



DATA SHEETS

Remote Vendor Management

XONA™ develops and markets a secure access management platform to specifically address secure remote operations, mobile operations and cybersecurity (i.e., ransomware) for critical assets. The **XONA** remote operations platform is currently used across multiple critical infrastructure industries. **XONA** supports customers in every region globally, including North and South America, EU, Middle East and Asia.

**THIRD-PARTY BREACHES
ARE ON THE RISE**

51% of businesses have suffered a data breach caused by a third party, with 44% suffering a breach within the previous 12 months. Out of these 44% organizations, 74% data breaches were the result of giving too much privileged access to third parties.

SOURCE: SECURITY BOULEVARD

XONA PLATFORM FOR REMOTE VENDOR MANAGEMENT

XONA employs a holistic and frictionless zero-trust approach for vendors and other third parties to authenticate and connect to critical infrastructure assets. Several **XONA** features combined provide large organizations a simple and secure vendor management, including:

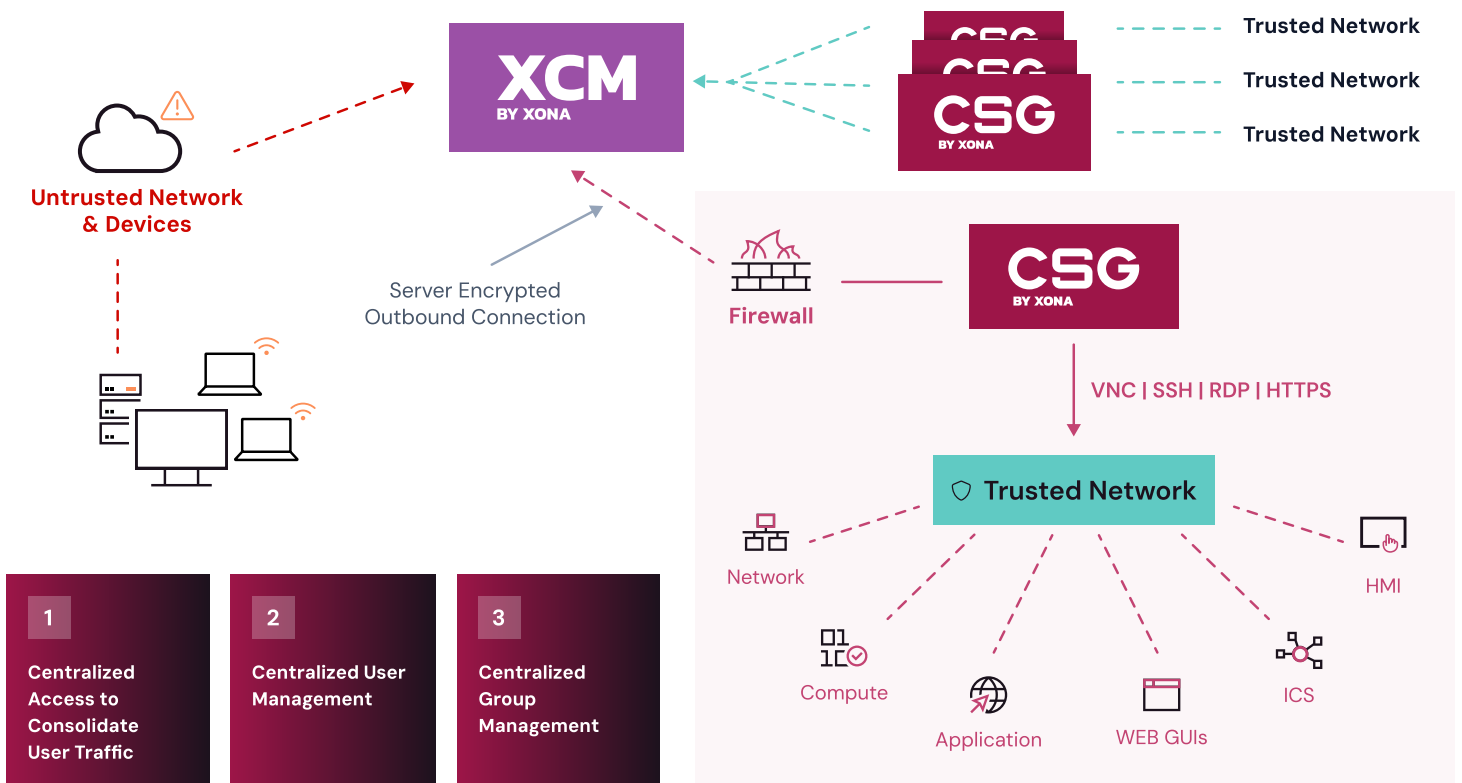
- **Utilization of clientless browser-based authentication and integrated hardware token-based multi-factor authentication (MFA)** – addresses the mismatch in access methodologies between organizations and third parties through a native browser over port 443
- **Asset and protocol isolation** – keeps each vendor isolated to only their assigned assets on the network.
- **Role-based access control (RBAC)** – provides granular control over access for organizations to allow specific functions such as operating a HMI or patching a server
- **Moderated secure file transfer** – files moving to or from a vendor system can be approved by the organization and logged for vendor access reporting and auditing purposes.
- **Moderated asset access control** – vendors accessing their critical assets can be moderated by managers to provide plant level control through a virtual “wait lobby” before connecting to their assets.
- **Full vendor access session logging and screen recording** – vendor access sessions are fully logged and recorded for both forensic and training purposes. Vendor access recordings can be utilized to ensure proper configuration or process initiation.

XONA PLATFORM – PRODUCT AND BUSINESS VALUE

The XONA Critical System Gateway (CSG) is a purpose-built appliance that meets the customer need for a simple, secure and cost-effective solution for users to access critical infrastructure assets.

- 1. Simple and Flexible Operation** – XONA can be easily implemented and configured by customers or their contractors in less than half a day.
- 2. Efficient Interfaces** – The CSG can interface with IT cybersecurity tools including firewall/UTMs, MFA tokens, SIEMS as well critical infrastructure asset discovery and cybersecurity solutions.
- 3. Reduces Operational Costs** – XONA allows companies to use less manpower at remote sites. XONA can be used by operators, contractors and vendors to securely access, patch and control critical systems remotely or locally using tablets for mobile operations.
- 4. Mitigates Operational and Training Issues** – Organization administrators or department managers can monitor field-based technicians in real time and provide guidance and training for new procedures or new technicians.
- 5. Meets Compliance Standards** – including IEC 62443, NIST 800-53, NERC IP, and others

XONA makes things **simple, secure, and transparent.**



ABOUT XONA

Xona provides the industry's leading zero-trust user access platform for Critical Infrastructure. Xona's mission is to enable your organization's workforce of employees, contractors, consultants, vendors and part-time workers to be more productive and more secure while reducing your operational costs. Xona seamlessly and securely enables secure adaptive access to your most critical systems and applications while also reducing operational and cyber risks and increasing operational efficiency.

