FORTINET® softwerx

A Security Approach for Protecting Converged IT and OT

Table of Contents

Executive Summary

Operational technology (OT)* networks, which control **equipment** in critical infrastructure such as utilities and manufacturing assembly lines, have traditionally been kept separate from **information technology (IT)** networks, which control **data** in all organizations. In recent years, compelling innovations in IT such as artificial intelligence (AI) and big data analytics promise to bring improved outcomes to OT networks as well. As a result, the integration of OT and IT networks is accelerating, and this expands the digital attack surface, exposing OT networks to attacks coming from IT networks. OT breaches are now commonplace. To thwart attacks and minimize OT risk, implement five best practices: 1) increase network visibility, 2) segment networks, 3) analyze traffic for threats, 4) enforce identity and access management, and 5) secure both wired and wireless access. These practices are presented as a foundation for enhancing OT security posture.

* OT is a synonym for **industrial control systems (ICS)**. OT was established as a term to contrast with IT, because OT protocols, vendors, and use cases are distinct. **Supervisory control and data acquisition (SCADA)** systems are an element of OT. SCADA systems use graphical user interfaces for high-level supervisory management of OT/ICS processes.

01: Why IT and OT Are Converging

From machine learning (ML) to augmented reality (AR) to the Internet of Things (IoT), new developments in IT are remaking processes and improving outcomes in many business sectors. This is typically referred to as digital transformation (DX).

In OT networks, which control critical infrastructures such as pipelines, electric grids, transportation systems, and manufacturing plants, change is coming more slowly. OT environments are vital to public safety and global economic well-being. They were developed decades before IT networks and have different vendors and proprietary protocols. There was little reason to connect OT and IT networks at first, especially because doing so increases the risk of cyberattacks.

However, three-quarters of OT organizations in a recent survey reveal they have made, at least, basic connections between IT and OT to boost productivity and cost efficiencies.[1] New digital technologies in OT environments are driving changes big enough to be summed up as the Fourth Industrial Revolution.[2] Sensors are optimizing production lines.[3] Augmented reality glasses are reducing errors for warehouse workers.[4] Gains are significant: Organizations scoring in the top quartile of digital transformation achieved almost twice the margins and profits of the bottom quartile.[5]

DX leaders earn 2x the margins and profits of laggards.

The challenge when integrating IT and OT is that the bigger digital attack surface increases the risk of cyberattacks. Nearly 90% of organizations with OT environments have experienced a breach in their OT networks.[6]

Nearly 90% of OT environments have been breached.

02: Recommended OT Cybersecurity Best Practices

So, how can risks be minimized while enabling gains to be maximized? The following are five areas OT leaders need to have checked in order to protect against malicious cyberattacks.

1. Identify Assets, Classify, and Prioritize Value

Improving security posture starts with visibility: you cannot protect what you cannot see. Lack of visibility is a critical security gap at many organizations, with 82% acknowledging they are unable to identify all the devices connected to their networks.[7]

Security teams need an up-to-date inventory of devices and applications running on the network. One challenge is that many OT networks cannot be actively scanned with the methods used for an IT network. An active scan can interfere with network performance or damage OT elements such as PLCs.[8]

Security teams should consider contacting a vendor or technology partner to conduct a threat assessment. This assessment sometimes uses a system such as a next-generation firewall (NGFW) that can recognize OT application protocols and passively observe network traffic, including encrypted traffic. The system uses the information it collects to profile and categorize devices on your network based on their characteristics and behavior. The result is a report that:

- Provides an inventory of connected devices
- Notes high-risk applications
- Detects and identifies top exploits of application vulnerabilities
- Assesses the risk value of each asset
- Identifies indications of malware, botnets, and devices that may be compromised
- Categorizes applications and analyzes their network usage

This information serves as a good foundation for prioritizing risks and optimizing a security plan.

72%

cannot identify all devices on their networks.

A complementary threat assessment can map your network.

2. Segment the Network

Network segmentation is one of the most effective architectural concepts for protecting OT environments.[9]

The idea is to divide the network into a series of functional segments or "zones" (which may include subzones, or microsegments), and make each zone accessible only by authorized devices, applications, and users. A firewall defines and enforces the zones, and it also defines conduits, which are channels that enable essential data and applications to cross from one zone to another.

