Binary Armor®
SCADA Network Guard Info Sheet

Protects Against Cyberattacks

Bridges IT/OT Networks

Detects and Blocks Insider Threats

Critical Infrastructure is Vulnerable

Our nation depends on safe, reliable, and secure Operational Technology (OT) for our critical infrastructure. These systems communicate realtime messages that control critical physical assets that underpin our energy infrastructure, transportation, and national defense, and represent the foundation of our economy.

While integration of OT assets with information technology (IT) systems has provided useful visibility of OT systems, it has also created significant security risks and led to a predictable culture clash between IT and OT.

IT Security ≠ OT Security

Many lawmakers, regulators, and decision makers have encouraged using IT frameworks and solutions on OT assets. However, while OT includes technical systems, they are fundamentally different than IT systems. Traditional IT security practice is threat detection and response, which is too costly for OT, and most importantly detection is too late.

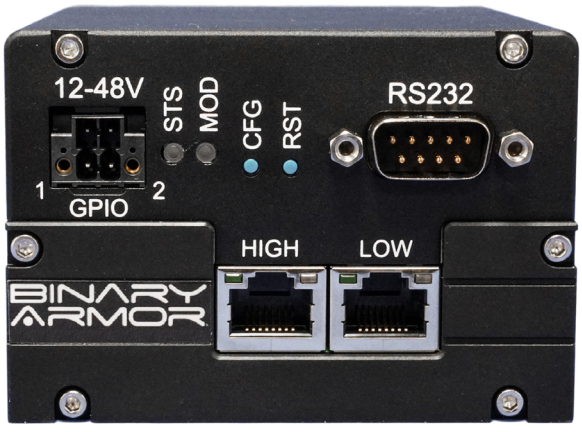
OT isn't an email server or a cloud-based data set, rather these systems control physical systems that, if compromised, could lead to severe economic loss, significant loss of life, and compromised national security. An OT focused security process should first and foremost PROTECT assets.

Decision Makers Need Data

The temptation to apply IT frameworks is exacerbated by the desire for greater visibility into OT operations. To achieve this, there have been increased efforts to integrate these assets into IT systems, causing a clash between IT and OT practitioners.

Historically, keeping IT and OT systems completely separated (i.e. "air gapped") has been the favored form of protection based on the assumption that hackers cannot access systems that are not connected.

If not handled properly, OT-IT integration will greatly increase risk for our US power grid, telecommunications, transportation, and national defense infrastructure.



sales@binaryarmor.com | binaryarmor.com

The OT Security Solution

Above all else, an OT focused security solution should protect operations from human negligence or sabotage, prevent (not just detect) cyber attacks, and securely support integration of data where required.

- **Workflow Enforcement:** By allowing only pre-approved, known safe messages to reach operational technology, Binary Armor protects against insider threats, human error and enforces workflow to reduce the likelihood of equipment damage & personnel injury
- **Cyber Threat Protection:** Protects machine to machine communication from cyber threats to prevent disruption and damage to critical assets
- **Secure Data Management:** Provides a secure method to bridge IT and OT networks

Designed and Built for Protecting OT

An OT focused security solution should first and foremost protect OT operations from human negligence or sabotage, prevent (not just detect) cyber attacks, and securely support data integration where required. Binary Armor provides this protection with the following technical solutions:

Operational Control

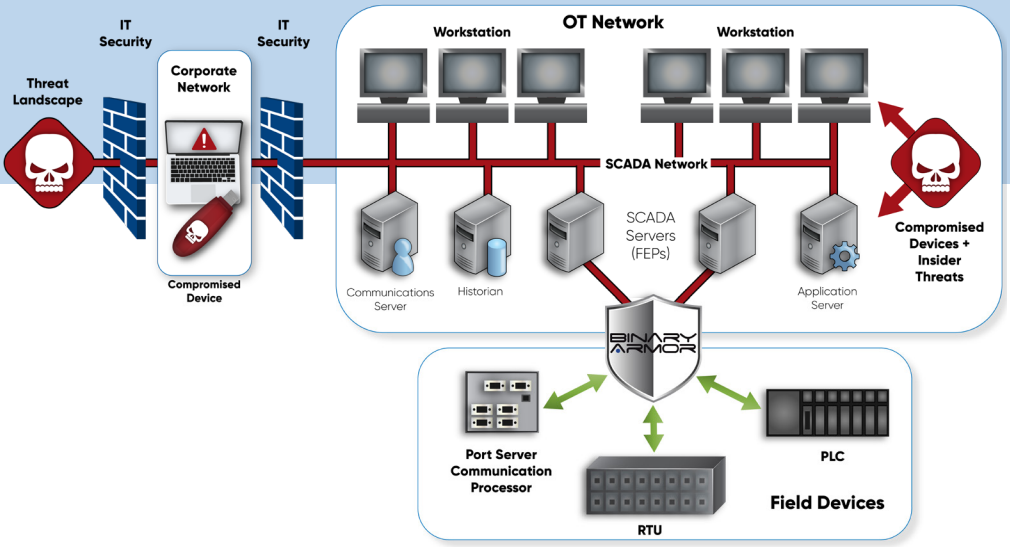
- Secure 2-factor hardware authentication
- Safe and secure emergency management/override
- Patented byte-by-byte message processing

Command Assurance

- Secure system integrity and configuration verification
- Support standard and custom OT protocols
- Patented state-based rules to match OT logic, i.e. "functional whitelisting"

IT/OT Bridge

- Secure link between IT and OT networks
- Centralized management and network syslog
- Patented bi-directional security across all communication layers



Binary Armor Pedigree

Continuously fielded since 2014 protecting utility SCADA and distributed automation systems
Tested by the EPRI Cyber Security Lab for protecting power delivery systems: EPRI report #3002014248
DoD Accreditations: DISA, NIAP and FIPS 140-2

sales@binaryarmor.com | binaryarmor.com