



OT ARMOR: GE VERNOVA'S CYBERSECURITY SOLUTION

OVERVIEW

To guard against cyber attacks and ensure the continuous availability of critical operational technology (OT) infrastructure, power generation plants must implement and sustain a growing number of vital security controls. However, with limited budgets and staff, it gets increasingly difficult to contend with these escalating demands.

CYBER THREATS IN OT

Approximately 90 percent of manufacturing organizations had their production or energy supply hit by some form of cyberattack.¹

Geopolitical risks in 2022 resulted in an 87 percent increase in ransomware incident.²

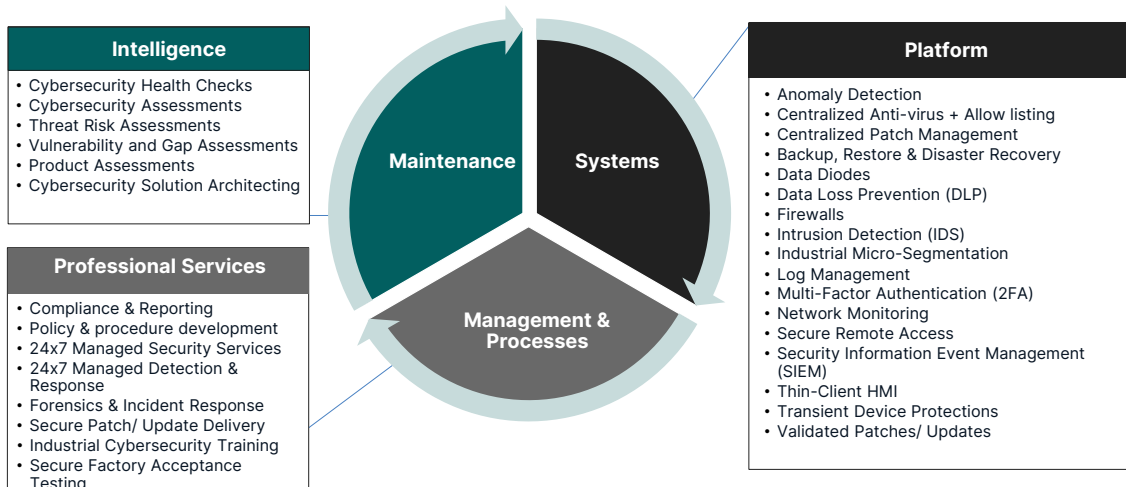
10.7% of observed cyberattacks targeted the energy industry.³

CHALLENGES

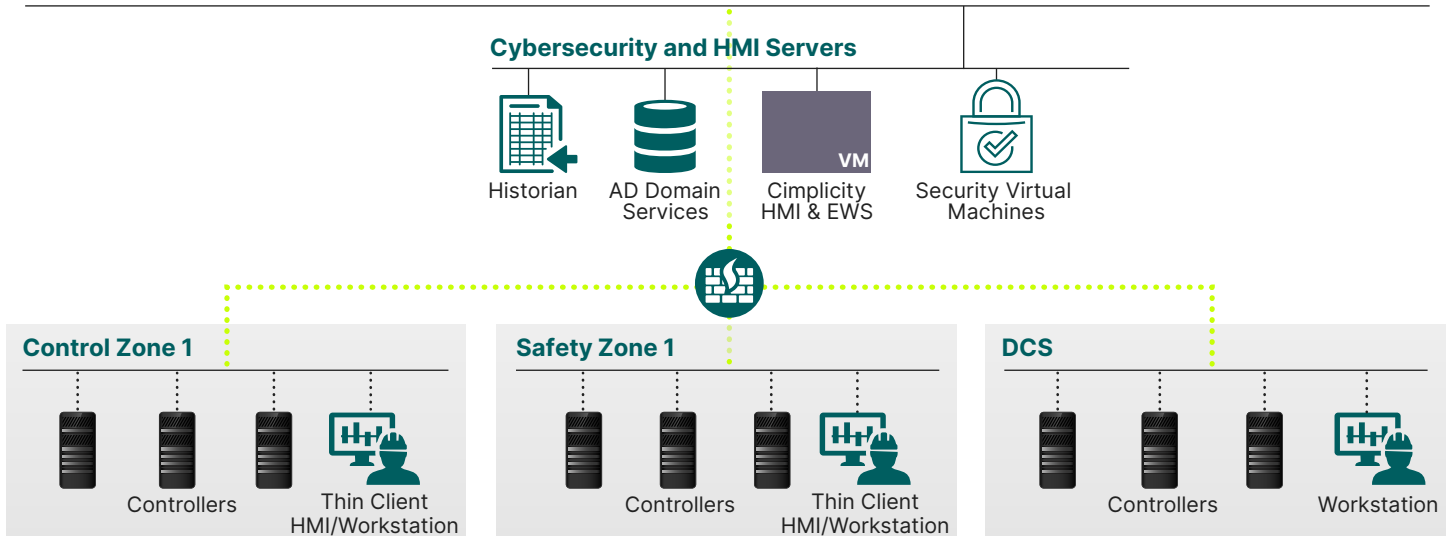
Today's organizations must guard against continuously evolving, increasingly advanced cyber threats. For the security teams in these organizations, a range of security mechanisms need to be implemented, but that's only the beginning. Threats—and the mechanisms needed to guard against them—evolve rapidly. Therefore, systems need to be tuned, monitored, and managed on a continual basis—and many teams struggle to keep pace with all these ongoing demands.

