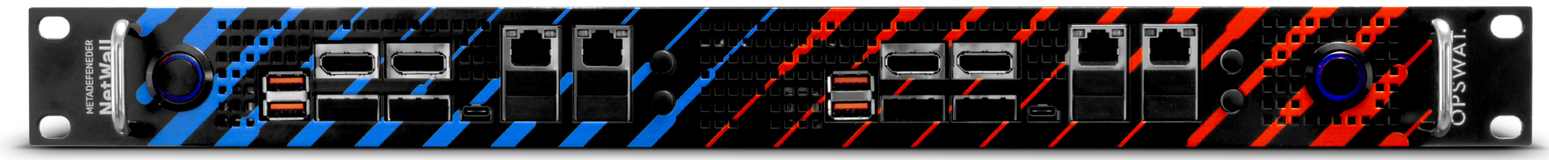
Available Form Factors

1U

DIN Rail



DIN Rail (Fend)



Features

Real-time transfers of OT data to business users without disrupting their work procedures

No risk of cyberthreats entering your protected OT network

File transfers and database/server replications without proprietary vendor hardware and software

High-assurance payload delivery that allows concurrent transfers of multiple data types†

† Available on USG model

No complicated firewall audit/configuration projects and risky backdoor channels to the OT network

Full support for industrial protocols including OPC DA, A&E, UA, IEC 104, and AVEVA PI, plus Modbus/TCP, file transfers, and TCP/UDP sockets

Fulfillment of compliance requirements including NERC CIP; NIST CSF/800-82/800-53/ICS; IEC 62443; NRC 5.71; CFATS; ISO 27001/27032/27103; ANSSI; IIC SF; and more. Protects against Industrial attack techniques outlined by MITRE ATT&CK for ICS

We offer a 100Mbps base platform that can be field upgraded to 1Gbps. Additionally, we offer an option for 10Gbps delivered on enterprise servers. The 10Mbps DIN Rail model is field upgradeable to 50Mbps.

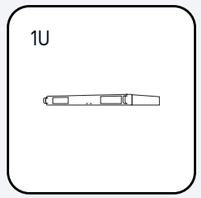
OPSWAT.

METADEFENDER™

Unidirectional Security Gateway

MetaDefender Unidirectional Security Gateway (USG) provides access to real-time OT data and enables secure IT-OT data transfers—with the full benefit of speed, low latency, and functionality—and with complete reliability and no data loss. Since no return-path networking is possible, MetaDefender USG assures real-time operations data can be sent to the corporate network users without the risk of introducing security threats to protected OT networks.

Available Form Factor



METADEFENDER USG provides one way data transfer over a serial connection

METADEFENDER BSG provides one way data transfer with data response

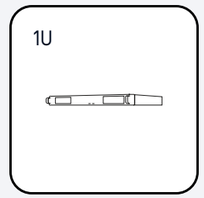
METADEFENDER™

Bilateral Security Gateway

In addition to all the capabilities of MetaDefender USG, MetaDefender Bilateral Security Gateway (BSG) supports applications such as historians and SQL database servers that require a data response in order to operate. MetaDefender BSG performs real-time replication of the data (with no data loss) and uses a bilateral mechanism to handle data responses without compromising the security and integrity of the OT network.

When a connection is initiated from the trusted network to a destination in the untrusted network, MetaDefender BSG performs a full protocol break,allowing select applications from the destination to securely return a data response to the source application over a non-routable connection. MetaDefender BSG will not allow a connection to be initiated from the untrusted network, ensuring that the communication channel cannot be exploited.

Available Form Factor



OPSWAT.

METADEFENDER™

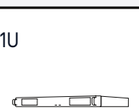
Optical Diode

MetaDefender Optical Diode (Fend) provides a hardware-enforced unidirectional transfer of real-time OT data and enables secure IT-OT data transfers over a reliable, high speed, low latency optical link. Since no return-path networking is possible, MetaDefender Optical Diode (Fend) transfers real-time operations data while conforming to industry regulatory requirements for deterministic one-way transfer device. MetaDefender Optical Diode (Fend) performs payload integrity checking and supports redundant optical links, achieving unsurpassed reliability and data delivery assurance.

MetaDefender Optical Diode (Fend) is available on enterprise servers or ruggedized DIN rail servers (multi and single box form factors) that can be deployed in harsh industrial environments.

Available Form Factors

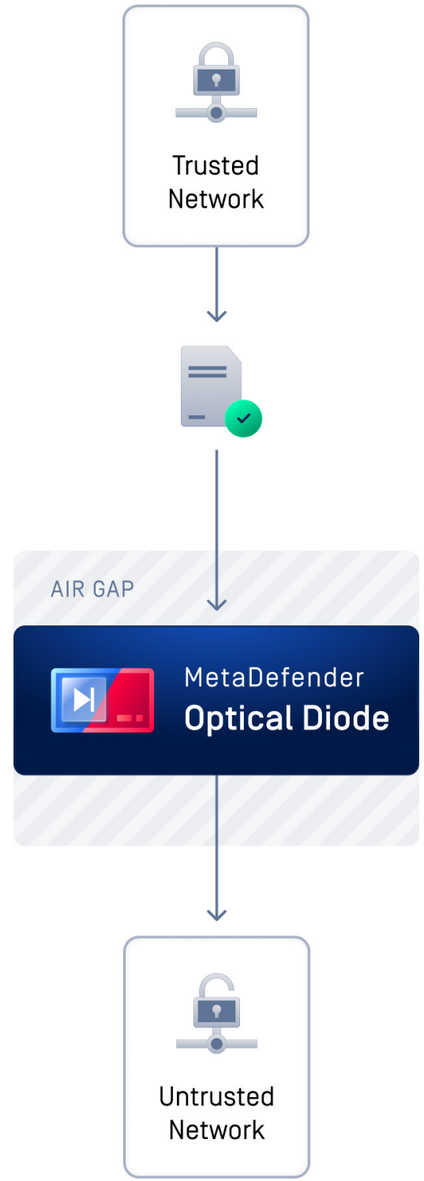
1U



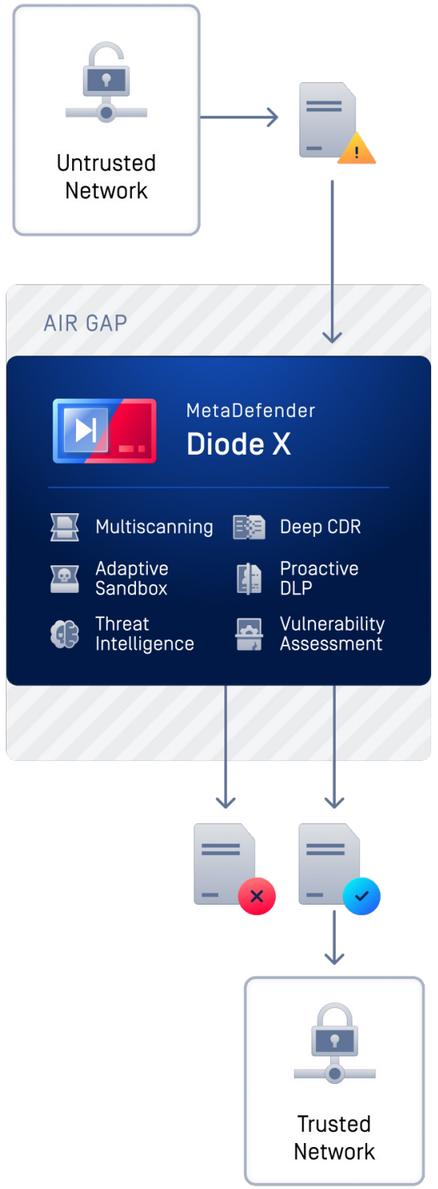
DIN Rail

DIN Rail (Fend)

*Not Available on Fend diodes



METADEFENDER OPTICAL DIODE provides one way data transfer using an optical link



METADEFENDER DIODE X provides one way data transfer with additional file sanitization by MetaDefender Core

METADEFENDER™

Diode X

Previously MetaDefender Transfer Guard

with File Sanitization

MetaDefender Diode X integrates OPSWAT's award-winning MetaDefender Core™ file sanitization engine. MetaDefender Core thoroughly scans and sanitizes files before they are securely transferred by MetaDefender Diode X across a network security boundary to the desired destination. It can be delivered on the MetaDefender Optical Diode platforms.

