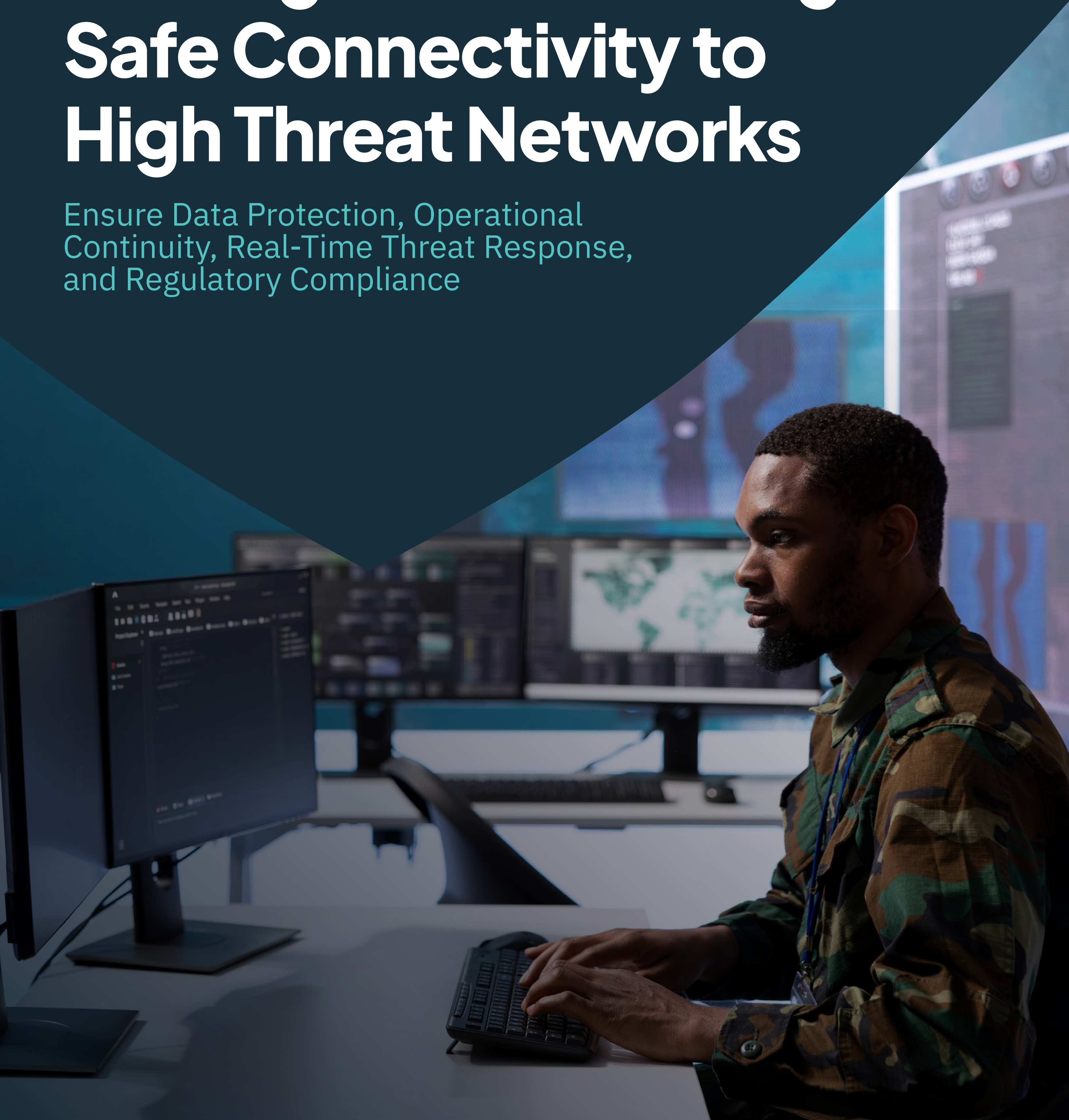
OWL Cyber Defense™

Strategies for Enabling Safe Connectivity to High Threat Networks

Ensure Data Protection, Operational Continuity, Real-Time Threat Response, and Regulatory Compliance



