

The Xona Platform versus VPN + Cloud



Introduction

Why Legacy VPN Solutions No Longer Meet OT Access Requirements

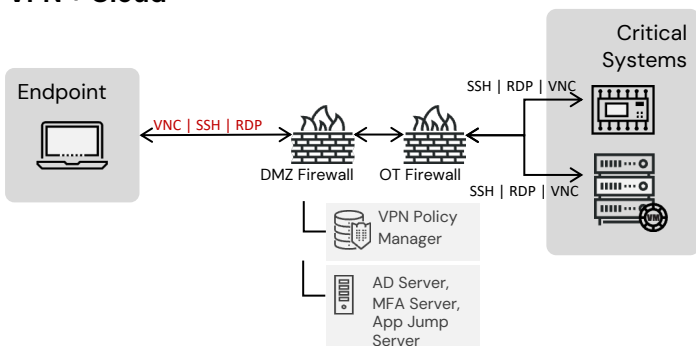
As critical infrastructure grows more connected, legacy access technologies like VPNs fail to keep pace with today's security, compliance, and operational requirements. Originally designed to provide private network access, VPNs now present serious risks in Operational Technology (OT) environments—especially when combined with cloud-based provisioning and unmanaged endpoints.

With increasing threats from ransomware, remote exploits, and credential misuse, the VPN model—based on broad trust and flat access—is fundamentally misaligned with modern cybersecurity mandates like Zero Trust, NERC CIP, TSA SDO2E, and IEC 62443.

Xona replaces this obsolete paradigm with a platform that is secure by design, purpose-built for OT, and effortless to deploy and use.

Solution Architecture Comparison

VPN + Cloud



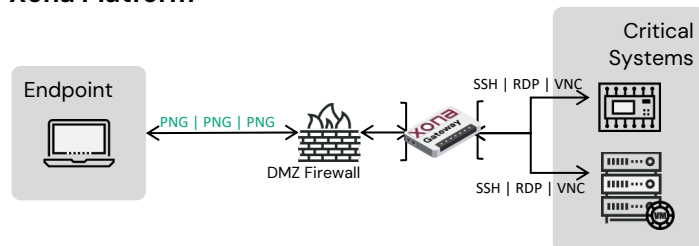
A typical OT remote access stack using VPN + cloud provisioning includes:

- **Client Agent:** Installed on a remote user's endpoint.
- **Public Cloud Service:** For provisioning, cert management, and access brokerage.
- **Onsite Hardware Gateway:** Limited in scale; requires tight integration into the control network.

Risks Introduced:

- Untrusted endpoints with full network access.
- Multiple software agents, certificates, and cloud dependencies.
- OT systems and protocols exposed outside the trusted OT network to unmanaged devices.

Xona Platform



Uses disconnected access and zero trust principles to deliver secure access to critical systems. It requires:

- **One hardened Gateway (CSG)** installed at each protected site.
- **No user endpoint software**—no VPN client software, no agents, no native software, no cloud access required.

Key Benefits:

- No user endpoint connectivity to critical systems.
- Streamed access via HTTPS (TLS 443) only.
- Enforces protocol and endpoint isolation.
- No reliance on cloud for session brokering or identity.

Key Feature Comparisons

Key Features	Xona Platform	VPN + Cloud
Zero Trust Architecture	✓	✗
Protocol Isolation (No Network Exposure)	✓	✗
No Data in Transit (Pixel Streaming)	✓	✗
Browser-Based Access (Zero Footprint)	✓	✗
Multi-Factor Authentication	✓	✗ (Based on provider)
Secure File Transfer (Moderated)	✓	✗
Live Session Monitoring	✓	✗
Session Recording (Video + Logging)	✓	✗
Deployment Time per Site	< 30 minutes	Days to weeks
Solution Scalability	Virtually unlimited	Typically, very limited
User Client Software Required	None	Yes (VPN client)
Maintenance Overhead for OT Teams	Low	High
Security Admin Experience	Streamlined and unified	Fragmented and siloed
NERC CIP-003, CIP-005, CIP-007, CIP-011	✓	✗
IEC 62443 (Access Control, Monitoring)	✓	✗
TSA SD02E (Pipeline Access Controls)	✓	✗
Saudi OTCC-1:2022 (Access Mgmt)	✓	✗
Zero Trust & Least Privilege Enforcement	✓	✗

Conclusion

VPNs are a relic of IT security thinking. In OT environments, they expose more than they protect—creating unacceptable risk for critical infrastructure operators. Xona replaces VPNs with a purpose-built platform for OT access:

- Eliminates insecure endpoints from connecting to critical assets, systems, and applications
- Reduces operational overhead and burdens on OT teams
- Ensures compliance across all major mandates
- Delivers secure access in under 30 minutes per site

It's not just more secure. It's safer. Simpler. Smarter.



Xona Platform Value for Different Teams

<p>OT Field Operators</p> <p>What they need: Quick access to systems to fix issues remotely.</p> <p>How Xona helps: Simple 3-click access with no IT friction or client software.</p> <p><i>"Xona lets me access any plant system securely—without dealing with VPNs, firewalls, or waiting for IT."</i></p>	<p>IT & Security Teams</p> <p>What they need: Security without complexity.</p> <p>How Xona helps: Enforce Zero Trust, eliminates endpoint threats, integrates with AD/MFA.</p> <p><i>"We no longer worry about patching VPN clients or managing third-party remote access risk."</i></p>	<p>Compliance Teams</p> <p>What they need: Built-in audit trails and regulatory coverage.</p> <p>How Xona helps: Full session capture, user logs, and regulatory mappings.</p> <p><i>"Xona checks every compliance box we have—without extra tooling."</i></p>	<p>Procurement</p> <p>What they need: Cost-effective, scalable solution for business continuity.</p> <p>How Xona helps: Replace multiple tools (VPN, etc.) with one platform.</p> <p><i>"Xona simplifies procurement and reduces risk across all of our industrial sites."</i></p>
---	---	---	---

“Secure access and threat detection are foundational critical infrastructure steps that companies should implement to address major operational and business risks. **Unfortunately, too many still rely on legacy technologies such as VPNs and jump boxes, leaving OT and ICS environments with visibility gaps, unprotected critical systems, and insecure user endpoints connecting directly to critical systems.** The Nozomi Networks and Xona platforms address these challenges, so their integration should give industrial enterprises an additional reason to consider both vendors’ products.”

Rik Turner
Senior Principal Analyst at Omdia

Why Choose Xona?

 <p>Best-in-Class Secure Access: Zero-trust architecture protects critical systems from insecure user endpoints.</p>	 <p>Real-Time Oversight and Control: Supports employees, 3rd party contractors, and OEMs whether onsite or remote.</p>	 <p>Proven Track Record: Trusted by global organizations in energy, oil & gas, manufacturing, and critical infrastructure.</p>
--	--	--



Xona is a leading provider of secure access solutions for critical systems and operational technology environments. By combining unmatched security with ease of deployment, Xona helps organizations reduce their attack surface and comply with industry regulations while offering the best user experience on the market. Trusted by industry leaders across energy, manufacturing, and utilities, Xona’s solutions protect critical systems around the world.