

Why Owl Data Diodes? (14 Value Propositions)

As is normal in commercial markets, competition arose and along with it some confusion about what a data diode is, how it works and what distinguishes one from another. This document identifies and clarifies some of the typical points of confusion between an Owl data diode and other products on the market such as a unidirectional gateway.

By way of introduction, the fundamental difference between Owl products and others is the one-way design implemented from the ground up, true single box format, exclusive use of intentional one-way techniques (not disabled or broken two-way methods), hardware based solution, very high reliability, super low latency and very long expected life span (11+ years).

Owl Computing Technologies, established in 1999, was the first to market with a data diode and has over 28 patents on the technology with a half dozen more pending. The design of the Owl data diodes was carefully considered to ensure everything was designed to defend against cyberattack and provide a robust and reliable data transfer mechanism.

The various attributes described below provide more detail on how Owl data diodes differ from competing products and why they offer a better value proposition.

1. One-way by Design

- All of the components and circuitry are designed to be one-way. Owl data diodes are not based on inherently two way components or protocols that are subsequently compromised to only work one-way. They are designed to be one-way from the ground up.
- The design includes two one-way diodes working as a pair (one send, one receive) and provides a tested, proven and accredited deterministic one-way only transfer.
- Owl data diodes use an Asynchronous Transfer Mode (ATM) based, one-way protocol to move data. ATM was designed to support high bandwidth, low latency one-way data transfers used in real-time telecommunications.

2. Secure Communication

- Payload only transfer - no original header information is transferred, thwarting any attacks originating in the packet itself.
- Non-routable data transfer - due to the payload only transfer, all routing information (IP address, etc.) associated with the originating network protocol remains secure within the source network and does not cross the data diode. In competing products the full original packets are transferred and the routing information is exposed outside of the protected network.
- Protocol conversion - in a precise sequence, the data payload in the originating protocol (TCP, UDP, etc.) packet is extracted, placed in an ATM packet, sent across the data diode, extracted from the ATM packet and inserted into a new packet that matches the original protocol and routed to the final destination.

3. Physically Secured

- Fully enclosed, single chassis
- No exposed cables or wires
- Tamper-proof screws
- Locking mechanism

4. Complete Separation of Source and Destination Networks

- Physical separation – Two data diodes embedded within the Owl data diode create a physical demarcation point between Source and Destination networks. Connected solely through the single one-way connection, the send and receive sides are otherwise physically separated, creating what is commonly referred to as an “air gap”. This airgap is a requirement of certain power industries (NERC, NRC) and the Owl data diode helps operators meet those regulations.
- Separate power supplies – one for the source side and one for the destination side.
- Separate fans – one for the source side and one for the destination side.
- Separate VGA and USB connectors – one for the source side and one for the destination side
- Separate admin ports – one for the source side and one for the destination side.

5. Unmatched Performance

- Fastest throughput - Owl solutions range from 5 Mbps up to industry leading 10 Gbps.
- Extremely low latency – packets are transferred across the data diode in less than 9 milliseconds.
- Zero data loss – the system is highly tuned and optimized to operate without packet loss within the specified bandwidth tier. There is no reason why packets would ever be dropped or lost.
- Single packet transmission – the reliability, high bandwidth and low latency of the design leads to single packet transmission. Competitive solutions rely on a strategy of multiple packet transmissions to ensure the data is transferred, lowering throughput, increasing latency and preventing multiple data flows from crossing a single solution.

6. Unparalleled Scalability

- Variable Bandwidth Licensing - Owl offers the exclusive ability to increase bandwidth capacity using a software license. Customers can purchase enough bandwidth to meet today’s needs with the knowledge that bandwidth can be quickly and easily increased at any time to meet future requirements.
- Expandable transfer capabilities - New protocols and interfaces can be added to existing solutions using a simple software license. A single Owl data diode solution can support multiple interfaces without having to add any new hardware.

7. Multiple Form Factors

- **Exclusive single box solutions:**
 - a. Full functionality embodied in a single device
 - b. No flanking servers required
 - c. Physically secured against tampering
 - d. Low SWaP (Size, Weight and Power) requirements
 - e. Configurations available for environmental extremes (temperature, smoke, dust)

Available in either:

1. 19” 1U rackmount solutions – horizontal rack solutions for enterprise IT environments
2. DIN rail solutions - compact, vertically mounted for industrial environments

- **PCIe Card Kit solutions:**

- a. Two server solution: one send card, one receive card
- b. Installed in two new or existing servers (one send server, one receive server)
- c. No other computing platforms (flanking servers) needed.
- d. Connected by single strand fiber cable.