The High Threat Network Dilemma

A Clear and Present Danger

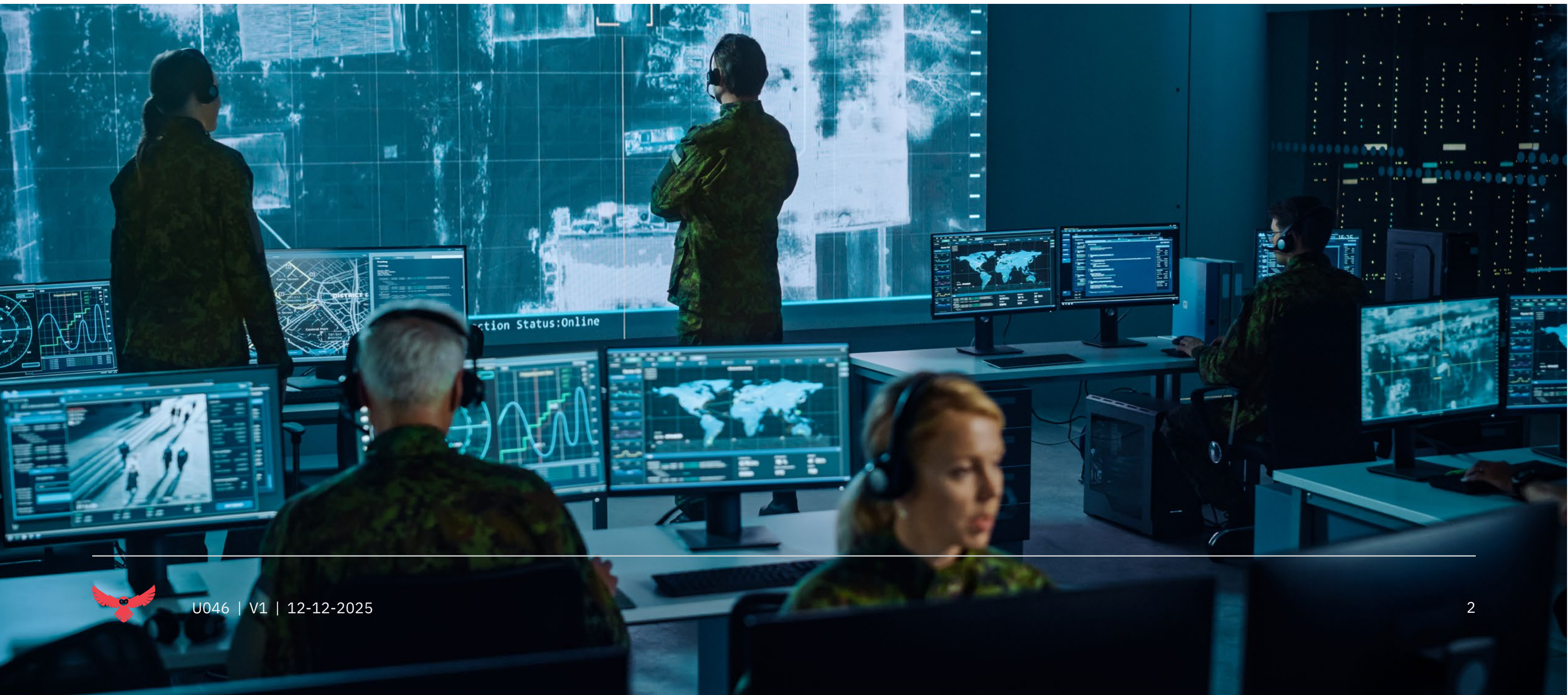
State-sponsored adversaries in and malicious actors are exploiting vulnerabilities in defense, intelligence, and critical infrastructure networks at unprecedented speed and scale. To enable mission-essential operations—such as real-time information sharing with coalition partners, remote management of distributed systems or integration with legacy infrastructure—agencies often have no other choice than to connect to risky networks, including High Threat Networks (HTNs).

