



OWL Cyber
Defense

EBOOK

The Definitive Guide to Data Diode Technologies

From Simple to State of the Art

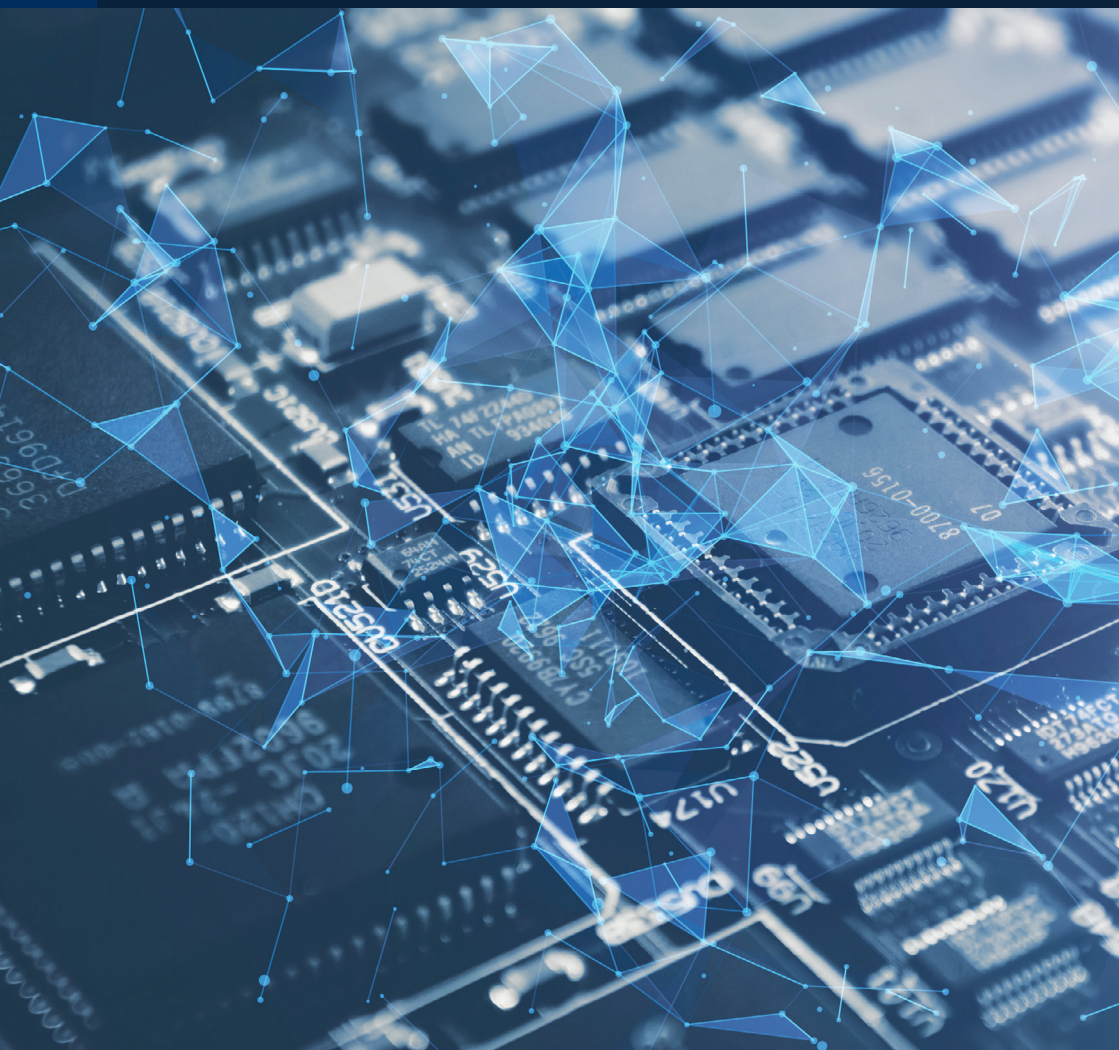






Table of Contents

Introduction 5

Overview 7

Purpose 8

Taxonomy of One-Way Transfer Technologies 17

Comparing One-Way Transfer Technologies 20

Data Diode State of the Art 26

Owl Intelligent Data Diodes 31

Conclusion 35



Foreword

Thank you for taking the time to read this book and for your interest in data diodes. We have endeavored to provide you with a comprehensive resource on data diodes, including what they are, their purpose and usage, a comparison of the various types of data diodes, and an in-depth look at the current state of the art in data diode technologies.

Specialized hardware-based data diodes started out in use by US government agencies in the late 90's. Soon after, the technology was adopted by the US Department of Defense and Intelligence communities. More recently, data diode products were developed to suit industrial and critical infrastructure use cases, and today they are being utilized across a variety of commercial industries, including healthcare, financial services, and more.

Data diodes are typically separated into two distinct markets, one for the US government and one for all other applications. Even though the underlying technology is similar between the two product lines, there are significant differences between them designed to meet the restrictions, regulations, interfaces, and accreditations of each market.

Those distinctions, along with the highly-controlled nature of cybersecurity architecture and technologies within classified government networks, have led us to focus the vast majority of this book primarily on the commercial use and application of data diodes and not on the military or intelligence applications.

We hope you find the book useful and welcome any comments, questions, or feedback you may have.



Scott W. Coleman

Director of Marketing & Product Management

scolem@owlcyberdefense.com



Introduction

Technology networks within critical infrastructure, the government, and commercial businesses form the backbone of developed nations. As the modern world continues to be more data driven and interconnected, these networks — from enterprise scale all the way down to smaller office and home networks — become more efficient, intelligent, and unfortunately, vulnerable.

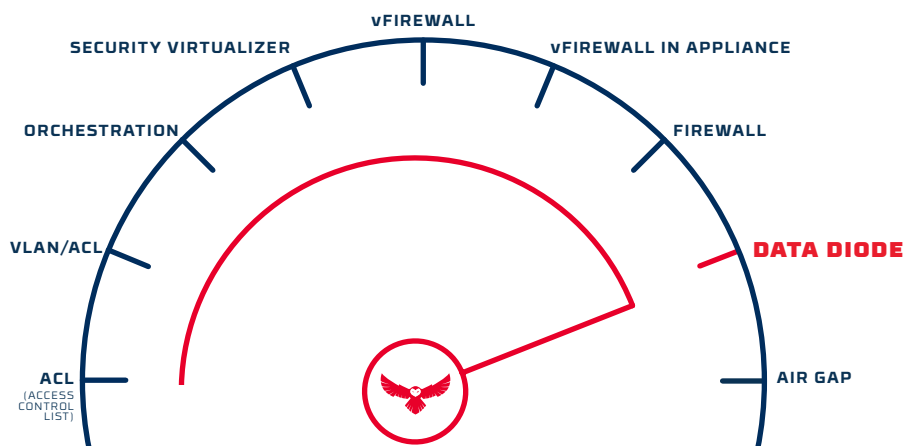
From industrial control system monitoring and CCTV feeds to laptops and intelligent home appliances, every new network connection introduces a new vector for cyberattack, and the surface area for such vulnerabilities has exploded in recent years. As such, there is a pressing, global need for more effective tools to combat cyber threats and protect these networks from attacks that might cause severe financial, physical, or personal damage.

Best practices for protecting these networks involve simplifying, reducing, and isolating network connections, including segmenting networks from one another by creating either a virtual or physical separation between them. However, physical or virtual separation can prevent information and data from getting to authorized users, and these networks often contain a wealth of information that is far too valuable to simply cut off. The traditional security challenge has been how to limit access, minimize risk, and keep these networks secure while getting valuable operational data to authorized users when it's needed.

“Prevent cyberattacks against digital assets within the protected network; securely share data outside the network”

One-way data transfer systems, generically called “data diodes,” were designed specifically to address this security problem by providing a hardened network defense while also securely sharing data. Data diodes isolate and protect networks from external cyber threats, while allowing these networks to import or export data in a highly controlled, deterministic manner. This can involve anything from Supervisory Control and Data Acquisition (SCADA) systems generating data in a nuclear power plant to transaction data created at a bank's ATMs.

