WHITE PAPER

Owl Best Practice:
NCSC 10 Steps to Cyber Security

Executive Summary

Cyber security is at the top of the agenda throughout the world, particularly with regard to critical infrastructure industrial control systems, where lapses in security, whether accidental or malicious, can have catastrophic consequences. The responsibility for developing, maintaining, and monitoring appropriate cyber risk management best practice strategies and security policies has escalated to Board level, supported by government frameworks and recommendations including the National Cyber Security Centre *10 Steps to Cyber Security* framework.

This document explains the Owl Cyber Defense "ABCs" of cyber security best practice:
A: Assessing requirements and designing the organisation's risk framework
B: Building the infrastructure that is needed to protect and secure network borders
C: Choosing the right technologies, and associated vendors, to meet cyber security requirements

Owl Cyber Defense provides a comprehensive range of data diodes, one-way hardware communications devices, that help critical infrastructure organisations design, implement and monitor their cyber security best practice strategy and policies. Owl products are used throughout the world and in all critical infrastructure applications, including chemical, commercial facilities, communications, critical manufacturing, defence, emergency services, energy, financial services, food & agriculture, government, healthcare, information technology, nuclear reactors, transportation, and water & wastewater.

Introduction

Cyber security is no longer solely the domain of the IT department: it is an organisation-wide strategic concern and needs to be addressed from the Board level right throughout the organisation.

Governments are providing recommendations and advice such as the EU Directive on the security of Network and Information Systems (NIS) and the UK National Cyber Security Centre (NCSC) 10 Steps to Cyber Security framework. It is prudent to take these recommendations and frameworks into account when designing and implementing cyber security policies and procedures.

Data diodes are a core technology that play a vital role in helping organisations protect themselves. Whether it is safely exporting information from the organisation, safely importing information to the organisation, or establishing two way communications systems, data diodes go beyond firewall technology by providing a hardware-based, one-way communications mechanism that enables the safe and secure transfer of data between networks, for network segmentation and security that, by its very design, cannot be hacked.

Owl data diodes allow organizations to send data in real time to information management systems in critical infrastructure applications without compromising the security of the network. Every day, data diodes protect some of the world's most valuable information and network infrastructure from theft, destruction, tampering, and human error, mitigating huge potential financial and work-hour losses.

The NCSC framework addresses a variety of issues, from the set up of a risk management regime through to incident management. Data diodes utilised in an organisation's OT/IT infrastructure play a key role in three of these steps: network security, secure configuration and malware protection. Additionally, the Owl range of data diodes incorporate a defence in depth approach within their own design, ensuring that organisations can be confident of their technology choices. These relate to the NCSC steps of managing user privileges, monitoring, removable media controls and home and mobile working. Finally, the presence of data diodes as part of an organisation's overall technology portfolio means that Owl helps inform organisations and provide input to the development of appropriate cyber risk management policies and procedures, relating to the NCSC framework steps of risk management regime, user education and awareness and incident management.

Assess Requirements and Design The Organisation's Risk Framework

Assessing requirements and designing the organisation's risk framework is a strategic activity with Board-level responsibility. It involves balancing the need for 'business as usual' with incorporating relevant frameworks and recommendations for a best practice approach to cyber security. Three of the NCSC 10 steps have most relevance here, and while data diodes do not have a direct role to play across every aspect of in this strategic process, it is important that organisations are aware of their capabilities and functionality to use them as part of the technology portfolio that can be used to implement the cyber security framework.

NCSC STEP: Set up your Risk Management Regime

"Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers."

At the core of the NCSC 10 Steps to Cyber Security framework is the requirement to set up the risk management regime for the organisation: determining the organisation's risk appetite, making cyber security risk a priority for the Board and producing supporting risk management policies. Security must be embedded within the entire organisation, rather than being a dedicated security function which could result in the organisation being overly cautious.

Organisations rely on technology to execute on their business goals, and there is an intrinsic need to use technology to share information with external organisations, including suppliers, customers, and partners. The role of data diodes with regard to this NCSC step is to provide a component of an organisation's overall technology arsenal: the more secure the network, the more it supports an educated, balanced approach to corporate risk and cost management. The awareness of available technologies, including data diodes, from certified and trusted suppliers, helps in informing the development and execution of and organisation's risk management policies.

NCSC STEP: User Education and Awareness

"Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks."

Users need to be aware of the organisation's overall security policy, as well as the appropriate use of technology within their corporate roles and responsibilities. Ongoing awareness programmes, highlighting user security policies as part of the overall corporate security policy, are essential. Organisations need to be kept informed with regard to the latest product and technology information available from vendors, including data diodes, in order to keep any relevant internal documentation or training up to date, as part of their overall cyber security good practice.

NCSC STEP: Incident Management

"Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement."

Incident management policies are essential in order to improve organisational resilience and support business continuity. As part of its monitoring capability and defence in depth strategy, Owl data diodes perform self-inspection and notify administration of configuration or software changes that might indicate attempts to compromise the system, thus helping to minimise the occurrence of security breach incidents.

