SOLUTION BRIEF

Fortinet and Nozomi Networks 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) are 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 savings 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 Guardian with Fortinet's extensive security product for OT/ICS/SCADA systems. Guardian's nonintrusive 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. It also works with FortiNAC to enable customers to profile assets within the OT environment.

FortiGate integration 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

Solution Benefits

- Fortinet Security Fabric with Nozomi Networks Guardian 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, FortiNAC, FortiManager, FortiAnalyzer, and FortiSIEM.
- Guardian 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.

FORTINET FABRIC-READY

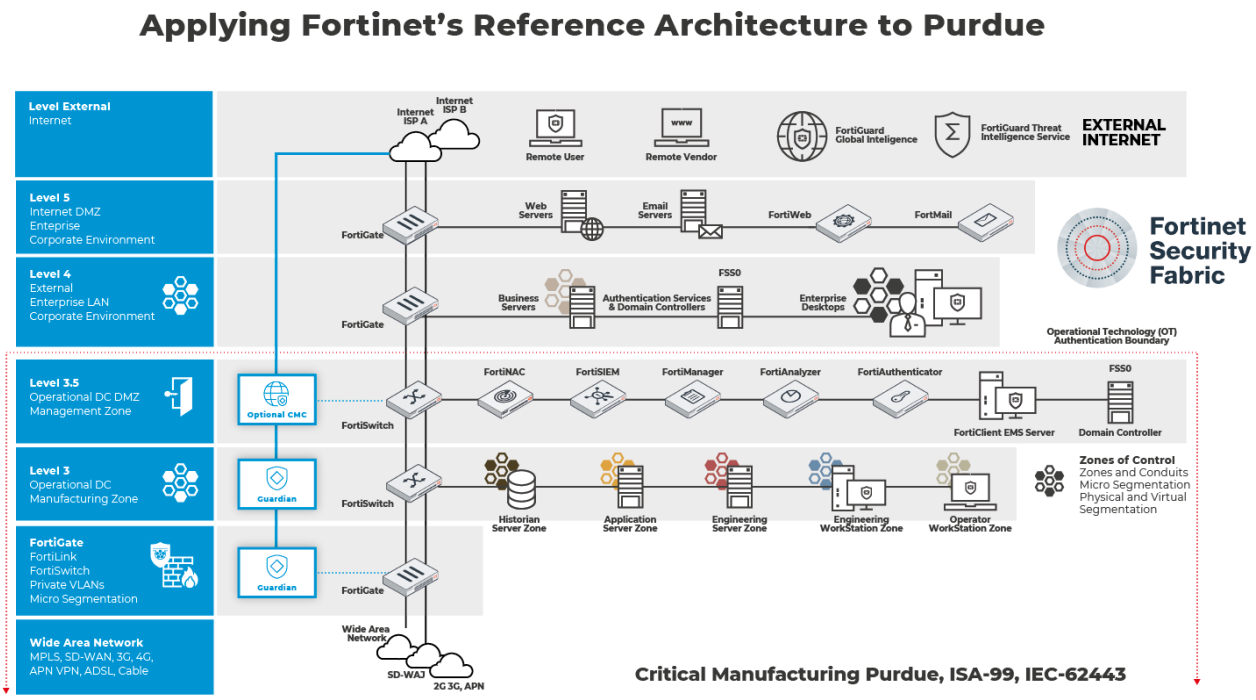

Figure 1: Tiered architectural approach for automated blocking of malicious traffic by Guardian in FortiGate.

generated and sent to security operators and network administrators. At the same time, Guardian 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).

Fortinet FortiNAC for Full Asset Visibility and Access Control

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).

FortiSIEM for Cross-correlation Across IT and OT

By continuously monitoring data from ICS networks, this integration enables customers to obtain real-time intelligence about OT risk and correlate it with other threat information from their IT networks.This integration allows FortiSIEM to unite IT and OT data for complete visibility that provide 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 (SIEM) solution combines this data with the data collected from the IT networks, providing customers with 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, we believe the integration with FortiSIEM will be valuable for customers.

