NIS2 COMPLIANCE – WITH SECURE ACCESS FOR CRITICAL INFRASTRUCTURE

How the Xona Platform Simplifies Regulatory Compliance for OT Environments

+1 866-849-6629 | info@xonasystems.com

The EU's NIS2 Directive sets a new standard for cybersecurity resilience across critical infrastructure. With expanded scope, stricter risk management expectations, and stronger mandates for access control, monitoring, and incident reporting, operators must now ensure their security frameworks are both effective and compliant.

The Xona Platform helps organizations meet these demands by providing a zero-trust, compliance-ready remote access solution. Purpose-built for critical infrastructure, Xona enforces least-privilege access, enables full session auditability, and supports integration with leading identity and security tools, all without requiring changes to existing network architectures.

"88% of industrial sites identify remote services as their top cybersecurity risk."

– DeNexus Report (2025)

THE CHALLENGE

NIS2 introduces new challenges for OT and ICS operators. They must:

- Ensure secure remote access while managing third-party vendors and distributed workforces.
- Enforce granular access control policies across hybrid OT/IT environments.
- Maintain real-time visibility, audit trails, and support access reviews.
- Replace insecure, complex legacy tools like VPNs, jump servers, and RDP tunnels.

THE SOLUTION:

The **Xona** Platform is designed to align directly with NIS2 Article 2, Section 11 access control requirements.

NIS2 Requirement	Xona Feature
Access granted based on least privilege	Role-based access control (RBAC) and policy enforcement. Xona enforces granular access per user based on roles and tasks.
Timely revocation of access rights	Just-in-time (JIT) access plus time limited sessions. Temporary, time-bound access minimizes standing privileges and automatically revokes rights. Xona also can automatically revoke rights that were instantiated by an IdP through its SAML connector.

NIS2 Requirement	Xona Feature
Access control procedures must be established and followed	Centralized access policy engine and management. Xona provides a centralized platform for defining and enforcing access policies systematically. Xona provides user access flexibility with native authentication designed for 3rd parties as well as integration with SAML to integrate with upstream IdP's as well as legacy LDAP/LDAPs for OT authentication.
Strong authentication mechanisms	Native multi-factor authentication (MFA). Xona can use either FIDO compliant hardware tokens or TOTP compliant mobile apps for its clientless native browser-based MFA access.
Monitoring and auditing of all access	Real-time session recording, monitoring, and audit logs. Every session is recorded and monitored for compliance, with detailed forensic logs.
Periodic access rights review	Native reporting and audit tools. Xona provides detailed user access logging and access recording which enables administrators to perform detailed periodic reviews of user access patterns and privileges for compliance checks. Xona also integrates with SIEMs and other log aggregation tools for additional reporting.
Xona also maps to IEC 62443 requirements for secure access control, and supports SAML, LDAP, Active Directory, and native OT authentication to unify identity across enterprise and industrial systems.	

