
Nexus Controls
a Baker Hughes business
Operational technology cybersecurity solutions

Overview

In a complex world of ever-changing technologies, Nexus Controls, a Baker Hughes business, realizes the importance of having an experienced partner to guide successful cybersecurity implementation. As a global leader of industrial controls, Nexus Controls is well-equipped to help customers improve their security posture and support external and internal compliance policies and requirements.

Nexus **OTArmor**™ cybersecurity technology is a core component of a platform-agnostic, defense-in-depth strategy that is necessary to achieve safe, reliable, and predictable plant and process operations in a critical infrastructure environment. The Nexus **OTArmor** is IEC 62443-2-4 and 62443-3-3, indicating the solution has undergone strict cybersecurity best practices demonstrating that systems are developed and implemented securely.

"The world is connected - countries, people, machines. These connections make us smarter, stronger and more productive but also bring with them vulnerability. Effective cybersecurity is a reality of business in our connected world."

You produce. We protect.

Cybersecurity by the numbers

1 in every 4

days the US power grid is struck by a cyber or physical attack.

$1M

The average cost of each NERC CIP Violation.

26%

of incidents investigated by ICS-CERT were spear-phishing, making it the leading threat for 2016.

74%

of exploits are targeted at applications, with more than 40% of those being Microsoft & Adobe.

59%

Insider threats are on the rise – a study showed that 59% of employees who left the company take proprietary information with them.

290

In 2016, US Homeland Security responded to 290 incidents of cyber invasions or breaches with 63 in Critical Manufacturing and 59 in Energy.

77%

Of 150 IT professionals in the energy, utilities and oil & gas segments interviewed, 77% reported at least one security breach in the last 12 months.

243

Average number of days before detection that a system is compromised.

Challenges for Critical Infrastructure Protection

Volume of expertise

Regulation challenges

Legacy infrastructure

Leader support

Constrained resources

Remote connections/ communications

Cybersecurity is a must-have in today's world. The challenge is knowing how to apply it.

Nexus Controls cybersecurity culture

Nexus Controls is committed to a culture of security to protect our systems, products, and customer operations. We strive to support our customers' efforts to secure energy and industrial operations, and we embrace industry efforts toward achieving cybersecurity excellence. With more than a decade of experience in securing industrial control systems, Nexus Controls is your partner in helping you securely realize the benefits of digital transformation.

Nexus Controls cyber history

Proven experience

Protection for the world's top operators in oil and gas and power generation including nuclear and renewable energy.

2008

Cyber Asset Protection Lab launched: pre-validated security updates for control system

2009

NETCAP launched: first generation security appliance

2013

SecurityST launched: multi-functional centralized security management

2014

GE Acquires Wurldtech:

- ICS Security Assessments
- Achilles Process Certification
- Achilles Communication Certification
- Intrusion Prevention Technology

2015

IEC 62443 2-4 Certification: we are the first GE business to become certified

2017

OEM Agnostic platform launched: multi-site & plantwide

2019 & 2020

Nexus OTArmor™ launched: major portfolio expansion:

- Asset Management
- Virtual Patching
- Portable Security
- Multi-Factor Authentication
- Secure Remote Connectivity
- Managed Security Services

IEC 62443 3-3 Certification

Our security program

Nexus Controls security program is designed to meet the demands of operating in today's complex threat environment, addressing the key areas of people, process and technology. Backed by leadership directives, our security program includes dedicated teams accountable for implementing security controls in ten key areas that span a secure development lifecycle, from product design to ongoing operational support.

Our people

Nexus Controls commitment to security begins and ends with our employees. This effort begins at the top with comprehensive cybersecurity policies regularly communicated throughout our organization. We have dedicated teams committed to IT, industrial, and product security. These organizations work together to drive cybersecurity best practices.

Our processes

Nexus Controls has adopted international security standards related to our infrastructure, as well as processes that impact its resilience. Where applicable, Nexus Controls seeks and obtains independent certifications aligned to internationally recognized security standards.

