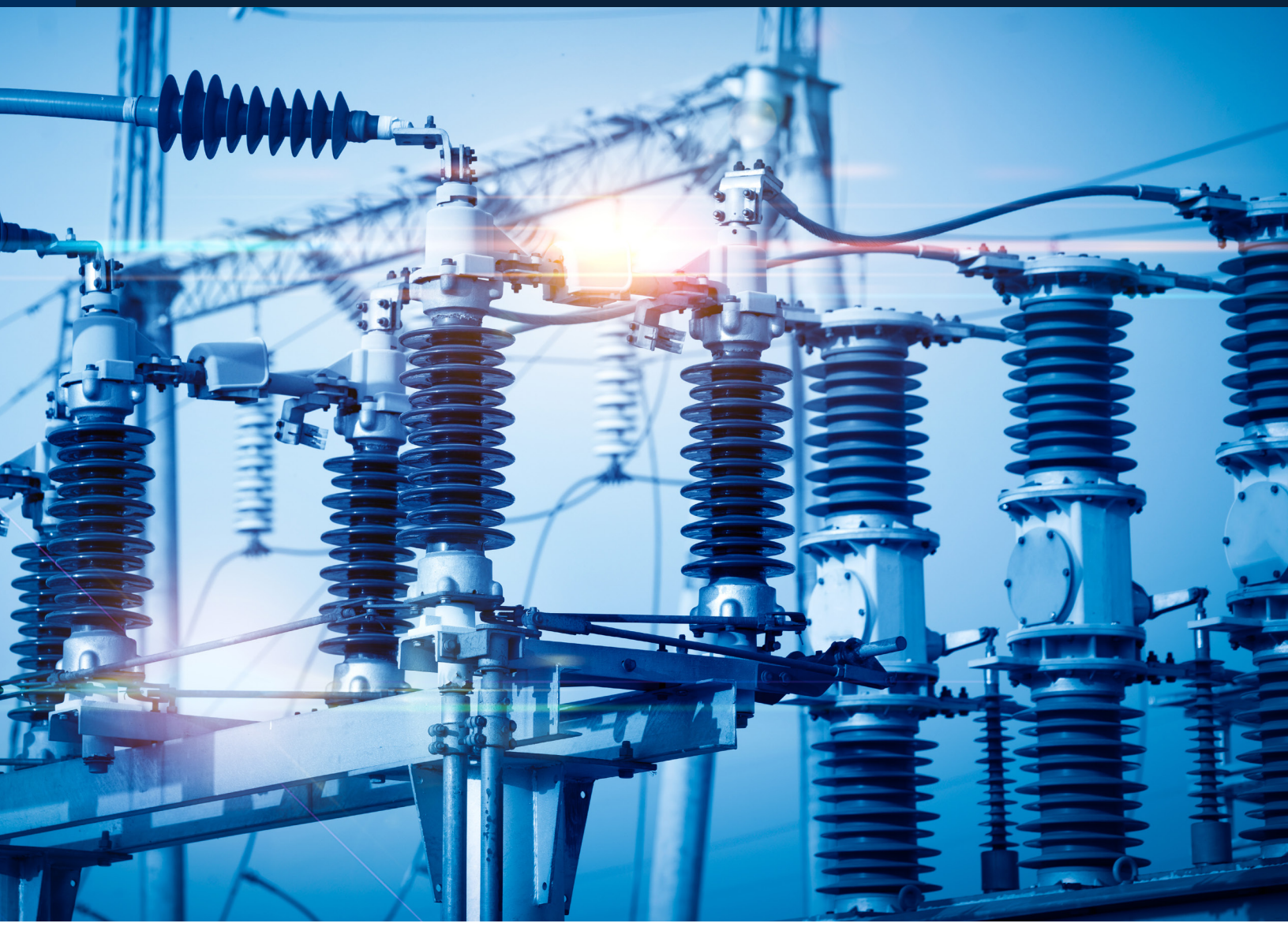
OWL Cyber Defense

WHITE PAPER

Data Diode Cybersecurity
For Power Transmission & Distribution

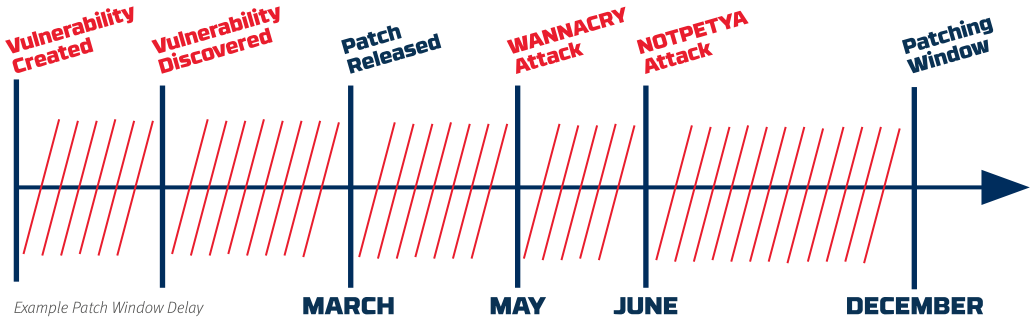


Cyber Threats to the Grid

The power grid and its associated bulk electric systems represent millions of disparate systems connected in networks that range from a single building to thousands of square miles. As a keystone of any country's infrastructure, power grid systems and devices are prime targets for cyber attacks. In the second half of 2017, no sector was targeted more among industrial control system malware attacks[1]. Unfortunately, these systems are also often under-protected. From substations and transmission equipment, to new microgrids and small scale power generation, nearly every facet of the electric grid faces the growing threat of cyberattack from increasingly sophisticated adversaries. From targeted malware to accidental touchpoint breaches, bad actors and their bots are constantly searching for new targets to breach, map, and stage attacks. Any system connected to the internet, either directly or indirectly, is a potential target.