In many organizations, security demands are growing too fast, and time, staff expertise, and money are in too short supply. Given these realities, many decision makers have been faced with highly unappealing scenarios around investments in comprehensive security programs vs increased exposure to cyber attacks.

GE Vernova's Gas Power offers a far more appealing alternative.



Supervisory Control Zone



GE Vernova's cybersecurity platform features a broad range of capabilities and offers efficient integration in OT environments. (Network configuration is only an example – configuration and implementation may vary.)

ADVANTAGES

GE Vernova's cybersecurity platform offers the following advantages:

- **Comprehensive coverage.**
Supports integration with a range of operating systems.
- **Improved for plant control and operational technology environments.**
Features close alignment with power generators' OT environments, including GE and third-party equipment.
- **Advanced automation.**
Automates patch deployments, configuration policy enforcement, configuration file backup, and more.
- **Optimized integration.**
Helps deliver applications, services, hardware, and configurations that are pre-integrated, tested, and tuned.
- **Enhanced flexibility.**
Helps customers address near- and long-term needs, featuring a modular approach that enables teams to start small and expand over time. Offers capabilities for feeding information into an enterprise security operations center, so teams can efficiently manage an entire fleet. Supports flexible integration of new technologies.

SOLUTION

GE Vernova's cybersecurity solution helps deliver comprehensive security capabilities in a single, pre-integrated platform, enabling your organization to establish robust, defense-in-depth controls in plant environments.

The solution provides security controls and OT maintenance tools for GE MarkVI and MarkVIe networks. With our solution, you can leverage a full suite of security capabilities—without all the time, cost, and effort of procuring, testing, integrating, and deploying these disparate solutions independently.

GE Vernova's cybersecurity platform collects, correlates, and forwards security logs and events, and it presents this information to plant personnel in a highly usable format. The solution offers identity and password management capabilities for control-system environments. In addition, the solution can be customized so it aligns with your existing environment, including your Security Information and Event Management (SIEM) platform, backup mechanisms, anti-virus technologies, log management platforms, and more.

GE Vernova's integrated cybersecurity platform offers the below features:

- Hardware appliance and operations console
- Hardened server and thin-client console
- Optional, hardened firewall
- Secure-by-design configuration
- Global regulatory certifications and hardware support

In addition, the solution features applications and services that deliver comprehensive security capabilities, supporting access control, patch management, log aggregation, and much more. The solution offers intelligence reporting for GE Vernova's cybersecurity platform servers, and, for assets managed by the solution, it reports on patch availability and vulnerabilities. The solution is backed by complete services and support, including assistance with setup, installation, and integration of workstations and network assets.

BENEFITS

By putting GE Vernova's cybersecurity platform to work in your organization, you can capitalize on the following benefits:

- **Reduce cost and staff inefficiencies**
GE Vernova's cybersecurity platform packages and pre-integrates dozens of security technologies—so your teams don't have to. The solution eliminates all the efforts that would be required to procure, integrate, deploy, and maintain these solutions individually. The solution centralizes the management of patches, anti-malware, backup and recovery, and user identities. Further, the solution helps deliver automation and advanced technology that streamlines ongoing management and maintenance.
- **Mitigate risk**
With GE Vernova's cybersecurity platform, you can gain actionable insights into your OT environment and security posture. You can quickly establish comprehensive security mechanisms that mitigate the risk of cyber attacks and failed compliance audits. The solution can help your team address a broad range of cyber security regulations, standards, and guidelines, including NEI 08-09, NERC CIP, and IEC-62443 (ISA 99).
- **Improve availability**
GE Vernova's cybersecurity platform helps your team ensure that the security controls implemented are aligned with your operational goals. The solution supports the implementation of maintenance and governance processes that help protect your most critical assets.