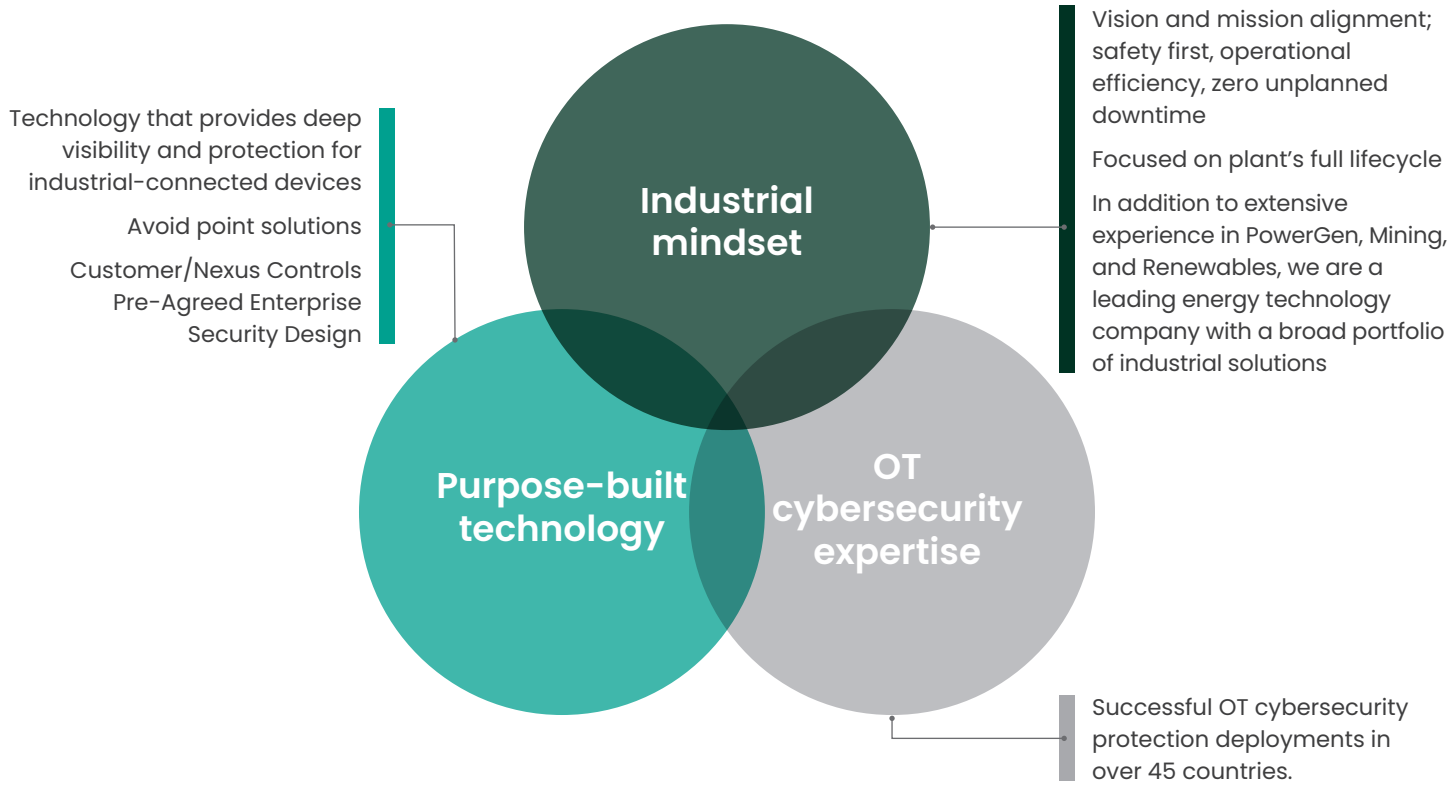
From product development through delivery and maintenance, our policies and procedures address security throughout an energy operation's lifecycle. Adoption of secure development lifecycle processes support the implementation of critical security controls for the delivery of both products and services. A dedicated team maintains relationships with key operating system, network device, and application vendors to closely track security issues, software updates, and newly released patches—with the intent to alert product users when needed. Newly available patches, malware detection signatures and anti-virus are evaluated and tested for applicability to the system.

Our technology

Nexus Controls equipment is engineered with security in mind. Our product development lifecycle includes product assessments (both internal and third party testing) and security design reviews as a regular practice within our development process. Updated tools and methods in both IT and OT security are applied throughout the product lifecycle to reduce risk and address vulnerabilities.

Long-term strategic partner

We are your long-term strategic partner in cybersecurity, focused on protecting your critical data and assets throughout their lifecycle. The approach we bring to every customer relationship centers around three key areas to ensure proper security for your OT network.



A holistic group of technical controls to mitigate risk

Security design

Assess controls

Controls security lifecycle

Maintenance

Security training

SERVICES	SERVICES	SOLUTIONS	SERVICES	TRAINING SERVICES
• Security governance consulting services • Security FAT – cyber secure lab	• Cybersecurity assessments • Create/review policy documents • Perform gap analysis to review compliance reporting	**Nexus OTArmor platform** • Access/password management • Centralized patch management • Automated backup and recovery • Security Information and Event Management (SIEM) • Firewall intrusion detection and protection • Asset management • Multi-factor authentication • Application whitelisting • And more	**Cyber Asset Protection (CAP)** • Subscription of updated patch and signature updates replicated in a control system environment • Patch applicability reports and ports and services documentation	• Security awareness training for responsible plant personnel

Expansive cybersecurity solution

Nexus **OTArmor** is a flexible and configurable cybersecurity solution specifically designed for operational technology networks. As a key part of a layered cybersecurity strategy, Nexus **OTArmor** offers the proactive protection policies and centralized reporting capabilities needed to reduce your threat surface, manage cyber risk, and comply with global security standards.

