OWL Cyber Defense

USE CASE BROCHURE

Critical Infrastructure Use Cases

Using Data Diode Cybersecurity to Defend Industrial Control Systems

OWL

Cyber Defense

Table of Contents

The Next Generation of Cybersecurity Solutions

The United States Department of Homeland Security (DHS) defines 16 sectors of critical infrastructure, whose assets, systems, and networks are considered to be vital to the United States such that their debilitation or destruction would have a significant effect on the nation's security, economy, and/or public health and safety.

The 16 Sectors of Critical Infrastructure

1. Chemical
2. Commercial Facilities
3. Communications
4. Critical Manufacturing
5. Dams
6. Defense Industrial Base
7. Emergency Services
8. Energy
9. Financial Services
10. Food & Agriculture
11. Government Facilities
12. Healthcare & Public Health
13. Information Technology
14. Nuclear Reactors, Materials, & Waste
15. Transportation Systems
16. Water & Wastewater Systems

This paper outlines **19 use cases** for the implementation of Owl data diode cybersecurity to defend a variety of these critical infrastructure sectors. The use cases feature industry leaders and demonstrate how Owl helped them meet a number of security and operational requirements through a one-way, deterministic data flow.

In each of these cases, Owl data diodes are interoperating with a wide array of leading operational technologies, including, but not limited to: OSIsoft® PI System, Schneider Electric Wonderware, GE Historian, Rockwell Automation FactoryTalk®, Modbus, OPC, mobile networks, and software firewalls. Please see the Index at the end of this document for a full list and references for all sectors and technologies included.

OSIsoft. Partner

Rockwell Automation Encompass™ Product Partner

Schneider Electric

GE

We hope these use cases provide a good introduction into the capabilities of Owl and some of the ways data diodes can be used to solve today's cybersecurity issues.

USE CASE: OIL & GAS

Global Oil & Gas Company Enables Secure, One-Way Production Data Transfer to HQ

Company Overview

A global oil and gas producer, manufacturer and marketer, with crude oil production of over 3 billion barrels annually.

Cybersecurity Challenge

A malware breach destroyed data and application servers, severely impacting daily operations. In response, the company disconnected their operational technology (OT) network from their wide-area network (WAN) and disconnected their WAN from the corporate IT network. While disconnecting the plant prevented malware proliferation across the various networks, it led to loss of business continuity and lack of visibility into plant operations.

REQUIREMENTS:

1. Restore business continuity and operational visibility
2. Maintain a “disconnected” or segmented cybersecurity architecture
3. Failover, redundancy, and load-balancing capabilities
4. Scalable architecture for additional volume or data types as needed
5. Ability to centrally monitor security operations and technology

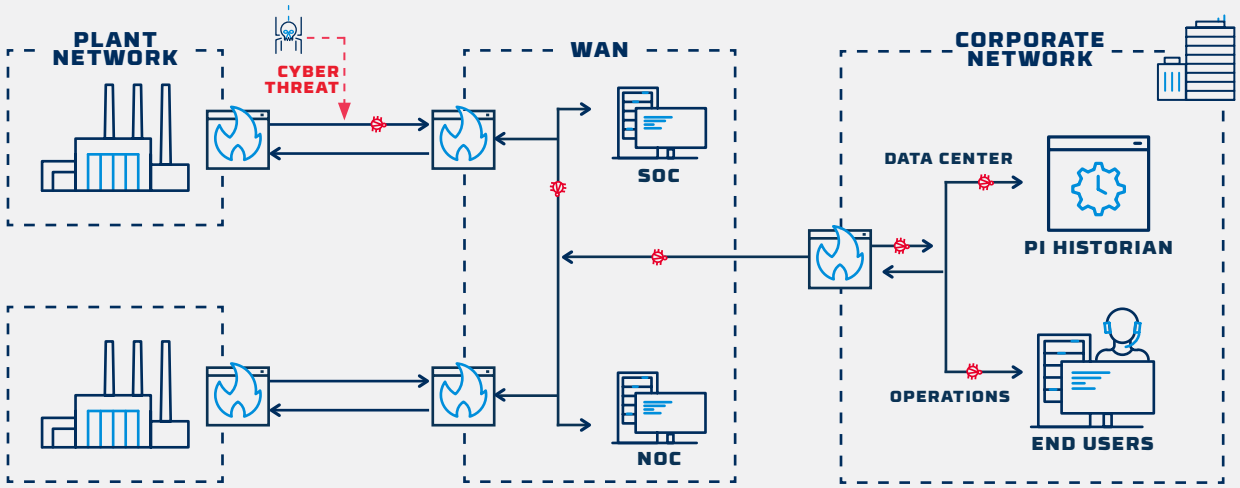
Case Summary

INDUSTRY:
Oil & Gas

SOLUTION:
Owl data diodes deployed along with OPTS PI System historian replication software.

CHALLENGE:
Malware breach destroyed data, causing company to disconnect operational and business networks.

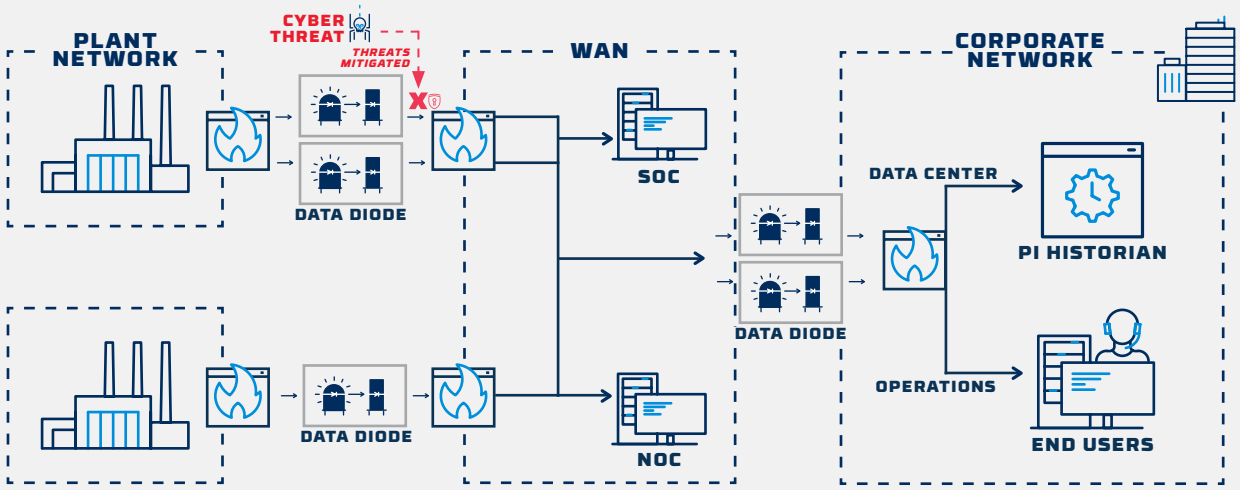
BENEFITS:
Deterministic, one-way flow of production data into HQ enabled increased visibility without increased risk. Centralized performance and data flow monitoring.



USE CASE (BEFORE)

SOLUTION

Owl data diode technology (OPDS/EPDS) was selected for effective network segmentation, and secure one-way data transfer, including IT syslog flow from plant assets to the Network Operations Center in the WAN. OSIsoft® PI System historian replication (OPTS) was also added to enable transfer of OT data to the HQ.



USE CASE (AFTER)

DEPLOYMENT

EPDS

Enterprise Perimeter Defense Solution

Data diode communication card pair, mounted on independent, send-only and receive-only commercial servers, for network segmentation and deterministic, one-way data transfer.

OPDS-MP

Owl Perimeter Defense Solution - Multi Purpose

Self-contained 1U data diode, purpose-built for network segmentation and deterministic, one-way data transfer.

INTERFACE MODULE

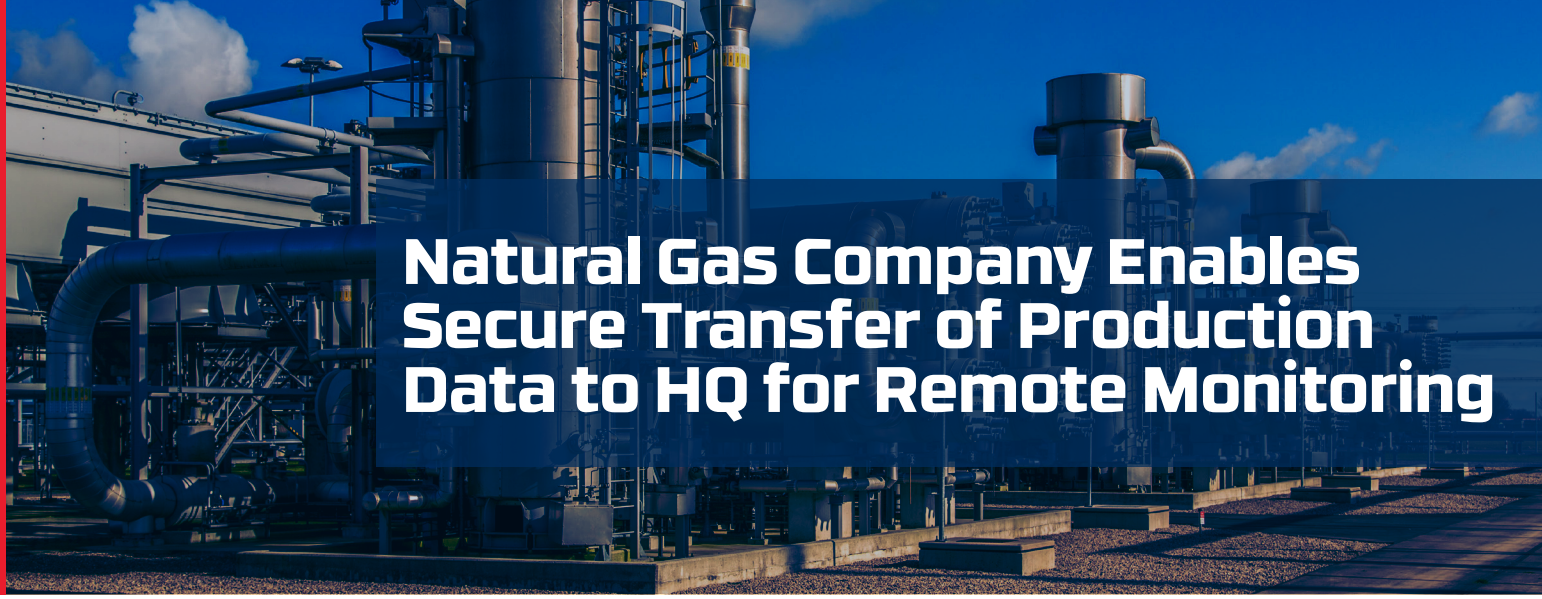
Owl PI Transfer Service (OPTS)

Specialized software developed specifically for secure replication and transfer of OSIsoft® PI System historian data across network boundaries.

RESULTS

1. Provided security through effective network segmentation at both the plant OT and headquarters IT network boundaries, helping to prevent malware breach and proliferation
2. Enabled redundant, deterministic outbound OT data flows from the plants into the corporate data stores
3. Replicated OSIsoft® data historians allowing full production data use and visibility from within the HQ
4. Provided full insight into security performance with central monitoring from the Security Operations Center

USE CASE: NATURAL GAS



Natural Gas Company Enables Secure Transfer of Production Data to HQ for Remote Monitoring

Company Overview

A liquefied natural gas producer, with total annual capacity of over 36 million tons.

Cybersecurity Challenge

A malware breach destroyed data and application servers, severely impacting daily operations. In response, the company disconnected their operational technology (OT) network from their corporate IT network. While disconnecting electronic communications with the plant prevented malware proliferation, it led to loss of business continuity and lack of visibility into plant operations.

REQUIREMENTS:

1. Restore business continuity and operational visibility
2. Maintain a “disconnected” or segmented cybersecurity architectur
3. Enable OSIsoft PI System historian replication from OT network to corporate IT network
4. Allow remote alarm monitoring from corporate network operations center

Case Summary

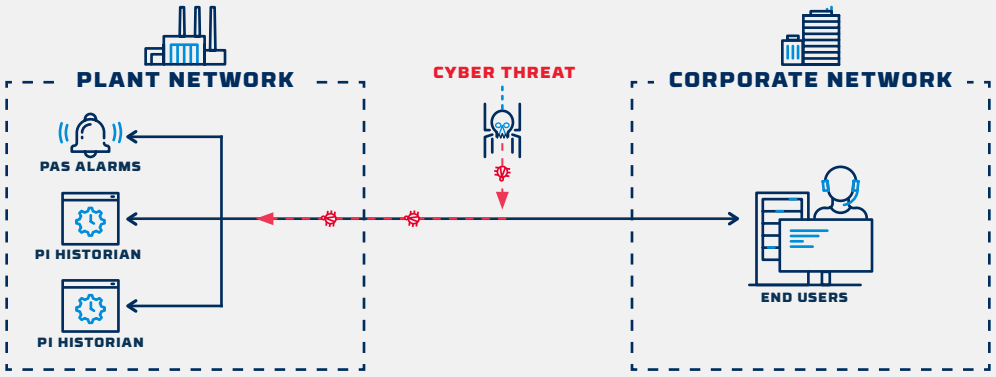
INDUSTRY:
Natural Gas Production

SOLUTION:
Owl EPDS data diodes deployed along with OPTS PI System historian replication application.

