DATA SHEETS

XONA CRITICAL SYSTEM GATEWAY (CSG) PROTOCOL ISOLATION

Protocol isolation, also known as protocol translation, is the practice of confining the use of certain protocols to a specific network location, such as a virtual machine, and isolating it from the rest of the network. As with network segmentation and other types of isolation, such as isolating browsers, protocol isolation helps protect systems against compromises and breaches by keeping all activity local and preventing malware from spreading. It also keeps threat actors from moving through the network.

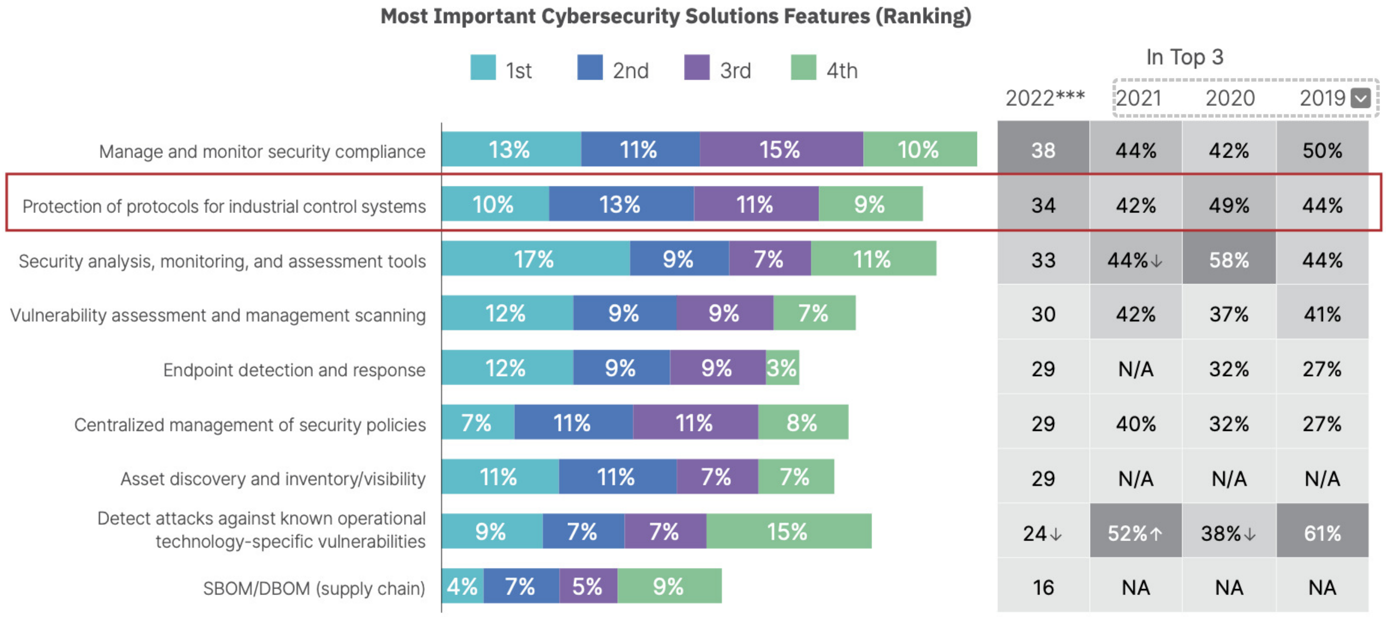
The demand for technology, such as the XONA CSG, that can effectively support secure user access, both remote and onsite, has expanded to include the operational technology (OT) and industrial control systems (ICS) that enable organizations in a variety of critical infrastructure (CI) sectors to function. This need now extends to employees, contractors, and vendors.

However, the priorities of a knowledge worker (i.e., the confidentiality of data) are inherently different than those of an OT operator (i.e., ensuring timely and reliable access to operational technologies, or the industrial control systems used to manage critical infrastructure). The latter needs to ensure system availability, with the potential to bring significant harm to humans and the environment if the systems were controlled by someone with malicious intent.

One way to protect against those with malicious intent is using protocol isolation. It involves confining the use of an explicit network protocol to the specific network location in which it is operating and isolating it from other environments such as the Internet or an IT network. As with network segmentation, protocol isolation helps protect systems against compromises and breaches by keeping all activity local. This keeps those with malicious intent from exploiting weaknesses in one protocol that might enable them to install, execute, and spread malware.