	Nexus OTArmor compact	Nexus OTArmor standard	Nexus OTArmor pro
	 **Server |** Up to 15 HMIs	 **Server |** Up to 30 HMIs	 **Server |** 30+ HMIs
Basic features	• Role-based access • Secure mode • Host-based patching, backup and AV	• Role-based access • Secure mode • Centralized patch management program • Centralized back-up • Redundant back-up domain controller	• Role-based access • Secure mode • Centralized patch management program • Centralized back-up • Redundant back-up domain controller • High-Availability configuration – Auto failover
Available enhanced features	• Application Wwhitelisting • Centralized backup • Centralized patch management program	• Application whitelisting • SIEM (logging and monitoring) • Network intrusion detection and prevention firewall options	• Application whitelisting • SIEM (logging and monitoring) • Network intrusion detection and prevention firewall options

Nexus OTArmor features

Role-based access control

This feature provides centralized control and management alerting specific to the controls environment. Simply put, it allows you to manage who can access the industrial control system and what permissions they have.

Backup and recovery

Automatic, centralized backup and recovery of the process control domain saves time and money through availability of a quick disaster recovery plan with minimal downtime. All backup activities are logged and easily accessed for generating reports to assist with compliance reporting.

Remote access security

Our remote access security options include multi-factor authentication, lockbox, data-diode (one-way directional), VPN, intrusion prevention and read-only access. By segmenting access using clear enforcement zones, you can better control who can access your critical assets and what information they can access.

Monthly patching program

The Cyber Asset Protection subscription provides monthly software and firmware updates for your HMI, Historians, switches, firewalls, OSM and RSG, including key security patches. With Nexus **OTArmor**, patches can be deployed centrally, eliminating an average of 4 hours per HMI of man hours, which can result in up to $20,000 monthly savings per plant.

Application whitelisting

With the application whitelisting option, devices have improved security by reducing the risk and cost of malware, improving network stability and reliability. This feature automatically identifies trusted software that is authorized to run on control systems while preventing software that is unknown or unwanted.

Network intrusion detection and prevention systems

This customizable network security option provides the ability to monitor and block malicious activity and attacks, and provides continuous visibility of unusual activity and potential threats to the control system network.

Security Information and Event Management (SIEM)

We provide a scalable solution with both real-time and historic dashboard views of cyber activity such as changing of switch configurations, failed login attempts, unauthorized port access and USB usage.

Asset management

This capability identifies all network assets and maps the flow of data traffic between them, analyzes network traffic and conducts deep packet inspection (PCAP data), and establishes a baseline which is then used to detect anomalies.

Secure implementation and chain of custody

As a cybersecurity solution provider, security starts with us. We build and prepare each Nexus **OTArmor** solution with strict attention given to physical and digital security through the use of physical perimeters, access control with video surveillance, and secure custody transfer. Our Longmont, Colorado Headquarters is certified to meet the needs of nuclear, oil & gas and power generation customers through strict adherence to standards required by IEC 62443 and NEI 08-09.


CYBER
SECURITY
CONFIRM
click here for more informati

Cyber Asset Protection (CAP) subscription – validated patch management service

Nexus Controls' Cyber Asset Protection patching program 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** platform for network-wide deployment.

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.

The importance of validation

With validated patch management, the updates are validated in a lab that mimics the plant environment in order 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. Our 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 an applicability report on a monthly basis.

Cyber Asset Protection patching program overview

What it is:

Validated cybersecurity subscription service for for Nexus **OnCore**™ and Mark* controls, hardware and software that includes:

- Windows patch updates (2008-2016), Microsoft Office, Adobe
- Antivirus updates (Sophos, McAfee)
- Intrusion detection signatures (Host & Network based IDS)
- Firmware updates (when required by security vulnerability)
- Work instructions for issues found during validation (new deployment scripts, modification instructions)
- Technical support through controls connect (TILs; TINs; direct communication)

How it helps:

Protects

- Validated patching protects HMI and endpoints, the most vulnerable point of the system
- Minimizes risk & downtime by ensuring updates are tested in a customer simulated environment with 3rd party validation to correct issues before delivery
- Accelerates your change management approval process

Supports reporting requirements:

- Provides an up-to-date and cumulative inventory of applicable updates and their status

