Nexus Controls
a Baker Hughes business

Nexus OTArmor† Remote Patch Management Solution

Why patching is critical

Patching your systems is one of the most effective things you can do to protect your assets and ensure the operating systems and programs running are updated 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 strong security posture.

Remote Patching Service

Having current patches is critical to not only meeting regulatory compliance requirements, but also improves the cybersecurity posture of an industrial plant. However, even with receiving validated monthly patches from OEMs and system integrators, the activity of deploying patches on a periodic basis (monthly, quarterly) can divert plant resources from revenue generating operations and maintaining equipment uptime.

Benefits

The Nexus Controls' Nexus OTArmor† Remote Patching Service eliminates the need to have skilled labor on site to deploy patches and improves efficiency of operations by reducing potential downtime.

Having a secure infrastructure also enables gateway for other services like health checks, advanced remote cybersecurity risk and vulnerability assessments, Managed Security Services (MSS), remote monitoring and diagnostics. Having secure connectivity will also enable collection of telemetry data from controller to perform advanced analytics.

Scope

Service scope includes initial setup and provision of the Nexus **OTArmor** Remote Patching Service to deploy software patches and updates via remote connection for all devices like HMIs, Historian, Virtual HMIs, etc. covered by the Nexus **OTArmor**† Cyber Asset protection (CAP) service scope at site. Typical contract terms include 1, 3 and 5 years.

What is included:

- Provision of tested and documented security updates that support your site's patch management activities
- Service for the pre-setup of the system, health check of the cyber configuration, system errors and backups
- Installation of the hardware and software required to provide the Nexus **OTArmor** Remote Patching Service
- Patching status reports
- Monthly Remote Patching for the assets under the CAP agreement

Remote Diagnostic Services (option)

- Fast, 24/7 access to diagnostic experts
- Response time typically less than 10-minutes
- Solution typically identified within 2-hours
- Measurable reduction in equipment downtime
- Secure remote connectivity
- Event-based and periodic progress reporting
- Proactive system checks ensuring readiness-to-serve
- Collaborative processes supporting site operations

Nexus Controls' Managed Remote Connectivity

Nexus Controls leverages state-of-the-art technologies to provide an intrinsically secure, remote connection from your site(s) to our data center. **Security Features include:**

a) Privileged identity management and access controls including multi-factor authentication (MFA)

b) Improved traceability of access and ease of audit

c) Stateful packet inspection firewalls that only allow approved and valid traffic

d) SSL/IPSec VPN data tunnel for data confidentiality

e) 24/7 Security Operations Center (SOC) monitoring the security of the remote connection along with all other Baker Hughes' networks

f) Airgap network switch to physically disconnect the network for full manual control over the connection

The equipment provided to site consists of the following:

a) Router

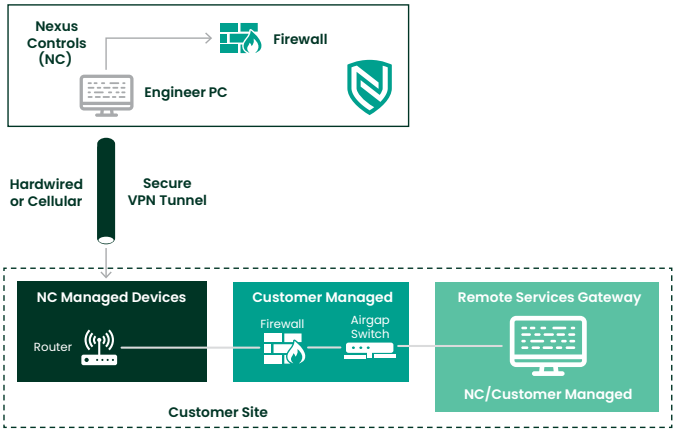
b) Firewall

c) Network Switch

d) Ethernet Cables

e) Hardwired or Cellular connection

High Level Architecture



NOTE: Plants with older, or no existing Remote Secure Gateway (RSG) will be provided with new Virtual Machine to install and configure in the existing Nexus **OTArmor** server (Formally SecurityST).

About Nexus OTArmor

With our **industrial mindset, expansive partner ecosystem and certified OT (Operational Technology) specialists**, Nexus Controls provides holistic **end-to-end industrial security solutions** to ensure you have an effective cybersecurity program, meeting the needs of legacy control systems, with limited expert resources, while accounting for modern technology and increasing cyber threats. Our team of cybersecurity experts is well-versed in designing **solutions** that meet multiple cybersecurity regulatory compliance standards across the globe, including NERC CIP, ISO/IEC 27036-3, and NIST SP800-161, IEC 62443, NIS-D, NEI-08-09 (US Nuclear), and N290.7-14 (Canada Nuclear).

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.

BHCS39206 (12/2021)

Baker Hughes

nexuscontrols.com