High Threat Networks–often outside an agency's security perimeter–are known to have inherently weak security which in turn makes it easier for attackers to access or steal data when connected. Examples of HTNs include the internet, partner networks, legacy systems, and more However, mission requirements—such as exchanging data with or receiving situational awareness from an HTN—often outweigh the risks of connecting to HTNs. This creates an imperative for robust safeguards to be in place to prevent adversaries from exploiting these connections.

Case in Point: High Threat Network Exposure

Consider the U.S. DoD's need to share real-time threat data with coalition partner networks. By connecting to these potentially high threat networks, the DoD is also exposing its own networks to significant risk. While operational collaboration is vital, linking with a partner whose network security is weak can increase the chances of sensitive targeting data being compromised, adversaries injecting false information, virtual defenses potentially being bypassed and/or live exercises being disrupted.

Federal mandates recognize that software-only defenses cannot mitigate advanced threats in asymmetric cyber battlespaces and are evolving requirements to ensure secure HTN connectivity via hardware-enforced separation and filtering at every connection point to ensure both operational effectiveness and robust security compliance.



What Are High Threat Networks?

(Definitions, Examples, Risks)

High Threat Networks are those networks whose cyber hygiene is known to be insufficient, lack robust and effective defensive cyber operations, or have unclear ownership and limited ability for your organization to influence their security posture. Examples include defense or intelligence unclassified networks connected to the Internet or NIPRNet, as well as information-sharing partner networks—even those classified—if their only protection against the Internet is basic boundary solutions, like firewalls. In such cases, even a partner's classified network can be considered a high threat network.

Connecting to HTNs introduces significant risks, especially when these networks are linked to sensitive or classified environments.

Key Risks Include:

→ Weak defensive measures due to traditional protections and lack of oversight make it easier for networks to be compromised.

→ Network infiltration, allowing attackers to exploit vulnerabilities, reach sensitive assets and/or gain unauthorized access.

→ Data exfiltration, including theft of classified or mission-critical information.

"The current level and tempo of cyber-attacks is not tolerable. Our adversaries see opportunity for strategic advantage through continuous activity in the domain. We must act purposefully to frustrate their intentions, increase their costs, and decrease their likelihood of success."

- ARMY LT. GENERAL PAUL NAKASONE -
Commander of U.S. Cyber Command and Director of NSA

Evolving Guidance for High Threat Networks

Across the U.S. Government, the requirements for mitigating risk when connecting to a HTN has grown significantly, to include:

The National Security Agency's National Cross Domain Strategy and Management Office (NCDSMO), which mandates hardware-enforced controls for Cross Domain Solutions (CDSs) through its Raise the Bar (RTB) guidance. These requirements aim to secure HTN connections by enforcing one-way transfer (OWT) design patterns, including physical separation and multi-stage filtering. All HTN traffic must traverse separate hardware-enforced, unidirectional paths for ingress and egress, with data processed through three independent filtering pipelines to block malicious content. While straightforward for unidirectional flows, bidirectional flows require layered defenses to thwart command-and-control attacks.

CMMC Level 3 requires contractors handling Controlled Unclassified Information (CUI) to implement strong safeguards against advanced persistent threats, ensuring secure government and supply chain data flows and reducing risks when sharing information across HTNs, thereby protecting the integrity of critical operations.

Executive Order 14028, which prioritizes securing the software supply chain, particularly "critical software" with elevated system privileges. It mandates rigorous mechanisms to ensure software integrity, transparency, and resistance to tampering—addressing vulnerabilities often exploited in HTN environments.

Together, these frameworks emphasize hardware-enforced security, multi-layered filtering, and supply chain rigor to counter evolving threats. By integrating RTB-compliant CDSs, CMMC safeguards, and EO 14028's software assurance, agencies can mitigate risks in high-threat data exchanges while maintaining compliance with federal mandates.

From Vulnerability to Confidence

Comparing Cybersecurity Solutions for HTN Connectivity Effectiveness

Traditional software-based solutions cannot guarantee the security required for HTN connectivity. Hardware-enforced solutions like protocol filtering diodes (PFDs) and advanced CDSs provide the deterministic, physical separation and multi-layered filtering necessary to defend against the sophisticated threats targeting mission-critical networks.