Build the Infrastructure to Protect and Secure Network Borders

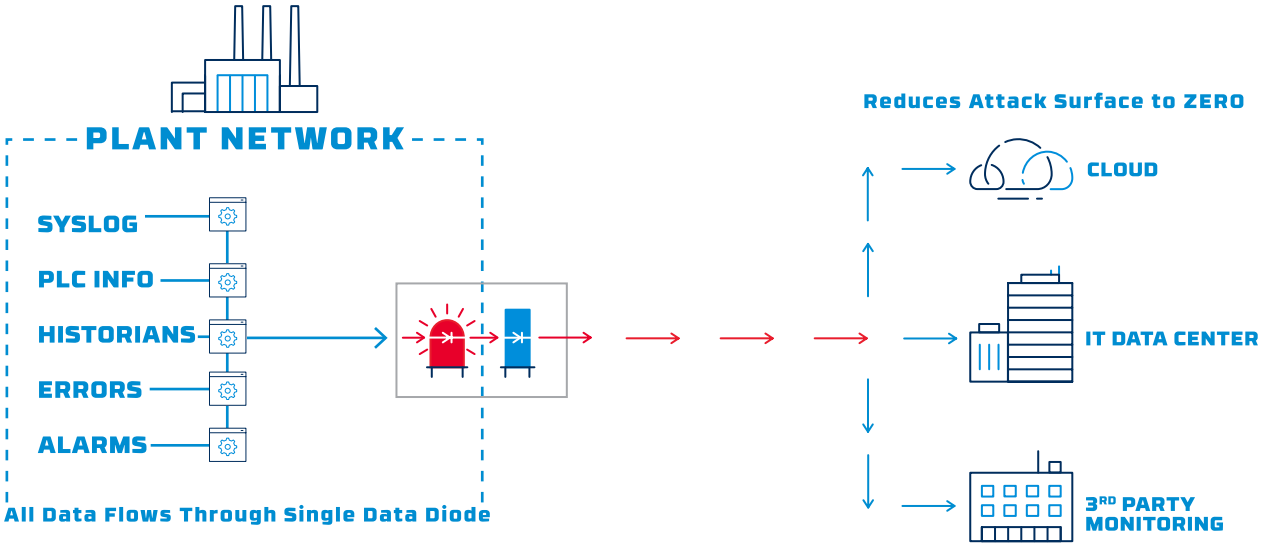
Building the appropriate technology infrastructure ranges from large scale infrastructure to individual workers, on or off site. This is the main way that data diodes, and Owl products in particular, help organisations implement cyber security best practice. Data diodes contribute directly to the three major NCSC steps of network security, secure configuration, and malware protection. Owl data diode products also contribute to the remaining four NCSC steps of managing user privileges, monitoring, removable media controls, and home and mobile working.

NCSC STEP: Network Security

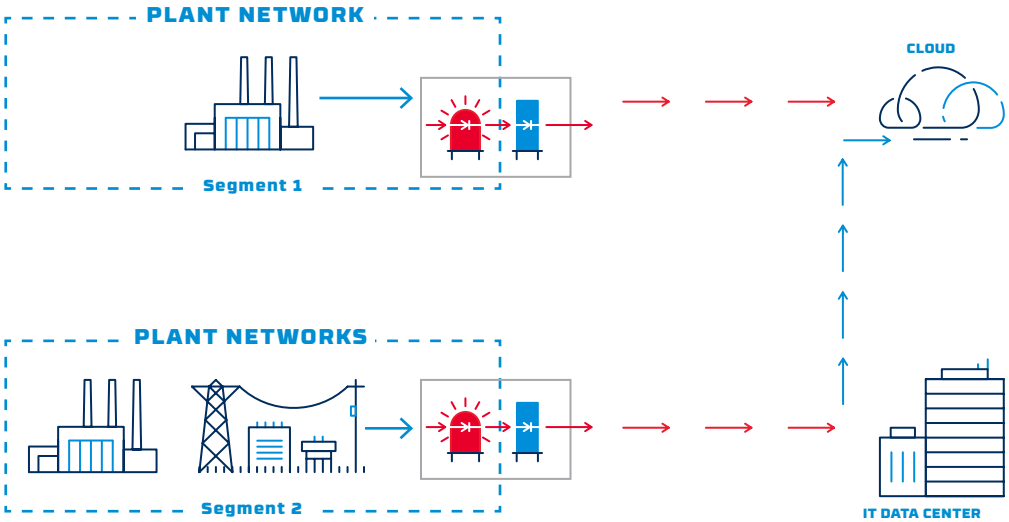
"Protect your network from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls."

Connections from ICS networks to the Internet and other external networks are essential in order to conduct business, but are also the most vulnerable to attack. Network security is the key to cyber security, and is where data diodes play the most important role in building a defendable environment.