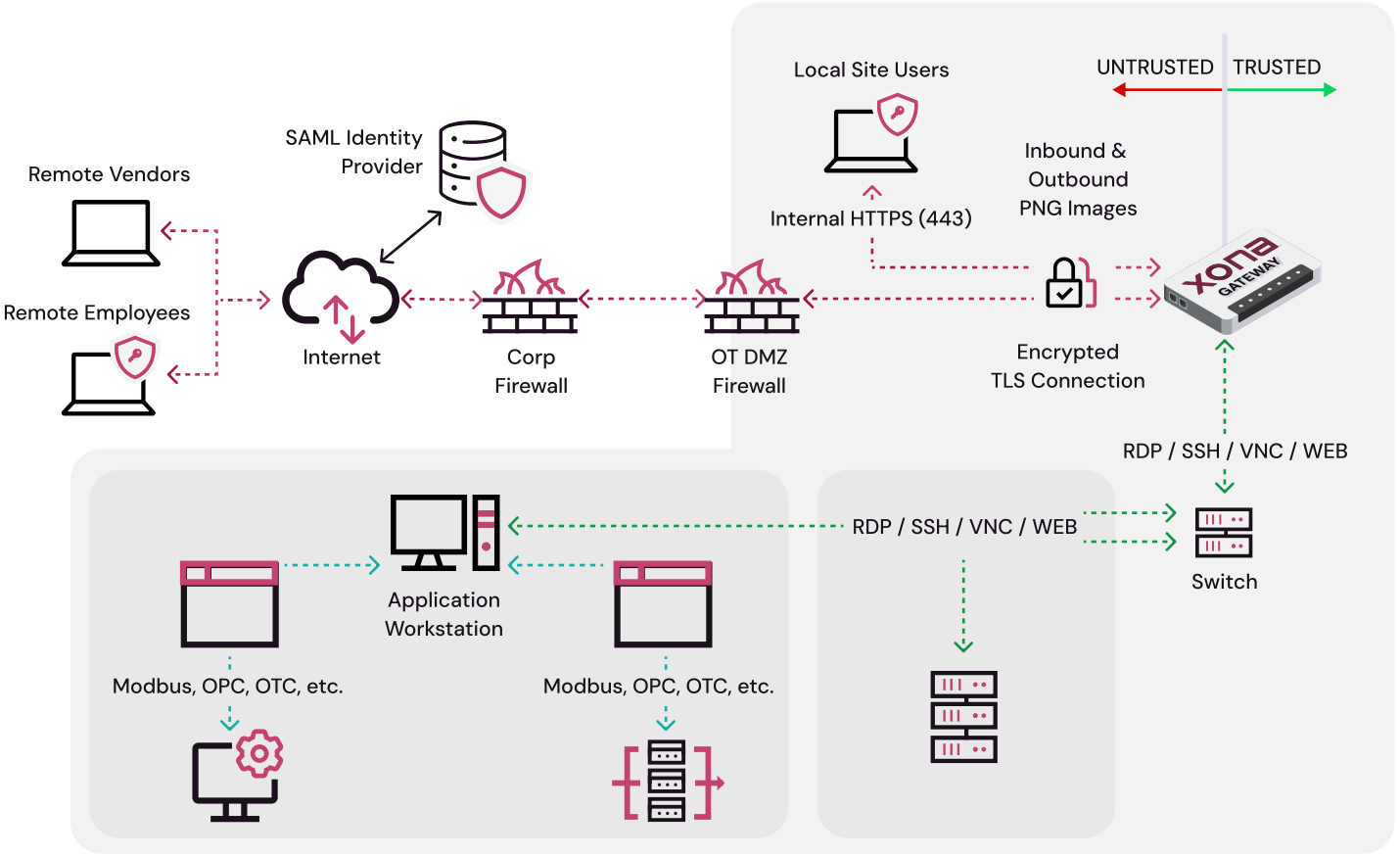
Xona Platform Benefits:

- Meets NIS2 Article 2, Section 11 requirements for access control and auditing
- Supports IEC 62443 and NIST 800-53 compliance
- Ensures access is role- and time-bound, minimizing insider risk
- Enables session logging and full forensic auditability
- Simplifies policy management across all users and sites
- Zero client or agent deployment makes it ideal for remote, distributed OT environments

Xona NIS2 Compliance Use Cases:

- Managing third-party vendor access with time-limited sessions
- Auditing remote access to OT assets for NIS2, NERC, and IEC mandates
- Replacing VPNs and jump servers to reduce compliance scope
- Performing periodic access reviews via Xona logs and SIEM integration
- Enforcing authentication standards across modern and legacy systems

XONA ARCHITECTURE – CORPORATE TO OT DMZ



ABOUT XONA

Xona's mission is to empower the heroes protecting the critical infrastructure (CI) our communities rely on every day. Xona delivers the first secure access for critical infrastructure platform—purpose-built to secure, control, and govern access to the world's most critical systems. Trusted by CI organizations in more than 40 countries, the Xona Platform replaces vulnerable legacy access tools like VPNs and jump servers. It delivers complete user access control, protects critical systems from insecure user endpoints, and ensures compliance with global security mandates, simplifying governance and strengthening operational security. Learn more at **www.xonasystems.com**.

+1 866-849-6629 | info@xonasystems.com