SOLUTION BRIEF

OT Security Simplified and Unified with Fortinet

Executive Summary

Both operational technology (OT) and information technology (IT) environments need cybersecurity protection, but OT environments have unique characteristics that require different cybersecurity considerations. The Fortinet Security Fabric accommodates these unique OT characteristics while also enabling both OT and IT cybersecurity to be managed from a single pane of glass. In addition, the Security Fabric provides true integration and automation across an organization's security infrastructure, delivering unparalleled protection and visibility to every network segment, device, and appliance, whether virtual, in the cloud, or on-premises. It reduces complexity, especially compared to a model of using multiple point security solutions that often do not work together.

OT Presents Unique Challenges for Cybersecurity

To secure OT environments, organizations must address a number of unique challenges. These include:

- OT downtime from a security incident can cause hundreds of thousands or even millions of dollars in lost production and revenue.
- Similarly, shutting down certain OT systems for patching is virtually impossible due to revenue risk.
- New Internet-of-Things (IoT) devices in OT environments introduce new risks as well as new compliance requirements that must be tracked and reported.
- Integrating artificial intelligence (AI), machine learning (ML), or other IP-based elements of digital transformation (DX) in OT environments also introduces new risks.

Compared to IT security, OT security requires different thinking and a different approach—one that is viewed through the prism of efficiency, safety, and availability. With that in mind, plant operations and manufacturing leaders should look for a security approach that complies with the following characteristics:

Integrated Solutions Are Easier to Manage

Many organizations create a fragmented security architecture by acquiring different point security solutions that solve different OT security problems. There are many to choose from, and few work together. A U.S. Department of Energy National Laboratories study identifies 57 OT security solutions in seven categories.[1] Organizations can quickly end up with multiple tools managed from multiple consoles, producing security data that must be manually correlated, reconciled, and analyzed. This leads to security gaps and increased human errors.

The Fortinet Security Fabric delivers an average cost and productivity savings of 11.5% compared to an architectural approach that relies on separate point security products.

The Fortinet Security Fabric simplifies cybersecurity by integrating security solutions in a coordinated and open security platform (see Figure 1). The Security Fabric spans IT and OT environments and enables security elements to work together, sharing threat intelligence to detect and prevent advanced threats. The Security Fabric includes integrated threat intelligence from FortiGuard Labs on newly detected zero-day attacks, advanced threats, botnets, indicators of compromise (IOCs), and more.[2] It also includes fully integrated sandboxing—using FortiSandbox—for detecting and preventing unknown and zero-day threats.

This holistic approach to security, managing all environments through a single pane of glass, simplifies staff training and lowers total cost of ownership (TCO). This has been corroborated: a third-party assessment of the Fortinet Security Fabric finds it delivers, on average, 11.5% in cost and productivity savings compared to managing separate, best-of-breed point security solutions from multiple vendors over a six-year period.[3]

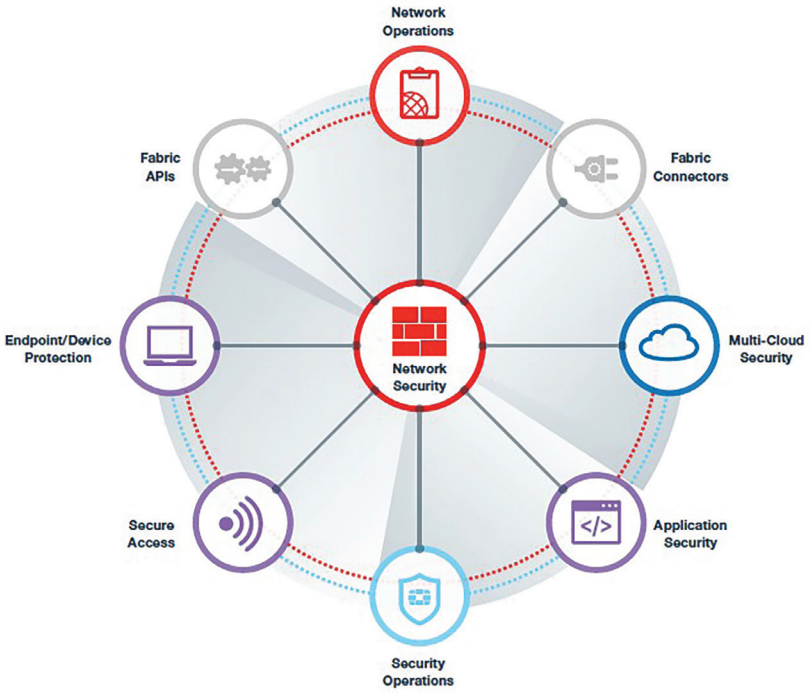

Figure 1: The Fortinet Security Fabric enables multiple security technologies to work seamlessly together, across all environments and supported by a single source of threat intelligence. This eliminates security gaps in the network and hastens responses to attacks and breaches.

