Case Study

Eliminating $1.2M in Annual OEM Site Visits: A Power Generation OEM's Remote Support Transformation

How a global gas turbine OEM standardized 200+ power plants across 30+ countries on a single secure platform — achieving NERC CIP compliance and eliminating 600+ on-site visits per year.

xona

Executive Summary

Organization	Global Gas Turbine OEM
Support Scope	200+ power plants across 30+ countries
Service Model	"Follow the sun" 24/7 remote and on-site support
Previous Approach	600+ on-site visits/year; multiple customer-specific access tools
Annual Visit Cost	$1.2M+ ($2,000+ average per visit)

A global gas turbine OEM providing lifecycle support to more than 200 power plants worldwide was spending over $1.2 million annually on on-site service visits. The barrier to remote support was not technology — it was trust. Utility and IPP customers systematically blocked VPN-based remote access, citing NERC CIP compliance requirements and lack of visibility into OEM sessions. Meanwhile, the OEM juggled multiple customer-specific access tools, creating tool sprawl, credential sharing risks, and inconsistent security.

By standardizing on Xona Systems, the OEM achieved what neither side could accomplish independently: a single secure platform that satisfied the most demanding utility compliance requirements while enabling the remote support capability the OEM needed. The result: $1.2M+ in eliminated site visit costs, support response reduced from days to minutes, and a new premium remote monitoring revenue stream.

The result is zero direct network connectivity — OEM technicians interact with plant systems in real time, but their endpoints are never connected to the OT network.

RESULTS AT A GLANCE	
$1.2M+	Annual savings from 600+ eliminated on-site visits
Days → Minutes	Support response time for routine and urgent issues
200+ Plants	Standardized on one platform across 30+ countries
NERC CIP-003-9	Section 6 alignment — enabling utilities to demonstrate compliance
Zero	Credential exposure — OEM techs never see plant passwords
New Revenue	Premium remote monitoring services unlocked as a new revenue stream

Industry Context: The OEM Remote Support Problem

Power generation OEMs depend on providing lifecycle support — maintenance, optimization, firmware updates, diagnostics — to installed equipment at customer sites worldwide. A single domestic site visit averages $2,000+; international visits to remote locations can exceed $5,000-$10,000. For an OEM supporting 200+ plants, 600+ annual visits adds up to over $1.2M in direct travel costs before accounting for engineer productivity or delayed response.

The problem runs deeper than cost. Urgent issues wait 24-72 hours for a qualified engineer to arrive. For plant outages costing $50,000-$200,000 per hour in lost generation revenue, this delay is extraordinarily expensive. And as installed fleets grow globally, maintaining proportional field service capacity requires continuous hiring — a model that does not scale.

Why Customers Block Remote Access

Utility customers were not being unreasonable. They faced genuine compliance requirements that legacy remote access tools could not satisfy:

- **NERC CIP-005 Intermediate System.** All interactive remote access to BES Cyber Systems must go through an Intermediate System with MFA. Standard VPN connections do not qualify.
- **CIP-003-9 Vendor Controls.** Utilities must preauthorize vendor access, monitor sessions in real time, maintain full recordings, and retain instant revocation capability.
- **Credential management.** Utilities cannot share plant credentials with OEM technicians and maintain CIP-004 compliance — yet this is exactly what VPN-based access required.

Research shows organizations use 6 to 16 different remote access tools on average — each representing its own attack surface. The OEM's patchwork of customer-specific VPNs, jump servers, and screen-sharing tools created inconsistent security, multiple credential sets, and no centralized visibility.

The Challenge

The OEM needed to simultaneously: (1) eliminate $1.2M+ in unnecessary site visit costs; (2) provide remote access that met NERC CIP requirements so utility customers would approve it; and (3) replace the patchwork of customer-specific tools with a single platform across all 200+ customer plants. Any solution had to be acceptable to customers — many of whom had blocked all OEM remote access for years.

The Solution

Xona's Critical System Gateway (CSG)

Deploys at each customer plant site as a NERC CIP-compliant Intermediate System. OEM technicians connect from anywhere via browser over HTTPS (port 443 only). The CSG terminates OT protocol sessions (RDP, SSH, VNC) inside the plant's trusted network and streams only encrypted pixel images back — no direct OEM-to-plant connectivity, no VPN, no agents.

Credential Injection: The Key for OEM Access

Plant credentials are stored in an encrypted vault within the CSG at the customer site. When an authorized OEM technician initiates a session, the CSG injects credentials automatically — the technician works through the browser session without ever seeing or handling the password. Utilities no longer need to share plant credentials with OEM personnel — the issue that had blocked remote access for years.

