SOLUTION BRIEF

Secure OT Field Sites with the Fortinet OT Security Platform

Executive Summary

Organizations with industrial sites that connect to the internet, such as electric substations, manufacturing facilities, power plants, and oil rigs, must secure their growing attack surface. The urgency to secure critical infrastructure is amplified by well-funded bad actors and threat groups coupled with increasing government scrutiny in the form of regulatory compliance standards. It's critical for organizations to implement basic segmentation, improve visibility, enable secure remote access, and secure field sites.

With the Fortinet OT Security Platform, CIOs, CISOs, and OT security teams can take the first steps to implement segmentation, improve visibility, and secure field access. The OT Security Platform provides advanced security solutions to manage field site security. It simplifies security, helps ensure consistent operations, and makes it easier to assess, secure, and report on risk, including regulatory compliance requirements.

OT is essential to businesses and governments around the world, including critical infrastructure, healthcare systems, and manufacturing operations. The indispensable nature of OT and ICS systems is precisely what puts them at elevated risk.[1]

OT Field Site Challenges

To secure the entire attack surface, many OT organizations deploy visibility solutions to inventory OT field sites, such as electrical substations, capped oil wells, waysides along railroad tracks, connected factories, and electric vehicle charging stations. OT organizations need a simple, centralized, and effective way to secure field sites, no matter the size or operational status of the site. The entire attack surface must be protected from the largest production facility to the smallest OT field site. However, many organizations face challenges in securing field sites because of:

- A lack of visibility into OT networks
- Vulnerable legacy or unpatched devices that are tied to critical operations
- Harsh environmental conditions that may include extreme temperatures, dust, and humidity
- The sheer volume of field sites that must be cataloged and secured to meet regulatory compliance requirements, such as the Network and Information Security 2 (NIS2) Directive and North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP)

Visibility into field industrial sites and their OT devices continues to be a challenge because many devices come from unique vendors and operate on specific protocols that traditional network visibility solutions can't see. This issue can create enormous blind spots for OT operators and security teams. Often, the sheer number of field sites that require visibility is staggering, so creating a complete inventory can be difficult. In some cases, the number of OT field sites can reach tens of thousands, so security solutions for OT field sites must be simple to deploy yet robust enough to scale.

OT Field Site Security

To meet today's OT challenges, Fortinet has enhanced its OT Security Service and released a suite of ruggedized network security products to properly secure OT field sites. Fortinet OT network security uses a single operating system, FortiOS, so management can be performed using a single view alongside IT security. This unified view improves visibility across the entire network and simplifies segmentation and secure remote access.

The FortiGuard OT Security Service provides broad security and enforcement coverage for OT environments. It includes more than 3,300 OT protocol rules, nearly 750 OT IPS rules, over 1,500 OT virtual patch rules, and 1,300 OT application detection rules. Using the FortiOS console, security teams can see their OT environment based on the Purdue model and the known vulnerability exploits for their devices. It also shows inbound connections to OT field sites and the associated OT protocol bandwidth. By taking advantage of these features, security teams can quickly and effectively establish compensating controls to secure legacy devices tied to critical operations while the devices await a patch.

Fortinet offers a fully ruggedized portfolio that spans firewalls, switches, access points, and cellular gateways. The FortiGate Rugged 70G and FortiGate Rugged 50G-5G Next-Generation Firewalls (NGFWs) provide compact, ruggedized security so organizations can securely connect and transform their field OT sites. They include a digital I/O (DIO) module to support SNMP traps and automation-stitch notifications when the DIO module alarm is activated. The DIO module triggers an alarm when it detects a change in any digital input, and the digital output is activated.

The notification support depends on how the config system digital-io and execute digital-io set-output settings have been configured prior to event notification. This feature allows operators to secure OT traffic at field sites and physical processes through the firewall. FortiGate Rugged models equipped with a serial RS-232 (DB9/RJ45) interface can now receive data in Modbus serial (RTU/ASCII) protocol and convert it to Modbus TCP, as well as receive DNP3 serial and convert it to DNP3 TCP/IP. With these new expanded features, FortiGate Rugged models can perform real-time monitoring, control, and coordination across the network.

