Binary Armor® Secure Environment
Security and Flexibility at the Edge

Protects Against Cyberattacks

Bridges IT/OT Networks

Detects and Blocks Insider Threats

Innovation Starts at the Edge!

Industrial IoT (IIoT) sensor and device deployments are forecast to increase far into the future because of the measurable operational benefits IIoT devices provide. One drawback with IIoT device proliferation is growing demand for network bandwidth and computing resources. As a result, computing traditionally done in data centers is migrating to the network edge, providing minimal latency and reduced network traffic.

Edge computing platforms need to be uniquely flexible to quickly adapt and integrate numerous, disparate IIoT sensors and applications. What is more, they need to have rock-solid cybersecurity features to protect the core network from insecure IIoT devices, and to likewise protect edge devices from IT-originated exploits. In addition, they need to be small, economical, and rugged. Simply put, edge computing devices have unique requirements that can only be met with innovative new designs.

Binary Armor with Secure Environment (SE) is precisely the rugged, secure, flexible computing platform needed at the edge of Industrial Control networks. Binary Armor's cybersecurity pedigree is widely recognized. Now, Binary Armor has an SE that provides 'sandboxes' for network owners, OEMs, system integrators, and value-added resellers to install IIoT and edge applications on a small form-factor, high-power edge computing device. Binary Armor SE helps industrial control network owners simplify integration and field new IIoT capabilities with a robust, secure, flexible solution at the edge.

sales@binaryarmor.com | binaryarmor.com

Best Security and Performance Practices:

Binary Armor SE utilizes Docker's Open Container Initiative (OCI) compliant containers to create virtualized run-time environments. This virtualized environment provides isolation from the underlying operating system. Some of the benefits of using Docker as the framework for Binary Armor Secure Environment include:

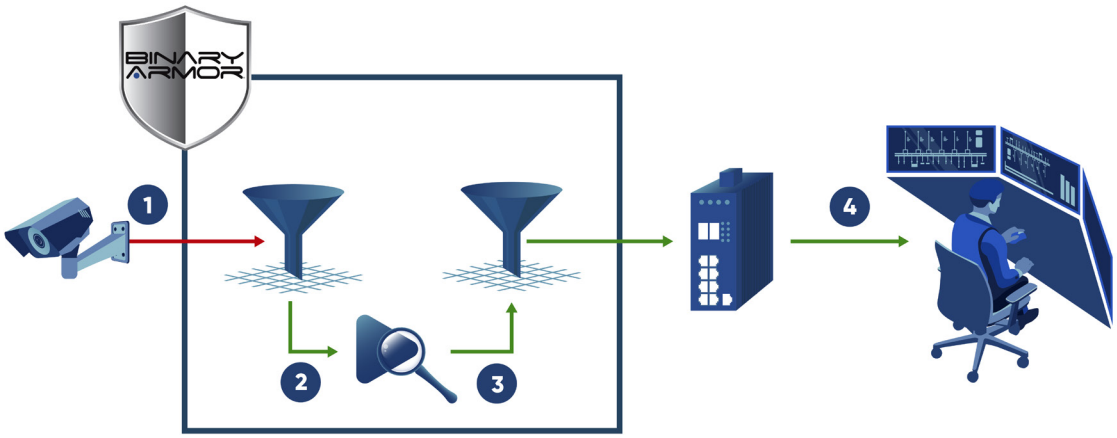
- Less memory used for each container
- Persistent storage and volume sizes
- Faster processing performance with lower CPU usage
- Ability to push environmental variables to containers
- Ability to execute runtime commands
- Ability to turn up multiple containers

Binary Armor Secure Environment creates a secure gateway platform that validates all data to and from containerized applications using Binary Armor's patented ruleset engine. This validation engine ensures containerized applications cannot be maliciously compromised and simultaneously protects edge devices from exploits. Applications that either have been or could be hosted in Binary Armor Secure Environment include:

- Real-time video analytics
- Edge network monitoring and data logging
- Protocol conversion for edge equipment inter-operability
- Local data reduction and compression to reduce use of metered wireless backhaul links
- Local equipment performance monitoring and real-time control
- Network performance visualization for maintainer use
- Remote automation / distributed automation – localized edge control to enable efficiencies and de-centralized control
- Data visualization and fusion

Edge Video Processing and Analytics Case Study

Video cameras are almost everywhere and, if deployment trends continue, will be everywhere indeed. Those cameras generate vast amounts of streaming data that threaten to consume most available network bandwidth. Technology solutions exist to perform video analytics at the edge to reduce network load. Some video analytics monitor, recognize, and generate email / text / SMS alerts only if triggered by some pre-defined event. Binary Armor SE hosts and protects edge video analytics applications from rogue internet connections that could seek to terminate video analysis prior to some dangerous event.

