SOLUTION BRIEF

Securing Cyber-Physical Systems with the Fortinet OT Security Platform

Executive Summary

Cybercriminals increasingly target cyber-physical systems (CPS) in the operational technology (OT) and critical infrastructure sectors, leading to production losses and business interruptions, and threats to the stability of critical infrastructure.[1] Because of the increased risk, OT security has been elevated to the corporate level, with 60% of organizations planning to move OT security under the CISO in the next twelve months.[2]

The Fortinet OT Security Platform is the most comprehensive portfolio of OT security solutions designed to secure OT environments. This security platform includes secure networking, security service edge (SSE), security operations solutions (OT SecOps), dedicated threat intelligence, and a far-reaching and expansive technology alliance ecosystem. All these solutions are fully integrated to enable vendor consolidation, centralized management, and IT/OT convergence, simplifying operations and enhancing network security while reducing the total cost of ownership.

> **OT**
>
> The Fortinet OT Security Platform was identified as the Sole Leader in the Westlands Advisory 2023 IT/OT Network Protection Platforms Navigator.[3]

The Need for OT-Specific Solutions

The CISOs, CIOs, and network security teams responsible for managing and securing OT environments face several unique challenges, including selecting and managing an often unwieldy number of OT security 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 employ an integrated platform to tackle vendor consolidation, the convergence of IT and OT technologies, and the optimization of scarce cybersecurity personnel. To address these challenges, CISOs ideally need an OT security platform to provide unified connectivity, segmentation, SSE, and OT SecOps solutions that integrate seamlessly with their existing solutions.

The Fortinet OT Security Platform is a full suite of network and security solutions designed specifically for OT, from initial connectivity to advanced SSE and OT SecOps solutions.
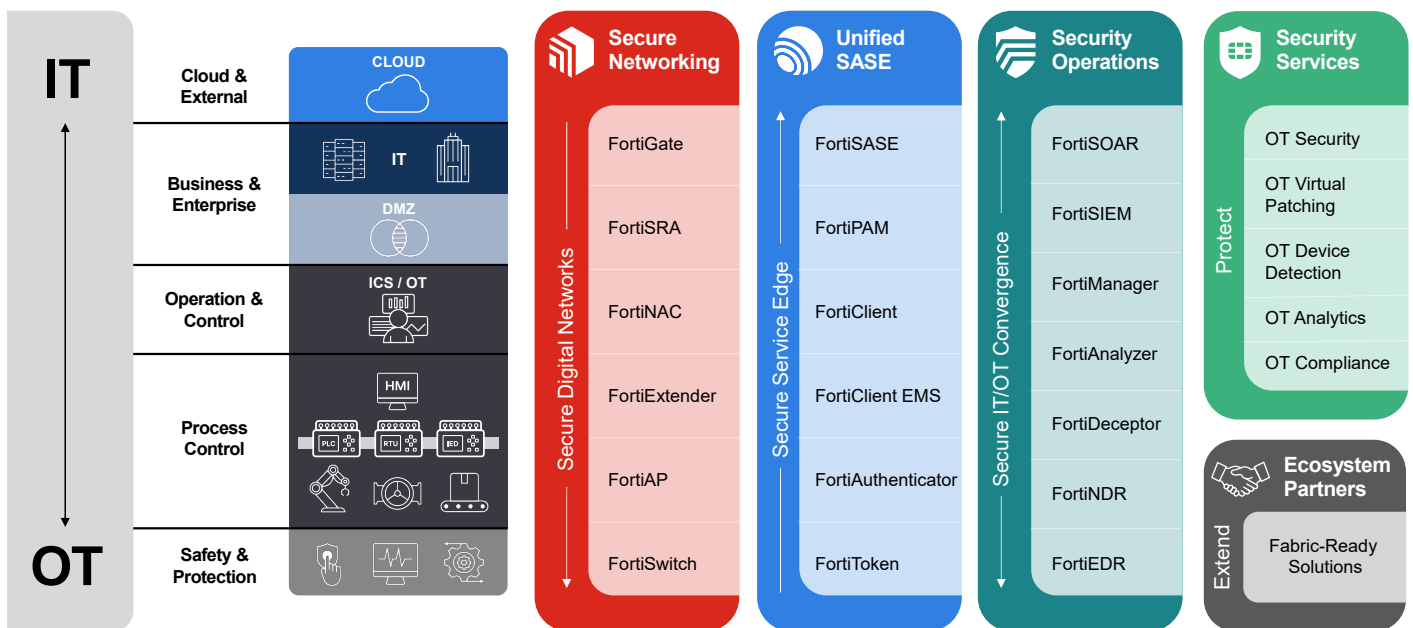

Figure 1: The Fortinet OT Security Platform

Connect and Protect OT Environments with Secure Networking

The Fortinet OT Security Platform provides initial connectivity to CPS using the FortiGate Next-Generation Firewall (NGFW) with follow-on segmentation provided by the Fortinet FortiSwitch. Secure remote access to resource-constrained OT networks and devices is provided by the FortiSRA secure remote access solution. These critical connectivity and access solutions have been specifically designed for OT environments, including ruggedized hardware and advanced AI-based 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 or compensating controls 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 a virtual patching engine. This engine also includes over 1,000 virtual patch rules to immediately protect unpatched vulnerable OT devices.

