FORTINET

OT Cybersecurity Designed for Critical Plant and Manufacturing Operations

5 Actionable Takeaways

Table of Contents

Executive Overview

Organizations are converging their operational technology (OT) and information technology (IT) environments for competitive advantages. This greatly increases cyber risk within the OT environment. Having a comprehensive, end-to-end security posture greatly reduces this risk. Plant operations and manufacturing leaders need to consider a security approach that integrates OT and IT security, is easy to adopt, accommodates OT limitations, is built on an open platform, and automates compliance and audit reporting.

64% of OT leaders say that keeping pace with change is their biggest challenge.[1]

78%

of OT leaders have only partial centralized visibility on their OT cybersecurity.[2]

01: Digitization of Plant Operations

Imagine machines on a plant floor that talk with each other, make adjustments to maximize uptime, and schedule their own proactive maintenance—all automatically. Imagine equipment with these capabilities in an electrical grid, oil field, or other environments with OT.

This is not far in the future. Digital transformation (DX) is already changing OT in myriad ways—from the way metals are processed,[3] to how large equipment is maintained,[4] to the ways in which prototypes are produced.[5]

Traditionally, OT and IT environments have been separated by an "air gap," or lack of a physical connection between them to completely isolate and secure the OT network. This is no longer the case: 75% of OT organizations report making, at least, basic connections between OT and IT technologies to gain competitive advantages.[6] This integration expands the digital attack surface, however, and increases the risk of cyberattacks.

Threat data proves this is the case: almost three-quarters (74%) of OT organizations report they have experienced a malware intrusion within the past year, and half experienced three or more breaches.[7]

OT environments, typically designed without cybersecurity in mind, need increased protection. Plant operations and manufacturing leaders indicate that "reducing security vulnerabilities response time" is their third most important success metric behind maximizing productivity and minimizing cost.[8]

The question is *how* to strengthen OT cybersecurity. What security approach accommodates the unique character of OT devices and systems, while supporting maximized uptime and minimized costs? To accomplish these goals, plant operations and manufacturing leaders should consider an approach that meets the following requirements:

Since OT systems are infrequently replaced, many are being exposed to today's advanced persistent threats for the first time.[9]

85%

of unique OT threats targeted machines running OPC Classic, BACnet, and Modbus.[10]

02: OT Security Must Be Easy to Adopt

Plant operations and manufacturing leaders must avoid the mistake that many organizations make when deploying cybersecurity for their IT environments by choosing a mix of best-of-breed point solutions that operate in isolated silos. As a result, security teams switch between multiple consoles and must correlate security feedback manually, increasing security gaps, risks, and the opportunity for error.

Instead, teams should seek a coordinated, integrated, and open security platform that enables security elements to work together, sharing threat intelligence and stopping advanced threats. In sum, this security fabric approach should provide broad, centralized visibility from a single pane of glass.

The same security management console should cover both OT and IT security environments. This enables one team to manage protection across the enterprise. Centralized management is high on the list of priorities for many OT organizations: 70% plan to bring OT security together with IT security in the next 12 months, making the CISO responsible for both.[11] This enables plant operations and manufacturing staff to shift additional resources from security to priorities in productivity and safety.

In addition to managing OT and IT environments, the security management console should extend to include security for cloud and Internet-of-Things (IoT) domains. A unified security console simplifies staff training and ongoing management because it enables teams to avoid switching between multiple solution interfaces. In addition, centralized security management adds agility. For example, an incoming intelligence update about an advanced threat can centrally trigger a policy modification on all firewalls across the enterprise, blocking that threat across every security vector.

A single management console also avoids the added risk of siloed security between IT and OT. A unified security approach is more effective at revealing and resolving security gaps. For instance, a serious gap existed at a number of U.S. energy grid companies that used "jump boxes," or utility boxes, to allow their technicians to move between IT and OT networks. While this enhanced the productivity of technicians, the jump boxes were inadequately monitored and defended, and hackers were able to exploit them by stealing employee credentials and using the boxes to move from IT to OT networks. The attackers then planted malware in OT equipment at two dozen companies and were poised to disrupt the energy grid before the FBI discovered their attacks.[12]

45% of organizations with OT environments are not making use of privileged identity management.[13]

To unify security, 70% of OT organizations plan to bring OT security under the CISO in the next 12 months.[14]

03: OT Security Must Accommodate OT Limitations

Much of the equipment found in OT networks is decades old and has proven itself through long service. But it was not designed with cybersecurity in mind, often because it was isolated from IT networks and the threats they carry. Now, due to the convergence of IT and OT, security is needed for OT devices that can accommodate their unique limitations.

As an example, some OT elements such as programmable logic controllers (PLCs) would be disrupted by active security scanning methods that are typical on IT networks. Here, plant operations and manufacturing leaders need to embrace an OT cybersecurity approach that uses passive network traffic analysis to profile each element in the OT network based on its observed characteristics and behavior.

In addition, many OT elements cannot host a security software agent, or software that connects them to centralized security solutions and enables them to be protected. Often, this limitation is a result of their being designed before the internet era.

To protect these OT elements, security teams should look for an OT security approach that uses a next-generation firewall (NGFW) to provide segmentation. The NGFW inspects network traffic to each device, blocks unauthorized traffic, and separates the devices from critical data and applications that are not pertinent. Segmentation also prevents the lateral (east-west) spread of malicious exploits and enables organizations to quickly quarantine compromised devices. The ability to enforce access controls for each device enhances security compliance by protecting against unauthorized access.

