WHITEPAPER

The Power of XONA™: Supporting Operational Technology's Cybersecurity Mission

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

XONA's operational technology (OT) user access control and analytics software platform serves as the secure operational link between IT and OT enterprise for any connected asset. **XONA** provides the core security and operational functions for remote operations, delivering a set of secure and compliant features that are unavailable with either custom-built IT projects or standard commercial communications products. **XONA** addresses and mitigates elements of cyber risk that are facing organizations across multiple industry segments, including manufacturing, oil and gas, power generation and distribution, public sector, solar, hydroelectric and wind power.

THE XONA PLATFORM

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 user access to connected OT. The CSG provides user analytics for monitoring and review.

XONA's technology supports an array of cybersecurity requirements in the OT environment. Wide-ranging benefits and features include:

- Secure "clientless" browser-based multifactor authentication (MFA)
- Secure operational link for IIoT
- Role-based third-party vendor management
- Secure application access for monitoring and session logging
- Application screen recording for forensics and training
- Centralized management, visibility and control of authorized user access
- NERC-CIP compliant

GARTNER'S FRAMEWORK FOR SECURITY CONTROLS FOR OT

Gartner recently released a recommended framework for Security Controls for Operational Technology to improve security posture across their facilities and prevent incidents in the digital world from having an adverse effect in the physical world. The XONA platform provides a number of the recommended controls, further validating XONA as a solution to a wide array of cybersecurity challenges.

