Endpoint Security for ICS and Mission Critical Systems

MOSAICS
2020
INDUSTRY
DAY

Overview

1. Protecting critical infrastructure and mission systems requires a layered, defense-in-depth approach including diverse technology

2. OT-focused endpoint security is a key component

3. SNC's *Binary Armor*® solves the following OT challenges:
   a) Human Factors – ensures safe operations in spite of user oversight or malicious acts
   b) Cyber Threats – prevents accessing, disrupting or damaging critical assets
   c) Secure integration of OT data and logs with IT tools and systems

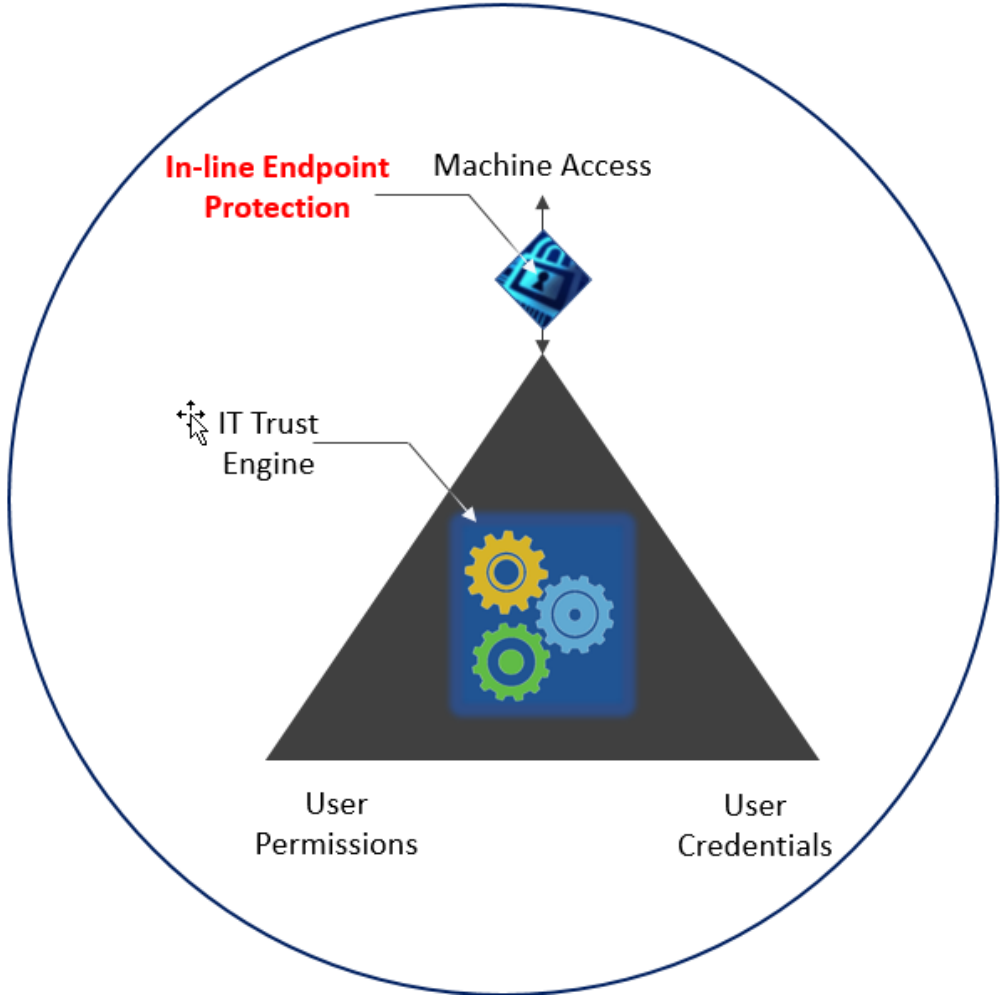
MOSAICS
2020
INDUSTRY
DAY

For Mission Critical Systems – Access Control is not enough

SIERRA NEVADA CORPORATION
BINARY ARMOR

1. Operational Security needs to take into account:
   a) Protocol and workflow compliance
   b) System operating state
   c) Mission continuity and safety

