AI Containment PRINCIPLES & USE CASES

OWL Cyber Defense™

ARCHITECTURE PRINCIPLES

Hardware-Enforced Boundary

Enforced outside the compute stack, where an agent can't influence it.

Can't Be Argued With

No software path to social-engineer, misconfigure open, or exploit.

One-Way & Filtered

Hardware-enforced one-way transfer, with filtering for supported protocols.

Governed Exchange

Policy-governed cross-domain data exchange for approved workflows.

Independent Audit Trail

Every transfer logged outside the agent: a defensible answer when regulators ask.

RTB Compliant

Meets NSA Raise the Bar requirements.

Designed & Made in USA

Made in the USA and relied on by the nuclear industry for rigorous compliance.

USE CASES



Data Center OT/IT Boundary

Protects power, cooling, and building controls with Owl Talon.



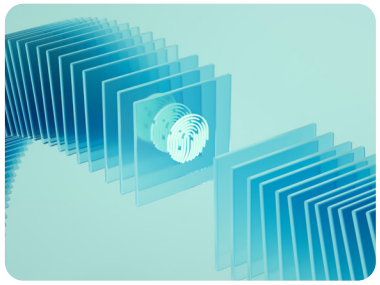
AI Factory Telemetry

Streams GPU-cluster security data out at high throughput. Nothing routes back in.



Bandwidth-Constrained Edge

Edge AI flags what matters. A CDS moves validated data to the high side.



Edge-to-Core Containment

One-way, filtered flows keep a compromised sensor or agent from reaching command.



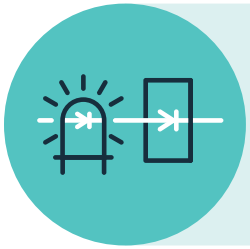
Trusted AI Training Data

Validates structured data at the point of collection to guard against poisoning.

Reference architecture built on Owl data diode and Cross Domain Solution technology. Filtering applies to supported protocols and defined data flows; scope varies by deployment.

BUILT ON TODAY'S OWL SOLUTIONS

Hardware-enforced one-way transfer where required, plus policy-governed cross-domain data exchange for approved workflows.



Data Diodes

Hardware-enforced one-way transfer where required. No return path.



Protocol Filtering

Governed, filtered traffic for supported protocols.



Cross Domain Solutions

Policy-governed exchange for approved workflows, with an audit trail of every transfer.

ATTACK CLASSES THIS ARCHITECTURE ADDRESSES

Protocol & Stack Exploits

Crafted or malformed packets that trigger flaws in a network stack or service.

HOW IT'S ADDRESSED

Network connections end at the protected boundary, keeping protocol based exploits out.

Malicious Payloads

Malware or weaponized files hidden inside otherwise valid-looking data.

HOW IT'S ADDRESSED

For supported formats, content is checked against policy. Non-conforming data is dropped and logged.

Command-and-Control Callbacks

A compromised system reaching back out for instructions or tools.

HOW IT'S ADDRESSED

When enforced by a diode, there is no return path to carry a callback.

Data Exfiltration

Sensitive data leaking out through channels that look legitimate.

HOW IT'S ADDRESSED

Defined flows only allow approved fields to cross. Everything else is filtered out and logged.

Lateral Movement & Pivoting

An intruder or rogue agent using one foothold to reach adjacent systems.

HOW IT'S ADDRESSED

When enforced by a diode, an intruder has no path to pivot back across the boundary.

Data Poisoning

Tampered training or operational data fed into a model or analytics pipeline.

HOW IT'S ADDRESSED

For defined workflows, structured data is validated at the point of collection, before it reaches the protected side.

Policy can be argued with. Hardware can't.

Industry leaders now agree that application-layer controls alone can't contain autonomous agents. This reference architecture applies Owl's data diode and Cross Domain Solution technology to AI environments: one-way where required, filtered for supported protocols, and governed for approved workflows, with an auditable record of every transfer.

Scan the QR code to learn more