SOLUTION BRIEF

Fortinet and Nozomi Networks Comprehensive OT and CPS Security Solution

Broad, Integrated, Automated Security with Real-Time Cybersecurity and Visibility for Industrial Control Networks

Executive Summary

The backbone of critical infrastructure, cyber-physical systems (CPS), are ubiquitous across all industries, including energy, electric, water, manufacturing, and even military operations. In the last decade, CPS solutions have become increasingly automated and advanced as well as more interconnected with traditional IT and enterprise networks. While this growing connectivity has enhanced operational efficiency for utilities and governments, it has also exposed CPS networks—and the devices within them—to a broader range of cyber and operational threats.

The integration of common network protocols, alongside the cost efficiencies and accessibility of Windows-based terminals like human-machine interfaces (HMIs) and SCADA Masters, has brought operational technology (OT) networks into closer contact with traditional IT systems. This has also introduced new risks.

Two primary concerns dominate this transformation. First, CPS networks supporting critical infrastructure cannot afford unplanned downtime, whether due to cyberattacks, maintenance, or patching updates, leaving Windows-based terminals vulnerable. Second, the legacy technologies used in CPS lack native security features, such as basic authentication or encryption, rendering these systems prone to vulnerabilities.

The Challenges

CPS security incidents have become more frequent and increasingly severe, resulting in potentially catastrophic consequences such as loss of life, widespread outages, billions of dollars in lost revenue, and significant infrastructure damage. High-profile malware attacks, including Industroyer/Crash Override, WannaCry, BlackEnergy, and Stuxnet, have had devastating effects on critical infrastructure, causing operational disruption and financial losses. And this alarming trend is likely to grow.

The Fortinet-Nozomi Networks Joint Solution

The joint solution combines the Nozomi Networks Platform with Fortinet's extensive OT/CPS systems security technologies. The Nozomi Networks Guardian Sensor's nonintrusive OT protocol monitoring capabilities, with embedded artificial intelligence (AI), profile the behavior of industrial devices to detect anomalies in the CPS network in real time. The Nozomi Networks Platform works closely with the Fortinet FortiGate and FortiSIEM—part of the Fortinet Security Fabric—to respond and provide a secure gateway between the OT and IT networks. It also works with FortiNAC to enable customers to profile assets within the OT environment.

Solution Components

- Nozomi Networks Vantage, Central Management Console, Guardian, and Arc
- Fortinet FortiGate, FortiSwitch, FortiNAC, FortiManager, FortiAnalyzer, and FortiSIEM

Solution Benefits

- Fortinet Security Fabric and Nozomi Networks Guardian bridge the gap between IT and OT networks.
- Together, they enable the sophisticated detection of CPS security issues and proactive threat detection and remediation, combined with unprecedented visibility.
- The broad, integrated, and automated portfolio of Fortinet products, including FortiSwitch, FortiGate, FortiNAC, FortiManager, FortiAnalyzer, and FortiSIEM, supports environmentally and nonenvironmentally controlled facilities.

