SIEMENS



JOINT SOLUTION BRIEF

Visibility and threat detection **for industrial control systems**

Mitigate cybersecurity risks with an integrated solution from Siemens and Nozomi Networks for signature and anomaly-based threat detection for Operational Technology (OT) networks from a globally trusted expert in designing, building, and protecting industrial networks.

siemens.com/pharma-manufacturing

Introduction

A comprehensive solution for automated OT/IoT asset inventory and threat detection across industrial control system networks to enable rapid, intelligent responses to cyber incidents and improve cyber resilience

As OT and IT (Information Technology) networks are linked to improve operational efficiencies, the converged networks are under increased scrutiny to prevent malicious entities from launching attacks.

Advanced industrialized nations have responded by adopting regulations to protect critical infrastructure installations such as electric power, transportation, manufacturing, oil and gas operations, and other industrial facilities. Thus, operations managers must achieve effective, real-world cybersecurity and compliance with government mandates to protect business continuity. The focus of securing OT networks in Industrial Control Systems (ICS) differs fundamentally from securing IT networks.

IT networks, which have a long history of interconnection to local and wide area networks, are designed to facilitate periodic maintenance windows for security updates. OT networks, on the other hand, operate continuously and must be robust, predictable, and reliable when executing tasks with millisecond precision.

Moreover, cyberattacks on IT systems essentially have economic consequences, while those on critical infrastructure can also have environmental repercussions or even threaten public health and lives. The IEC 62443 standard recommends Defense-in-Depth, a risk-based, multi-layered security concept for industrial automation and control systems. This standard takes a risk-based approach to ensuring cybersecurity by addressing not only the technology that comprises a control system, but also the work processes, countermeasures, and employees. This includes establishing a security program with **physical security** to authorize access and ensure security of sensitive areas, **network security** for the ICS with DMZ (demilitarized zone), network segmentation, and data encryption, and finally, **system integrity** with system hardening to make OT networks resilient to cyberattacks.

> *"Protecting OT networks to ensure business continuity requires visibility, automation, and non-intrusive, cost-effective solutions with minimal footprint."*

One of the elements of establishing such a program is achieving real-time visibility throughout the network to detect threats and anomalies. Visibility can provide actionable insights to operations personnel responsible for preventing network disruptions. The Nozomi Networks Guardian™ application, hosted on the RUGGEDCOM APE1808 computing module, provides these functionalities and strengthens system integrity.

Solution description

Nozomi Networks Guardian™ deployed on the RUGGEDCOM APE1808 (Application Processing Engine) provides operational visibility and rapid detection of cyber threats for operational control centers and field station environments. Its automated discovery process maps the network topology, assets, connections, protocols, and SCADA/ICS commands. It monitors network behavior for risks and provides the information stakeholders need to respond quickly to prioritized threats. Nozomi Networks Threat Intelligence™ continuously updates Guardian™ appliances with rich data and analysis so you can detect and respond to emerging threats faster. Guardian™ correlates Threat Intelligence™ information with broader environmental behavior to deliver maximum security and operational insight.

This solution enables operational managers and security professionals to:

- **See** all OT and IoT assets and network behavior on a single dashboard
- **Detect** cyber risks, vulnerabilities, and anomalies for faster, targeted responses
- **Unify** security, visibility, and monitoring across all operational assets for improved resilience

The Nozomi Networks Guardian™ on the RUGGEDCOM APE 1808, which can monitor up to 1,000 nodes for a single remote site, together with either the Nozomi Central Management Console (on-premise, optionally pre-installed on a server platform) or Nozomi Vantage (SaaS) make up the integrated solution and include all the necessary licenses, setup, and activation support. This integrated solution can be further enhanced with optional subscriptions to Nozomi's Threat Intelligence, Threat Intelligence Expansion (powered by Mandiant), Asset Intelligence, Smart Polling, and Vantage IQ services.

RUGGEDCOM RX1500 series

The RUGGEDCOM RX1500 series of managed, modular switches and routers offers a utility-grade, multi-service platform certified for reliable communications for networks in harsh environments. These versatile devices ensure reliable operation between -40 °C (-40 °F) and +85° C (185° F) without fans or other moving parts. They demonstrate a high level of immunity to electromagnetic interference (EMI). They support VPN and firewall functions and ensure data security at the Local Area Network (LAN) level through passwords, PKI authentication, and strong encryption algorithms. They are typically used as the main entry point between the LAN and the WAN, forming a secure gateway to the Industrial Control System.

RUGGEDCOM APE1808

The RUGGEDCOM APE1808 is a powerful, industrial-grade application hosting platform, and a line module for the RUGGEDCOM Multi-Service Platform family of switches and routers. The APE1808 provides a standards-based platform for commercially available software applications and eliminates the complications and costs of installing an external industrial PC.

