WHITE PAPER

Why an OT-centered Cybersecurity Platform Is Critical for Industrial Applications

Roger Chen
Manager of Cybersecurity Market Development

MOXA®

Changing Needs in OT Cybersecurity

When Stuxnet, a computer worm targeting SCADA and PLC systems, paralyzed a nuclear program in the Middle East in 2010, the incident served as a wake-up call that the OT (operational technology) industry was not immune to malware and other IT security risks. In fact, the stakes are even higher when critical infrastructure is involved, elevating the risk to national security level. For this reason, today's OT network security and operational security must stay ahead of the game to protect critical infrastructure from new and constantly evolving threats.

Not only did the number of malware attacks and other security incidents increase in recent years, the nature of cyberthreats also evolved with the changing and increasingly challenging ICS (industrial control system) environment. From the targeted ICS attacks of the past to random extortion executed by worms, it becomes increasingly difficult to identify the motive of attacks and formulate appropriate defense strategies.

Released on November 4, 2022

Moxa is a leading provider of edge connectivity, industrial computing, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things. With 35 years of industry experience, Moxa has connected more than 82 million devices worldwide and has a distribution and service network that reaches customers in more than 80 countries. Moxa delivers lasting business value by empowering industry with reliable networks and sincere service for industrial communications infrastructures. Information about Moxa's solutions is available at www.moxa.com.

How to contact Moxa

Tel: 1-714-528-6777
Fax: 1-714-528-6778

MOXA

Towards a cybersecurity platform for OT

As cybersecurity threats remain ever-present, IT cybersecurity professionals are hard-pressed to find the ideal solution for the unique demands of the OT field.

To start, we need to remind ourselves that the OT field, which often covers production lines and critical infrastructure, employs stringent requirements. In many scenarios, the primary goal of OT is to support operational processes and ensure they run under optimal conditions. While the "zones and conduits" model may have served us well in the past, it is no longer adequate to meet the latest security standards. When it comes to malware or advanced attacks, real-time security updates are required to detect and respond to threats as quickly as possible to protect line operations and minimize potential downtime. Traditional firewalls constantly monitor network packets based on firewall rules to identify malicious activity all the while making sure no valid packets are being dropped. However, this may cause latency on the network and affect performance. A robust cybersecurity solution should maintain system performance, rather than undermine it with overhead, in order to swiftly identify and prevent advanced attacks as they happen in real time.

Only a tailor-made cybersecurity platform can truly protect industrial applications

A cybersecurity platform requires a high level of customization to be able to truly protect critical OT systems such as SCADA systems. A tailor-made platform takes into account industrial protocols, application payloads, and network commands and data. This is particularly true in vertical market applications such as energy and transportation. By correctly interpreting legitimate network commands and stopping malicious ones, a cybersecurity platform prevents hackers from infiltrating and tampering with devices on the network.

In the future, as Industry 4.0 improves field manufacturing efficiency, network requirements as well as cybersecurity vulnerabilities will change. **An OT tailor-made cybersecurity platform** offers the flexibility to include more protection mechanisms that can be deployed at different control points, so OT systems can quickly adapt to changing security threats and improve the overall level of protection.

Centralized network management reduces human error and greatly improves operational efficiency and security

To adapt to changing threats, OT asset owners need to make sure network security policies are up to date. Firewall rules are an essential part of these policies. However, as the network grows in scale and complexity and firewall rules expand, maintaining and managing the network efficiently becomes a challenge. Without proper management tools, the network is more prone to human errors such as misconfigurations which can expose network vulnerabilities or even lead to breaches.

A centralized security management platform plays an important role in avoiding human error. As security is centrally managed, deployment complexity is greatly reduced as a result. Moreover, it provides flexibility in authority delegation. Different management privileges can be assigned to specific zones or roles, further reducing possible human errors. A centralized security management platform also records, aggregates, and visualizes data on network traffic and security events. This provides OT managers with valuable analytical insights to monitor and manage the security network more efficiently.

On-site maintenance personnel with a tight schedule day-in day-out are bound to make firewall configuration errors from time to time. A defense-in-depth cybersecurity strategy helps on-site operators work more efficiently and helps prevent errors when configuring settings. Having a user-friendly OT-centric security platform with central control network management reduces deployment time and enhances network protection.

