Nexus Controls
a Baker Hughes business

Nexus OTArmor† Network Intrusion Detection and Preventions Systems

The Nexus **OTArmor** platform includes the following suite of products for network security:

- IDS and IPS (Intrusion Detection and Prevention System)
- Network Segmentation
- Network Monitoring

Network Intrusion Detection and Preventions Systems (IDS/IPS)

The IDS and IPS solutions help: a) suppress spread of a cyber incident, like network worm propagation in a flat network, b) deploy a transparent network security device in front of uplink port of existing L2 network switches, enabling secure network segmentation by policies, and protocol filtering without changing logical network configuration, and c) establish a new network segment by deploying a secure network device with routing and virtual patching.

A customizable network security option monitors and blocks malicious activity and attacks and provides continuous visibility of unusual activity and potential threats to the control system network.

Solution

The Nexus **OTArmor** network IDS/IPS solution centralizes all the logs from IDS and IPS, as well as events in a single console, to shorten the response time of cybersecurity specialists, thereby improving the efficiency of plant operations.

The IDS solution monitors network traffic searching for suspicious activity and known threats against a target application or a computer, sending alerts when it finds such items. It also monitors traffic and reports its results to an administrator but cannot automatically take action to prevent a detected exploit.

The IPS solution monitors network traffic searching for suspicious activity and known threats against a target application or a computer, sending alerts when it finds such items and has the ability to block those threats.

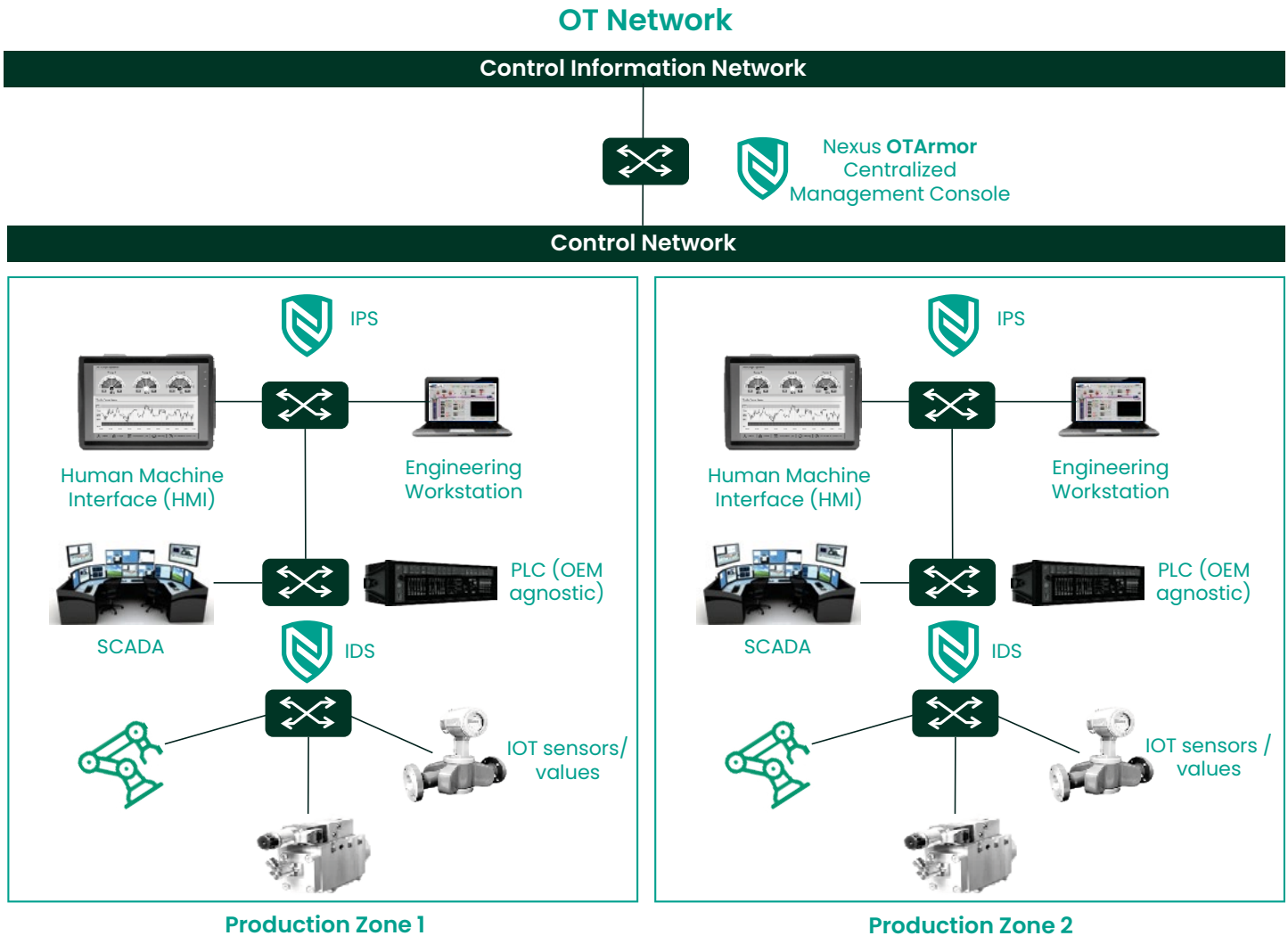
Features

- Multiple industrial protocol support
- Ability to switch between Monitor and Prevention modes
- Denial of Service prevention
- Protection against threats
- Asset information
- Ability to customize policies
- Management – centralized, individual or cloud-based device management
- Syslog capable
- Flexible segmentation and isolation

The Nexus **OTArmor** industrial management console provides a Graphical User Interface (GUI) for policy management in compliance with manufacturing operating procedures. It centrally monitors operations information, edits network protection policies, and sets patterns for attack behaviors. The console offers full visibility into assets, operations, and security threats. IPS and policy enforcement configuration can be assigned per device group, allowing all devices in the same device group to share the same policy configuration.

Scope

- Network segmentation and segregation
- Adaptive network deployment
- Zone protection
- Virtual patch
- OT (Operational Technology) protocol application control



Network Security

Segmentation of OTArmor and Plant Wide Cyber

Nexus Controls uses the concept of segmentation or zoning in accordance with International Society of Automation (ISA) Standard 99. Network segmentation of the **OTArmor** system from systems of differing trust levels is achieved by establishing controlled Electronic Access Points (EAP) between the different trust zones. Access to the **OTArmor** network will be controlled by the firewall to allow only necessary trusted communications to occur. The Nexus Controls Firewall solution is an integrated next-generation firewall platform that monitors and protects the **OTArmor** system from unauthorized or malicious access. The firewall platform provides detection and notification of known suspicious network activity occurring between the **OTArmor** system and the plant control network.

Network Intrusion Detection System

The Network IDS (NIDS) and/or firewall option is an integrated platform that monitors and protects the network. It provides detection of malicious or suspicious network activity based on defined signatures and rules. The NIDS includes OT-specific threat signatures to ensure that known anomalies on control system-specific protocols are identified and alerted on. When configured to provide firewall segmentation, intrusion signatures may be configured to monitor traffic that spans the network boundary between multiple networks.

Supports a Wide Range of Industrial Protocols

Our IDS and IPS products support OT protocols including Modbus, Ethernet/IP, IEC61850, OPC, GE EGD, and more, allowing OT and IT security system administrators to collaborate. This allows for seamless operation with existing network architecture.

Baker Hughes