GE VERNOVA

FACTSHEET

GE Vernova's Cybersecurity Solution - OTArmor

ASSET VISIBILITY AND ANOMALY DETECTION

KEY FEATURES

Rapidly detect cyber threats and process anomalies

Quickly monitor ICS networks and processes with real-time insight

Significantly streamline troubleshooting and forensics

Efficiently implement a solution aligned with your environments

Easily share network monitoring data across multiple environments

"Cyber incidents are inevitable in today's world. It's our job to understand what is most important to the business and manage the risk. If an incident does happen, proper response is key in determining the level of impact it will have on your business. Now, as cyber threats against energy and other critical infrastructure industries continue to rise, our customers are asking for advanced solutions to monitor and detect cyber attacks against their OT networks."

Teresa Zielinski, SVP, CISO,
GE Power Security.

OVERVIEW

GE Vernova offers leading capabilities that have been proven to help power generators improve reliability, safety, cyber security, and operational efficiency in industrial control system (ICS) environments. Once deployed, the asset visibility solution from Nozomi Guardian* automatically discovers OT network topologies and connected devices. The solution develops security and process profiles and monitors systems in real time to detect anomalies and unexpected changes.

Our asset visibility solution offers this comprehensive blend of features:

- Multi-faceted capabilities for detecting ICS threats, employing behavioral analysis and artificial intelligence-powered risk assessment.
- Automatic discovery of **vendor agnostic** industrial assets and visibility into their vulnerabilities and cyber security risks.
- Continual monitoring of ICS networks and processes with real-time insights.
- Rapid, automated detection of cyber threats and process anomalies.
- Superior incident capture and tools that streamline troubleshooting and forensic efforts.
- Easy integration with existing IT and OT infrastructure.
- Enterprise-class scalability when deployed with the complementary Central Management Console from GE Vernova.

ADVANCED CAPABILITIES

Multi-faceted Threat Detection

- Behavior-based cyber threat and process anomaly detection
- Signature- and rule-based detection through the OT ThreatFeed service
- Faster and more accurate threat identification

Operational ICS Visibility

- Automated asset discovery
- Intuitive network visualization
- Real-time network monitoring

Superior Incident Response and Forensic Tools

- Dynamic learning reduces false- positive alerts
- Smart grouping of related alerts to provide visibility into attack paths
- Automatic full packet capture
- Time machine system snapshots for forensics
- Real-time, flexible query tool to help you find the information you need

ESSENTIAL CAPABILITIES FOR ICS CYBER SECURITY AND OPERATIONAL VISIBILITY

Asset Inventory and Network Visualization

With GE Vernova's asset visibility solution, you can improve system and process awareness with a visualization interface that shows all assets and links. The solution offers automated discovery of network assets, helping staff save time and gain up-to-date visibility. Using passive, non-intrusive deployment, the solution connects to network devices via Switch Port Analyzer (SPAN) or mirror ports. In addition, the solution triggers automated alerts when it detects anomalies and changes and offers views that make it easy to drill down on asset information.

Vulnerability Assessment

The solution automates the identification of device vulnerabilities, which means your team can save time and improve cyber resiliency.

Dashboards and Reporting

Featuring built-in and customizable dashboards, detailed reports, and ad-hoc querying capabilities, the solution provides intuitive, real-time visibility that improves both cyber security and operational efficiency.

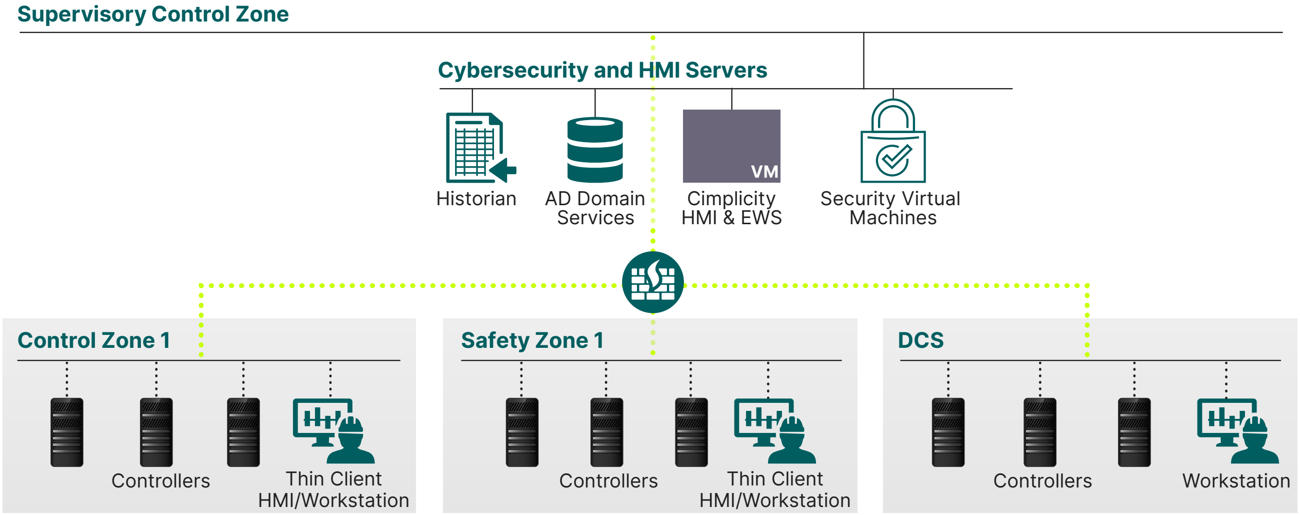
Anomaly and Threat Detection

GE Vernova's anomaly detection solution provides the advanced features that enable your team to rapidly detect cyber security threats, risks, and process anomalies. The solution switches from learning to protection mode automatically, helping speed anomaly detection. Once in protection mode, you'll be alerted to any changes in your environment. For example, the system can generate alerts if new assets connect to the network or changes are made in process variables.