CHALLENGE:
Malware breach destroyed operations data, causing company to disconnect operational and business networks.

BENEFITS:
Deterministic, one-way data flow of PI System/OT data into HQ enabled increased visibility without increased risk to production facilities. Restored remote alarm monitoring to corporate IT.

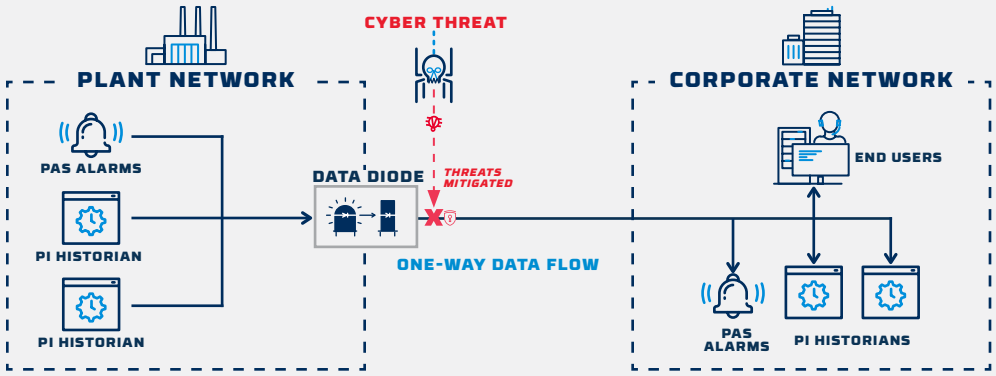
USE CASE (BEFORE)



SOLUTION

Owl data diode technology (EPDS) was selected for effective network segmentation, and secure one-way data transfer, including IT syslog flow from plant assets to the corporate HQ. OSIsoft® PI System historian replication (OPTS) was also added to enable transfer of OT data to the HQ.

USE CASE (AFTER)



DEPLOYMENT

EPDS

Enterprise Perimeter Defense Solution

Data diode communication card pair, mounted on independent, send-only and receive-only commercial servers, for network segmentation and deterministic, one-way data transfer.

INTERFACE MODULE

Owl PI Transfer Service (OPTS)

Specialized software developed specifically for secure replication and transfer of OSIsoft® PI System historian data across network boundaries.

RESULTS

1. Provided network cybersecurity with effective segmentation of the plant OT network, helping to prevent malware breach and proliferation
2. Permitted deterministic outbound OT data flows from the plants into the corporate data stores
3. Replicated PI System data historians allowing full production data use and visibility from within the HQ
4. Restored alarm data flow from plant assets to corporate users

USE CASE: GAS TURBINE

Gas Turbine Support Vendor Enables Centralized Remote Operation & Maintenance Monitoring

Company Overview

Major gas turbine maintenance vendor and spare parts supplier, specializing in turbine technical maintenance needs and performance optimization. Oversees operation and maintenance (O&M) of over 60 turbines across multiple sites; relying on remote monitoring to determine when on-site maintenance is required.

Cybersecurity Challenge

The turbine maintenance service required structured and secure remote monitoring of 60+ turbines at multiple sites for analytics and optimization. However, direct internet access to the turbines would render them vulnerable to cyberattack. The company required a solution which would enable remote monitoring without allowing remote access to the turbines.

REQUIREMENTS:

1. Protect turbines from cyberattack
2. Automate transfer of turbine maintenance data from multiple sites to centralized collection point
3. Data transfer must be compatible with OPC DA
4. Centralized monitoring data must be accessible via web-portal

Case Summary

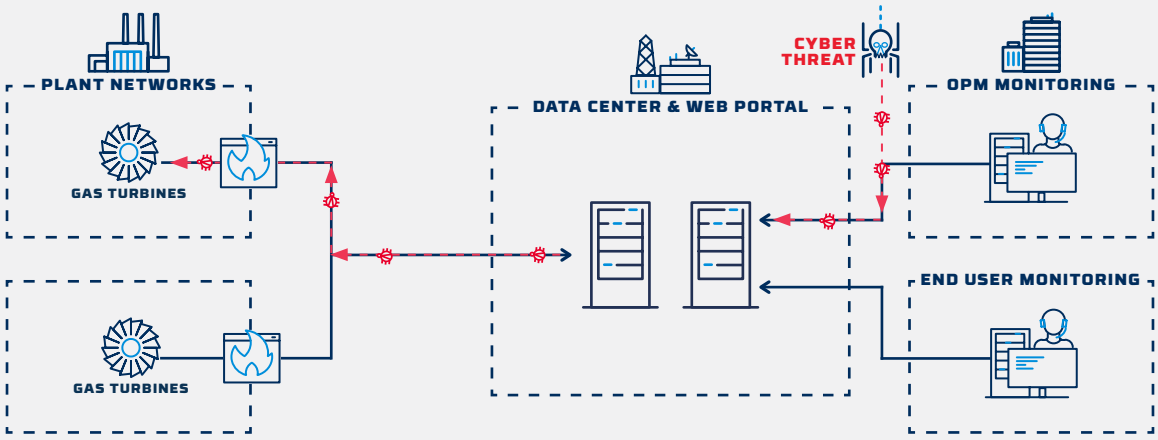
INDUSTRY:
Power Generation

SOLUTION:
OPDS-100D data diode solution selected to transfer OPC DA tags oneway, from turbines to a centralized remote monitoring center.

CHALLENGE:
Provide secure, centralized remote monitoring of turbine O&M data without allowing remote access to the process control network, DCS or turbines.

BENEFITS:
Turbine performance data is available remotely for centralized O&M monitoring, while the process control network and turbines are secured from external cyber threats.

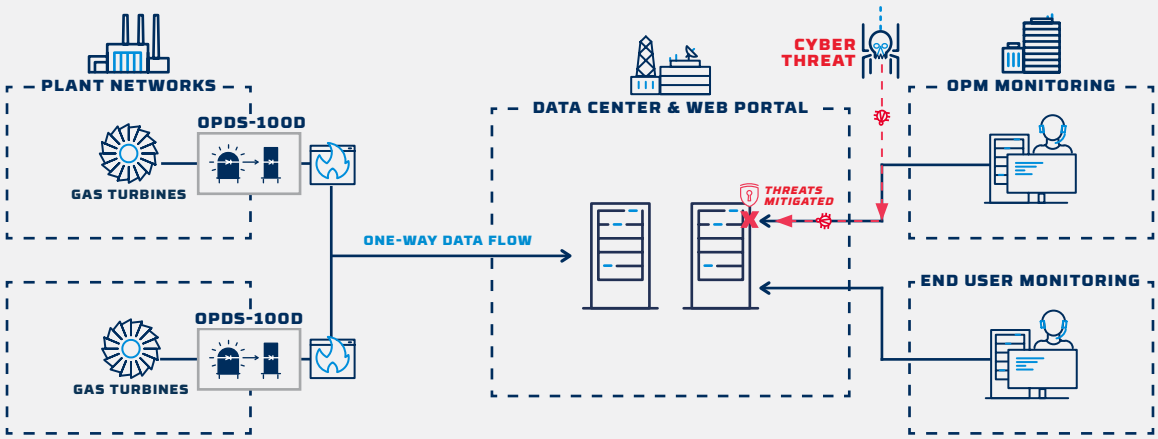
USE CASE (BEFORE)



SOLUTION

OPDS-100D data diode solution selected and deployed at each site to move OPC DA tags one-way, from turbines to remote monitoring web portal for operation and maintenance analytics. Data is collected from over 60 turbines across 9 physical sites, with one data diode at each site supporting all collection. From there the data is passed on to the remote monitoring center where the vendor can perform analytics and provide operation and maintenance recommendations to their customers.

USE CASE (AFTER)



DEPLOYMENT

OPDS-100D

Owl Perimeter Defense Solution - 100D

DIN rail compatible data diode solution for deterministic, one-way data transfer and effective network segmentation. Supports a wide range of data formats and transport layer protocols at up to 5 Mbps.

RESULTS

1. O&M data securely and automatically collected and transferred to a web-accessible centralized repository
2. Systems securely connected via hardware-enforced data diode for one-way-only data transfer
3. Data is available offsite for remote monitoring and analytics while the turbines are secured from external access

USE CASE: PETROCHEMICAL

Petrochemical Company Enables Secure, One-way Production Data Flow To Business IT

Company Overview

Major petrochemical manufacturer with annual production over 2 million tons.

Cybersecurity Challenge

A malware breach destroyed data and servers, severely impacting daily operations. In response, the company disconnected their operational technology (OT) network from their wide-area networks (WAN), and the WAN from their corporate IT network at HQ. While this prevented any future malware proliferation, it led to lack of visibility and business continuity, due to the severed electronic communications.

REQUIREMENTS:

1. Maintain a “disconnected” or segmented cybersecurity architecture
2. Restore plant performance data to corporate IT networks via replication of Open Platform Communications (OPC) servers
3. Enable OSIsoft® PI System historian replication from OT network to corporate IT network
4. Allow real-time OPC alarm monitoring at corporate HQ

Case Summary

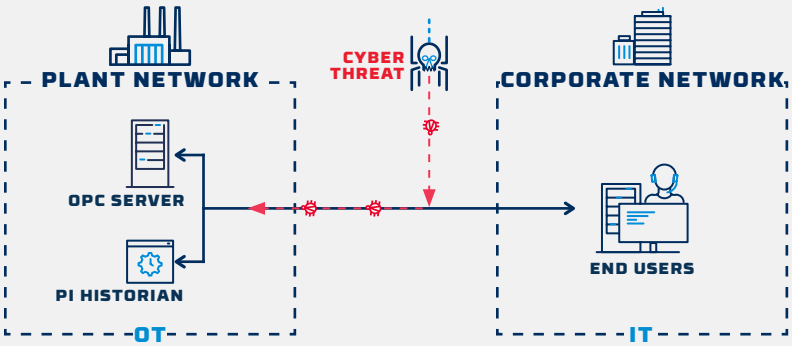
INDUSTRY:
Petrochemical Production

SOLUTION:
OPDS data diodes deployed along with OPTS PI System replication and OSTS OPC replication applications to reestablish business continuity.

CHALLENGE:
Malware breach destroyed data, causing company to disconnect operational and business networks.

BENEFITS:
Deterministic, one-way data flow of PI System/OT data into HQ increased visibility without increasing risk. Enabled real-time OPC alarm monitoring at corporate HQ.

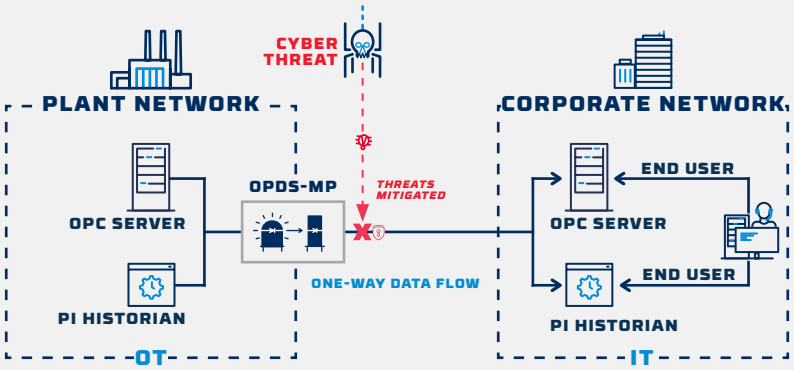
USE CASE (BEFORE)



SOLUTION

Owl data diodes utilizing patented technology (OPDS-MP) were selected for effective network segmentation and deterministic, one-way data transfer from OT assets to the corporate network. PI System replication (OPTS) added to enable transfer of plant operations data to the business unit, as well as OPC server replication (OSTS).

USE CASE (AFTER)



DEPLOYMENT

OPDS-MP

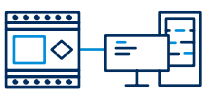
Owl Perimeter Defense Solution - Multi Purpose

Self-contained 1U data diode, purpose-built for network segmentation and deterministic, one-way data transfer.

