



Nexus OTArmor[†] Plant Security Asset Management

Proactively Manage Your OT Assets

The Nexus **OTArmor[†]** asset management solution includes industrial visibility features that gather event logs to discover attack vectors that could compromise the safety and availability of the OT (Operational Technology) environment. It also analyzes network traffic and conducts deep packet inspection without interrupting operations. The asset management module provides the ability to discover assets on the control system network by passively monitoring a mirror of the network traffic. It establishes and displays an active asset inventory of the critical network infrastructure.

Benefits

- **Proactively Fix Vulnerabilities**

Once the visibility and mapping are established in the OT environment in terms of connected devices and network traffic, the module will allow the user to drill down and look at common vulnerabilities and exposures (CVEs).

- **Detect Threats Sooner**

The solution will utilize the repetitive nature of the OT network to make it easier to distinguish normal from abnormal behavior. The system will use machine learning to understand what “normal” looks like on the network. It will also create a secure baseline and generate actionable alerts anytime unexpected behavior occurs.

- **Get an Accurate Map of Your Network**

The data gathered over a period of time will be used by employing machine learning to construct a baseline of normal operations which is then used to detect anomalies. This data is then used to create graphical network maps of the monitored assets.

Key features

- **Deep Protocol Inspection and Visibility**

The Nexus **OTArmor** asset management solution performs deep protocol inspection on many industrial vendors and communications protocols to obtain a detailed view of the systems it is monitoring. The deep protocol inspection provides detailed information on system operation and asset inventory. This includes items such as operating system, firmware, and installed modules. In addition, the system provides notification of potentially malicious or unauthorized activities being performed on industrial control assets by observing the types of commands issued to devices on the network. By monitoring down to the application layer, the solution gains visibility to information not gathered by traditional IT (Information Technology) security tools.

- **Configuration Management**

The solution provides the base platform for centralization of Configuration Management and File Integrity Monitoring protection. The centralized compliance management console provides a single point of entry into the configuration management policies and identification of deviations detected on monitored systems. This security module is designed to support by detecting change and conducting scoring against MITRE Attack and international frameworks. Supported frameworks include ANSI/ISA, CIS, ISO, NEI, NERC, and NIST.

- **Vendor Agnostic Detection**

The asset management solution understands and interprets several different industrial protocols to ensure complete discovery. It also understands different vendor specific configurations and values to interpret asset inventory information correctly. It includes three methods of discovery – active, passive and hybrid.

- **Network Intrusion Detection system**

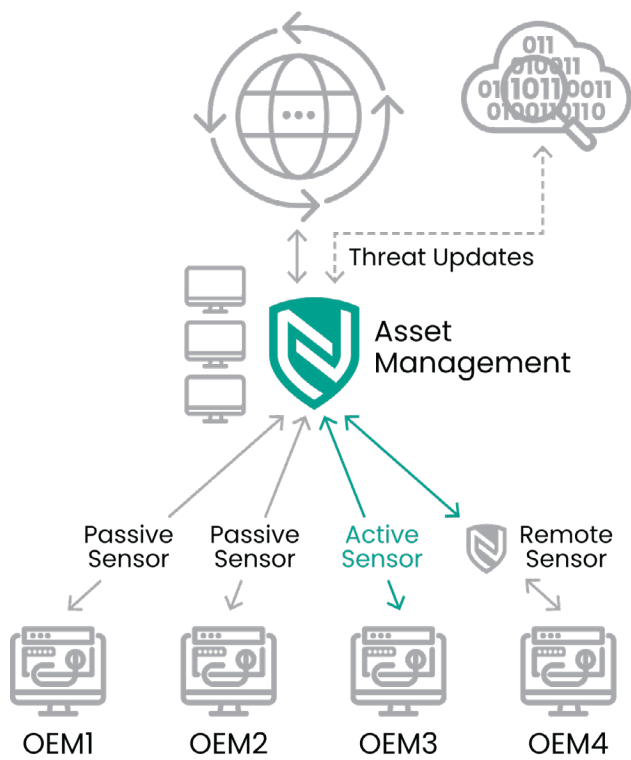
The Network Intrusion Detection System (NIDS) option is an integrated platform that monitors and protects the network. It provides detection of malicious or suspicious network activity based on defined signatures and rules. The NIDS includes OT specific threat signatures to ensure that known anomalies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

About Nexus Controls

Nexus Controls LLC (formerly GE Energy Controls Solutions) exists as the collective experience and history of multiple companies whose expertise, knowledge, and lineage spans over 150 years.

Our global team of domain experts are in 44 countries on all six continents and have successfully delivered over 11,000 successful projects in the power, oil & gas, and various industrial markets.

Nexus OTArmor[†] Plant Security Asset Management



[†] Registered trademark of Baker Hughes in one or more countries.

Other names may be trademarks of the respective owners and are used herein for identification purposes only. Use of any names or marks owned by a third party does not imply endorsement by or a relationship with the third party.