

Financial Services Solutions

Secure One-Way Transfers Using Protocol Breaks

Owl Cyber Defense provides hardware-enforced data diode cybersecurity products for reliable one-way data transfer and network segmentation to protect against malware, ransomware, control override, and other forms of cyberattack. By creating a “break” or air-gap between the source and destination, the protected network or device cannot be probed, pinged, or accessed by cyber threats. Meanwhile, data can be easily shared one-way with external users or systems that need it through nearly any protocol, including HTTP, TCP/IP, UDP, FTP, and more.

Data Diode Use Cases:



Data Vault: Ensure the integrity of your data storage by using data diodes to enforce the one-way flow of data into your data vault or secured repository. At the same time, safely monitor security and system health information with a separate one-way link from the air-gapped data vault. Ideal to protect data vaults from ransomware, malware, and other destructive attacks.



Segment Networks: Segment your critical transaction processing networks and create separate ingress and egress paths. Data diodes increase lateral network security far beyond firewalls and enable safer processing and storage. Ideal for applications such as cryptocurrency exchanges & wallets, payment processing, and proprietary investment models.



Secure Customer Data Submissions: Secure customer analysis data and eliminate data leakage. Owl data diodes can scan incoming file submissions for malware and ensure that incoming files don't find their way out, accidentally or intentionally.



Collection of SIEM Data: Allow the flow of Security Information and Event Management (SIEM) log files and alerts from your secure networks to your Security Operations Center (SOC). Data diodes prevent malware intrusion into secure networks and the unauthorized exfiltration of data from the SOC.



Remote Monitoring: Enable a safe path for operational data to flow from secured networks to less secure or public networks. Data diodes can pass metrics, reports or video streams to external monitoring centers, support staff, or the cloud without increasing risk to internal data repositories.



Vendor Communication: Reduce your attack surface and mitigate third-party risk. Data diodes can be used to transfer data to or from partners, service providers, software OEMs, and other vendors to ensure that a compromised vendor network doesn't become an entry point to attack your systems.



Secure FIX Protocol Gateway: Provide a safe way to make FIX connections to counterparties with a specialized bidirectional data diode solution (ReCoN). FIX Protocol doesn't provide for security, and standard two-way socket connections present an opportunity for intruders.



Managed File Transfer: Secure and shield your trusted network by preventing direct connectivity between external partners and internal servers. A data diode ensures files can be sent from your internal network to your DMZ or the open internet through a one-way link. Owl works with leading MFT vendors to assure easy integration of our enhanced security solution with your choice of MFT platform.



20+
Years
of Experience



40+
Granted
Patents



2,500+
Deployments



20+
Countries

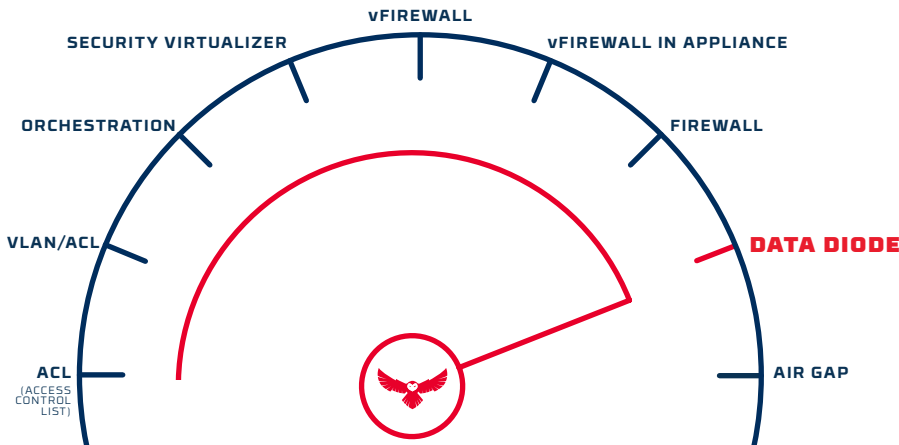
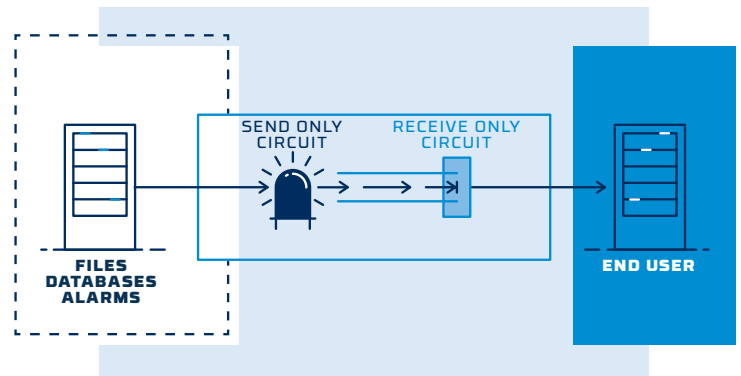


What is a Data Diode?

Owl uses a multi-layered, patented approach to the design of our data diodes. Owl data diodes are hardware-enforced, electronic cybersecurity devices designed with two separate circuits – one send-only, and one receive-only – which physically constrain the transfer of data to one direction only, forming an “air gap” between the source and destination networks.

Data diodes separate and create boundaries between trusted and untrusted networks and straddle 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.

Data diodes can be used to protect very small network segments, such as an individual data repository, an ATM, or a single workstation, or they can be used to protect a very large segment, such as an entire corporate network.



Why Hardware-Based Security



Software

- » Configuration-enforced
- » Zero-day exploits
- » Malware / Ransomware
- » Heavy ongoing management



Hardware

- » Physics-enforced
- » Unhackable
- » Invulnerable to malware
- » Little to no ongoing management

OWL Cyber Defense

Owl Cyber Defense Solutions, LLC leads the world in data diode and cross domain network cybersecurity. With a constant focus on customers in the military, government, critical infrastructure, and commercial communities, Owl develops market-first, one-way data transfer products to meet a variety of operational needs, from entry level to enterprise.

For more information on Owl, or to schedule a demo, visit www.owlcyberdefense.com



@OwlCyberDefense

203-894-9342 | Info@owlcyberdefense.com