Built to Accommodate OT Limitations

OT networks often include many trusted legacy devices such as programmable logic controllers (PLCs) that have proven themselves through long experience. However, they have unique characteristics that must be accommodated when securing them.

"Virtual patching" protects OT devices that cannot be patched otherwise.

For instance, PLCs and other OT elements cannot be actively scanned with the techniques used in IT network security. Here, the Security Fabric can passively scan network traffic and profile each OT network element and its status based on observed characteristics and behavior. It can also note the need for software updates to patch vulnerabilities.

But therein lies another challenge: Many OT elements cannot be patched. FortiGate next-generation firewalls (NGFWs) have a unique way of solving this challenge. FortiGate NGFWs use FortiGuard Industrial Security Services,[4] part of the FortiGate Enterprise Bundle[5] and 360 Bundle subscription services,[6] to receive updated signatures that enable the FortiGate NGFWs to identify and police the most common OT protocols. Using the signatures, the NGFWs can detect and block attempted exploits of known OT vulnerabilities (see Table 1). The result is "virtual patching" that safeguards legacy OT equipment.

Another OT limitation is that many OT devices cannot receive security client software. The FortiGate NGFW protects these elements without security client software by providing segmentation that separates them from critical data and applications. Segmentation also prevents the lateral spread of malicious exploits and enables organizations to quickly quarantine compromised devices. Further, the ability to control access to devices enhances compliance with regulations such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework in the U.S. or the Network and Information Systems (NIS) Directive in the EU.

Open Security Platform Integrates Many Legacy Solutions

The Fortinet Security Fabric includes prebuilt application programming interface (API) connections for more than 70 Security Fabric-Ready Partners. This ensures deep integration of many third-party solutions across all of the Security Fabric elements.[7]

Additionally, for security products that are not part of the Fabric-Ready Partner ecosystem, REST APIs and DevOps scripts make it easy and fast for customers to add them to the Security Fabric, sharing telemetry information and automating security provisioning, configuration, and response, among other functions.

OT Protocols	
BACnet	MMS
DNP3	Modbus
Elcom	OPC
EtherCAT	PROFINET
EtherNet/IP	S7
HART	SafetyNET
IEC 60870-5-104	Synchrophasor
IEC 60870-6 (TASE.2)/ICCP	MMS
IEC 61850	
LonTalk	

OT Applications and Vendors		
7-Technologies/ Schneider Electric	Honeywell	RealFlex
ABB	ICONICS	Rockwell Automation
Advantech	InduSoft	RSLogix
Broadwin	Intellicom	Siemens
CitectSCADA	Measuresoft	Sunway
CODESYS	MicroSys	TeeChart
Cogent	Moxa	VxWorks
DATAC	PcVue	Wellintech
Eaton	Progea	Yokogawa
GE	QNX	

Table 1: FortiGuard Industrial Security Services Sample OT Support.

To simplify connectivity, the Security Fabric can interact with and control switches and wireless APs from a variety of vendors. This includes 2,000 different models from more than 170 vendors such as Cisco, HP, and Ruckus.[8] In most instances, this enhances an organization's security posture while saving administrative time. It also protects existing investments by delaying the need to upgrade or replace devices.

Automated Intrusion Prevention, Detection, and Incident Response Processes

The different elements of the Fortinet Security Fabric work in unison with each other, including firewalls, email, endpoint security, sandboxing, switches, and wireless APs, to automatically identify malware, create and share signatures for its prevention, quarantine threats, or send alerts. Since today's threats move at machine speed by using AI and ML, security solutions must also move at machine speed to stop them.

When a threat is detected, the Security Fabric automates workflows that combine policy-based event triggers, response actions, and approvals to quickly contain the threat. Security incidents can be automatically passed to an information technology service management (ITSM) solution, with security analysts able to choose from a catalog of responses that can be implemented automatically from a central location. These capabilities reduce response times to minutes rather than days, allowing limited security staff to focus on expert-level decision-making rather than monitoring and information routing.[9]

Automated Compliance and Audit Tracking and Reporting

Preparing for audits traditionally involves gathering data from different security solutions and manually correlating and analyzing it. This work is painstaking and typically diverts multiple members of the security team from performing far more vital tasks. Here, FortiManager and FortiAnalyzer save valuable staff time by automating compliance tracking and reporting required by industry regulations and security standards.

The Security Fabric reduces response times to minutes rather than days or often weeks.

The Security Rating Service provides a single score reflecting overall security posture as well as specific areas in need of remediation.