Adding fuel to this fire is the recent release of a number of exploits[2] for major brands of software firewalls, generally the first line of defense for distributed systems, and Windows-based operating systems. Last year, it was discovered that hackers had attempted or successfully infiltrated nearly every major power generation and grid network in the United States.

There are also often critical grid systems and applications that cannot be patched because they are outdated, inaccessible, have no free memory, or more commonly because they work as is, and no one wants to risk an update. That being said, even being "up-to-date" doesn't necessarily mean that all vulnerabilities have been patched. It's possible that no one, outside of a few elite hackers, knows the vulnerabilities exist, so again there is no way to patch.



The timing for protecting these systems could not be more urgent.

[1] *https://www.infosecurity-magazine.com/news/energy-sector-ics-infrastructure*
[2] *https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778*

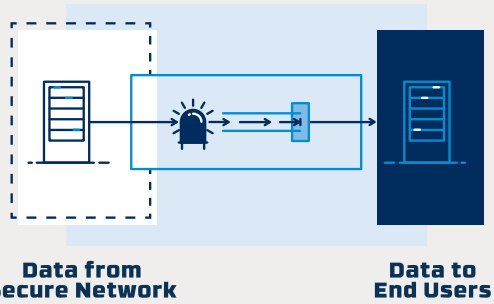
Data Diode Cybersecurity

As cyber-attacks continue to increase and prove that “standard” software-based cybersecurity technologies (firewalls, RBAC, etc.) aren’t enough anymore, organizations are turning to hardware-enforced security solutions, such as data diodes, to provide the only cybersecurity that absolutely cannot be hacked.

