DATA SHEET

OWL Cyber Defense

OWL ADVANTAGE

THE GOLD STANDARD IN DATA DIODE TECHNOLOGY

Remote Monitoring

THE REMOTE ACCESS SECURITY PROBLEM

The problem is, it's not secure! As evidenced by numerous breaches, perhaps most notably in the Ukranian power grid incident, malicious actors can utilize these same remote access pathways, through phishing, brute force, malware, etc., to gain entry into (and sometimes even control of) operational networks. Even if the data inside these networks may not be sensitive, the systems within them are often extremely sensitive, and in some cases, such as in water treatment, chemical processing, and other critical infrastructure, their protection is vital to the safety and well-being of the public.

However, it's painfully obvious to anyone with a news feed that traditional methods of boundary protection (role-based access controls, firewalls, etc.) won't provide sufficient security to prevent a breach. If countless users and systems connecting into the network is the norm, there are simply too many ways in, and too many things that could go wrong.

Following the principle of "least privilege", only those users who absolutely require access to any given system should be given such access, and only to the extent required to perform job functions. Also, ideally (for security purposes), the less connected these systems and networks are, the better, to reduce the possible avenues of attack or exposed "surface area". For example, the regulators at the Nuclear Regulatory Commission prohibit any sustained connections from external networks into nuclear power plants. But there's no place for disconnection in the IoT, so where does that leave remote monitoring?

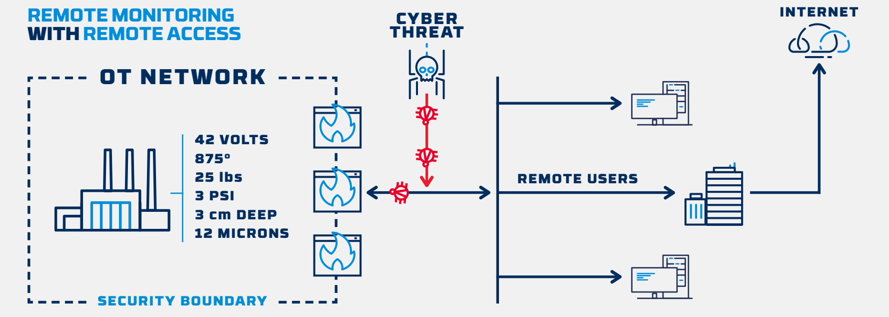
Remote Monitoring without Remote Access

Remote monitoring is most often thought of as users at remote locations (HQ, support & service center, engineering, etc.), accessing information stored within a secured network; inferring that remote monitoring requires remote access. At Owl we are changing the paradigm. While the information generated in these secured networks is necessary for remote personnel to perform their job duties, users no longer need to access the network to access the data. Remote monitoring without remote access is a method by which information is transmitted one-way out of a network to an offsite data repository (typically either a corporate IT network or the cloud) where it can be then monitored remotely by users. This one-way-only transfer of data is vital to reduce risk to the secured network, while preserving data sharing.

The IoT and Data Sharing

In critical infrastructure, the machinery and operational equipment, including SCADA systems, historians, PLCs, etc., is increasingly becoming "smart". Being "smart" basically means these digital devices generate operational data, provide remote interfaces, and are inter-connected to an operational network – and are sometimes connected beyond that to the Internet.

By connecting these devices (or "things") and networks together, you have, in a nutshell, the Internet of Things (IoT). Increased connectivity allows a variety of personnel located offsite to connect to and remotely access the systems (via VPN, dial up connection, etc.) to do their jobs – everything from alarms and safety monitoring to efficiency analysis. This "remote access" model is common among many organizations, as it affords operations, maintenance, and other users fairly free and easy access to the data they need to perform job functions.

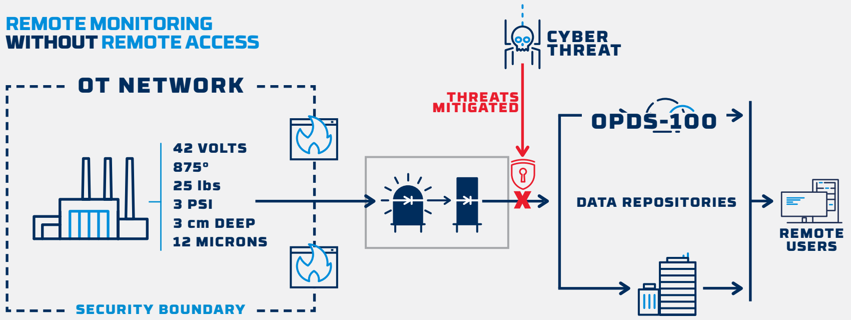


Users remotely access the secure OT network to collect operational data, leaving the OT network vulnerable to cyber attack

USE CASE

HOW TO PERFORM REMOTE MONITORING WITHOUT REMOTE ACCESS

In order to allow users to get at the data without allowing them to access the systems which generate it, the data must be sent offsite while also preventing access to those systems. The logical solution would be to allow data to flow in only one direction, out of the operational network, to another network (HQ, the cloud, offsite storage, etc.), while preventing data flow into the operational network. Thankfully, there is a device designed precisely for this task – the data diode.



Operational data is securely transferred out of the secure OT network through a data diode to data repositories; allowing remote users to retrieve OT data without opening up the OT network to attack.

REMOTE MONITORING WITHOUT REMOTE ACCESS USING OWL DATA DIODES

- Sensitive networks are completely secure from external cyber threats
- Data can be sent to various networks, the cloud, or end users for real-time access
- Improves time to market and business continuity, while reducing downtime and inefficiency
- Helps achieve regulatory compliance, including NERC CIP, NRC, HIPAA, PCI-DSS, etc.
- “Set and forget” operational reliability with 10+ years MTBF
- Immune to software vulnerabilities such as malware, misconfiguration, zero day exploits, etc.

What is a Data Diode?

A data diode is a hardware-based device which only transfers data in one direction. It secures its source network by preventing all traffic from entering, while allowing data to be transferred out to other networks, the cloud, or end users. Often compared to firewalls, as that is usually the first point of reference in network security, data diodes hold a few particular distinctions and advantages. First, a data diode is a hardware-based device, which means that it is immune to software-based vulnerabilities, such as misconfiguration and zero-day exploits. Second, data diodes are non-routable – bound by the laws of physics to transfer data in only one direction – and cannot be configured otherwise. Third, for the purposes of many regulatory organizations, including the NRC, data diodes provide an effective “air gap” between networks, meaning that they are considered, for all intents and purposes, disconnected.

No other cybersecurity technology comes close to the level of protection afforded by data diodes. This elite technology is second only to the complete physical disconnection of systems in terms of preventing unauthorized access to sensitive networks.

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