OWL Cyber Defense™

USE CASE

Secure Connectivity to High Threat Networks

Safely Connect to Risky Networks Without Compromising Operations

Summary

Challenge

Enabling secure, real-time data exchange with High Threat Networks without exposing classified systems to cyber threats, data leaks, or unauthorized access remains the core challenge.

Solution

Owl's RTB-compliant CDSs and Talon PFDs provide secure, hardware-enforced connectivity to HTNs, ensuring safe, policy-controlled data exchange per federal mandates..

Outcome

Secure, compliant data sharing with HTNs while fully protecting classified systems from cyber threats and unauthorized access.

OWL CYBER DEFENSE

RAISE THE BAR

READY

FLYING ABOVE THE BAR

Challenge: Balancing Collaboration and Security with High Threat Networks

The U.S. Department of Defense (DoD) faces the challenge of securely connecting to High Threat Networks (HTNs)—external networks that may lack strong cybersecurity, such as those operated by coalition partners, foreign governments, commercial entities, or legacy/industrial control systems—while protecting classified systems from advanced cyber threats. These connections are essential for operational collaboration and intelligence sharing but significantly increase the risk of data breaches, malware infiltration, unauthorized access, and disruption of mission-critical operations. Balancing the need for secure collaboration with the imperative to safeguard sensitive environments remains a complex and ongoing challenge.

High Threat Network Connectivity Solution with Owl's CDS Solution

Federal guidance for connecting to High Threat Networks requires hardware-enforced separation, multi-layered filtering, and strict policy controls to prevent unauthorized access and data breaches. Owl Cyber Defense addresses these mandates with its Cross Domain Solutions (CDSs) and Owl Talon Protocol Filtering Diodes (PFDs). CDSs provide accredited, policy-driven data transfer between classified and HTNs, while Owl Talon PFDs enforce one-way data flow and protocol termination in hardware. Together, they deliver Raise the Bar(RTB)-compliant, secure, and efficient unidirectional or bidirectional connectivity, protecting sensitive environments while enabling essential collaboration and mission operations.

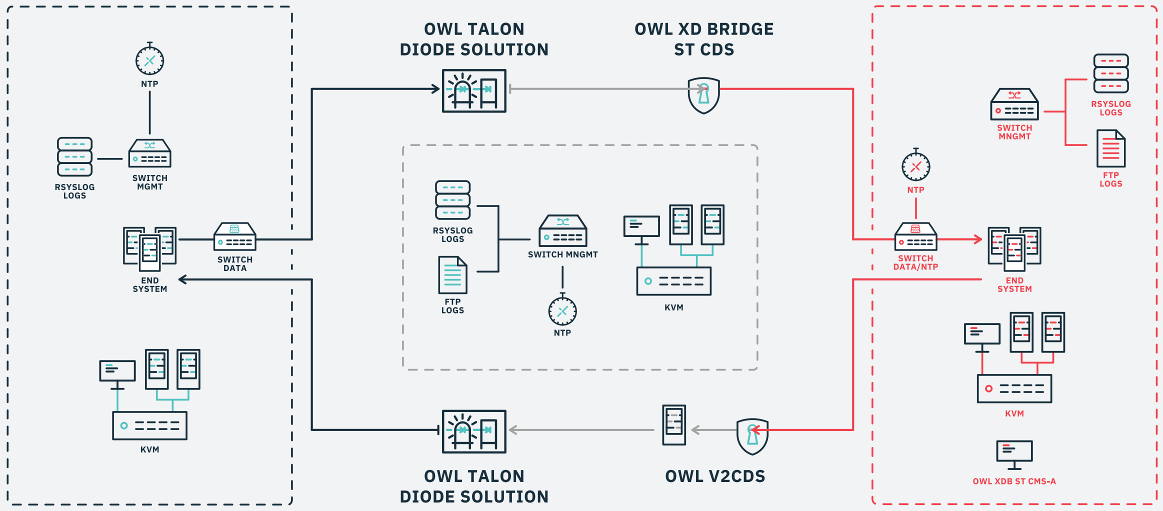
Key Benefits

Unmatched Security and Compliance Hardware-enforced separation and multi-layered filtering meet RTB and federal mandates, blocking cyber threats and unauthorized access during data exchange with High Threat Networks.

Operational Continuity Secure, policy-controlled data sharing with HTNs, supporting mission-critical collaboration without risking disruption or compromise of classified environments.

Efficient, Policy-Driven Data Sharing Owl's certified CDSs and Talon PFDs deliver real-time, high-speed data transfer, ensuring organizations meet operational and regulatory requirements while maintaining strict control over information flow.

Owl's HTN Solution: How it Works



Unidirectional Flow from HTN to Trusted Network:

In situations where data needs to move unidirectionally from a HTN to a trusted network (e.g. sending logs to IT networks, continuous monitoring to meet CSfC requirements etc.), structured data is moved first through an Owl Talon PFD to perform a hardware break between the HTN and CDS. It's then passed to the first CDS, Owl's XD Bridge ST for processing. Finally, the XD Bridge ST CDS sends filtered data to the trusted network for receipt and further processing as needed.

Bidirectional Flow between HTN & Trusted Network:

In cases where our customers need bidirectional transfer with HTN's, after the unidirectional flow is performed (outlined above), data is filtered and sent through Owl's V2CDS CDS for processing then through a second Owl Talon PFD for a final hardware break before reaching the HTN/ untrusted network.

Owl Talon One: 1U is a compact, rack-mountable protocol filtering diode that enforces secure, one-way data transfer at up to 1 Gbps. It physically blocks inbound threats, supports multiple protocols, and ensures absolute network separation—helping agencies meet high threat network regulatory requirements via reliable, hardware-enforced cybersecurity.

Owl V2CDS is a Raise the Bar-ready, U.S. Government certified Cross Domain Solution that enables secure, real-time voice, video, and structured data communication across classified and unclassified networks. It enforces strict protocol filtering and mitigates covert channels—ensuring rapid, reliable collaboration with- and threat prevention for high threat networks.

Owl XD Bridge ST is a Raise the Bar-ready Cross Domain Solution that enables secure, hardware-enforced data transfer between networks of differing security levels. It uses diode-based isolation and linear pipeline filtering to inspect and sanitize data, ensuring only validated information crosses domains—ideal for high-threat networks requiring robust, RTB-compliant protection.

Owl Cyber Defense Solutions, LLC, headquartered in Columbia, MD, is a pure play cybersecurity company solely focused on purpose-built, made-in-the-USA data diode and cross domain solutions. Trusted to protect the most sensitive government and commercial networks worldwide, our technologies are developed and manufactured to meet the strictest U.S. security standards. Owl enables secure, near-instantaneous collaboration across network boundaries—powering faster, safer, and smarter decisions for military, federal, and commercial critical infrastructure organizations. With a focus on scalability, interoperability, and regulatory compliance, Owl ensures resilient communication in the most high-threat environments. Rigorously tested. Globally trusted.

Visit **www.owlcyberdefense.com** or contact us at **info@owlcyberdefense.com** for more details.