Binary Armor® Virtual Guard Info Sheet

Binary Armor virtual guard solution is a device-independent software implementation of Binary Armor

Protects Against Cyberattacks

Bridges IT/OT Networks

Detects and Blocks Insider Threats

Security within OT Equipment is Paramount to Protecting Critical Infrastructure

Binary Armor virtual guard is ideal for OEMs that desire best-of-breed cybersecurity capabilities hosted within their own control systems or network devices. Binary Armor virtual guard delivers the same trusted and proven technology that powers the SCADA network guard in a virtualized environment, enabling extreme flexibility and protection for a broad range of devices.

Binary Armor's virtual functionality is customized to meet your requirements. The software and cybersecurity experts behind Binary Armor will work with your team to optimize a solution for your product line.

Three Reasons to use Binary Armor Virtual in your Products

1. Binary Armor is a proven solution that has been extensively certified and validated:
   - DISA Approved CyberSecurity Tool (TN 1804001)
   - NIAP Common Criteria Approved (CCEVS-VR-VID10879-2018)
   - FIPS 140-2 Encryption (Red Hat OpenSSL)
   - Independently validated by the Electric Power Research Institute (EPRI) (Report #3002014248)
   - Independently validated by DoE cybersecurity labs
2. Binary Armor's patented technology is the only solution that can protect against all threats
   - Protection against insider and advanced persistent threats
   - Processes and validates entire contents of all messages to and from control systems
   - Customizable to enforce workflow and operational processes, preventing critical system downtime
3. Integrating Binary Armor enables accelerated go-to market in a cost effective manner

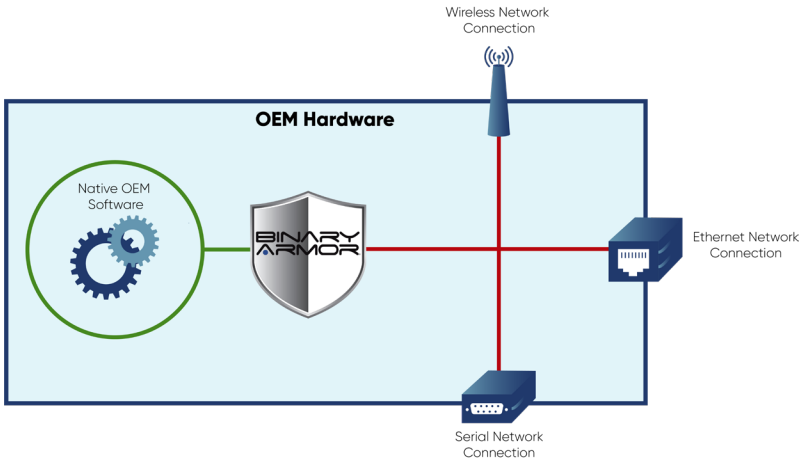
sales@binaryarmor.com | binaryarmor.com

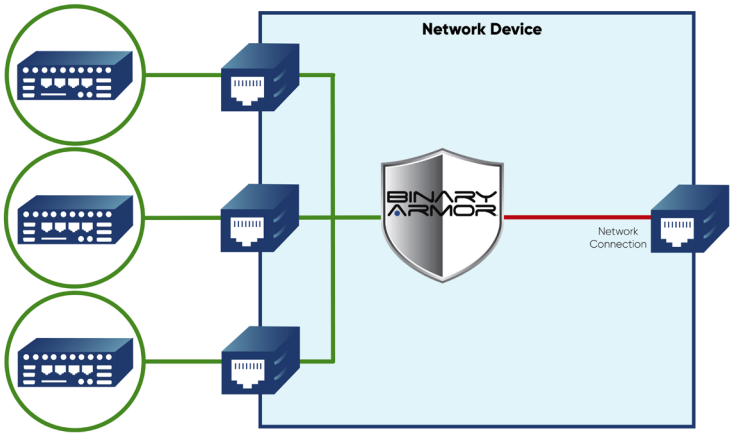
Binary Armor Virtual Provides a Variety of Options to Meet your Needs

Customized virtual integrations enable Binary Armor cybersecurity functions on even the most resource-constrained OT devices.

Customized integrations are optimal to provide best-of-breed cybersecurity to existing OT equipment, such as:

- **Programmable Logic Controllers (PLCs)**
- **Remote Terminal Units (RTUs)**
- **Smart Meters**



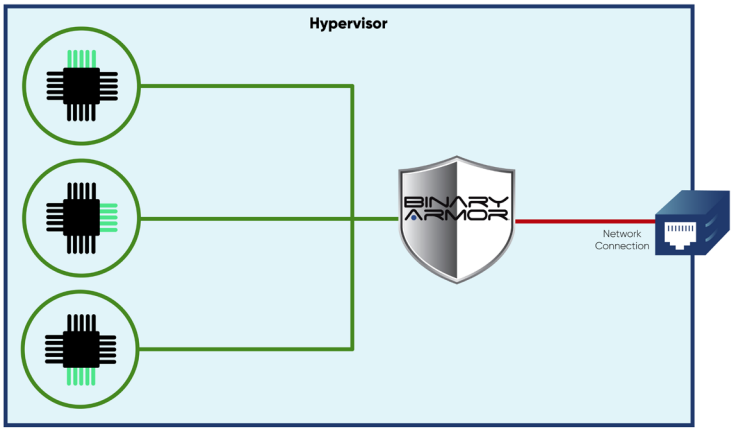


Virtual Network Appliance Installations insert Binary Armor cybersecurity into cutting edge OEM network equipment, including network switches, firewalls, and access points.

Binary Armor virtual network appliances are optimal for smart-grids and new deployments utilizing software defined networking.

Enterprise Virtual Deployments enable Binary Armor to protect assets residing in OEM core virtual environments.

Enterprise virtual capabilities provide a wide range of functionality to support dev ops, including continuous integration and test, independent penetration testing, and vetting deployments in lab environments.



sales@binaryarmor.com | binaryarmor.com