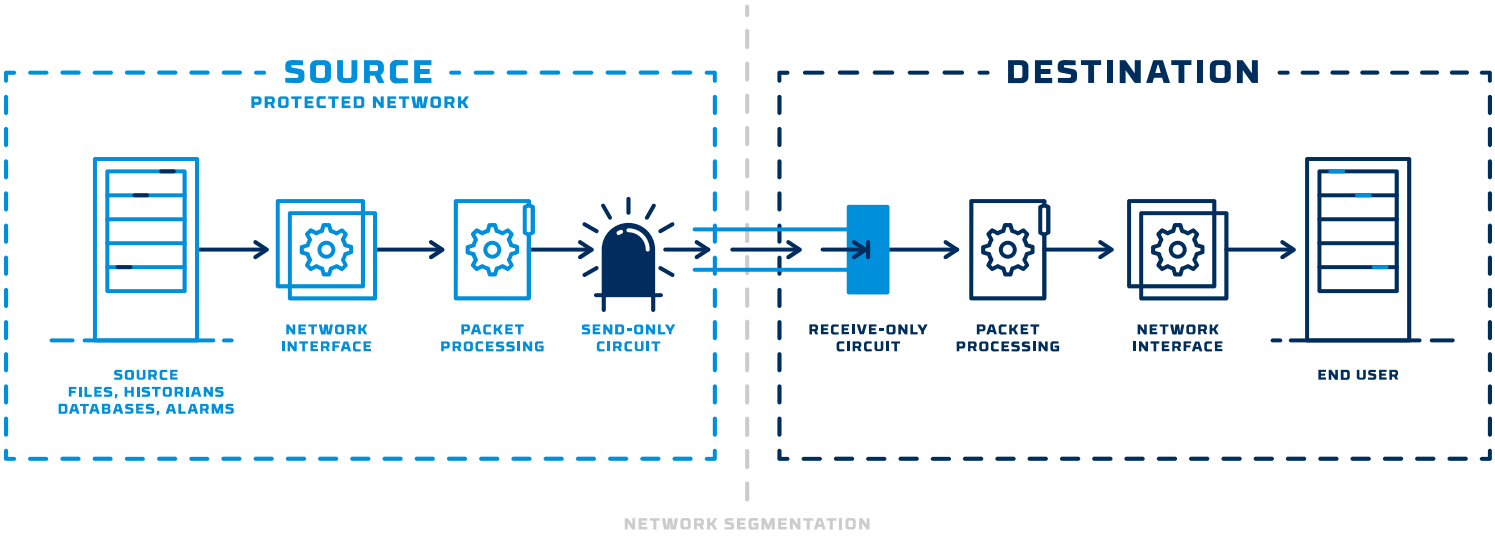
A data diode is a piece of hardware that physically enforces a one-way flow of data. As one-way data transfer systems, data diodes are used as cybersecurity tools to isolate and protect networks from external cyber threats, while still allowing isolated networks to share data with outside users and systems. It is perhaps simplest to think of data diodes as digital one-way valves for data, allowing data to flow out, without a way back in.

One-Way Data Valve

One-Way Data Diode Circuit



The purpose of data diode one-way transfer devices is two-fold: network security through segmentation (separation), often in place of a physical air gap; and data availability (getting the data to the end-users), whether it be via file transfer, or more complex functions such as database replication.



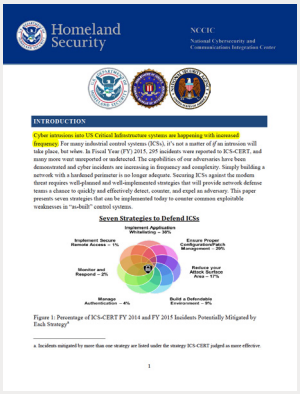
Since the early 1990’s, data diodes have met the elite cybersecurity needs of the most demanding users, including the US DoD and intelligence agencies. Today, Data diodes are used across many critical infrastructure industries, including power grid and power generation operators to achieve compliance with NERC CIP and other regulatory mandates, as well as meeting industry best practices, such as those set forth by the DHS.

Call **203-894-9342** or email **Info@owlcyberdefense.com**

Operating Globally

In the wake of the devastating attacks on the Ukranian power grid[3] in 2015, the U.S. Department of Homeland Security (DHS), in conjunction with the FBI and NSA, released their findings after studying the methods involved, along with a list of seven steps[4] to counter the cybersecurity vulnerabilities that were exploited.

These strategies feature the use of data diodes and include white-listing, reduction of attack surfaces, managing authentication and providing secure remote access. The DHS concluded that these steps are so important and effective, that if system owners had implemented them, 98 percent of the incidents the ICS-CERT responded to over a two year period would have been prevented.


Homeland Security

INTRODUCTION

Seven Strategies to Defend ICSs

Figure 1: Percentage of ICS-CERT FY 2014 and FY 2015 Incidents Potentially Mitigated by Each Strategy[a]

a. Incidents mitigated by more than one strategy are listed under the strategy ICS-CERT judged as more effective.