The FortiSwitch Rugged 108F (FSR-108F) and FortiSwitch Rugged 112F (FSR-112F-POE) switches expand and update the 100 series with small form factors for the type of small deployments that are typical in OT field sites. By using rugged FortiGate NGFWs and FortiSwitch switches, organizations can extend advanced threat protection to field sites and harsh environments. Because the solutions run on the unified FortiOS operating system, segmentation and security policies can be implemented down to the port level for enhanced protection. In addition, the FortiExtender Rugged 511G (FER-511G) and FortiExtender Vehicle (FEV-511G) wireless WAN solutions provide secure 5G and Wi-Fi 6 in a single device for secure connectivity from field sites and vehicles.

With the ability to scale to even the largest OT environments, the Fortinet OT Security Platform can provide visibility, segmentation, and secure connectivity for thousands of sites and vehicles using a single pane of glass. Fortinet management solutions provide robust capabilities and quick at-a-glance information so IT and OT security operations personnel can generate relevant reports for stakeholders and monitor adherence to regulatory frameworks.

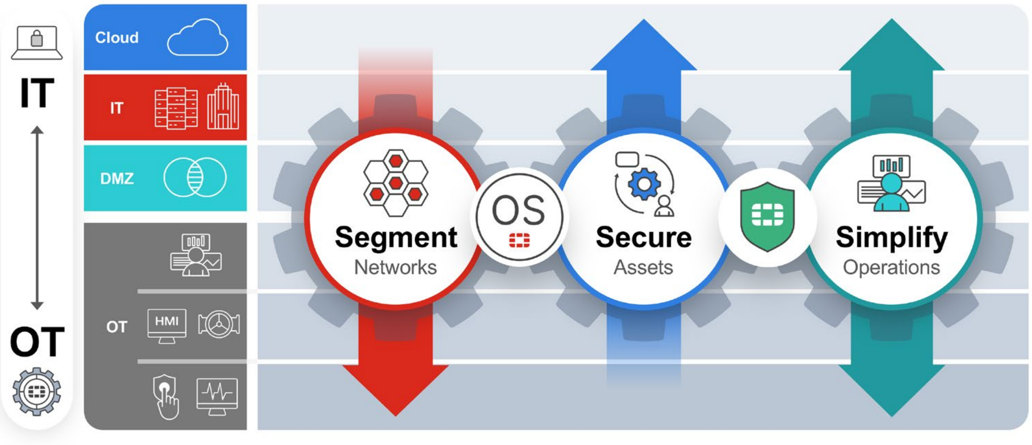

Figure 1: The Fortinet OT Security Platform

The Benefits of a Platform

To protect the entire attack surface, OT teams need a unified OT-specific platform that can catalog field industrial sites and provide deep visibility into the devices, protocols, applications, and users within those sites.

The vast amount of legacy or unpatched devices tied to critical operations at field sites may include desktops with outdated operating systems; supervisory control and data acquisition (SCADA) systems and human-machine interface (HMI) systems; and even field controllers for compressors, pumps, pressure sensors, furnaces, gauges, and more. Legacy devices, when connected to untrusted networks like the internet and cloud, open an entire organization and operations to risk and invite malicious cyberthreats. OT-specific solutions unified by a platform and single operating system can help OT organizations monitor the entire attack surface.

The harsh conditions at field industrial sites, such as extreme temperatures, shock, vibrations, and contaminants mean that firewalls, switches, and cellular gateways must be ruggedized. Securing OT environments requires effective ruggedized security solutions that are designed specifically for OT and capable of securing any OT field site, no matter where it may be located.

Secure Field Sites More Effectively

Cataloging, connecting, and securing field industrial sites and legacy OT devices can seem daunting, given the increase in regulatory compliances and rise of OT cyberthreats. Lack of visibility, harsh environmental conditions, and the sheer scale of such projects often can impede organizational progress.

> As OT organizations introduce new digital tools and technologies, security challenges have grown more complex. As the National Institute of Standards and Technology (NIST) notes, “While security solutions have been designed to deal with these issues in typical IT systems, special precautions must be taken when introducing these same solutions to OT environments. In some cases, new security solutions that are tailored to the OT environment are needed.”[2]

The Fortinet OT Security Platform makes the task of securing field industrial sites simpler and more effective. It unifies visibility and enforcement capabilities and provides an end-to-end portfolio of ruggedized infrastructure, which can all be managed through a single pane of glass. Contact your Fortinet seller or partner representative today to learn more about the Fortinet OT Security Platform.

[1] Fortinet, 2024 State of Operational Technology and Cybersecurity Report.

[2] Keith Stouffer et al., Guide to Operational Technology (OT) Security, NIST, September 2023.

May 22, 2025 7:41 PM / MKTG-969-0-0-EN