KEY CAPABILITIES

Identity Management and Role Based Access Control

With GE Vernova's cybersecurity platform, your organization can establish least-privileged access controls for administrators, which is a central tenet to complying with security best practices and many regulatory mandates. The solution enables your team to establish central management of user identities and role assignments.

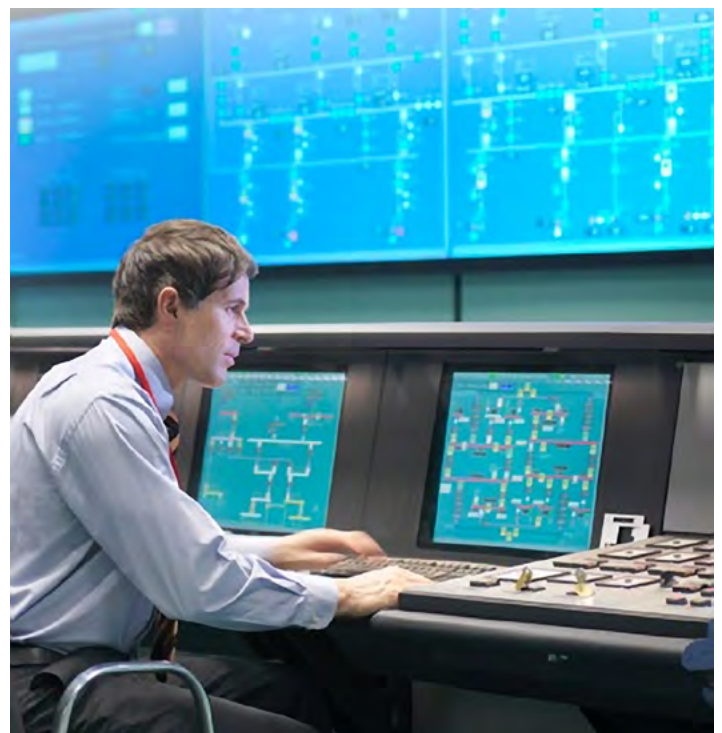
GE Vernova's cybersecurity platform helps your team create password complexity rules and enforce policies around secure passwords. For example, it enables you to prohibit the use of vendors' default passwords. The solution augments these capabilities by offering certificate services and encryption that secure communications between GE's HMIs and controllers.

Malware Protection

GE Vernova's cybersecurity platform features antivirus capabilities that detect and disrupt malicious code discovered on the network. The solution also offers application control capabilities that help ensure only authorized software runs in the environment.

System Hardening

GE Vernova's cybersecurity platform employs a number of hardware and software configurations that make assets more difficult to attack. GE Vernova's cybersecurity platform features a hardened appliance with secure-by-design configurations. Based on the server, the solution includes mounting hardware, security bezel, and blockers for unused USB and network ports.



The platform establishes secure configuration of privileges and implements a least-privileged approach for administrative access. The solution offers a number of configuration management capabilities. The solution collects baseline configurations for managed assets, it creates alarms when configurations are changed, and it automatically corrects unauthorized changes. The configuration management software's agentless deployment streamlines implementation and ongoing administration.

Supporting Windows and Linux operating systems, the solution's host intrusion detection system helps deliver capabilities for file integrity monitoring, log monitoring, rootkit detection, and active response to alerts.

System Backup and Recovery

GE Vernova's cybersecurity platform is fully customizable, so you can effectively adapt it to meet the specific needs of your environment. With the solution, you can leverage your existing technologies and the feature sets integrated within a range of operating system environments. The solution's lightweight deployment requires minimal configuration. The solution automates backup of critical configuration files to support fast, efficient system recovery in the event of system corruption, misconfiguration, or compromise.

Log Aggregation and Security Information and Event Management (SIEM)

GE Vernova's cybersecurity platform includes a SIEM that offers asset and software discovery capabilities and that enables you to do event correlation and logging. The SIEM is configured to monitor your control networks and your GE Vernova's cybersecurity platform environment. The solution features customizable dashboards and pre-packaged dashboard views, offering visibility into network traffic, system state, security alarms, and recent events.