As a part of every organization's "defense-in-depth" strategy, with layers of security working together to protect data and systems, data diodes are part of an evolving first line of defense on the edge of networks. In combination with the other layers of cybersecurity tools, devices, software, and best practices in the defense-in-depth strategy, data diodes help users, operators, security professionals, and everyday people to reduce risk and provide the strongest, best chance to protect their networks and data from cyber threats. Because of this, the U.S. Department of Homeland Security now specifically recommends data diodes in its seven strategies to protect critical infrastructure.¹



This document will look into the nature of data diodes, in an effort to clarify what they are, and to examine their role and use in network security, beyond what used to be considered a niche cybersecurity tool. It will also analyze the various implementations of one-way data transfer systems, comparing their quality of service, reliability, and security, among other factors. Finally, it will lay out the data diode "state of the art," which overcomes the limitations of other one-way data transfer technologies, and is currently in use around the world today.

¹ https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf

Overview

While data diodes are becoming more common in network security across many industries, there still remains some confusion about what exactly constitutes a data diode and what its capabilities are. The term “data diode” is a compound of “data” (electronic information) and “diode” (a specialized electronic component that conducts electricity between two terminals in only one direction).

In broad terms, a data diode could be defined as:

Data Diode: da-ta di-ode | /ˈdā-də ˌdī ˌōd/ | noun

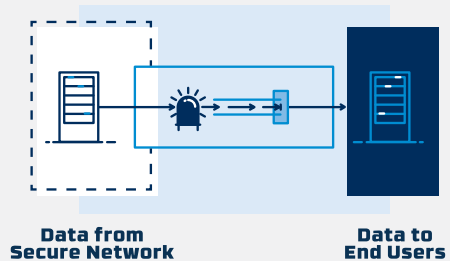
A device with two nodes or circuits — one send only and one receive only — that allows the flow of data in one direction only, from a source to a destination, while securing the source and/or destination networks and applications from external access.

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



It is relatively easy to create a simple one-way data transfer system (it could be accomplished by simply clipping the return wire on a pair of serial communication cables). However, it's far more difficult to engineer a high-performance, reliable, and secure one-way data transfer system that presents a high level of service and is also easy to implement. But before getting into the various types of data diodes that exist today, let's first take a deeper look at their purpose and fit within the defense-in-depth strategy.

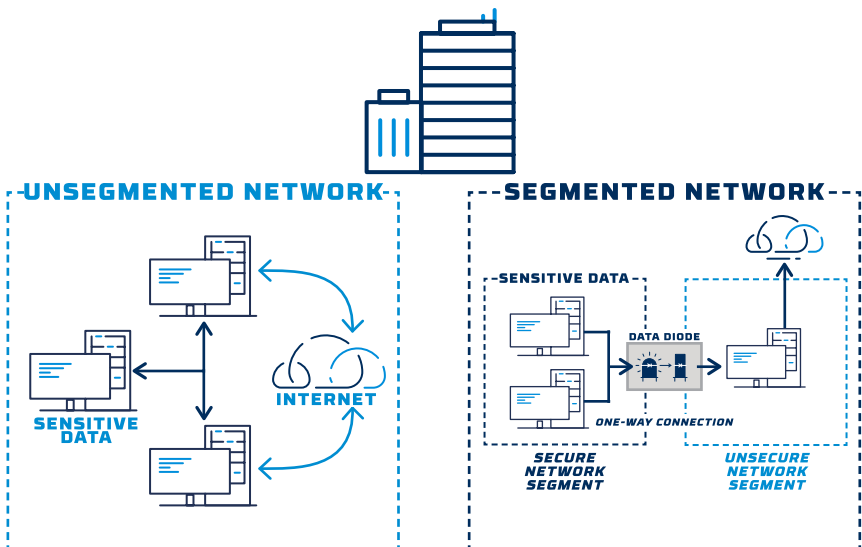
Purpose

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.

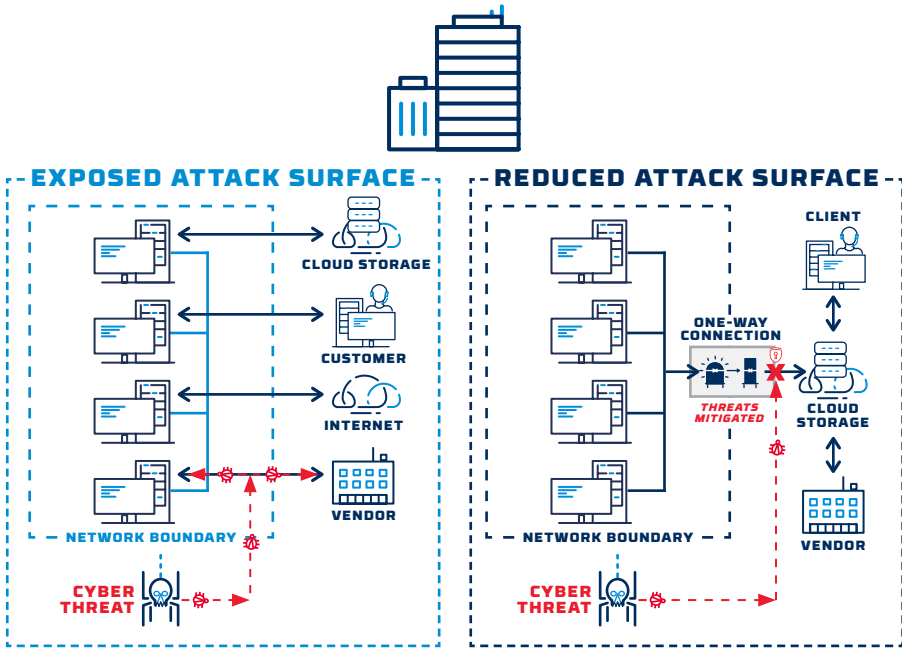
Network Security & Segmentation

Data diodes are intended to separate and create boundaries between trusted and untrusted networks, straddling the demarcation line between them. This separation between networks is more commonly known as “network segmentation” – a basic and vital part of any comprehensive cybersecurity strategy. Just as locked doors and gates provide security between open and private physical spaces, data diodes provide effective cybersecurity at the boundaries of networks.

Network segmentation enables greater control over network access, and the ability to create different levels of security. A single, large network must share the same security level across all resources, but if it is segmented into two (or more) separate networks, one segment can have a higher or lower security level than another. These security “gates” create additional layers of defense in depth, as well as further granularity in security controls.



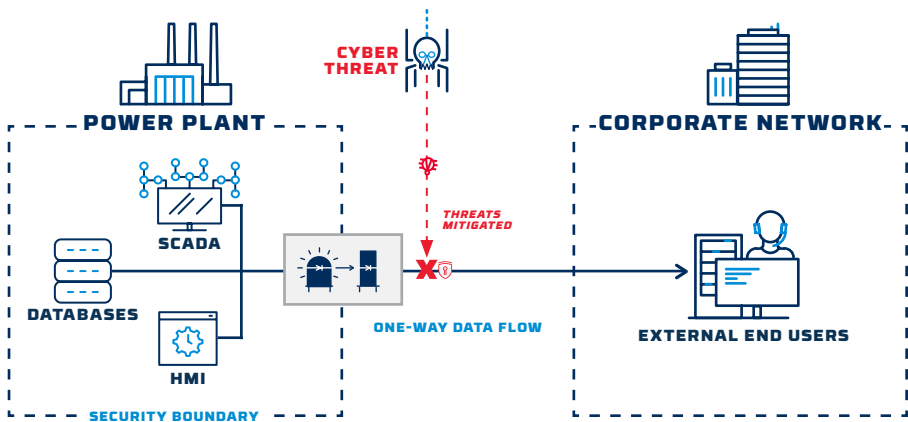
Because every external connection represents a possible threat vector, every connection that is routed out through a data diode, instead of directly to the internet or end-users, reduces the attack surface of the source network. Thus, if all connections from the source to external networks are directed through data diodes, then the source network would be completely secure from external cyber threats.