☰ Proprietary Algorithm

Owl utilizes a proprietary, patent-pending database query algorithm to perform extremely reliable, real-time database replication between source and destination networks. For example, Owl data diodes could replicate data from a high security source database to a read-only (for users) database on a different security domain, thereby protecting the sensitive source network from cyberattack, while still allowing users on the lower security network limited access rights to the data. This technology has also been recently tested and verified for use with Oracle GoldenGate software.



8. Tested and Accredited Solution

- Tested & proven technology in use for 17 years
- Common Criteria EAL certified, independent 3rd party testing verified Owl Dual Diodes:
 1. Are hardware enforced one way devices.
 2. Maintain network security if a device failure occurs.
 3. Cannot be altered through software modifications.
 4. Perform a non-routable protocol conversion - maintaining the confidentiality of the protected network domain.
- UCDSMO Baseline-listed (Authorized, Accredited and Approved to operate in DOD and Intelligence community networks).
- Recommended by DHS to protect critical infrastructure.

9. Lowest Total Cost of Ownership

- Range of solutions available to meet different requirements and budgets.
- Entry level solutions start at \$6000 for an all-inclusive, single appliance solution.
- Shipped pre-configured and ready to install (most customers install it themselves).
- Extremely low on-going operating expenses - Set it and forget it.
- Highly reliable, long lifespan hardware - MTBF > 11 years.
- Supports multiple interfaces, protocols and data types simultaneously on a single box.

10. Multi-Function Solutions

- Hundreds of sources and destinations can be supported by a single solution.
- Support multiple simultaneous data flows.
- Supports the transfer of multiple protocols (TCP, UDP, Files, OPC, Modbus, etc.) simultaneously. Resulting in lower cost per supported application.

11. Defense in Depth Built In

- Secure operating system implemented per US 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 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 - admin ports separated from data transfer ports.



12. Long-Lasting and Durable

- Industry leading MTBF - full system tested to 11+ years mean time before failure (MTBF) of any component.
- Far exceeds any typical commercial enterprise computing platform lifespan.
- Full support for Active/Standby configurations.
- Specialized solutions designed to operate in environment extremes (high/low temperature, heavy smoke, dust, etc.).
 - a. Sealed, fan-less operation
 - b. -40°F to +140°F

13. Fast and Easy Deployment

- All single-box solutions come preconfigured and ready-to-install
- Minimal time to install – typically up and running within a few hours
- Most customers require no onsite assistance for deployment
- “Set it and forget it” – once installed solutions require little to no on-going support or maintenance

14. DualDiode Technology

Operating as a single data diode solution, Owl's solutions all utilize the patented DualDiode technology comprised of a pair of diodes. The pair of dedicated diodes (one send, one receive) are Common Criteria EAL tested and proven to provide deterministic, one-way only data transfers. The send diode circuits are designed to only allow data to be sent, with no physical capability to receive data. The circuits of the receive diode are designed to only receive data and are physically prevented from transmitting data.

The DualDiode technology exists in three formats: a pair of PCIe cards, a pair of PC/104 cards and a single, proprietary silicon board with two independent, fully separated sides.

Use:

- PCIe card solutions are installed in separate off-the-shelf servers, creating a send server and receive server as a complete data diode solution.
- PC/104 card solutions are components used within the Owl high-end, single appliance solutions. Provides a single box solution with independent send and receive elements within a single enclosure.
- The patented, single board solution is used in single box solutions that support lower bandwidth requirements and smaller physical size.

For the patented, “World's Smallest Data Diode”, the printed circuit board is designed with three zones: a send zone on one half of the board where only send components exist, a receive zone on the other half of the board where only receive components exist and a neutral zone in between that separates them. No components exist in the neutral zone and no electrical connections cross the neutral zone. Data is transmitted from the send side to the receive side using a one-way only digital isolator. Only digital differential signals cross from one side to the other, completely isolating the send side from the receive side.

Conclusion

From the world's fastest, to the world's smallest, a technical understanding of the design employed by Owl illuminates the differences and benefits of the Owl data diode over other solutions that may seem at first glance to be similar. The intentional use of one-way technology from the ground up allows Owl data diodes to operate at the highest speeds, with the lowest latency and superior reliability. Able to easily handle multiple data flows, data types and protocols simultaneously, while competitive products need one solution per data type, protocol or data flow, in combination with Owl's long service life and small footprint, provide the best return on investment.

About Owl

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

With over 2000 deployments globally, data diodes from Owl Computing Technologies enable hardware-enforced network segmentation and deterministic, one-way transfer of all data types and file sizes. USA owned and operated, Owl offers validated and accredited products, serving the intelligence, military, and government communities, as well as critical infrastructure, industrial and commercial organizations.