DHS Seven Steps to Effectively Defend Industrial Control Systems

1. APPLICATION WHITELISTING

Only allow predesignated applications to run and access data.

Owl solutions only accept data from whitelisted data sources, restricted to a unique IP address, port, and protocol. This prevents malware from communicating over the data diode.

2. CONFIGURATION & PATCH MANAGEMENT

Ensure systems are up to date and that a secure method for introducing authenticated software patches is used.

Owl solutions authenticate software patches and updates, then securely transfer them into control centers without using potentially contaminated laptops or portable media.

3. REDUCE ATTACK SURFACE AREA

Isolate control system networks from untrusted networks, lockdown unused services and ports, and use a data diode to provide network segmentation.

Owl solutions provide hardware-enforced network segmentation and support the DHS recommendations for isolating control networks, reducing the attack surface to zero.

4. BUILD A DEFENDABLE ENVIRONMENT

Segment networks and restrict host-to-host paths to prevent the spread of infection.

Owl data diodes are purpose built as the most effective network segmentation devices available.

5. MANAGE AUTHENTICATION

Implement "least privilege", increase password length, change passwords regularly, and require separate credentials for corporate and control network zones.

Owl solutions provide an intrinsic separation of corporate and control network zones, as well as authentication on all transfers, and allow for long passwords requiring regular changes.

6. IMPLEMENT SECURE REMOTE ACCESS

Implement monitoring-only data access enforced by data diodes, remove backdoors, and any persistent remote connections.

Owl data diodes are specifically designed to facilitate secure remote monitoring without enabling remote access or any remote connections.

7. MONITOR & RESPOND

Monitor traffic at and within control system boundaries, perform login analysis, and watch for access control manipulation.

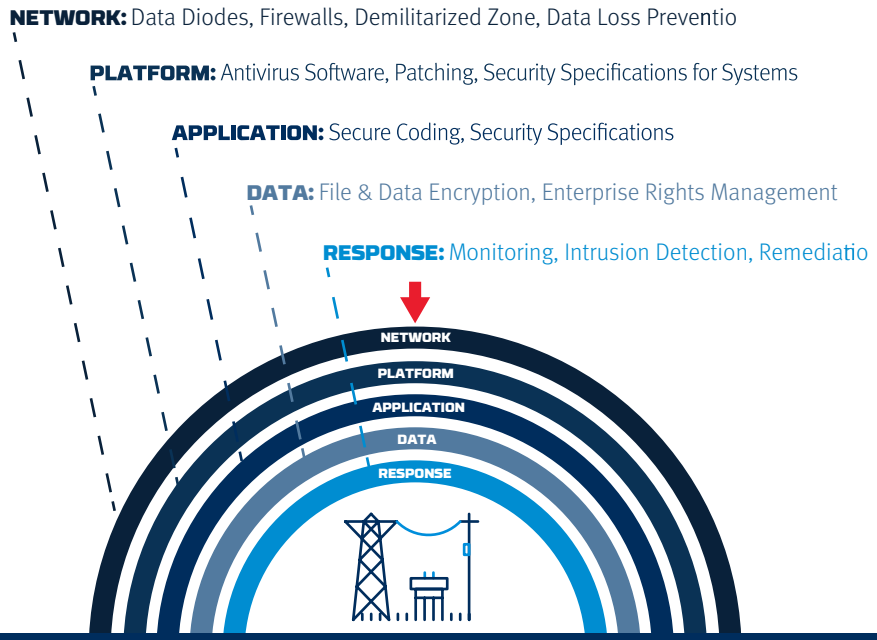
Owl solutions provide real-time monitoring, display & analysis of all connections, and allow offsite auditing of all network activity.

[3] *https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid*
[4] *https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf*

Defense in Depth

It takes layers of security to defend against today's cyberattacks; this layered approach is referred to as "defense-in-depth." A defense in depth approach prevents a cybersecurity architecture from relying on a single strategy or element to defend a network.

Data diodes, a hardware-based network cybersecurity technology designed to protect critical networks while allowing secure, one-way-only data sharing, play an integral part in this layered cybersecurity approach. These multiple layers create a matrix of protection which greatly reduces risk by blocking possible threats across different vectors.