FORTINET FABRIC-READY

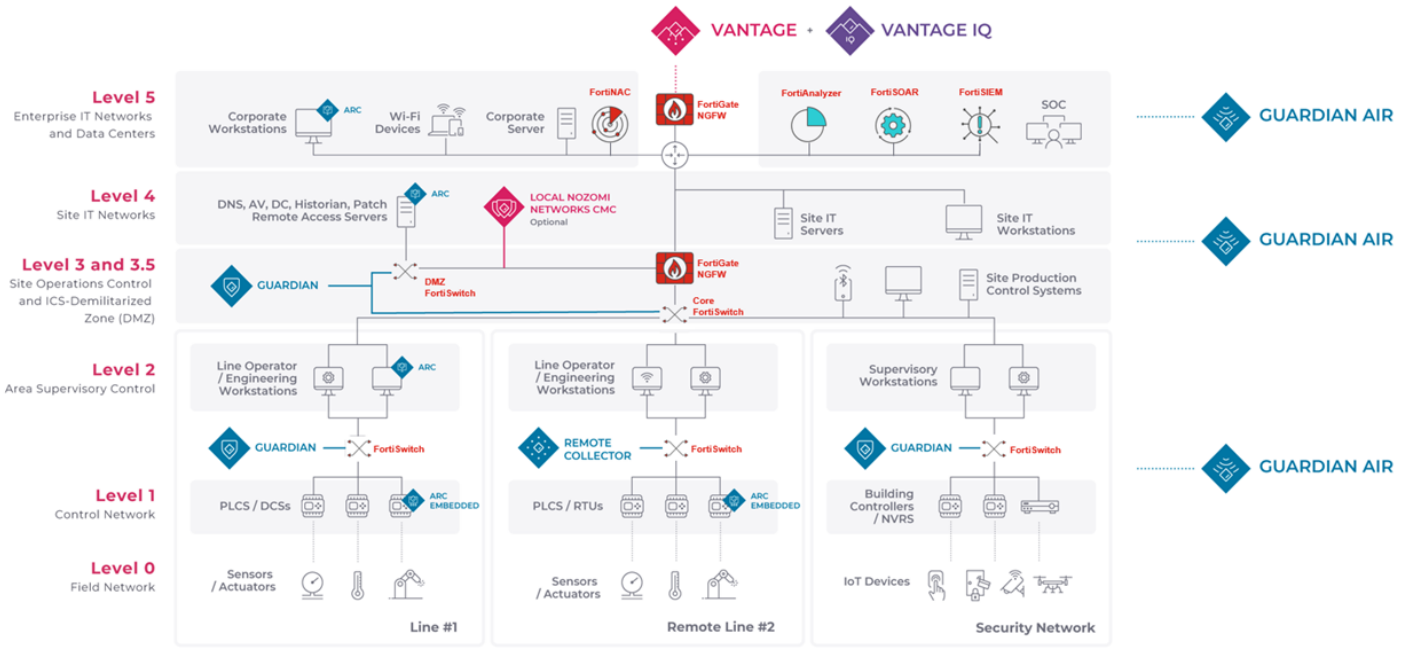

Figure 1: Tiered architectural approach for automated blocking of malicious traffic by Guardian in FortiGate

FortiGate integration leverages the passive monitoring of network traffic to create an internal representation of the entire network, including its nodes and the behavior of each device in the network. Once an anomaly or suspicious behavior is detected, an alarm is generated and sent to security operators and network administrators. Guardian can also automatically modify the corresponding policy in FortiGate to block the suspicious traffic. A tiered architectural approach is engaged to scale the solution deeper into a CPS network (Figure 1).

Fortinet FortiNAC for Full Asset Visibility and Access Control

Nozomi Networks is the leader in industrial cybersecurity, delivering a powerful solution for real-time visibility that enables organizations to manage cyber risk and improve resilience for their industrial operations. With one solution, customers gain advanced cybersecurity, improved operational reliability, and easy IT/OT integration. Innovating the use of artificial intelligence, Nozomi Networks helps the largest industrial facilities around the world "See and Secure" their critical industrial control networks by integrating with FortiNAC for policy enforcement. Today, Nozomi Networks supports over tens of millions devices in critical infrastructure, energy, manufacturing, mining, transportation, and utilities, making it possible to tackle the escalating cyber risks targeting operational networks.

Solution Benefits cont.

- Guardian protects the entire OT internal system and works in tandem with the Fortinet Security Fabric in quarantining and blocking malware.
- Designed to minimize system downtime and limit data loss, this joint solution optimizes productivity and business continuity in industries reliant on CPS networks.

FortiSIEM for Cross-Correlation Across IT and OT

By continuously monitoring data from CPS networks, this solution enables customers to obtain real-time intelligence about OT risk and correlate it with other threat information from their IT networks. Critical integration allows FortiSIEM to combine IT and OT data for complete visibility, providing security operations centers and incident responders with complete, comprehensive, and global access to alerts.

The Nozomi Networks solution prioritizes alerts based on risk by using a combination of machine learning and threat intelligence. The Fortinet security information and event management (FortiSIEM) solution combines this data with data collected from the IT network, providing visibility and automated response and remediation (ARR) in a single, scalable solution. Reducing the complexity of managing network and security operations and improving breach detection makes the integration of Nozomi Networks solutions with FortiSIEM highly valuable for today's organizations.

Fortinet Security Fabric and Nozomi Networks

With the adoption of standard IP networking, the typical CPS network follows usual networking conventions—which means it is relatively flat and open. The resulting lack of segmentation means that once a threat enters the system, it can move at will, increasing the amount of damage it can cause.

IT networks address this issue by segmenting their internal networks with firewalls, ensuring malware is contained to only a portion of the network. This same protection strategy can be applied to CPS networks by deploying FortiGate-Guardian pairs deeper into the CPS network, as shown in Figure 2. This scales the solution across the whole CPS network while providing a greater granularity of protection.