All Owl data diodes support isolating networks, locking down services and other potential attack vectors, and protecting network segments. By definition, Owl data diodes only allow one-way communications over restricted paths, not just reducing the attack surface but bringing it all the way to zero. Owl also offers a bidirectional communications solution, where two pairs of data diodes provide a restricted, single TCP/IP connection to provide bidirectional communication. Because data diodes are used in both directions, the layers of protection afforded to one-way communication are applied to the bidirectional solution.



Providing network segmentation is the primary use case for Owl data diodes, designed specifically to allow only one-way communication. In keeping with the defence in depth strategy, Owl uses the ATM protocol to transfer data across the data diode, creating a protocol break between the protected network and outside threats. This restricts host-to-host paths and prevents infections from propagating from one segment to another. The data diodes do not perform or allow any IP routing and prevent all routable information (IP addresses, etc.) from ever crossing the data diode.



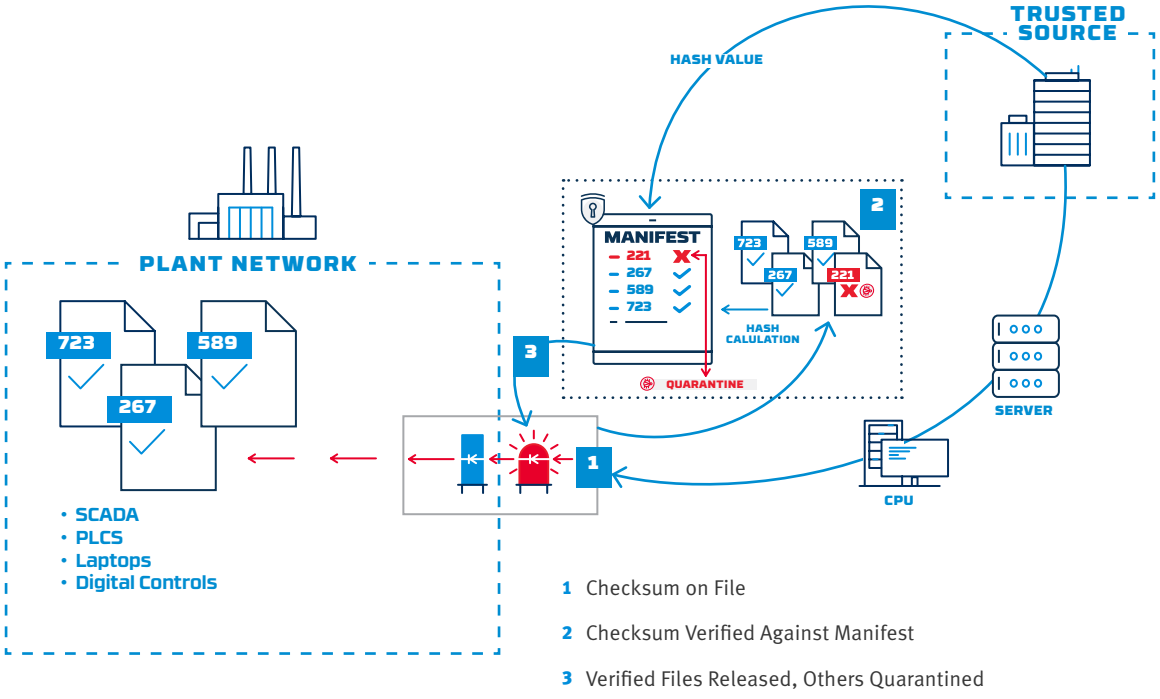
NCSC STEP: Secure Configuration

"Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices."

Organisations need a secure strategy to remove or disable unnecessary functionality and to quickly fix known vulnerabilities, usually via patching. Systems that are not properly managed are more susceptible to attack, whether via unauthorised changes to systems, exploitation of software bugs or exploitation of insecure system configuration. Secure configuration precautions include the use of supported software, policies to update and patch systems, hardware and software inventories, white-listing and execution control and limiting user ability to change configurations.

The Owl Secure Software Update Solution (SSUS) is a data diode product designed specifically to help critical infrastructure operators address software update issues and keep their systems current. SSUS securely transfers software patches and updates into the control centre without the risk of using potentially contaminated laptops or portable media. The core data diode provides network-segmentation security while the application uses the vendor's secure hash code to verify the authenticity of each file. The files are also subject to antivirus scanning and other vetting. Any issues found with the file cause it to be quarantined and prevent it from reaching the control network.

Since the Owl data diode is hardware-based, patching is not required for the device itself to keep the one-way policy in place and operational, and software changes or revisions never impact the operation of the data diode. Software patches are only needed to modify interfaces to network devices (OS changes, historians, OPC or Modbus interfaces, etc.), never to transfer data or prevent access to the network. Once the file is transferred, the application running on the destination side of the Owl data diode receives the file.



