OWL Cyber Defense

Securing OT & IIoT Connections to the Cloud

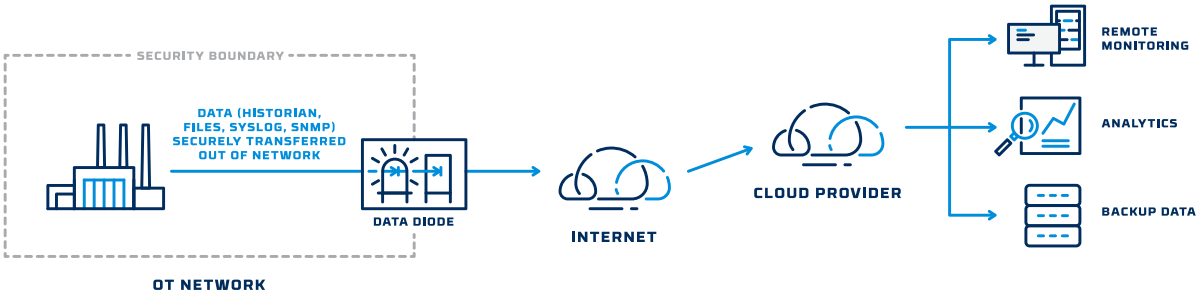
BROCHURE

The convergence of digital OT and IIoT assets with cloud computing can provide numerous benefits to efficiency, productivity, and reliability. Cloud services providers are pushing OT asset owners hard on these benefits with the promise of substantial improvements. However, every additional connected asset also represents a potential access point for bad actors, up to and including nation-state level threats. This is particularly compounded by the use of geographically distributed and sometimes wirelessly connected edge assets in the Industrial Internet of Things (IIoT).

When it comes to OT environments, a single connection from the internet can be considered an unacceptable risk, whether into a manufacturing plant or a bulk electric power system. Firewalls, long a network security mainstay, have been proven ineffective in stopping cyber threats with any level of sophistication and are no longer considered a viable security control. OT asset owners now face the dilemma of potentially opening up their facilities to cyber threats or losing out on the benefits of cloud-enabled analytics, data storage, systems monitoring, and other applications.

A Proven Approach to a Novel Problem

For decades, critical infrastructure and industrial organizations have utilized hardware-enforced data diodes to securely transfer data one-way to external users and systems without opening a potential cyber threat vector. The problem has been developing compatible solutions capable of supporting secure cloud data transfers and synchronization using newer, inherently bidirectional internet and IoT-based protocols.

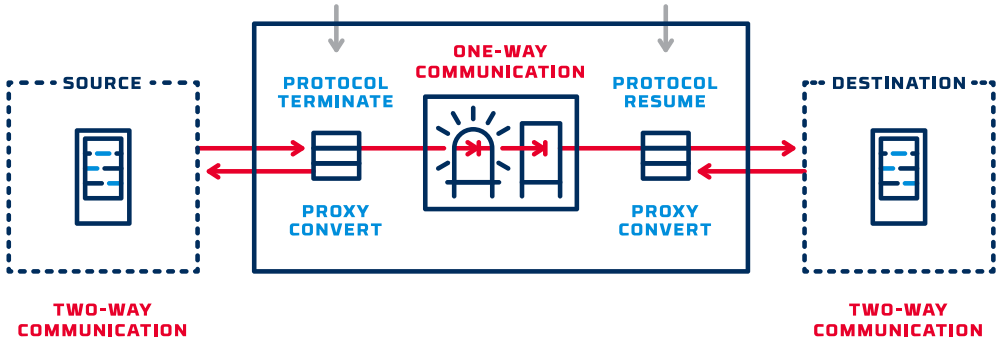


As the world's #1 provider of data diode and cross domain technologies, Owl has developed a suite of cloud-compatible solutions and protocol adapters, including bidirectional internet and IoT-based protocols, such as HTTP/S, MQTT, and AMQP, to connect to a variety of cloud-based platforms and applications, including AWS, MS Azure, Dell APEX, and IBM Cloud.

But wait, how does "bidirectional" work one-way?

