FERTINET

SOLUTION BRIEF

Securing Cyber-Physical Systems with the Fortinet OT Security Platform

Executive Summary

Cybercriminals increasingly target cyber-physical systems in the manufacturing and utilities industries, leading to production losses and business interruptions. Because of the increased risk, operational technology (OT) security has been elevated to the corporate level. CISOs are especially concerned with adding or updating the security of OT environments where the facility previously operated in isolation or was "air gapped" from other systems.[1]

The Fortinet OT Security Platform is a comprehensive system designed to protect OT environments. This platform includes secure networking, zero trust support, security operations solutions, dedicated threat intelligence, and a far-reaching and inclusive technology alliance ecosystem. All of these solutions are fully integrated to enable vendor consolidation and centralized management, simplifying operations and enhancing network security while reducing the total cost of ownership.

The Fortinet OT Security Platform was identified as the Sole Leader in the Westlands Advisory 2023 IT/OT Network Protection Platforms Navigator.[2]

The Need for OT-Specific Solutions

The CISOs and security teams responsible for managing and securing OT environments face several unique challenges, including selecting and managing an often unwieldy number of vendors. Setting up security in such a complex OT environment while simultaneously addressing operational priorities, such as personnel safety and production reliability, can be difficult. But today, many organizations are also tackling vendor consolidation, the convergence of IT and OT solutions, and the optimization of scarce cybersecurity personnel. To address these challenges, CISOs ideally need an OT security platform to provide unified connectivity, segmentation, zero-trust support, and security operations solutions that integrate seamlessly with their existing solutions.

The Fortinet OT Security Platform is a full suite of industrial network and security solutions, from initial connectivity to advanced zero-trust and OT security operations solutions.

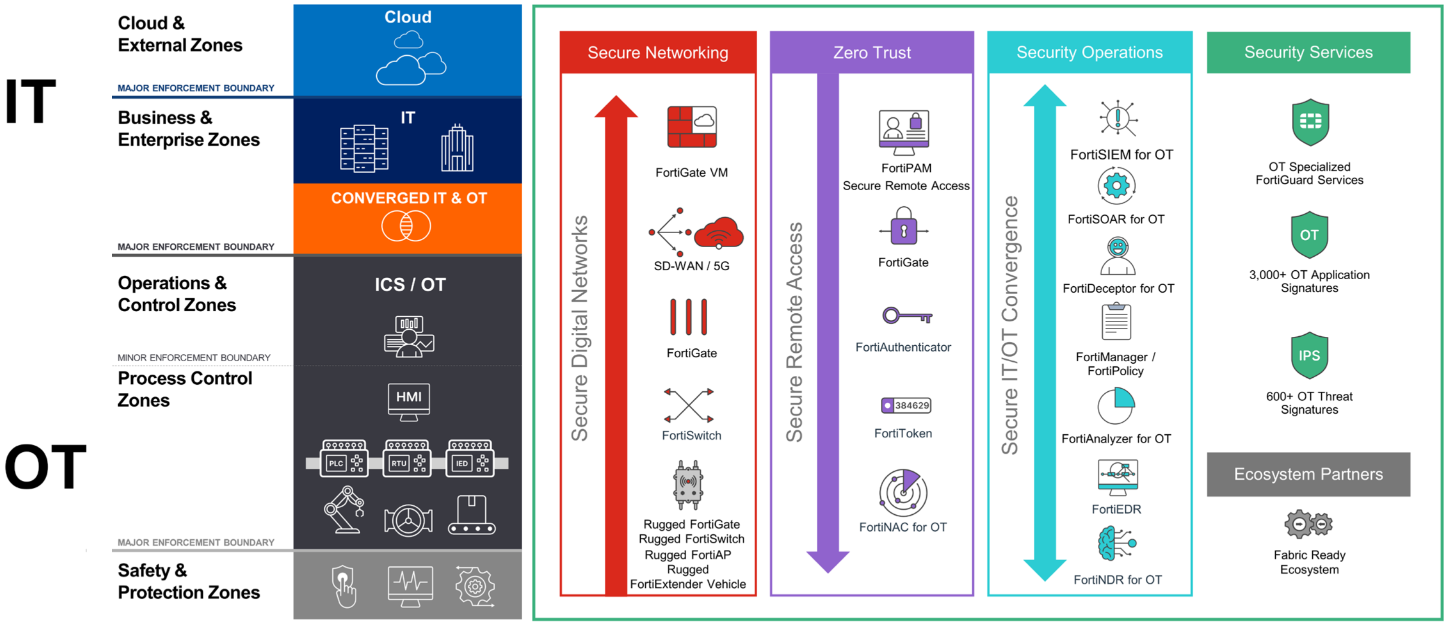

Figure 1: The Fortinet OT Security Platform

Connect and Protect OT Environments with Secure Networking

The Fortinet OT Security Platform provides initial connectivity to cyber-physical systems using the FortiGate Next-Generation Firewall (NGFW) with follow-on segmentation provided by the Fortinet FortiSwitch. These critical connectivity solutions have been specially designed for OT environments, including ruggedized hardware and advanced OT security services.