INTERFACE MODULES

Owl PI Transfer Service (OPTS)

Specialized software developed specifically for secure replication and transfer of OSIsoft® PI System historian data across network boundaries.



OPC Secure Transfer Service (OSTS)

Specialized and certified application for secure, real-time OPC data and event monitoring across network boundaries.

RESULTS

1. Preserved effective network segmentation at the plant OT network boundary helping to prevent malware breach and proliferation
2. Permitted deterministic outbound PI System/OT data flows from the plants to the corporate data stores for increased visibility and business continuity
3. Replicated real-time OPC data allowing full performance, alarm, and event data access by corporate end users

USE CASE: MINING

Rare Earth Mining Company Secures Operational Network From Advanced Persistent Threats

Company Overview

Rare earth and rare metal mining and manufacturing company with facilities across 10 countries.

Cybersecurity Challenge

The company suffered repeated attacks from advanced persistent threats (APT). In response, the company disconnected their operational technology (OT) network from all outside networks. While this prevented attack, it led to lack of visibility and business continuity with their operations facilities.

REQUIREMENTS:

1. Store all operational data generated by Rockwell PLCs in OSIsoft® PI System historian
2. Replicate PI System data from OT network to business end users
3. Maintain a “disconnected” or segmented cybersecurity architecture, preventing any inbound data flow to OT network

Case Summary

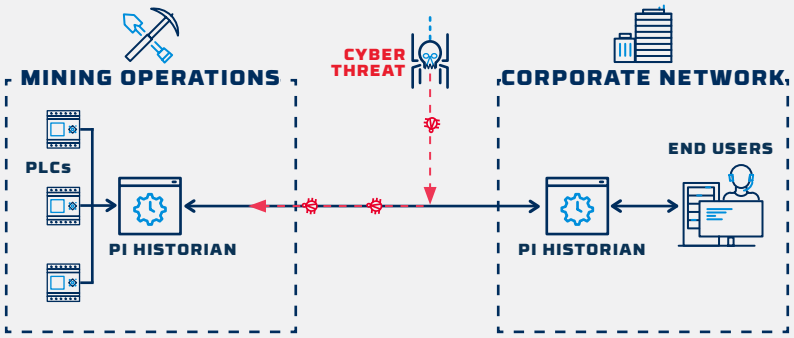
INDUSTRY:
Rare Earth Mining

SOLUTION:
OPDS data diodes deployed along with OPTS PI System replication application.

CHALLENGE:
Repeated breach attempts by APT caused company to disconnect OT networks from any outside network connection.

BENEFITS:
Deterministic, one-way data flow secured OT network from outside influence or attack and enabled PI System replication to corporate end users.

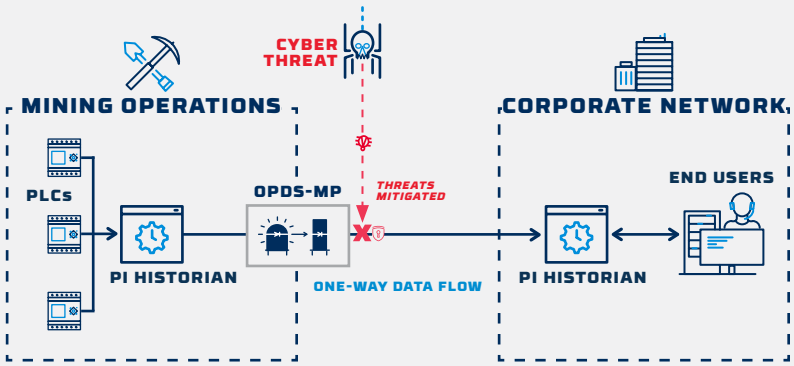
USE CASE (BEFORE)



SOLUTION

Owl data diodes utilizing patented technology (OPDS-MP) was selected to secure the OT network from APT. This Provided effective network segmentation, and deterministic, one-way data transfer out of OT network. PI System replication (OPTS) was added to enable transfer of mining operations data to the business unit.

USE CASE (AFTER)



DEPLOYMENT

OPDS-MP

Owl Perimeter Defense Solution - Multi Purpose

Self-contained 1U data diode, purpose-built for network segmentation and deterministic, one-way data transfer.

INTERFACE MODULE

Owl PI Transfer Service (OPTS)

Specialized software developed specifically for secure replication and transfer of OSIsoft® PI System historian data across network boundaries.

RESULTS

1. Provided security through effective network segmentation of the OT network, helping to prevent breaches by APT
2. Permitted deterministic outbound data flows from OT network to the corporate data stores for increased visibility and business continuity
3. Rockwell operations data captured in local PI historian and replicated to corporate network
4. Replicated PI System historians allowed full performance, alarm, and event data access by corporate end users

USE CASE: WATER-WASTEWATER

Water/Waste Water Company Implements DHS Defense-In-Depth Cybersecurity Strategies

Company Overview

Major regional water/waste water authority serving over 800,000 customers.

Cybersecurity Challenge

In accordance with Department of Homeland Security (DHS) guidance issued in the paper, "Seven Strategies to Defend Industrial Control Systems," the company created a cybersecurity plan to reduce the surface area of their operational technology (OT) networks and create a more defensible environment.

REQUIREMENTS:

1. Change security policy and only execute command and control operations from within the OT/ plant network boundary
2. Implement a "disconnected" (segmented) cybersecurity architecture to eliminate all remote access to the OT/plant network.
3. Maintain business continuity through remote-only monitoring policies
4. Enable Human Machine Interface (HMI) screen replication at HQ

Case Summary

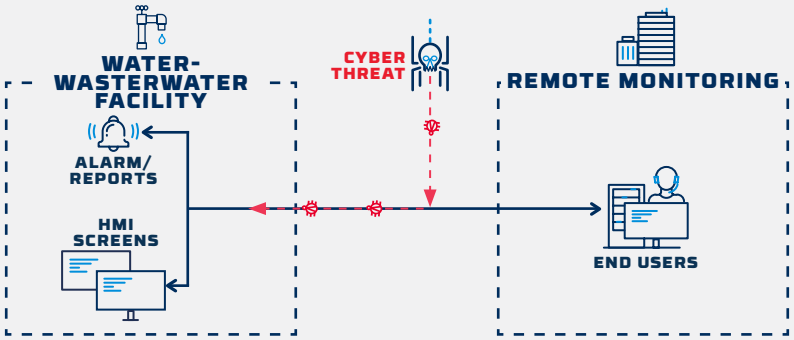
INDUSTRY:
Water / Wastewater

SOLUTION:
OPDS-MP data diodes deployed to transfer reporting & alarming information and provide remote HMI screen replication.

CHALLENGE:
Company recognized need to improve cybersecurity posture, following guidance from DHS, while retaining business continuity.

BENEFITS:
Deterministic, one-way data flow secured OT network from outside influence or attack, and enabled realtime, remote HMI screen monitoring at HQ.

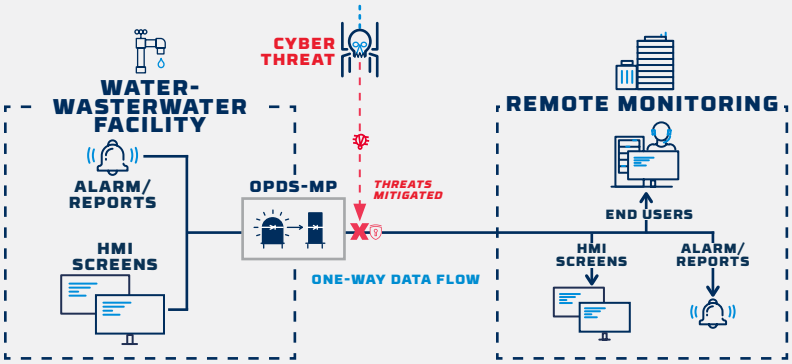
USE CASE (BEFORE)



SOLUTION

Owl data diodes utilizing patented technology (OPDS-MP) was selected to remove remote access to the OT network and provide effective network segmentation, and deterministic, oneway data transfer out of OT network. Along with OV2S application, this provided remote system monitoring, transfer of operational reports and a means to replicate HMI screens at remote locations.

USE CASE (AFTER)



DEPLOYMENT

OPDS-MP

Owl Perimeter Defense Solution - Multi Purpose

Self-contained 1U data diode, purpose-built for network segmentation and deterministic, one-way data transfer.

INTERFACE MODULE

Owl Virtiual ScreenView Service (OV2S)

Specialized software developed specifically for secure replication and transfer of OSIsoft® PI System historian data across network boundaries.

RESULTS

1. Improved security according to DHS strategies for defending industrial control systems
2. Removed all inbound communications to OT networks while providing deterministic outbound data flow for monitoring and business continuity
3. Enabled HMI screen replication for real-time offsite monitoring
4. Allowed remote access to operations reports and alarms at HQ

Nuclear Power Facility Meets US Nuclear Regulatory Commission Cybersecurity Regulations

Company Overview

A US-based nuclear power plant with over 1,000 megawatt generating capacity.

Cybersecurity Challenge

As a US nuclear power facility, the plant is subject to Nuclear Regulatory Commission (NRC) cybersecurity regulations, including Title 10 of the Code of Federal Regulations, as outlined in NRC Regulatory Guide 5.71. To achieve compliance, the company created a plan to upgrade cybersecurity according to the NRC guidance. The company also required OSIsoft PI System historian data replication, and remote Modbus critical cyber asset monitoring by business end-users on the corporate IT network.

REQUIREMENTS:

1. Clearly define network segments and eliminate all connections to critical OT systems from external networks
2. Enable one-way data flow from OT network to corporate IT network
3. Maintain business continuity via PI System replication to IT end users
4. Enable remote monitoring of critical cyber assets via modbus replication to corporate IT unit

Case Summary

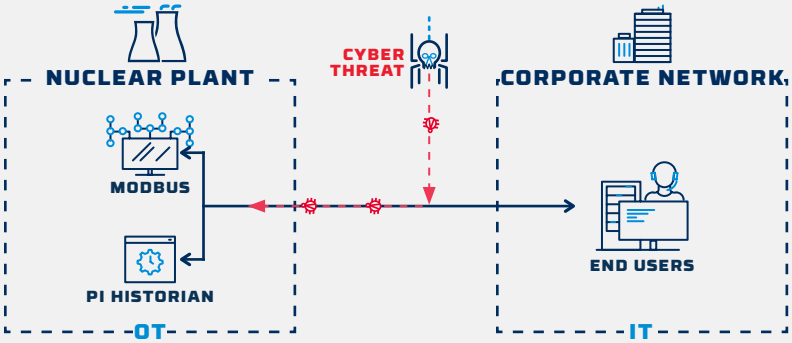
INDUSTRY:
Nuclear Power Generation

SOLUTION:
OPDS-1000 data diodes deployed along with OPTS PI System historian replication, and OMBI Modbus data replication.

CHALLENGE:
Company required increased cybersecurity and network defense according to US Code of Federal Regulations and NRC Regulatory Guide.

BENEFITS:
OT network secured from external influence or attack. PI System data and Modbus critical data asset monitoring data made available to business end users.

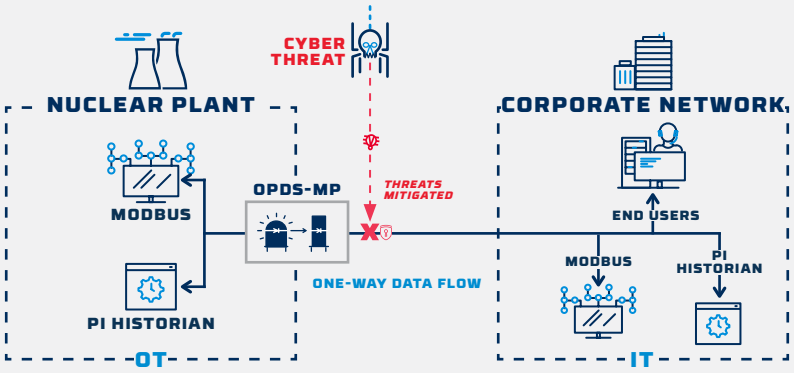
USE CASE (BEFORE)



SOLUTION

Owl data diodes utilizing patented technology (OPDS-1000) was selected to prevent remote access to the OT network, provide effective network segmentation, and enable deterministic, one-way data transfer. Added OSIsoft® PI System replication (OPTS) to transfer historian data from OT to IT network, and used OMBI Modbus integration to replicate critical cyber asset monitoring data.

USE CASE (AFTER)



DEPLOYMENT

OPDS-1000

Owl Perimeter Defense Solution - 1000

Self-contained 1U data diode, purpose-built for network segmentation and deterministic, one-way data transfer up to 1 Gbps.

