Case Study

When Ransomware Hit Their Competitor, This Refinery Was Already Protected

How protocol isolation secured 500+ critical OT assets at a leading energy company — and why ransomware never had a chance.

Executive Summary

When a competitor refinery suffered a devastating ransomware attack that shut down operations for weeks, leadership asked: "Could this happen to us?" The answer was no — because they had already deployed Xona's protocol isolation architecture. This leading, vertically integrated energy company operates major refineries in the Americas with hundreds of users and more than 500 critical OT/ICS assets — DCS, PLCs, SIS, and HMIs.

By deploying the Xona platform, the refinery eliminated every direct connection between user endpoints and operational technology, rendering the ransomware attack vector that devastated its competitor structurally impossible. The result is zero direct network connectivity — users interact with OT systems in real time, but their endpoints are never connected to the OT network.

RESULTS AT A GLANCE	
500+	Critical OT/ICS assets protected (DCS, PLCs, SIS, HMIs)
Zero	Recorded security incidents attributable to remote access since deployment
Days, not months	Full deployment completed in just a few days
"Light years ahead"	User experience vs. previous solution
100%	Elimination of direct endpoint-to-asset connectivity

The Threat Landscape: Why This Matters Now

The 2024–2026 period has been the most dangerous in the history of industrial cybersecurity. The Dragos 2025 OT/ICS Cybersecurity Year in Review documented an 87% year-over-year spike in industrial ransomware. Manufacturing has been the most-attacked sector for four consecutive years, with 4,701 ransomware incidents recorded globally in the first nine months of 2025 alone — up 34% year-over-year.

Volt Typhoon, a Chinese state-sponsored threat group, has pre-positioned inside U.S. critical infrastructure — targeting energy, communications, and transportation networks. Using "living off the land" techniques with legitimate administrative tools, these actors maintain persistent access for months or years undetected. The IISS concluded Volt Typhoon has "redrawn the boundary for acceptable state behavior in cyberspace."

FrostyGoop became the first documented OT malware to use Modbus TCP/502 to directly manipulate industrial processes, causing heating outages for 600+ apartment buildings in Ukraine. The investigation revealed 46,000 internet-exposed ICS devices worldwide, identified in 2024.

65% of OT environments have insecure remote access. 75% of OT attacks begin as IT breaches that pivot into OT. Adversaries move from IT into OT using valid credentials and trusted remote access paths.

Before Xona: The Legacy Problem

Direct endpoint-to-asset connectivity created routable paths from potentially compromised endpoints into DCS, PLCs, SIS, and HMIs. **Cumbersome legacy tools** generated friction for hundreds of users — lag, complex logins, and poor UX led to security-degrading workarounds. **Complex administration** consumed IT resources. No protocol isolation meant OT protocols were exposed across the network boundary. With 500+ critical assets and hundreds of users, the legacy architecture presented an expansive target.

The legacy environment had evolved over more than a decade, accumulating layers of remote access tooling that were never designed to coexist. VPN concentrators provided broad network-level access to internal segments, giving any authenticated user — or any attacker with stolen credentials — a routable path into the OT network. Jump servers acted as shared staging points, but they introduced their own risks: unpatched operating systems, shared local administrator accounts, and cached credentials that persisted between sessions. Multiple teams had deployed different remote desktop solutions for different asset types, resulting in a patchwork of TeamViewer, RDP gateways, and vendor-specific remote access tools — none centrally managed, none consistently audited.

Credential management was fragmented. Vendor technicians often shared passwords over email or retained VPN credentials long after their maintenance windows closed. There was no time-based access control — a vendor authorized to perform a four-hour calibration could, in theory, reconnect at 2 AM on a Sunday without anyone knowing. Session recording was nonexistent for most access paths, which meant the security team had no forensic evidence when investigating suspicious activity. The lack of centralized logging also created a compliance blind spot: auditors would request access records, and the team would spend days manually correlating VPN logs, jump server event logs, and badge-in records to reconstruct who had accessed which asset and when. The refinery's legacy architecture was not merely insecure — it was operationally unsustainable, consuming IT staff time, frustrating end users, and leaving the organization unable to answer the most basic security question: **who is connected to our OT systems right now?**

The Solution: How Protocol Isolation Works

The refinery deployed Xona Critical System Gateways (CSGs) to replace the legacy architecture with a completely disconnected access model:

Browser-Based Connection

Users connect via any web browser over HTTPS port 443. No VPN, no agent, no plugin.

Authentication & Policy

MFA via SAML 2.0; RBAC and TBAC policies authorize users for specific assets during specific time windows.