The OT Security Platform also addresses other common challenges faced by security teams. OT systems and devices often go unpatched because of the lack of vendor patches or competing production priorities, so implementing proactive security measures is imperative. The OT Security Platform provides security controls for OT applications and protocols, network segmentation and microsegmentation for OT networks, and vulnerability management controls such as virtual patching.

In addition to enabling asset and network visibility, the OT Security Platform includes the Fortinet OT Security Service, which provides vulnerability protection for OT applications and protocols from major ICS manufacturers. Updated signatures and vulnerability protection data allow the FortiGate NGFW to detect attempted exploits of known OT system vulnerabilities. The OT Security Service includes over 70 industrial automation and control system protocols and uses a list of over 19,000 vulnerability signatures, with more than 600 of them focused explicitly on OT security and powered by the FortiGate intrusion detection system engine.

Because many OT devices and systems run without patches, the ability to catch exploits and prevent attacks through virtual patching or vulnerability shielding is invaluable. The Fortinet OT Security Platform offers the following capabilities:

- Security control and policy enforcement using the FortiGate NGFW
- Complete user and device visibility and control in the network and support for network microsegmentation using FortiSwitch
- Centralized monitoring, logging, and reporting for FortiGate appliances deployed across IT and OT using FortiAnalyzer
- Centralized device management and security policy implementation for FortiGate appliances across IT and OT using FortiManager
- Real-time, up-to-date, actionable information and mitigation measures for threats, vulnerabilities, and zero-day exploits from FortiGuard Labs

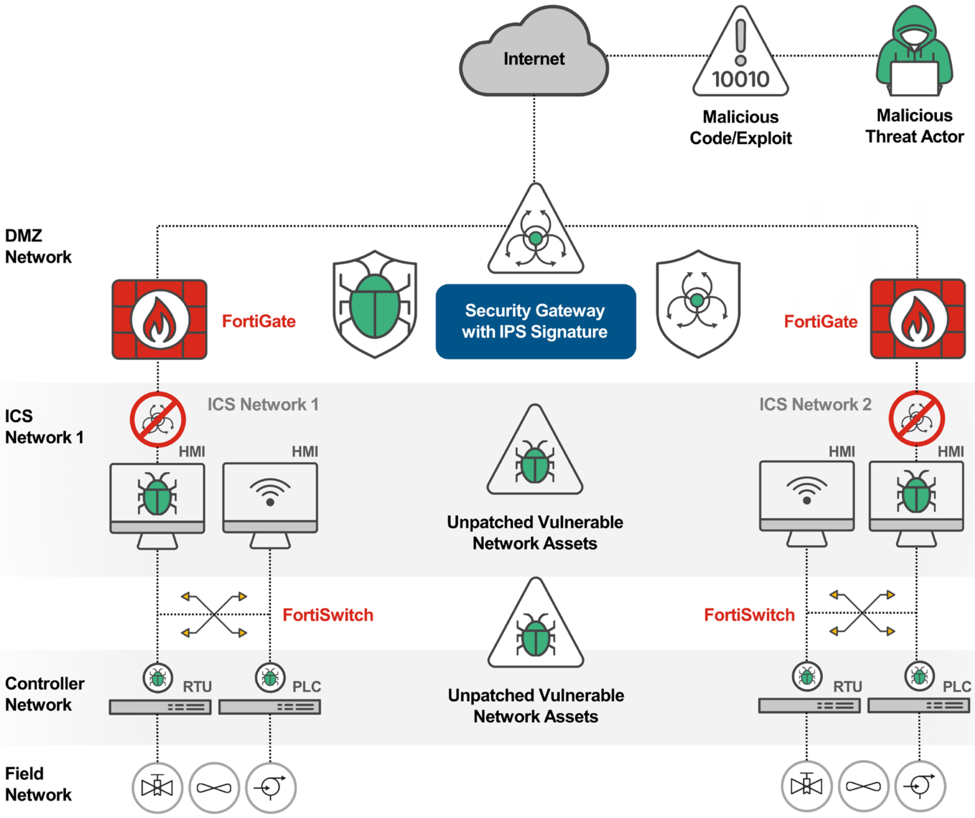

Figure 2: Virtual patching in ICS/OT networks

Zero-Trust Solutions for OT

Extending a zero-trust strategy into OT networks can be challenging because of competing operational priorities, the sensitivity of critical ICS networks and devices, and a lack of OT-specific zero-trust solutions. The OT Security Platform includes secure remote access (SRA), privileged access management (PAM), and network access control (NAC) to help you overcome these challenges.