Cyber Asset Protection scope

Validation covers

- Nexus **OnCore** systems
- Mark V-VIe control systems
- EX2000-EX2100e
- LS2000-LS2100e
- Control software including Cimplicity and ControlST
- Baker Hughes HMIs, Historians, System1, Remote Services Gateway (RSG) and Onsite Monitor (OSM)
- Windows® Operating Systems
- Unified Threat Management (UTM) firewalls and intrusion detection/prevention systems
- Networking routers and switches
- Microsoft Word® and Excel®
- Adobe® programs

How it is delivered

- Offline secure delivery (Tamper Evident Seals/Hash comparison tool)
- CAP secure portal (download approved ISO's)

The validation and testing process

Questions answered during validation:

- What files are modified?
- New user accounts or services?
- New established ports?
- Impact to other applications?
- US-CERT applicability status?
- Can I safely install?

Interrogation Testing Criteria:

- Each update baseline is defined
- Each update follows the same testing process (not a fast fail test)
- Representative hardware environment
- Driver/firmware testing
- Communication testing (intra/inter-system/network/serial)

What's Included with your subscription

- **CAP PROGRAM BINDER:** contains important information about the components of CAP software update subscription as well as process instructions, reports, and storage sleeves for assessment and update DVDs
- **COMPLIANCE:** includes support documentation to assist with compliance (NERC CIP, NEI, etc.) and online access to ports, services and hardening documentation
- **DOCUMENTATION:** assists with compliance, system design, reliability, and configuration baseline documentation; ports, services and hardening documentation. monthly updates are documented and scripted for operating system, applications and antivirus signatures
- **SUPPORT:** access to cybersecurity support team, with CAP-related phone support. CAP service managers will contact the site to monitor the program and provide any additional assistance required

Nexus Controls support for regulations and standards – a trusted partner for compliance

As a manufacturer of industrial controls, Nexus Controls embraces its responsibilities to assist critical infrastructure owners to improve their security postures and support adherence to industry standards.

Nexus Controls aligns to multiple best practices frameworks and standards, and helps customers meet regulations such as NERC CIP and NEI 08-09.

In addition to regulations, our team is well versed in supporting common architecture frameworks and standards such as the NIST 800 series, CIS Controls, and ISO 27002. Our extensive experience can also help those organizations who are working toward developing and meeting internal standards.

NIST 800-82 Guide to Industrial Control Systems

The NIST 800 series of special publications addresses process, organizational and technical aspects required to implement a full life-cycle cybersecurity management program. NIST 800-82 is one of the few non-vendor funded publications that specifically addresses Industrial Control System Security. Nexus Controls security governance services can help organizations develop and implement full life-cycle frameworks that consist of customer-specific requirements, international standards, and Nexus Controls own critical infrastructure and process control cybersecurity best practices.

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 was developed by IEC Technical Committee 65, in collaboration with the International Instrumentation Users Association (previously WIB) and ISA 99 committee members. The table below represents BHGE's alignment to specific requirements of this standard.

Solution staffing	Network security	User security	Application security	Security information and event management (SIEM)	Patch management	Patch management
						

 Nexus OTArmor platform

 Services

 Cyber Asset Protection (CAP)

NERC CIP Rev 5 & 6

Many U.S. electric utilities are now federally mandated to comply with NERC CIP requirements that dictate industrial security and remediation technology. 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. The table below represents Baker Hughes alignment to specific requirements of this regulation.

CIP-001-5 Sabotage Reporting	CIP-003-6 Security Manage-ment Control	CIP-004-6 Personnel & Training	CIP-005 Electronic Security Perimeter (ESP)	CIP-006-6 Physical Security of BES Cyber Systems	CIP-007-6 System Security Management	CIP-009-6 Recovery Plans for BES Cyber Systems	CIP-010-2 Configuration Change Management & Vulnerability Assessments	CIP-011-2 Information Protection
								

 Nexus OTArmor platform

 Services

 Cyber Asset Protection (CAP)

NEI 08-09

Baker Hughes supports nuclear compliance efforts for NEI 08-09 by providing baseline configuration documentation for current and certain legacy controls, and by supporting asset operator cyber vulnerability assessments and associated mitigations. The table below represents Nexus Controls alignment to specific requirements of this regulation.

Access controls	Audit & Accountability	CDA, System, and communications protection	Identification & Authentication	System hardening	Contingency planning
●	●	●	●	●	●
	○		○	○	

● Nexus OTArmor platform ○ Cyber Asset Protection (CAP)

“We offer expansive cybersecurity solutions that are grounded in our deep knowledge of operational technology assets and networks - keeping you in compliance and protected from ever-changing threats, so you can focus on producing at optimal output.”

BHCS32714C (10/2020)

Baker Hughes

nexuscontrols.com