Why Firewalls Fall Short

Traditional software-based firewalls rely on configurable code to block known threats and basic attacks. However, they are limited against advanced, multi-vector cyber threats and were not designed to stop coordinated, persistent attacks. Attackers can exploit software vulnerabilities, misconfigurations, or bypass inspections, making firewalls insufficient for protecting sensitive systems connected to HTNs.

Protocol Filtering Diodes for One-Way Connections to High Threat Networks

PFDs provide hardware-enforced, one-way data transfer between segmented networks, mitigating software vulnerabilities and misconfigurations. By processing and filtering protocols in hardware, PFDs allow only authorized, properly formatted data and prevent backflow and unauthorized access. This supports U.S. Government mandates for hardware-enforced separation and filtering at HTN boundaries to protect mission-critical data. PFDs help agencies comply with federal standards while enabling efficient, secure, lossless data exchanges across HTNs.

Modern Cross Domain Solutions for Secure, Policy-Controlled Multi-Domain Data Exchange Across High Threat Networks

Modern CDSs combine hardware-enforced protections with strict policy controls to enable secure, compliant data transfer across domains of varying security levels, including HTNs. CDSs enforce organizational policies and provide separation at network, protocol, and content levels, ensuring only authorized data moves between trusted and untrusted domains. Built on trusted operating systems, CDSs support complex environments and help agencies comply with federal directives like DoD Zero Trust and Raise the Bar, enabling secure mission-critical data exchange across HTNs

Combined Defense: Layering Protocol Filtering Diodes and Cross Domain Solutions

For maximum HTN connectivity and collaboration security, solutions should integrate content filtering from CDSs with hardware-enforced protections from PFDs. CDSs combine software filtering with hardware separation, using physically distinct High-to-Low and Low-to-High paths coordinated for secure bidirectional exchange. PFDs enable one-way transfers and provide the hardware break required for HTN connectivity. Together, CDSs and PFDs enforce policy-driven data flows, permitting only authorized, properly formatted information. This layered approach significantly reduces risks, blocks malware, and ensures compliance with federal mandates while enabling efficient, secure data sharing across domains.

The Owl Solution for Secure HTN Connectivity & Collaboration

Owl Cyber Defense offers an RTB compliant, hardware-enforced solution for secure connectivity between classified networks and HTNs. The Owl solution integrates our leading CDSs including:

V2CDS: the only NCDSMO Baseline-listed voice and video CDS that can also support structured data and is approved for use by the U.S. DoD and intelligence community.

XD Bridge ST: a hardware-enforced CDS with U.S. Government approved data diodes for structured data transfers.

Owl Talon PFDs: which provide secure, hardware-enforced, one-way transfer.