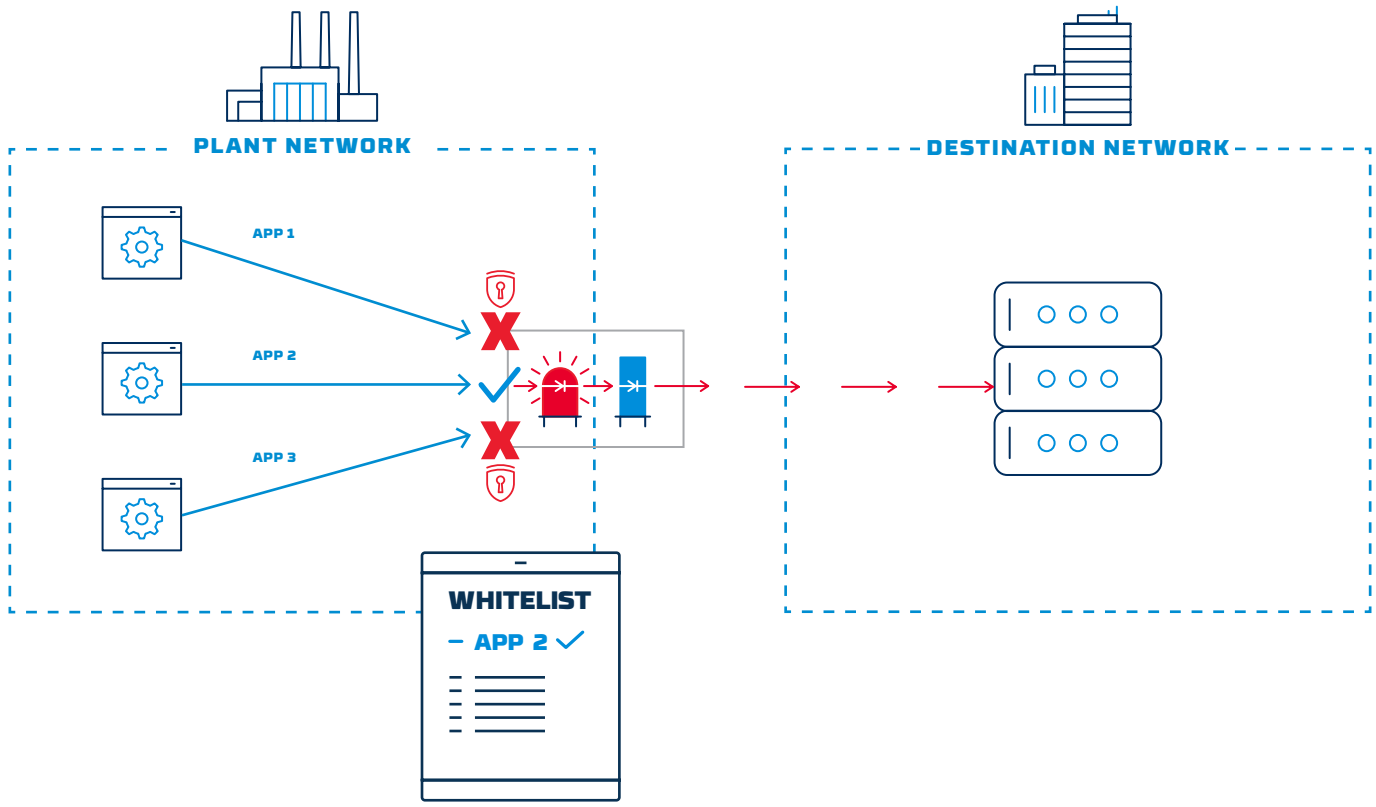
NCSC STEP: Malware Protection

"Produce relevant policies and establish anti-malware defences across your organisation."

Any exchange of information brings with it the risk that malware might be exchanged, with consequences ranging from minimal to catastrophic. Whether it is getting data into the organisation or out of the organisation, the only way to truly eliminate malware is through physical separation using a data diode, which is where Owl plays a crucial role.

Owl data diodes only accept data from known 'whitelisted' data sources. Data sources and destinations are deterministic and restricted to a unique combination of IP address, network port, and protocol. There are two mapping tables physically separated by the data diodes. The source side table maps a whitelisted data source to a channel for transfer to the destination side. On the destination side the channel is mapped to the true destination address. In this architecture, the source side doesn't know where or what the destination is. Even in the event that a rogue application was able to hijack a valid outbound IP address, network port and protocol combination, it could only communicate with the blind, paired end destination and would not be able to 'phone home' or attack targets of its own choice.

Owl data diodes protect themselves against unauthorised applications using two measures. The first is a whitelist of valid executables that are allowed to run, and the second is that under normal operating conditions, there is no mechanism for even loading files onto the data diode. This is achieved by not providing a command line interface or supporting any kind of file transfer capability through the menu system. These commands allow an application to submit a file for transfer to the proxy running on the source server.



