



Securing Distributed Infrastructure at Scale

Kyle Shepard, Chief Engineer, SNC

UNDERSTANDING THE PROBLEM

Legacy Systems and greater IT connectivity are contributing to the rise in cyber-attacks, leaving Operational Technology (OT) vulnerable and susceptible to exploitation. These systems have been built with technologies that do not implement modern security protocols and are designed to run in small standalone enclaves. However, recent attacks have emphasized the interconnected nature of these systems, the ease of exploit, and the impacts of failing to secure these systems:

- Oldsmar, Florida (February 2021): A rogue actor was able to log into a municipality water treatment facility through remote desktop and attempted to poison water supply.
- Colonial Pipeline (May 2021): A ransomware attack on the corporate IT systems led the company to shut off the pipeline out of fear of the reach of the ransomware.
- Chinese Cyber Espionage Activities (2023-2024): Between 2023 and 2024, Chinese state-sponsored hacking groups, notably Volt Typhoon and Salt Typhoon, conducted extensive cyber espionage campaigns targeting U.S. critical infrastructure, including telecommunications and energy sectors. These sophisticated attacks aimed to gather intelligence and potentially disrupt essential services.
- Iranian and Pro-Russian Cyber Activities (Late 2023 – Early 2024): In late 2023 and early 2024, cyber actors affiliated with Iran and pro-Russian groups gained access to and, in some cases, manipulated U.S. industrial control systems in sectors such as food and agriculture, healthcare, and water and wastewater. These breaches highlighted vulnerabilities in critical U.S. systems and the potential public safety threats posed by such intrusions.

HOW THE PROBLEM IS HANDLED TODAY

Securing critical infrastructure presents numerous operational and technical challenges. Upgrading OT systems for security is often considered too costly and potentially disruptive to operations. Consequently, the industry has largely adopted a defense-in-depth strategy, incorporating IT concepts such as boundary firewalls¹ and network sensors². These feed into a centralized monitoring and alerting system managed by a security operations center (SOC).

While this approach significantly enhances visibility, it still has notable gaps. For example, it relies heavily on dependable remote connectivity; if a site is disconnected from the data aggregation system, it loses its defense mechanisms, making this solution impractical for sites with limited or no connectivity or those considered too critical to risk connecting to a larger network.

Additionally, these solutions have limitations in response strategies. Continuous monitoring can reduce response time but assumes that the monitoring system will detect threats and that the team can respond before significant damage occurs. In practice, the effectiveness of monitoring solutions depends on the expertise of the personnel interpreting the data and the ability of corporate functions to promptly deploy incident responders to contain and mitigate threats.

¹ A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules, acting as a barrier between a trusted internal network and untrusted external networks. Its primary function is to prevent unauthorized access and protect the network from cyber threats.

² A sensor in a network is a device or software component that detects and monitors network traffic or specific events, providing data to enhance visibility and support security measures.

SNC'S APPROACH AND ADVANTAGES

SNC's Binary Armor® is an endpoint security device designed to protect OT networks from insider threats, human error, and to enforce workflow by allowing only pre-approved, safe messages to reach operational technology.

Available as both a hardware device (Figure 1) and a software application, Binary Armor functions as a network sensor and policy enforcement tool within OT systems. It can be deployed for east/west endpoint protection and north/south boundary protection between network enclaves, as depicted in Figure 2.