Addressing NERC CIP Compliance with Owl Data Diode Technology

NERC CIP

Virtually all major facilities involved in the North American bulk electric system (BES), including non-nuclear electricity generation, distribution and transmission, are subject to regulation by the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) plan.

The essence of NERC CIP is in identifying and protecting those connected Cyber Assets which, if compromised, would have a negative impact on the BES. Table R1 in Section 005 of CIP lays out out a number of requirements to ensure the protection of the Cyber Assets including: creating a strong Electronic Security Perimeter (ESP), disconnecting BES Cyber Systems from external connections, limiting or eliminating the use of routable protocols (which expose IP information within the ESP, are bi-directional, and are susceptible to hacking), and forcing all traffic through a protected Electronic Access Point (EAP).

Owl has a well-established history of success in helping organizations to meet the cybersecurity requirements of NERC CIP compliance, including v5 & v6. This document includes examples to assist BES operators in finding approved data diode solutions to each of the section 005 requirements.

Changes to NERC CIP

It takes layers of security to defend against today's cyberattacks; this layered approach is referred to as "defense-in-depth." A defense in depth approach prevents a cybersecurity architecture from relying on a single strategy or element to defend a network.

Data diodes, a hardware-based network cybersecurity technology designed to protect critical networks while allowing secure, one-way-only data sharing, play an integral part in this layered cybersecurity approach. These multiple layers create a matrix of protection which greatly reduces risk by blocking possible threats across different vectors.

NERC CIP & Data Diodes

Approved by NERC for the use of network segmentation and one-way data transfer, data diodes combine absolute information assurance and unhackable cybersecurity with the ability to share and monitor operational data. As one-way data transfer systems, data diodes isolate and protect networks from external cyber threats, while allowing systems within these networks to transfer data to other networks in a highly controlled, deterministic manner.

With a non-routable, hardware-based platform, data diodes create an absolute electronic security perimeter by physically only permitting data to transfer in one direction, from one network segment to another, across a network security boundary. When utilized effectively, data diodes can help operators achieve NERC CIP compliance, eliminate all external cyber threats, and provide business continuity through remote monitoring and offsite data analytics.

As the world leader in data diode technology, as well as a strategic technology partner for many industrial automation vendors, Owl is uniquely positioned to provide both the strongest network security available with the broadest range of data transfer services, supported file types, and software integrations on the market. Owl's breadth of supported file types and specialized interfaces, including PI System, Wonderware, OPC, Modbus, and Syslog, among others, enable customers to seamlessly replicate and transfer historians, HMIs, email, and more.

Success Stories

Owl has been providing data diode technology for almost 20 years and for the last 8 years, with hundreds of deployments across North America, Asia, and Europe, Owl has been helping power grid and power generation operators reduce cyber risk, and achieve NERC CIP compliance. Owl's unrivaled expertise in data diode cybersecurity for critical infrastructure reduces time to deployment and increases reliability, from protecting a single device, up to an entire fleet of power stations.

Owl data diodes can relieve up to 40% of the administrative compliance burden of NERC CIP, saving valuable time and money while allowing operators to focus on the vital aspects of their plants and infrastructure. They allow operational data to be sent to other networks or the cloud for analysis, predictive modeling, remote monitoring, and other applications, improving business continuity and ROI in facility technology.

ENVIRONMENTS INCLUDE:

+ Coal, Hydro, Oil, and Natural Gas Power Plants
+ Transmission and Distribution Substations
+ Fuel and Materials Storage Facilities

DATA TYPES TRANSFERRED:

+ Historians & HMIs - PI System, Wonderware, GE Historian, MC Historian, FactoryTalk
+ Modbus, OPC, DCS Data
+ Nearly Any File Type or Streaming Source (TCP, UDP)

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.

