Case Study

How a Fortune 500 Manufacturer Replaced a Failed PAM Deployment in 14 Days

How Xona Critical System Gateways Delivered 100% OT Asset Coverage, IEC 62443 Compliance on the First Attempt, and a 68% TCO Reduction After 18 Months of IT-Centric PAM Failure.

Executive Summary

A Fortune 500 diversified manufacturer operating 42 facilities with 850+ OT assets spent 18 months and $765,000 attempting to deploy an IT-centric PAM solution. After covering only 12 of 42 sites, accumulating 7 compliance findings, and achieving user satisfaction of 4.2/10, the organization replaced the failed deployment with **Xona Critical System Gateways**.

The result is what Xona calls "disconnected access" — users interact with OT systems in real time, but their endpoints are never connected to the OT network. Deploying across all 42 facilities in just 14 days — with an 18-minute average per site and no network changes — the manufacturer achieved 100% asset coverage, passed its IEC 62443 audit on the first attempt, reduced security incidents by 87%, and cut projected 5-year TCO by 68% to $1.985 million.

RESULTS AT A GLANCE	
42 Sites / 14 Days	Complete Deployment
90%	Faster Deployment vs. Legacy PAM
$1.985M	5-Year TCO (68% Reduction)
87%	Fewer Security Incidents
100%	OT Asset Coverage (was 35%)
9.1 / 10	User Satisfaction (was 4.2)
0	Compliance Findings (was 7)

The Challenge: 18 Months, 12 Sites, and a Growing Compliance Gap

This manufacturer produces chemicals, polymers, and building materials across 42 process manufacturing facilities. With 850+ OT assets connected via Modbus, OPC UA, EtherNet/IP, and Profinet, the organization required secure remote access for 275 internal OT engineers and 180+ third-party vendors and OEM contractors. Eighteen months earlier, the organization invested in an IT-centric PAM platform. The results were deeply disappointing.

- **Stalled deployment:** After 18 months and $765K ($425K licensing + $340K professional services — 80% cost overrun), only 12 of 42 facilities were operational.
- **No OT protocol support:** No native support for Modbus, OPC UA, EtherNet/IP, or Profinet. OT teams maintained parallel access methods, undermining the deployment.
- **7 compliance findings:** Audit gaps in access governance, session monitoring, and evidence. The PAM tool lacked OT-specific session recording and protocol isolation required by IEC 62443.
- **3.2 security incidents/month:** With only 35% asset coverage, unauthorized access attempts, credential sharing, and unmonitored vendor sessions persisted.
- **4.2-hour vendor access time:** Provisioning required coordination across IT, OT, and the PAM vendor's support team. Open tickets were unresolved for 4+ months.
- **4.2/10 user satisfaction:** OT engineers actively circumvented the tool using unauthorized methods — increasing risk.
- **$6.28M projected 5-year TCO:** Extrapolating the deployment pace to all 42 sites — not including production downtime costs.

Evaluating Alternatives

The CISO and OT Security Director evaluated several options:

- **OT visibility vendors (Claroty xDome):** Bolt-on SRA to a broader platform; deployment complexity and timeline concerns.
- **Emerging OT specialists (Dispel, Cyolo):** Lacked the combination of pre-configured hardware, zero-footprint access, and comprehensive IEC 62443 documentation.
- **Extending existing PAM:** Rejected — 18 months of evidence proved the IT-centric architecture could not meet OT requirements.

Xona was selected for: OT-native design (protocol isolation, industrial hardware, OT protocol support), deployment speed (20-minute per-site verified in POC), and IEC 62443 alignment (third-party tested against ANSI/ISA-62443-2-1, 3-3, and 4-2).

Why IT-Centric PAM Fails in OT

This experience is not unique. IT PAM tools — designed for servers, databases, and cloud infrastructure — consistently fail in OT:

WHY IT-CENTRIC PAM FAILS IN OT ENVIRONMENTS	
Agent Requirements	IT PAM tools require software agents on endpoints and targets. Most OT assets — PLCs, RTUs, DCS controllers — cannot run agents, and installing them risks stability and voids warranties.
Protocol Gaps	IT PAM supports RDP and SSH but lacks native support for Modbus, OPC UA, EtherNet/IP, and Profinet — forcing OT teams to maintain parallel access methods.
Deployment Complexity	Extensive network integration, firewall reconfiguration, and professional services. This organization's IT PAM took 18 months to cover 12 of 42 sites.
Operational Disruption	IT security tools assume scheduled maintenance windows. OT runs 24/7/365 where brief outages cost $185,000+ per hour in lost production.
Compliance Gaps	IT PAM provides IT audit trails but not OT-specific session recording, protocol isolation, or intermediate system capabilities required by IEC 62443 and NERC CIP.