Data diodes always move data from a source network to a destination network; however, depending on how they are deployed, they can protect either the source or the destination network, or both.

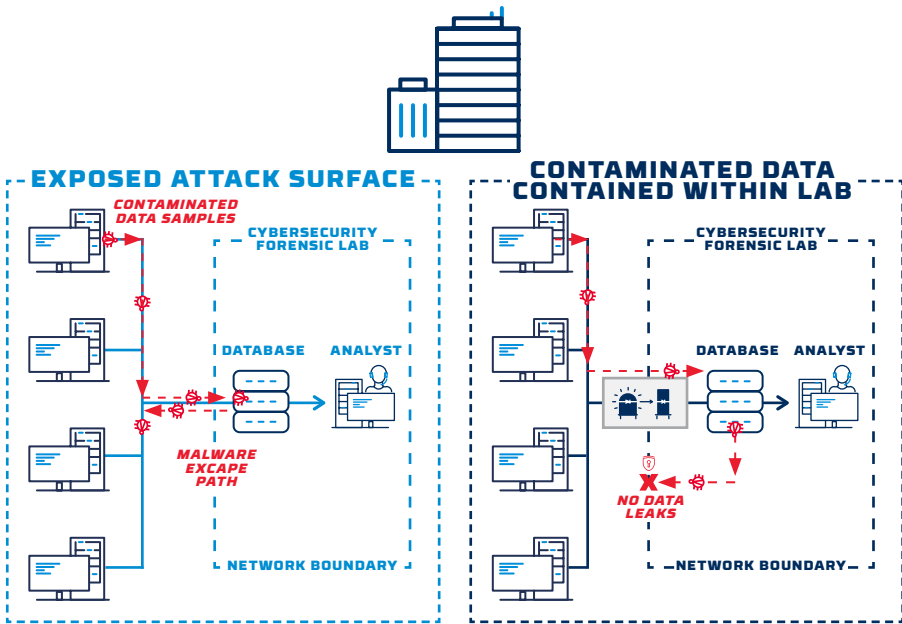
Determining where data diodes should be deployed depends on the security goals. If the primary goal is to protect the source network, then the data diode is deployed at the edge of the security border of the source network. The data diode prevents any possibility of an external party hacking into the source network while making data available outside of the source network.

For example, a power plant may need to control access to the facility to prevent breaches or the hijacking of controls, however they may have multiple data connections to external end users to transfer data from supervisory control and data acquisition (SCADA) systems, and historian databases, and to provide remote human-machine interface (HMI) access. If all of these connections are isolated to a one-way transfer that sends data offsite, the plant's operational technology network would be secure from external cyber threats while the data is made available to the end users.



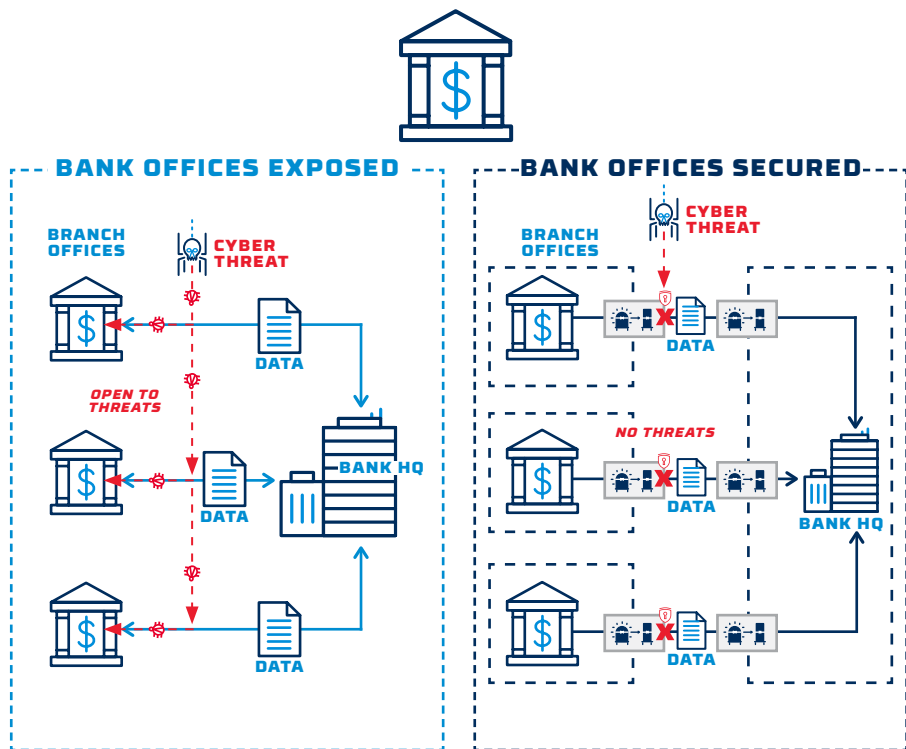
However, if the primary goal is to protect the destination network and prevent unauthorized data access, removal, or destruction (e.g. backup database, financial records, etc.), then the data diode is deployed at the security border of the destination network. Data can be transferred into the destination network but cannot be accessed or removed (or leak) back through the one-way path.

For example, a cybersecurity forensics laboratory may need to analyze forensic data, including malware samples, in a forensic database, without the possibility of that data being leaked or contaminating to other systems. In this case, the data diode is placed in front of the forensic database, and all other external connections are eliminated, mitigating data leaks and malware propagation.



And if the goal is to protect both networks, one-way hardware is typically applied at the security border of both the source and destination networks, creating a single, isolated path through which all data flows.

For example, a bank may have multiple branch offices, which each send data back to the corporate headquarters. The headquarters may also want to make sure that the data is not accessible to external sources. In this case, a data diode would be placed both at the edge of all branches, to allow data to be sent out and no access in, and also placed in front of the database at headquarters, to allow data in, but not out.



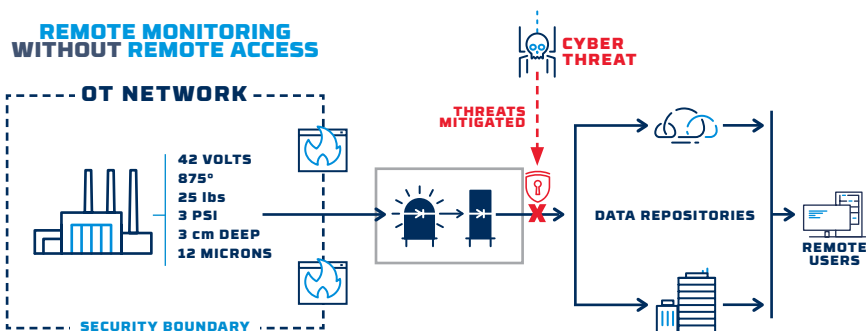
Data Availability

In many cases, data from inside a sensitive network is needed outside of the network in order to perform job functions. Data diodes transfer information across network boundaries from a source network to a destination network, without exposing additional attack surface or introducing possible threat vectors. Data from the source network remains available to external users and systems for monitoring, use, and analysis, but the source network itself is inaccessible to external cyberthreats.

Data diodes are perfectly suited for a variety of data availability scenarios, such as confidential file transfer, data streaming, database replication, remote system/sensor data monitoring, backup/disaster recovery, and patch/update management.

+ Remote Monitoring (without Remote Access)

Many believe that remote monitoring cannot be achieved without remote access to systems. However, as previously stated, if remote access is provided via an external two-way connection, then a threat vector is created. By utilizing data diodes, a high-security network, such as an oil and gas refinery, is secured by one-way transfer hardware, preventing all external access. Meanwhile the data required for remote monitoring, backup, or analysis is sent one-way to another network or the cloud, where end users and applications can access it as needed without compromising the integrity of the refinery controls.



