INDUSTRY INSIGHTS

Fortinet OT Security Platform: Securing Cyber-Physical Systems

Industries such as energy, manufacturing, transportation, communications, building management, healthcare, utilities, warehousing, and others include operational technology (OT) environments. OT has expanded to include a wide range of cyber-physical systems (CPS), smart building solutions, Internet of Things (IoT), Industrial IoT (IIoT), and Internet of Medical Things (IoMT) devices, which are increasingly connected to IT networks and the Internet. Most of these systems are now monitored and managed remotely and interact directly with the physical world. They may include dangerous environments or critical infrastructure, and as more devices are connected, the OT attack surface expands and becomes more vulnerable.

Staying Ahead of the Curve

Like IT networks, OT networks and security must be able to connect every device and also rapidly evolve to keep up with new threats and changing technology. In the past, OT security relied on security through obscurity; nothing was connected to external systems because it was "air gapped." Over the last five years, this approach has changed rapidly, leading to nimbler, more responsive OT environments and increased risk.

CISOs have begun taking on more responsibility for connecting and protecting OT networks, often by adopting an OT secure networking strategy. As OT security matures, CIOs also take on more OT risk mitigation responsibility as they expand their security operations (SecOps) capabilities to include OT. In addition, the increased global pressure of regulation and compliance is forcing the entire C-suite to rapidly survey the evolving OT security space. They are taking a closer look at OT-specific solutions that work together as part of a platform. But because this market is new, it is quickly filling with unproven security start-ups and solutions that may result in the same security sprawl, vendor overload, and siloed solutions that have plagued IT networks for years.

Selecting an OT Security Platform

Any OT security platform must be able to secure devices, networks, and applications. But additional unique requirements across an OT security platform need to be addressed as well, including:

- **Rugged networking devices:** An OT platform must include products in a variety of ruggedized form factors that can withstand harsh environmental conditions.
- **OT support:** Integrated, purpose-built tools should be designed to run on, monitor, and support OT-specific systems, including industrial control systems.
- **Secure remote access:** An effective OT platform must make it possible for OT users and devices to securely connect to connected devices and external systems and support zero-trust controls.

The Fortinet OT Security Platform

The Fortinet OT Security platform protects devices, employee and supply chain access, application access, and IT/OT convergence and is also integrated into the wider OT vendor ecosystem.