Available Form Factor

1U

OPSWAT.

Focus on Maximum Security and Reliability

MetaDefender NetWall vs. Firewalls

Traditional firewalls, router rules, and VLANs can restrict or segment traffic, but they still rely on bidirectional, routable connections—which leaves the OT network exposed to cyber risks.

Optical diodes enforce true unidirectional security, physically preventing external connections into the protected OT domain. This makes them fundamentally more secure than firewalls while still enabling controlled data flows outward.

Gateways: Like Diodes, with Guaranteed Delivery

Unlike traditional data diodes that enforce one-way communication without confirming receipt, Security Gateways combine unidirectional data transfer with guaranteed payload delivery, preventing data loss and retransmission. This ensures data integrity, prevents data loss, and removes the need for retransmission, providing organizations with the security of a data diode and the assurance that every critical packet reaches its destination intact.

Feature	NetWall	Networking Solution
Routing configuration	✓	✓
Protocol break, completely removed from TCP/IP connection	✓	
Meets functional requirements of data diodes (NetWall USG)	✓	
Guaranteed delivery with non-repudiable data movement	✓	
No complex rule-building	✓	
Guaranteed prevention of malware propagation	✓	
No ARP, BGP, TCP/IP handshake	✓	

MetaDefender Optical Diode vs. Other Data Diodes

Unlike other data diodes, MetaDefender Optical Diode offers greater delivery assurance with greater scalability as well as simpler configuration and deployment.

Feature	Optical Diode	Other Data Diode
One-Way Data Flow	✓	✓
Complete protocol break	✓	✓
Redundant optical connections for high data delivery assurance	✓	
Widest range of throughput from 5Mbps to 10Gbps	✓	
Hardware dongle for admin access	✓	
Fast and easy to deploy	✓	
Cost effective with competitive subscription or perpetual license options	✓	

OPSWAT.

USE CASE

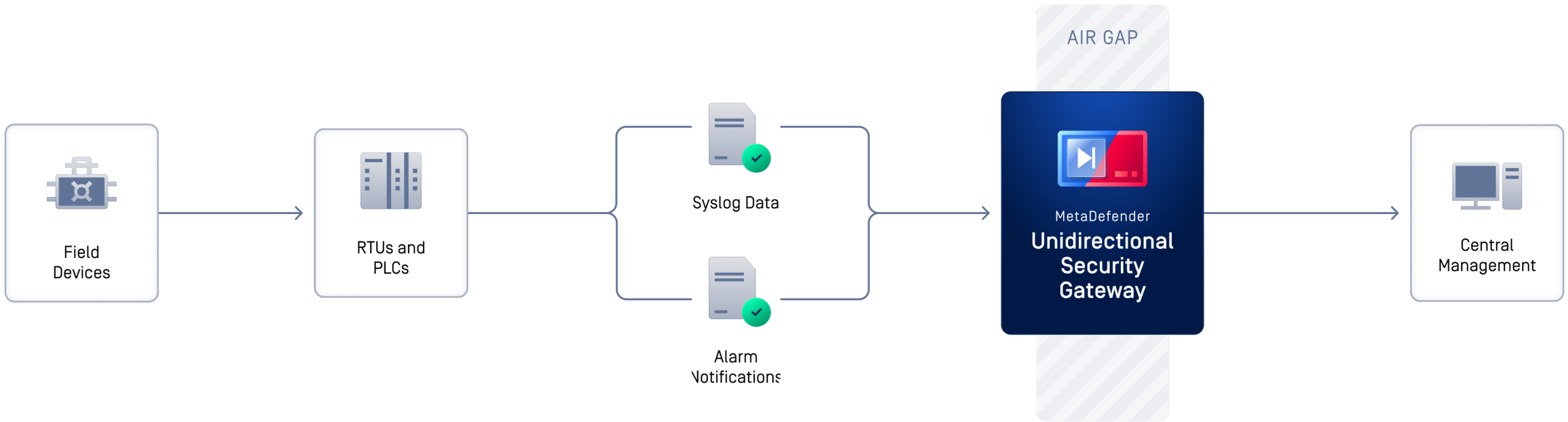
Efficiently Monitor Electrical Substation while Complying with NERC CIP Requirements

Challenge

Comply with NERC CIP requirements to protect data substations from outside threats while creating an operationally efficient method to monitor substations.

Solution

MetaDefender Unidirectional Security Gateway (USG) replicates log files and supports transferring syslog to one or more SIEM systems. MetaDefender USG's assured data delivery architecture delivers data in real time, supporting highly efficient system monitoring and alert management.



OPSWAT.

USE CASE

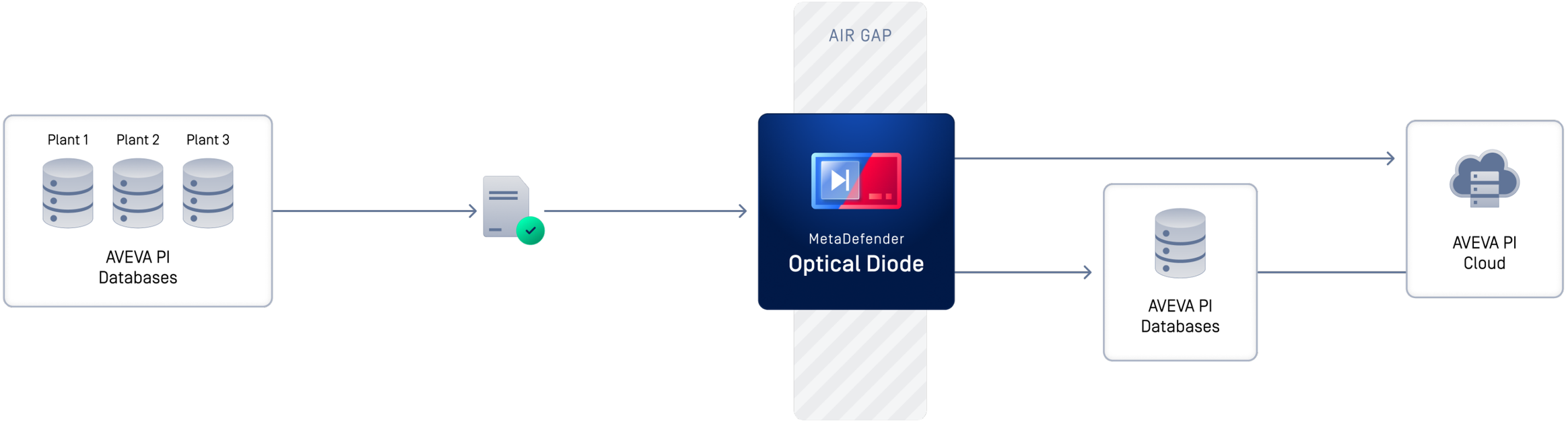
AVEVA PI Data Replication Between Three Power Plants and Enterprise Historian

Challenge

Historical data is captured for three power generation turbine plants in AVEVA Pi historians. When a security perimeter is established around plant assets, there needs to be a way of securely sharing OT historian data with the IT business network.

