Nexus Controls
a Baker Hughes business

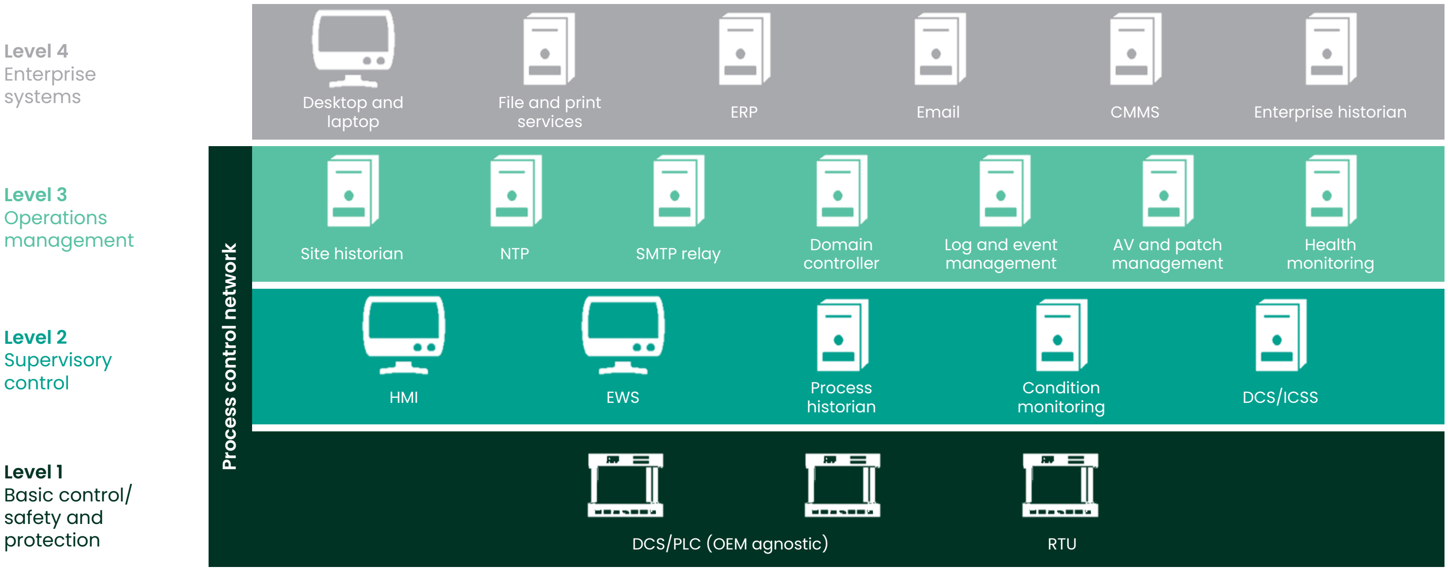
Nexus OTArmor† – Cyber Asset Protection (CAP) subscription service

Overview

In a complex world of ever-changing technologies, Nexus Controls realizes the importance of having a long-term strategic partner to guide successful industrial cybersecurity implementations. As a global leader of industrial control and safety systems, Nexus Controls is well-equipped to help customers improve their security posture and support compliance efforts. Our products are built with industrial security in mind and are easily integrated into broader plant-level systems and companies' OT/IT architectures.

Nexus Controls' Cyber Asset Protection (CAP) subscription solution is a key part of a defense-in-depth system for turbine, plant, and generator controls environments. The subscription service includes operating system and application patches as well as anti-virus/intrusion detection signatures to cover updates for HMIs, servers, switches, and network intrusion detection devices. Monthly updates can be applied to individual HMIs or via the Nexus **OTArmor**† Centralized Patch Management Virtual Appliance. for plant wide and multi-site deployment.

The Cyber Asset Protection subscription is part of Nexus Controls' Nexus **OnCore**† and GE Mark VIe solution and commissioning services. The solution has undergone strict cybersecurity best practices demonstrating to customers that systems are developed and implemented with security in mind. The Cyber Asset Protection subscription is designed to support the plant operation's compliance to several cybersecurity standards and guidelines including NERC CIP, NEI 08-09 and IEC 62443-2-4.