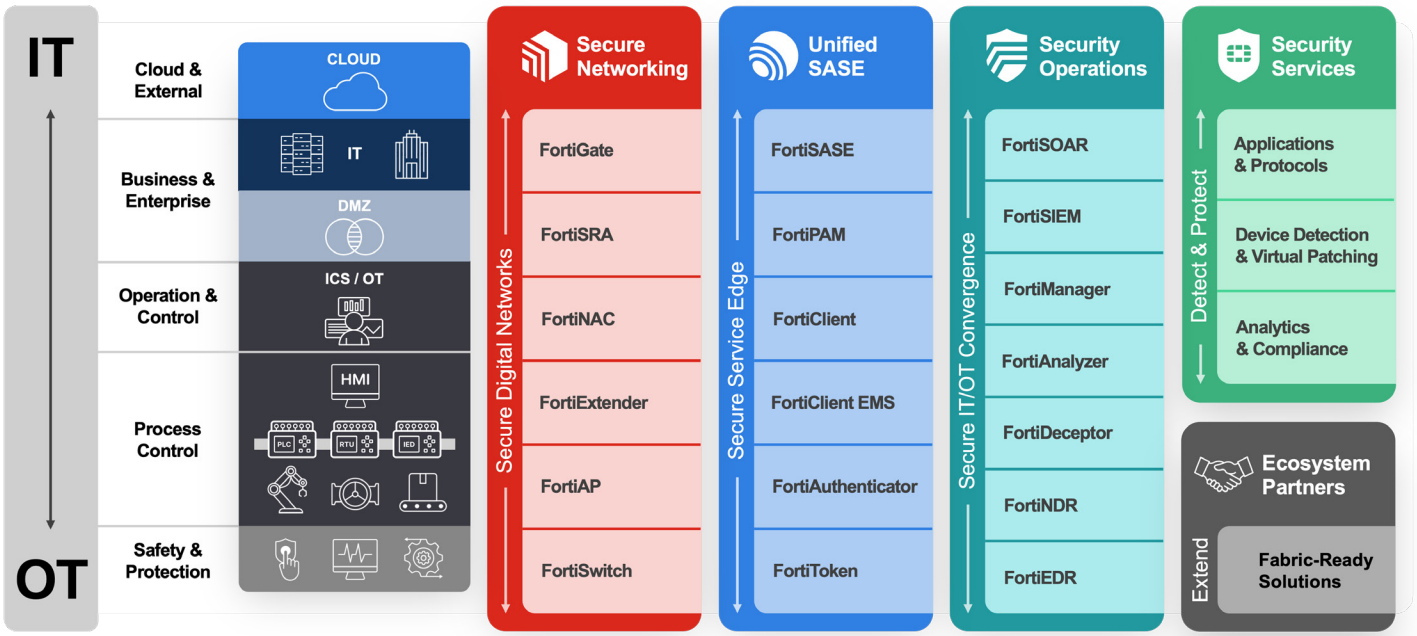

Figure 1: The Fortinet OT Security platform

Secure networking

Secure networking is perhaps the most visible area of OT security because it enables OT systems to connect to the outside world. Some OT environments can be harsh, so Fortinet offers a full range of hardened or rugged firewalls, switches, access points, and 5G extenders. Because getting agents on OT devices can be difficult, physical microsegmentation within the network is offered across the entire stack.

Unified SASE

With more devices connecting to cloud applications, it is critical to secure application access. In addition, some sites cannot host a full security stack so that FortiSASE can provide security in the cloud rather than on the devices themselves.

Security operations

Most IT information security systems aren't designed for OT environments. They were originally designed to work with devices and interactions in the physical world, but Fortinet has added specific OT modules to its IT SecOps products, so they work in an OT environment.

OT security services

To apply efficient network access control and microsegmentation strategies, it's important to understand each OT device, what it does, how it's connected, and what it can talk to. This strategy also allows virtual patching to be deployed to protect against urgent vulnerabilities. FortiGuard OT virtual patching, device detection, and analytics are the most comprehensive in the industry.

Ecosystem partners

The OT ecosystem can contain many different vendors, and Fortinet focuses on two main groups. The first is industrial automation companies. Fortinet has developed partnerships with these global OT organizations to integrate the functionality fully over the long term or become an OT-native within the overall solution. The second set of partners includes Armis, Claroty, Dragos, and Nozomi Networks, which focus on the identification and threat analysis of specific OT environments. They provide information to Fortinet through Fabric-Ready technology integrations to facilitate determining what to allow or block.

Recent Additions to the Fortinet OT Security Platform

Recently, Fortinet expanded its comprehensive OT security platform with the following capabilities:

OT secure networking

- Enhanced asset identification and OT network topology in the FortiOS OT view with configurable asset location to improve asset identity, location, and communication pathways.
- Expanded virtual patching capabilities and new capabilities in FortiOS. The introduction of virtual patching signatures in the FortiGuard OT Security Service provides wide-ranging vulnerability protection and unpatched OT asset shielding.
- Two new series of rugged switches. The FortiSwitch Rugged 216F-POE (Power over Ethernet) is designed to support bandwidth-intensive industrial environments and redundant architectures, and the FortiSwitch Rugged 424F-POE has features designed to power IIoT devices.
- FortiSRA secure remote access to support remote third-party contractors, auditors, and employees, protecting critical OT systems against threats from remote access and untrusted networks.
- FortiExtender Vehicle fleet management and features a ruggedized form factor that can withstand harsh environmental conditions. It provides secure LAN extension from remote FortiGate Next-Generation Firewalls to create a unified platform for vehicles and first responders.

AI-driven OT security operations

- Expanded OT capabilities in FortiSOAR include the introduction of OT View. This IT/OT overview dashboard includes OT asset management and new compliance playbooks to increase OT network and asset visibility and remediation for OT.
- FortiAnalyzer has more analytics and reporting capabilities with NERC CIP, IEC 62443-3-3, and IT/OT risk reports. An upcoming IoT/IIoT/OT dashboard includes analytics support for medical IoT devices to further assist with regulatory compliance and security posture evaluations.
- FortiNDR for OT provides network behavior analysis to identify known and unknown threats across the IT/OT infrastructure and to detect OT network anomalies.
- FortiDeceptor-as-a-Service offers expanded deception for OT and IoT with additional devices and protocols and simplified deployments to streamline user experiences.

OT partnerships

- Integration has been set up between Claroty xDome and FortiManager.
- The Armis threat intelligence feed is now easily accessible from the FortiSIEM graphical user interface.
- Fortinet has a new Engage Preferred Services Partner OT practice designation to empower OT channel partners with the tools they need to design and deploy OT network infrastructure.

Learn more about OT security, the Fortinet OT Security platform, and other OT solutions.

September 11, 2024 8:40 PM / 2839169-0-0-EN