Owl Incident Response Diode™

Secure, Hardware-Enforced Forensic Transfer

Key Features & Benefits

- → Enforces hardware-based, one-way transfer for assured data security
- → Replaces untrusted USB storage devices with a hardware-enforced one-way device that enables one-way simple drag-and-drop file transfer
- → Plug-and-go portability for rapid, in-field evidence collection
- → Filter protocols for secure, file-only data exfiltration
- → Encrypt data to isolate sessions with unique, per-session encryption keys
- → Maintain chain-of-custody with consolidated, device-specific audit logs
- → Protect analysis enclaves from cross-contamination and reinfection

Securely Extract Files from Compromised Endpoints

In high-threat operational environments, endpoints on classified mission systems face constant, evolving cyber threats. If and when these systems are compromised, safely moving files from a potentially infected or otherwise untrusted computer to another for analysis—without exposing the analysis computer to potential active cyber threats on the untrusted device—is a necessary step, but to date has carried significant risk.

Bidirectional connections can expose analysis tools, enable command-and-control callbacks, or trigger hidden payloads. USB mass storage devices are well known for the risk of corruption or contamination by malware. Data diodes, on the other hand, provide one-way data movement, creating a security barrier between untrusted devices and analysis computers—enabling rapid, safe evidence collection from untrusted systems without risking reinfection or cross-contamination of trusted investigative environments.

Owl Incident Response Diode™ for Portable, Assured Data Collection

Owl's Incident Response Diode™ (IRD) is the latest innovation in our cross-domain solutions suite, purpose-built for the secure, one-way transfer of data to support rapid incident response forensics. This portable, all-in-one appliance integrates two USB mass storage endpoints (source and destination) with a hardware-enforced data diode optimized for file-only transfer. The IRD enforces a strict file-only policy, isolates each session, and generates auditable logs—ensuring verified, secure evidence collection for analysis and intelligence.

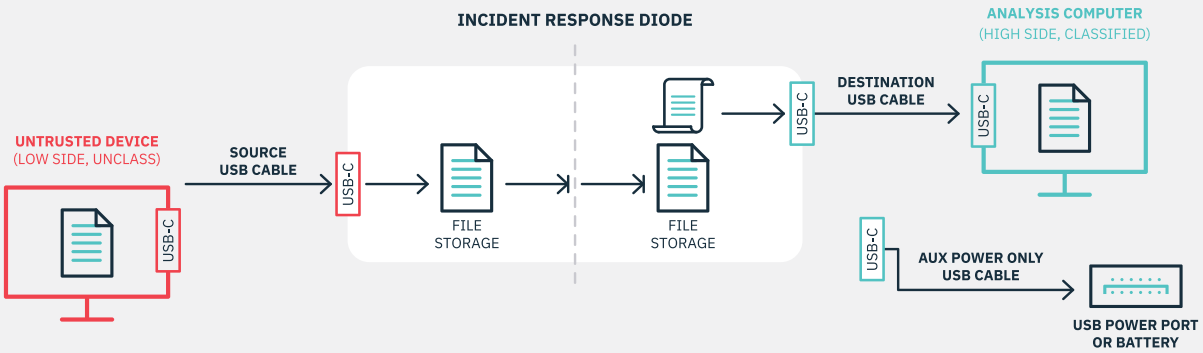
Use Case: Field Data Collection

After finding out a system was breached, an operator connects the IRD between the breached computer and a trusted analysis computer. The device appears as USB mass storage on both systems. Files are copied (drag-and-drop) off of the untrusted system, onto the IRD and then transferred onto the Analysis computer via the one-way data diode. In this way, files can easily be collected without ever connecting another device directly to the untrusted system.

203-894-9342 | owlcyberdefense.com

How it Works

The Destination USB is connected from the IRD to the analysis computer, followed by the Source USB from the IRD to the untrusted computer. The IRD powers up and mounts as distinct USB mass storage devices on both systems. Files are dragged and dropped (copied) from the untrusted system to the IRD's Source-side storage; once a file completes, the IRD automatically transfers it one-way to the Destination side, with the LED indicating activity. After transferring, files appear on the Destination storage for copying to the analysis workstation. Optional debug buttons allow retransmit or destination refresh. If needed, copy the session log from the Destination side. When finished, unplug the USB and power cables to power down and wipe the session encryption key, rendering the storage contents on both sides unreadable.



Owl Incident Response Diode™: Unparalleled Security, Flexibility, Performance.

The Owl IRD is the first and only 'pocket-sized' diode delivering assured one-way security with plug-and-go simplicity and flexible deployment across diverse mission environments. It integrates multiple layers of hardware-enforced security to ensure one-way data transfer and protect sensitive analysis enclaves. A protocol-filtering diode, per-session encryption, and isolated power path prevent malware propagation and cross-contamination from contested environments. With non-removable storage and consolidated audit logs linked to a unique device ID, the IRD enforces strict data collection policies and maintains a verifiable chain of custody—enabling rapid, secure evidence collection for mission-critical intelligence and forensic analysis. And by using a Protocol Filtering Diode based on Owl's Torrent implementation, files are transferred without use of USB as a transport mechanism between computers, ensuring hardware-based isolation between the source and destination computers.

OWL Cyber Defense™

Owl Cyber Defense Solutions, LLC, headquartered in Columbia, MD, leads the industry in data diode and cross-domain network cybersecurity solutions for faster, safer and smarter decision making. We create solutions tailored for high-risk sectors including the military, government and critical infrastructure. Our advanced technologies enable secure, near-instantaneous collaboration, bridging network barriers to protect critical missions. With a focus on scalability and interoperability, Owl ensures that organizations can maintain secure, reliable, and compliant communication channels against evolving cyber threats.

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

203-894-9342 | owlcyberdefense.com