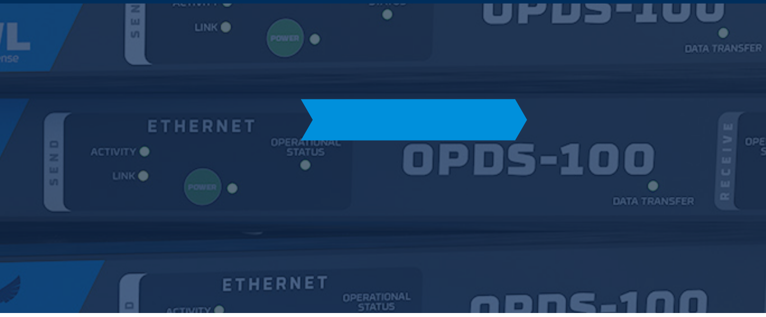
OWL Cyber Defense



Data Diodes and “Unidirectional Gateways”

MAKING AN INFORMED DECISION

Controlling the flow of data between a high security network and a lower security network is a must-have capability for military, intelligence, and critical infrastructure operations. Data diode technology is the most effective and efficient option for achieving this goal, whether data must travel in one direction or two.

Some vendors whose products lack the capabilities of true data diodes—for example, the ability to provide secure two-way communication—position their products as “unidirectional gateways” and attempt to describe their limitations as advantages.

Data Diodes: Secure by Design

Data diodes allow data transfer in only one direction and cannot be altered. For use cases that call strictly for one-way communications, such as outgoing data from a nuclear energy facility, data diodes are the only acceptable technology.

For use cases that require bidirectional communication, data diodes can be used in pairs, with inalterable controls over the types of data that are permitted to travel in each direction. This approach provides equal security, with simpler implementation and management, than any solution based on unidirectional gateways.

Unidirectional Gateway: What’s in a Name?

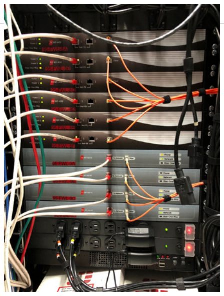
The term “unidirectional gateway” was coined to describe network security technology that does not meet Evaluation Assurance Level certification standards for true data diodes.

Products sold as unidirectional gateways can be any combination of hardware and/or software, with varying levels of sophistication. One thing they all have in common is that they are based on technology that was initially designed to allow simultaneous two-way communication. Data diodes, on the other hand, are based on technology that is inherently one-way and cannot be compromised.

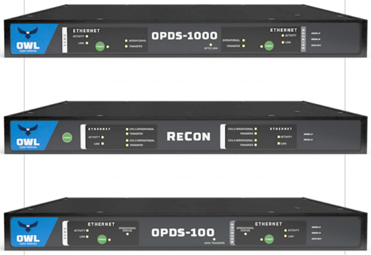
Data Diodes vs Unidirectional Gateways: Side by Side

A US-based critical infrastructure operator recently chose to replace their cumbersome, hard-to-maintain “unidirectional gateway” system with an Owl data diode solution.

The existing gateway solution consisted of ten components, with additional supporting equipment. With only three Owl components—an OPDS-1000, ReCon, and OPDS 100—the customer was able to achieve the highest possible level of security for its data, while reducing costs and resource demands.



Unidirectional Gateways



Owl Data Diodes

Data Diodes: Fact vs Fiction

Vendors whose products compete with data diode technology often try to create confusion about how diodes work and how they compare to “unidirectional gateways” or other approaches.

Here are some actual quotes from other network security providers, and the truth behind them.

FICTION

“Sometimes the entire solution – both diodes and both hosts – are wrapped up in a single hardware box. A copper wire comes into the box, a copper wire goes out, and there is ‘diode magic in the middle.’”

FACT

Data diodes are not magic—they’re a proven technology that has been in use by military, intelligence, and critical infrastructure organizations for three decades. Owl provides detailed information on the architecture and functionality of our diode solutions.

Packaging two data diodes in a single hardware box, as in the Owl ReCon, significantly simplifies the implementation of secure bidirectional communications. (See “Data Diodes vs Unidirectional Gateways: Side by Side” above for a real-life example.)

FICTION

“Secure/bilateral/magic diodes are the wrong way to provide visibility into industrial systems and data, because most attacks occur in TCP payloads and forwarding those attack packets or attack payloads provides no protection.”

FACT

Owl data diodes do not forward TCP packets. All Owl products incorporate protocol breaks as data travels across the diode.

Bidirectional data diode communication is the most secure method to share data from a high security network (e.g., a plant OT network) to a lower-security network. A TCP/IP connection can only be initiated from the high security network, meaning that the lower security side cannot initiate communication into the device.

Data diodes are specifically recommended in the Department of Homeland Security publication "Seven Strategies to Defend Industrial Control Systems," which does not mention unidirectional gateways at all.

FICTION

“A Unidirectional Gateway is typically delivered as a network appliance containing two hosts and a single set of unidirectional hardware.”

FACT

Two hosts and a set of hardware (transmitter and receiver) is four components, not a single appliance. Non-diode unidirectional gateways rely on inferior technology that cannot be housed in a single 13" device—the configuration described in the vendor statement requires either four separate modules, or a 48" deep cabinet. ReCon, by comparison, is a true appliance, contained in a single 13" 1U component.