WHITE PAPER

# Mitigating OT Cyber Risk With the Fortinet Security Fabric

## Strategies for OT Cybersecurity Leaders

## Executive Summary

Digital transformation (DX) is accelerating operational technology (OT)* and information technology (IT) convergence and driving businesses forward. Organizations leverage digital technologies such as Internet of Things (IoT), cloud computing, artificial intelligence (AI), and others to optimize operations, improve safety and reliability, and gain a competitive edge. However, despite the many benefits, both the convergence of OT and IT and the increased implementation of digital technologies have expanded the OT attack surface and increased its vulnerability to cyber threats.

How then can organizations mitigate OT cyber risk? The answer is with the Fortinet Security Fabric, a transformative and unique security architecture. The Security Fabric integrates best-in-class security solutions to provide broad visibility across both the OT and IT attack surface, while automating operations and providing continuous trust assessments. Following five cybersecurity best practices can strengthen the OT cybersecurity posture and components of the Security Fabric map to each of them. In this way, the Fortinet Security Fabric can serve as a secure foundation for converging IT and OT environments.

A complimentary threat assessment helps identify and prioritize risk.

*OT is synonymous with industrial control systems (ICS). "OT" was coined as a term to contrast with IT, because OT protocols, vendors, and use cases are distinct. Supervisory control and data acquisition (SCADA) systems are an element of OT. SCADA systems use graphical user interfaces for high-level supervisory management of OT/ICS processes.

## Cybersecurity Designed by Fortinet for Converging OT/IT Networks

As organizations adapt their IT and OT infrastructure to account for convergence and DX, they must also undergo a security transformation to protect against evolving cyber threats. Fortinet provides a proactive and transformative approach to cybersecurity, the Fortinet Security Fabric, as shown in Figure 1. The Security Fabric delivers:

- Broad visibility of the entire OT and IT attack surface for coordinated threat detection and policy enforcement
- Integrated and unified security, operations, and performance across different technologies, locations, and deployments for complete visibility
- Automated operations and response by AI and machine learning (ML) to deliver near-real-time, user-to-application coordinated protection across the Security Fabric

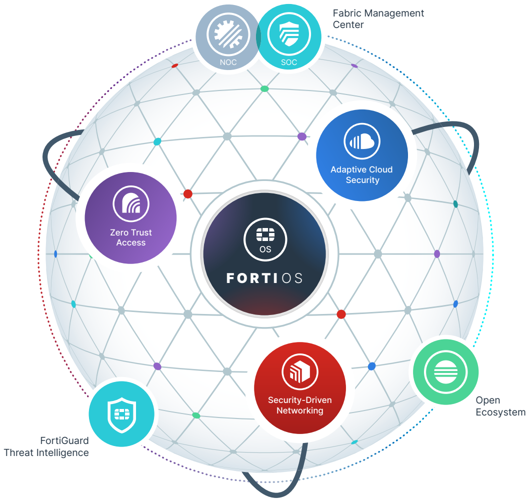

Figure 1: Powered by FortiOS, the Fortinet Security Fabric enables multiple technologies to work together across OT and IT environments. With a rich open ecosystem, the Security Fabric spans the extended digital attack surface and cycle, enabling self-healing security and networking to protect devices, data, and applications.

## Recommended OT Cybersecurity Best Practices

Deploying the Security Fabric is a journey to a desired state that provides visibility, integration, automation, and resilience in a security environment. The Security Fabric can be achieved in stages that align with organizational security priorities. As an organization plans those stages, it is wise to incorporate the following best practices.

**Network segmentation restricts an attacker's ability to move within and between networks.**

### 1. Identify Assets, Classify, and Prioritize Value

For a CISO seeking to improve their organization's OT security posture, the first step is to obtain an up-to-date inventory of the devices and applications running on their network. Fortinet can provide this inventory with a complimentary Fortinet Cyber Threat Assessment, which is available to qualified customers. It begins by using a FortiGate next-generation firewall (NGFW) or FortiNAC network access control (NAC) solution to passively observe network traffic. This passive traffic analysis is then used to identify and profile devices based on their characteristics and behavior. The resulting report:

- Notes high-risk applications
- Detects and identifies top exploits of application vulnerabilities
- Assesses the risk value of each asset
- Identifies indications of malware, botnets, and devices that may be compromised
- Categorizes applications and analyzes their network usage

CISOs can work with Fortinet to use this information as the basis for optimizing a security plan.