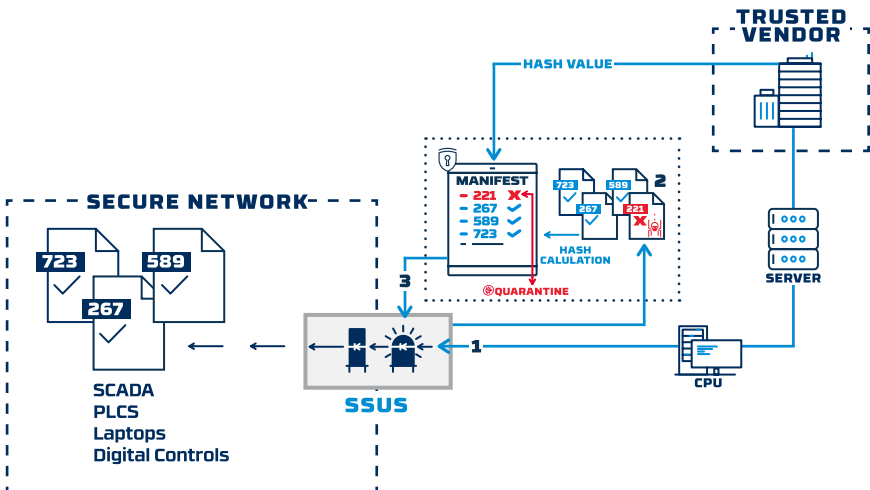
Operational data is securely transferred out of the secure OT network through a data diode to data repositories; allowing remote users to retrieve OT data without opening up the OT network to attack.

+ Software Updates

When software updates or patches need to be installed on equipment within a secured network, data diodes can be used to apply a variety of security policies to the software updates before transferring them into the secured network. This is similar to the approach that the DoD and Intelligence communities routinely use to thoroughly vet and then transfer data through data diodes from unclassified environments to secure enclaves.

Before the data diode performs the transfer, a number of user-defined security policies can be applied to the designated file. These policies include antivirus scanning, filtering, file type checking, ASCII checks, whitelisting, hashing algorithms, and others. Once the file has been vetted and approved, a single, isolated port (as recommended by the DHS²) is used to transfer the software update/patch across the data diode to the secure network. If the file does not pass the security policy check(s), then it is either automatically deleted or placed in quarantine.

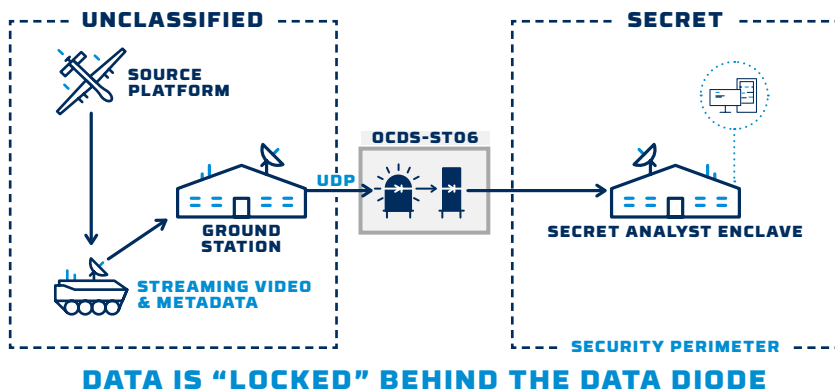
This method leverages the inherent security benefits of data diodes in combination with additional security and data assurance measures, providing a highly-controlled and verifiable method for data transfers from “low to high” security networks.



In this example, a hash code security policy is being used to validate and transfer a required software patch to the secure network. The IT department first downloads the software patch from the vendor and then independently obtains the hash code for that file and inserts it in a manifest on the data diode. The hash code for the file is calculated and compared to the value provided by the vendor in order to ensure that the file hasn't been tampered with or replaced. If the hash codes match, the file is transferred and installed, otherwise it is quarantined.

+ Cross Domain Solutions

In the US military and intelligence communities, data transfers from “low to high” or “high to low” security domains are performed for data availability. They utilize specially accredited and controlled cross domain solutions (CDS), which require the ability to send data from one security domain (e.g. Unclassified, Secret) to another domain of higher or lower security. This could be from a UAV in the field to a secure enclave, or from a soldier in the field to a ground station, or even from one secure network to another in the same building. These solutions enable data from one security domain to be available in another domain of differing security without compromising the source or destination. For more information on CDS products, see the Owl Cross Domain Solutions product brochure.³

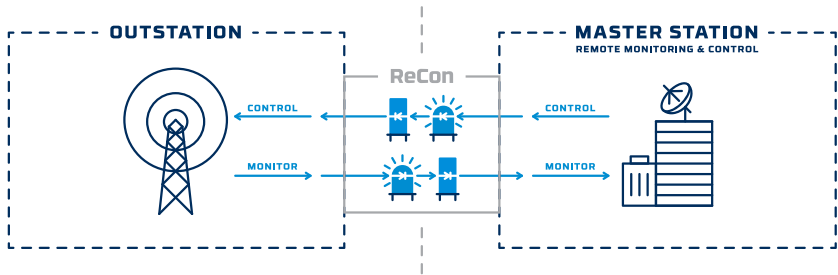


² https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S5o8C.pdf

³ http://library.owlcyberdefense.com/brochure_cross-domain-solutions

+ Bilateral / Bidirectional Transfers (ReCon)

Despite all of the security benefits of one-way data diode solutions, in many cases, limited bidirectional communication is still necessary for confirmation or command and control. In these cases, the U.S. Department of Homeland Security's guidance advocates using "a single open port over a restricted network path" to severely limit the attack surface. A bilateral solution includes two independent data diode one-way paths that permit a single, round trip session between pre-configured IP addresses: a one-way data transfer solution responsible for outgoing traffic, and another responsible for incoming traffic.



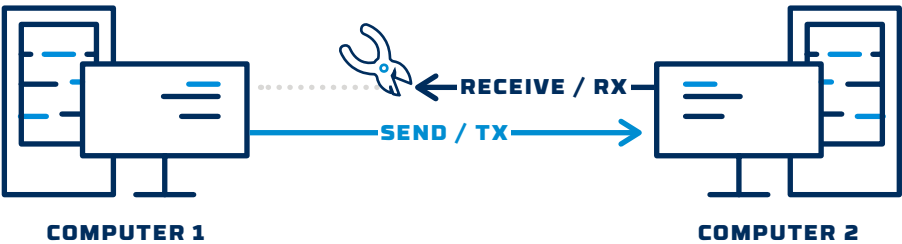
Taxonomy of One-Way Transfer Technologies

In making a decision on which one-way transfer technology is appropriate for the particular needs of your architecture and situation, it's important to draw a distinction between the various types that have been developed over the years. While these one-way technologies are often grouped together, they actually have a number of critical differences.

METHOD	EXAMPLES
One-Way Cable Assembly	RS-232 with clipped return line
Firewall-Enabled Policy	Box in the middle, UDP routing rules
Unidirectional Gateway	Two hardware devices (send/receive) with additional flanking server hardware for each side
Intelligent Data Diode	One-way system hardware with built-in electrical diodes and proxies (send/receive)

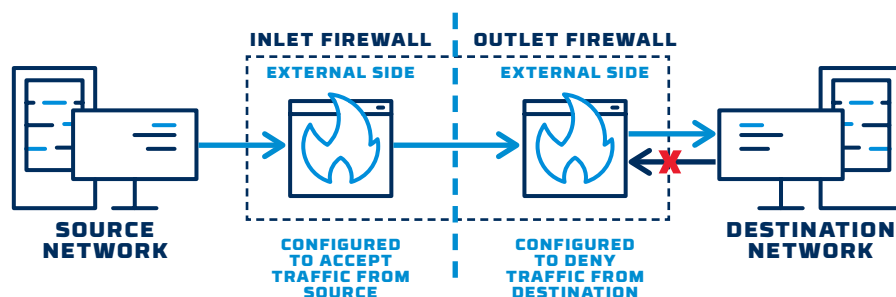
One-Way Cable Assembly

A data diode configuration can be as simple as a **one-way cable assembly**: a set of two transmit/receive cables connecting two computers, with one of the cables disconnected or clipped at one end. This leaves the two computers with a single connection over which only one computer can transmit, and the other can only receive.