Moderated Access: Customer Oversight

When an OEM technician requests access, the plant operator receives a real-time notification and must approve the session before it begins. During the session, operators can shadow the OEM's work live and terminate it instantly via the Kill Button. This transformed the dynamic from adversarial — "we can't let you in" — to collaborative: "we can see everything, so connect anytime."

Session Recording for Warranty and SLA Documentation

Every session is video-recorded with timestamps and metadata. For the OEM, recordings document work performed for warranty claims and SLA compliance. For customers, they satisfy NERC CIP-003-9 session recording requirements.

Solution Highlights — Key Xona Features
• **Protocol Isolation - Encrypted pixel streaming; no direct OEM-to-plant connectivity**
• **Xona Central Manager (XCM) - 200+ plants managed from a single console**
• **Credential Injection - OEM techs never see customer plant passwords**
• **Moderated Access / Wait Room - plant operators approve and supervise every session**
• **Full Session Video Recording - video evidence for warranty, SLA, and compliance**
• **Kill Button & Lockbox for — customers retain instant termination capability**
• **Time-Based Access Control - OEM access scoped to maintenance windows**
• **Low-Bandwidth Optimization - reliable streaming over constrained international links**

Implementation: Phased Rollout Aligned to Contract Cycles

Phase 1 — Months 1–6

Phase 1 covered 25 strategic accounts with the highest site visit frequency. The XCM deployed at the OEM's global service center provided centralized management. Each site deployment averaged 20-30 minutes with no changes to customer firewalls or SCADA networks.

Phase 2 — Months 6–18

Expanded to 125+ plants, including sites that had previously blocked all remote access.

Phase 3 — Months 18–36

Completed global standardization across 200+ plants, decommissioning all legacy customer-specific tools.

Results

Metric	
Annual site visit reduction	**600+ visits eliminated (~85%)**
Direct travel cost savings	**$1.2M+/year**
Engineer productivity gain	**~4,800 recovered travel hours/year**
Support response time	**24-72 hours → under 15 minutes**
Tool sprawl	**Multiple tools → one platform**
NERC CIP compliance	**Xona's architecture addresses all applicable NERC CIP-003-9 Section 6 requirements for vendor electronic remote access — enabling utilities to demonstrate compliance with third-party tested documentation.**
3-Year ROI	**>400%**

ROI Calculation

Previous annual spend	**$1.2M+ (600+ visits × $2,000+ per visit)**
Xona platform cost	**~$200K-$250K/year (enterprise volume pricing for 200+ CSGs + XCM)**
Net annual savings	**~$950K-$1M — platform paid for itself in under 3 months**
Additional value	**4,800 recovered engineer hours, faster response, new monitoring revenue**

Service Quality

24/7 "follow the sun"	**Global support centers provide continuous coverage — a plant issue at 2:00 AM gets the same response as one at noon.**
Expert-to-asset matching	**The right specialist connects to any plant worldwide without geographic constraints.**
Customer satisfaction	**Plant managers report higher satisfaction with speed and quality, strengthening service contract renewals.**

The OEM Business Case: From Cost Center to Revenue Enabler

Secure remote access fundamentally changes the economics of OEM service delivery. With compliant, secure, on-demand access to customer plants, the OEM now offers premium remote monitoring and predictive maintenance subscriptions as a new revenue tier. "Remote-first" service contracts are priced competitively while maintaining margins — competitors relying on site visits cannot match the economics.

Session recordings resolve warranty disputes objectively, reducing reserves and accelerating claims. And as the installed fleet grows, the OEM scales service without proportional headcount increases. For OEMs evaluating Xona, the platform is not just a security investment — it is a service delivery transformation that improves margins, accelerates growth, and creates sustainable competitive advantage in aftermarket services.

Looking Ahead

With the global fleet standardized on Xona, the OEM is pursuing several strategic initiatives:

Renewable equipment expansion

Extending secure remote access to wind turbine, solar inverter, and battery storage support.

Customer self-service portal

Integrated scheduling, session recording access, and policy management for plant operators.

AI-assisted diagnostics

Combining secure remote access with predictive analytics to identify issues before unplanned outages.

Channel partner enablement

Extending the platform to authorized service partners under the OEM's governance umbrella.

> *"We spent years trying to convince our customers to let us connect remotely. The answer was always: 'You can't meet our security requirements.' With Xona, we don't have that conversation anymore. Customers see the moderated access, the session recording, the credential injection, and they say, 'When can you deploy it?' That's a complete reversal."*
>
> *— VP Service Operations, Global Gas Turbine OEM*

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***