- **Restrict an attacker's ability to move within the network.**
- **Strict access controls limit access to each zone.**

The architectural model of zones and conduits greatly reduces the risk of intrusion. It restricts an attacker's ability to move in an "east-west" or lateral direction. Users or devices authorized for a specific activity in a specific zone are limited to functioning properly within that zone.

Segmentation is a fundamental best practice for securing OT, as described in ISA/IEC-62443 (formerly ISA-99) security standards.[10] These were created by the International Society of Automation (ISA) as ISA-99 and later renumbered 62443 to align with the corresponding International Electrotechnical Commission (IEC) standards.

ISA/IEC-62443 standards provide practical guidance on how to segment OT networks. Each zone is assigned a security level from 0 to 4, with 0 representing the lowest level of security and 4 the highest. Strict access controls limit access to each zone and conduit based on the authenticated identity of the user or device.

Security teams should consider a firewall with purpose-built security processors, designed to accelerate specific parts of the packet processing and content scanning functions, compared to the general CPUs found in many firewalls. Purpose-built security processors enable high-speed cryptography and content inspection services without degrading network performance. This is important in keeping zones and conduits from becoming bottlenecks.

3. Analyze Traffic for Threats and Vulnerabilities

Once NGFWs divide an OT network into segments and conduits, it is valuable to analyze network traffic for known and unknown threats.

Security teams should seek to integrate an NGFW capable of inspecting encrypted application traffic. Additionally, the NGFW should be integrated with a live-feed service to provide updates on the most common OT protocols and OT application vulnerabilities. A service of this type enables the NGFW to inspect OT application traffic and spot exploits. Real-time global intelligence alerts update the firewall so it can identify even new and sophisticated threats. When integrated with a compatible endpoint security solution, the NGFW can monitor endpoints for indicators of compromise (IOCs) gleaned from a variety of sources around the globe.

The firewall can also learn from traffic on a network and establish a baseline or understanding of what is normal or abnormal across IT and OT systems. It can quarantine, block, or send alerts when it detects abnormal activity or IOCs. Integrated as part of the NGFWs, AI capabilities, which are delivered as part of a self-evolving threat intelligence system, develop signatures to catch zero-day threats before they are even written.

To make threat hunting and compliance reporting easier, security teams should add a security information and event manager (SIEM) that can correlate data from point security solutions and device logs across IT and OT networks. The optimal approach is integrating a SIEM that can map a real-time topology of the network and track and record security events. Such an approach yields correlation of information from different solutions to deliver context, minimize response time, and simplify reporting.

- **A security rating score quantifies security performance.**
- **A live global feed provides updates on application vulnerabilities.**

A security rating score, delivered as part of a threat intelligence feed bundle, is needed to quantify security performance and enable comparison of an organization's security posture against industry peers. This is valuable for compliance reporting and answering queries from senior leadership about security effectiveness.

45%

do not monitor accounts with high-level access.

4. Control Identity and Access Management

Stolen credentials are an element of many OT cyberattacks, including three of the four profiled earlier. Spear phishing used to steal credentials was a key part of those attacks. In fact, two-thirds of installed malware in the threat environment is being delivered by email.[11] A first layer of defense in controlling identity and access management (IAM) exploits should be a secure email gateway with signature- and reputation-based prevention.

45% of OT organizations do not use role-based access control.

Another common access-control vulnerability is based on the fact that 45% of OT respondents surveyed do not use privileged identity management for administrators, allowing organizations to monitor high-level accounts in their IT environments.[12] This increases the risk of damage from stolen administrator credentials, a coveted target for many attackers.