How an IPS cybersecurity platform can enhance OT network defense

Virtual patching for legacy equipment vulnerabilities

OT professionals all agree that applying security patches is important. However, many older software and devices do not support new patches and quickly become cybersecurity liabilities in OT applications. Indeed, updating devices in the industrial field is not easy. For this reason, patching is often delayed and only scheduled when it becomes critical for ensuring uninterrupted operations. When "Patch Tuesday" comes around, operational disruptions can lead to cybersecurity weaknesses as they expose many devices to risk. Industrial intrusion prevention systems (IPS) leverage virtual patching to act as a shield for key equipment in industrial networks that is unavailable for patching, or simply cannot be patched. Virtual patching works by updating the IPS protecting the vulnerable asset using the latest security signatures, instead of patching the asset itself. IPS are capable of monitoring the network environment, protecting the equipment, and delivering patches in a timely manner without interrupting operations. They offer a solution that meets the special needs of industrial networks.

Leveling up security with IPS visualization, monitoring, and protection

IPS can proactively detect suspicious activity and known attack patterns on the network. The IPS engine continuously analyzes network traffic and compares bit stream and internal traffic patterns to identify potential attacks. Once a malicious activity is detected, the IPS will discard the packet and block the traffic from the attacker's IP address, while still allowing legitimate traffic to pass through.

In addition, IPS also have other advanced monitoring and detection features, such as

- HTTP string and substring matching
- Generic pattern matching
- TCP connection analysis
- Packet anomaly detection
- Traffic anomaly detection

To achieve around-the-clock network protection, IPS receive the signatures sent from the intelligence database to continuously monitor or block threats. IPS also have a set of safety management systems that learn and recognize traffic patterns, alert safety personnel, and generate safety reports.

IPS achieve better defense-in-depth

Before cyberattacks can even reach other security devices, IPS offer comprehensive protection to prevent DDoS (Distributed Denial-of-Service) attacks from reaching the firewall and crashing the system. By providing a holistic, in-depth network defense perimeter, IPS can filter out malicious attacks so network devices can continue to operate normally.

Deploying, managing, and maintaining IPS for the best performance

The IPS should be deployed prior to essential equipment going online. The IPS acts as a shield to protect capital investment, reduces the likelihood of equipment malfunctions that may put worker safety at risk, and ensures normal production line operations. For the best performance, the IPS should be tweaked to prioritize the following areas:

1. The protection of essential equipment
2. Instant warnings when a threat is detected
3. Performance optimization to achieve maximum operational efficiency

Moreover, IPS settings should be in line with the company’s security policies and meet compliance and operational requirements.

Next-generation security and centralized management software

Integrate IPS functions to enhance protection

While network partitioning and network security control provide customers with better control of their devices, a dedicated array of features such as virtual patching, network visibility, real-time protection, and network packet monitoring, help combat external threats and keep the network secure. These features and technologies are specifically built with the needs of OT in mind. Several industrial-grade IPS available on the market today are already outfitted with such robust and comprehensive cybersecurity features.

Cybersecurity platforms tailor-made for OT

For the best possible result, it’s important to choose cybersecurity platforms that are designed for OT applications. When evaluating solutions, keep in mind what kind of industrial environment it will be used in, and check if it meets the necessary performance, efficiency, stability, and security requirements.

Consider the following OT needs when reviewing candidate solutions:

- Advanced functionality such as DPI (deep packet inspection)
- Support for industrial protocols (Modbus TCP/UDP, DNP3, IEC 60870-5-104)
- High-bandwidth connectivity for performance-heavy applications
- Industrial certifications for use in specific OT environments
- Security functions based on industry-recognized standards such as IEC 62443-4-2

Centralized network management platform

To effectively manage all the security policies and permissions governing access to network devices, the IPS should be paired with centralized network management software. User-friendly network security management software streamlines deployment and enables centralized management of cybersecurity assets, allowing users to easily configure firewall and IPS rules correctly. This helps reduce human error, simplifies firewall management, and provides essential network security information for decision makers.

Moxa Solutions

Moxa’s industrial-grade EDR-G9010 Series all-in-one firewall/NAT/VPN/switch/router offers a comprehensive cybersecurity package featuring IPS, enhanced security functions, and high-speed connectivity.

The MXsecurity management software further simplifies cybersecurity deployments by providing centralized control over EDR-G9010 Series devices and streamlines network security management.

For more information, visit the EDR-G9010 Series and MXsecurity Series product pages.

Disclaimer
This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied by law, including implied warranties and conditions of merchantability, or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document.