In addition to enabling asset and network visibility, the OT Security Platform includes the FortiGuard OT Security Service, which provides vulnerability protection for OT applications and protocols from major industrial control system (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 80 industrial automation and control system protocols and uses a list of over 18,000 vulnerability signatures, with more than 4,000 of them focused explicitly on OT security and powered by the FortiGate intrusion prevention 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 with or without FortiSwitch

- Centralized monitoring, logging, and reporting with FortiAnalyzer for FortiGate appliances deployed across IT and OT

- Centralized device management and security policy implementation with FortiManager for FortiGate appliances across IT and OT

- Real-time, up-to-date, actionable information and mitigation measures for threats, vulnerabilities, and zero-day exploits from FortiGuard Labs
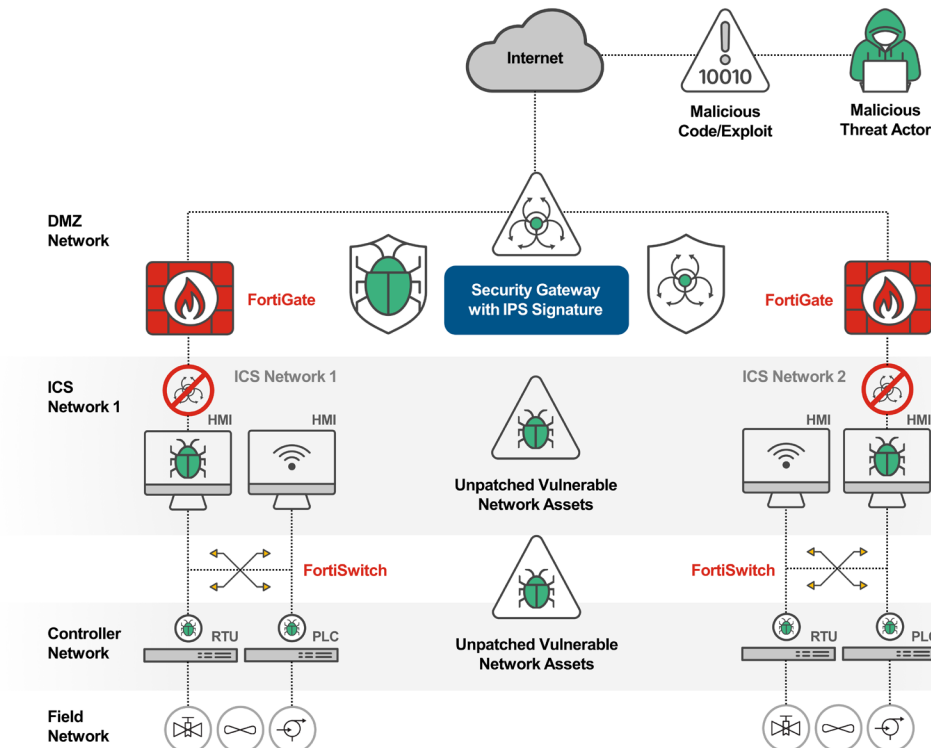

Figure 2: Virtual patching in ICS/OT networks

SSE Solutions for OT

Extending an SSE 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 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 SSE 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. FortiSRA enables secure remote access to support remote third-party contractors, auditors, and employees, protecting critical OT systems against threats from remote access and untrusted networks.

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 SSE solutions include:

- FortiGate NGFW provides security control and policy enforcement.

- FortiNAC offers visibility, control, and automated response for everything connected to the network.

- FortiSRA provides agentless, secure remote access for OT environments.

- 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 states: "Overall interest in CPS security (and particularly OT security) is growing as seen not only in Gartner surveys but also in Gartner client inquiry trends. This is driven by threat actors (in some cases, with nation-state involvement) increasingly targeting critical infrastructures and industrial systems, as well as by enterprises' attack surface expanding due to digital transformation initiatives. Meanwhile, compliance requirements have also been increasing, such as those related to the planned EU's NIS2 Directive and Cyber Resilience Act and the U.S.'s updated NIST Cybersecurity Framework."[4]

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 OT SecOps solutions are customized for converging network and security operations into a unified management and monitoring platform for OT network and security infrastructure. They include asset identification and network communication with a topology map referencing the Purdue Enterprise Reference Architecture, MITRE ATT&CK for ICS matrix, OT playbooks, 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 goal, Fortinet OT SecOps solutions include:

- FortiGate NGFW provides security control and policy enforcement.

- FortiAnalyzer provides unified log management along with OT security analytics and reporting including IT/OT risk, IEC 62443, and NERC CIP compliance reports.

- 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 (OT device decoys and protocol lures) to deceive, expose, and eliminate external and internal threats before significant damage can be done.

- FortiNDR offers network detection and response 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 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 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 CPS 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, SSE, and SecOps solutions. The Fortinet OT Security Platform provides the flexibility and solutions organizations need to secure their OT infrastructures.

[1] CISA, Critical Infrastructure Sectors, accessed August 1, 2024.

[2] Fortinet 2024 State of OT and Cybersecurity Report.

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

[4] Gartner, Emerging Tech: Top Factors Driving Cyber-Physical Systems Security Growth, April 26, 2024.

F⊟RTINET

www.fortinet.com