Firewall-Enabled Policy

This form of one-way transfer relies on software configuration, which is not inherent in what most would consider a data diode, as data diodes are almost always hardware-enforced devices. **Firewall-enabled policy** refers to an implementation of one or more firewalls configured to transfer data in only one direction. While a single firewall may be configured to enforce a one-way data transfer, a pair of firewalls configured back-to-back provide a more secure implementation, as each firewall presents their external faces to separate isolated networks.

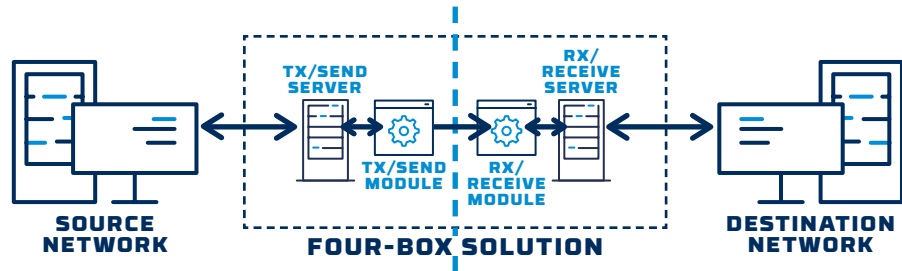


Unidirectional Gateway

A **unidirectional gateway** includes dedicated separate send and receive hardware with a single connection between them with the addition of proxy computers on each side (one send and one receive). These proxy computers typically operate independent of the data diode and are often configured separately. As unidirectional gateways operate using two-way protocols, the purpose of these proxies is to assist the send and receive hardware in negotiating the one-way data transfer – transmitting packets, identifying packets received, and rebuilding the packet stream to try and match the original stream. They also deal with the networks on either side of the unidirectional gateway, sending and receiving the expected confirmations and handshakes.

These complex solutions are configured with the requisite flanking servers and the dedicated send and receive boxes – one for the send side proxy server, one for the send side of the data diode, one for the receive side of the data diode, and one for the receive side proxy server, for a total of four devices. All of these devices are then connected together. Because the proxy servers essentially operate independent of the data diode, all configuration and administration of the solution is performed on them, while the data diode hardware itself functions purely as the pathway for the one-way transfer.

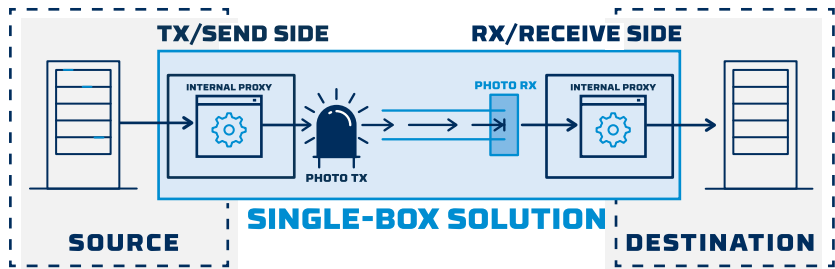
Notably, for each data flow or data type to be transferred (files, streaming data, database replication, etc.), a full set of devices is needed. The nature of the device does not allow for multiple, simultaneous data streams or data types to be transferred.



Intelligent Data Diode

The most advanced form of a data diode is an “**intelligent data diode**”. This purpose-built, hardware enforced, one-way transfer system, builds the one-way security policy of a diode into every facet of the device. Intelligent data diodes include two electrically isolated diodes (one for sending, one for receiving) which maintain physical separation of source and destination networks. The send side diode is inherently incapable of receiving data from the receive diode. While the receive side data diode is incapable of sending data back to the send side; ensuring secure one-way-only data transfer. The intelligent data diode uses a purposely designed non-routable one-way protocol to transfer data from the send side to the receive side. It is built on a fundamental one-way-only design that is hardware enforced and coupled with hardened, built-in proxy servers for high reliability and low latency.

Intelligent data diode design is typically composed of a single enclosed device with all one-way transfers occurring safely inside, to help prevent tampering and reduce the size, weight, and power (SWaP) requirements of the solution. They do not require any additional hardware or flanking servers to operate, and support multiple data flows, protocols, and data types simultaneously through the single device.



Comparing One-Way Transfer Technologies

It can be difficult to draw conclusions on new technology when you don't know what to look for. Below are some of the key differentiators among the four major categories of hardware-based one-way transfer technologies, along with an explanation of their significance in practical use.

Security

The level of security provided by the device, and its inherent risk of data breach. Determines whether the device can be used in very high security implementations.

+ Cable Assembly

The physical one-way link configuration cannot be hacked (with software). However, as with any cable assembly architecture, a change in cable arrangement, whether accidental or intentional, defeats the security policy. These solutions also provide no capabilities for security policy enforcement.

+ Firewall-Enabled Policy

Due to their commodity nature and high degree of configurability, not to mention the inherent vulnerabilities of software-based solutions, firewalls require skilled resources to implement and maintain them. They are particularly prone to probing and malware attacks, as well as zero-day exploits of software flaws, and are completely reliant on policy, which can be changed. If a malicious actor is able to find even one port, default user/password, or protocol that is permitted to pass through the firewall, they can open up an ever-increasing number of avenues of attack, until the firewall is completely defeated.

+ Unidirectional Gateway

The fundamental architecture of the one-way transfer is hardware-based, preventing access to the source network from the destination network. However, unidirectional gateways utilize a routable protocol and all configuration takes place in separate flanking servers, which may make them vulnerable to reconfiguration.

+ Intelligent Data Diode

The hardware-based nature of this configuration, enforced by the fundamental laws of physics, places it at the highest possible level of security, short of complete physical separation. It cannot be hacked or reconfigured to change its core functionality. It can be used to secure the source network from the destination network and vice versa.




Connection

How the solution is connected and what type of hardware is utilized. Determines how the solution communicates between sending and receiving sides of the one-way transfer, as well as communication between each side of the solution to the source and destination.

+ Cable Assembly

A one-way cable assembly, typically derived from a two-way cable that is rendered one-way by disconnecting or clipping the return line, and no supporting proxy servers.

+ Firewall-Enabled Policy

Firewalls communicate directly through Ethernet cables. The source traffic is typically filtered and/or inspected before being passed on to the destination. Destination to source traffic is disabled by software policy, rather than a physical restriction.

+ Unidirectional Gateway

A one-way fiber optic cable between the send and receive devices, each of which are connected to two separate, additional proxy servers to help negotiate and manage communication errors with source and destination networks. Due to multiple transfers across the various devices, and the lack of a true one-way methodology and protocol, transfers are erratic and often must be performed multiple times.

+ Intelligent Data Diode

A one-way fiber optic cable between two electric diodes in a single enclosure. Proxies are built-in and designed to handle all communication with the source and destination networks, including conversion of two-way protocols to one-way protocol (and one-way back to two-way). This purpose-built architecture allows it to achieve reliable, consistent transfers.



Protocol

How the solution communicates between the sending and receiving sides of the one-way connection. Determines efficiency, dependability, and assurance of transfer.

+ Cable Assembly

No change to existing protocol – almost always a two-way protocol sent over the disabled two-way cable, which functions as a one-way connection. Results in errors from the broken two-way protocol forced to operate in a one-way fashion. No assurance of correct or completed transfers.