INDUSTRY:

Power T&D Substations

CHALLENGE:

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

SOLUTION:

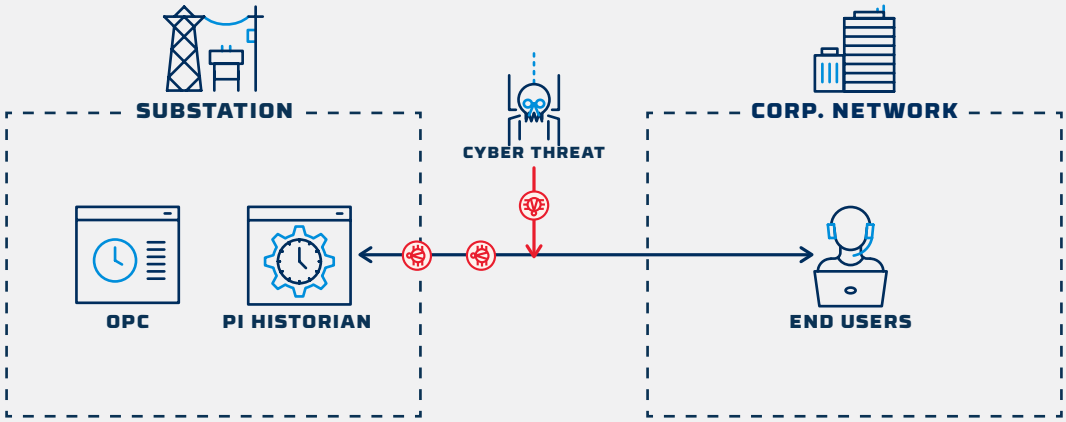
OPDS data diodes deployed, PI System data replication and Owl OPC data replication software.

BENEFITS:

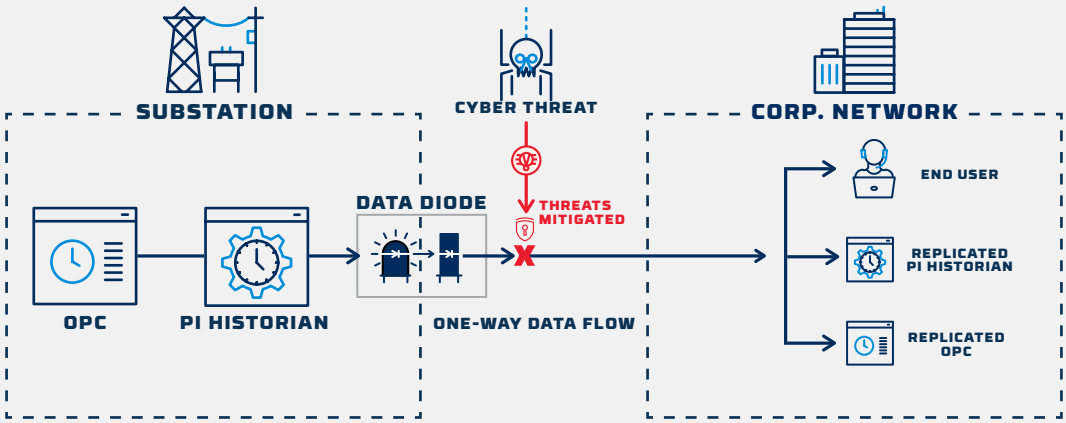
Achieved NERC CIP compliance via deterministic, one-way data transfer, and enabled remote access to PI System and OPC monitoring data by business end users.

Power T&D Substations

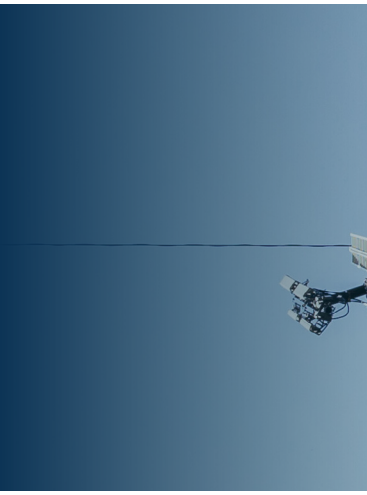
USE CASE (BEFORE)



USE CASE (AFTER)



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

INDUSTRY:

Electric Grid

CHALLENGE:

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

SOLUTION:

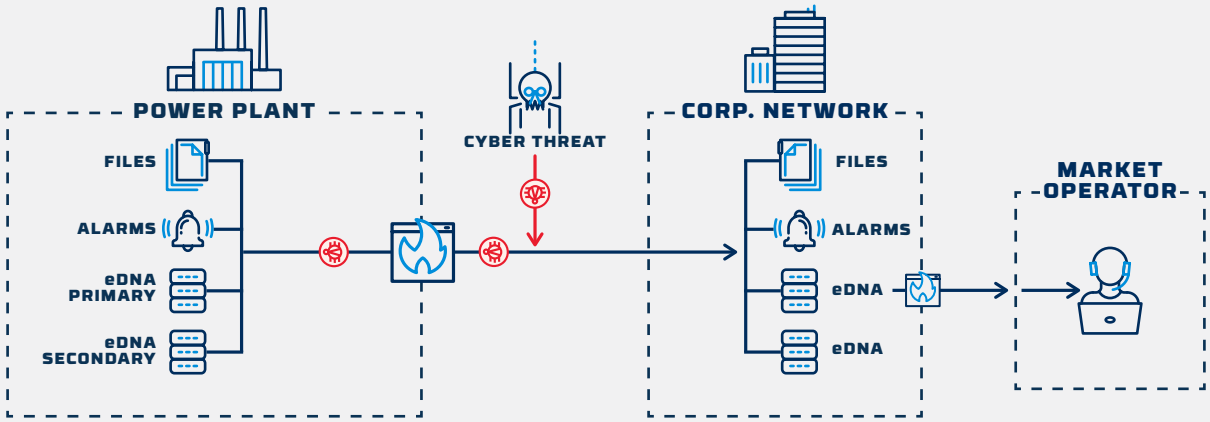
A single OPDS-100 installed at each plant to securely transfer eDNA production data, alarms and adhoc reports to end-users outside of the plants.

BENEFITS:

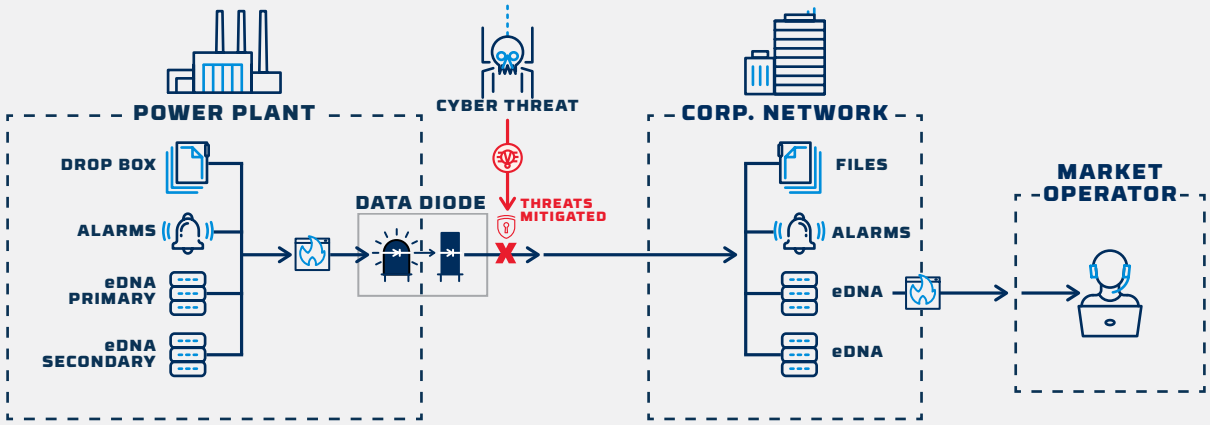
Plants are now isolated and secured from network cyberattacks. Single low maintenance device in place with ability for software license upgrades in the future.

Electric Grid

USE CASE (BEFORE)



USE CASE (AFTER)



Summary

Defending the grid from cyberattack has never been more challenging or necessary than right now. Thankfully, government agencies, the regulatory community, and cybersecurity experts are defining new best practices and documenting numerous use cases for operators to learn from and implement. While they may be the most targeted of any critical infrastructure sector, by utilizing the best tools and practices available, grid operators can greatly reduce their risk of successful intrusions from malware, ransomware, or other hacking attempts.

With years of experience protecting critical infrastructure from cyberattack, including some of the largest and most complex organizations in the world, Owl has a great depth of expertise in the power generation, transmission, and distribution markets.

To learn more, visit www.owlcyberdefense.com to learn how data diode cybersecurity can help protect your connected grid systems.

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