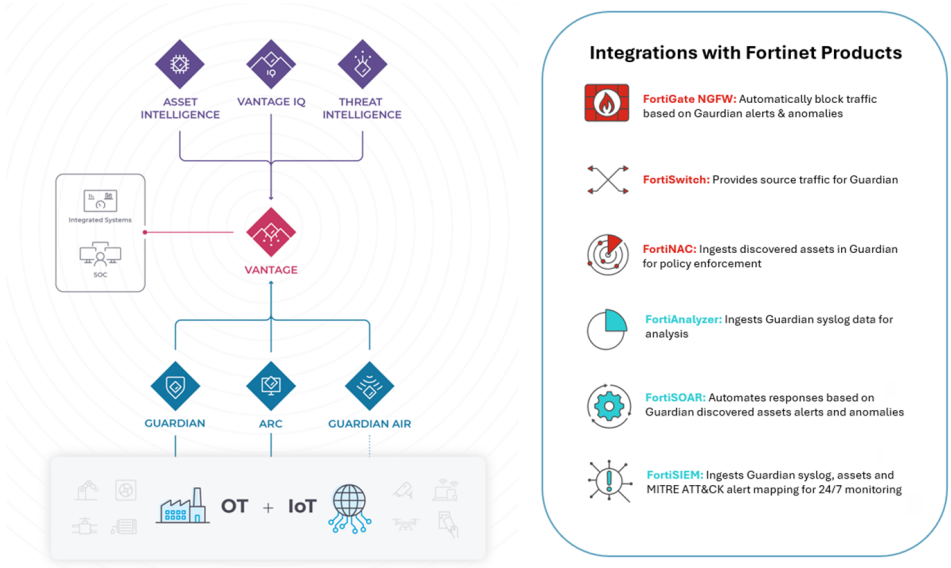

Figure 2: Granular security benefits of FortiGate-Guardian deployment

Solution Components

The Nozomi Networks Platform

Nozomi Networks' industrial cybersecurity solutions are designed to protect mission-critical environments across all industries and sectors, including today's OT and Internet-of-Things (IoT) physical devices and processes. Nozomi Networks uniquely combines network (wired and wireless) and endpoint visibility, threat detection, and AI-powered analysis for faster, more effective response.

The Nozomi Networks platform methodology revolves around the incident response life-cycle phases of visibility, detection, and response. It provides a wide range of components and form factors to flexibly deploy and scale on-premises and in the cloud, as well as a wide range of industrial and corporate environments. Solutions include:

- **Vantage:** A SaaS solution for unified security monitoring and risk management
- **Central Management Console (CMC):** Centralized visibility and management of Guardian sensors in distributed sites
- **Guardian:** Industrial strength sensors for comprehensive visibility and network monitoring; ANSSI-certified and FIPS-compliant
- **Arc:** Enhanced data collection and asset visibility across endpoint attack surfaces
- **Remote Collectors:** Low-resource sensors for offshore, remote, and distributed locations
- **Guardian Air:** A plug-and-play sensor for the visibility and monitoring of wirelessly connected assets

Fortinet Security Fabric

The Fortinet Security Fabric allows security to dynamically expand and adapt as more workloads and data are added. Security seamlessly follows and protects data, users, and applications as they move between IoT devices and cloud environments throughout the network. FortiGate Next-Generation Firewalls are the foundation of the Fortinet Security Fabric, expanding security via visibility and control by tightly integrating with other Fortinet security products and Fabric-Ready Partner solutions.

Use Cases

Once interconnected with a corporate network, CPS systems are exposed to the same potential cyberthreats and damage as regular IT security breaches. These often come with broad security implications or the potential for safety risks, even loss of life. For example, according to the Federal Office for Information Security in Germany, a targeted attack in 2014 on a steel mill using spear-phishing emails coupled with social engineering enabled access to the steel mill's IT network, leading the hackers to the OT network. The impact was an uncontrolled blast furnace shutdown, causing massive damage, downtime, and significant safety risks. Unplanned outages such as this minimally involve damages in the hundreds of thousands of dollars in equipment repair and typically escalate to hundreds of millions in lost revenue.

Fortinet and Nozomi Networks Bridge the Gap Between OT and IT

With the accelerating convergence of IT and OT environments, the combined intelligence provided by the integration of FortiSIEM, FortiNAC, FortiGate, and Nozomi Networks eliminates network blind spots while expanding FortiNAC automated threat response capabilities beyond traditional IT environments into OT.

This innovative integration not only strengthens security across IT and OT domains but also ensures seamless and continuous monitoring, reducing the risk of cyberattacks and operational downtime.

By combining Nozomi Networks' real-time cybersecurity and operational visibility with Fortinet's industrial security products, OT networks benefit from today's most comprehensive cybersecurity solution. This integrated approach empowers organizations to improve threat detection, accelerate incident response times, and strengthen overall cyber resilience.

About Nozomi Networks

Nozomi Networks is the leader in OT and IoT security for critical infrastructure. Our platform uniquely combines network and endpoint visibility, threat detection, and AI-powered analysis for fast, effective incident response. Customers around the world rely on us to minimize risk and complexity while maximizing operational resilience.

From day one, our solutions have been deeply rooted in addressing the complex requirements of industrial and critical infrastructure environments. As OT converges with the vastly different worlds of IT and IoT, that experience has given us a unique understanding of the tools and processes associated with the largest networks in the world. We've earned a global reputation for unmatched service, superior cyber and physical system visibility, advanced OT and IoT threat detection, and scalability across distributed environments.

We provide real-time asset visibility, threat detection, and actionable intelligence that keeps you in control of your critical infrastructure.

April 3, 2025 11:46 AM / MKTG-1216-0-0-EN