+ Firewall-Enabled Policy

Utilizes the two-way protocols for which they are configured. While traffic is not passed in more than one direction (from source to destination), the firewall itself inherently communicates bidirectionally.

+ Unidirectional Gateway

No change to existing protocol – almost always a two-way protocol that functions over the one-way connection. Results in errors from the broken two-way protocol forced to operate in a one-way fashion, and necessitates retransmission of packets. No assurance of correct or completed transfers.

+ Intelligent Data Diode

Converts all incoming protocols to a purpose-built one-way protocol for transfer across the data diode. After transfer, it converts the data back to the original protocol. Packetized transfer ensures completion and accuracy in a single transfer. Highly reliable, stable, and efficient.

Routability

The inclusion or exclusion of network address routing information in the transfer. Determines whether the data transfer can be routed to another destination and compliance with requirements for non-routable transfers.

+ Cable Assembly

The routable two-way protocol contains all routing information, including network and device addresses, which can be re-routed to any other destination.

+ Firewall-Enabled Policy

As an inherently two-way device, firewalls utilize routable two-way protocols that contain all routing information, including network and device addresses, which can be re-routed to any other destination. Cannot be used in any scenarios requiring one-way-only devices.

+ Unidirectional Gateway

The routable two-way protocol contains all routing information, including network and device addresses, which can be re-routed to any other destination.

+ Intelligent Data Diode

The non-routable one-way protocol does not include any identifying network information (IP addresses, ports, etc.) ensuring that the source network is opaque to the destination network and the outside world (the internet) . Transfers are deterministic and must be preconfigured locally on the device through a separate access point.



Reliability

The degree of integrity and level of accuracy of the data on the receiving side of the one-way transfer.

+ Cable Assembly

Data transfers occur blindly and without any controlling mechanism. Thus, transfers are highly unreliable and cannot be assured.

+ Firewall-Enabled Policy

As “pass-through” devices, firewalls are highly reliable in data transfer accuracy.

+ Unidirectional Gateway

Due to the lack of a confirmation mechanism, data transfers are unreliable and cannot be assured. As a result, data packets must be transmitted multiple times and reconstructed to ensure complete, accurate transfers. The reconstruction process means these solutions cannot support multiple simultaneous data flows or data types.

+ Intelligent Data Diode

Data flows are highly reliable and assured through packetized transfer with sequenced headers. As a result, these solutions can support multiple data flows and data types simultaneously with near absolute data assurance and integrity.



Latency

The delay from the sending to the receiving of the data during a one-way transfer.

+ Cable Assembly

There is usually no restriction or added processing on data transfers, so these devices have near zero latency.

+ Firewall-Enabled Policy

Even with the highest performing firewalls, complex rule sets, added filters, inspections, and other processes all introduce significant latency on transfers.

+ Unidirectional Gateway

Requires multiple packet transmission attempts to complete a single transfer, introducing significant latency and limiting performance potential.

+ Intelligent Data Diode

The protocol conversion and packetized transfer method introduces minimal latency. Most transfers occur within 2 milliseconds.

Throughput

The bandwidth capability of the one-way transfer solution hardware, as well as the ability to transfer multiple data types/streams simultaneously.

+ Cable Assembly

While there is technically no limitation on the throughput or data types in the basic data diode, the extreme unreliability of the solution may result in many attempts to complete one transfer, so throughput should be conservatively considered low overall.

+ Firewall-Enabled Policy

Throughput is generally high, although it is highly dependent on the rule sets implemented and other filters and inspections taking place within the firewall. It can transfer any number of data types/streams simultaneously.

+ Unidirectional Gateway

The required multiple attempts to complete a single transfer reduces potential throughput and eliminates the capability of multiple simultaneous transfers or data types.

+ Intelligent Data Diode

Maximizes potential throughput with one-way specialized protocol, capable of transferring at a full line rate of 10 Gbps. Can process and transfer multiple data types/streams simultaneously.

Form Factors & Configurations

Typical configuration and components of the solution.

+ Cable Assembly

Usually a pair of cables with one return clipped or disconnected.

+ Firewall-Enabled Policy

Most often firewalls are software devices, although there are also hardware devices that are single box solutions. Requires heavy configuration and on-going maintenance by specialized resources.









+ Unidirectional Gateway

Requires multiple devices per solution, on the order of four or more boxes, sometimes packaged together in a rack-mounted cabinet. The two transfer hardware boxes are usually connected by a single exposed fiber optic cable susceptible to tampering.

+ Intelligent Data Diode

There are a variety of form factors, most solutions are single enclosure, including standard 1U size boxes and DIN rail compatible boxes. Some solutions consist of two separate PCIe cards (installed in commercial servers) connected by a fiber optic cable.

Technology Comparison Chart

		CASE ASSEMBLY	FIREWALL ENABLED POLICY	UNIDIRECTIONAL GATEWAYS	INTELLIGENT DATA DIODES
	CONNECTION	Simple one-way connection	Software-configured one-way connection	One-way connection with support servers	One-way internal connection
	PROTOCOL	Two-way (Broken)	Two-way	Two-way (Broken)	Two-way (w/Conversion)
	ROUTABILITY	Routable	Routable	Routable	Non-routable
	RELIABILITY	Very unreliable	Very reliable	Unreliable	Very reliable
	LATENCY	Low	High	High	Low
	THROUGHPUT	Low	Moderate	Low	High
	FORM FACTOR	Case assembly	Software or single box	4+ devices	Single box or two cards

Data Diode State of the Art

One-way data transfer systems present a unique set of technical and policy challenges, most of which are related to the absence of any form of transfer acknowledgement. However, the value provided by the absolute assurance of hardware-based cybersecurity tools is clearly unmatched by any software-based cybersecurity. For these reasons, the highest performance, reliability, and security are presented by the systems with intentionally designed one-way hardware: intelligent data diodes.

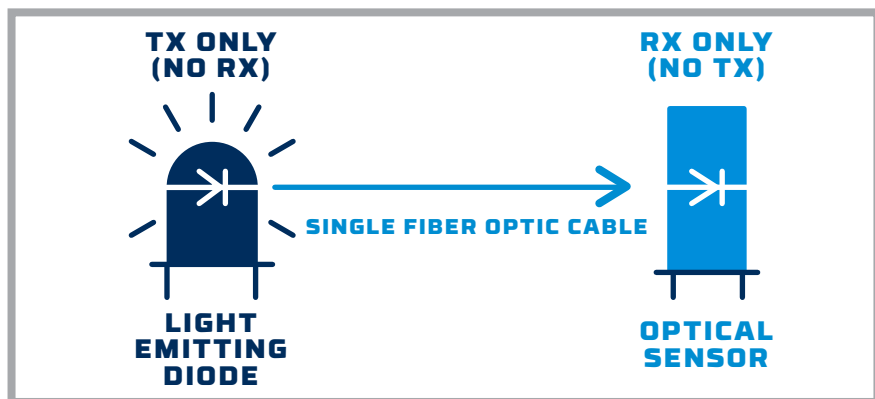
Representing the “state of the art” in data diode technology, intelligent data diodes provide a number of economic and quality-of-service advantages over competing technologies.

Physical Design

All of the components and architecture in intelligent data diodes are designed to be one-way from the ground up. This starts with circuitry that allows data to physically flow in only one direction. The design includes two electrical diodes, one on each of the send and receive sides, which enforce the one-way-only flow throughout the device. This architecture enables fast, reliable data transfers with very low latency.

The basic functionality inside an intelligent data diode is fairly straightforward. Data travels on a one-way path between two embedded computing platforms connected by a single transmitter and receiver – typically an LED and a photodetector connected by a fiber optic cable. Data is transmitted in the form of light by the LED through the fiber optic cable and received by the photodetector on the other side.

Though they are connected solely through the single one-way connection, the send and receive sides are otherwise physically separated, with no shared circuitry and no ability to transfer data bidirectionally, creating what is commonly referred to as an effective “air gap.”