Why patching is critical

Patching your systems is one of the essential first steps to take to protect your assets and assure the operating systems and programs running have updates to provide the latest security protection without risking your operation. Listed as two of the “First Five Quick Wins” by The SANS Institute, a well-respected authority on information security and cybersecurity training, patching of application and system software is critical to improving and maintaining a high security posture.

How it works

The Cyber Asset Protection subscription provides monthly updates for your HMI, data historians, switches, firewalls, OSM and RSG. Software updates include:

- Microsoft Windows® operating system
- Nexus **OnCore**
- GE cimplicity (ICS-CERT-specific)
- Intrusion detection signatures
- Anti-virus signatures
- Switch firmware updates, when impacted by security vulnerability

The CAP subscription service also provides a monthly report of patches that need to be installed and the areas of which are critical for attention. Only the necessary patches are provided. Installing unnecessary patches, such as those coming directly from Microsoft, can increase the risks to the plant.

Benefits

- Provides tested updates to keep your legacy critical infrastructure current
- Reduces downtime by providing only the necessary validated patches which are tested in an environment to assure applicability and compatibility
- On a monthly basis, CAP keeps your risk profile updated and increasingly improves your security posture, by protecting your critical assets from known vulnerabilities
- Helps you meet regulatory requirements and avoid fines
- Improves safety and reliability by preventing loss of view
- Provides a dedicated service manager for cybersecurity issues

The importance of validation

With validated patch management, the updates are validated in a lab that mimics the plant environment to identify any incompatibilities that may exist before the patch is applied. This allows operators to determine what alterations need to be made to ensure uptime and protection against cyber threats without having to create simulators themselves.

Nexus Controls’ testing is done in a secure lab environment using both physical hardware and software, which is the

best method to guarantee industrial controls receive tailored patches and a monthly applicability report. Nexus Controls understands that plants do not have test controls environments, the CAP program ensures you're able to install pre-validated updates without requiring a plant wide outage.

A trusted partner for compliance

As a vendor of industrial controls, Nexus Controls embraces its responsibilities to assist critical infrastructure owners as they improve their security postures and support compliance efforts related to Nexus Controls' provided equipment throughout the 10 to 20-year lifecycle of the control system itself. Nexus Controls can offer security support that spans from initial system design to commissioning, all the way through ongoing support and maintenance, and multi-year industrial cybersecurity roadmaps.

NERC CIP

Many U.S. electric utilities are now federally mandated to comply with NERC CIP requirements that dictate industrial security and remediation technology, including required compliance. To be considered in adapting operations to these regulations is the difficulty of patching industrial controls and the frequent attacks on the equipment. In addition, customers need to address known ICS vulnerabilities without disrupting operations. Because of these factors, electric utilities require a solution that is easy to implement and provides visibility into the industrial network and compliance.

NEI 08-09

US nuclear power companies are federally mandated to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber-attacks.

As part of having a cybersecurity plan, operators are required to address known ICS vulnerabilities and have solutions in place for operating system, application and third-party software updates, Host Intrusion Detection (HID), and non-repudiation, among others.

IEC 62443-2-4

IEC 62443-2-4 is a published international standard, defining cybersecurity capabilities that Industrial Automation and Control System (IACS) service providers may implement and offer. The standard can help asset owners consistently procure and manage control systems security expertise. IEC 62443-2-4 was developed by IEC technical committee 65, in collaboration with the International Instrumentation Users Association (previously WIB) and ISA 99 committee members. Nexus Controls hardens customer systems using a combination of technical and procedural measures (including patch management) that have been certified to meet IEC 62443-2-4 security standards. These standards specify a comprehensive set of security requirements for the installation and maintenance of IACS.

To read more about our capabilities on these three standards and regulations, visit our website, **bakerhughesds.com/nexus-controls/industrial-cybersecurity**

[†] 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.

Baker Hughes ™

nexuscontrols.com