RUGGEDCOM APE1808 – specs at a glance



The APE1808 module, left, hosts the Guardian™ solution. It plugs into the RUGGEDCOM RX1500 Multi-Service Platform, right.

Ethernet ports	2 x Gigabit, RJ45 ports
USB ports	2 x USB 3.0
Processor	Intel Atom x5-E3940, 4 cores, x86_64
Display	Intel HD 500 (Display port)
RAM	8 GB DDR3 with ECC
Operating System	Debian Linux
Storage	80 GB eMMC

The Nozomi Networks Guardian™

The Nozomi Networks Guardian™ application enables comprehensive, automated asset discovery and inventory. Each asset's characteristics – manufacturer, model number, maintenance and security patch history, and current status – are displayed on an intuitive, easy-to-master user interface.

Nozomi Guardian™ "learns" the baseline behavior for each asset and the entire network using advanced machine learning algorithms. Once standard behavior patterns are established,it switches to a "protect" mode providing alerts for human operators, from routine maintenance to conditions requiring immediate intervention. Each Guardian™ license provides regular Threat Intelligence™ updates.

Nozomi Guardian's Anomaly Detection

Nozomi Guardian's Anomaly Detection provides non-intrusive, signatureless early warning notifications that may be undetectable by conventional IT security tools. These notifications incorporate user-defined policies and alerts to network vulnerabilities and cyber threats.

The Guardian™ Deep Packet Inspection (DPI)

examines data packets for protocol-specific commands (such as Step7, IEC 61850, Modbus, and other OT protocols) without slowing down network traffic. This passive implementation secures data communications between operational control centers and IT networks without sacrificing network efficiency or causing disruption.

Nozomi Guardian™ application can be further enhanced with subscriptions to Nozomi's Threat Intelligence™ and Asset Intelligence™ services.

- The Nozomi Threat Intelligence™ service delivers ongoing OT and IoT threat and vulnerability intelligence and reduces the mean-time-to-detection (MTTD) of cyberattacks.
- The Nozomi Asset Intelligence™ service delivers ongoing OT and IoT asset intelligence for faster and more accurate anomaly detection and reduces the mean-time-to-response (MTTR).

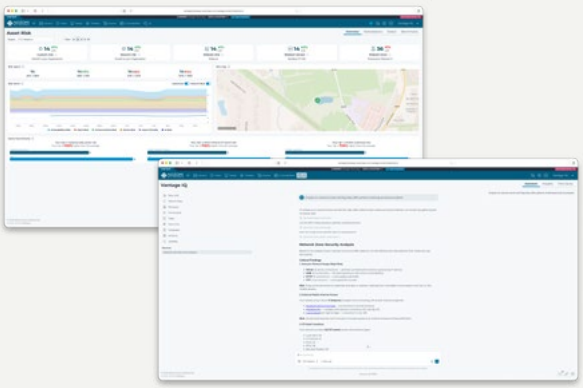
Additional cybersecurity software such as next-generation firewalls, intrusion prevention systems, and secure access management solutions can be pre-installed to complement Guardian™'s IDS and DPI applications or added on later.

Platform Management and OT Service Management

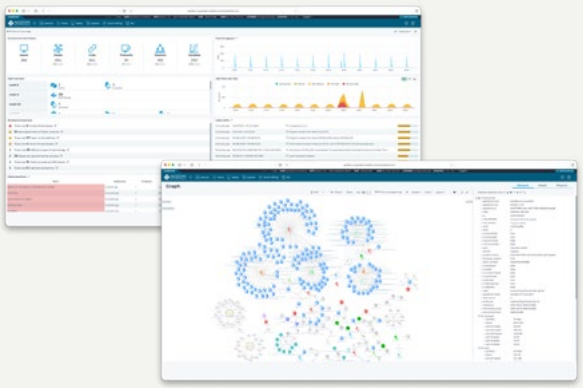
While Nozomi Guardian™ generates foundational asset and security data, deployments across systems and facilities can be centrally managed and extended with OT service management capabilities:

- Nozomi Central Management Console™ provides centralized, on-premises management of Guardian sensors across distributed sites, with aggregated visibility and unified sensor management for faster response and troubleshooting.
- Nozomi Vantage™ adds cloud-powered security at scale, AI-powered analytics, and asset-based risk scoring and prioritization to support a risk-based approach to OT security.
- Nozomi Compass is an OT-native asset and service management platform, unifying cyber-physical security and OT service management, built on deep first-party asset data.