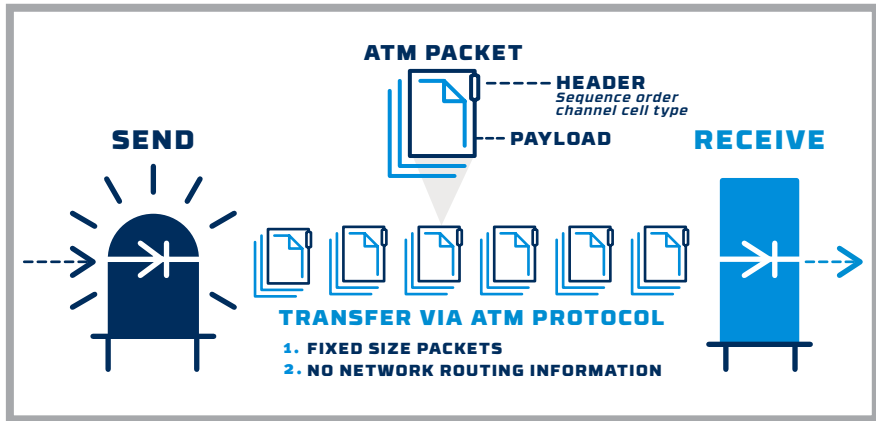
Intelligent data diodes also feature separate power supplies, fans, and administration ports. Each side of the data diode is administrated separately, and there is no shared routing information, administration, or configuration between the two sides.

One-Way, Non-Routable Protocol

In order to transfer data in only one direction, intelligent data diodes utilize a one-way protocol, based on Asynchronous Transfer Mode (ATM). Rather than attempting to use or modify protocols designed for two-way communication (e.g. User Datagram Protocol [UDP], Transmission Control Protocol or Internet Protocol [TCP/IP]) to make them work in a one-way fashion, the purpose-built ATM-based protocol provides a far more reliable means to transfer data one-way across the data diode.

ATM was developed by the telecommunications industry for the high speed, low latency requirements of one-way, real-time voice communications. It encodes data into fixed-size packets for consistent, reliable data transfer, without the need for receive-side confirmation. This consistent packet transfer method is ideal for a connection that must handle both low-latency content (video, voice, etc.) and high-throughput data (files, directories, etc.). It can flawlessly transfer data without multiple sending attempts or bidirectional communication.

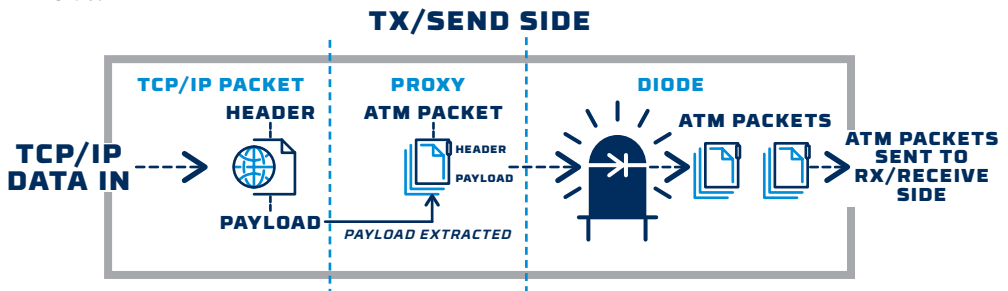
The ATM protocol also provides a non-routable solution, which is required by many electric utility installations. Two-way to ATM protocol conversion has the unique benefit of hiding all the IP and MAC address information from the outside world and preventing any probing of the network. This is very different than other solutions that pass the original packet stream through the solution, allowing the network's routing information to be exposed.



Protocol Conversion & Payload-Only Transfer

Converting the data from a two-way protocol to ATM involves extracting the payload from the originating protocol packet by the send side proxy. This process adds another layer of defense by stripping away all of the protocol and routing information, and then inserting the data “payload” into ATM packets for transfer.

This conversion mitigates any malware or exploits that rely on attributes of the original packet protocol (TCP, UDP, etc.), as none of the source routing information is sent across the data diode, and new packets with new routing information are created on the receive side.

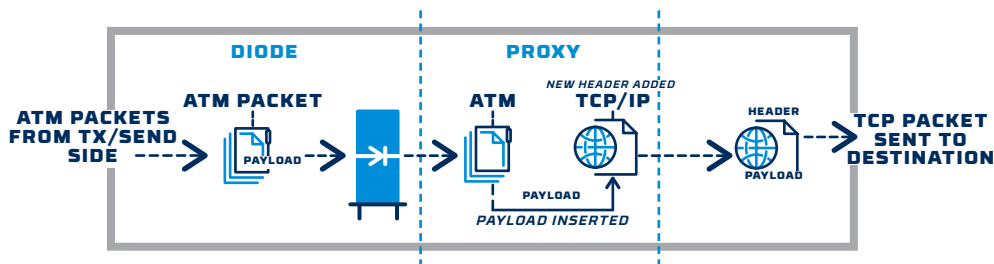


Assured Delivery

When learning about intelligent data diodes, people often ask, “How does the send side know the data reached the receive side?” Because it’s physically impossible to send a confirmation back to the send side from the receive side, assured delivery in intelligent data diodes changes the paradigm to put the onus on the receive side.

In order for the receive side to be assured that it has received all the data (and to raise an alert if it doesn’t), each ATM packet receives a sequenced identifying header on the send side, utilizing a unique hashing sequence. This enables the receive side to verify accurate receipt of the data set.

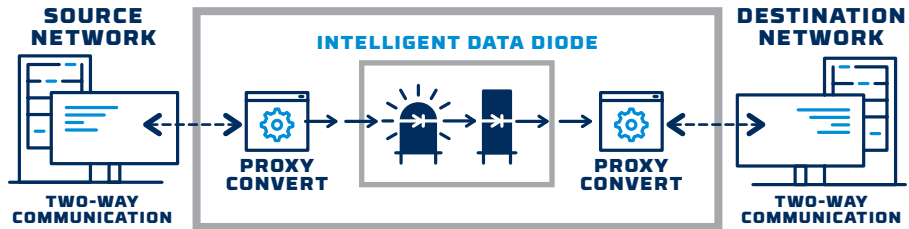
Once transferred, the receive side reconstructs the payload in sequence, and then places the payload back into a packet corresponding to the original protocol. From this point, the data is either transmitted to its intended destination using a new two-way session with the endpoint, or stored on the receive side of the diode for pickup by an application or user.



One-Way in a Two-Way World

A successful one-way data transfer also requires meeting the expectations of a two-way world. A majority of network traffic involves some sort of acknowledgement or two-way connection in order to function (an obvious exception is UDP). The “secret sauce” of the intelligent data diode is in providing a one-way transfer, with a true separation between source and destination networks, while maintaining simultaneous two-way communications with both the source network and the destination network to avoid disruption. This is accomplished through the use of proxies running on each side of the intelligent data diode.

The send side proxy communicates with the source network acknowledging receipt of packets before extracting the payload and sending it across the diode. On the receive side, the proxy receives the payload, builds a new packet around it using the original protocol and sends the data on its way over the two-way protocol. In this way, the data diode achieves a one-way transfer in the middle of two two-way exchanges.

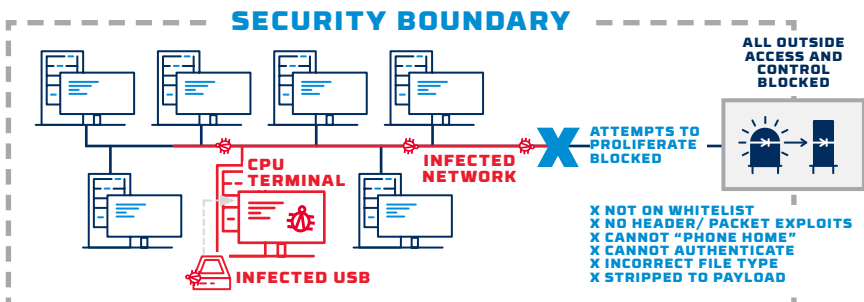


Prevention of Malware Proliferation

In addition to preventing attackers from gaining access into the segmented network, intelligent data diodes can prevent threats introduced locally, e.g. via portable media, from getting out of the network. All transfers through the diode are deterministic and payload-only, due to the conversion to the non-routable ATM protocol.

