

Secure Access Meets Real-Time OT Visibility Enabling Cyber Resilience Across Critical Infrastructure



Introduction

Bridging the Gap Between Access and Visibility

Critical infrastructure organizations face mounting threats from insecure remote access, expanding third-party ecosystems, and siloed security tools. Traditional solutions like VPNs and jump servers expose OT systems to unnecessary risk while creating operational bottlenecks.

To address this challenge, Xona and Forescout have partnered to deliver a tightly integrated solution that merges secure, zero-trust access with dynamic OT asset visibility, monitoring, and enforcement. This joint solution empowers OT security teams to manage, govern, and respond to all access activity with full context—and no exposure.

Why Forescout + Xona?

Forescout delivers unmatched visibility and control over OT, IT, and IoT assets. Its 4D OT Security platform enables real-time device discovery, deep packet inspection, threat detection, and network segmentation across industrial networks.

Xona delivers the first platform for secure access to critical infrastructure, enabling secure, clientless access to critical systems with full session supervision, endpoint isolation, and role- and time-based access controls. Together, these platforms offer a comprehensive approach to OT security that simplifies compliance across operational networks.

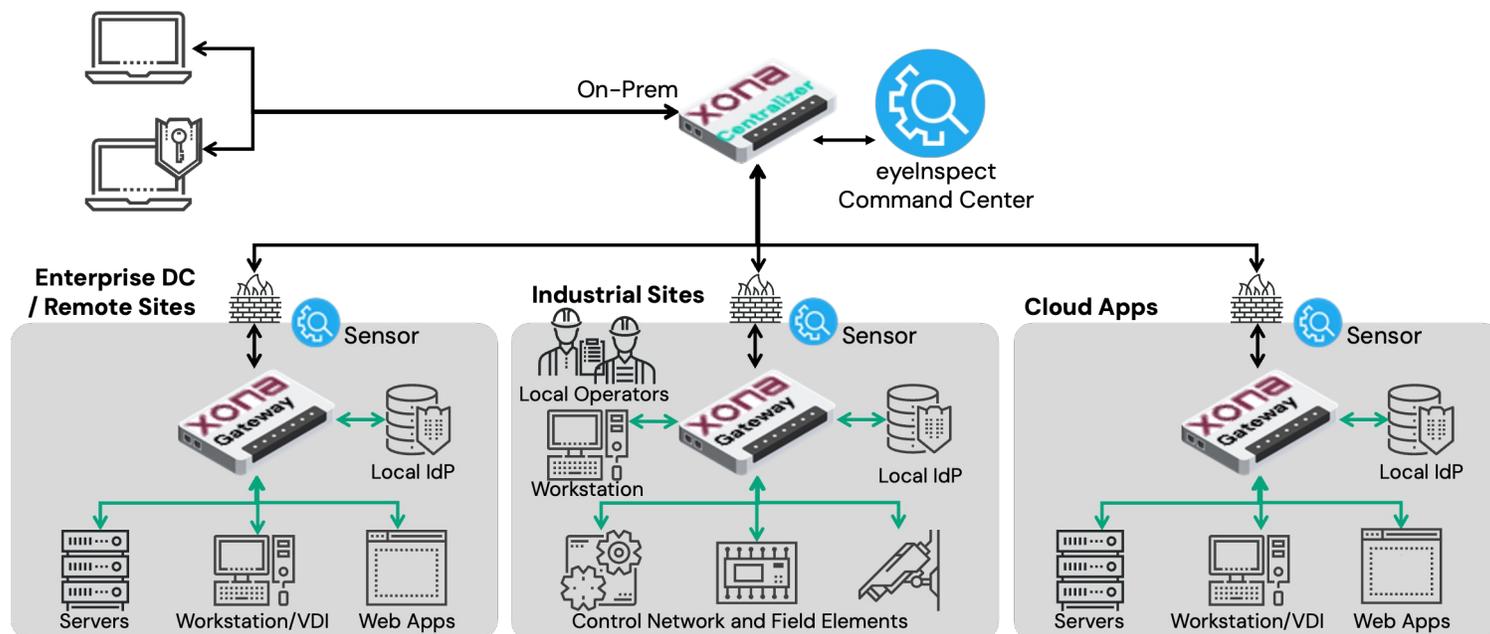
Better Together: Key Solution Capabilities