Figure 1: Binary Armor® Hardware

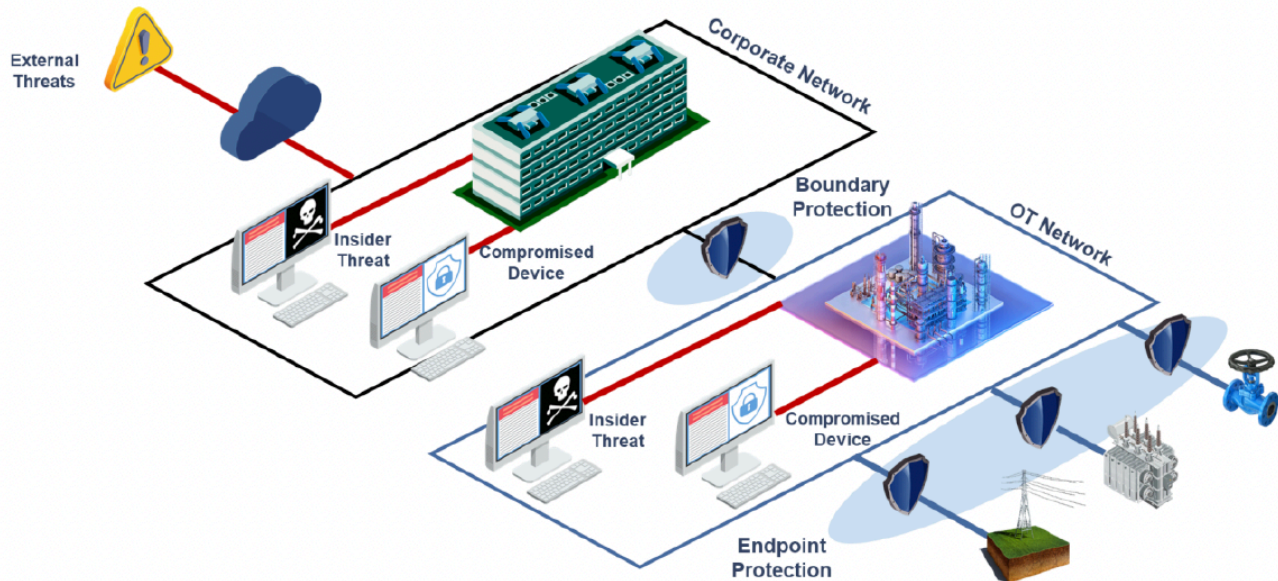


Figure 2: A Notional Deployment of Binary Armor®

Binary Armor is highly configurable to align with an organization's specific priorities and risk profile, allowing it to be initially installed in a more permissive state and gradually tightened as familiarity with the tool increases. Key features of Binary Armor include access control, continuous monitoring, operation and workflow enforcement, and analytic enforcement.

ACCESS CONTROL

Binary Armor fundamentally provides essential access control functions to protect the devices it secures. This includes standard firewall protections and deep packet inspection³ of known protocols to prevent fuzzing attacks via regular interfaces. Additionally, Binary Armor offers two key access control functions to mitigate high-criticality vulnerabilities through advanced deep packet inspection techniques:

- **Port Locking:** Binary Armor can restrict access to specific ports, such as administrative webpages, requiring users to log in with a multifactor token to open a maintenance window for resource access.
- **Read-Only Enforcement:** Binary Armor can enforce "read-only" modes on known protocols, enabling remote status monitoring of critical systems while preventing any unauthorized operations.

CONTINUOUS MONITORING AND REDLINE ALERTS

Since Binary Armor is deployed at critical enforcement points within the network, it can analyze all network traffic at those locations and report the data to common log management and analysis tools⁴ such as Elastic and Splunk. Utilizing open standards and protocols for reporting, Binary Armor ensures maximum compatibility with an organization's existing tools for centralized data collection and monitoring.

³ Deep packet inspection (DPI) is a network analysis technique that examines the content of data packets beyond the header information to identify, classify, and manage traffic based on the payload and application data.

⁴ Log management and analysis tools are software solutions designed to collect, store, index, search, and analyze log data generated by various systems and applications. These tools help organizations monitor system performance, troubleshoot issues, gain operational insights, and perform root cause analysis by providing real-time data analysis and visualization capabilities. Examples include Splunk, Elastic (Elasticsearch), and Graylog.

ENDPOINT SAFE OPERATION AND WORKFLOW ENFORCEMENT

Beyond the basic access control features mentioned earlier, Binary Armor can enforce more granular policies directly on a device. While such features are typically integrated into an organization's human-machine interface (HMI)⁵, Binary Armor performs this enforcement at the device level to mitigate risks arising from HMI misconfigurations, operator errors, and malicious attackers bypassing HMI controls. Examples of these policies include:

- Enforcing boundary conditions when controlling equipment
- Restricting the rate at which settings can be changed (i.e., the Aurora Attack⁶)
- Requiring a specific sequence of commands to be followed for a particular workflow to be executed

ENDPOINT ANALYTIC MONITORING AND ENFORCEMENT

One of Binary Armor's most sophisticated features is its ability to monitor critical datapoints directly at the endpoint. This enables organizations to detect anomalous behavior even on disconnected systems and ensures that anomaly-based detection continues to function in intermittent environments where reporting all metrics from the OT system back to a central location is impractical. Additionally, this capability can help reduce costs associated with connecting devices over metered connections.

⁵ A Human Machine Interface (HMI) is a user interface or dashboard that connects an operator to a machine, system, or device. It allows for interaction through graphical displays, touchscreens, buttons, and other input methods, enabling the user to monitor, control, and manage processes and equipment in industrial and other technical environments.

⁶ The Aurora attack refers to a cyberattack that targeted a power grid system, demonstrating the potential for hackers to cause physical damage to infrastructure. In 2007, the U.S. Department of Homeland Security conducted a test, known as the Aurora Generator Test, which simulated an attack on a power generator. By rapidly opening and closing circuit breakers out of phase with the grid, the attack induced mechanical stress, ultimately leading to the generator's destruction. This highlighted vulnerabilities in critical infrastructure and the need for robust cybersecurity measures.

IMPACT

Incorporating Binary Armor into a security stack enhances current best practices with several key capabilities, resulting in a more robust cybersecurity solution and potential cost savings depending on the architecture. The benefits include:

- **Scalable Cybersecurity:** Binary Armor addresses basic firewall needs and can enhance protection as an organization's security policies evolve.
- **Machine-Speed Incident Response:** Organizations can enforce policies on their OT, ensuring safe operation of equipment and adherence to business processes.
- **Protection at the Equipment Level:** Binary Armor offers protection for OT systems that cannot reliably connect to a centralized monitoring solution.
- **Reduced Costs:** By enriching and minimizing the data sent to a centralized monitoring point over metered network connections, Binary Armor helps reduce associated costs.
- **Validation:** Bolstered by Common Criteria and DISA certifications along with comprehensive penetration testing, Binary Armor provides a robust solution to significantly enhance your organization's security posture.

CONNECT WITH US

✉ hello@binaryarmor.com

🌐 binaryarmor.com