Intelligent data diodes feature two routing tables (one on each side) that are blind to each other, so malware on the inside cannot be directed to a specific destination. The malware would also need to spoof a valid protocol and port combination that is on the whitelist.

This means data transfers out of the source network cannot be hijacked, and prevents malware from proliferating across network boundaries, “phoning home,” or exfiltrating data through the intelligent data diode.





Owl Intelligent Data Diode

As the world leader in intelligent data diode technology, Owl has spent over 17 years designing, developing, and refining data diode technologies, consistently well ahead of any other competing solution. While it's important to recognize that data diodes are one piece of a larger defense-in-depth strategy, many of the benefits of Owl intelligent data diodes are unique, and can play a significant role in helping organizations to defend against the ubiquitous threat of bad actors infiltrating sensitive networks.

Unmatched Performance

Owl solutions feature transfer rates at up to an industry-leading 10 gigabits per second, with a packet transfer latency of 2 milliseconds or less. In addition, the reliability, high bandwidth, and low latency of Owl solutions means packets never require retransmission, creating a highly tuned and optimized solution with zero data loss when operating within the specified bandwidth rate.

Scalable & Upgradeable

Owl intelligent data diodes offer the exclusive ability to increase bandwidth capacity using a simple software license key. Users can purchase a product with bandwidth to meet today's needs with the knowledge that it can be quickly and easily increased at any time to meet future requirements. Owl products also feature expandable transfer capabilities, allowing new protocols and interfaces to be added to existing solutions. A single Owl data diode solution can support multiple interfaces, protocols, and data flows without having to add new hardware.



Multiple Form Factors

Operational networks take many forms, from industrial DIN rail cabinets to generic IT server racks. Owl has designed intelligent data diode products that integrate easily into nearly any existing environment.



OPDS-100

Owl Perimeter Defense Solution-100

Owl's standard, all in one, 1U rack-mountable DualDiode cybersecurity platform, designed to address critical infrastructure applications requiring low to moderate data throughput. The OPDS-100 delivers scalable performance from a base of 10 Mbps up to 104 Mbps, easily upgradeable through Owl's variable bandwidth licensing mechanism.

OPDS-100D

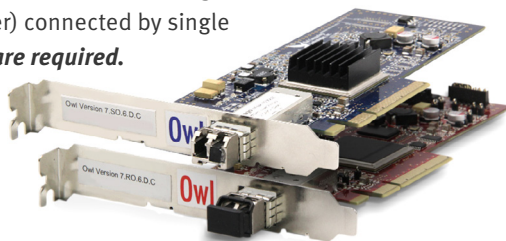
Owl Perimeter Defense Solution-100D

Optimized to meet the needs of most industrial control applications, the OPDS-100D delivers scalable, deterministic one-way transfer capabilities from 10 Mbps up to 104 Mbps. Designed specifically for low size, weight, and power (SWaP) requirements, the compact form factor is DIN rail mountable and readily deployable in plants, substations, and other CI facilities.



Owl Communication Card Kits - Version 7

PCIe Card Kit solutions –installed in two new or existing servers (one send server, one receive server) connected by single strand fiber cable. **No other hardware required.**



+ Lowest Total Cost of Ownership

Owl solutions have the lowest total cost of ownership of any comparable network cybersecurity appliance, aligning with that of other popular perimeter security technologies, such as firewalls.

Owl intelligent data diodes feature extremely low ongoing operating expenses, and a highly reliable, long lifespan with a minimum mean time before failure (MTBF) of over 10 years. Owl offers a range of solutions to meet different requirements, environments, and budgets, including entry level, all-inclusive solutions starting at under \$6,000.

+ Tested & Accredited

Owl intelligent data diodes have received a number of certifications and recommended uses. These include: OPC Foundation, Common Criteria (EAL), NERC CIP, NRC, NIST, U.S. Department of Homeland Security, and more.

+ Multi-Functional with Broad Support

Hundreds of sources and destinations can be supported by a single Owl intelligent data diode solution. Each device is capable of supporting multiple simultaneous data flows within multiple protocols (TCP, UDP, files, OPC, Modbus, etc.) of nearly any data type. In cooperation with our technology partners, Owl products also feature seamless integrations with a variety of common databases, historians, HMIs, and other interfaces.

+ Long lasting & Durable

All Owl solutions are built to last, with all components tested and validated at over 10 years MTBF, far exceeding any typical commercial enterprise computing platform lifespan. This is especially important in industrial environments where systems are operational 24x7 with limited maintenance windows. Specialized solutions designed to operate in tactical or extreme environments (high/low temperature, heavy smoke, dust, etc.) are also available.

+ Defense-in-Depth Built In

Recognizing the strengths of the “defense in depth” strategy for protecting networks and other data systems, Owl also built layers of defense into the data diodes themselves. Security features include:

- Secure operating system – implemented per government operating specifications.
- Role-based access controls (RBAC) – supports long passwords and passphrases.
- Menu-based interface – prevents access to command line when operating.
- Secured against tampering – system check audits the system for any file changes, automatically shuts down if tampering occurs.
- Internal logs and alarms – stored on the system to track and audit all activity.
- Supports separation of duties – administration ports separated from data transfer ports.



Conclusion

Though one-way data transfer technologies have long been considered a niche, specialty, or prohibitively expensive cybersecurity device, the intelligent data diode transcends many of the stereotypes placed upon its less advanced forebears. Easy to implement and configure, extremely fast and reliable, rarely requiring changes or replacement, and easy to audit, they help to achieve the cybersecurity goal of any organization to reduce the most risk for the least resources consumed.

Intelligent data diodes are now present in government, military, critical infrastructure, financial services, healthcare, transportation, telecommunications, and more. The unhackable nature of hardware-based enforcement, combined with new innovations for greater efficiency, flexibility and performance, have made intelligent data diodes an effective and cost-effective piece of the defense in depth strategy for many organizations in a variety of industries.

Organizations are increasingly looking to intelligent data diodes to secure or augment their cybersecurity architectures to minimize or neutralize the attack surface of sensitive networks, prevent network probing, and mitigate external threats, while preserving data availability to authorized users for monitoring, use, analysis, and backup.

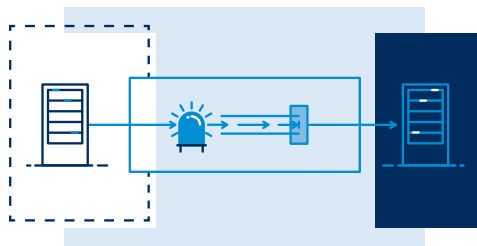
Intelligent data diodes are now being developed for small office environments, as well as miniaturized versions as small as a quarter. Going forward, this advanced intelligent data diode technology will enable network segments to get smaller, providing better security. Segments could be as small as a single digital controller on a turbine, the control systems in a crane at construction site, a car going down the highway, or even small enough to defend a medical device like a pacemaker.

As the Internet of Things expands, security must also advance to protect our networks and devices from potential cyberthreats. The new generation of intelligent data diodes hold great promise to help organizations and individuals protect themselves in the new era of an increasingly connected world, and we may have only scratched the surface of their potential.

For more information on Owl intelligent data diode solutions, visit www.owlcyberdefense.com

What is a Data Diode?

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 and prevent penetration from any external sources. A data diode sits at the edge of the network security perimeter; relying on its physical hardware components to mitigate all network cyber threats against the network while simultaneously allowing the transfer of data out of the network in a highly controlled, deterministic manner.



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