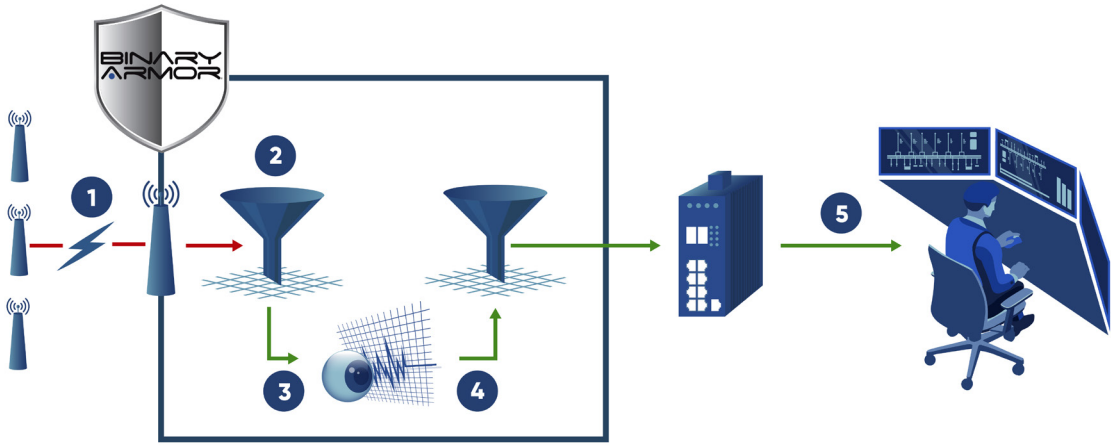


1. Camera delivers streaming video to Binary Armor
2. Binary Armor ruleset validates meta-data before passing data to Video Analyzer application
3. Video Analyzer generates automated alert based on predefined trigger criteria
4. Binary Armor ruleset validates and releases alert to security operations center

Figure 1 - Binary Armor Secure Environment Hosting Edge Video Analyzer Application

Edge Network Monitoring Case Study

Thousands of widely dispersed, data rich, security vulnerable IIoT sensors must be monitored for anomalous behavior in real time. Network security monitors can be hosted in Binary Armor SE for edge analytics and decision making. Alerts can be generated to a central site only if malicious behavior is detected, thus preserving precious bandwidth for other mission-critical functions. Security rulesets provided by Binary Armor ensure that the monitor application itself is protected.

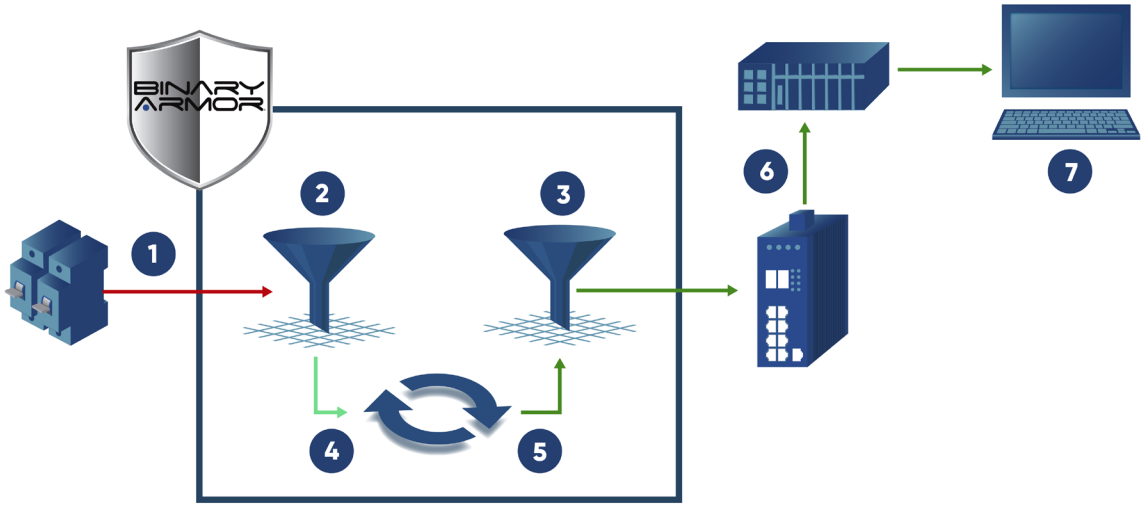


1. Unregistered edge wireless sensor delivers status report to LTE modem
2. Modem passes sensor data to Binary Armor for validation
3. Binary Armor ruleset blocks data from invalid source and generates alert to Network Monitor
4. Network Monitor delivers alert to security operations center
5. Network Monitor AI system correlates edge alert information with amplifying information and generates guidance to remediate the threat

Figure 2 - Layered Cybersecurity at the Edge

Protocol Conversion Case Study

IIoT technologies frequently have to interact within Industrial Control System (ICS) networks. For example, edge sensors may deliver status reports in a standard industrial protocol, but may need to be converted to a proprietary OEM protocol with the conversion function located on a centralized SCADA system server. Thousands of edge sensor reports place demand on computing functions that could delay other important SCADA control functions. Binary Armor SE can host protocol converters to securely perform protocol conversion at the edge. Doing so frees server compute cycles to perform primary SCADA control functions.



1. SCADA device provides status report to Binary Armor
2. Binary Armor evaluates status message for compliance with ruleset
3. Binary Armor passes valid status message to SCADA server via switch
4. Binary Armor logs message validity and sends to internal protocol converter
5. Binary Armor converts status message to a SCADA system-compliant format
6. Binary Armor delivers status message to SCADA server via switch
7. Binary Armor status report displayed on SCADA HMI

Figure 3 - Status Message Delivery Directly to SCADA System

Monetize the Edge - Securely

Binary Armor with SE is an enabler for quick, secure deployment of new edge capabilities. The new Secure Environment also enables new business models for Innovative Value Added Resellers (VAR) and System Integrators (SI) who solve unique customer problems by hosting third party applications to deliver meaningful proprietary solutions. Binary Armor with Secure Environment – the solution that fosters innovation at the edge!