MEETING EU CYBER RESILIENCE ACT COMPLIANCE THROUGH SECURE ACCESS CONTROL

How the Xona Platform Simplifies Compliance with the EU Cyber Resilience Act

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

The EU Cyber Resilience Act (CRA) introduces broad expectations for manufacturers and vendors of digital products, emphasizing that cybersecurity should be integrated throughout the product lifecycle. With guidance around secure-by-design architecture, vulnerability handling, secure update delivery, secure access, and clear user documentation, the CRA holds developers and manufacturers accountable for mitigating strong security practices across product development, delivery and maintenance.

The Xona Platform helps critical infrastructure operators and industrial solution providers enable CRA-aligned practices by delivering secure remote access and auditability in OT and industrial environments. Built on zero-trust principles, Xona's secure access solution enforces least-privilege controls, supports secure patching and update workflows, and facilitates real-time monitoring and response, all without requiring changes to existing networks.

THE CHALLENGE

The Cyber Resilience Act increase compliance pressure on organizations that:

- Develop or integrate connected digital products and software into OT/ICS environments.
- Must demonstrate security-by-design, including secure maintenance and update processes.
- Need mechanisms for vulnerability reporting, secure update delivery, and logging.
- Are transitioning from legacy remote access tools that lack CRA-aligned protections.

THE SOLUTION:

The Xona Platform is designed to support CRA Chapter II & III objectives around secure product design, access controls, and cybersecurity management by enabling organizations to strengthen their patching, maintenance, and remote support capabilities.

CRA Requirement	Xona Feature
Implementation of security-by-design principles	Agentless, hardened access portal with least-privilege architecture
Secure access and user authentication	Role-based Access Control (RBAC) and Multi-Factor Authentication (MFA)
Event logging and activity monitoring	Full session recording, SIEM integration, and audit-ready logging

CRA Requirement	Xona Feature
Secure update and patch workflows	Enables controlled vendor access for patching and update validation
Vulnerability handling and risk mitigation	Time-bound access for incident response teams and real-time visibility
Minimization of attack surfaces	Eliminates VPNs, jump servers, and RDP tunnels
Xona also integrates with common enterprise security tools (SAML, LDAP, native OT protocols) to reduce integration overhead and ensure consistent control across connected systems.	

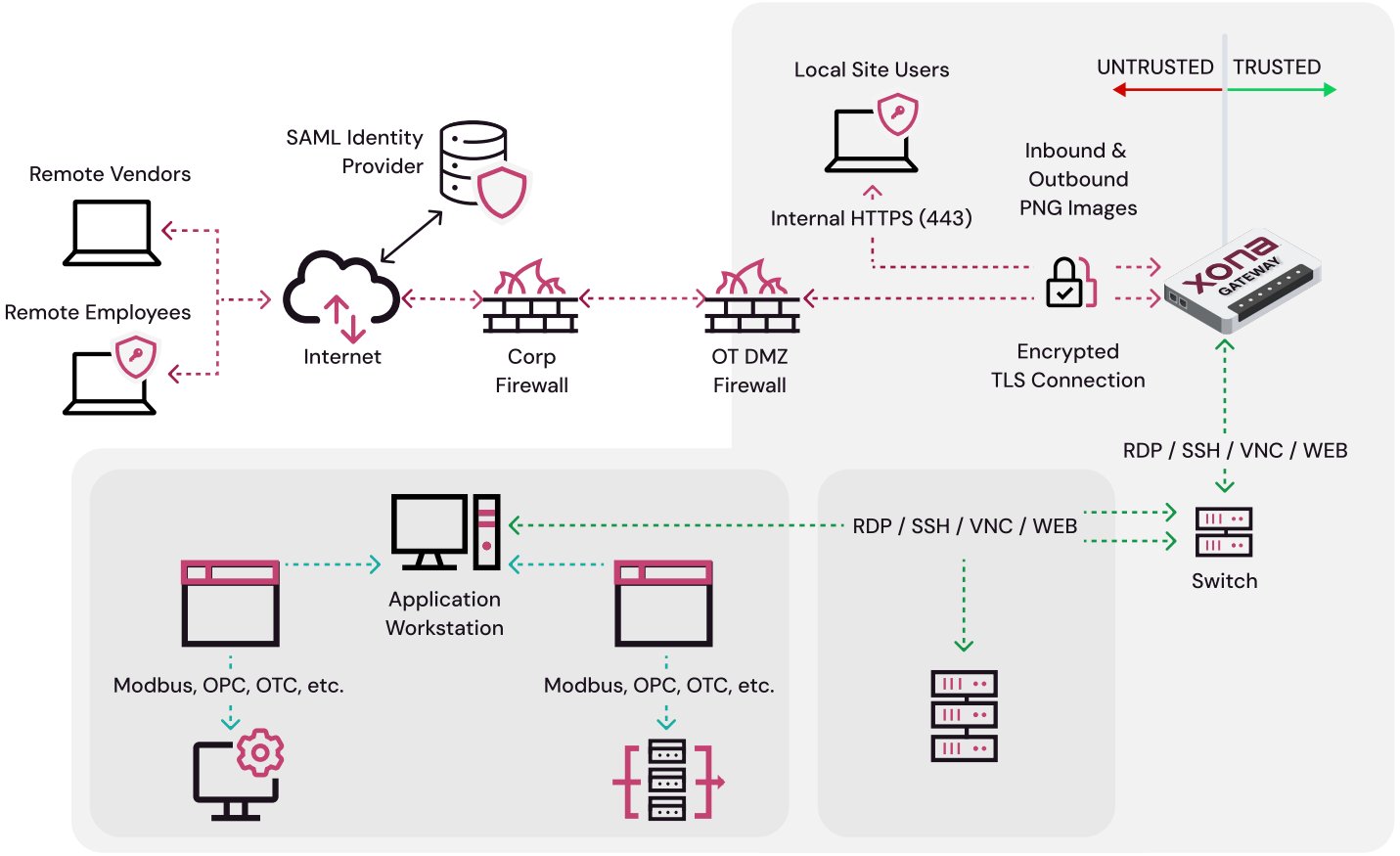
Xona Platform Benefits:

- Supports CRA Articles 10-15 for secure-by-design, access enablement, and logging
- Supports IEC 62443, NIST 800-53, and EU CRA-aligned obligations
- Prevents unauthorized access via role- and time-based controls
- Enables full forensic traceability through session logs and audit records
- Reduces supply chain risk by securing third-party vendor update workflows
- Requires no agents, making it ideal for complex industrial environments

Xona CRA Compliance Use Cases:

- Enabling CRA-aligned remote access for maintenance of industrial digital products
- Supporting secure update deployment through controlled vendor sessions
- Logging and auditing access for CRA and IEC 62443 reporting
- Minimizing product exposure by eliminating legacy access pathways
- Facilitating secure-by-design architectures in connected OT environments
- Supporting cybersecurity in delivery and maintenance phases with secure remote access for updates and enhancements

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 (SAFe-CI) 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