INTERFACE MODULES

Owl PI Transfer Service (OPTS)

Specialized software developed specifically for secure replication and transfer of OSIsoft® PI System historian data across network boundaries.

Owl Modbus Interface (OMBI)

Specialized software developed for secure replication and transfer of Modbus protocol data across network boundaries.

RESULTS

1. Improved cybersecurity, achieving compliance with NRC Regulatory Guide and federal mandates for nuclear power facilities
2. Data diodes removed all inbound access to OT networks while providing deterministic outbound data flow for monitoring and business continuity
3. Enabled PI System historian and Modbus critical cyber asset replication for access by business users at corporate network

USE CASE: COAL POWER

Coal Power Facility Meets NERC CIP Version 5 Cybersecurity Regulations

Company Overview

A US-based coal power facility with over 2,500 megawatt capacity.

Cybersecurity Challenge

As a US-based fossil power facility, the plant is subject to North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) version 5 cybersecurity guidelines. To achieve compliance, the company had to disconnect critical operational technology (OT) networks from outside access However, it also needed to retain access to OSIsoft® PI System historian data and OPC client/server data by the business IT unit.

REQUIREMENTS:

1. Clearly define network segments and eliminate all connections to critica
2. OT systems from outside networks according to NERC CIP v5
3. Enable one-way communication from OT network to business IT network
4. Maintain business continuity through PI System historian replication
5. Allow remote monitoring of OPC data via replication to business IT

Case Summary

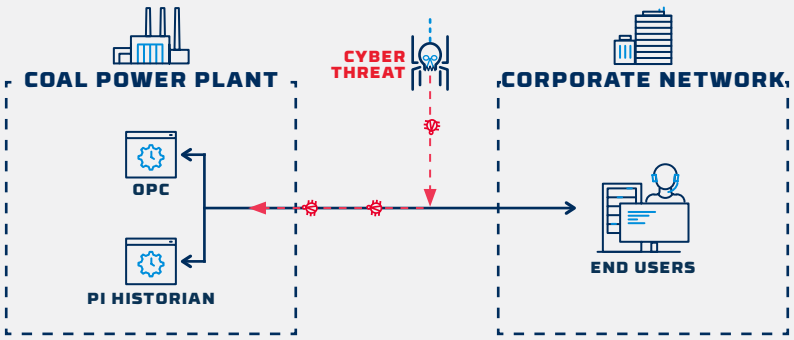
INDUSTRY:
Coal Power Generation

SOLUTION:
OPDS-MP data diodes deployed along with OPTS PI System replication and Owl OPC data replication.

CHALLENGE:
Meet cybersecurity compliance according to NERC CIP v5 without disrupting access to OT data by business end-users.

BENEFITS:
Deterministic, one-way data flow secured OT network from external threats, and enabled transfer of PI System data and OPC monitoring data to corporate network.

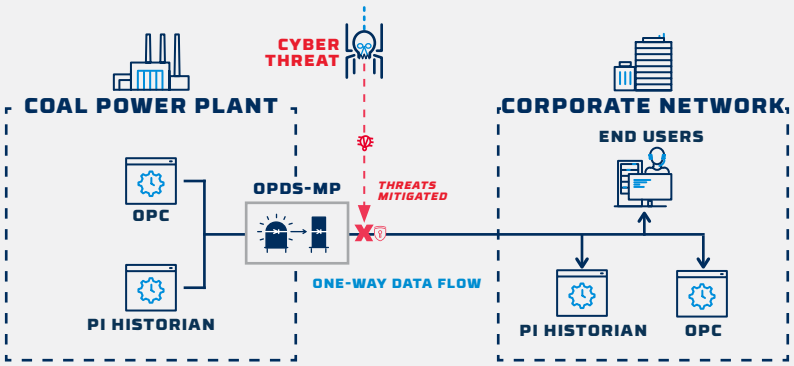
USE CASE (BEFORE)



SOLUTION

OPDS-MP was selected to prevent remote access to the OT network and provide deterministic, one-way data transfer out of OT network. Added PI System replication (OPTS) and OPC data replication for remote plant monitoring and data access by business endusers unit.

USE CASE (AFTER)



DEPLOYMENT

OPDS-MP

Owl Perimeter Defense Solution - Multi Purpose

Self-contained 1U data diode, purpose-built for network segmentation and deterministic, one-way data transfer.

INTERFACE MODULE

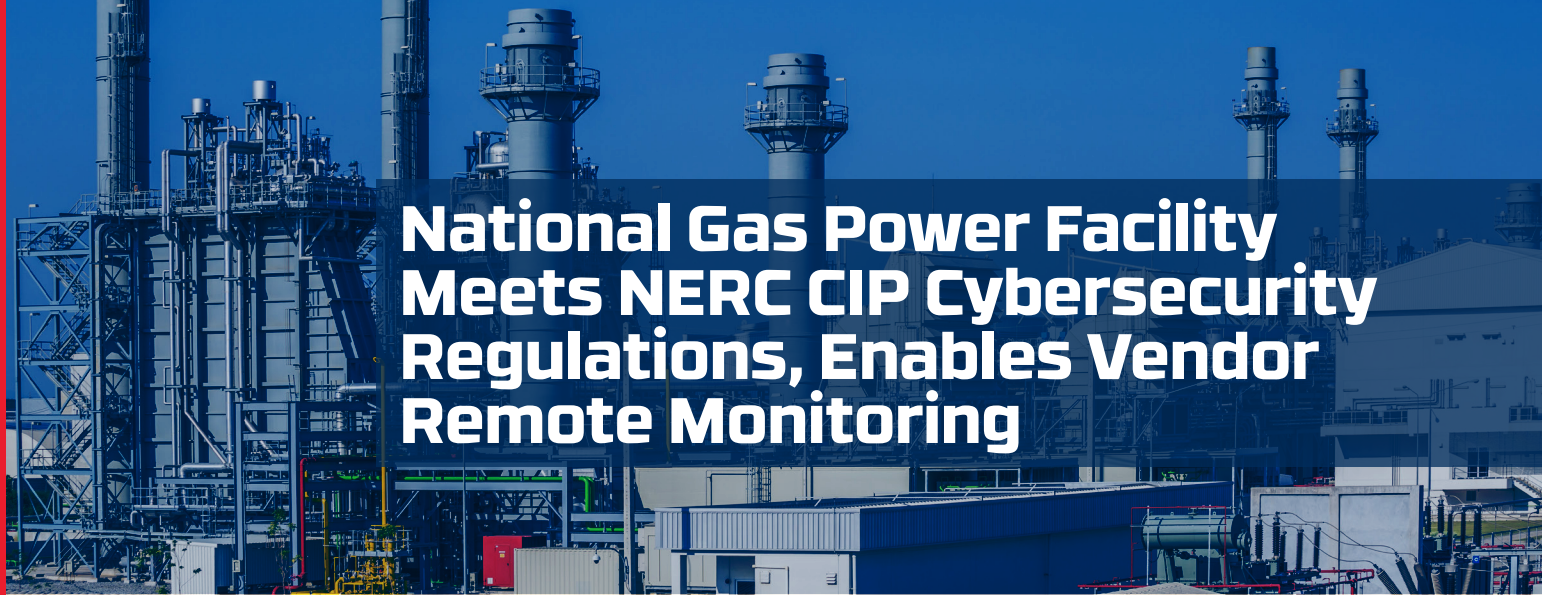
Owl PI Transfer Service (OPTS)

Specialized software developed specifically for secure replication and transfer of OSIsoft® PI System historian data across network boundaries.

RESULTS

1. Achieved compliance with NERC CIP v5 regulations for US coal power facility cybersecurity
2. Data diodes installed to reduce risk per NERC CIP v5 guidelines, eliminating all inbound connections/ threats to OT networks while providing deterministic, one-way outbound data flow
3. Enabled PI System historian and OPC monitoring data replication to IT network, allowing business unit staff to “get their jobs done”

USE CASE: GAS POWER



National Gas Power Facility Meets NERC CIP Cybersecurity Regulations, Enables Vendor Remote Monitoring

Company Overview

A US-based nuclear power plant with over 1,000 megawatt generating capacity.

Cybersecurity Challenge

The power facility is subject to North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) version 5 cybersecurity guidelines. To achieve compliance, the company had to disconnect critical operational technology (OT) networks from external access, including their turbine vendor However, according to their service level agreement (SLA), the vendor needed to access turbine monitoring data from the plant.

REQUIREMENTS:

1. Clearly define network segments and eliminate all connections to critical OT systems from outside networks according to NERC CIP v5
2. Enable one-way communication from OT network to external end-users
3. Provide operations data to turbine vendor's global monitoring center to meet SLA

Case Summary

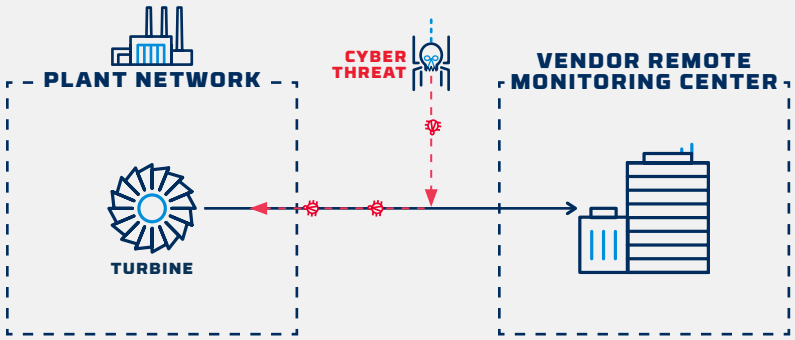
INDUSTRY:
National Gas Power Generation

SOLUTION:
Owl OPDS-100 data diodes with DataDiode Technology deployed to transfer turbine operations information to monitoring center.

CHALLENGE:
Meet cybersecurity compliance with NERC CIP v5, and maintain turbine vendor access to OT monitoring data to meet SLA.

BENEFITS:
Deterministic, one-way data diode secured plant from external threats and allowed vendor to receive turbine data at remote monitoring center.

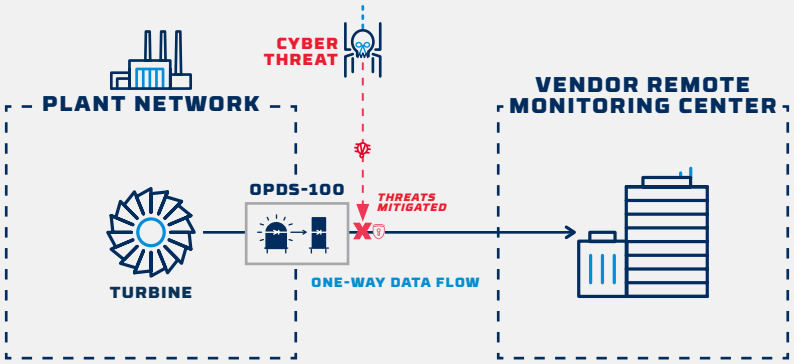
USE CASE (BEFORE)



SOLUTION

OPDS-100 was selected to remove remote access to the OT network and provide deterministic, one-way outbound data flow. This helped the plant to achieve NERC CIP v5 compliance, and enabled the transfer of turbine data to the vendor global monitoring center.

USE CASE (AFTER)



DEPLOYMENT

OPDS-100

Owl Perimeter Defense Solution - 100

Self-contained 1U data diode, purpose-built for network segmentation and deterministic, one-way data transfer.

RESULTS

1. Achieved compliance with NERC CIP v5 regulations for US natural gas power facility cybersecurity
2. Data diodes installed to reduce risk per NERC CIP v5 guidelines, eliminating all inbound connections/ threats to OT networks while providing deterministic outbound data flow
3. Met SLA through one-way transfer of turbine operations data to vendor global monitoring center

Public Power Authority Meets NRC, NERC CIP Cybersecurity Regulations Across 10 Plans

Company Overview

A US-based, federally-owned regional power authority serving over 150 municipalities, with a fleet of nuclear, fossil and hydro power plants.

Cybersecurity Challenge

An audit by the US General Accounting Office (GAO), revealed a number of cybersecurity vulnerabilities. With nuclear, fossil and hydro plants in their fleet, the power authority is also subject to both the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) and Nuclear Regulatory Commission (NRC) cybersecurity guidelines. The authority had to remediate identified cybersecurity vulnerabilities and meet regulatory compliance while maintaining business continuity.

