Executive Summary

The connection operational technology (OT) has to the physical world means that a cyber disruption can impact lives in a way that an IT attack never can. OT technology such as industrial control systems (ICS) and supervisory control and data acquisition (SCADA) equipment have become popular targets for advanced threats, and there has been steady growth in threat actors identifying OT vulnerabilities and building them into exploit tools they sell on the dark web.¹

As protective air gaps disappear with greater digitization, OT systems are increasingly barraged with both recycled information technology (IT)-based attacks and exploits targeted at OT. Operations leaders in these environments need to implement cybersecurity measures that provide threat prevention, detection, and response capabilities that are designed for the sensitive nature of OT systems. The integrated architecture of the Fortinet Security Fabric offers OT-native security that fulfills these critical needs.

IT Convergence Puts OT Systems in Jeopardy

Digitization increases the number of devices exposed to attack, so advanced threats can effectively make their way across all parts of an organization’s network, including OT systems in industrial, manufacturing, and critical infrastructure environments. As IT and OT environments continue to converge, the air gap that kept OT secure through isolation is dissolving. Now any threat that is capable of a successful IT breach has a pathway to vulnerable and potentially valuable targets on the OT side. The introduction of new technologies such as the Industrial Internet of Things (IIoT) and 5G further expands the attack surface, exposing industrial systems to increased risk.

Protecting OT environments from advanced threats requires a prevention, detection, and response plan powered by an integrated platform and threat intelligence. From basic security to advanced tools featuring artificial intelligence (AI) and machine learning (ML), the Fortinet Security Fabric includes solutions that are specifically designed to protect both OT and IT systems from advanced threats.

Prevention: Implementing OT Security Controls

Fortinet solutions support internal network visibility, access controls, and policy enforcement to prevent movement of threats across the network. They prevent movement both north-south (in and out of OT environments) as well as east-west (laterally across the network).

FortiGate Next-Generation Firewalls (NGFWs) can be deployed within OT environments to provide comprehensive visibility as well as threat-intelligence sharing across the broader organization (both IT and OT). FortiGate NGFWs can also be used for internal segmentation of OT environments, creating inspection points for detecting and blocking threats. A database of over 55 OT-specific protocols comprised of more than 1,800 commands enables FortiGate NGFWs to detect anomalous or malicious OT traffic and prevent a threat in one segment from spreading through the OT network. FortiGuard OT-specific threat intelligence enables FortiGate NGFWs to virtually patch OT systems against both old and newly discovered vulnerabilities. The OT-specific application signatures and vulnerability protections are available and kept current through the FortiGuard Industrial Security Service.

FortiSwitch Ethernet switching integrates directly into the Fortinet Security Fabric to become an extension of the FortiGate NGFW. This extension enables OT administrators to enforce NGFW policies at the Ethernet port level, which helps ensure a secure, reliable OT environment without introducing complexity.

In combination with FortiGate, FortiNAC network access control (NAC) continually monitors all parts of the network. FortiNAC automatically identifies all of the devices that are connected or attempting to connect and tests their compliance against the organization's established security policies.
Detection: Spotting and Blocking Sophisticated Attacks

Advanced cyber threats employ sophisticated and targeted attacks that are designed to evade traditional threat detection. Fortinet solutions use AI and ML capabilities to accelerate discovery of new malware techniques, which improves detection by 20%.

As an additional complement to FortiGate, FortiAI uses AI to optimize security operations and enhance the productivity of security analysts. The solution uses a self-learning deep neural network (DNN) to automate rote security tasks that help accelerate responses and remediation. For example, FortiAI can learn to identify new file-based and fileless malware in sub-seconds.

FortiSandbox detects both emerging and zero-day threats. It quarantines any suspicious objects found in network traffic and observes them in a simulated environment. And unlike some sandboxing products, FortiSandbox supports OT operating systems, so it can analyze OT-specific malware and detect adversaries operating within the OT environment.

FortiDeceptor decoys emulate OT control systems such as programmable logic controllers (PLCs) to trick attackers into revealing themselves. With FortiDeceptor, OT operations teams can identify threats already within the network and extract intelligence about the adversary’s tools and operations.

FortiSIEM security information and event management (SIEM) provides a centralized solution for collecting logs and analyzing security events. These capabilities help accelerate threat detection, simplify regulatory compliance processes, and eliminate inefficient manual workflows. FortiSIEM reduces risks while conserving limited human resources. It has Perdue Model dashboard displays commonly found in OT architectures.

FortiInsight user and entity behavior analytics (UEBA) technology prevents insider attacks by continuously monitoring users and endpoints with automated detection and response capabilities. FortiInsight automatically identifies noncompliant, suspicious, or anomalous behavior and rapidly provides alerts about any compromised user accounts.

Because they are part of the Fortinet Security Fabric, these integrated solutions feed real-time threat intelligence to FortiGate NGFWs to share any detected threats across the entire organization. The Security Fabric then can automatically block any similar threats and thwart coordinated, multivector attacks before any damage can be done.

Response: Bolstering Security Operations

As an integrated platform, the Fortinet Security Fabric observes network traffic across the organization’s full attack surface looking for both known and unknown imminent threats. This automated aggregation of intelligence helps pinpoint “patient zero” compromised systems in real time.

FortiEDR helps automatically contain device-based breaches without disrupting operations. The Fortinet endpoint detection and response (EDR) solution provides advanced threat protection for endpoint devices connected to OT environments. It proactively reduces the OT attack surface, prevents malware infection, detects and defuses potential threats in real time, and can automate response and remediation procedures with customizable playbooks.

FortiSOAR security orchestration, automation, and response (SOAR) allows security operations teams to create a custom automated framework that pulls together all of the organization’s security tools while eliminating alert fatigue and reducing context switching.

To help minimize human analysis and decisions, playbooks can be automated. The ability to provide accurate contextual awareness across OT environments, combined with the ability to offload IT security tasks like threat analysis, helps accelerate mitigation processes and minimize windows of exposure.
Security Designed for Industrial Operations

OT convergence with IT networks has opened a “Pandora’s box” of advanced threats for OT environments, and traditional point security solutions cannot help. But Fortinet is uniquely positioned to address this complex and rapidly evolving intersection of OT and IT. The Fortinet Security Fabric spans both OT and IT environments with solutions that prevent, detect, and respond to a full spectrum of risks, including previously unknown and zero-day attacks. The Fortinet Security Fabric provides a complete view of the entire organization because all of the security tools on both the IT side and OT side can report to the same management and analysis tools. The Fortinet Security Fabric not only provides top-rated security that’s designed to be compatible with OT operating systems, it also simultaneously streamlines security operations to reduce costs and conserve resources.

3 FortiGuard Labs research, October 2020.