ARC VIEW

JANUARY 5, 2023

Today's OT Systems Need IT Security Capabilities

By Sid Snitkin

Keywords

OT Cybersecurity, Network Security Solutions, Fortinet

Summary

Industrial companies need strong OT cybersecurity programs to deal with today's sophisticated threat environment. Facilities have become prime targets for ransomware and sophisticated nation-state attacks. Insecure IoT devices, cloud connections, and increased use of remote access have exploded the pathways for attacks on critical systems.

Industrial companies require stronger OT cybersecurity programs to deal with today's sophisticated threat environment. Managers need to accept this fact and invest in more advanced cybersecurity capabilities that can enable active defense of critical operations.

Many industrial facilities have invested in some basic cybersecurity defenses, but they lack the resources and security management tools to sustain their effectiveness. Most facilities also lack the capabilities to rapidly detect and manage compromises before they create operational impact.

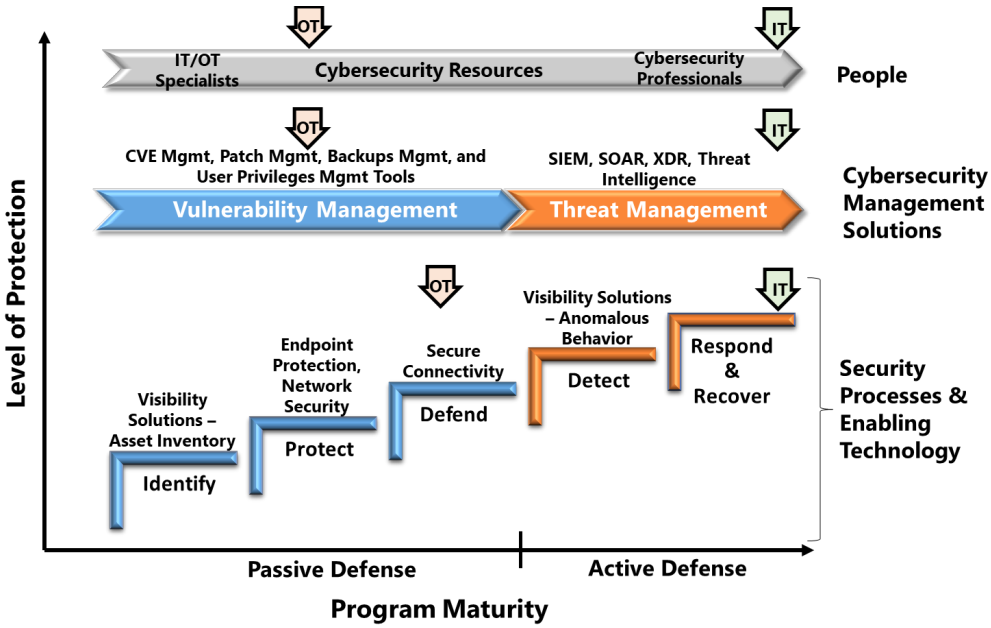
Basic security programs may have been adequate for traditional, isolated OT systems, but modern developments

demand extensive connectivity. This means that today's OT systems face many of the same threats as IT systems and need comparable cyber defenses. Managers of industrial companies need to accept this fact and invest in more advanced cybersecurity capabilities that can enable active defense of critical facilities.

This ARC report describes the major gaps in today's OT cybersecurity programs and what's needed for today and tomorrow's more challenging threat environment. A review of Fortinet's security offerings is included to show how one leading IT security company has developed OT cybersecurity offerings that can help critical infrastructure operators ensure that their facilities remain safe and secure.

Today's Threats Demand Better Industrial Cybersecurity

ARC's Industrial/OT Cybersecurity Maturity Model provides a useful tool for understanding industrial cybersecurity program requirements. This model provides a roadmap for implementing the security technologies, cybersecurity management solutions, and human resources needed to support NIST cybersecurity framework recommendations. The colors in the model distinguish the basic passive defensive measures that are recommended to protect systems against conventional hackers, from the active defense capabilities needed for more sophisticated attacks.



ARC Industrial/OT Cybersecurity Maturity Model

A key goal of the ARC model is to highlights the need to maintain alignment of people, processes, and technology capabilities. Security technologies must be maintained to be effective and security teams need the right tools to effectively perform these tasks. Likewise, cybersecurity professionals are only effective when they have good visibility of risks and the ability to rapidly isolate and remediate threats. The real effectiveness of a cybersecurity program, or its maturity, is determined by the weakest element.

As the figure shows, most industrial IT cybersecurity programs are significantly more mature than those for OT. IT security programs include passive and active defenses. They also have teams of cybersecurity professionals and advanced cybersecurity management solutions that help them maintain security posture and manage attacks. Sophisticated attackers may compromise

IT systems, but rapid detection, isolation, and remediation enable security teams to minimize the impact.

