COMPETITIVE COMPARISON GUIDE

The Xona Platform versus Jump Servers

Introduction

Why Jump Servers Fall Short in Critical Infrastructure Environments

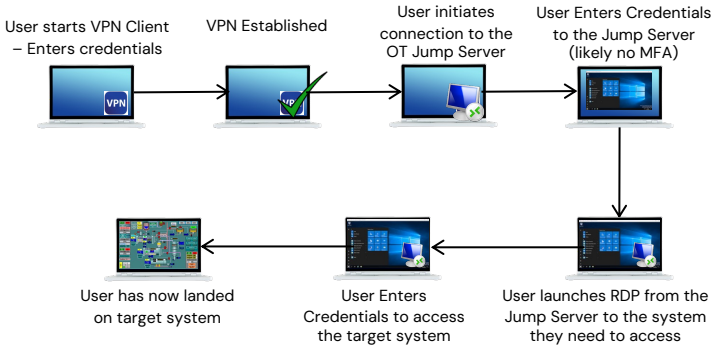
Jump servers, or bastion hosts, were historically used to create a single point of access to OT systems. While better than raw remote desktop exposure, traditional jump servers are fundamentally inadequate for today's threat landscape. They often:

- Rely on direct connectivity to OT systems exposing critical systems to insecure endpoints
- Require complex integration with MFA, firewalls, VPNs, and identity stores
- Are managed inconsistently across different facilities or sites
- Lack visibility, supervision, and compliance-ready logging

In contrast, **Xona replaces jump servers entirely** with a hardened platform that integrates access control, protocol isolation, audit, and zero-trust enforcement—all in one.

Solution Comparison

Traditional Jump Server



A jump server implementation typically involves:

- A Windows or Linux host with remote desktop software.
- Tightly coupled firewall/VPN configuration.
- MFA, logging, and encryption layers—added separately.
- Admin access into critical OT environments, often with full network reach.

Risks Introduced:

- Patchable attack surface inside the OT network.
- Lateral movement possible from compromised user endpoints.
- Manual and error-prone configuration.
- No built-in session monitoring or control override.

Xona Platform

The Xona Platform is purpose-built for OT and includes:

- 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:

- Replaces the jump server with streamed, isolated session access.
- Acts as both session broker and compliance monitor.
- Requires no direct connection to the user endpoint.
- Browser-based access (no RDP/VNC exposure).
- Includes built-in session recording and monitoring.

Key Feature Comparisons

Key Features	Xona Platform	Jump Servers
Zero Trust Access Enforcement	✅	❌
Protocol Isolation (No Network Exposure)	✅	❌
Hardware Token-Based MFA	✅	❌ (optional)
Secure File Transfer (Moderated)	✅	❌
Session Monitoring and Control Override	✅	❌ (limited)
Session Recording (Video + Logging)	✅	❌ (limited to none)
Resilient to Endpoint Compromise	✅	❌
Patchable Host OS / General Purpose OS	❌	✅ (risk)
Deployment Time per Site	< 30 minutes	Days to weeks (multi-layer)
Maintenance Overhead for OT Teams	Low	High
Centralized Admin and Monitoring	✅	❌ (fragmented & complex)
Firewall / VPN Dependency	❌	✅
User Training and Support Requirements	Low	High
Scalable Across Multi-Site Fleets	✅	❌ (siloed per site)
NERC CIP-003, CIP-005, CIP-007	✅	❌
IEC 62443 (Access Control, Monitoring)	✅	❌
TSA SD02E (Pipeline Access Controls)	✅	❌
Saudi OTCC-1:2022 (Access Mgmt)	✅	❌

Conclusion

It's Time to Retire the Jump Server

Jump servers are brittle, risky, and outdated. They offer a veneer of security—but leave OT systems exposed to credential misuse, endpoint threats, and compliance failures. Xona's Platform does more than just replace the jump server: It redefines access control for OT environments with built-in security, visibility, and simplicity.

- Purpose-built for OT
- Compliance out of the box
- Secure access in under 30 minutes per site
- No VPN. No RDP exposure. No patching.

Xona doesn't just improve access. It protects what matters.

Xona Platform Value for Different Teams

OT Field Operators

Challenge: Jump servers create friction when responding to issues.

How Xona helps: Instant, secure access from any browser of OT assets.

"I can finally access the HMI without calling IT to unlock the jump box."

IT & Security Teams

Challenge: Hardening and maintaining multiple jump servers increases risk.

How Xona helps: Enforces least, privilege, reduces the attack surface, integrates with existing IAM.

"With Xona, I sleep better. There is no shell access, no patching, and no worries."

Compliance Teams

Challenge: No audit trails, inconsistent configs, and compliance blind spots.

How Xona helps: Full session capture, user logs, and regulatory mappings.

"Xona gives us what the jump server never could – provable user access control."

Procurement

Challenge: Managing licenses and maintenance contracts across facilities.

How Xona helps: One scalable platform with simple pricing that replaces multiple tools.

"It's the only solution we've seen that scales without scaling our overhead."

"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
Senion Principal Analyst at Omdia

Why Choose Xona?

Best-in-Class Secure Access: Zero-trust architecture protects critical systems from insecure user endpoints.

Real-Time Oversight and Control: Supports employees, 3rd party contractors, and OEMs whether onsite or remote.

Proven Track Record: Trusted by global organizations in energy, oil & gas, manufacturing, and critical infrastructure.

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.