THE 10 OPERATIONAL TECHNOLOGY SECURITY CONTROLS

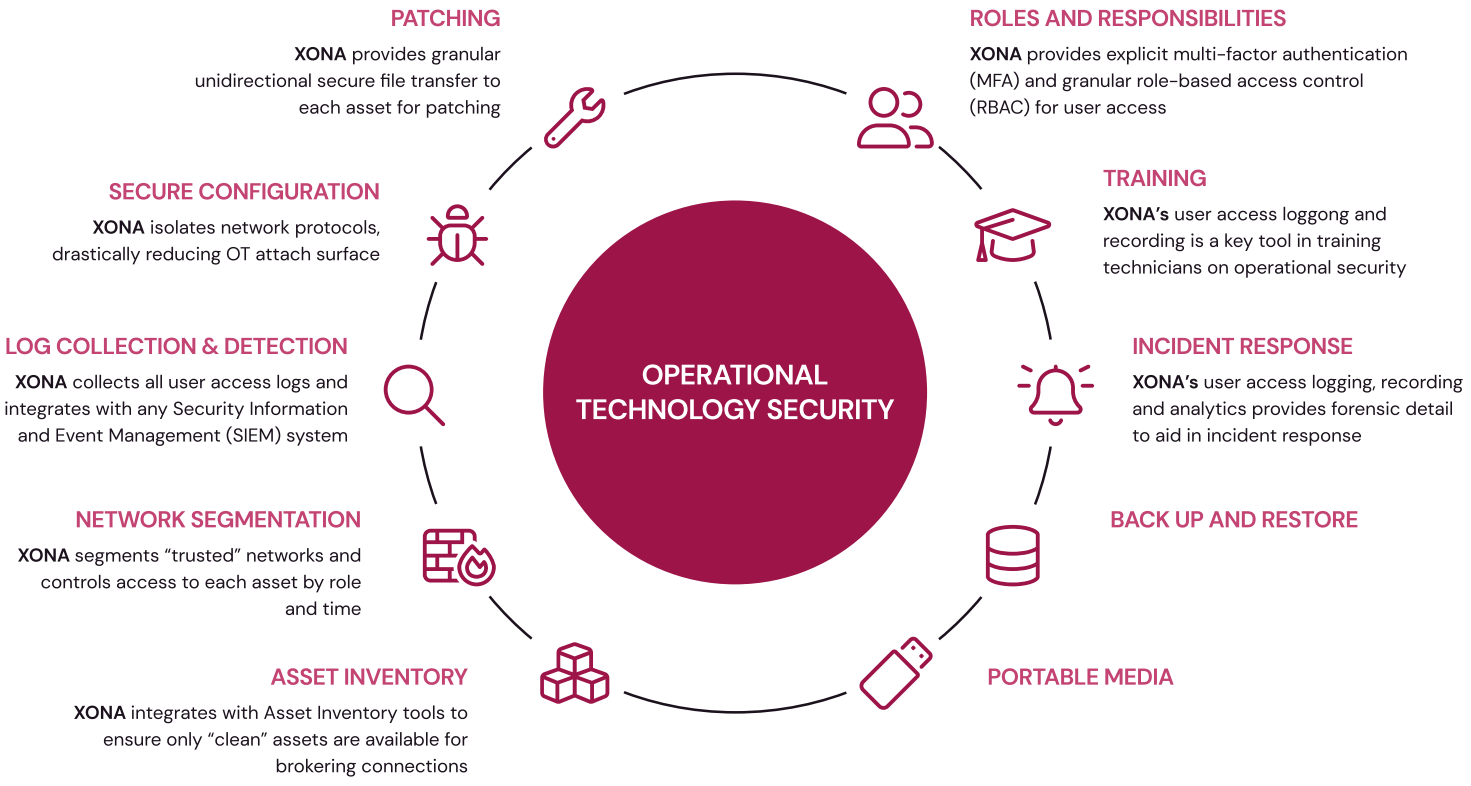

Figure 1. Gartner 10 OT Security Controls

APPLICATION OF XONA IN SUPPORT OF OT CYBERSECURITY SERVICES

PROTECT CONNECTED ASSETS WITH THE REQUIRED AUTHENTICATION AND AUTHORIZATION

OT assets need to employ a zero-trust user access platform that includes multi-factor authentication (MFA), flexible role- and time-based user and vendor access controls, as well as full session logging, monitoring and recording to directly address attacks to connected assets or open ports.

Critical infrastructure systems including OT connected assets are being exploited by threat actors. The new reality is that these actors are targeting weaknesses in the OT environment such as open ports, lack of proper OT network segmentation, lack of MFA on points of access and back doors through third party vendors.

NIST Zero Trust Architecture recommends a Policy Enforcement Point (PEP) for enabling, monitoring, and eventually terminating connections for connecting to an enterprise resource. The PEP should be capable of providing explicit authentication and authorization for access to an asset. The ZTA recommends use of trusted and untrusted ports. The **XONA** platform aligns directly with these ZTA requirements.

The **XONA** CSG provides a secure operational link or PEP between the IT and OT enterprise or for any connected assets. The CSG directly mitigates cyber risk and physical security gaps that are prevalent in the OT environment. These security features are extended to include any remote access to Critical infrastructure systems including OT connected assets are being exploited by threat actors. The new reality is that these actors are targeting weaknesses in the OT environment such as open ports, lack of proper OT network segmentation, lack of MFA on points of access and back doors through third party vendors. connected assets.