To provide these capabilities, plant operation and manufacturing leaders need to look for NGFWs that understand and analyze proprietary OT protocols. As a result, they can detect and block threats and exploits in OT traffic. The NGFWs should be able to consolidate multiple intelligence feeds in one console. And one of those intelligence feeds should update them on OT protocols and known OT vulnerabilities, increasing their ability to safeguard the network. Through segmentation, they can provide "virtual patching" to the many OT devices that cannot be patched.

Segmentation can protect OT devices that cannot have security added and guard against east-west movement of malicious intrusions. However, 53% of OT organizations do not employ segmentation. [15]

04: OT Security Should Be Built on an Open Platform

To protect an organization's existing investment in security, an OT cybersecurity approach must accommodate mixed vendor security solutions with integrations using application programming interfaces (APIs) and connectors. It should also have deep API and REST API connections to integrate threat intelligence from multiple security solutions. Security tools need to work together to gather, correlate, and provide unified visibility into the local threat environment. An open and unified platform provides the basis for this synchronization.

OT leaders should also seek a security approach that can integrate, interact with, and control a variety of switches and wireless APs from different vendors. This can enable greater network security through legacy switches and APs without needing to upgrade or replace them.

Security tools need to work together to provide unified visibility.
Further, an open platform protects legacy investments.

05: OT Security Ought to Automate Incident Responses

Many of today's digital threats move at machine speed, enabling exfiltration of corporate data in minutes. With 68% of breaches taking months or longer to discover, speed—or lack thereof—is a serious problem.16 This is why an OT security approach needs to move at machine speed as well, automating intrusion prevention, detection, and incident response capabilities.There are huge potentials here, with experts indicating upwards of 80% of a security team's daily work can be automated, thereby freeing them for higher-value tasks.[17] To achieve these automation results, plant operations and manufacturing leaders should consider an approach that can:

- Automatically detect and create signatures for malware detection and prevention
- Automatically send alerts or quarantine the detected threats
- Engage third-party devices in alerts and quarantines and aggregate and reconcile them in one threat feed
- Automate incident response workflows, enabling network and security teams to share data and work faster and better together.[18]

68%

of breaches still take months or longer to discover. Up to 80% of a security team's daily work can be automated, freeing them for higher-value tasks.

06: OT Security Should Automate Compliance and Audit Reporting

Compliance audits often require extensive manual labor to aggregate, reconcile, and normalize data from many different security and network vendors' tools. No silo of security data should be left untouched. Plant operations and manufacturing leaders should look for a solution that automates compliance tracking and reporting and provides the capability to evaluate the network environment against best practices, including the ability to measure compliance risks.

The solution should provide real-time reports about pertinent industry and government regulations as well as industry standards, such as the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS). The NIST Cybersecurity Framework, for instance, helps organizations reduce risk with customized measures and guides them in making prioritized security improvements. Major companies from around the world have embraced the NIST Cybersecurity Framework, and analysts project that 50% of organizations will be using it by next year.[19]

47% of OT organizations do not have scheduled security compliance reviews, which exposes them to potential regulatory fines and penalties and/or creates greater risk.[20]

50%

of organizations will use the NIST Cybersecurity Framework by next year. Organizations not adhering to NIST security standards will find themselves playing catch-up.

07: Join the Leaders in OT Digital Transformation

Like every other area of business, OT is being changed by DX. Plant operations and manufacturing leaders are seizing the opportunity to improve productivity, efficiency, and safety by integrating OT with technologies such as machine learning, big data, and IoT. Integrating OT and IT technologies dissolves the air gap that once protected OT environments.

Pursuing these opportunities requires building a cybersecurity foundation that mitigates risk. It should unify OT and IT cybersecurity, be easy to adopt, accommodate OT limitations, and be built on an open platform to protect existing solutions and investments. It should also automate compliance and audit reporting to enhance security and enable overstretched security teams to focus on higher-value projects.

[1] "State of Operational Technology and Cybersecurity Report," Fortinet, accessed April 18, 2019.

[2] Ibid.

[3] Bernard Marr, "What is Industry 4.0? Here's A Super Easy Explanation For Anyone," Forbes, September 2, 2018.

[4] Clint Boulton, "10 machine learning success stories: An inside look," CIO, December 4, 2018.

[5] Cornelius Baur and Dominik Wee, "Manufacturing's next act," McKinsey & Company, June 2015.

[6] "Independent Study Pinpoints Significant SCADA/ICS Cybersecurity Risks," Fortinet, May 7, 2018.

[7] "State of Operational Technology and Cybersecurity Report," Fortinet, accessed April 18, 2019.

[8] Ibid.

[9] Fortinet 2019 Operational Technology Security Trends Report, Fortinet, May 8, 2019.

[10] Ibid.

[11] "State of Operational Technology and Cybersecurity Report," Fortinet, accessed April 18, 2019.

[12] Rebecca Smith and Rob Barry, "America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It," The Wall Street Journal, January 10, 2019.

[13] Fortinet 2019 Operational Technology Security Trends Report, Fortinet, May 8, 2019.

[14] "State of Operational Technology and Cybersecurity Report," Fortinet, accessed April 18, 2019.

[15] Ibid.

[16] "2018 Data Breach Investigations Report," Verizon, April 10, 2018.

[17] Cynthia Harvey, "8 Ways Security Automation and Orchestration Is Transforming Security Operations," eSecurity Planet, September 5, 2018.

[18] "Bridging the NOC-SOC Divide: Understanding the Key Architectural Requirements for Integration," Fortinet, August 23, 2018.

[19] "Cybersecurity Framework," NIST, accessed May 4, 2019.

[20] "State of Operational Technology and Cybersecurity Report," Fortinet, accessed April 18, 2019.

www.fortinet.com

391834-0-0-EN

June 27, 2019 7:37 PM

eb-ot-cybersecurity-plant-and-manufacturing-operations