Advanced compliance capabilities include hundreds of prebuilt, ready-to-use reports that are easy to schedule, along with more than 400 charts and 35 templates for report customization. In addition, FortiAnalyzer offers an automated, in-depth analysis of security operations to determine the scope of risk in the attack surface and then identify where immediate response is required. This capability also informs the Fortinet Security Rating Service, which provides a dashboard with a single view of an organization's overall security posture, as compared with peer organizations and accepted security standards. Part of the FortiGate Enterprise Bundle[10] and 360 Bundle subscription services,[11] the Fortinet Security Rating Service is an easy way to keep executive management and the board of directors informed about high-level trends in a consumable format (see Figure 2).[12]

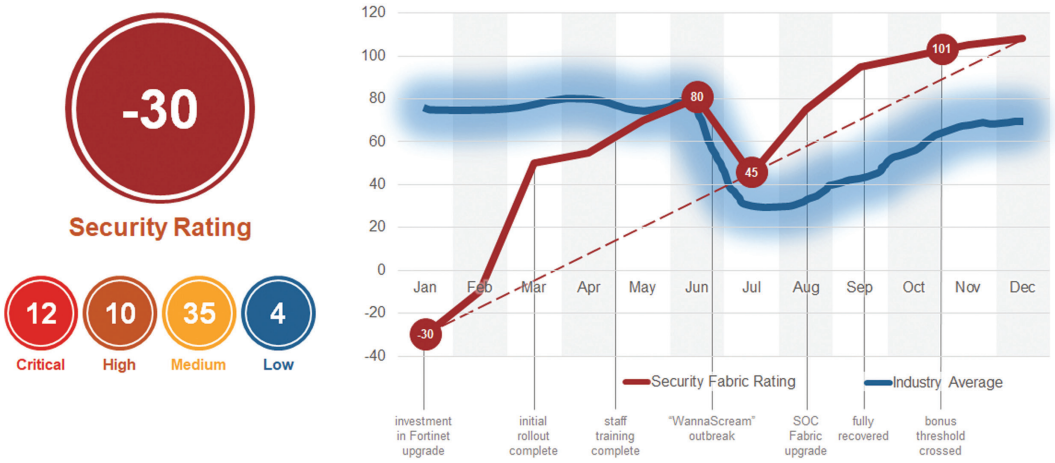

Figure 2: Fortinet Security Rating Service. Track both a point-in-time and trend analysis of your environment's security posture, compared with industry averages, using the Fortinet Security Rating Service.

Unify Cybersecurity to Minimize Complexity and Risk

With the Fortinet Security Fabric, organizations can integrate their OT and IT cybersecurity with an approach that accommodates the unique challenges of OT networks. Built around a unified OS, an open API-driven architecture, and single-pane-of-glass management, the Security Fabric allows organizations to more effectively collect, correlate, share, and respond to critical threat intelligence. This security approach reduces risk while enabling security teams to do more with less.

Additionally, when security elements work as an integrated ecosystem, organizations can immediately identify, isolate, and remediate affected devices anywhere in the network, automatically find and remove malware, and orchestrate security policy updates everywhere—from OT to IT and from IoT devices to the cloud. At the same time, complexity is reduced and security and compliance are enhanced. This is important, for as OT organizations embrace digital transformation such as IoT sensors, AI, ML, and big data, they can do so with assurance that these assets are protected.

[1] Carl M. Hurd and Michael V. McCarty, "A Survey of Security Tools for the Industrial Control System Environment," Idaho National Laboratory, U.S. Department of Energy, June 12, 2017.

[2] "FortiGuard Labs," Fortinet, accessed March 22, 2019.

[3] Zeus Kerravala, "How to Enable Digital Transformation and Improve ROI with Fortinet Security Fabric," ZK Research, February 2018.

[4] "Industrial Control Systems," Fortinet, accessed March 25, 2019.

[5] "Comprehensive Security with the FortiGate Enterprise Protection Bundle," Fortinet, January 21, 2019.

[6] "360 Protection Bundle: Delivering Real-Time Network Management, Comprehensive Security and Operational Services, and Advanced Support," Fortinet, March 26, 2019.

[7] "Technology Alliances," Fortinet, accessed April 21, 2019.

[8] "FortiNAC: Network Access Control," Fortinet, accessed April 27, 2019.

[9] "Purpose-built Integrated NOC-SOC Management and Analytics," Fortinet, September 11, 2018.

[10] "Comprehensive Security with the FortiGate Enterprise Protection Bundle," Fortinet, January 21, 2019.

[11] "360 Protection Bundle: Delivering Real-Time Network Management, Comprehensive Security and Operational Services, and Advanced Support," Fortinet, March 26, 2019.

[12] "Proactive, Actionable Risk Management with the Fortinet Security Rating Service," Fortinet, April 5, 2019.

FORTINET

www.fortinet.com

June 5, 2019 3:34 PM

392073-0-0-EN

D:\Fortinet\Work\2019\June\060519\Task 2\sb-plant-operations-ot-security-selection-complexity