### 2. Segment the Network

In many OT breaches, attackers move laterally within and between IT and OT networks, but network segmentation restricts this movement. It is a fundamental best practice for securing OT as described in ISA/IEC-62443 (formerly ISA-99) security standards.[1]

Segmentation divides the network into a series of functional segments or "zones" (which may include subzones or microsegments), and "conduits" (channels between zones). A **FortiGate internal segmentation firewall (ISFW)** defines and enforces the zones and conduits using **Fortinet intent-based segmentation**. This approach continuously monitors the trust level of users, devices, and applications and dynamically controls their access based on business intent, behavior, and risk. By dramatically shrinking the attack surface in this way, it becomes more difficult for intruders to find vulnerabilities and exploit them.

### 3. Analyze and Protect Traffic Against Threats and Vulnerabilities

It is valuable to analyze network traffic to identify and block threats. Fortinet management and analytics integrates information from the following sources:

**FortiSIEM** (security information and event management) automatically discovers everything attached to a network and builds a configuration management database (CMDB). It also builds an auditable traffic record used for proactive risk mitigation and demonstration of compliance with regulatory and security standards.

**FortiManager** provides a dashboard view showing up-to-the-minute Security Fabric status, as well as a unified perspective that serves both security operations center (SOC) and network operations center (NOC) teams. SOC teams can see the scope of security alerts and issues, and the NOC team can see if any performance degradations are the result of a security incident. With this insight, the operations team is more likely to understand and readily consent to security team requests to reconfigure or quarantine assets.

**FortiAnalyzer** automates log management and real-time threat analysis. It leverages an indicators of compromise (IOCs) service from FortiGuard Labs consisting of a daily package of approximately 500,000 IOCs gleaned from a variety of sources around the globe. This information helps to identify any communications with servers that have been shown to be malicious. FortiAnalyzer can also provide quantified risk scoring, both internally over time and against similar organizations, through the FortiGuard Security Rating Service.

In addition to the above, Fortinet management and analytics leverages FortiGate NGFWs to inspect traffic to protect against malicious files, applications, and exploits.

**FortiGate NGFWs** use **FortiGuard Industrial Security Services**, which is part of the FortiGate Enterprise Bundle and 360 Bundle subscription services, for updated signatures that enable them to identify and police the most common OT protocols, as well as detect and block attempted exploits of known OT vulnerabilities (see Table 1). Blocking known exploits is especially critical in OT environments where equipment is routinely run without patches or updates of firmware.

To detect threats and enforce policies, FortiGate NGFWs scan encrypted secure sockets layer (SSL)/transport layer security (TLS) traffic. According to FortiGuard Labs, the total percentage of encrypted web traffic is now around 85%, so inspection of encrypted traffic is nonnegotiable.[2] Unlike other firewall solutions that experience dramatic performance impact, FortiGate NGFWs use purpose-built security processors (SPUs) to minimize performance degradation. So, organizations can avoid retrofitting and adding more appliances to their firewall infrastructure, whether in the data center or on the edges of the network.

| OT Protocols | | OT Applications and Vendors | | |
|---|---|---|---|---|
| BACnet | MMS | 7-Technologies/ Schneider Electric | Honeywell | RealFlex |
| DNP3 | Modbus | ABB | ICONICS | Rockwell Automation |
| Elcom | OPC | Advantech | InduSoft | RSLogix |
| EtherCAT | PROFINET | Broadwin | intellicom | Siemens |
| EtherNet/IP | S7 | CitectSCADA | Measuresoft | Sunway |
| HART | SafetyNET | CODESYS | Microsys | TeeChart |
| IEC 60870-5-104 | Synchrophasor | Cogent | Moxa | VxWorks |
| IEC 60870-6 (TASE.2)/ICCP | MMS | DATAC | PcVue | Wellintech |
| IEC 61850 | | Eaton | Progea | Yokogawa |
| LonTalk | | GE | QNX | |

Table 1: FortiGuard Industrial Security Services.