While powerful individually, these solutions also work together to validate who and what is connecting to the OT network, limiting access to only those appropriate resources based on the device's or user's roles. Fortinet zero-trust solutions then securely connect users to applications no matter where the user is located or where the application is hosted.

NAC selectively grants user access to applications and identifies and secures IT, OT, and Industrial Internet of Things (IIoT). Asset owners and operators also gain complete visibility into and control over anything connected to the network. FortiPAM, FortiAuthenticator, and FortiToken identity and access management solutions work together to restrict access to only authorized users. At the same time, FortiGate segmentation further enhances zero-trust access by dividing IT/OT networks according to business needs. The Fortinet zero-trust solutions include:

- FortiGate NGFW provides security control and policy enforcement.
- FortiNAC offers visibility, control, and automated response for everything connected to the network.
- FortiToken provides two-factor authentication with a one-time password (OTP) application, push notifications, or a hardware time-based OTP token.
- FortiAuthenticator enables single sign-on and user authorization that identifies users, queries access permissions from third-party systems, and communicates access requests to the FortiGate NGFW to implement identity-based security policies.
- FortiPAM offers identity and privileged access management capabilities, enabling zero-trust security implementation for critical assets. It controls user access to critical applications and systems, monitors and tracks user activity, and allows secure remote access to critical assets.

Gartner stated: "As organizations look to simplify operations, vendors are consolidating platforms around one or more major cybersecurity domains. For example, identity security services may be offered through a common platform that combines governance, privileged access, and access management features. Security and risk management leaders must continuously inventory security controls to understand where overlaps exist and reduce the redundancy through consolidated platforms."[3]

Improving OT Security with OT-Specific Security Operations

Using an OT-specific platform makes it possible to integrate multiple data sources, speeding up time to detection and making it possible to automate security responses. Fortinet Security Operations solutions are customized for OT security requirements. They includes asset identification and network communication with a topology map referencing the Purdue model, MITRE ATT&CK for ICS matrix, and risk and compliance reporting.

IT and OT teams also need to balance security needs with operational priorities. When mitigating risk, remediation actions may have to be deferred to the OT security or operational teams to ensure production and services are not disrupted. The ultimate goal is to optimize a converged IT/OT security operations center that leverages threat intelligence, analytics, threat detection, deception or honeypots, incident response, threat hunting, and governance and compliance that will not disrupt the OT environment. To achieve this, Fortinet Security Operations solutions include:

- FortiGate NGFW provides security control and policy enforcement.
- FortiEDR offers real-time, automated endpoint threat detection and protection, orchestrated incident response, and forensics.
- FortiSIEM ingests and analyzes log data from IT and OT systems and correlates threat actor behavior that spans both environments. FortiSIEM can also show threat activity in the MITRE ATT&CK framework for enterprise IT and ICS environments.
- FortiSOAR is a customizable security operations platform that provides automated playbooks, incident triaging, and real-time remediation so OT enterprises can identify, defend, and counter attacks.

- FortiDeceptor provides honeypot deployments to deceive, expose, and eliminate external and internal threats before significant damage can be done.
- FortiNDR offers network detection and response (NDR) capabilities powered by artificial intelligence and artificial neural networks to provide sub-second investigation. It harnesses deep-learning technologies that assist SOC analysts with automated responses to remediate different breeds of attacks. To do this, FortiNDR includes a Virtual Security Analyst that rapidly identifies, classifies, and responds to threats.
- Security Operations Center-as-a-Service (SOCaaS) is a cloud-based managed security monitoring service that analyzes security events generated from FortiGate NGFWs and other security products. It performs alert triage and escalates confirmed threat notifications.
- FortiRecon digital risk protection (DRP) is a SaaS-based service that combines three powerful modules: external attack surface management, brand protection, and adversary-centric intelligence. FortiRecon provides a view of what adversaries are seeing, doing, and planning to help counter attacks at the reconnaissance phase and significantly reduce the risk, time, and costs of later-stage threat mitigation.

Support Consolidation and Convergence with the OT Security Platform

Securing cyber-physical systems is a complex technical challenge that is often difficult because of competing operational priorities. Securing OT environments starts with securely connecting OT networks to the rest of the enterprise, often for the first time, to implementing a fully functional OT security operations center. At the same time, many OT organizations are looking to optimize operations through vendor consolidation and the convergence of their IT and OT resources. The Fortinet OT Security Platform addresses these challenges through its OT-specific network connectivity, zero-trust support, and SecOps solutions. For CISOs responsible for OT security, the Fortinet OT Security Platform provides the flexibility and solutions they need to secure their industrial environments.

[1] Fortinet 2023 State of OT and Cybersecurity Report.

[2] Fortinet Named Sole Leader in 2023 IT/OT Network Protection Platforms Navigator™ Report, July 27, 2023.

[3] Gartner, Gartner Identifies the Top Cybersecurity Trends for 2023, April 12, 2023.

December 8, 2023 5:37 PM
2436831-0-0-EN