Solution

MetaDefender Optical Diode reliably replicates AVEVA Pi historian data using the MetaDefender AVEVA Pi Connector. Data is transferred over a non-routable protocol break enhancing security and confidentiality of the source network.



OPSWAT.

USE CASE

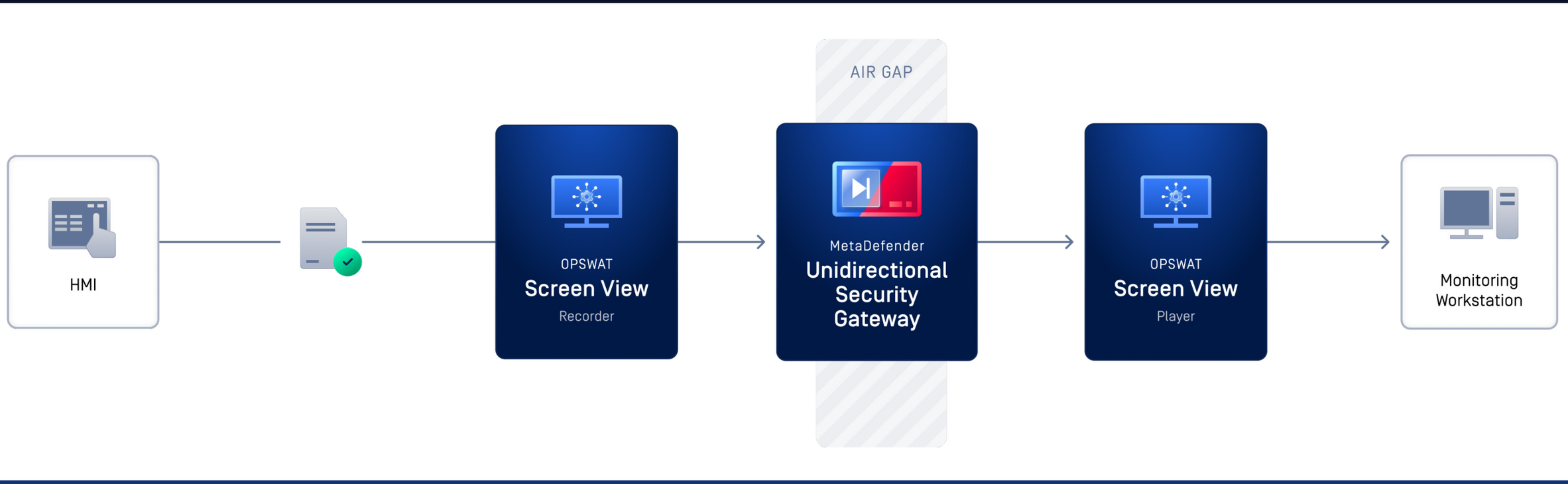
Energy Provider Requires Secure Replication of HMI Screens

Challenge

Replicate OT HMI screens to Central Monitoring facility without compromising OT infrastructure security.

Solution

MetaDefender Unidirectional Security Gateway captures real-time HMI screen images, within the plant, and replicates them to a remote monitoring location on the IT network. MetaDefender Screen View connector replicates HMI screen images over an enforced one-way transfer using a non-routable protocol break.



OPSWAT.

USE CASE

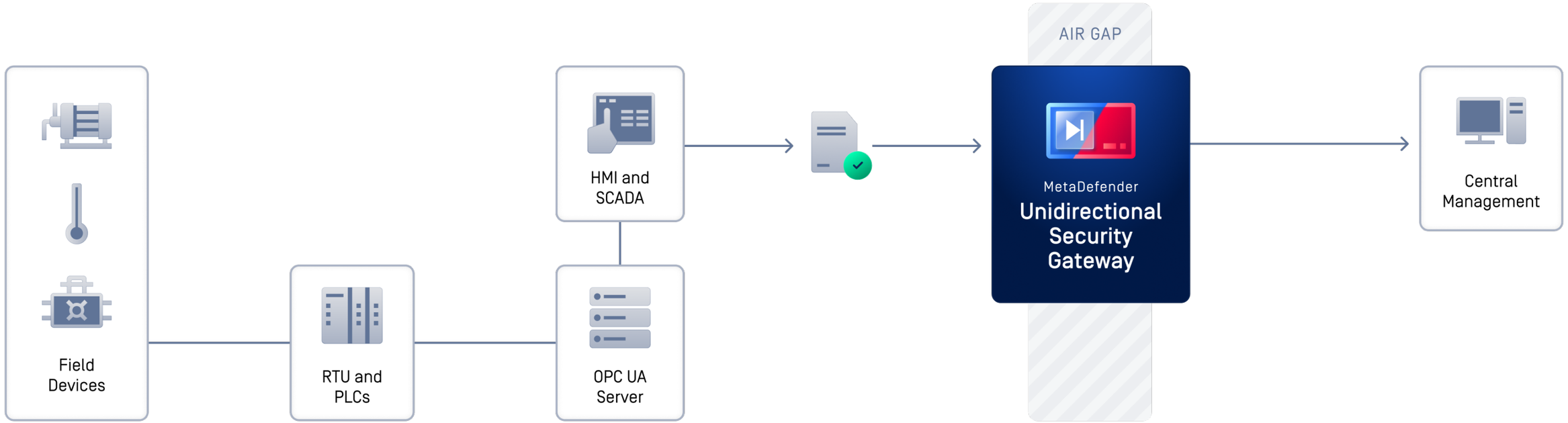
Water Treatment Plant Requires Real-Time Replication of OPC Data

Challenge

Transfer real-time operational data for OT to IT without compromising OT infrastructure security in water/waste-water facilities.

Solution

MetaDefender Unidirectional Security Gateway, which natively supports Open Platform Communications Unified Architecture (OPC UA), will integrate with OPC UA server in the OT domain and transfer real time values to IT over an enforced one-way transfer using a non-routable protocol.



OPSWAT.

