

OCTOBER 25, 2023

Counter AI Threats & Securely Replicate AVEVA PI System Data with Defensive Hardware

Dennis Lanahan, VP of Commercial Markets



Agenda

- About Owl: who we are and what we do
- How to prevent AI threats
- How to isolate and separate OT and IT with hardware-enforced separation
- How to securely share AVEVA PI System data between networks and systems that are 100% confidential from each other
- Critical infrastructure use case examples
- How to replicate AVEVA PI System data to the cloud



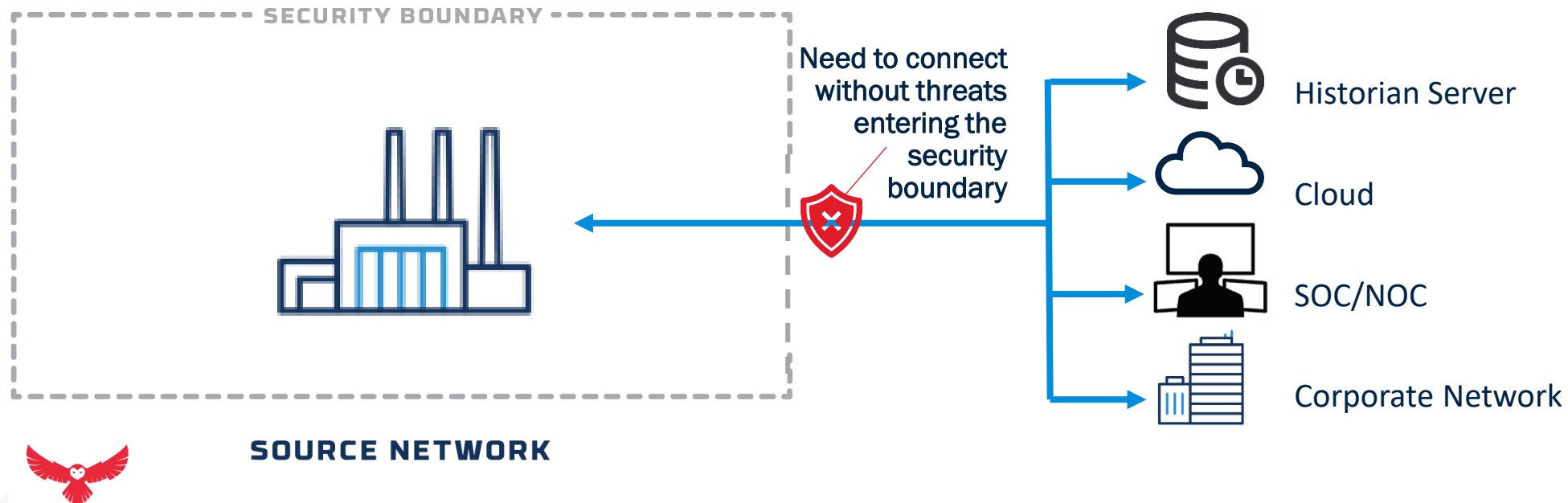
Owl History

- 23 years securing Government and critical Infrastructure networks
- Pioneer and leader in the data diode market - first patented data diode on the market 23 years ago
- USA Sandia Labs based security technology designed to ensure the safest network boundary possible
- Over 3000 Global deployments
- Offices in the US (HQ), UK, Saudi Arabia, UAE, and Kuwait
- Elite hardware-enforced solutions and services that protect against the world's most sophisticated advanced persistent threats
- Expanded from supporting US Government Defense and Secret Networks in 2007 to defend US Nuclear and Fossil generation facilities in Support of NRC 5.71 and NERC CIP
- Deployed in oil and gas and petrochemical networks following Shamoon virus attacks in 2014



