

Fortinet and Nozomi Comprehensive OT Security Solution

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

Business Drivers

The backbone of critical infrastructure, industrial control systems (ICS), is ubiquitous in all industries including energy, electric, water, manufacturing, and even military applications. In the last decade, ICS have grown to become more automated and advanced, but also more connected to conventional and enterprise networks than ever before. While this increase in connectivity has helped utilities and governments alike reach a higher level of efficiency, it has also exposed ICS networks, and their devices, to new cyber-borne and operational vulnerabilities.

The advantages of leveraging common Internet protocols, combined with the ease and cost saving of using Windows-based terminals such as HMIs and SCADA Masters brought operational technology (OT) networks on a collision course with traditional IT systems and associated security risks. Two key issues with this transformation prevail. First, ICS networks involved with critical infrastructure can't afford any unexpected outages—aka unplanned downtime—even for unscheduled maintenance or basic update patching, leaving the Windows-based terminals vulnerable. The second issue is that those serial protocols of ICS, which were merely encapsulated in TCP/IP, have no security features built into them, like basic authentication or encryption, again a fundamental vulnerability.

New Reality

ICS security incidents have increased in frequency with disastrous results including loss of life, major outages, billions in lost revenue, and large-scale infrastructure damage, and this trend is only likely to grow. Industroyer- Crash Override, WannaCry, BlackEnergy, and Stuxnet are examples of malware that have negatively impacted ICS with significant consequences.

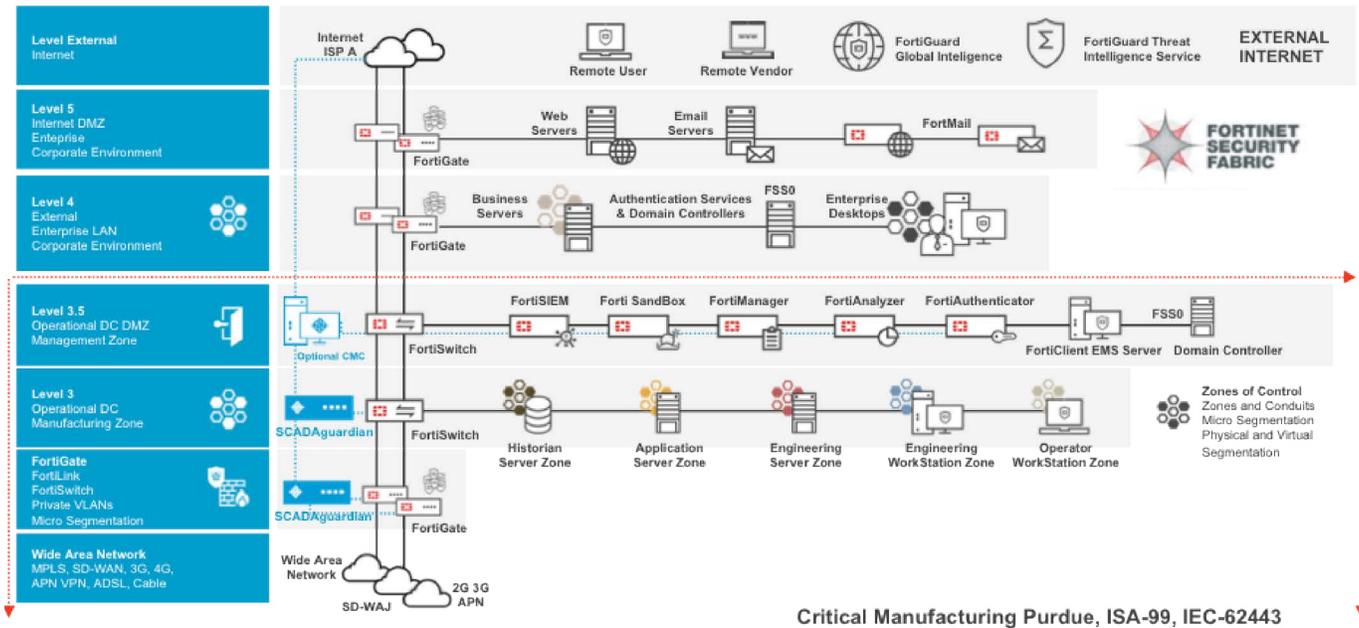
The Fortinet-Nozomi Networks Joint Solution

The joint solution combines Nozomi Networks' SCADAguardian with Fortinet's extensive security product for OT/ICS/SCADA Systems. SCADAguardian's non-intrusive ICS protocol monitoring capabilities with embedded artificial intelligence (AI) profile the behavior of industrial devices to detect anomalies in the ICS network in real time. It works closely with the Fortinet FortiGate and FortiSIEM as part of the Fortinet Security Fabric to respond and provide a secure gateway between the OT and IT networks.

Solution Benefits

- Fortinet's Security Fabric with Nozomi's SCADAguardian bridges the gap between IT and OT networks.
- Enables sophisticated detection of ICS security issues with proactive threat detection and remediation, combined with unprecedented visibility.
- Broad, Integrated, and Automated portfolio of Fortinet products for environmentally and nonenvironmentally controlled facilities, including the FortiSwitch, FortiGate, FortiManager, FortiAnalyzer, and FortiSIEM.
- SCADAguardian protects the entire OT inside system and works in tandem with Fortinet Security Fabric in quarantining and blocking malware.
- Designed to minimize system downtime and limit data loss, the joint solution optimizes productivity and business continuity in industries reliant on ICS networks.