NCSC STEP: Managing User Privileges

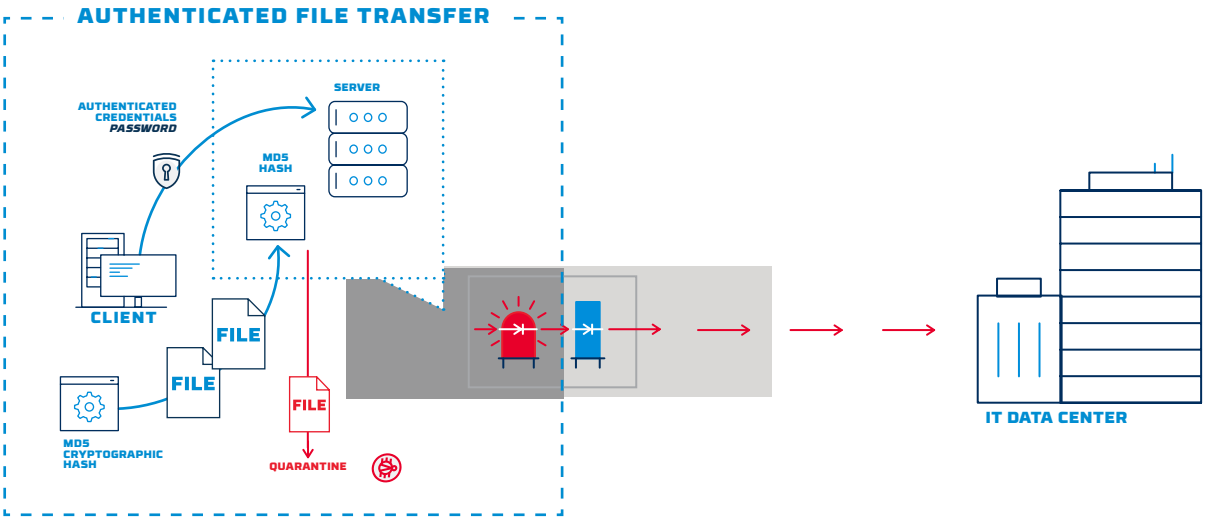
"Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs."

The fundamental tenet of this step is that all users should be provided with reasonable but minimal levels of system privileges and rights needed for their role. This avoids the misuse of such privileges, either accidentally or deliberately.

The Owl approach supports an organisation's overall cyber security policy by incorporating a defence in depth approach into its own technology. Not only do Owl data diodes follow the recommended provisions for long passwords, separating IT and OT users, changing passwords, and least privilege, they also provide authentication on the files they transfer. Using Owl's RFTS (Remote File Transfer Service), a more secure and robust version of protocols like FTP and NFS, the client/server architecture ensures unauthenticated files do not cross the data diode.

The client runs outside of the data diode and is registered with the server application running. Each client user has to authenticate with the server using login ID and password over their assigned port otherwise files never even reach the data diode. The files are also assessed pre- and post-exchange between client/server using MD5 to make sure the correct files are queued for transfer.

The Owl products contain security measures that can support the security policies and procedures implemented in industrial control networks. Users with appropriate credentials can use passwords up to 14 characters long and password change intervals are configurable between seven and 90 days. User roles are controlled by the Linux operating system and further constrained by the role-based menu systems with narrowly defined user roles. Not only are separate credentials for IT and OT networks required, but there is also physical separation of the admin functions between OT and IT. There is no way to provision the OT side from the IT network and vice versa. In addition, the admin ports are further separated with each side having a dedicated ethernet connection distinct from data traffic.

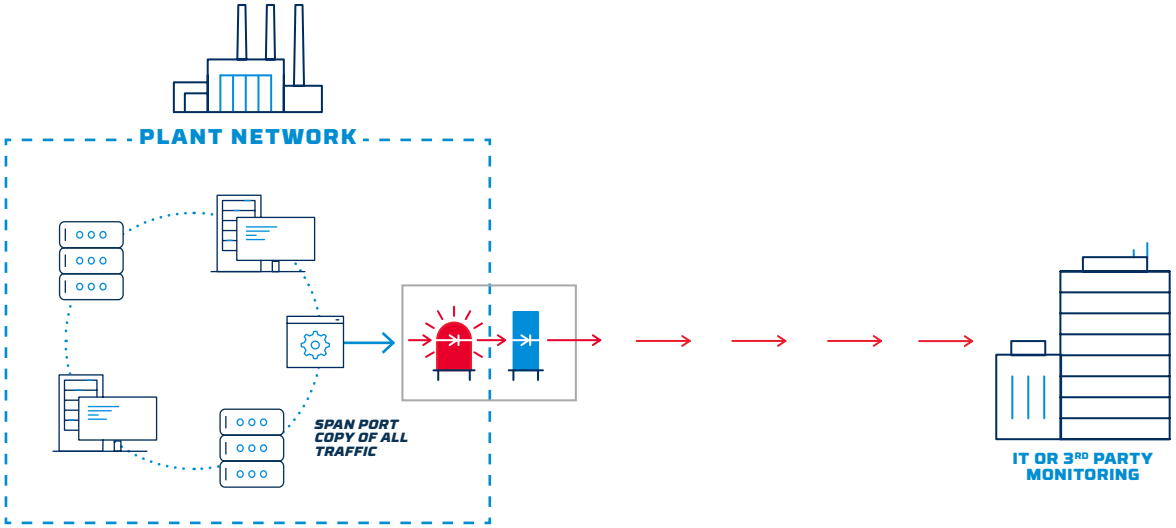


NCSC STEP: Monitoring

"Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack."