The fundamental problem is architectural: IT PAM was designed for systems that run standard OSes, accept agents, use IT protocols, and operate in well-connected data centers. OT environments have proprietary protocols, legacy systems that cannot be modified, constrained networks, and zero tolerance for downtime. A purpose-built solution addresses these constraints by design.

The Solution: Xona Critical System Gateway

Xona's architecture addressed every gap that caused the IT PAM deployment to fail:

Protocol Isolation

OT protocols terminate inside the trusted plant network. Users connect through a browser over HTTPS port 443 and receive only encrypted pixel streams — never a direct connection to the OT asset. This architecture eliminates ransomware propagation, lateral movement, and malware injection vectors.

Native OT Protocol Support

Sessions to assets communicating via Modbus, OPC UA, EtherNet/IP, Profinet, DNP3, and serial interfaces through a single browser interface — no parallel access methods.

Pre-Configured Hardware

DIN-rail or 1U rack appliances arrive ready to install. Mount, connect Ethernet, assign IP. No agents, plugins, or VPN clients on any endpoint.XCM Centralized Management

Centralized Management (XCM)

Fleet-wide policy, SAML 2.0 identity federation, centralized logging, and unified reporting across all 42 sites.

Solution Highlights — Xona Features Deployed
✓ Protocol Isolation (pixel streaming, HTTPS 443)
✓ JIT Vendor Access with Moderated Approval
✓ OT Protocol Support (Modbus, OPC UA, EtherNet/IP, Profinet)
✓ Full Session Recording (RDP, SSH, VNC)
✓ Pre-configured Hardware & VM Deployment
✓ Credential Injection (no shared passwords)
✓ Zero-Footprint Browser Access (no agents)
✓ IEC 62443 Alignment (third-party tested)
✓ XCM Centralized Multi-Site Policy
✓ SIEM Integration (Splunk, QRadar, Sentinel)

Implementation: 42 Sites in 14 Days

Following a POC at 3 facilities, full deployment was authorized. Critically, the **production deployment was completed by a different two-person team** than the POC team — demonstrating that Xona's simplicity does not depend on specialized expertise.

- **Timeline:** 14 calendar days from authorization to full operational coverage across all 42 facilities.
- **Average per site:** 18 minutes from hardware mounting to first authenticated session.
- **Team:** 2 engineers (one hardware, one remote XCM configuration).
- **Network changes:** Zero. Overlay architecture requires only HTTPS 443 outbound.
- **Vendor onboarding:** 180+ third-party vendors with individual SAML identities, enforced MFA, scoped asset access, and time-based controls. Credential injection eliminated all shared passwords.

Results: Before and After

Metric	Before (IT PAM)	After (Xona)	Improvement
Deployment Completion	12/42 sites (18 months)	42/42 sites (14 days)	90% faster
5-Year TCO	$6.28M (projected)	$1.985M	68% reduction
Security Incidents/Month	3.2	0.4	87% reduction
OT Asset Coverage	35%	100%	+65 points
Vendor Access Time	4.2 hours	8 minutes	97% faster
Compliance Findings	7	0	100% eliminated
Help Desk Overhead	Baseline	−40 hrs/month	Significant
User Satisfaction	4.2/10	9.1/10	+4.9 points
IEC 62443 Audit	Not attempted	Passed first attempt	—
NERC CIP-003-9	Non-compliant	Compliant (90 days)	—
Production Losses	$6.5M/yr at risk	Recovered	High-value ROI

Financial impact: Beyond the 68% TCO reduction, the organization recovered approximately $6.5 million per year in avoided production losses. The previous tool's access failures contributed to ~35 hours/month of unplanned downtime at $185,000/hour. A single prevented access-related incident returns the entire 5-year platform cost.

> *"We spent 18 months and $765,000 getting to 12 sites with our previous solution. Xona covered all 42 in two weeks. When we passed IEC 62443 on the first attempt, the board asked what else we could deploy Xona on."*
>
> **— CISO, Fortune 500 Industrial Manufacturer**

Looking Ahead

- **IEC 62443 Level 3 path:** Pursuing Level 3 security assurance for highest-risk manufacturing zones, leveraging Xona's advanced session controls and cryptographic log signing.
- **Forescout integration:** Automated asset discovery and dynamic risk-based access policy — high-risk asset conditions automatically restrict Xona sessions.
- **Acquisition integration:** New facilities brought onto Xona within days, making secure access a standard part of facility onboarding.
- **NERC CIP-003-9:** Full Section 6 compliance achieved within 90 days — well ahead of the April 1, 2026 deadline.About Xona Systems

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.***