While one-way protocols such as UDP lend themselves naturally to the one-way data transfers in data diodes, most protocols, including most in common use for internet- and cloud-related applications, are inherently two-way. Owl data diodes utilize a proxy-based protocol termination to enable one-way transfers of two-way protocols such as TCP/IP.

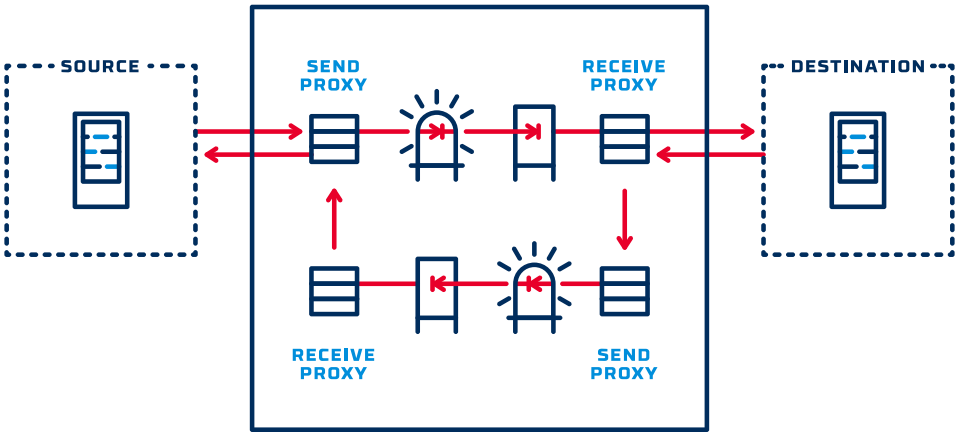
PROXY-BASED UNIDIRECTIONAL CONNECTION



What if it can't be one-way?

Some cloud protocols may require a truly bidirectional solution with a return path. In that case, Owl has designed specially configured cross domain security products which still provide the protocol termination while also providing true bidirectional functionality.

BIDIRECTIONAL CONNECTION



Compatible Platforms & Applications

aws
Azure
APEX
IBM Cloud
splunk>
LogRhythm
Schneider Electric
OSIsoft.
Rockwell Automation

Cloud-Compatible Owl Solutions

OPDS-100D

Compact, DIN rail-compatible data diode solution for hardware-enforced network segmentation and one-way data transfer at up to 104 Mbps.

OPDS-1000

19″ 1U data diode appliance, purpose-built for hardware-enforced network segmentation and deterministic, one-way data transfer at up to 1 Gbps.

EPDS

2U, enterprise-level data diode mounted on independent, send-only and receive only commercial servers, for network segmentation and deterministic, one-way data transfer at up to 10 Gbps.

DATA DIODE

IXD

The world's first and only cross domain solution developed specifically for OT networks and protocols, IXD features 1 Gbps one-way or two-way data transfers with advanced content filtering.

CROSS DOMAIN SOLUTION

Available Protocols

S/FTP	MQTT	IEC104	SNMP
TCP/IP	AMQP	DNP3	SMTP
HTTP/S	OPC	UDP	NTP

Use Cases

While other edge security providers may act as though the cloud is “just another platform” with all the same protocols, data types, and other requirements, Owl has developed new solutions and software specifically to address the unique needs of cloud applications and integrations. Learn more about some of our successful, secure OT to cloud data transfer implementations, from food manufacturing, to energy asset monitoring, to oil & gas IIoT devices.