USE CASE

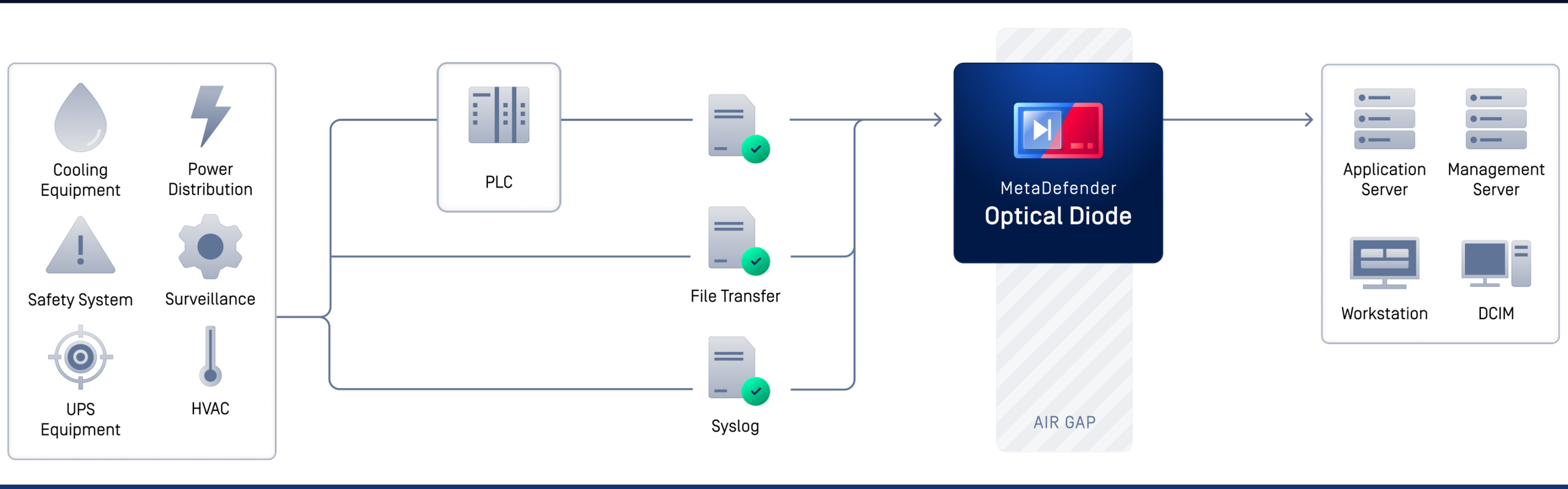
National Healthcare Provider Requires Secure Transfer of Data Center Alerts and Monitoring Data

Challenge

Replicate Data Center alerts and monitoring data without compromising OT infrastructure security.

Solution

MetaDefender Optical Diode securely transfers alerts and monitoring data to a central monitoring location. MetaDefender Modbus, SFTP and SMTP (email) connectors transfer data over an enforced one-way non-routable protocol break.



OPSWAT.

USE CASE

File Transfer of Compliance Reports from OT to IT

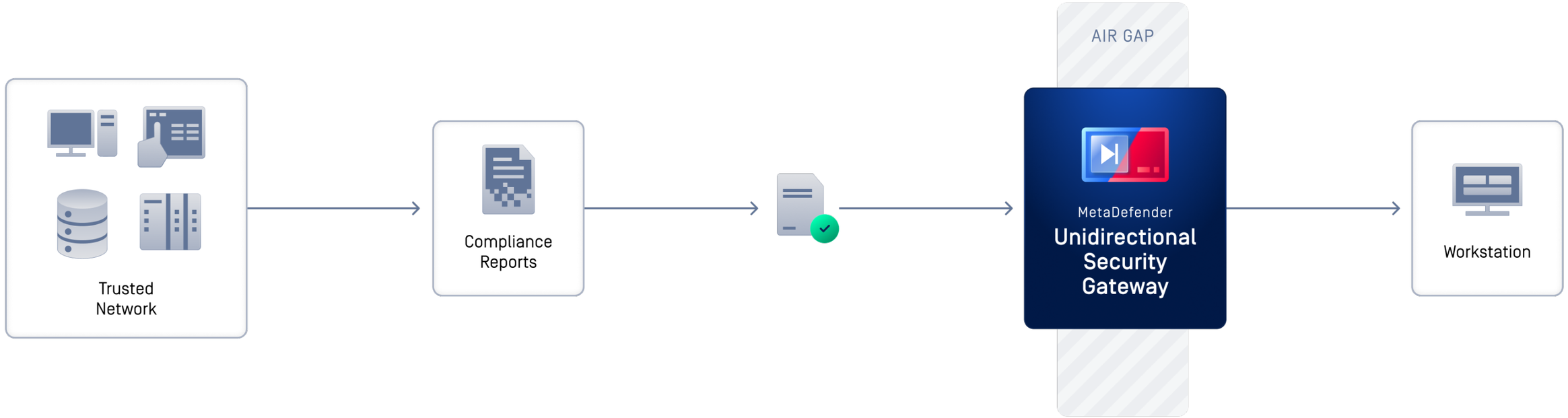
Oil & gas supplier requires secure file transfer from bulk plant OT network to corporate IT network.

Challenge

Plant compliance reports are captured as files on the OT network and transferred to the IT network. When a security perimeter is established around the Bulk Plant, there needs to be a way of securely sharing the compliance reports with the outside business network.

Solution

MetaDefender Unidirectional Security Gateway reliably transfers compliance reports utilizing a Secure File Transfer (SFTP). Files are securely transferred over a non-routable protocol break ensuring the data is transferred unidirectionally and that no communications can occur back into the OT network.



OPSWAT.

USE CASE

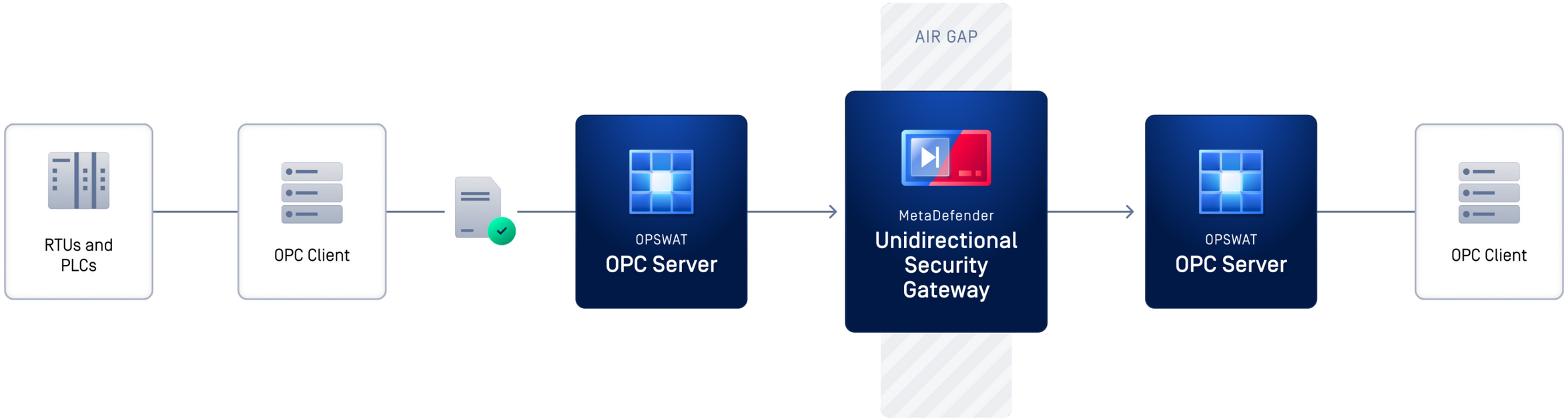
Liquid Natural Gas Producer Requires Secure Real-Time Replication of OPC DA/AE Data

Challenge

Transfer real-time OPC DA/AE data from OT to IT without compromising OT infrastructure security.