REQUIREMENTS:

1. Clearly define network segments and eliminate all connections to critical OT systems from outside networks according to NERC CIP v5 and NRC Regulatory Guide 5.71.
2. Enable one-way data flow from OT network to business IT network
3. Replicate local PI System historians, from across the fleet, to a centralized PI System historian at HQ for access by business group

Case Summary

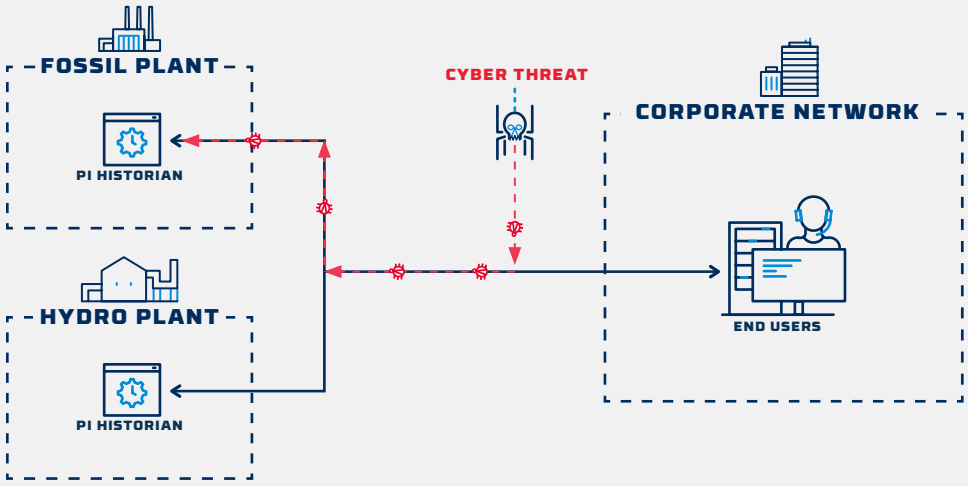
INDUSTRY:
One of the top 10 public power suppliers in the US

SOLUTION:
Owl EPDS data diodes along with OPTS PI System replication application.

CHALLENGE:
Remediate cybersecurity vulnerabilities and meet compliance with NERC CIP v5 and NRC security guidelines.

BENEFITS:
One-way data flow secured OT network from external threats, and achieved compliance with NERC CIP v5 and NRC guidelines. Maintained business continuity through replicated PI System historian at HQ.

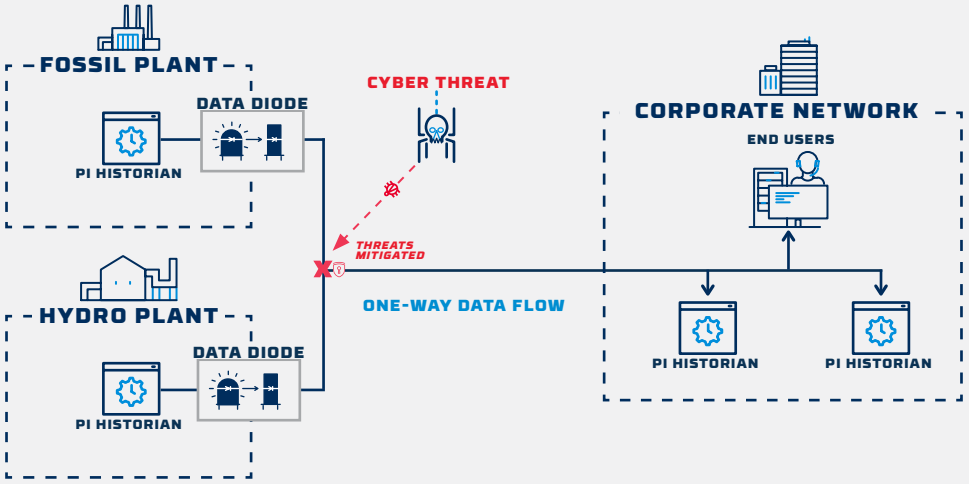
USE CASE (BEFORE)



SOLUTION

Owl data diodes (EPDS) were selected to meet specific risk-based criteria of NERC CIP v5 and NRC Regulatory Guide 5.71 regulations. Data diodes removed external access to OT network and enabled deterministic, one-way data flow to HQ. OPTS PI System data replication software deployed to transfer fleet-wide historian monitoring data and operation management reports to HQ.

USE CASE (AFTER)



DEPLOYMENT

EPDS

Enterprise Perimeter Defense Solution

Data diode communication card pair, mounted on independent, send-only and receive-only commercial servers, for network segmentation and deterministic, one-way data transfer.

INTERFACE MODULE

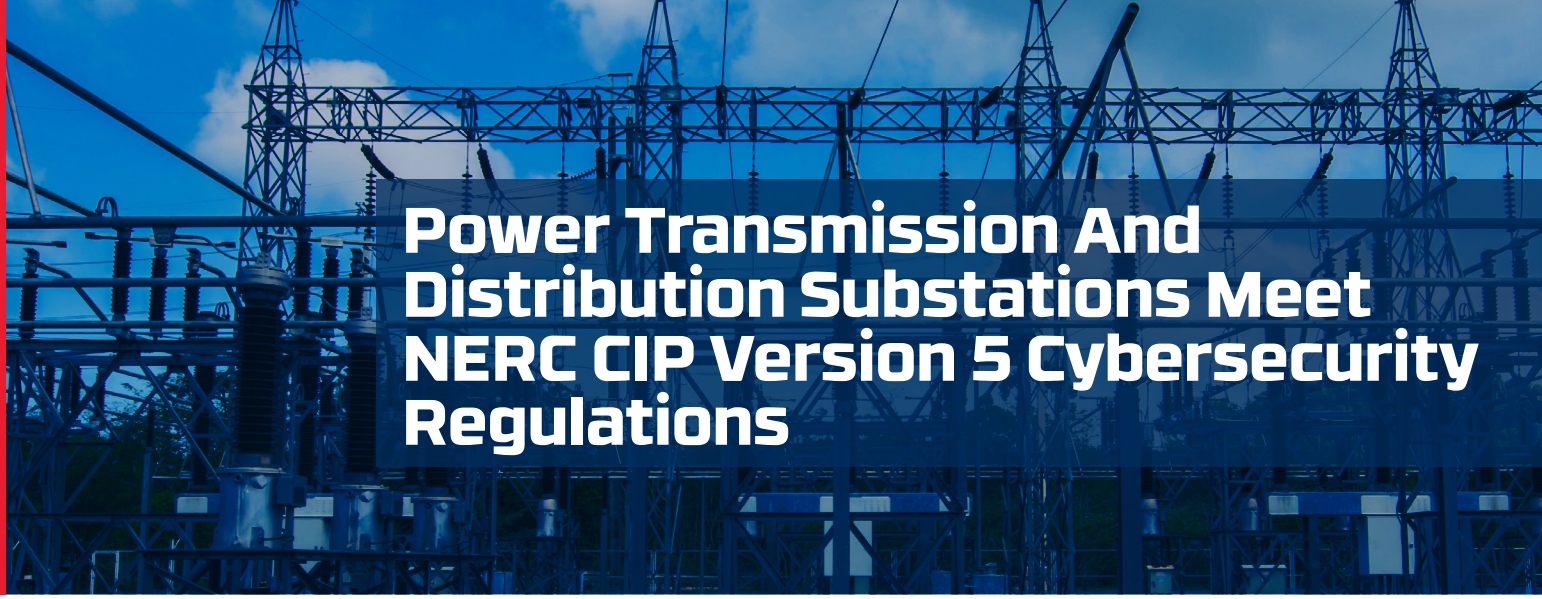
Owl PI Transfer Service (OPTS)

Specialized software developed specifically for secure replication and transfer of OSIsoft® PI System historian data across network boundaries.

RESULTS

1. Met defense-in-depth cybersecurity requirements according to GAO guidance, NERC CIP v5, and NRC Regulatory Guide for US power facilities
2. Data diodes installed, eliminating all inbound connections/threats to OT networks while providing deterministic outbound data flow
3. Maintained business continuity through replicated fleetwide PI System historian data from OT networks to HQ IT network

USE CASE: T&D SUBSTATIONS



Power Transmission And Distribution Substations Meet NERC CIP Version 5 Cybersecurity Regulations

Company Overview

Bulk electric system (BES) operator with many disparate power transmission and distribution (T&D) substations located across the United States.

Cybersecurity Challenge

T&D substations subject to North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) version 5 cybersecurity guidelines are required to mitigate network threats to the BES. To achieve compliance, the company had to disconnect substation operational technology (OT) networks from external access. However, the business end-users needed to retain access to OSIsoft PI System historian data and OPC data generated within the substation OT network.

REQUIREMENTS:

1. Clearly define network segments and eliminate all connections to critical
2. OT systems from external networks according to NERCCIP v5
3. Enable one-way data transfer from OT network to business IT network
4. Replicate and transfer PI System historian data to IT network for business continuity
5. Allow OPC client/server remote data monitoring

Case Summary

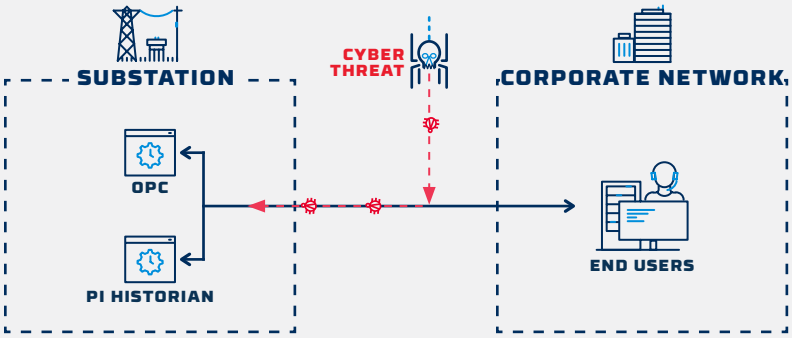
INDUSTRY:
Power T&D Substations

SOLUTION:
OPDS-100D data diodes deployed PI System data replication and Owl OPC data replication software.

CHALLENGE:
Meet cybersecurity compliance according to NERC CIP v5 without disrupting access to OT data by business end-users

BENEFITS:
Achieved NERC CIP compliance via deterministic, one-way data transfer, and enabled remote access to PI System and OPC monitoring data by business end users.

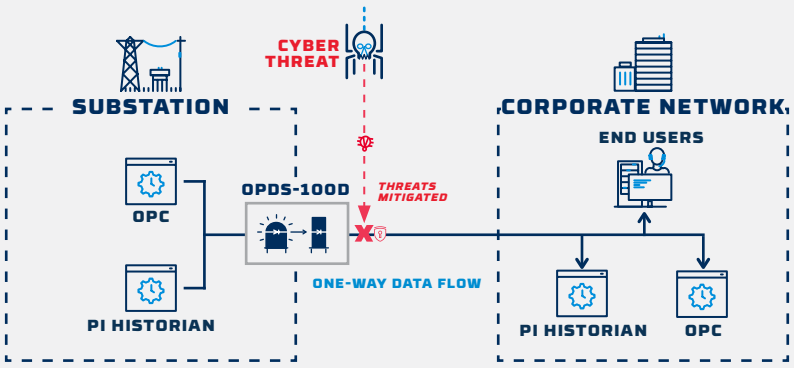
USE CASE (BEFORE)



SOLUTION

OPDS-100D was selected to eliminate external access to the OT network and provide effective network segmentation, and deterministic, one-way data transfer out of OT network. Owl applications for OSIsoft® PI System replication (OPTS) and OPC client/server replication were also deployed for remote substation monitoring and data access by corporate end users.

USE CASE (AFTER)



DEPLOYMENT

OPDS-100D

Owl Perimeter Defense Solution - 100D

DIN rail compatible data diode solution for deterministic, one-way data transfer and effective network segmentation. Supports a wide range of data formats and transport layer protocols at up to 5 Mbps.

INTERFACE MODULE

Owl PI Transfer Service (OPTS)

Specialized software developed specifically for secure replication and transfer of OSIsoft® PI System historian data across network boundaries.

RESULTS

1. Achieved compliance with NERC CIP v5 regulations for US power T&D cybersecurity
2. Data diodes installed to reduce risk per NERC CIP v5 guidelines, eliminating all inbound connections/ threats to OT networks while providing deterministic outbound data flow
3. Enabled PI System historian and OPC monitoring data replication to IT network, maintaining business continuity and operational insight

USE CASE: BANKING ATM

National Bank Secures ATM Data Collection Via Email At Central Repository Database

Company Overview

A national bank with ATMs located across many disparate locations.

Cybersecurity Challenge

Transaction and security data from many disparate ATMs is sent back, via email, to the bank's central repository database for use and analysis. However, after a security review, the bank determined that software firewalls were no longer sufficient to protect its central repository database from external cyber threats. The bank required increased network cybersecurity but also the ability to continue collecting data from its ATMs into the central repository.