Protocol isolation is particularly important to critical infrastructure organizations, where operational technology (OT) employs a mix of protocols to connect to OT assets that may not be secure. This mix of network protocols can involve connections to products of varying complexity and functionality, complicating the task of securing an environment from cyber-attacks. When it’s not possible for teams to individually secure the full range of assets and protocols in use, isolating them within their specific network is a practical approach.

Fortinet's 2022 State of OT and Cybersecurity Report underscores the value of protecting protocols for ICS, which OT professionals ranked as the 2nd most important feature.


Most Important Cybersecurity Solutions Features (Ranking)

	1st	2nd	3rd	4th	2022***	In Top 3 2021	2020	2019
Manage and monitor security compliance	13%	11%	15%	10%	38	44%	42%	50%
Protection of protocols for industrial control systems	10%	13%	11%	9%	34	42%	49%	44%
Security analysis, monitoring, and assessment tools	17%	9%	7%	11%	33	44%↓	58%	44%
Vulnerability assessment and management scanning	12%	9%	9%	7%	30	42%	37%	41%
Endpoint detection and response	12%	9%	9%	3%	29	N/A	32%	27%
Centralized management of security policies	7%	11%	11%	8%	29	40%	32%	27%
Asset discovery and inventory/visibility	11%	11%	7%	7%	29	N/A	N/A	N/A
Detect attacks against known operational technology-specific vulnerabilities	9%	7%	7%	15%	24↓	52%↑	38%↓	61%
SBOM/DBOM (supply chain)	4%	7%	5%	9%	16	NA	NA	NA

WHY PROTOCOL ISOLATION IS IMPORTANT

Enterprise IT has standardized to a great extent on the TCP/IP. RDP, SSH, VNC, and Web are common protocols in OT.

Organizations that use these protocols may open the door for malicious actors to harvest credentials and move throughout the network. As the Cybersecurity and Infrastructure Security Agency (CISA) points out, whoever controls the routing infrastructure of a network essentially controls the flow of data. An attacker with a presence on an organization's gateway router, or internal routing and switching infrastructure, can monitor, modify, or deny traffic either to and from the organization or within its network. Isolating protocols and functions, along with segmenting the network, limits what threat actors can do once inside the network.

In industrial settings, the ability to isolate protocols such as RDP, SSH, and VNC is critical. Traditionally, these protocols were assumed to be secure because they were used in OT environments with assets that were "air gapped" from the public Internet and IT networks. This made attacking OT environments difficult – if not impossible and made attempts to compromise them less likely than attacks against more "value rich" IT systems. It also made it very unlikely that an attack against an IT network would originate from an OT environment.

However, IT and OT systems are converging, combining the use of both IT and OT protocols. That merging has increased efficiencies, allowing the use of data and analytics to streamline operations, and enabled remote plant operations for geographically dispersed organizations.
But it has also introduced vulnerabilities and made OT systems, many of which were never intended to be connected to untrusted networks, a more attractive target for threat actors.

So, while IT has standardized on TCP/IP, the OT world still uses an array of protocols, many of which can be specific to the functional operations of equipment, a type of industry, or even geographical locations. Integrated IT and OT systems may use the same hardware, but they still operate differently, with significant variations in the software and protocols used.

Too many OT systems are also outdated from a systems standpoint, with them running unsupported and/or unpatched software. These systems may rely on outdated operating systems, such as Windows XP. OT systems that are networked with IT systems can also be vulnerable through open ports that lack proper access and protocol controls.

Each of these factors has increased the importance of protocol isolation, as the air gaps that once existed between OT and IT systems need to be effectively replicated by other means to protect those systems. Protocol isolation is a great way to address this challenge.

HOW ISOLATING PROTOCOLS IMPROVES NETWORK SECURITY

The practice of isolating systems, protocols and other elements of a network is gaining attention as organizations become increasingly cloud-based and geographically dispersed. Treating an OT network like an IT network holds the potential for disaster as the requirements for each are very different. While an IT organization may recover from a data breach by a malicious actor, someone gaining access to a nuclear power plant’s control systems speaks to a far more dire set of consequences.

Network segmentation is one way to prevent malicious actors who may gain illegal access to a network from moving laterally across the overall network to steal data or inflict damage. In this instance, a network is divided into sub-networks, or zones, of systems that share operational functions and risk profiles. Communication between the subnets, consisting of Virtual LANs (VLANs), is prohibited unless specifically granted.