The platform also offers advanced log aggregation capabilities, providing a centralized system that can aggregate device logs from a range of sources, including event logs in Microsoft Windows-based systems, syslog data and other log formats from Linux-based systems, logs from network devices and embedded systems, and application-level log files. The solution offers customizable dashboards and it enables you to do centralized review, management, reporting, and searching on alerts. In addition, logs can be forwarded to the GE Vernova's cybersecurity platform SIEM and third-party SIEMs for event correlation and automated log analysis.

Network Infrastructure Management

GE Vernova's cybersecurity platform offers a number of capabilities that support efficient, automated management and maintenance of network equipment, including switches, routers, and firewalls. The solution

does automated backup of configuration files, which enables more rapid and efficient recovery from issues and outages.

Patch Validation Program

This optional program offers comprehensive patch management services, covering all the GE assets in the environment that are managed by GE Vernova's cybersecurity platform. This program offers testing and validation of anti-virus and host intrusion detection signature updates as well as operating system patches.

Through this program, we help deliver patches via a convenient, secure web portal. These patches are delivered in complete, scripted packages that are easy to deploy. Featuring cumulative updates, these packages also help you ensure you're current with the latest releases. Plus, using the GE Vernova's cybersecurity platform appliance, you can establish automated, centrally managed deployment of patches.

Remote Access Security

Our remote access security options include Multi-Factor Authentication (MFA), 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.

Application Allow listing

With the application allow listing option, Windows and Linux based devices have improved security posture 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 system HMIs 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.

Asset Visibility

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.

Intelligence Reporting

On an ongoing basis, GE delivers reports on patch availability and vulnerabilities affecting equipment in scope. Through this reporting, you can gain timely, intuitive insights into your organization's cybersecurity posture and its areas of exposure.

BACKED BY EXTENSIVE SUPPORT AND A COMMITMENT TO QUALITY

GE Vernova’s cybersecurity platform is backed by extensive services and support. Our experts will set up the system in your environment, performing installation, commissioning, and start up of the included applications and services. We offer your team two days of onsite, hands-on training. We also offer documentation, optional factory acceptance testing, and optional ongoing maintenance.

We are committed to quality services and support, and empower team members to make customer-focused quality the highest priority. Further, our team participates in a number of external quality certification programs, including ISO-9001:2015 and ISO-27001:2013.

GE VERNOVA’S SUPPORT FOR REGULATIONS AND STANDARDS – A TRUSTED PARTNER FOR COMPLIANCE

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

GE Vernova 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. GE Vernova’s security governance services can help organizations develop and implement full life-cycle frameworks that consist of customer-specific requirements, international standards, and GE’s 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 GE Vernova’s alignment to specific requirements of this standard.

 Solution Staffing	 Network Security	 User Security	 Application Security	 Security Information & Event Management (SIEM)	 Patch Management
					


























 GE Vernova’s Cybersecurity Platform




 Services

 Patch Validation Program

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 GE Vernova's alignment to specific requirements of this regulation.



									
CIP-002 Asset Identification and Classification	CIP-003-6 Policy and Governance	CIP-004-6 Personnel & Training	CIP-005 Network Security	CIP-006-6 Physical Security of Cyber Assets	CIP-007-6 System Security Controls	CIP-008 Cybersecurity Incident Response	CIP-009-6 Recovery Plans for BES Cyber Systems	CIP-010-3 Change and Vulnerability Management	CIP-011-2 Protection of BES Cyber System Information
	 				 	 	 	 	

 GE Vernova's Cybersecurity Platform
  Services
  Patch Validation Program

NEI 08-09

GE Vernova 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 GE Vernova's alignment to specific requirements of this regulation

					
Access Controls	Audit & Accountability	CDA, System, and Communications Protection	Identification & Authentication	System Hardening	Contingency Planning
	 		 		 

 GE Vernova's Cybersecurity Platform
  Patch Validation Program



GE VERNOVA

1 <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/how-to-enhance-the-cybersecurity-of-operational-technology-environments>

2 S&P Global, "Feature: Energy industry faces unprecedented cyber threats almost daily," July 19, 2018, www.spglobal.com/platts/en/market-insights/latest-news/electric-power/071918-feature-energy-industry-faces-unprecedented-cyber-threats-almost-daily

3 <https://securityintelligence.com/articles/2022-industry-threat-recap-energy/>

governova.com

Information contained in this document is indicative. No representation or warranty is given or should be relied on. Information provided is subject to change without notice.

© 2023 GE Vernova and/or its affiliates. All rights reserved.

GEA35050A (11/2023)