Another 45% of OT organizations do not use role-based access control for employees, increasing the risk of insider threats,[13] though most organizations say they do have plans to adopt these technologies.[14] Security teams should seek an IAM solution that:

- Enforces role-based access for each user, limiting access through integration with the firewall to only appropriate resources and network microsegment
- Validates identity with multi-factor authentication, combining something the user knows (such as username and password) with something the user has, such as a phone, laptop certificate, or physical security key, or something the user is, such as a fingerprint or other biometric
- Enables single sign-on (SSO), saving time by enforcing enterprise user identity-based security without requiring additional sign-on screens
- Authenticates devices attached to the network by observing their characteristics and behavior and noting the need for software updates to patch vulnerabilities
- Restricts access to only authenticated devices, locking down all other ports

5. Secure Both Wired and Wireless Access

In an OT environment, two attractive targets for cyberattacks are network switches and wireless access points (APs). Both should have security by design, administered from one central interface, instead of being protected by add-on point security solutions managed through multiple interfaces.

Security management that is centralized not only reduces risk but it also improves visibility and minimizes administration time for security and operations teams.

In many OT companies, exposure to potential attacks through wired and wireless APs is growing. Every company in one survey had some wireless or IoT technologies, which may include connections to OT networks.[15] An average of 4.7 IoT technologies were connected, with GPS tracking and security sensors the top two choices.[16]

Increased risk exposure can be minimized by choosing a firewall that is part of a holistic security platform. The platform enables administrators to centrally push out granular security policies to integrated switches and wireless APs and control customized VLANs for different groups of employees and equipment. This type of firewall also enables centralized provisioning and management of popular legacy switches and wireless APs from third-party vendors.

Centralized security management for access points reduces risk.

Another distinct feature to consider in firewalls, switches, and wireless APs is a ruggedized form factor, enabling deployment in the extreme conditions of field sites found in OT, such as an electrical grid, oil pipeline, or other distributed system. The devices should be designed to function in the hottest and coldest places on earth. They should support centrally created security policies at the far edges of the network, where threat actors are likely to attack because they expect less security. A failure of equipment at the network edge is not just an annoyance; it can mean costly critical downtime and time-sensitive deployment to resolve the equipment failure.

A holistic security platform can push out customized VLANs globally.

Conclusion: Proactively Limit Risk in OT Networks

To stay competitive, organizations are connecting OT environments to their IT networks. In most instances, IT and OT convergence is planned and strategic to an organization. It is also possible that integration exists that was not planned or even known. For example, Project SHINE (SHodan INtelligence Extraction), which consists of a multiyear global scan of the internet, identified 2 million connected OT devices (including infrastructure supporting OT control devices, such as HVAC controllers and serial converters).[17]

While IT and OT integration is becoming a strategic initiative, it is also increasing the likelihood of OT breaches. Experience suggests that a cybersecurity breach is less a matter of “if” than “when.” While breaches cannot be stopped 100% of the time, they can be limited through network segmentation, detected faster through traffic analysis, and minimized in frequency through identity and access management, and wired and wireless access control. Following these best practices can greatly reduce the cost and potential downtime if an attacker is able to get a foothold in an OT network.

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

[2] The first three industrial revolutions were 1) a change from muscle to steam power in the 18th century, from steam to electrical assembly lines in the 20th, and the rise of automation early in the 21st. Bernard Marr, "What is Industry 4.0? Here's A Super Easy Explanation For Anyone," Forbes, September 2, 2018.

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

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

[5] Robert Bock, et al., "What the Companies on the Right Side of the Digital Business Divide Have in Common," Harvard Business Review, January 31, 2017.

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

[7] Jeff Goldman, "IoT Security Fail: 82 Percent of Companies Can't Identify All Network-Connected Devices," eSecurity Planet, November 8, 2017

[8] Kyle Coffey, et al., "Vulnerability Analysis of Network Scanning on SCADA Systems," Hindawi, March 13, 2018.

[9] Keith Stouffer, et al., "Guide to Industrial Control Systems (ICS) Security," NIST, May 2015.

[10] "ISA Standards: Numerical Order," International Society of Automation, accessed January 3, 2018.

[11] David Finger, "Provide Customers with Advanced Threat Defense Against Email-Based Attacks," Fortinet, April 26, 2018.

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

[13] Ibid.

[14] Ibid.

[15] Ibid.

[16] Ibid.

[17] Taylor Armerding, "Critical infrastructure: Off the web, out of danger?" CIO, March 22, 1017.

www.softwerx.com   www.fortinet.com

358609 -0-0-EN

February 28, 2019 1:54 PM

eb-converged-it-and-ot