SCADAguardian passively monitors network traffic to create an internal representation of the entire network, 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. At the same time, SCADAguardian can automatically modify the right policy in FortiGate to block the suspicious traffic. In order to scale the solution deeper into an ICS network, a tiered architectural approach is engaged (Figure 1).



Critical Manufacturing Purdue, ISA-99, IEC-62443

Fortinet Security Fabric and Nozomi Networks

With the adoption of standard IP networking, the typical ICS network follows normal networking conventions, which means that it is relatively flat and open. This lack of segmentation means that once a threat enters the system, it can move at will, increasing the amount of damage it can potentially cause. IT networks address this issue by using firewalls to segment their internal networks so that malware can be contained to only a portion of the network.

This same protection can be applied to ICS networks by deploying FortiGate-SCADAguardian pairs deeper into the ICS network, as shown in Figure 2, scaling the solution across the whole of the ICS network and providing a greater granularity of protection.

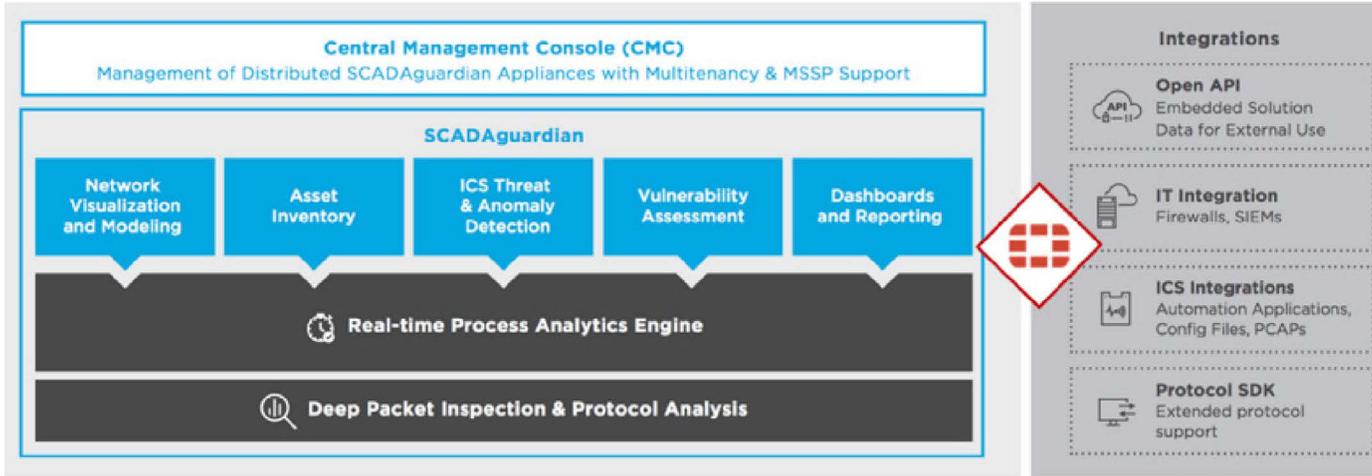


Figure 2: Granular Security Benefits of Fortigate/Scadaguardian Deployment

Use Cases

With Once interconnected with a corporate network, ICS are exposed to the same potential cyber threats and damage as regular IT security breaches. These often come with national security implications and/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 first enabled access to the steel mill's IT network, which then led the hackers to the OT network. The impact was an uncontrolled shutdown of a blast furnace, causing massive damage and downtime, along with significant safety risks. Unplanned outages minimally involve damages in the hundreds of thousands in equipment repair and typically escalate to hundreds of millions in lost revenue.

Components of the Joint Solution

The Nozomi Networks Solution

The Nozomi Networks Solution is comprised of the SCADAguardian appliance and the Central Management Console (CMC). SCADAguardian is a physical or virtual, passive appliance that provides real-time cybersecurity and operational visibility for industrial control networks. The CMC aggregates data from up to hundreds of facilities, providing high availability centralized and remote cybersecurity management. Together they deliver comprehensive OT visibility, cyber resilience, and reliability that extend visibility and intelligence deep into OT networks.

Fortinet FortiGate Enterprise Firewall

The Fortinet Enterprise Firewall Solution delivers end-to-end network security with one platform, one network security operating system, and unified policy management with a single pane of glass—for the industry's best protection against the most advanced security threats and targeted attacks. Innovative security processor (SPU) technology delivers high-performance application layer security services (NGFW, SSL inspection, and threat protection), coupled with the industry's fastest SSL inspection engine, to help protect against malware hiding in SSL/TLS encrypted traffic. The platform also leverages global threat intelligence of Fortinet FortiGuard Security Subscription Services to enable visibility and control for next-generation protection against advanced threats, including zero-day attacks.

Fortinet Security Fabric

The Fortinet Security Fabric allows security to dynamically expand and adapt as more and 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. FortiGates are the foundation of the Security Fabric, expanding security via visibility and control by tightly integrating with other Fortinet Security products and Fabric-Ready Partner solutions.

About Nozomi Networks

Nozomi Networks is the leader of industrial cybersecurity, delivering the best solution for real-time visibility to manage cyber risk and improve resilience for industrial operations. With one solution, customers gain advanced cybersecurity, improved operational reliability and easy IT/OT integration. Innovating the use of artificial intelligence, the company helps the largest industrial facilities around the world See and Secure™ their critical industrial control networks. Today Nozomi Networks supports over a quarter of a million devices in sectors such as critical infrastructure, energy, manufacturing, mining, transportation and utilities, making it possible to tackle escalating cyber risks to operational networks (OT).



www.fortinet.com

Copyright © 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

February 6, 2019 9:14 PM