FORTINET

POINT OF VIEW

Industrial Networks Require Trailblazing OT Cybersecurity

Purpose-Built and Protocol-Driven Threat Protection for Industrial Control Systems

Executive Summary

Production and personnel safety are critical in industrial control systems (ICS). Industrial networks include IT servers and unique, protocol-driven operational technology (OT) devices. OT security solutions must be customized to be effective in the vast industrial communication protocol environment. Thus, security solutions for OT must be protocol-driven, and protocol communication must be analyzed to identify malicious threats.

Also, the best OT cybersecurity should be able to analyze application control parameters to further expose threats in industrial networks. Trailblazing industrial cybersecurity services need to continuously receive deep and timely updates to stay ahead of attackers.

Increasing Attacks on Already Vulnerable OT Networks

In addition to the increase in the complexity, production risks, and safety issues in industrial networks, cyberattacks are also on the rise. These attacks include ransomware, intellectual property (IP) theft, and nation-state infiltrations. Compounding the security challenges, industrial organizations struggle with inadequate resources, training, and remote work complications.

In a recent survey, close to 50% of respondents suffered an operational outage that affected productivity, while more than 33% saw revenue, data loss, compliance, and brand-value impacts—and even threats to physical safety.[1]

Additionally, most industrial networks in the installed base don’t have cybersecurity included because they were built before they needed to connect to the internet—or were unconnected (air-gapped) from traditional networks due to safety and production concerns. Another issue is that immature industrial networks are flat or unsegmented, allowing easy access and lateral movement within the network by malicious actors. Combined, sophisticated, and plentiful industrial adversaries and a lack of mature industrial security solutions pose considerable challenges to organizations trying to secure their OT networks properly.

OT asset identification and communication control are becoming more standard. More advanced protection requires malicious intrusion prevention via vulnerability signature identification and application-specific policies and rules, including parameters and commands among OT devices.

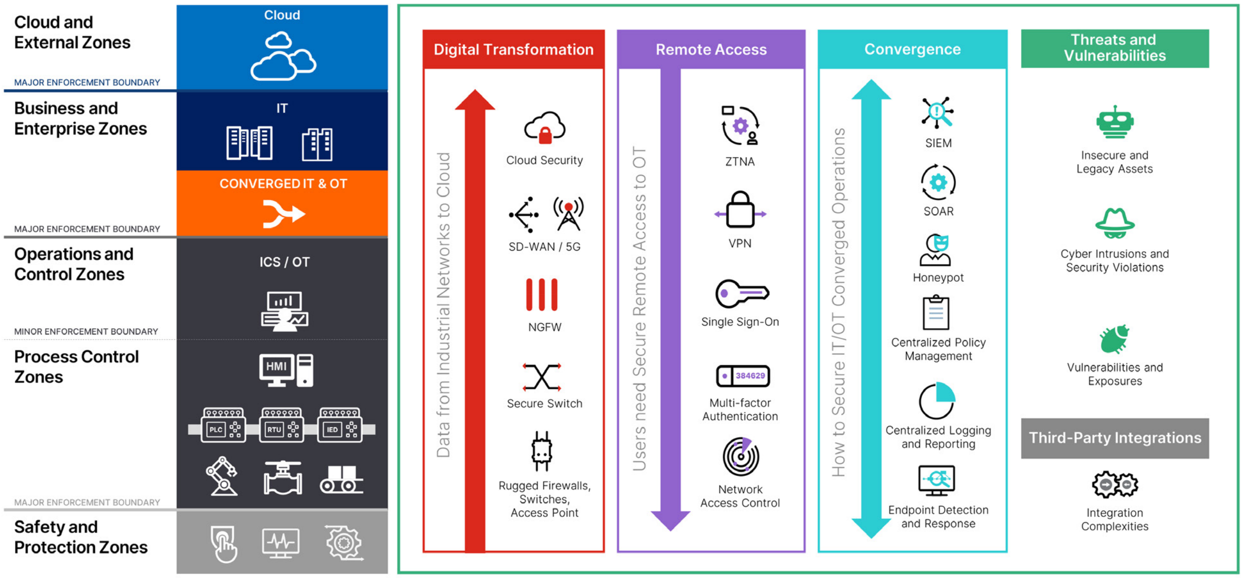
Cloud and External Zones
Cloud
MAJOR ENFORCEMENT BOUNDARY
Business and Enterprise Zones
IT
CONVERGED IT & OT
MAJOR ENFORCEMENT BOUNDARY
Operations and Control Zones
ICS / OT
MINOR ENFORCEMENT BOUNDARY
Process Control Zones
HMI
PLC
RTU
IED
MAJOR ENFORCEMENT BOUNDARY
Safety and Protection Zones
Digital Transformation
Data from Industrial Networks to Cloud
Cloud Security
SD-WAN / 5G
NGFW
Secure Switch
Rugged Firewalls, Switches, Access Point
Remote Access
Users need Secure Remote Access to OT
ZTNA
VPN
Single Sign-On
384629
Multi-factor Authentication
Network Access Control
Convergence
How to Secure IT/OT Converged Operations
SIEM
SOAR
Honeypot
Centralized Policy Management
Centralized Logging and Reporting
Endpoint Detection and Response
Threats and Vulnerabilities
Insecure and Legacy Assets
Cyber Intrusions and Security Violations
Vulnerabilities and Exposures
Third-Party Integrations
Integration Complexities

