

USE CASE

Strengthen Defensive Cyber Operations with Owl PFDs

Hardware-enforced network protection without creating new attack surfaces

Challenge

→ Connecting DCO tools to classified or OT networks opens bidirectional attack paths.

Solution

→ Owl Talon Data diodes enable one-way streams of telemetry data without any return path.

Benefits

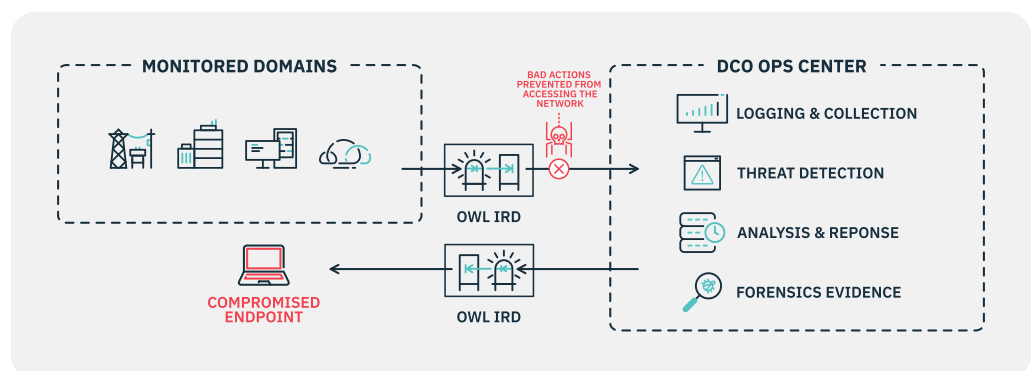
→ Hardware-enforced protection across every phase of the DCO lifecycle.

Challenge: Monitoring Sensitive Networks Creates Risk

Defense cyber operations (DCO) teams need continuous, enterprise-wide visibility into sensitive, classified, and operational technology (OT) networks to detect threats and maintain mission readiness. But every monitoring connection is a potential attack vector. Traditional tools like firewalls, managed switches, software-defined controls rely on configurable rules that adversaries can exploit, bypass, or manipulate. This means that the very act of monitoring a sensitive network can introduce the vulnerability teams are trying to prevent. The result is a forced trade-off between operational awareness and network integrity, one that no software-based control can fully resolve.

Solution: Owl PFDs Enable Safe DCO Visibility

Owl Cyber Defense® Protocol Filtering Diodes (PFDs) go beyond simple data diodes by enforcing unidirectional data flow at the hardware level using FPGA-based technology. Owl Talon® and Owl Talon Torrent® are deployed permanently at OT/IT and classified network boundaries, continuously streaming logs, SIEM telemetry, and sensor data outbound to a centralized cyber operations platform. When an active incident is detected, the Owl Incident Response Diode™ (IRD) extends this same hardware guarantee to the endpoint level, allowing forensic evidence to be collected from a compromised host and transferred one-way to a clean analysis environment with zero reinfection risk. Together, this comprehensive suite covers the full DCO lifecycle: persistent boundary monitoring, high-throughput enclave data transfer, and field incident response.



The Result: Measurable Security Gains Across the DCO Lifecycle

Unbreakable network isolation: Hardware-enforced one-way flow cannot be misconfigured or bypassed remotely, eliminating the attack surface that bidirectional monitoring tools introduce.

Continuous, compliant threat monitoring: Owl Talon data diodes satisfy CSfC and U.S. Government continuous monitoring requirements by enabling safe outbound log and telemetry transfer from classified and OT environments.

Safe forensic collection at the endpoint: The Owl IRD allows incident responders to extract evidence from compromised systems on-site without connecting those systems back to trusted networks or risking lateral spread.

Unified architecture, consistent enforcement: Owl data diodes share a consistent PFD foundation, enabling a common management experience and defensible audit trail across all DCO touchpoints.



Owl Protocol Filtering Diode Suite

Owl Protocol Filtering Diodes (PFDs) are purpose-built, U.S. Government-validated, and designed to fit wherever mission demands take you. From rack-mounted enterprise deployments to rugged field kits and whether securing OT networks, streaming ISR and sensor data, connecting to the cloud, transferring files or collecting forensic evidence on-site, Owl PFDs feature multi-layer security, next-gen performance throughput speeds, multiple simultaneous protocols on a single platform and the extensibility and adaptability modern mission require. Enforce hardware-guaranteed, one-way transfer across every use case with Owl PFDs

Learn more at www.owlcyberdefense.com



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.