REQUIREMENTS:

1. A secure network perimeter device which would permit only whitelisted and trusted emails and files to flow into the data repository
2. Remove outside connections from the repository, so that no data can be externally accessed or extracted

Case Summary

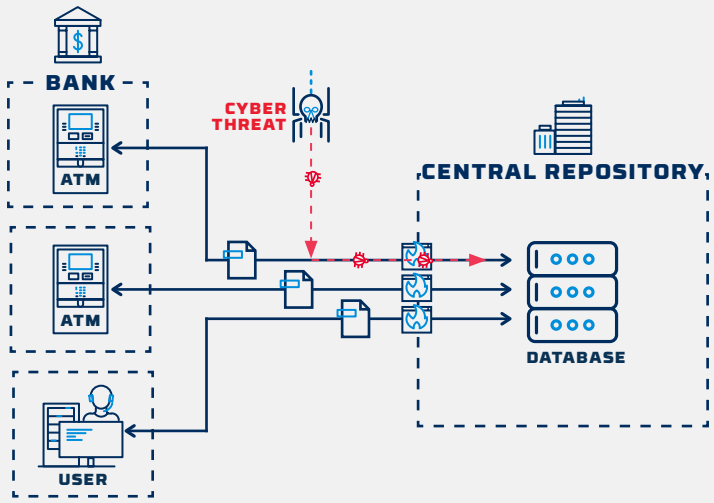
INDUSTRY:
Banking

SOLUTION:
OPDS-MP data diodes deployed in conjunction with existing firewall solution.

CHALLENGE:
Isolate and secure central data repository while preserving the collection of trusted files from ATMs in the field via email.

BENEFITS:
Deterministic, one-way data flow secured OT network from outside influence or attack and enabled PI System replication to corporate end users.

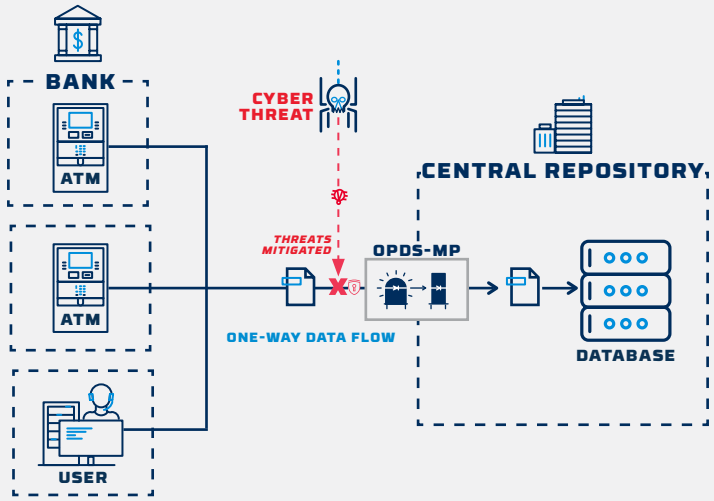
USE CASE (BEFORE)



SOLUTION

OPDS-MP was selected to eliminate remote data repository access and enable deterministic, one-way data transfer of ATM security and transaction data into the database via email. Working in conjunction with the pre existing firewall, the data diodes allow only whitelisted and trusted files into the data repository.

USE CASE (AFTER)



DEPLOYMENT

OPDS-MP

Owl Perimeter Defense Solution - Multi Purpose

Self-contained 1U data diode, purpose-built for network segmentation and deterministic, one-way data transfer.

RESULTS

1. Secure, hardware-enforced boundary created between the ATM network and the central data repository
2. Data diodes eliminated all outbound connections from data repository while providing inbound flow of trusted ATM data via email
3. Data cannot be exfiltrated from data repository through any outside network connection
4. Business continuity maintained through highly controlled, one-way data flow into data repository

Regional US Bank Enables Network Monitoring

Company Overview

A regional US bank with over 150 branch locations, 100,000 customers and a high demand transaction environment.

Cybersecurity Challenge

To mitigate cyber threats, the bank isolated their transaction center from all external networks. However, due to the high demand on the system, bank operations needed to be monitored constantly to assure peak performance and downtime as close to zero as possible. The bank required a way to enable on -call IT staff to remotely monitor banking operations 24x7 without opening the transaction center back up to external cyber network threats.

REQUIREMENTS:

1. Preserve “disconnected” architecture of transaction network, with no connections or access from external networks
2. Permit alarm and event notifications to be transferred to on-call IT staff for remote monitoring of transaction center systems

Case Summary

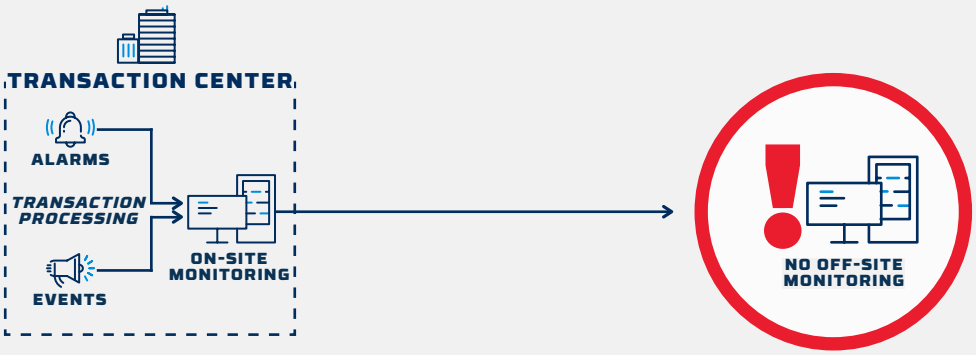
INDUSTRY:
Banking

SOLUTION:
OPDS-100 data diodes capable of transferring email notifications, alarms and files.

CHALLENGE:
Preserve security and isolation of bank operations center while enabling remote monitoring.

BENEFITS:
One-way data flow ensures bank transaction network is secure from external cyber threats. Enabled IT staff to remotely monitor system performance, alarms and events.

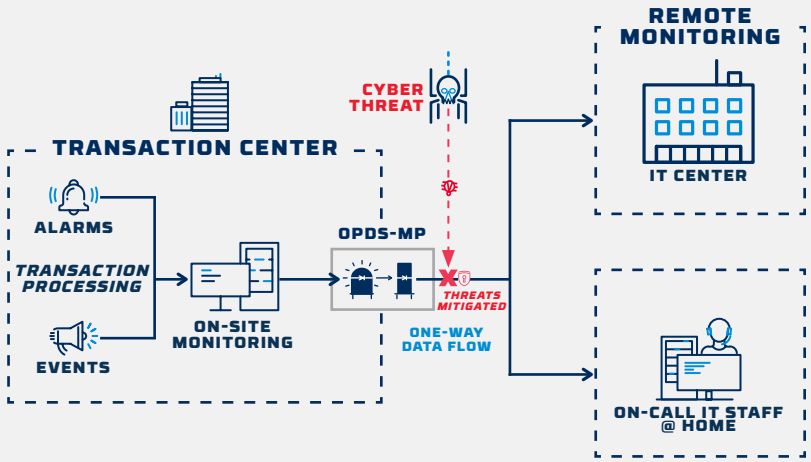
USE CASE (BEFORE)



SOLUTION

OPDS-100 was selected to preserve disconnected nature of the bank transaction network and enable deterministic, one-way data transfer of performance, alarm and event files to IT staff for remote monitoring.

USE CASE (AFTER)



DEPLOYMENT

OPDS-100

Owl Perimeter Defense Solution - 100

Self-contained 1U data diode, purpose-built for network segmentation and deterministic, one-way data transfer.

RESULTS

1. Provided deterministic outbound flow of performance, alarm and event files, including email notifications
2. Enabled IT staff to remotely monitor performance, alarm and event data from transaction center
3. Created secure, hardware-enforced boundary around the bank transaction network to preserve disconnected architecture
4. Bank transaction network cannot be accessed via any external network connection

Mid-Market National Bank Securely Captures and Collects Forensic Data Files

Company Overview

A mid-market national bank with over $500 million in assets and capital.

Cybersecurity Challenge

Capturing and analyzing cyber asset forensic metadata related to exposure of bank cyber assets (laptops, servers, PCs, etc.) to various networks, websites, users, etc. is vital to investigating and ultimately remediating cyber threats. The bank needed a method to capture, package, and copy compromised cyber assets and their associated metadata, then securely transfer them to their forensic lab for analysis. The bank also wanted to ensure that only trusted files were allowed into the lab network, and that no potentially infected data would be allowed out.

REQUIREMENTS:

1. Compatibility with software utility which scans compromised assets and their metadata and packages them into forensic data files
2. Enable a secure method to transfer the forensic data files from the bank network to the forensic lab environment
3. Preserve “disconnected” secure architecture of forensic lab network, keeping it inaccessible from external networks

Case Summary

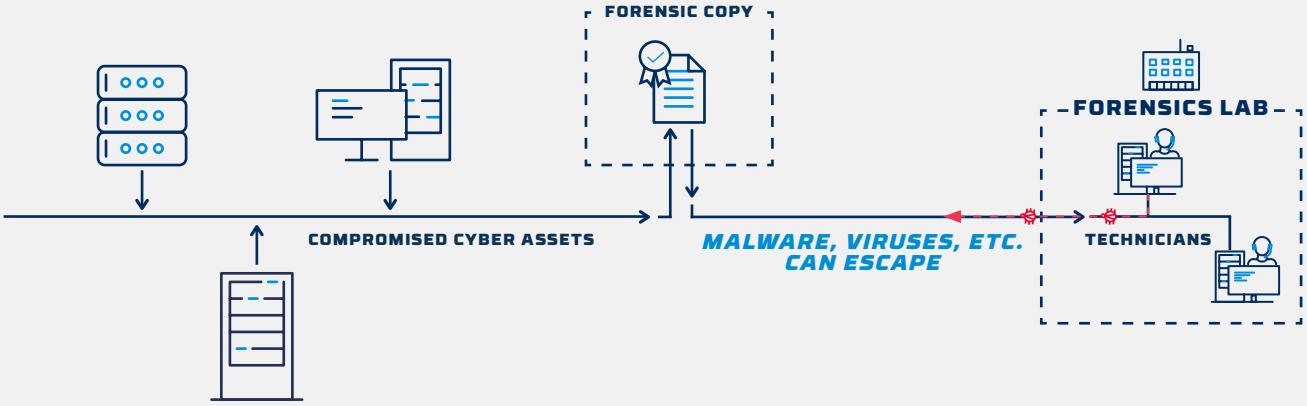
INDUSTRY:
Banking

SOLUTION:
OPDS-1000 data diodes deployed to capture and contain forensic evidence.

CHALLENGE:
Enable transfer of forensic data files to bank’s secured forensic lab network while preserving the isolation of the lab environment.

BENEFITS:
One-way data flow enables file transfer to forensic lab, while ensuring the lab environment remains isolated and secure from external cyber threats.

USE CASE (BEFORE)



SOLUTION

OPDS-1000 was selected to transfer the forensic data files, packaged by a 3rd party software tool, to the secured lab environment. The diodes also preserved the disconnected nature of the forensic lab network, preventing access from external networks.

USE CASE (AFTER)

DEPLOYMENT

OPDS-1000

Owl Perimeter Defense Solution - 1000

Self-contained 1U data diode, purpose-built for network segmentation and deterministic, one-way data transfer up to 1 Gbps.

RESULTS

1. Provided deterministic, one-way transfer of packaged forensic data files from bank network to secured forensic lab
2. Preserved disconnected architecture of lab network with secure, hardware-enforced boundary
3. Bank forensic lab network cannot be accessed via any external network connection and potential evidence cannot be tampered with
4. Potentially harmful cyber infections cannot escape the forensic lab

Regional US Bank Secures Offsite Backup of Transactions and Customer Records

Company Overview

A midsize regional US bank with over 40 branch locations.

Cybersecurity Challenge

The bank required timely and secure backups of their systems to ensure business continuity. However, the security of software firewalls used to protect the bank's network connections became a significant concern. The remote backup sites located in the cloud and on 3rd party networks exposed the network to far too much risk. The bank needed a more secure way to allow backup files to be sent offsite without creating a possible threat vector into the bank.