Solution

MetaDefender Unidirectional Security Gateway natively supports Open Platform Communications (DA/AE). The MetaDefender OPC Connector acts as an OPC Client on the OT network and an OPC Server on the IT network. MetaDefender l transfers real-time OPC values and alarms/events over an enforced one-way transfer using a non-routable protocol break.



OPSWAT.

USE CASE

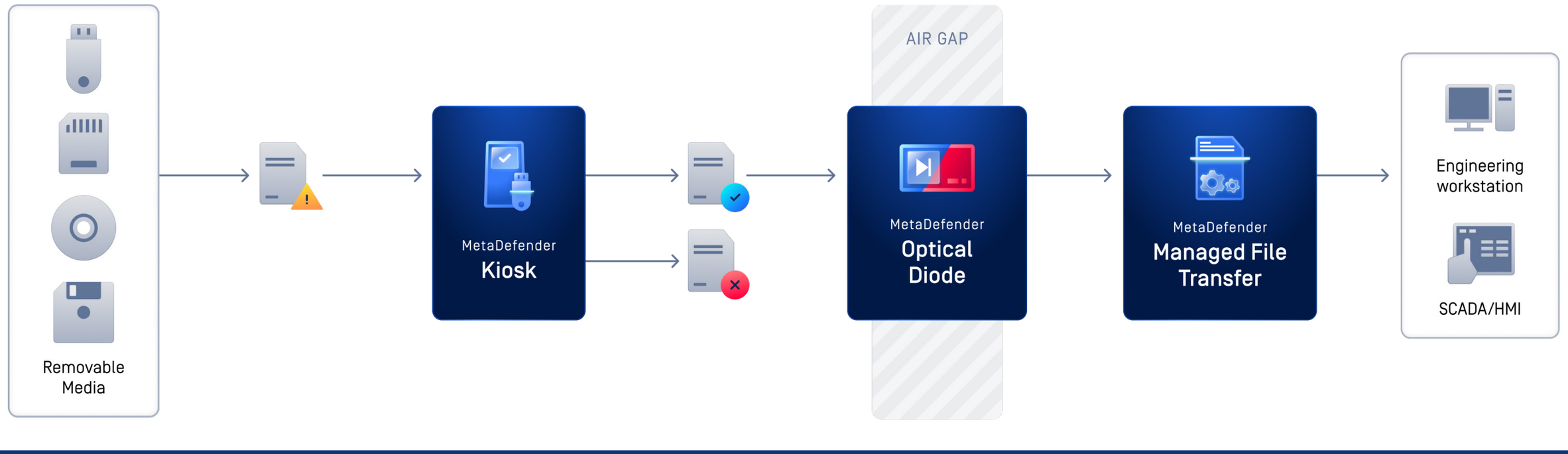
Secure File Transfer from MetaDefender Kiosk to Managed File Transfer

Challenge

Secure file transfer to enable the transfer of software updates, patches and files, stored on portable media. Files need to be sanitized on the IT network to prevent malware from propagating into the OT network.

Solution

MetaDefender Kiosk Multiscanning AV engines and file sanitization ensure that only known good files are transferred across the network boundary. MetaDefender Unidirectional Security Gateway provides air-gapped network separation and file transfer into the MetaDefender MFT.



OPSWAT.

USE CASE

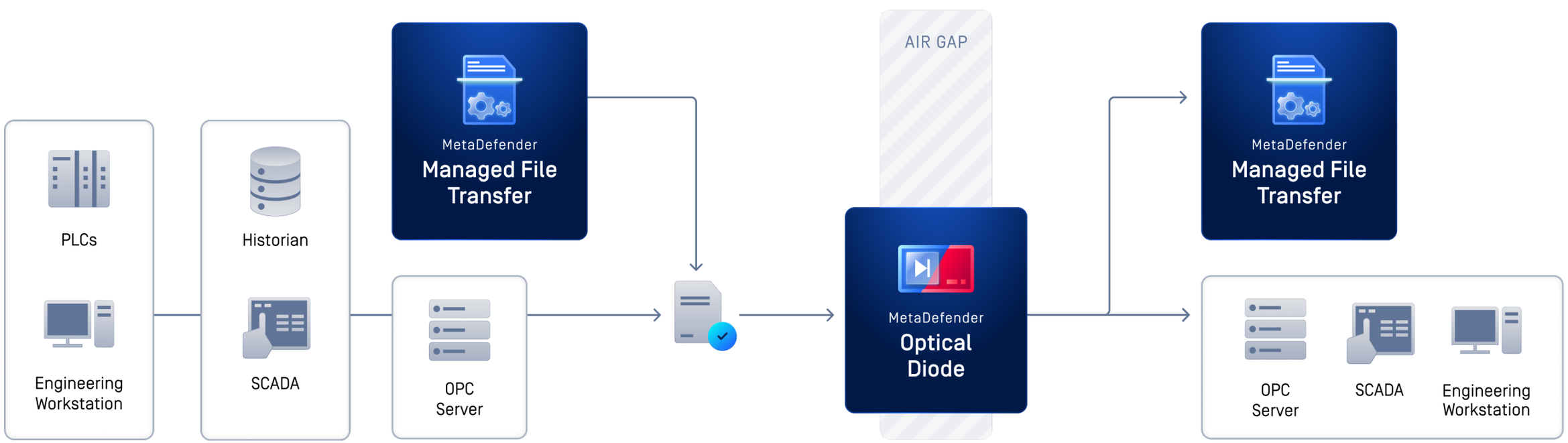
Creating a Secure Backup at a Disaster Relief Facility for Power Generation Plants

Challenge

A secure backup site is needed to restore operations in the event of a physical or cyber issue where normal operations are compromised. The site needs to be isolated to prevent malware from propagating to the disaster recovery facility.

Solution

MetaDefender Optical Diode replicates real time supervisory control and data acquisition (SCADA) data to the backup disaster recovery site while isolating it from the compromised environment. MetaDefender Managed File Transfer (MFT) to MFT replication stores the latest version of device software at the backup facility.



OPSWAT.

USE CASE

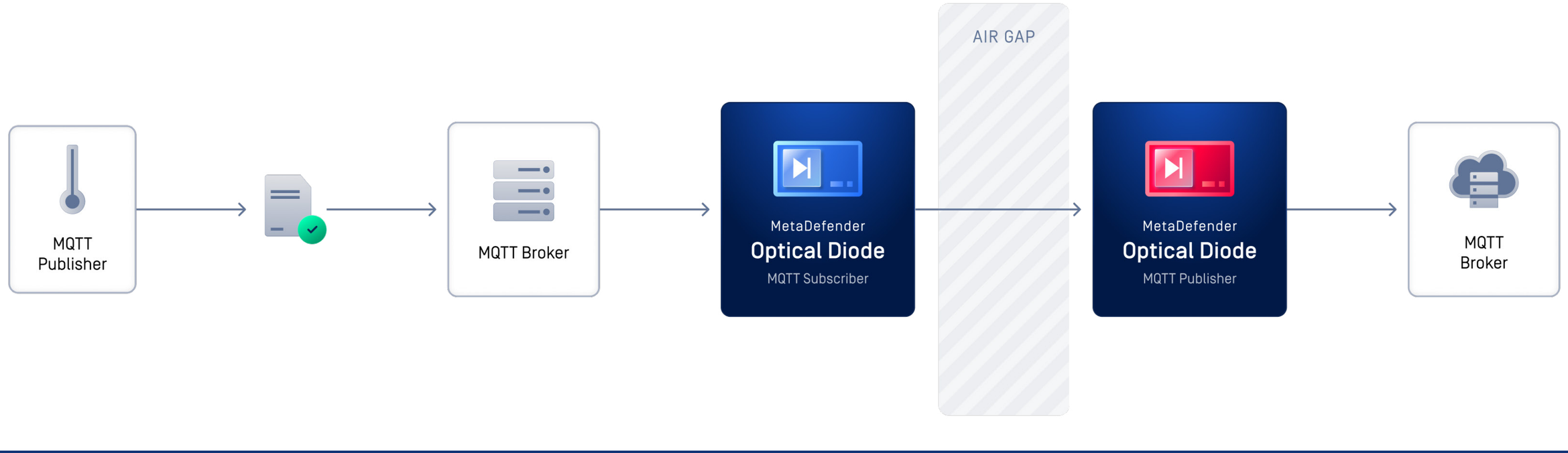
Food Processing Plant Requires MQTT Messages to be Securely Replicated to Cloud-Based Broker