Continuous monitoring is essential to ensure that attacks can be effectively responded to, and to ensure that systems are being used appropriately in accordance with organisational policies.

The Owl family of data diodes includes self-inspection as part of its defence in depth approach, contributing to an organisation's overall monitoring strategy. Extensive logging is incorporated into the data diode which can alert on abnormal activity. An auditor role is also included so that log files can be examined. One of the options Owl data diodes provide is the ability to securely transfer network traffic to external networks for analysis. 100% of line-rate traffic can be captured and transferred to another enclave, allowing third parties to perform network analysis without ever accessing the control network. The Owl data diode performs self-inspection, notifying administrators of configuration or software changes that might indicate attempts to compromise the system.



NCSC STEP: Removable Media Controls

"Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system."

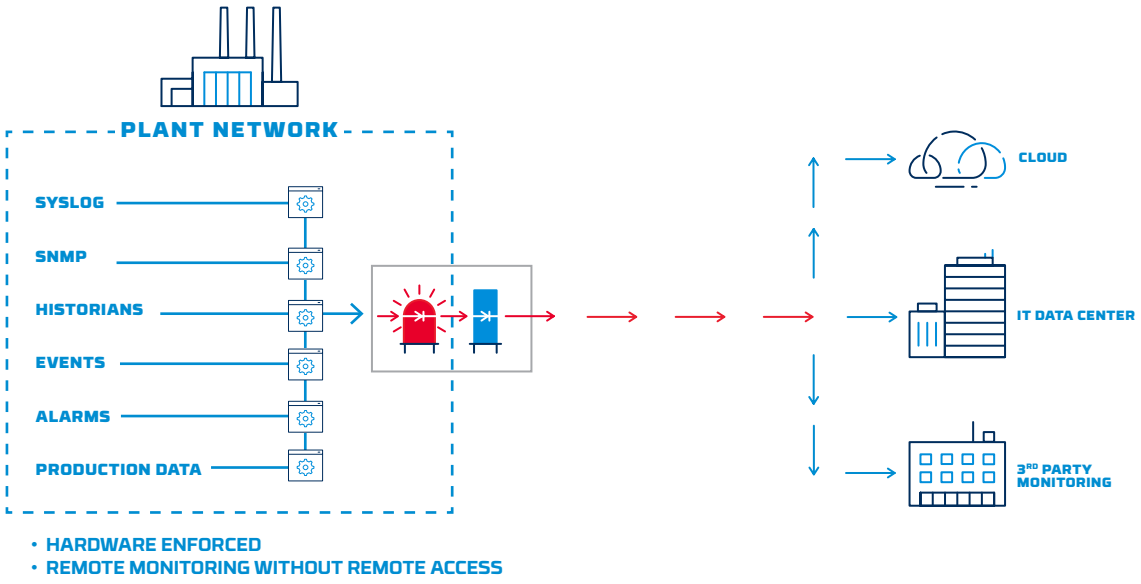
Removable media is a key manner in which malware can be introduced to a network or whereby sensitive data can be accidentally or deliberately exported. Data diodes provide a more secure and controllable alternative to removable media, allowing organisations to further limit or eliminate their use in walk-nets and other use cases. Data diodes provide a 100% secure connection due to the physical separation of networks using the data diodes.

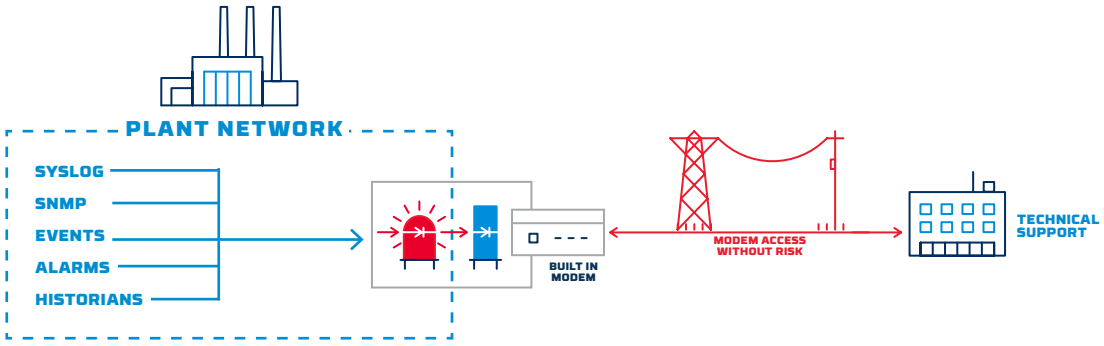
NCSC STEP: Home and Mobile Working

"Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest."