2. Endpoint protection is a key component that both provides protection and enables connectivity



MOSAICS
2020
INDUSTRY
DAY

Introducing Binary Armor

SIERRA NEVADA CORPORATION

BINARY ARMOR

1. Binary Armor is an endpoint cybersecurity device optimized for machine-to-machine and control systems

2. Binary Armor employs a unique approach to cybersecurity, combining message whitelisting, deep content inspection,
state-based processing and encryption

3. Binary Armor is on the DISA APL and has been tested and validated by preeminent U.S. government and industry cybersecurity organizations

4. In operation since 2014 protecting commercial utilities and DoD operational networks

Binary Armor SCADA Network Guard

Specifications	
Voltage	12-48 VDC
Dimensions	3.66 x 3.37 x 2.32 in
Weight	1.2 lb
Power	4.5 W Nominal
	9 W Max
Temp Range	-40° to +85° C
Mounting	DIN Rail
	VESA 50x50mm
	Direct Mount
Interfaces	2 x Gigabit RJ-45
	1 x RS-232 Serial DB9
	2 x TTL GPIO
Protocols	DNP3, Modbus, EtherNet/IP,ROC Plus, BACnet, IEC-61850, HTTP, FTP, SMTP, NTP, Protobuf, XML, FMV, PPLI, COT, NMEA
	Out-of-the-box support for custom binary or ASCII protocols

MOSAICS
2020
INDUSTRY
DAY

The Binary Armor Difference

SIERRA NEVADA CORPORATION

BINARY ARMOR

1. **Deep Content Inspection** – Analyzes every byte of every message to and from control systems

2. **State-Based Processing** – Adjusts cybersecurity based on operational conditions including command sequences, system state and security posture

3. **Open Architecture** – Enterprise management and alerts with an open API and a secure environment to host applications at the edge. All designed for ease of integration and efficiency

Critical OT Cybersecurity Functions	Binary Armor	Your OT Security
Protection against insider and advanced persistent threats	✓	?
Security that takes into account state of control	✓	?
Deep content inspection to validate full message content	✓	?
Workflow & operational process enforcement	✓	?
Validation of entire messages to and from control systems	✓	?
Secure unidirectional traffic flow	✓	?
Secure bi-directional data traffic flow	✓	?
Anomaly detection w/ custom protocol specific logging	✓	?
FIPS-140-2 encryption for legacy protocols and devices	✓	?
Deep packet inspection of headers & common fields	✓	?
Filter unwanted network addresses, ports & protocols	✓	?