- **Zero-Trust Access with Reduced Operational Complexity:** Xona delivers secure, browser-based access to critical systems without VPNs, clients, or network tunnels. With Forescout's real-time asset discovery teams can dynamically identify and import assets for identity-level controls — ensuring users only access what they're authorized to.
- **Context-Aware Policy Enforcement:** Forescout's dynamic risk scoring and segmentation logic (via eyeControl and eyeSegment) automatically influence access permissions and session behavior inside Xona. High-risk assets can be isolated, and user access can be denied or revoked in real time—preventing lateral movement and enforcing least-privilege across the OT environment.
- **Secure Vendor and Third-Party Access Without Exposure:** Together, Xona and Forescout eliminate the traditional blind spots around remote access. Contractors, OEMs, and internal users can gain time-limited access with full oversight—without ever exposing underlying network layers or requiring standing credentials.
- **Built-In Compliance, Simplified Governance:** The joint solution supports audit-ready access governance for NERC CIP, IEC 62443, TSA SD2, NIS 2, and other standards. All session metadata and video logs are centrally recorded and correlated with Forescout's network-level intelligence.

Joint Solution Highlights

- **Stronger OT Security:** Eliminates insecure endpoints connecting to OT assets, reducing ransomware risks.
- **Automated Asset Discovery:** Forescout automatically discovers OT assets for onboarding into Xona's platform.
- **Seamless and Secure Access:** Identity-based controls enforce Zero Trust, preventing unauthorized access.
- **Regulatory Compliance:** Meets IEC 62443, NERC CIP, NIST 800-53 mandates and more.
- **Reduced Operational Complexity:** Eliminates VPNs, jump servers, and complex configurations, reducing IT burden.
- **Rapid, Agentless Deployments:** No client software, agents, plugins, or network architectural reconfigurations needed.

The Xona Platform with Forescout Integrations



The Joint Deployment Overview

Secure Access + Cyber Physical Systems Visibility

Forescout Components: Forescout's OT Security solutions deliver asset discovery, threat detection, and policy-based segmentation.

Xona Components: The Xona Platform deployed for critical systems access policy enforcement, attack surface reduction, and full logging and recording.

Integration Flow: Detailed asset visibility automates and informs asset configurations for identity-level access controls and least privileged access.

Purpose-Built for Critical Infrastructure

- Works across OT/ICS/XIoT/CPS domains.
- No required changes to existing network architectures.
- Supports disconnected and low-bandwidth environments.
- Enables third-party/OEM access without shared credentials.
- Integrates with AD, LDAP, SAML, and local identities.

Customer Benefits

- **Reduce Risk:** Stop insecure endpoint access and eliminate endpoint-based threat vectors to critical systems.
- **Improve Resilience:** Maintain uptime while enforcing zero-trust policies.
- **Accelerate Compliance:** Capture and report all session activity across access and network layers
- **Simplify Operations:** Automate and manage user access, asset visibility and threat detection through an integrated stack.

“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..”

Rik Turner

Senior Principal Analyst at Omdia

Why Choose Xona + Forescout?



Best-in-Class Secure Access: Xona's Zero Trust architecture protects critical systems from insecure endpoints.



Context-Aware Enforcement: Forescout continuously monitors asset postures and risk indicators.



Proven Track Record: Trusted by globally in energy, manufacturing, oil & gas, transportation, healthcare, and critical infrastructure.

"OT environments demand both visibility and control. Our partnership with Xona extends that control to secure remote access, ensuring every session is verified, authorized, and monitored with zero exceptions. Together, we're helping customers enforce zero trust principles across their most critical infrastructure to protect OT, IT, and cloud environments at scale."

Christina Hoefler

Vice President of OT/IoT Vertical and Strategy,
Forescout Technologies

Take the Next Step

Find out how Forescout and Xona can help your organization strengthen its secure remote access strategy while simplifying administration and compliance.

- **Schedule a Consultation:** Speak with our experts to discuss your specific security challenges.
- **Experience a Live Demo:** See the platforms in action through a guided demonstration.
- **Test the Technology:** Deploy a trial version to experience the benefits firsthand.

Contact us today to learn more about how Xona + Forescout can transform your secure access!

XONA

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.

<) FORESCOUT

For more than 20 years, Fortune 100 organizations, government agencies, and large enterprises have trusted Forescout as their foundation to manage cyber risk, ensure compliance, and mitigate threats. The Forescout 4D Platform™ delivers comprehensive asset intelligence, continuous assessment, and ongoing control over all managed and unmanaged, agented and un-agentable assets across IT, OT, IoT, and IoMT environments. Forescout's open platform makes every cybersecurity investment more effective with seamless data integrations and automated workflow orchestration across more than 100 security and IT products.

Forescout Research – Vedere Labs is the industry leader in device intelligence, curating unique and proprietary threat intelligence that powers Forescout's platform.