Home and mobile working can encompass not only organisational employees working from home or travelling, but also the use of third-party monitoring applications. Protecting points of entry to and exit from the organisation using data diodes can protect home and mobile users from risk when communicating with the organisation.

From a monitoring perspective, Owl data diodes are specifically designed to facilitate secure, remote monitoring without incurring the risks of remote access. As a hardware-based solution, it does not rely on 'read-only' software configurations, it eliminates backdoors, and monitoring information can flow across the Owl data diode to remote end-users. Remote engineers and technicians can observe systems in near real-time while equipment vendors can monitor their equipment and fulfil SLAs from centralized monitoring centres. Monitoring data can include tag information, alarms, alerts, SNMP traps, syslog messages, etc. While modems can create risks to the control network, Owl has solved this problem by providing a data-diode product that has a built-in modem. The control network is still protected behind the data diode; however, monitoring data is now available via secure remote access. The data is transferred across the data diode and then stored on the IT side of the data diode. The built-in modem then allows remote users to 'dial-in' to retrieve the data without ever opening up access to the control network.





Choosing the Right Technologies

It is important to select the technology portfolio that is most appropriate for the organisational cyber security requirements and overall risk management regime. This involves taking into account the likelihood of risk, the severity of risk, overall cost management and the need to simply get on with running the business. There is no such thing as a 'one size fits all' approach, rather it is about specifying, using and managing the right combination of technologies and products.

It is clear that data diodes have an essential role in protecting critical infrastructure across a range of network sizes in a variety of industries, with multiple applications. The one thing all of these deployments have in common is the requirement for 100% assurance in the inability to hack the communication mechanism. Owl is the vendor of choice for organisations around the world, and there are a number of key reasons why...

Comprehensive Range of Products Available From a Single Vendor

The Owl product line ranges from the entry-level DiOTa, designed for ease of use and supporting applications requiring throughput of 3 Mbps or less, through to the most powerful EPDS supporting enterprise applications needing up to 10 Gbps. All products support a wide range of data formats and transfer protocols including SNMP, FTP / SFTP, TCP and UDP.

Product	Max Link Speed	Single Box	DIN-rail Compatibility	Upgradable Bandwidth
Entry Level				
DiOTa	3 Mbps	●	●	
Mid-Range				
OPDS-100D	104 Mbps	●	●	●
OPDS-100	104 Mbps	●		●
High-Performance				
OPDS-1000	1 Gbps	●		●
EPDS	10 Gbps			●

More information about the Owl products is available on the Owl web site at www.owlcyberdefense.com.

Range of Applications and Industries

Owl's family of cyber defence solutions are used for a wide range of applications. These include:

- File transfer: reliably transfer files or data sets one-way across network/security boundaries
- Real-time data streaming: transfer real-time data one-way, as packet streams
- Historian and database replication: replicate full or partial historian and relational databases across network domain boundaries
- Remote monitoring: enable real-time remote monitoring without remote access
- Process control interfaces: securely transfer DCS and SCADA data to external/business networks without jeopardizing plant network security
- Software updates and patching: safely vet, import, and install software updates in isolated control networks

The Owl family of data diodes are used across a range of industries to meet a number of security and operational requirements. Some examples include:

Customer	Challenge	Solution	Benefits
Oil & Gas Producer	Malware disconnecting operational and business networks	Owl data diodes and software to replicate one-way data transfer from the OT network to the WAN to the corporate network	Secure network with increased data visibility without increased risk
Gas Turbine Vendor	Malware destroyed data and disconnected OT network	Owl data diodes to secure real-time one-way data monitoring via UDP	Remote monitoring system enabled and secure from external threats
Water/Waste-Water Utility	Need to proactively improve cyber security position	Owl data diodes and software to provide remote HMI screen replication	One way data flow secure from external cyber attack, with real-time remote alarm and alert monitoring
Rail Transport Company	Preventing cyber attacks on rail sensor network while maintaining remote monitoring capability	Owl data diodes to protect systems, with interface to cellular transmitter to securely transfer data	One-way data flow ensuring monitoring network is secure from external threats

Ground Up Design with Defence in Depth

The Owl family of data diodes have been specifically designed from the ground up with nothing but cyber security best practice and defence in depth in mind: a true single-box format, fit for purpose and evolving as government regulations and recommendations evolve. Owl data diodes are one-way by design: all of the components and circuitry are designed to be one-way, with a physical air gap separation between the send and receive side. Communication is secure, with all routing information remaining secure within the source network, not crossing the data diode. As well as helping protect organisations, the Owl data diode family incorporates its own defence in depth provisions to ensure that its products contribute to the organisation's overall cyber security strategy and policies.