REQUIREMENTS:

1. Remove outside connections into the bank operations network, so that the bank cannot be breached by external cyber threats
2. Permit regular scheduled backups to be sent securely from the bank operations network to remote storage sites

Case Summary

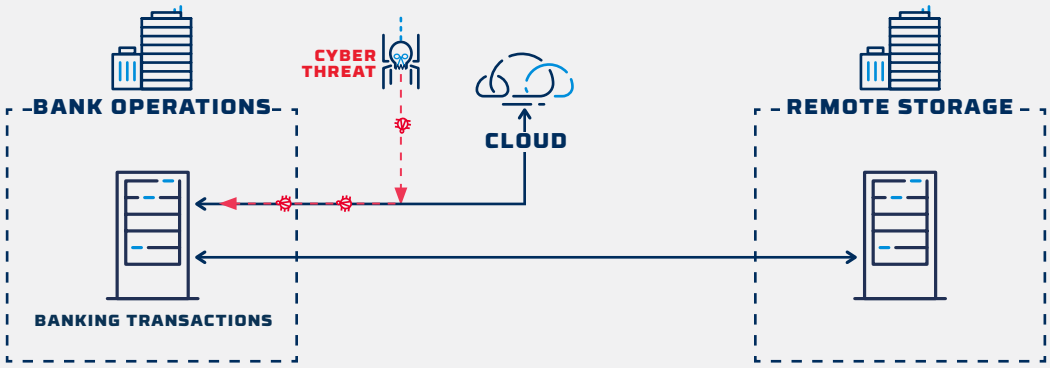
INDUSTRY:
Banking

SOLUTION:
OPDS-100 data diodes deployed in conjunction with existing software firewall.

CHALLENGE:
Ensure security of bank operations networks and enable regular data backup to offsite storage.

BENEFITS:
One-way data flow ensures bank operations network is secure from external cyber threats. Data diodes allow one-way transfer of trusted files to offsite backup.

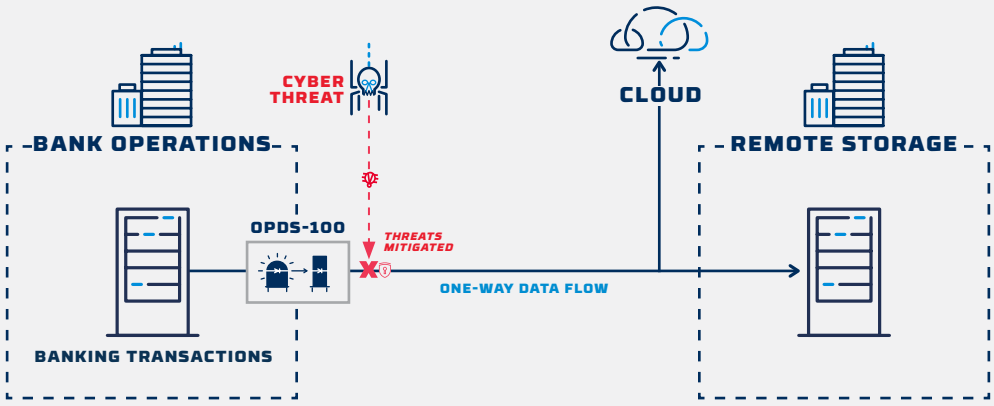
USE CASE (BEFORE)



SOLUTION

OPDS-100 was selected to eliminate remote access to the bank operations network and enable deterministic, one-way data transfer of transaction and customer data to remote backup.

USE CASE (AFTER)



DEPLOYMENT

OPDS-100

Owl Perimeter Defense Solution - 100

Self-contained 1U data diode, purpose-built for network segmentation and deterministic, one-way data transfer.

RESULTS

1. Secure, hardware-enforced boundary created around the bank operations network
2. Data diodes eliminated all inbound connections to bank operations while providing deterministic outbound flow of trusted backup data
3. Bank operations network cannot be accessed through any outside network connection
4. Business continuity maintained through highly controlled one-way data flow to offsite backup

USE CASE: RAIL TRANSPORTION

National Commuter Rail Transportation Company Secures Remote Monitoring of Railcars and Track

Company Overview

A national commuter rail transportation company operating over 15,000 trains daily.

Cybersecurity Challenge

To collect both performance and safety metrics, the rail company installed sensors on its railcars and tracks. The sensors allow remote monitoring from a centralized facility, but they also created the potential for cyber threats. Recognizing a need for cybersecurity, the company required a solution that could both isolate the sensor monitoring and data aggregation system from external network access, while allowing sensor data to continue being sent to the central monitoring operations center, via wireless transmission.

REQUIREMENTS:

1. Create a “disconnected” architecture for rail monitoring network, with no incoming connections from external networks
2. Enable secure transfer of rail performance and safety data to central monitoring center via wireless transmission

Case Summary

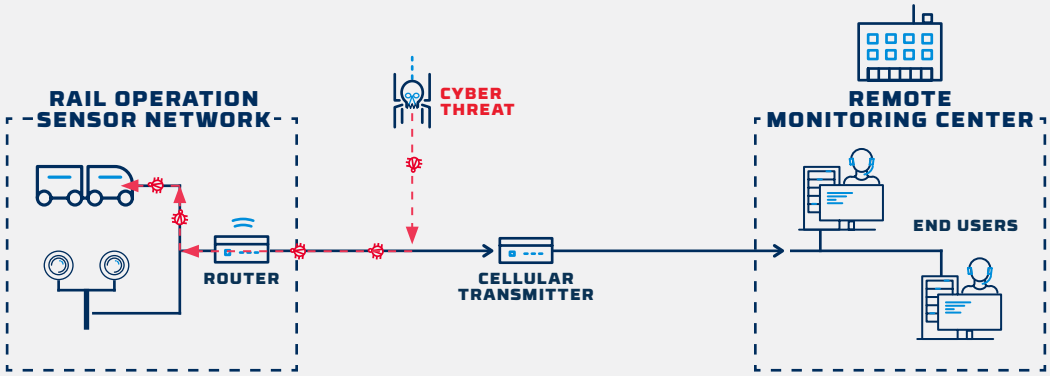
INDUSTRY:
Transportation Rail

SOLUTION:
OPDS-100 data diodes deployed to transfer sensor data.

CHALLENGE:
Isolation and security of rail sensor network while preserving remote monitoring capabilities.

BENEFITS:
One-way data flow ensures rail monitoring network is secure from external cyber threats. Preserved remote monitoring capability from central monitoring operations center.

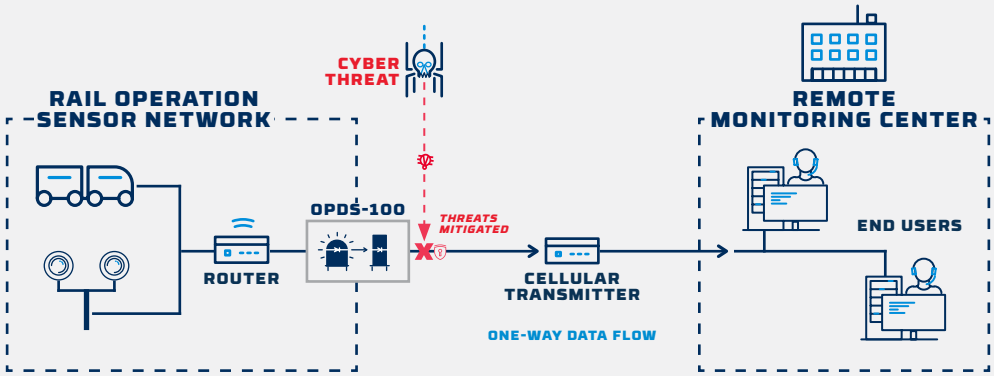
USE CASE (BEFORE)



SOLUTION

OPDS-100 was selected to isolate the rail monitoring and aggregation network from external access. Data diodes also enabled deterministic, one-way data transfer of performance and safety sensor data for transmission to remote monitoring operations center.

USE CASE (AFTER)



DEPLOYMENT

OPDS-100

Owl Perimeter Defense Solution - 100

Self-contained 1U data diode, purpose-built for network segmentation and deterministic, one-way data transfer.

RESULTS

1. Created secure, hardware-enforced boundary around the rail monitoring network
2. Rail sensor and monitoring network cannot be accessed via any external network connection
3. Enabled deterministic outbound flow of performance and safety sensor data to monitoring center via wireless transmission system
4. Preserved remote monitoring of rail and track sensor data from central monitoring operations center

Healthcare System Secures Research Database of Electronic Medical Records

Company Overview

A university healthcare system featuring 4 hospitals with over 500 beds, and involved in more than 1,000 medical research projects.

Cybersecurity Challenge

The healthcare system maintains a database of hundreds of thousands of electronic medical records (EMR) containing Protected Health Information (PHI). To access EMR, hospital personnel use healthcare management software which restricts them to only the patient they are treating. However, university researchers could bypass these software system safeguards and had full access to the EMR database, beyond what was authorized for research – a HIPAA violation. The organization required a controlled way to allow access to authorized EMR for research, in a manner compliant with HIPAA regulations.

REQUIREMENTS:

1. Create a new isolated and controlled network where researchers can view selected patient records in compliance with HIPAA
2. Preserve EMR access through the healthcare management software for healthcare workers with access privileges

Case Summary

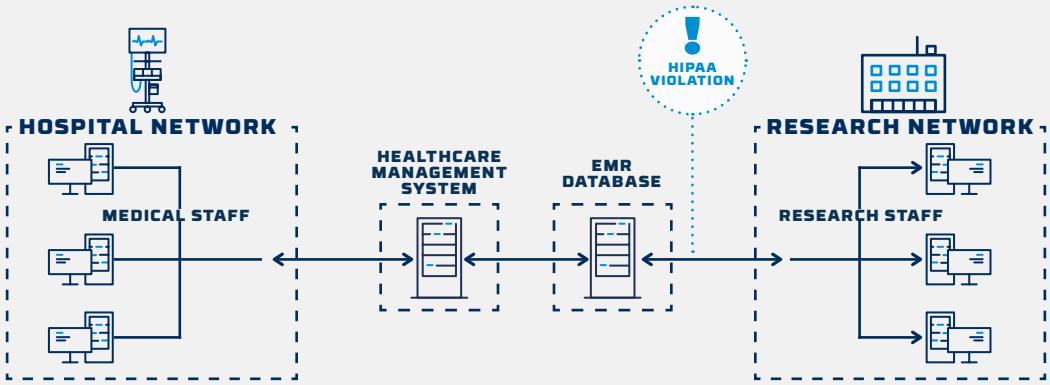
INDUSTRY:
Healthcare

SOLUTION:
OPDS-100 data diodes deployed.

CHALLENGE:
Provide selected EMR for research compliant with HIPAA regulations and isolate the sensitive research network.

BENEFITS:
One-way data flow ensures EMR database network is secure from external cyber threats, while allowing researchers to access authorized PHI.

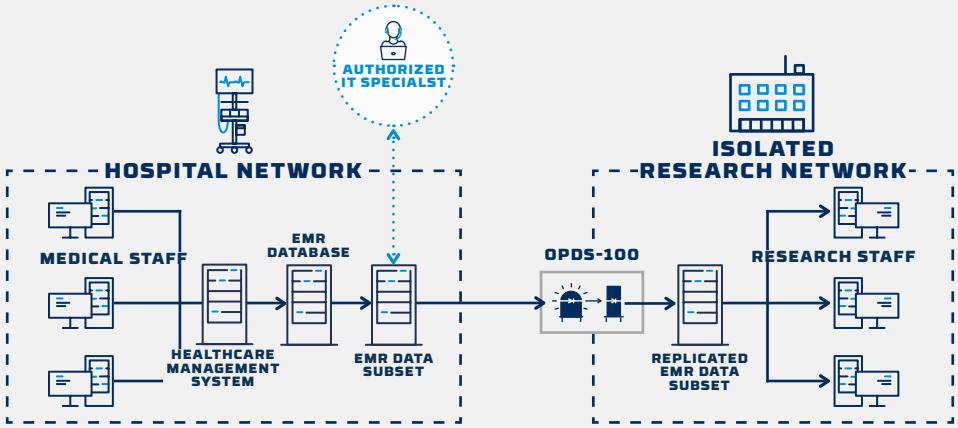
USE CASE (BEFORE)



SOLUTION

OPDS-100 was selected to isolate the EMR research network and create a subset of research PHI data from the full database. Data diodes enabled deterministic, one-way data transfer of EMR data into controlled research database.

USE CASE (AFTER)



DEPLOYMENT

OPDS-100

Owl Perimeter Defense Solution - 100

Self-contained 1U data diode, purpose-built for network segmentation and deterministic, one-way data transfer.

RESULTS

1. Created secure, hardware-enforced boundary around the EMR research network, isolating the researchers from the full EMR database
2. Ensures compliance with HIPAA regulations for EMR & PHI access
3. Allowed research staff to continue analysis on selected approved patient records

USE CASE: NUCLEAR

Secure Remote Monitoring of Video Surveillance and Alarms Enabled at Nuclear Power Facility

Company Overview

A nuclear power plant with over 35,000 megawatt generating capacity.

Cybersecurity Challenge

A nuclear power facility needed to establish and enforce both an electronic and physical security perimeter around the plant. This meant that in addition to preventing external access to the operational technology (OT) network, they also required that all video surveillance and alarm data be available at remote monitoring centers 24/7 for physical security. The company needed a way to keep the operational network secure from external cyber threats while also allowing the surveillance and alarm data to be sent offsite.