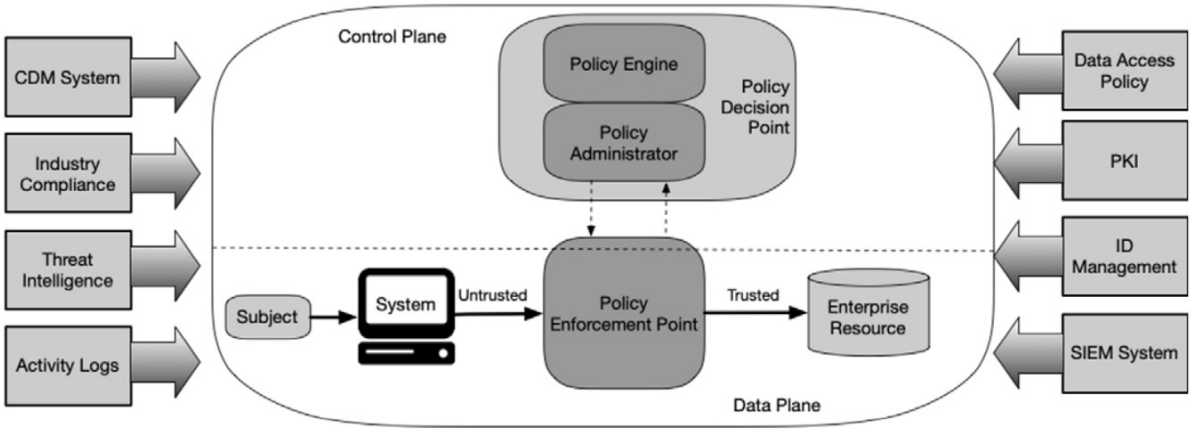

Figure 2. NIST SP 800-207 Zero Trust Architecture - Core Logical Components

While threat actors may penetrate a network with stolen credentials and passwords, a secure operational gateway with built-in hardware token- based MFA and protocol and asset isolation effectively blocks credential theft, directly reducing OT cybersecurity risk. The CSG is particularly effective against ransomware attacks moving laterally from IT networks or attacks against an OT port connected directly to stand alone network.

A recent NSA alert recommends encryption and authentication for all connected assets:

NSA ALERT: STOP MALICIOUS CYBER ACTIVITY AGAINST CONNECTED OPERATIONAL TECHNOLOGY (APRIL 2021)

Without direct action to harden OT networks and control systems against vulnerabilities introduced through IT and business network intrusions, OT system owners and operators will remain at indefensible levels of risk.

ENHANCE THREAT INTELLIGENCE AND FORENSICS

XONA can be integrated with asset management and threat intelligence solutions to provide integrated control and awareness of user access to assets, plus user-to-asset access analytics for enhanced threat intelligence and forensics.

Cyber experts and threat monitoring agencies recommend OT operators create an asset and network map that identifies all known connected OT assets or networks, as recommended in this recent NSA alert:

NSA ALERT: STOP MALICIOUS CYBER ACTIVITY AGAINST CONNECTED OPERATIONAL TECHNOLOGY (APRIL 2021)

Recommends OT owners create a known OT network map and device settings baseline and validate all equipment on the network.

Once an asset inventory or mapping has been established, deploying the XONA CSG on connected assets or OT networks provides the capability to monitor user access to an identified asset. XONA's session logging, monitoring and recording can feed analytics to a variety of applications, including asset management tools, control room, SIEM and threat intelligence solutions.

SUPPORT REMOTE PATCHING

XONA can be used to support remote patching of systems supporting Industrial Control Systems by providing a moderated unidirectional file transfer mechanism for OT assets to allow for operators to meet compliance and security objectives for their patch management and configuration monitoring program.

The XONA CSG can be used to establish the secure connection. Existing session logging capabilities of the CSG provide a complete history of logging activities for verification purposes, proof of compliance (i.e., NERC-CIP, Asset Management, etc.), training and network forensics.

PROVIDE MONITORED USER ACCESS TO CRITICAL ASSETS FOR THIRD PARTIES

XONA can be used to support role or time-based access to critical OT assets for third-party access management. User access control features include defining specific roles such as allowing remote access to defined assets or file transfer capabilities to these assets. In addition, access can be limited to time windows for each asset and require specific MFA through standards-based authentication protocols (i.e., WebAuthn, U2F, or OTP).

USER ACCESS FORENSICS FOR INVESTIGATIONS AND TRAINING

XONA can be used to obtain user forensics and for enhanced training. Forensics for both employees' and third parties' (OEM, outside vendors/contractors, etc.) accesses to OT assets can be enhanced with XONA. Detailed user access logging, recording and reporting enhances internal cybersecurity readiness as well as operational efficiencies (i.e. user-to-HMI operational process recordings).

ABOUT XONA

XONA enables frictionless user access that's purpose-built for operational technology (OT) and other critical infrastructure systems. Technology agnostic and configured in minutes, XONA's proprietary protocol isolation and zero-trust architecture immediately eliminates common attack vectors, while giving authorized users seamless and secure control of operational technology from any location or device. With integrated MFA, user-to-asset access controls, user session analytics, and automatic video recording, XONA is the single, secure portal that connects the cyber-physical world and enables critical operations to happen from anywhere with total confidence and trust.

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