Reliable, Robust, High Performing Product Family

With the industry's leading throughput, the Owl solutions provide up to 10 Gbps of bandwidth, with the appropriate solution selected based upon need and expanded by software license as required in the future. Extremely low latency means that packets are transferred across the data diode in single-digit milliseconds with no packet loss and no need for packet transmission, creating a highly tuned and optimised solution. Owl also provides industry-leading reliability, with long lifespan solutions and a high MTBF. The solutions are quick and easy to deploy and upgrade as requirements evolve.

Optional Software Modules

To expand the applicability of the Owl product line, Owl has developed a library of optional software modules, allowing Owl products to interoperate with a wide range of process control devices and provide additional functionality. These include modules for performance management, log forwarding, historian replication, OPC server replication, remote screen view, database replication, Modbus transfer and remote file transfer.

Technology Partners

As well as its distribution partners, Owl cybersecurity solutions have been designed to interface with and protect a large number of devices and software tools available from various critical infrastructure equipment providers as part of the company's technology partnership programme. Partners include ABB, General Electric, Mitsubishi Electric, OSIsoft, Rockwell Automation, Schneider Electric, Curtiss-Wright and Yokogawa.

Further information can be found at:

- **The Owl web site: www.owlcyberdefense.com**
- **NCSC NIS guidance web site: www.ncsc.gov.uk/collection/nis-directive**
- **NCSC 10 Steps to Cyber Security framework: www.ncsc.gov.uk/collection/10-steps-to-cyber-security**

Owl Data Diode Cyber Security

ONE-WAY BY DESIGN

SECURE COMMUNICATION

COMPLETE SEPARATION OF NETWORKS

UNMATCHED PERFORMANCE

UNPARALLELED SCALABILITY

MULTIPLE FORM FACTORS

LOWEST TOTAL COST OF OWNERSHIP

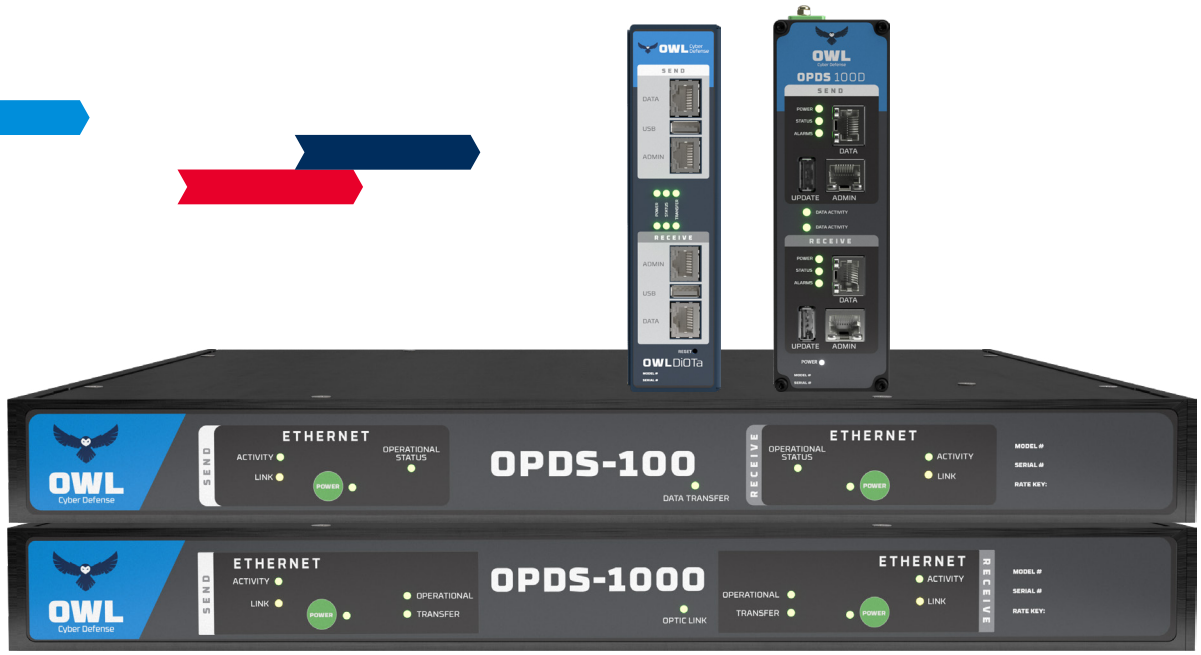
TESTED & ACCREDITED SOLUTION

SIMULTANEOUS MULTI-FUNCTION SOLUTION

DEFENSE IN DEPTH

INDUSTRY-LEADING MTBF

FAST & EASY DEPLOYMENT



With Owl Cyber Defense, critical infrastructure industries can design, implement and monitor the cyber security best practice that is most appropriate for their organisation, balancing commercial requirements and business realities with available technologies and government recommendations. Be secure of your security.

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

+1 203-894-9342 | Info@owlcyberdefense.com