The solution employs multi-faceted capabilities to identify threats through built-in behavior-based anomaly detection and contextual threat information from the OT ThreatFeed service. OT ThreatFeed is an additional subscription service that includes rules, signatures, and other indicators to help you detect new and emerging threats. With this complete ICS security solution, your team can detect:

- Malware, ransomware, and other malicious software
- Zero-day attacks
- Complex threats and attacks
- Man-in-the-middle attacks
- Brute-force and Distributed Denial-of-service (DDos) attacks
- Unauthorized behavior

SAMPLE DEPLOYMENT ARCHITECTURE



A representative deployment architecture

VALUE DELIVERED TO MULTINATIONAL OPERATORS

Operational Visibility

GE Vernova's asset visibility solution provides real-time visualization of network equipment and topology. The solution monitors assets, communications, and processes, and it presents actionable information in dashboards. With the solution, your users can do real-time querying of any aspect of network or ICS performance, reducing the need to work with spreadsheets.

Easy Integration with IT and OT Environments

The solution offers built-in integration with the following products:

- SIEMs, including HPE ArcSight, IBM QRadar, LogRhythm, and Splunk.
- Firewalls from such vendors as Cisco, Check Point, Fortinet, Palo Alto Networks, and more.
- User authentication directories, including Active Directory and LDAP.
- Ticketing systems, including ServiceNow for case management.
- Endpoint security tools, including antivirus and host intrusion detection systems.

The solution uses an open API to easily integrate with other IT and ICS tools in your environment. The solution includes built-in support for over 100 IT and OT protocols, with new ones being added regularly. Additionally, your team can use the Protocol SDK to add support for new and custom protocols. The solution makes it easy to export data for analysis and presentation in other applications, and it offers a number of customizable components that help you adapt the solution to your specific environment.

Realize Value Quickly

You can deploy the solution quickly, without making any disruptive network changes. With the solution, you can establish centralized monitoring of tens of thousands of industrial devices across multiple geographically dispersed sites.

BROAD SUPPORT FOR ICS VENDORS, ISC, AND IT PROTOCOLS

ICS Vendors

ABB, Allen-Bradley/Rockwell, Bristol Babcock, Beckhoff, Emerson, General Electric, Honeywell, IBM, Mitsubishi, Motorola, Rockwell Automation, Schneider Electric, Siemens, Yokogawa.

ICS Protocols

Aspentech Cim/IO, BACNet, Beckhoff ADS, BSAP IP, CEI 79-5/2-3, COTP, DNP3, Emerson DeltaV, Enron Modbus, EtherCAT, EtherNet/IP - CIP, Foundation Fieldbus, Foxboro IA, Generic MMS, Honeywell, IEC 60870-5-7 (IEC 62351-3 + IEC 62351-5), IEC 60870-5-104, IEC-61850 (MMS, GOOSE, SV), IEC DLMS/COSEM, ICCP, Modbus/RTU, Modbus/TCP, MQTT, OPC, PI-Connect, Profinet/DCP, Profinet/I-O CM, Profinet/RT, Sercos III, Siemens S7, Vnet/IP.

IT Protocols

ADS, ARP, ABB PGP2PGP, CIM I/O, BACNet, BROWSER, BSAP IP, Bittorrent, CC-LINK IE, CDP, COTP, CEI 76/3, CSP2, DCE-RPC, DNP3, DRDA (IBM DB2), DHCP, DHCPv6, DNS, Dropbox, Edonkey, Enron Modbus, EtherCAT, Ethernet/IP, Foundation Fieldbus, Foxboro IA, FTP, GE EGD, GE iFix 2 iFix, GE SRTP, GOOSE, GVCP, HoneywellExperion Read, HoneywellExperion Station to Server, HoneywellExperion DSA, HSRPv2, HTTP, ICMP/PING, IEC 60870-5-104, IEC 60870-5-7 (IEC 62351-3 + IEC 62351-5), IEC DLMS/COSEM, IGMP, IKE, Indigo Vision, Kongsberg Net/IO, Kerberos, LDAP, LLDP, LLMNR, MDNS, Mitsubishi Melsoft, Mitsubishi SLMP, MMS, MQTT, Modbus/TCP, Modbus/TCP - Schneider Unity extensions, MySQL, NTP, Netbios, OPC, OPC-UA, OSPF, TNS, PCCC, Physical Security, PTPv2, Profinet/DCP, Profinet/I-O CM, Profinet/RT, RDP, RNRP, ROC, RTCP, RTP, RTSP, S7, STPlus, SNMP, SSH, STP, SV, Sercos III, SMB, SQLServer, SSDP, Symantec Endpoint Manager, Syslog, TeamViewer, Telvent OASyS DNA, Triconex TSAA, Vnet/IP, ZMTP.

Support for additional systems and protocols is constantly being expanded. Visit www.nozominetworks.com/products/technical-specifications/ for the latest technical specifications. In addition, with the solution's Protocol SDK, your organization can quickly add support for additional protocols.

PRODUCTS

In addition to the physical appliance that provides real-time cyber security and operational visibility of industrial control networks. GE Vernova also offers a Central Management Console that aggregates data from multiple appliances, enabling centralized cyber security monitoring. Together, these products support comprehensive cyber resilience and reliability in ICS environments. An optional OT ThreatFeed subscription identifies threats present in the industrial network and generates correlated alerts combined with operational context in order to provide detailed insights.

GE VERNOVA

*Guardian is a trademark of Nozomi Networks Inc.

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.