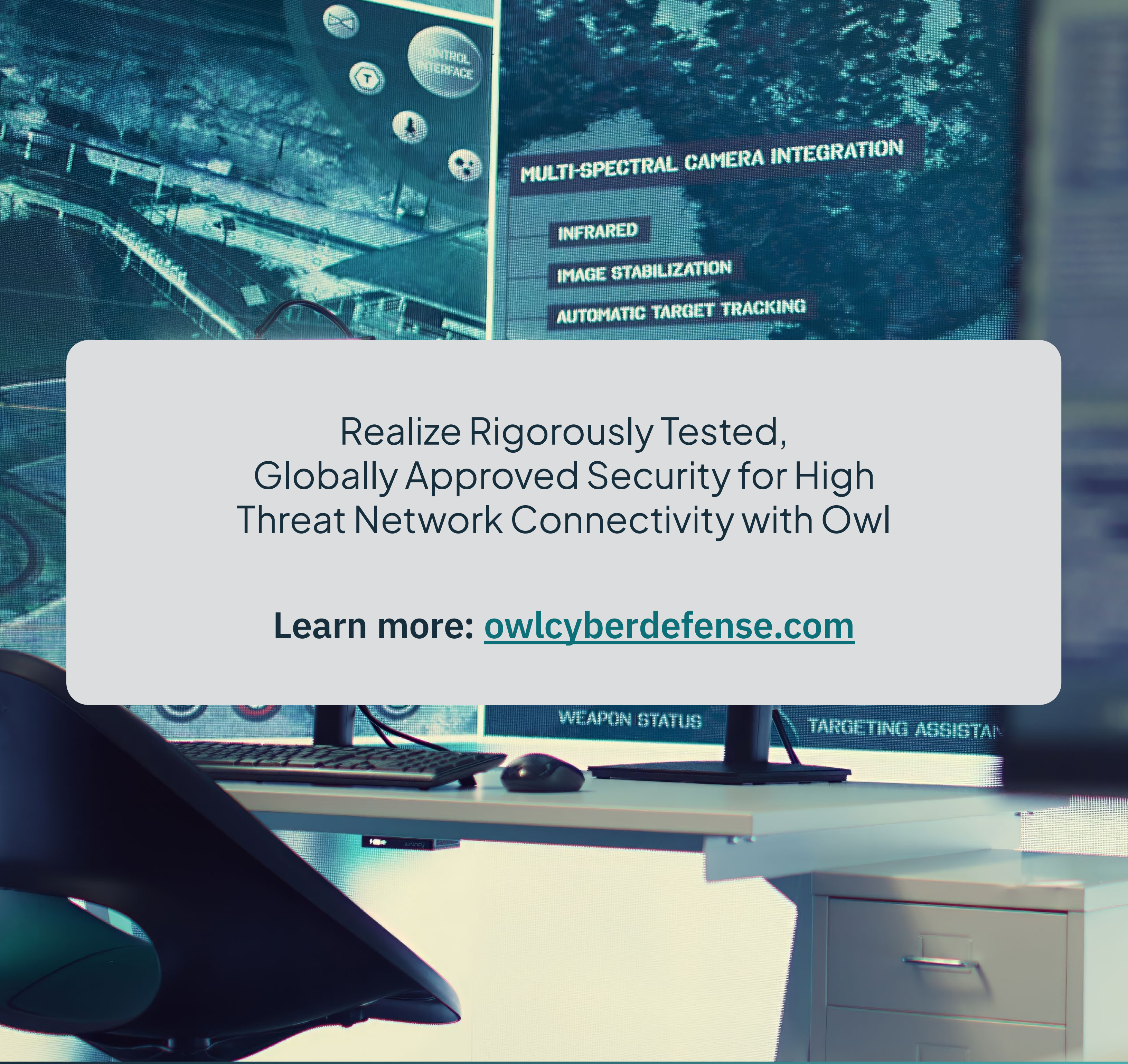
With Owl, agencies can realize unidirectional or bidirectional transfer with HTNs without compromise. Owl's HTN solution uses two CDSs – XD Bridge ST for HTN-to-trusted transfer and V2CDS for trusted-to-HTN transfer – and ensures CDSs never interact with HTNs through the deployment of Owl Talon PFDs.

Conclusion

Enabling Resilient Operations Through Safe High Threat Network Integration

The cyber threat landscape requires a shift to proactive resilience. Connecting to High Threat Networks remains vital for intelligence and mission success. Agencies can secure these connections with multi layered, hardware-enforced defenses like accredited Cross Domain Solutions and Protocol Filtering Diodes. Owl's solutions enable safe, agile operations—supporting warfighters, protecting critical systems, and enabling global defense collaboration—without sacrificing speed or innovation. National security's future depends on safely connecting to HTNs while staying ahead of adversaries.

Don't let risky networks compromise your mission. Contact Owl Cyber Defense today to deploy solutions that fortify your agency against emerging threats while meeting the highest standards of security and compliance.



Realize Rigorously Tested, Globally Approved Security for High Threat Network Connectivity with Owl

Learn more: owlcyberdefense.com

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. Owl cybersecurity specialists are intimately familiar with a wide variety of industry pain points, technologies, and best practices, and have helped hundreds of organizations around the world secure their networks with Owl's patented hardware-enforced, un-hackable data diode solution

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