Protocol isolation can prevent malicious actors from lateral movement across a network. In contrast, the VPN technology used by some CI organizations isn't designed to isolate systems or protocols. An attacker who uses stolen credentials to access a network via a VPN has free movement once inside

Along with other security measures such as enforcing the principles of least privilege and securing access to devices within the infrastructure, organizations can use protocol isolation and network segmentation to restrict movement. Some recommended best practices include:

- Logically segregate a network by physical or virtual means, allowing admins to isolate OT assets and their associated protocols within network segments. Virtual LANs (VLANs) are the most common way to segment networks.
- Use protocol-aware firewalls configured to filter traffic and deny the flow of packets within the network.
- Implement a VLAN access control list (ACL), to filter access to/from VLANs, based on protocols, ports, and traffic direction, denying the flow of data across VLANs.

Protocol isolation is a part of a comprehensive, holistic approach to network security.

HOW XONA USES PROTOCOL ISOLATION

As mentioned previously, the demand for technology such as XONA CSG, that can effectively support secure user access, both remote and onsite, has expanded to include the OT and ICS that enable organizations in a variety of critical infrastructure (CI) sectors to function.

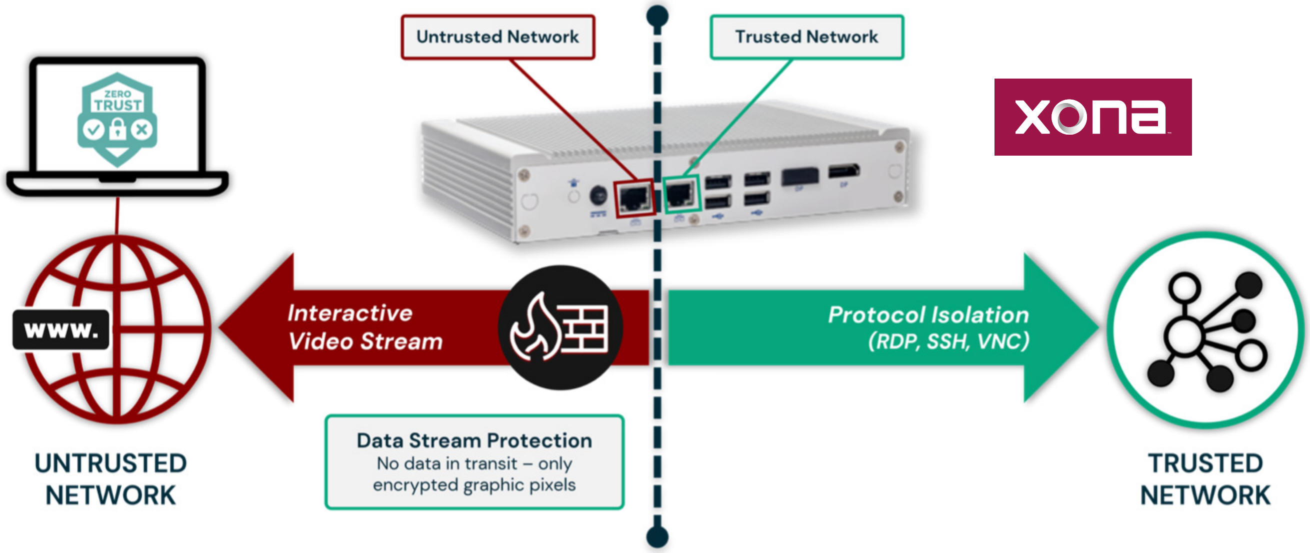
Yet, the priorities of a knowledge worker are inherently different than those of an OT operator. The latter needs to ensure system availability, with the potential to bring significant harm to humans and the environment if the systems were controlled by someone with malicious intent.

As such, the ability to isolate protocols such as RDP, SSH, and VNC is critical to helping keep OT environments secure. Protocol isolation enables employees, contractors, and vendors using a XONA CSG to access OT/CI assets securely, without the possibility of attacking those assets or exposing them to untrusted external networks.

Protocol isolation is one example of how a XONA CSG protects the assets and data streams from a trusted network from the external world. It only allows the live data stream carried by the protocol to transit as far as the trusted side of the XONA CSG. At that point the data stream is converted into encrypted graphics and delivered via interactive video stream to the end- user device. These graphics are rendered like a movie in which the end user can engage.

HOW XONA USES PROTOCOL ISOLATION

Below is a visual depicting XONA's approach to protocol isolation in our CSG gateway.



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. Learn more by visiting www.xonasystems.com