	Technology	Focus	Capabilities for OT
Visibility Solutions	**Asset Inventory**	Detect all assets within OT systems, collect information about device type, configuration, hardware, software, firmware, and data flows between system assets.	Active and passive scanning that can identify OT devices while avoiding any disruptions in legacy controllers
	Anomalous Behavior	Rapidly detect any anomalous behavior occurring within OT devices, networks, user actions, and physical processes.	Network traffic analysis, device monitoring, UBEA, and deception technology
	Endpoint Protection	Protecting the data, code, and integrity of endpoint devices by blocking malicious software downloads and unauthorized actions.	Anti-malware, device firewalls, and application whitelisting
	Network Security Solutions	Protecting OT system devices and limiting attacker access to critical systems through use of perimeter defenses, network segmentation, and blocking of unauthorized messages within systems.	Next-generation firewalls, routers, and switches that support granular policies and industrial deep packet inspection
	Secure Connectivity	Protecting OT systems by ensuring that interactions with external entities (other systems, mobile devices, cloud apps, third-party sites, and connected workers) don't provide new pathways for attacks by malicious people or compromised devices and apps.	Network Access Control (NAC), Identity and Access Management (IAM), Privileged Access Management (PAM), Secure Remote Access (SRA), and Secure Internet Access (SIA)
Cybersecurity Management	**Vulnerability Management**	Enable efficient and effective maintenance of all security defenses. This includes identification and classification of security risks, rapid evaluation of vulnerability alerts, management of patches and AV updates, maintenance of system backups, and consistent management of all user access privileges.	Security management tools that cover CVE management, Patch management, User privileges management, and Backup management
	Threat Management	Enable efficient and effective response to perceived security threats. This includes management and analysis of system alerts, integration of threat intelligence, and integration of tools that help defenders triage, investigate, identify, isolate, remediate, and restore systems.	Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), Extended Detection and Response (XDR), Threat Intelligence

OT Cybersecurity Technology Requirements

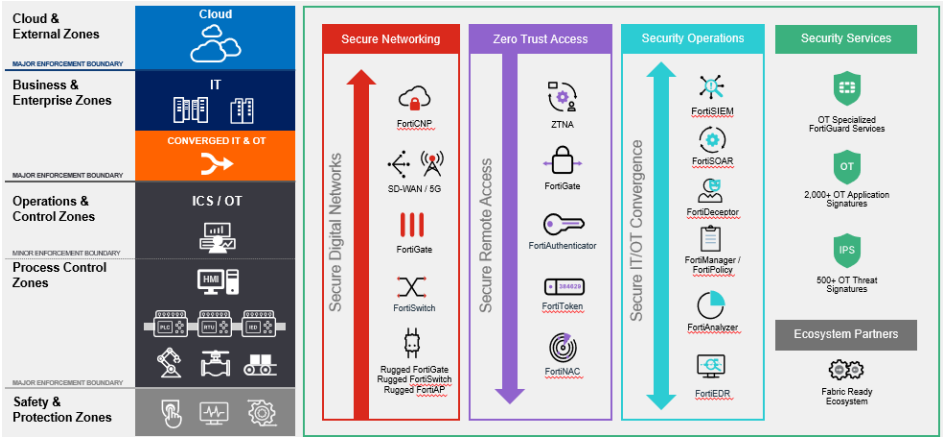
The current state of OT cybersecurity places our critical infrastructure at risk of serious cyber incidents. And these risks are growing with more sophisticated attackers, unmanageable IoT devices, and the proliferation of external connections. Closing the gaps between OT and IT cybersecurity programs is an urgent issue that every facility needs to address. ARC's model highlights the kinds of improvements needed and the table above describes the capabilities that organizations should look for in solutions they select in upgrading their OT cybersecurity technology stacks.

Fortinet Helps Companies Close OT Cybersecurity Gaps

US-based Fortinet is a leading supplier of networking and security products including next-generation firewalls, intrusion detection and prevention, SIEM, SOAR, Deception, etc. The Fortinet Security Fabric platform provides security integration and automation across their products and those offered

by notable OT security partners, such as Nozomi Networks, Claroty, Dragos, and Armis.

ARC's discussions with company executives revealed Fortinet's deep understanding of the challenges OT security teams face. ARC was also impressed with the comprehensive suite of security solutions the company offers to address OT security challenges.



Fortinet Security Fabric Solutions for Operational Technology

The following sections discuss how Fortinet's Security Fabric Solutions address the recommendations in this report.

Asset and Network Visibility Solutions

Fortinet's partnerships with leading OT security companies like Nozomi Networks, Claroty, Dragos, and Armis provides visibility capabilities that are pre-integrated with Fortinet's Security Fabric. This allows Fortinet to offer customers a range of OT visibility options and provides current users of these products with a convenient and seamless path to adopt the advanced security products, from Fortinet and other partners in Fortinet's Security Fabric, which are needed to address the gaps in today's OT security programs and achieve active defense capabilities.

