SOLUTION BRIEF

Xona: Secure Access for Critical Infrastructure

Xona isolates access to critical infrastructure at the protocol level. No VPN tunnels. No endpoint agents. No network changes. Users connect through encrypted pixel streams, not network tunnels. Their endpoints never touch the OT environment. With Xona, ransomware risk is mitigated as the remote contractor laptop is removed from the attack surface.

40+	20	1M+
COUNTRIES	MIN. DEPLOY	ASSETS PROTECTED

KEY DIFFERENTIATORS

Protocol Isolation Technology

Proprietary technology translates critical system protocols into interactive video streams, breaking the cyber kill chain.

20-Minute Deployment

Rapid implementation without network reconfiguration or downtime.

Network-Independent Deployment

Deploys as an overlay on existing infrastructure. On-premises, hybrid, or air-gapped. No network changes required.

Zero Footprint Access

Browser-based solution requiring no clients, agents, or plugins.

WHY TRADITIONAL MODELS FALL SHORT

VPNs

Extend network connectivity. Lateral movement possible, persistent attack surface.

PAM

Manages credentials, but doesn't govern what happens inside a session.

Jump Hosts

Require patching, endpoint trust, and ongoing management overhead.

WHY CHOOSE XONA?

1. **Eliminate Endpoint Risk**
   Protocol isolation ensures insecure user endpoints never connect directly to the critical OT network.
2. **Operators Connect in Seconds**
   Browser-based access from any device, including tablets in the field. Sub-100ms latency over satellite inks. Supports Windows XP, Modbus, and DNP3 without modification.
3. **Streamline Compliance and Auditing**
   Automatic session recording, metadata capture, and compliance-aligned evidence artifacts. Audit prep: 6 months to 3 weeks.

BUILT FOR OT OPERATORS

Security controls only work if they support how operations actually function.

Granular, Zero-Trust Access Control

Just-in-Time (JIT) & Role-Based Access, Moderated Secure File Transfer, and Credential Injection ensuring users never handle passwords.

Session Hold and RDP Auto-Reconnect

Your session survives a dropped VSAT link or a network switchover. Pick up where you left off, no re-authentication required.

Session Transfer

Authorized live handoff between users without disconnecting.

Centralized Oversight

Administrators shadow live sessions, take over control, and replay access recordings from one console. Every site, every session, governed from the Xona Central Manager.

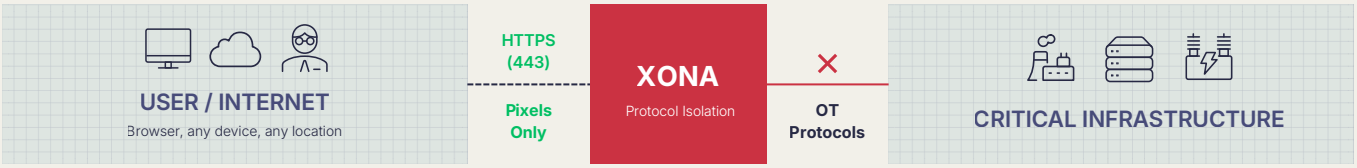
Concurrent Multi-Protocol Sessions

Run RDP, SSH, and Web connections simultaneously in a single window.

Operational Efficiency

Deploy in 20 minutes. Your field engineer and the OEM specialist work the same session from different locations. Session Transfer hands off control without disconnecting.

PROTOCOL ISOLATION ARCHITECTURE



No direct connection. User endpoints never touch the OT network.

TARGET USE CASES

Control Third-Party Vendor & OEM Access

Enable vendors and contractors to securely access specific systems without needing VPNs or jump servers. Fully managed, just-in-time access.

Enable Secure Employee Access

Provide real-time oversight for users working remotely or onsite. Minimize the internal attack surface.

Replace Legacy Access Technology

Consolidate the tech stack and reduce costs by replacing multiple legacy solutions (VPNs, jump servers, basic PAM tools) with one unified platform.

COMPLIANCE ALIGNMENT

✓ NERC CIP | ✓ IEC 62443 | ✓ NIST 800-53 | ✓ NIS2 | ✓ OTCC-1:2022 | ✓ TSA Security Directives

Protect Critical Operations with Secure, Verified Access.

REQUEST A DEMO

www.xonasystems.com

© 2026 Xona Systems, Inc. All rights reserved.