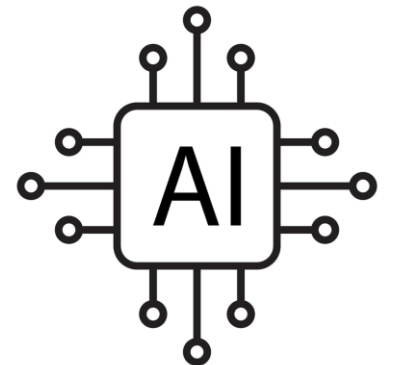
Current Market State

- Secure critical infrastructure networks need to connect with untrusted/less trusted networks without compromising security of the operations network
- Organizations want assurance that the access to a secure network is protected and/or limited, while still enabling the sharing of data between networks
- Value is in the data - sharing data securely and protecting your assets is a “must have”

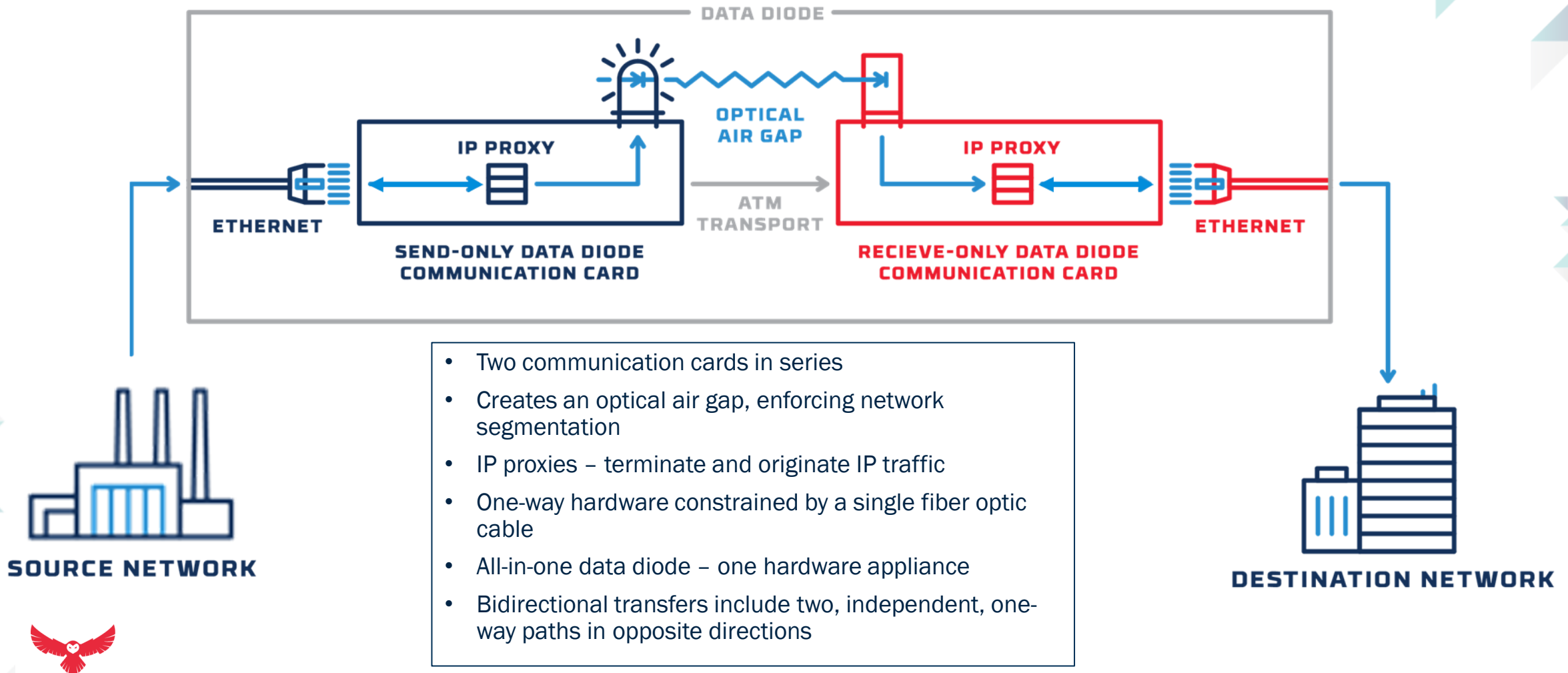


Prevent the Risk of AI Attacks

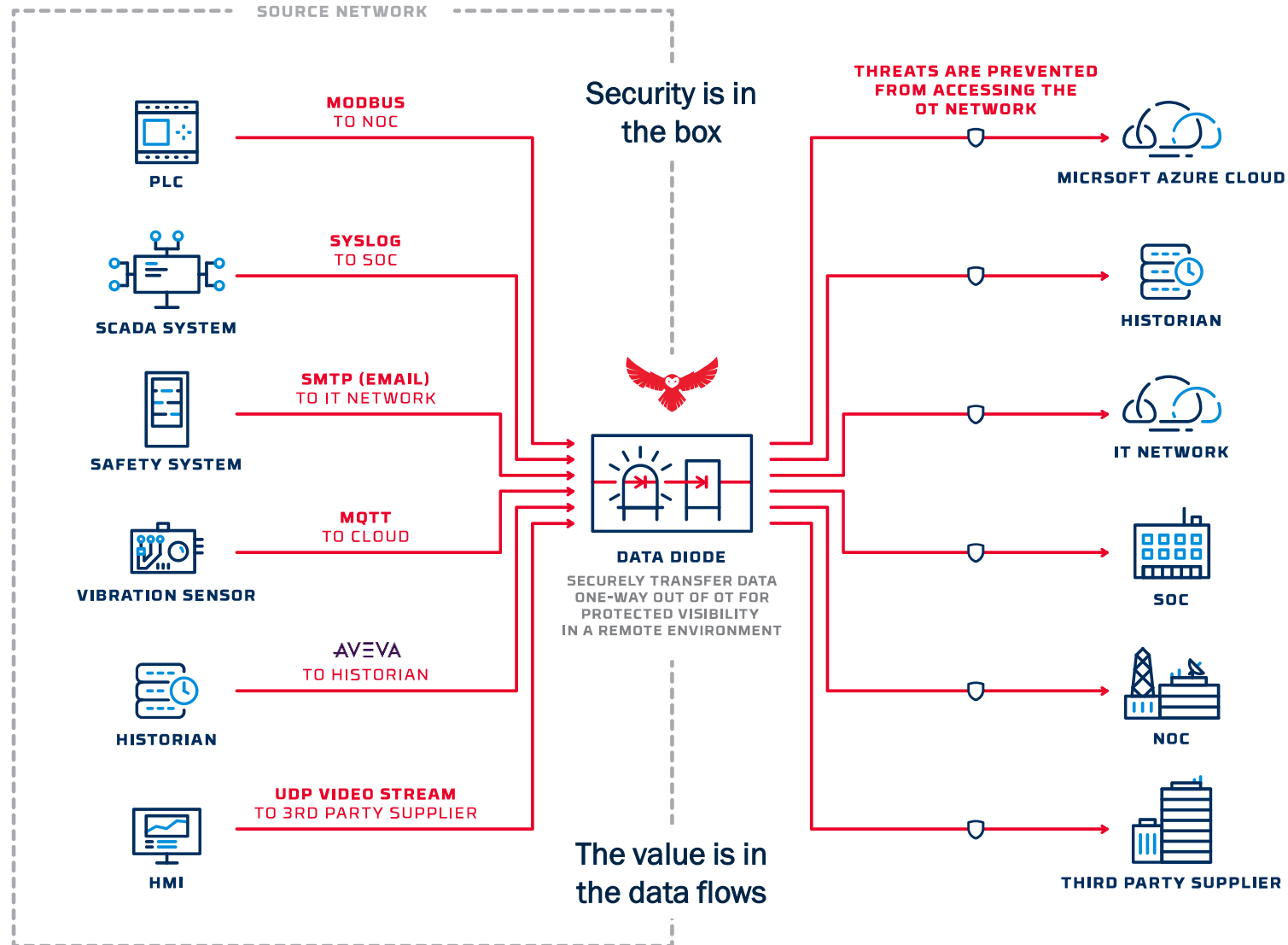
- Artificial intelligence has the power to elevate hacking novices to experts rapidly
 - Spoof credentials
 - Breach security measures
 - Allow attackers to penetrate OT environments and access PLCs, SCADA, DSCs, historians, and other crucial systems
- Hardware-enforced cybersecurity is an absolute and isn't susceptible to being “faked out” by AI threats