Challenge

Securely replicate and transfer MQTT messages from OT to a cloud-deployed MQTT broker without compromising OT infrastructure security.

Solution

MetaDefender Optical Diode Din Rail natively supports MQTT. The MQTT connector acts as a MQTT subscriber on the OT network and a MQTT publisher on the IT network. Optical Diode transfers MQTT messages over a TLS connection to the cloud-based broker over an enforced one-way transfer using a non-routable protocol break.



OPSWAT.

USE CASE

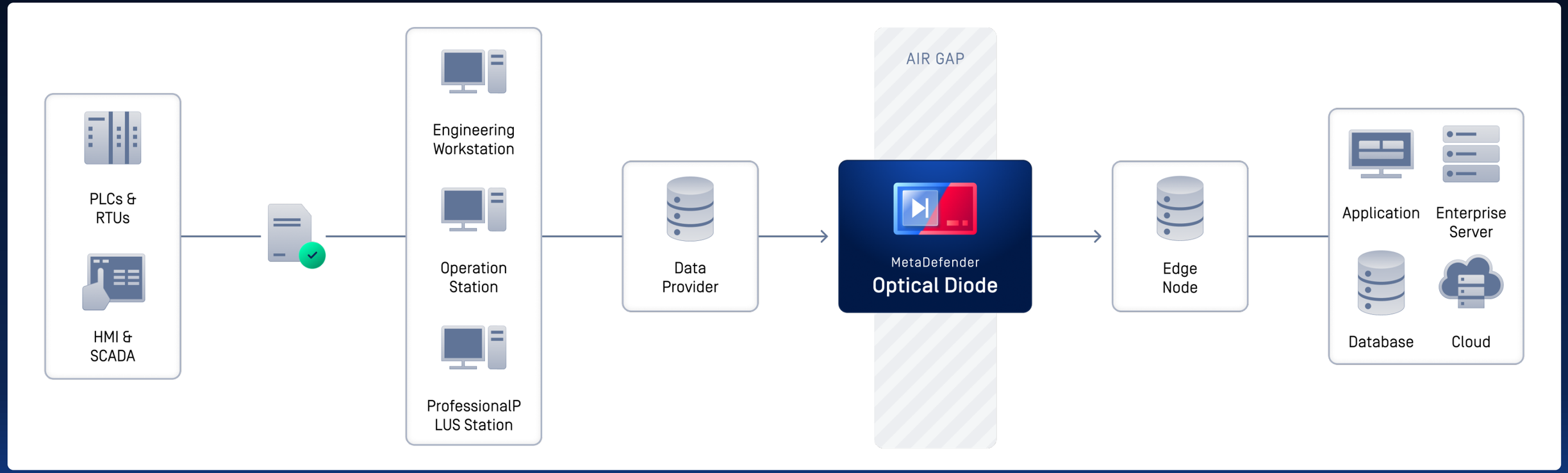
Establish Security Perimeter Around DeltaV Control Network

Challenge

Secure transfer data from the data provider to the edge node while eliminating external intrusion or data being written back to DeltaV.

Solution

MetaDefender Optical Diode directly connects the data provider and the edge node. MetaDefender HTTPS connector transfers data over an enforced one-way, non routable protocol break ensuring there is no possibility for external intrusion or data being written back to DeltaV.



OPSWAT.

USE CASE

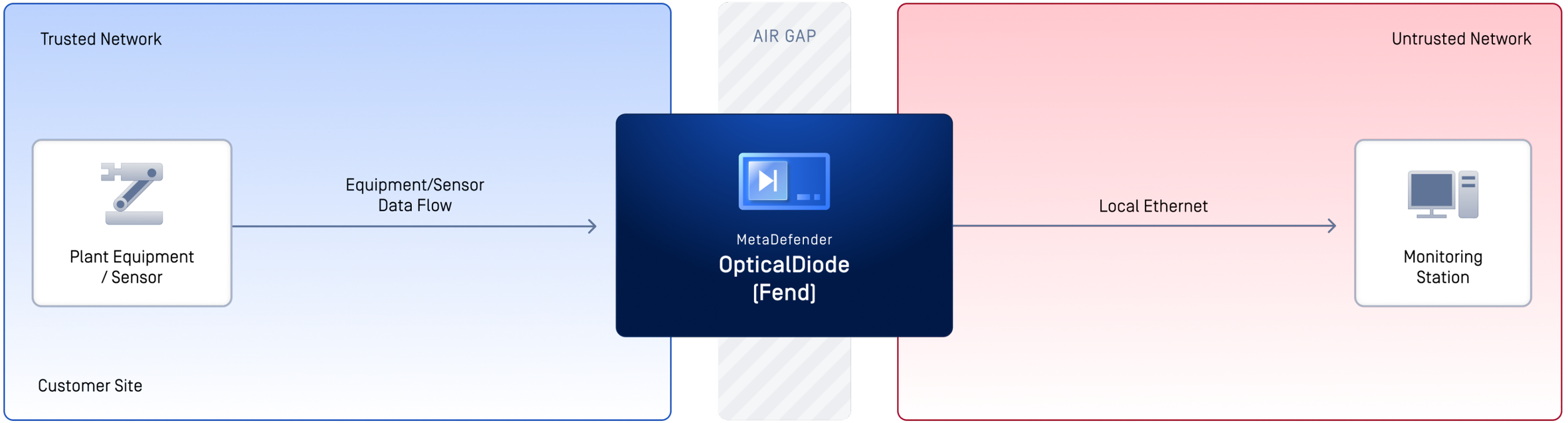
Send Industrial Modbus Data for Remote Monitoring with Fend Diodes

Challenge

Water utilities rely on thousands of industrial sensors and controllers across treatment plants and distribution systems. These systems often run Modbus TCP or Modbus RTU. Operators and engineers need timely access to operational data for monitoring plant performance and ensuring water quality. However, opening network pathways to provide this access to Modbus controllers and PLCs exposes critical equipment to cyber risks, including ransomware and remote exploitation.

Solution

With onboard Modbus TCP and Modbus RTU support, MetaDefender Optical Diode (Fend) enables secure, unidirectional transfer of sensor and controller data from treatment plant networks to remote servers at monitoring centers. MetaDefender Optical Diode (Fend) can even do onboard protocol translation, such as translating legacy Modbus RTU to Modbus TCP or modern JSON formats. Operators gain visibility into process performance without creating a backchannel into sensitive OT assets. This ensures continuous monitoring, regulatory compliance, and operational efficiency while maintaining a physically isolated control environment.