MAJOR PACKAGED FOODS MANUFACTURER

CYBERSECURITY CHALLENGE

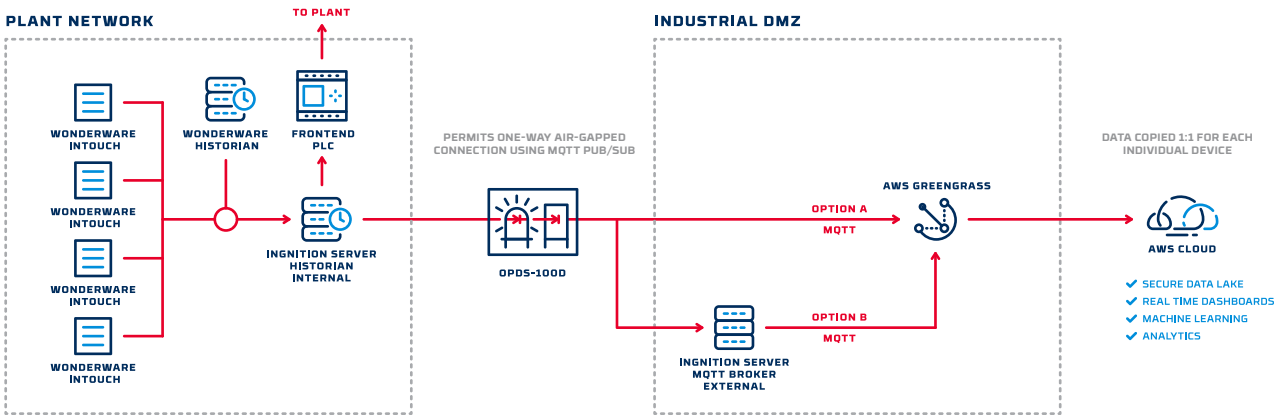
Sending processing plant data to the cloud without creating a network pathway into the plant

SOLUTION

2 x OPDS-100D DIN-Rail Data Diodes – one each for dedicated SFTP and MQTT transfers

BUSINESS BENEFIT

Cloud-based analytics leveraged digital transformation for dramatically improved productivity



INTERNATIONAL ENERGY CONGLOMERATE

CYBERSECURITY CHALLENGE

Enable Schneider Energy Asset Monitoring as a service for their customers without adding network security risk

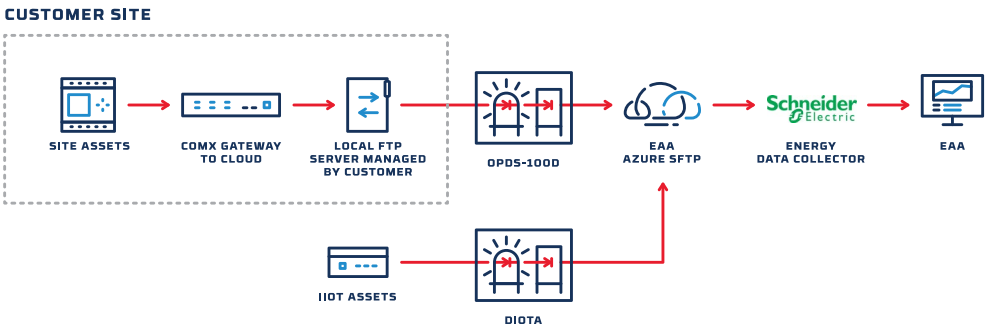
SOLUTION

5 x OPDS-100D DIN-Rail Data Diodes – Each collecting an FTP data stream from a customer site

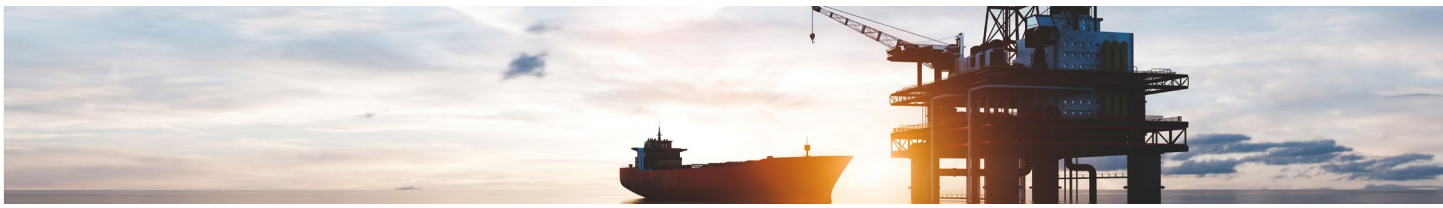
30,000 x DiOTa Compact Data Diodes – To secure individual site assets streaming data directly to the Schneider EAA Energy Data Connector

BUSINESS BENEFIT

Real-time remote monitoring provided process optimization and improved maintenance for reduced downtime.