Hardware-Enforced Data Diode Network Separation



The Most Secure One-Way Architecture



Use Case Markets



NRC nuclear regulated market



NERC coal regulated market



Oil and gas



Mining



Petrochemical



Pharma



- **We support:**
 - AVEVA PI System
 - eDNA
 - AVEVA Historian Powered by Wonderware

AVEVA PI System Replication

- AVEVA PI System data needs to be replicated one-way out of a secure network without introducing risk to the secure network
- Software-based solutions fail to protect secure networks from cyber attacks
- Hardware-enforced solutions provide a physical layer of security that prevents threats from entering back into the secure network through AVEVA PI System replication



Transition to Replicate PI Systems

Challenge:

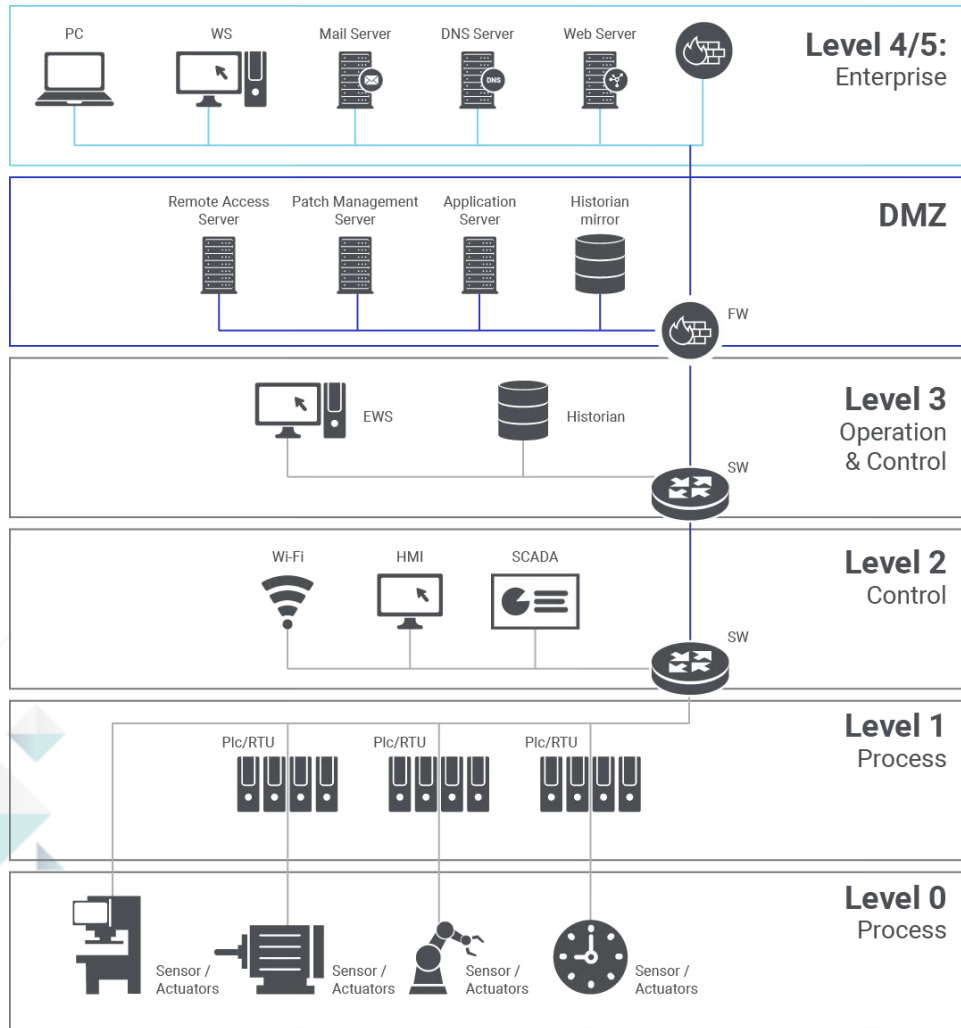
- Many networks have a single AVEVA PI System at level 3.5
- OT and IT access that AVEVA PI System from their respective sides of the DMZ
- If both sides of the DMZ can access the AVEVA PI System, then IT threats can get through to OT