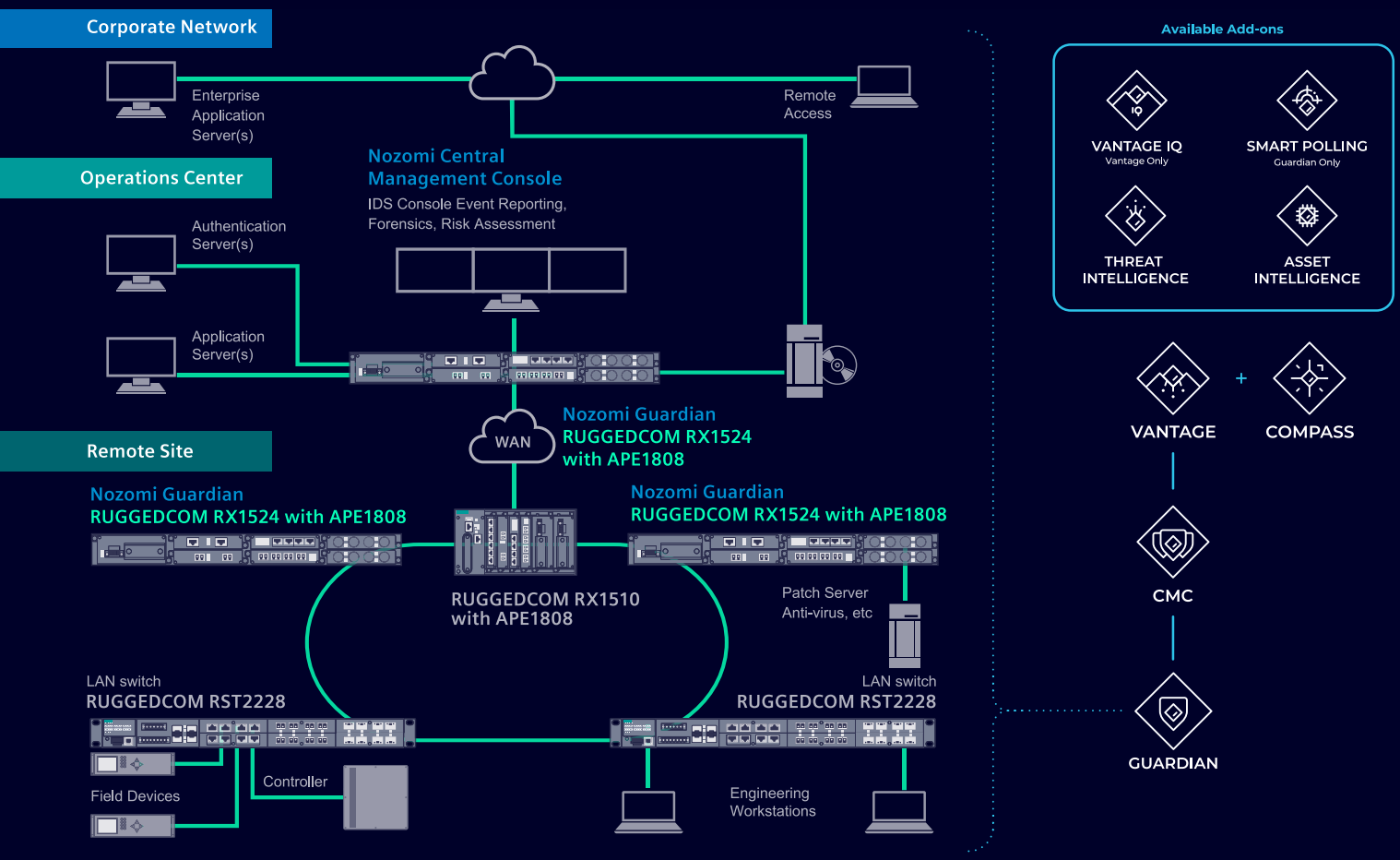
Nozomi Vantage™ centralizes risk management into a single application, providing asset-based risk scoring, AI-powered analytics, and distilled threat intelligence cards.



Nozomi Guardian™ collects foundational data for OT and IoT cybersecurity, including asset inventory updated in real-time, vulnerability registries, dynamic network visualization and advanced anomaly and threat detection.



Solution integration and architecture



The Nozomi Guardian™ solution deployed on the RUGGEDCOM APE1808 inventories assets, monitors network behavior, and sends prioritized, actionable intelligence on assets and threats to a central management console for stakeholders.

Typical applications

Automating OT/IoT asset inventory

Scenario

Distributed networks in electric power generation and smart grids, and remote installations in oil and gas control systems with large number of assets seeking an efficient method for complete visibility on their assets

Challenge

Creating and maintaining an accurate, detailed, and up-to-date inventory of OT/IoT network assets in large scale deployments has proven to be costly, time-consuming, technically daunting, and outside my organization's resources and expertise."

Solution

For legacy devices and brown-field installations, the integrated solution of a pre-installed Nozomi Guardian™ on the RUGGEDCOM APE1808 application processing engine deployed on the RX1500 Layer 3 Ethernet switch and router is a quick and cost-effective method to automate OT/IoT asset inventory.

