Binary Armor®

Modes: Strong Protection, Flexible Response

Protects Against Cyberattacks

Bridges IT/OT Networks

Detects and Blocks Insider Threats

Introduction

Binary Armor has strong, patented, certified whitelist-based protection mechanisms that have been tested and validated by numerous government agencies. A less well-known, but equally important feature is the flexibility of Binary Armor, with several different operational methods to account for both common and infrequent network events.

The flexibility of Binary Armor starts with security. The device's configuration can be modified in the field, but only by those possessing the correct credentials. The two-factor authentication strikes a balance between security and flexibility to ensure the most important feature of an Industrial Control System: availability.

Binary Armor Modes

- **Nominal Mode:** Binary Armor will operate in Nominal Mode most of the time, employing its rule set configurations to examine every message on a byte-by-byte basis before either delivering or blocking them. Rule-sets continuously enforce security policies when Binary Armor is in Nominal Mode.

- **Configuration Mode:** Occasionally, because of network settings or equipment change, Binary Armor may have to update its rule-sets accordingly. Trained network operators or administrators can update the Binary Armor rule-sets within minutes using the operator interface. Once rule-sets are modified, they are encrypted, signed, and then activated when Binary Armor returns to Nominal Mode.

- **Learning Mode:** There are some use-cases where Binary Armor will be deployed as a passive sensor. In those cases, Binary Armor will often be placed on a switch's mirror port operating in Learning Mode. In Learning Mode, Binary Armor logs and reports the content of every message – but does not block any message traffic. Log reports can be delivered to a central monitoring location for real-time situational awareness. Several Binary Armor systems operating in Learning Mode can be deployed at select points in a network's lower levels for granular insight into data flow and operations.

- **Override Mode:** Override Mode is a privileged state that temporarily modifies the nominal security posture after an authorized user provides the elevated credentials. In override mode, the rules governing traffic through Binary Armor can be modified to significantly increase or decrease or simply modify authorized traffic as the situation demands. Two situations that may require entering Override Mode:

    - One of Binary Armor's primary functions is to protect deployed Intelligent Electronic Devices (IEDs). Occasionally, however, IEDs require software or firmware updates delivered from a remote location. Remote access, often via web GUI, can present a potential attack vector. Binary Armor can be configured to block web or remote access to prevent unauthorized (re)configuration of IEDs. Only authorized users using two-factor authentication would be able to place Binary Armor temporarily into Override mode and allow local or remote configuration updates. Binary Armor returns to Nominal State upon successful competition of updates.

sales@binaryarmor.com | binaryarmor.com

- Override Mode Continued
    - Emergency commands to operational technology could be initiated by malware during otherwise normal operations with the intent of interrupting revenue producing processes, or worse. In Nominal Operations, Binary Armor would block potentially damaging or dangerous commands. However, those same commands, issued by an operator under emergency conditions, may be necessary to prevent damage to equipment or loss of life. In that case, Binary Armor can quickly enter Override Mode to allow authorized emergency commands.

- **Lockdown Mode:** Binary Armor can be placed into a read-only Lockdown Mode based on an elevated security threat that can be triggered from a detected network intrusion, a physical security breach, or other serious situation. In the most extreme cases, Lockdown Mode could be commanded to block all traffic with the net effect of Binary Armor behaving like an air gap for complete enclave separation.

Availability and Reliability

The two primary characteristics expected of Industrial Control Systems (ICS) are availability and reliability. Binary Armor is designed and optimized to protect operational technology from malware and dangerous operator actions so that ICS remains available under adverse conditions.

The Binary Armor adaptive operating modes enable the device's protection policy to be modified in real-time so that the network itself remains available and/or protected in all situations