OPSWAT.

USE CASE

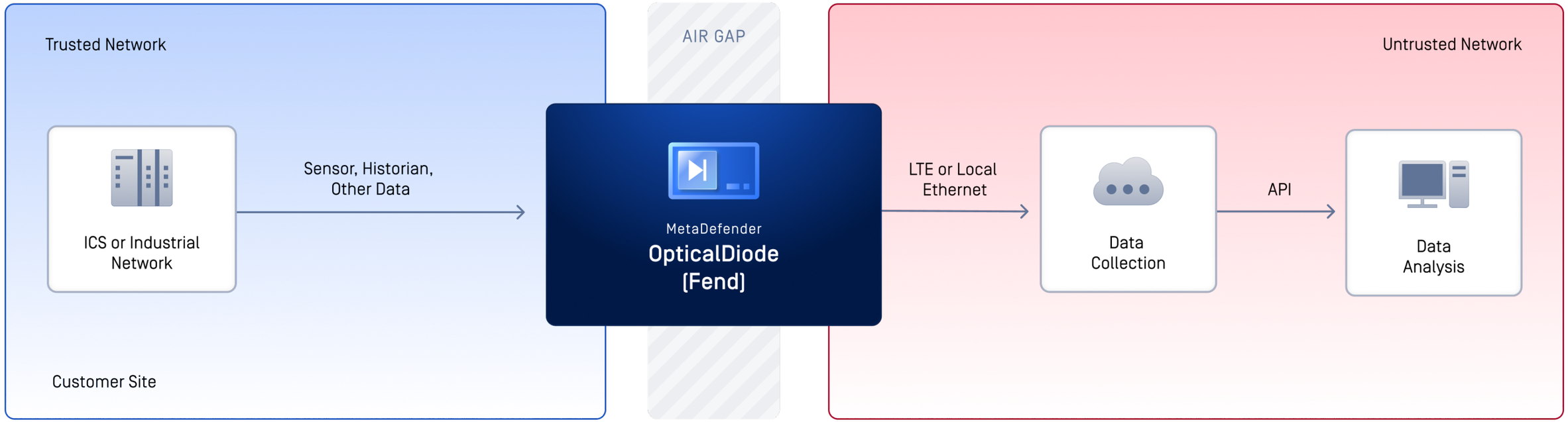
Cloud-Based Analytics for Secure Data Transport with Fend Diodes

Challenge

Manufacturing plants are turning to cloud-based analytics for predictive maintenance, energy optimization, and production efficiency insights. However, directly connecting production environments to the cloud risks introducing malware or command channels that could disrupt operations.

Solution

MetaDefender Optical Diode (Fend) securely extracts data from production environments and transmits it via local Ethernet or LTE to the Fend Cloud. From there, the data is collected and securely delivered to third-party or in-house analytics platforms via APIs. This approach ensures data confidentiality and integrity while blocking all inbound connections to critical manufacturing assets.



OPSWAT.

USE CASE

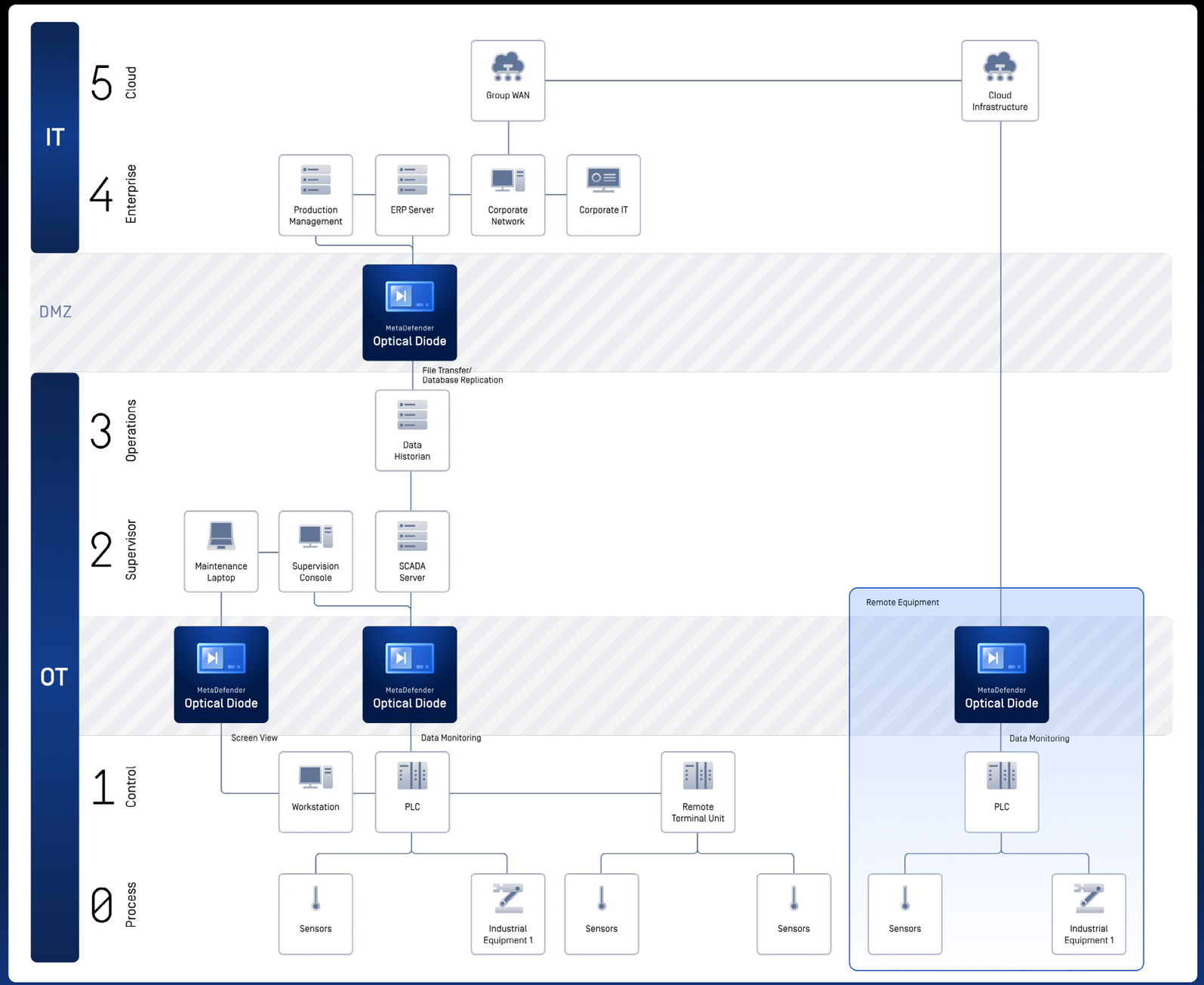
Unidirectional Protection for OT to IT Transfer of Industrial Control Data in Oil & Gas Production Networks

Challenge

Oil & gas networks host critical assets like PLCs, SCADA servers, and RTUs that run drilling, compression, and refining. Corporate IT and supervisory teams need continuous access to logs, compliance reports, and performance metrics, often over UDP/TCP. But opening these pathways exposes production networks to cyber risks, misconfigurations, and attacks that could disrupt operations or safety.