MOSAICS
2020
INDUSTRY
DAY

Binary Armor Synergies with MOSAICS

SIERRA NEVADA CORPORATION

BINARY ARMOR

1. Binary Armor provides endpoint security, alerts and logging

2. Binary Armor enables connectivity of new sensors and systems over any available network

3. Binary Armor's secure environment provides a solution to host edge processing and analytics

4. Binary Armor's open architecture can be seamlessly integrated with any orchestration of visualization solution

MOSAICS
2020
INDUSTRY
DAY

AFCEC COINE Use Case: Connecting Offline / Critical Systems

SIERRA NEVADA CORPORATION

BINARY ARMOR

1. AFCEC is piloting Binary Armor for several applications

2. Objective: demonstrate ability to connect mission critical systems currently “offline”

3. Goal: provide increased situational awareness and operational efficiencies without compromising security

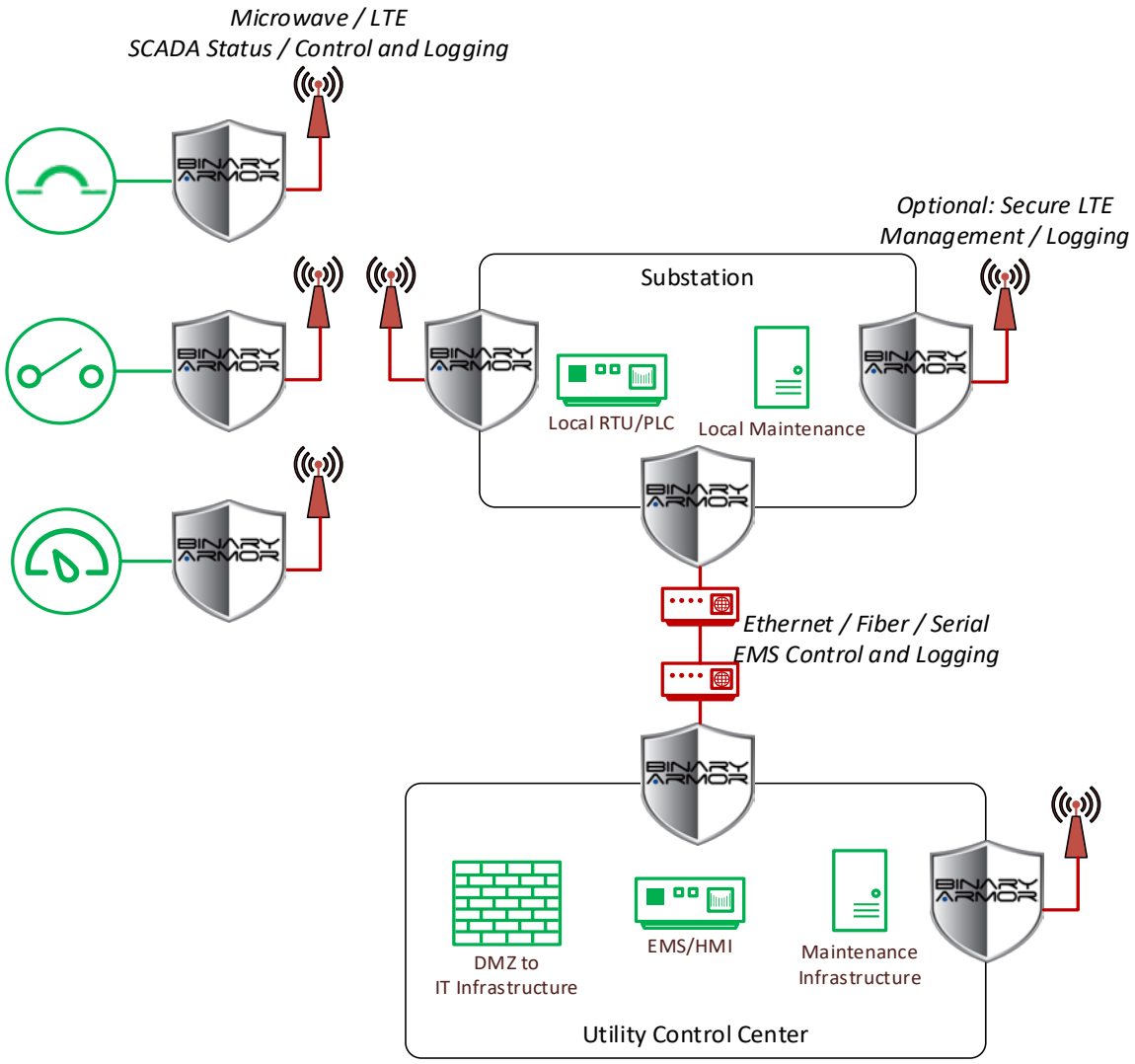
MOSAICS
2020
INDUSTRY
DAY

Utility Use Case: Protecting SCADA and Remote Sensors

SIERRA NEVADA CORPORATION

BINARY ARMOR

1. Binary Armor enables utilities to use commercial communications to rapidly field solutions
2. Binary Armor is in operation at utilities for the following:
   a) Protecting substation automation
   b) Protecting distributed automation and smartgrid
   c) Securing remote monitoring and sensors networks



MOSAICS
2020 INDUSTRY DAY

Final Thoughts

1. Defense-in-Depth requires technology diversity. Partnerships are a key component to protecting DoD and industry critical infrastructure.

2. Endpoint cybersecurity using Binary Armor provides operational efficiency and facilitates new technology adoption such as 5G.

3. SNC as a DoD prime systems integrator is capable of providing end-to-end cybersecurity and integration services.

4. Binary Armor products and services are commercially available for DoD through the GSA schedule or our channel partners.

MOSAICS
2020
INDUSTRY
DAY

Contact Information

SIERRA NEVADA CORPORATION

BINARY ARMOR

1. Peter Fischer – Sr. Director of Cyber Programs
   peter.fischer@sncorp.com

2. Additional resources available at www.binaryarmor.com and www.sncorp.com