The Nozomi Guardian™ solution automatically creates and maintains an up-to-date inventory of OT and IoT assets. Guardian™ identifies each asset by name, manufacturer, serial number, firmware version, and meta-properties such as site, IP address, and MAC address and monitors each asset's status, giving detailed information on every asset. It also maps the network's topology, including logical node subsystems such as circuit breakers and switches, measurement points, and PC operating systems, and installed software applications with their version numbers. Data from each remote installation can be aggregated and viewed at the central management console, giving a panel of glass view for the entire network.

Knowing OT network vulnerabilities as they are identified

Scenario

Known network vulnerabilities can be exploited by malicious entities to orchestrate cyberattacks. It is necessary to prioritize patch management in the ICS network to minimize the risk of business loss.

Challenge

> *"Knowing which vendors' IEDs, RTUs, PLCs, and other devices are at risk would help our organization prioritize our cybersecurity staff's time and resources."*

Solution

The integrated RUGGEDCOM/Guardian™ solution provides a real-time update of identified vulnerabilities from the National Vulnerability Database (NVD) operated by the National Institute of Standards and Technology (NIST) of the US government. It displays the asset/device vulnerabilities by vendor, their standardized name, description, severity score, and other variables on a dashboard. Furthermore, it also displays detailed troubleshooting and remediation support for each vulnerability, which helps to prioritize the deployment of patches throughout the OT environment.

Intrusion detection and mitigation on OT/IoT protocols and incidents

Scenario

Critical infrastructure networks such as electric power grids, rail, and ITS networks need to balance continued operations with cyber risk mitigation. However, non-malicious acts and human errors can sometimes have similar debilitating consequences as a malicious act.

Challenge

> *"If our organization could swiftly identify unintentional and accidental cyber incidents, we could reduce operational risks and prioritize our cybersecurity staff's time and resources."*

Solution

The integrated RUGGEDCOM/Guardian solution continuously learns the normal communication patterns of the ICS network, establishing a behavioral baseline of devices, protocols, and data flows. Once this baseline is established, Nozomi Guardian alerts on deviations from expected behavior—detecting subtle changes caused by non-malicious acts, misconfigurations, or human errors that signature-based tools alone would miss. This anomaly-based detection works in tandem with signature-based threat detection generated by Nozomi Threat Intelligence and Threat Intelligence Expansion (powered by Mandiant). STIX indicators, packet rules, and YARA rules identify suspicious indicators and malicious activity within network communications, OT/IoT protocol exchanges, and files. Generated alerts are then correlated with identified network devices and related alerts, giving OT system operators a comprehensive, real-time view of both suspicious and malicious activity occurring throughout the environment—so that operational disruptions, whether accidental or intentional, can be identified and addressed before they escalate into business loss.

Integrated solution benefits

- The integrated RUGGEDCOM/Guardian™ solution provides an end-to-end solution from a single source with a proven expertise in OT and cybersecurity
- The Guardian™ application for IDS and DPI is fully integrated prior to deployment and its installation and operation are non-intrusive with zero disruption to operations
- Rugged, modular hardware, ideal for harsh environments, lowers capex investment and contributes to maximum availability
- Scalability and flexibility of security functions with minimal hardware footprint due to the compact APE module
- User-friendly and intuitive interface reduces training expenses, lowering the total cost of ownership

Support

About Nozomi Networks

Nozomi Networks accelerates digital transformation by protecting the world's critical infrastructure, industrial, and government organizations from cyber threats. The solution delivers exceptional network and asset visibility, threat detection, and deep operational insights for OT and IoT environments. Customers rely on Nozomi Networks to minimize risks while maximizing resilience.

About RUGGEDCOM

RUGGEDCOM hardware and software products are part of the industrial communication portfolio. They provide a level of robustness and reliability that has set the standard for communications networks deployed in harsh environments. RUGGEDCOM devices offer proven reliability in extreme temperature ranges, Zero-Packet-Loss™ technology that ensures immunity to high levels of electromagnetic interference, and fault-tolerant topologies with HSR and PRP. RUGGEDCOM devices can be found in mission critical networks used in electric power, intelligent transportation, manufacturing, and oil and gas industries around the world.

For more information, please visit:
siemens.com/ruggedcom

Siemens AG
Process Industries and Drives
Process Automation
Postfach 48 48
90026 Nürnberg
Germany

Siemens Canada Limited
300 Applewood Crescent
Concord, Ontario, L4K 5C7
Canada

© Siemens AG 2026
Subject to change without prior notice

Security information
Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept.

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit: **siemens.com/industrialsecurity**

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under:
siemens.com/industrialsecurity

The information provided in this brochure contains descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice. All product designations may be trademarks or product names of Siemens AG or supplier companies whose use by third parties for their own purposes could violate the rights of the owners.