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-Guardian 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.

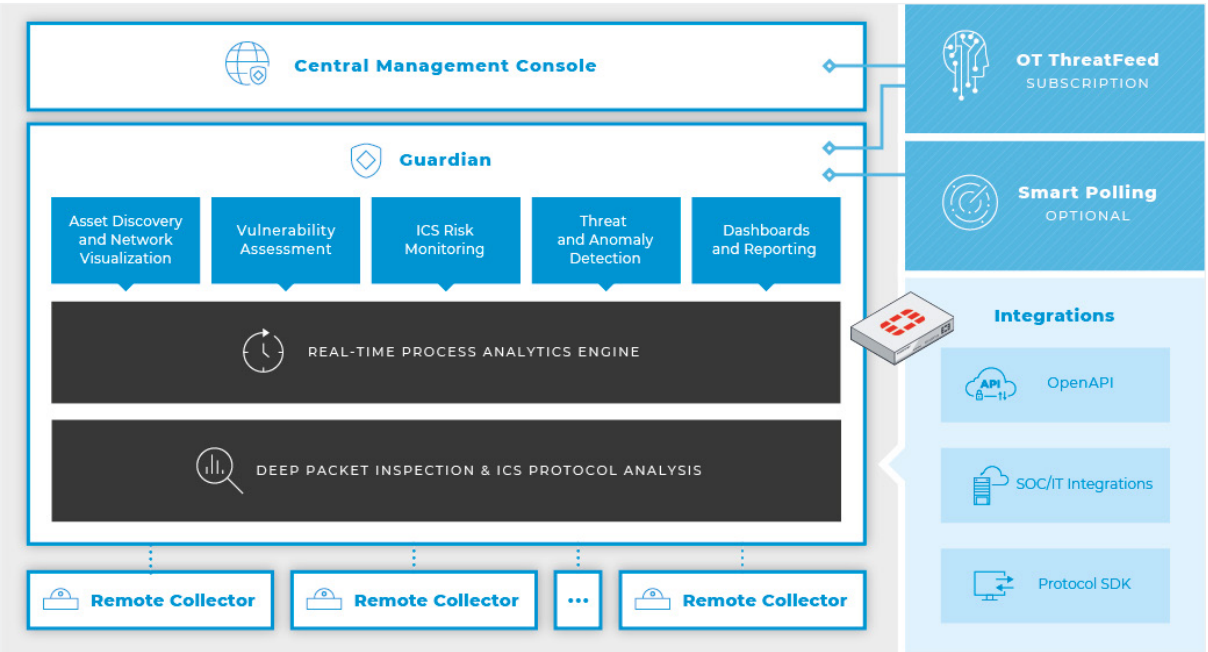

Figure 2: Granular security benefits of FortiGate/Guardian deployment.

Use Cases

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 Joint Solution

The Nozomi Networks Solution

The Nozomi Networks solution is comprised of the Guardian appliance and the Central Management Console (CMC). Guardian 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 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 Internet of Things (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.

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 and expands FortiNAC automated threat response capabilities beyond traditional IT environments into OT environments.

The innovative integration between the Nozomi Networks solution and Fortinet industrial security products provides OT networks with the most comprehensive cybersecurity solution available today.

About Nozomi Networks

Nozomi Networks is accelerating the pace of digital transformation by pioneering innovation for industrial cyber security and operational control. Leading the industry, we make it possible to tackle escalating cyber risks to operational networks. In a single solution, Nozomi Networks delivers OT visibility, threat detection and insight to thousands of the largest critical infrastructure, energy, manufacturing, mining, transportation and other industrial sites around the world.

May 21, 2021 4:04 PM

C:\Users\cyan\Documents\Creative Services - Misc\Document Edits\sb-fortinet-and-nozomi-networks-comprehensive-ot-security-solution\sb-fortinet-and-nozomi-networks-comprehensive-ot-security-solution-052121

478820-B-0-EN