Other Security Fabric elements that analyze traffic and protect against threats include:

The **FortiMail** email gateway mitigates threats, such as spear phishing, a tactic often used in OT breaches to steal credentials. OT organizations report that malware and phishing are the most common intrusions.[3] FortiMail can also be set to pass suspected but unknown threats to **FortiSandbox**, which analyzes actions and can identify threats before they are delivered to the end-user. FortiSandbox can also accept potential threats from other access points (APs) such as endpoints, the network, cloud deployments, and file shares. Because FortiSandbox is fully integrated into the Security Fabric, it automatically shares threat intelligence in real time across all of the security elements.

**FortiDeceptor** uses decoys to divert and analyze threat activity and share information across the Security Fabric. **FortiIsolator** is a browser isolation solution that creates a visual air gap between user browsers and websites. It displays web content in a remote, disposable container, which isolates any malware threat.

### 4. Control Access by Users and Devices

The Security Fabric controls the ability of users and devices to access the network by coordinating capabilities from the following:

**FortiGate NGFWs** can be used to create user and device groups and enforce security policies for each of them. Different controls, for instance, can be set for local users compared to remote users.

**FortiAuthenticator** validates user identity and applies granular control of user access to each zone and conduit. It identifies users, queries access permissions from third-party systems, and communicates this information to FortiGate devices so they can enforce identity-based policies.

**FortiToken** further validates identity with multi-factor authentication (MFA). By combining user credentials with a hardware or software token or a fingerprint or other biometric, MFA makes using stolen credentials much more difficult.

Multi-factor authentication makes the use of stolen credentials, a frequent OT breach tactic, much more difficult.

**FortiNAC** authenticates devices attached to the network by observing their characteristics. Once profiled, FortiNAC can apply policies to devices to control if and how they connect to the network and to what segments of the network they have access. FortiNAC can also lock down ports as desired. No devices or applications are allowed until they are permitted. A port will not provide network connectivity until the connecting device is authorized. FortiNAC can enforce a policy that any device added to an OT network must first be approved by authorized staff.

**FortiClient** integrates with FortiGate NGFWs to provide visibility into endpoint devices in OT environments and to trigger vulnerability alerts.

### 5. Secure Both Wired and Wireless Access

In many types of OT environments, exposure to potential attacks through wired and wireless APs is growing. DX is often driving this increased risk. Some manufacturing plants and warehouses, for example, use automated guided vehicles (AGVs), which are wirelessly connected as they move goods and materials. Deploying wireless or IoT increases the attack surface, including connections to OT networks.

To minimize risk, security teams should centrally administer wired and wireless access from one interface. Through a FortiGate NGFW, they can push firewall capabilities and policies to ports on **FortiSwitches** and **FortiAPs** throughout the organization using proprietary, secure, encrypted tunnels.

Security teams can also use FortiNAC to centrally configure third-party switches and wireless APs, including up to 2,000 network devices from 170 vendors.

Ruggedized FortiSwitches, FortiAPs, and FortiGate NGFWs are designed for the shock, vibration, dust, moisture, and extreme temperatures found in OT environments—from offshore oil rigs, to shipping containers, to factory floors.

## Increasing OT Security

OT technologies were developed in the early 20th century, many decades before the rise of IT. Traditionally, OT and IT networks were separated by an air gap. Now, the two are being integrated to increase business value. Integrating IT and OT increases the digital attack surface, but with the right controls and technologies in place, CISOs protect their OT environments by:

1. Gaining broad visibility of the attack surface
2. Segmenting the network to limit the impact of any intrusion
3. Analyzing traffic, including encrypted traffic and common OT protocols, to protect against threats
4. Controlling access by users and devices and enforcing identity-based policies with continuous trust assessment
5. Securing both wired and wireless access and centrally administering controls from one interface

The Fortinet Security Fabric joins IT and OT security solutions through a common operating system called FortiOS. It provides broad visibility into the entire attack surface, integrated AI-driven breach prevention, and automated operations, orchestration, and response. Achieving its full reality and benefits can be accomplished in stages that are aligned with organizational security priorities and starts with a complimentary threat assessment that prioritizes risks.

[1] "ISA Standards: Numerical Order," International Society of Automation, accessed January 3, 2018.

[2] Nirav Shah, "Keeping Up With the Performance Demands of Encrypted Web Traffic," Fortinet, August 4, 2020.

[3] "2021 State of Operational Technology and Cybersecurity Report," Fortinet, May 26, 2021.

June 10, 2021 10:35 PM
1080552-0-0-EN