Solution

MetaDefender Optical Diode (Fend) provides hardware-enforced one-way communication for UDP, TCP, and Syslog from production to IT. Data, alarms, and logs flow out securely, while inbound traffic is blocked. This isolation gives real-time visibility and compliance assurance without exposing PLCs or equipment, helping operators reduce downtime and strengthen safety.



OPSWAT.

USE CASE

SQL Server Replication

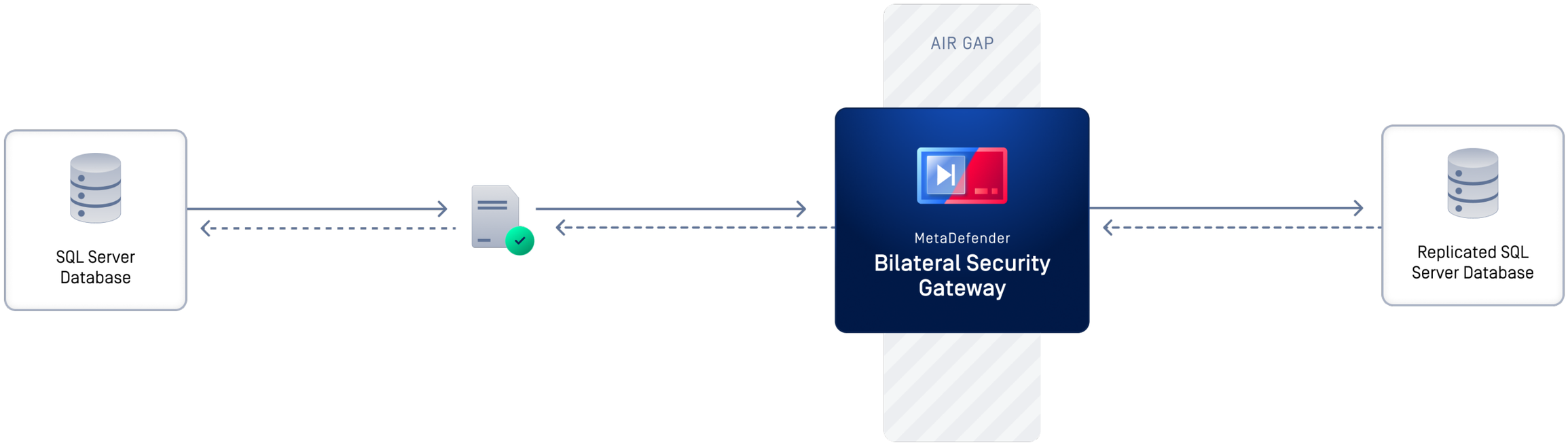
Challenge

Enable secure, real-time replication of a large Microsoft SQL database using native replication tools while assuring no synchronization issues.

Solution

MetaDefender Bilateral Security Gateway employs Microsoft's standard transactional replication services, removing the need for complicated scripting, custom installation, or modification of the SQL environment. SQL server replication is also transparent to users.

Standard buffering takes over if the connection is temporarily lost. MetaDefender maintains Microsoft replication constraints and does not introduce any additional requirements.



OPSWAT.

USE CASE

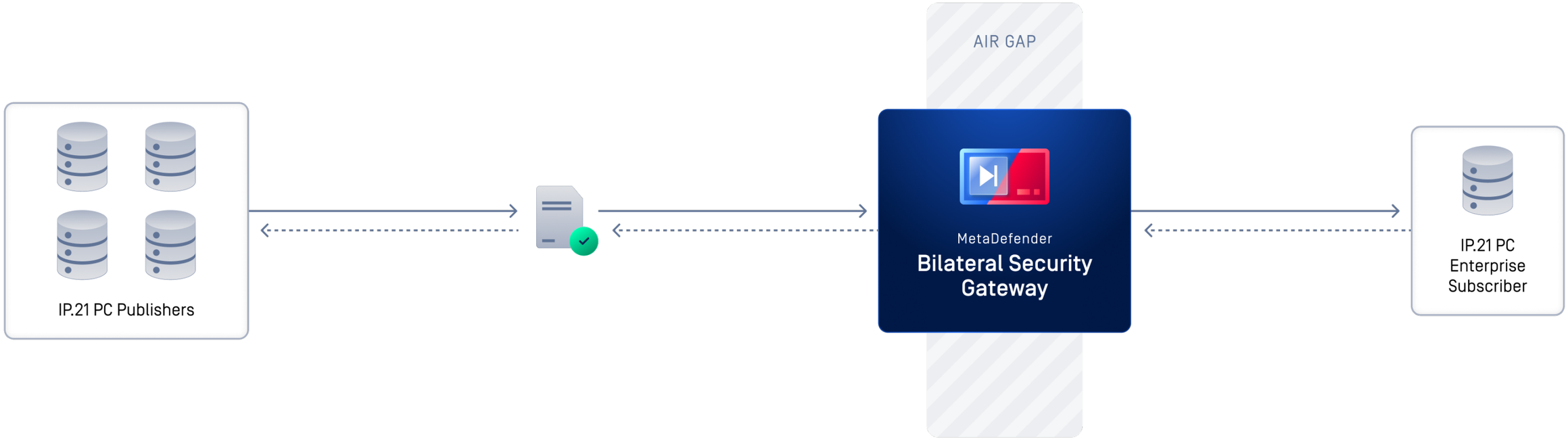
AspenTech IP.21 Replication Between Plant and Enterprise Historian

Challenge

Plant historical data is captured in special purpose databases referred to as historians. When a security perimeter is established around plant assets, there needs to be a way of securely sharing historian data with the outside business network.

Solution

MetaDefender Bilateral Security Gateway reliably replicates historian data using the native AspenTech IP.21 replication facility. Data is transferred over non-routable protocol breaks enhancing security and confidentiality of the source network.



GET STARTED

Are you ready to put MetaDefender NetWall on the front lines of your cybersecurity strategy?

Talk to one of our experts today.

Scan the QR code or visit us at:
opswat.com/get-started
sales@opswat.com

OPSWAT.
Protecting the World's Critical Infrastructure

For over 20 years OPSWAT, a global leader in IT, OT, and ICS critical infrastructure cybersecurity, has continuously evolved an end-to-end solutions platform that gives public and private sector organizations and enterprises spanning Financial Services, Defense, Manufacturing, Energy, Aerospace, and Transportation Systems the critical advantage needed to protect their complex networks from cyberthreats.

Built on a "Trust no file. Trust no device.™" philosophy, OPSWAT solves customers' challenges like hardware scanning to secure the transfer of data, files, and device access with zero-trust solutions and patented technologies across every level of their infrastructure. OPSWAT is trusted globally by more than 1,900 organizations, governments, and institutions across critical infrastructure to help secure their devices, files, and networks from known and unknown threats, zero-day attacks, and malware, while ensuring compliance with industry and government-driven policies and regulations.

Discover how OPSWAT is protecting the world's critical infrastructure and securing our way of life; visit www.opswat.com.

©2026 OPSWAT Inc. All rights reserved. OPSWAT, MetaScan, MetaDefender, MetaDefender Vault, MetaAccess, Netwall, OTfuse, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device. are trademarks of OPSWAT Inc. Rev. 2026 May