How it Works:

- **Step 1:** AVEVA PI System at level 3.5 becomes an OT asset
- **Step 2:** Replicate AVEVA PI System goes in the destination network
 - Corp, Data center, Cloud, On Prem, Off Prem
- **Step 3:** Owl Solution with OPTS is deployed between the source and the destination networks to securely transfer data
- **Step 4:** AVEVA PI System data is replicated in the destination network
 - Users in IT networks use AVEVA PI System in the IT network to get their job done – no longer need access to OT or the DMZ to do get data



Secure Segmentation within the Purdue Network Model



4) Secondary AVEVA PI System for business use outside the DMZ and OT network

3) Unidirectional data flow from DMZ to level 4/5

2) Source AVEVA PI System of record and history protected in secure DMZ

1) Collection of asset data to the source AVEVA PI System



Owl PI Transfer Service (OPTS)

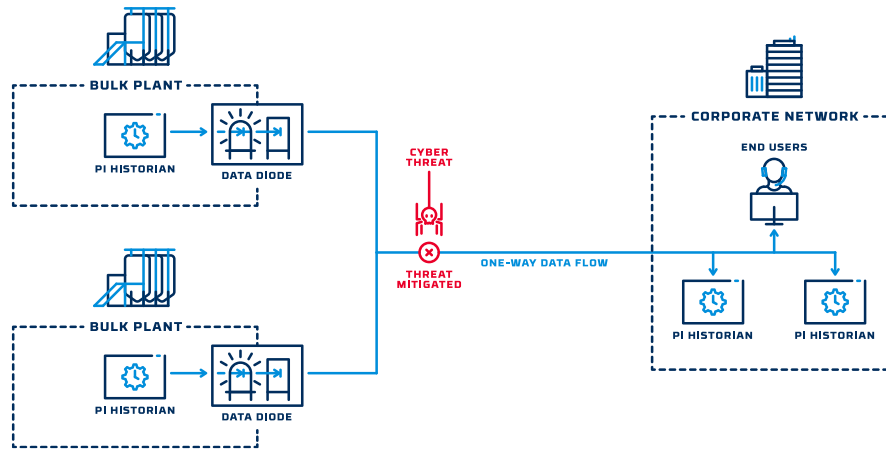
Key Features of Owl Solutions with OPTS:

- Dedicated PI System® platform for critical application support
- Auto-build of database configurations; auto-discovery of adds/deletes/changes
- Real-time transfer of data points:
 - Point records
 - Snapshot data
 - Historical records
 - Digital state tables
- Realtime and continuous point backfill – auto backfill due to network outages
- AVEVA PI System replication of over 500K points
- Secure LINUX operating system for transfer reliability
- System setup and configuration as both PI Systems are live and operational
- AVEVA PI System Collective HA support
- Owl High Availability with failover and redundancy