Isolated Protocol Session

The CSG initiates the OT session (RDP/VNC/SSH) from the gateway to the asset, entirely inside the trusted OT network. The user's endpoint is never connected to the OT network.

Encrypted Pixel Streaming

The CSG converts protocol output into encrypted PNG pixels delivered to the browser over TLS. Users interact in real time but receive only pixels — no data, no protocol traffic.

Continuous Monitoring

Every session is video-recorded. Administrators can shadow sessions live and terminate instantly via the Kill Button. All activity is logged and forwarded to SIEM.

Solution Highlights — Xona Features Deployed
• **Protocol Isolation (PNG pixel streaming)**
• **Critical System Gateway (CSG) hardware**
• **Xona Central Manager (XCM) for centralized oversight**
• **MFA via SAML 2.0 + identity provider integration**
• **Role-Based + Time-Based Access Control (RBAC/TBAC)**
• **Full Session Video Recording**
• **Live Session Shadowing & Kill Button**
• **SIEM Integration (Splunk)**
• **Moderated File Transfer with Malware Scanning**
• **Credential Injection (vault-based)**

- **Lockbox Emergency Access Revocation**
- **Zero Footprint — browser-based, no agents**
- **HTTPS Port 443 Only**

Kill Chain Analysis: Xona Breaks Every Stage

The following analysis maps how protocol isolation disrupts each stage of a typical OT-targeted attack:

Kill Chain Stage	Traditional VPN / Jump Server	With Xona Protocol Isolation
1. Reconnaissance	VPN endpoints visible; service banners expose versions	BLOCKED — Only HTTPS/443; no OT service exposure
2. Initial Access	Stolen VPN credentials grant broad network access	BLOCKED — MFA + SAML; browser-only; no network access
3. Execution	Malware traverses VPN tunnel into OT network	BLOCKED — No tunnel; endpoint receives only encrypted pixels
4. Persistence	Backdoors installed on jump servers or OT assets	BLOCKED — No endpoint-to-asset path; moderated file transfer
5. Lateral Movement	Full network access enables IT-to-OT pivot	BLOCKED — Sessions scoped to individual assets; no traversal
6. Command & Control	C2 traffic blends with authorized VPN sessions	BLOCKED — Only pixel streams cross boundary; C2 impossible
7. Impact	Ransomware deploys across OT; data exfiltrated via VPN	BLOCKED — No payload delivery path; malware scanning on files

At every stage of the cyber kill chain, protocol isolation eliminates the attacker's path forward. There is no stage at which a compromised endpoint can reach the OT environment, deliver a payload, or establish persistence.

Implementation and Results

- **Deployed in days, not months.** The Xona deployment was completed in just a few days using the platform's overlay architecture — no network reconfiguration, no firewall changes, no modifications to OT assets. A different team from the one that ran the POC completed the deployment, demonstrating operational simplicity.
- **Zero latency for end users.** From day one, users reported zero perceptible latency. The pixel streaming architecture delivers responsive real-time interaction even for graphically intensive HMI and DCS interfaces.

> *"This is one of the better user interfaces I have used. The overwhelming experience is light years ahead of our old solution."*
>
> **— Senior Applications Engineer, Instrumentation and Process Control**

- **Zero recorded security incidents attributable to remote access since deployment.** All 500+ critical assets are now protected with no direct endpoint-to-asset connectivity. A complete audit trail — full video recording, detailed event logs, and SIEM integration — provides comprehensive forensic capability. When the board asks "could this happen to us?" the security team can demonstrate exactly why it cannot.

> *"When our board asked if what happened to our competitor could happen to us, our security team had a two-word answer: protocol isolation. It doesn't reduce risk — it structurally eliminates the attack path."*
>
> **— CISO, Leading Energy Company**

Looking Ahead

With Volt Typhoon and similar state-sponsored groups continuing to target energy infrastructure, and industrial ransomware growing at double-digit rates year over year, protocol isolation represents a structural advantage — not merely a point-in-time fix. The energy company is now evaluating expansion of the Xona platform to upstream and midstream operations, applying the same protocol isolation architecture to pipeline SCADA, wellhead controllers, and compressor station control systems across its vertically integrated portfolio.

For any refinery or energy operator asking "could this happen to us?" the answer depends on one question: does an attacker have a path from an endpoint to your OT network? With protocol isolation, the path simply does not exist.

About Xona Systems

Xona Systems is the secure access platform purpose-built for OT and critical infrastructure. Recognized as an Overall, Product, Innovation, and Market Leader in KuppingerCole's 2025 Leadership Compass for Secure Remote Access for OT/ICS, Xona is deployed in 40+ countries across energy, utilities, manufacturing, oil & gas, maritime, water, defense, and mining.

*Learn more at **xonasystems.com***