INTERNATIONAL GAS & OIL MAJOR



CYBERSECURITY CHALLENGE

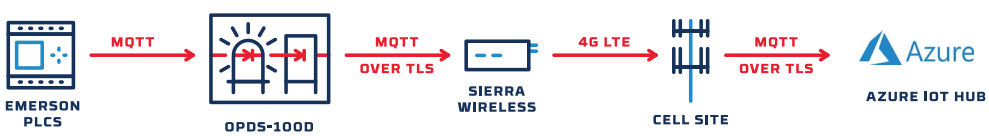
Securely sending IIoT data to the cloud without compromising the plant with myriad external connections

SOLUTION

5 x OPDS-100D DIN-Rail Data Diodes – Transfer Emerson IIoT device data to wireless transmitter via MQTT over TLS for transit to Azure IoT Hub

BUSINESS BENEFIT

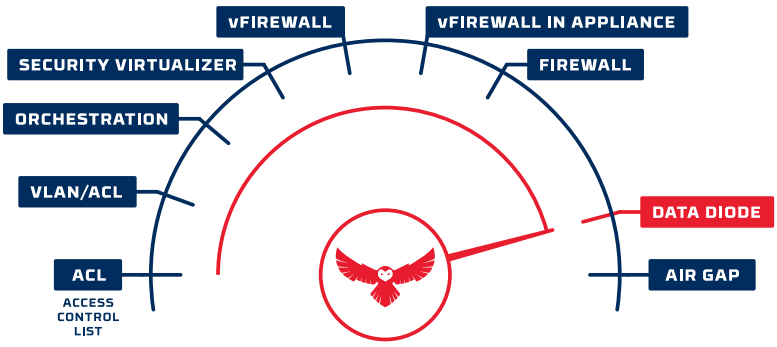
Wireless connectivity of field assets reduced network complexity and enabled digitalization benefits



Hardware-Enforced Security

"Hardware-enforced" or "hardware-based" in the context of security means that there is one or more hardware element(s) within a device which is part of or the primary source of security enforcement. For example, this may take the form of hardware security modules which can provide hard-coded cryptographic support. In the case of data diodes and cross domain solutions, it takes the form of a one-way data transfer mechanism which is enforced by a physical hardware design: An optical isolation device (optocoupler) or digital isolation device, comprised of separate, dedicated transmitter and receiver hardware, physically rendering it capable of only transferring data one-way.

Unlike software-enforced or "configuration-based" security such as firewalls, the primary benefit of hardware-enforced domain separation is that because it is physically unable to transmit data from the receive side to the transmit side of the device, it maintains an effective air gap between the domains in that direction.



WHY HARDWARE-BASED SECURITY

SOFTWARE

- Configuration-enforced
- Zero-day exploits
- Malware / ransomware
- Heavy ongoing management

HARDWARE

- Physics-enforced
- Unhackable
- Invulnerable to malware
- Little to no ongoing management

Hardware-enforced network segmentation is required by NERC CIP regulations, and recommended to secure external connections, including the cloud, within all OT networks within critical infrastructure and industrial organizations by the U.S. Department of Homeland Security (DHS) and the U.S. Cybersecurity and Infrastructure Security Agency (CISA).

Summary

The potential benefits of OT-to-cloud connectivity grow more apparent each year, creating additional incentives for critical infrastructure operators and device manufacturers to support secure external network connections. The adoption of hardware-enforced security technology to deliver data to the cloud can help the industry accelerate adoption of cloud services, without the need for complex network analysis, and while fully meeting all regional and federal regulatory requirements. With a securely enabled OT-to-cloud data flow, protected by hardware-enforced security technology, critical infrastructure organizations can optimize operational performance and device maintenance, thereby reducing operating expenses and delivering increased uptime, output, and value.

OWL Cyber Defense

About Owl

Owl is the world's #1 provider of cross domain and data diode secure data transfer solutions, trusted by global intelligence, defense, and critical infrastructure communities for over 20 years. With deep ties to the U.S. intelligence community and DoD, as well as over 75 major organizations in the critical infrastructure market, Owl is uniquely positioned assist in developing and applying the world's highest security standards to critical systems.

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

@OwlCyberDefense 203-894-9342 | Info@owlcyberdefense.com

B022 | V5 | 08-16-21