Endpoint Protection

Fortinet's FortiEDR provides enhanced endpoint protection for a wide range of OT assets. This product prevents, detects, and defuses threats while keeping systems online across IT and OT environments. It comprehensively secures endpoints for pre- and post-infection and includes several key capabilities for defending vulnerable OT endpoints. This includes ML-based next-

generation antivirus, application communication control, automated EDR, real-time blocking, threat hunting, incident response, and virtual patching capabilities. These capabilities come in a lightweight agent that spans a variety of modern and legacy operating systems and ensures high availability of critical OT system assets like historians, jump boxes, engineering workstations, HMIs, and traditional IT systems that are commonly found in OT environments.

FortiEDR leverages the Fortinet Security Fabric and integrates with many advanced security components, including FortiGate NGFWs, FortiSandbox, and FortiSIEM. FortiEDR has been successfully deployed in various industrial environments, including manufacturing, automotive, water treatment plants, and life sciences industries.

Network Security Solutions

Fortinet is recognized as a leading supplier of networking products including next generation firewalls and secure network switches that incorporate the powerful FortiOS operating system. While traditional security solutions are designed and intended for the world of offices and corporations, the FortiGate Rugged Series offers an industrially hardened, all-in-one security appliance that delivers specialized threat protection for securing critical industrial networks against malicious attacks.

With FortiGuard's Industrial Security Service enabled, the FortiGate (including rugged, non-rugged, and VM series) NGFW supports policy setting for over 70 OT protocols, including deep packet inspection (DPI) and parameter-based policies for Modbus TCP, IEC-104, and DNP3. The FortiGate NGFW also protects assets against over 500 known OT vulnerabilities using the FortiGate's Intrusion Prevention System (IPS) capability.

The FortiGate Rugged 60F Series features an integrated hardware security module, also known as Trusted Platform Module (TPM), that hardens physical networking appliances by generating, storing, and authenticating cryptographic keys. Hardware-based security mechanisms protect these products against malicious software and phishing attacks. Fortinet prides itself on FortiGate's ASIC-based security processing units (SPUs) that accelerates processing of high throughput real-time OT network traffic.

Fortinet's network security solutions are managed through FortiManager. This solution can manage all Fortinet NGFWs and itis designed to meet the

needs of OT cybersecurity. The solution has a federated architecture that supports on-prem and cloud-based deployments and can be used as a totally disconnected product for isolated networks.

Fortinet advised ARC that they are continuing to enhance their network security solutions to support OT needs. For example, FortiManager upgrades include a new Purdue model-based view for visualizing and monitoring OT network devices.

Secure Connectivity

As a leading supplier of network security solutions, Fortinet offers a broad range of solutions to ensure secure connectivity for all types of networks being adopted in modern industrial companies. This includes connections with mobile devices, cloud services, third-party sites, WAN, and connected workers. Their products protect systems from attacks by malicious people and compromised devices and apps.

ARC's discussions with company executives demonstrated the company's understanding of the challenges that OT security teams face in enabling connected workers and their products for network access control (NAC), Multi-Factor Authentication (MFA), Single Sign-On (SSO), and VPN can enable zero trust for all these interactions.

Cybersecurity Management

The Fortinet Security Fabric includes several highly relevant offerings that are applicable to IT and OT. Fortinet's product strategy includes putting OT-specific capabilities into these products to simplify the management of threat detection, protection, and management. Examples include enhancements to FortiSIEM, FortiSOAR, and FortiDeceptor that leverage the Purdue Model and include the MITRE ATT&CK for ICS Framework for threat analysis. FortiDeceptor can also deploy decoys and lures that mimic OT devices such as HMIs, PLCs, and SCADA workstations. The ruggedized version of FortiDeceptor can simulate up to 100+ decoys in one appliance. FortiManager and FortiAnalyzer present a single pane of glass for managing policies across IT and OT and for processing log data from both sides.

FortiGuard Labs provides the threat intelligence foundation for Fortinet Security Fabric solutions to ensure that they are continuously updated with the latest threat-intel and protection information. This includes threats specifically related to OT industries.

Conclusion

Threats to industrial operations have outpaced the capabilities of most OT cybersecurity programs. Most facilities lack the security resources, technologies, and cybersecurity management tools to defend operations against ransomware and sophisticated attackers. They also lack people and expertise to ensure security of new digital transformation efforts and expanded use of remote workers. Today's OT security teams face the same security challenges as their IT counterparts and need comparable capabilities. No company can afford to ignore the growing risks of serious cyber incidents.

This report provided ARC's recommendations for what companies need to do to ensure that their OT cybersecurity programs can ensure safe and reliable operations. The review of Fortinet's products and services demonstrates that there are companies who offer solutions that can help end users make a smooth transition to required security capabilities. So, the biggest risk to critical infrastructure are users that ignore the urgency in addressing these critical issues.

For further information or to provide feedback on this article, please contact your account manager or the author at srsnitkin@arcweb.com. ARC Views are published and copyrighted by ARC Advisory Group. The information is proprietary to ARC and no part of it may be reproduced without prior permission from ARC.