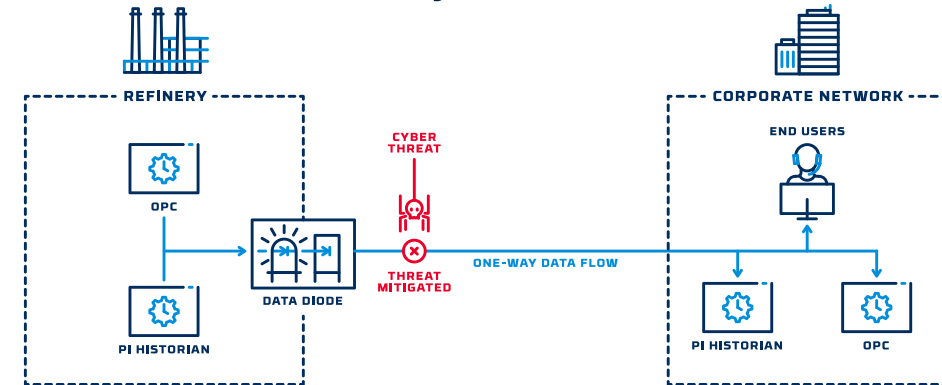


Use Cases

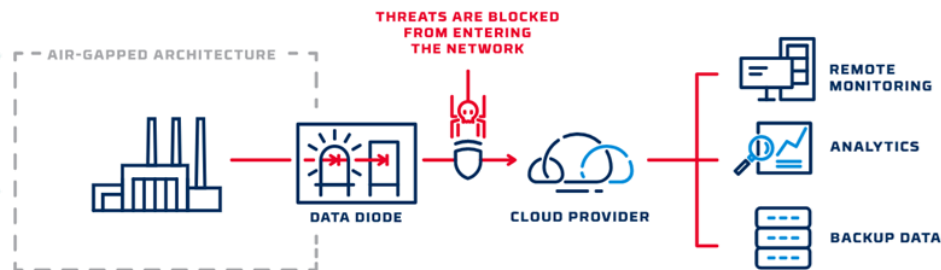
Multi-Plant to Corporate Replication



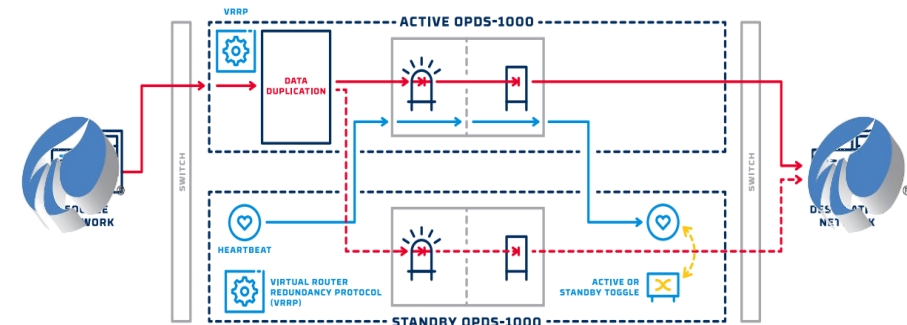
Secure OPC Transfer of Asset Data to PI System



OT-to-Cloud Use Case



Owl High Availability Architecture



How Can We Help?

- **UNDEFEATED** for over 20 years
- We specialize in defending networks – we've been enabling critical networks to share data and communicate with untrusted networks
- With a defense that strong, you can have the assurance that your critical network is secured, while still being able to connect externally
- Our customers have told us that even when they are under attack, they can sleep peacefully knowing they are protected, unlike other areas of the organization





OWL Cyber
Defense

Contact Us!

www.owlcyberdefense.com

Dennis Lanahan, VP of Commercial Markets

dlanahan@owlcyberdefense.com

Visit us at booth #43

AVEVA