REQUIREMENTS:

1. Clearly define network segments and eliminate all connections to critical OT systems from external networks
2. Enable one-way data flow from OT network to corporate-based monitoring centers
3. Transfer video surveillance and alarms data to remote monitoring centers for physical security

Case Summary

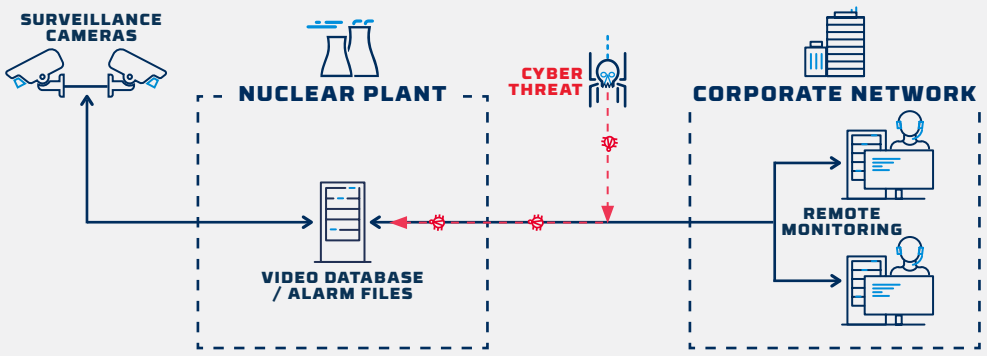
INDUSTRY:
Nuclear Power Generation

SOLUTION:
OPDS-1000 data diodes deployed at OT network perimeter.

CHALLENGE:
Company needed a way to keep the OT secure from external cyber threats while allowing video surveillance and alarm data to be sent offsite.

BENEFITS:
OT network secured from external influence or attack. Video surveillance and alarm monitoring data made available to remote monitoring centers.

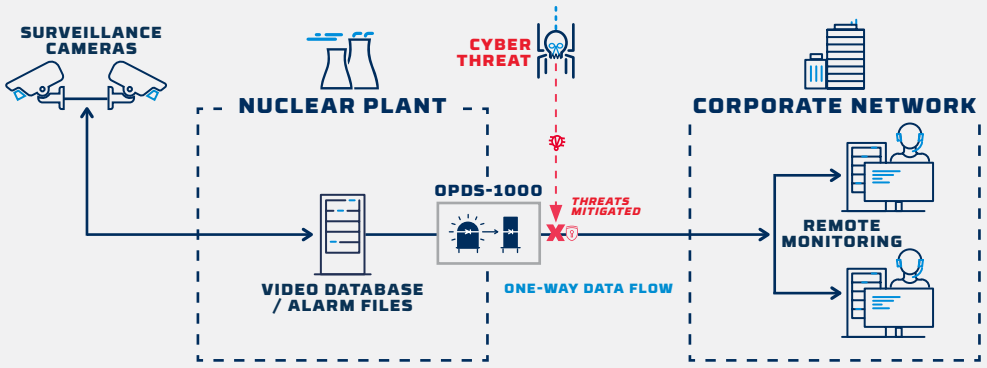
USE CASE (BEFORE)



SOLUTION

OPDS-1000 was selected to prevent remote access to the OT network, provide effective network segmentation, and enable deterministic, one-way data transfer. Video surveillance and alarms data transferred to corporate remote monitoring centers.

USE CASE (AFTER)



DEPLOYMENT

OPDS-1000

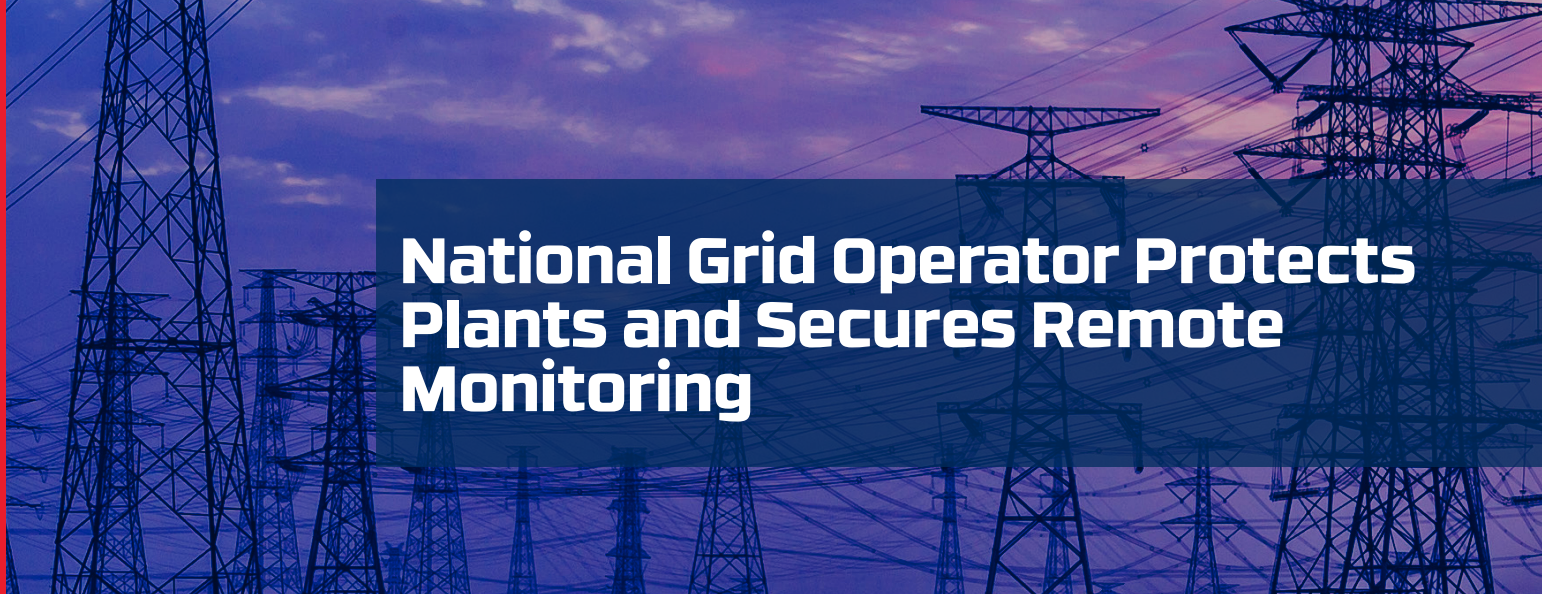
Owl Perimeter Defense Solution - 1000

Self-contained 1U data diode, purpose-built for network segmentation and deterministic, one-way data transfer up to 1 Gbps.

RESULTS

1. Enabled 24/7 remote video surveillance and alarms monitoring to maintain physical security of facility
2. Provided deterministic outbound flow of remote video surveillance and alarms data to corporate IT network
3. Improved cybersecurity, removing all inbound threats to OT networks

USE CASE: NATIONAL GRID



National Grid Operator Protects Plants and Secures Remote Monitoring

Company Overview

A National Grid Operator in South Asia operating a number of regional power generation plants.

Cybersecurity Challenge

The Grid operator needed to securely move SCADA / historian information, files, alarms and other adhoc data requests out of the power generation plants to remote users including the market operator so real-time production decisions and adjustments can be performed. The data needed to be transferred out of the secure plants without opening a threat vector into the plant.

REQUIREMENTS:

1. Provide a secure, one-way transfer of multiple data types from multiple sources over a single device
2. Replicate eDNA servers in each plant to external eDNA servers accessible by market operator
3. Support redundant eDNA servers
4. Ability to transfer multiple data flows (2 from historians, 3 for alarms and 1 for files) and multiple protocols (eDNA replication via TCP/IP, FTP for alarms, RFTS for files) simultaneously
5. Have the ability to expand throughput as future requirements are identified and implemented

Case Summary

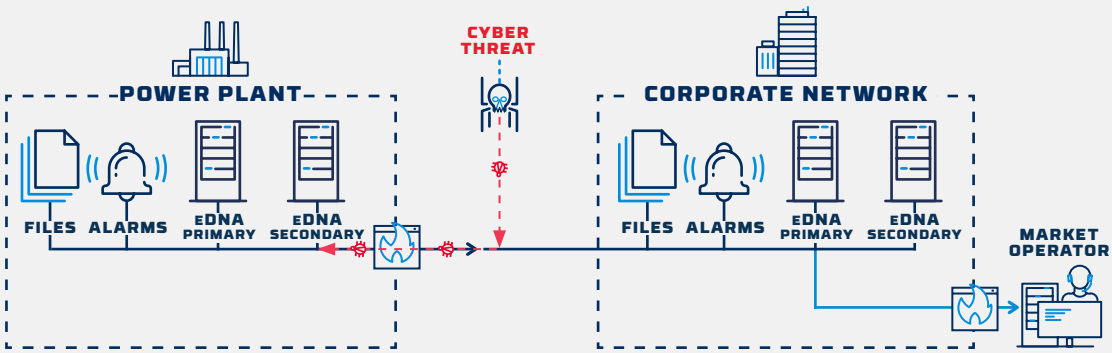
INDUSTRY:
Electric Grid

SOLUTION:
A single OPDS-100 installed at each plant to securely transfer eDNA production data, alarms and adhoc files to end-users outside of the plants.

CHALLENGE:
Maintain secure plants while transferring production data to the Market Operator.

BENEFITS:
Plants are now isolated and secured from network cyberattacks. Single low maintenance device in place with ability for software license upgrades in the future.

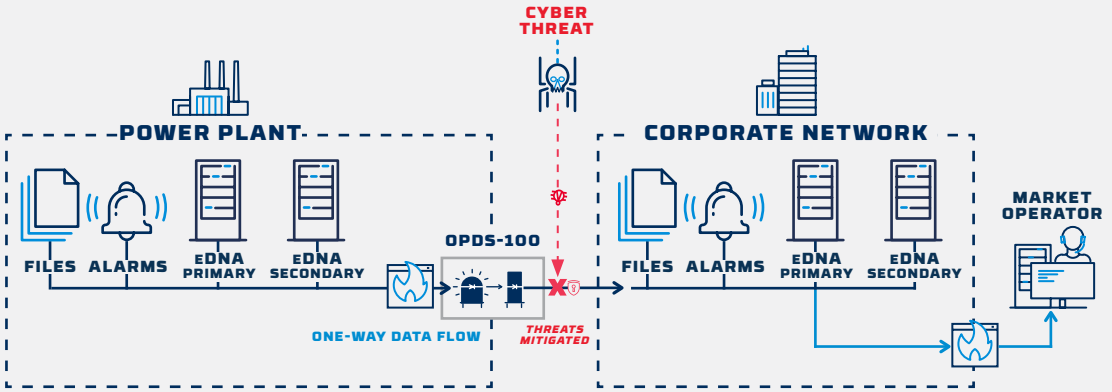
USE CASE (BEFORE)



SOLUTION

The OPDS-100 was selected to protect the plants in three separate regions from network attacks and securely transfer data to end-users. It is a single, low maintenance device with an MTBF of 14+ years. Each device is configured to handle the various data flows, data sources, protocols and replication requirements of the plant with capacity still available to handle future growth and expansion.

USE CASE (AFTER)



DEPLOYMENT

OPDS-100

Owl Perimeter Defense Solution - 100

Self-contained 1U data diode, purpose-built for network segmentation and deterministic, one-way data transfer.

RESULTS

1. Each plant in each region is fitted with a single, one-way only OPDS-100
2. All required traffic flows through the OPDS-100 in near realtime (single digit millisecond latency)
3. A “drop-box” was created for internal plant users to automatically send ad-hoc data requests to external Endusers
4. Redundant eDNA servers at each plant are replicated and accessible by Market Operator
5. All OPDS-100 devices are available for future expansion projects now being designed

Index

The following is a comprehensive list of the sectors, products, software, technologies, and regulation standards bodies from the preceding use cases, including references on where to find them within this document.

SECTORS

TECHNOLOGIES

PRODUCTS

Hardware

Software

REGULATION STANDARDS BODIES

Notes

OWL Cyber Defense

Owl Cyber Defense Solutions, LLC leads the world in data diode and cross domain network cybersecurity. With a constant focus on customers in the military, government, critical infrastructure, and commercial communities, Owl develops market-first, one-way data transfer products to meet a variety of operational needs, from entry level to enterprise.

For more information on Owl, or to schedule a demo, visit www.owlcyberdefense.com

@OwlCyberDefense

203-894-9342 | Info@owlcyberdefense.com

B011 | V5 | 10-30-19