Figure 1: Security Fabric: Operational Technology

Network Vulnerability Is Also a Product of Timing

The signatures used to protect industrial networks can be created by institutions, security vendors, and individual security researchers. The time between discovering and deploying a signature that can detect and block malicious traffic is critical. Consequently, it is equally important to understand how these services are updated and by whom. Factors to consider include personnel, geography, sensor networks, alliances, and the effectiveness and efficiency of the signatures.

Typically, threats are mitigated by patches. However, historically, patching was delayed or dismissed due to production priorities and the perception that industrial networks were not a cyber target. Therefore, too many OT devices remain unpatched and vulnerable to attack.

Rapidly Maturing OT/ICS Solutions

Securing ICS, conceptually, can follow many IT best practices. However, the security solutions and devices differ significantly in deployment, technology, and reliability. Tactically, ICS is much different from deploying traditional IT security solutions. Organizational security policies or the implementation of security frameworks must be adapted or modified to accommodate the unique requirements of the industrial networks.

More than 90% of organizations that were attacked disclosed the incident to shareholders and authorities and reported that the impact was substantial in 49% of the cases.[2]

Basic security controls consist of device and software inventories and flat network segmentation. Advanced controls manage and monitor the ICS network communication traffic. Using passive deep packet inspection (DPI), firewalls examine the ICS communication traffic and can identify communication errors. Passive inspection is necessary to maintain sensitive industrial processes' stability.

Next-Generation Firewall

In addition to a firewall, an intrusion detection system (IDS) can identify malicious communication packets by comparing packet contents against known malicious threat signatures. Going further, an intrusion prevention system (IPS) can identify malicious packets and then take action to block the threat. The combination of a firewall with an IPS system is called a next-generation firewall (NGFW).

NGFWs for ICS networks must be able to inspect industrial protocol traffic. Likewise, the signatures used for IPS must be explicitly created to identify malicious industrial activity different from IT malicious traffic.

Another advanced control that mimics traditional IT practices is application control. Here again, ICS apps are separate and distinct from the equivalent in the IT environments. Thus, signatures are used to control application commands, and parameters must be designed for OT protocol and device applications.

In short, traditional security principles can be implemented in ICS networks with purpose-built industrial control devices. Industrial NGFWs and industrial protocol-driven IPS signatures and application controls provide the unique solutions necessary in industrial networks.

66% of industrial organizations delay, don't at all, or don't know regarding patch deployment on OT devices.[3]

ICS Solutions Need to Be Powered by ICS Research

Deploying ICS security devices like NGFWs is a critical advanced control in OT networks. The library of malicious signatures used by the IPS in NGFWs is just as important. Regarding signature libraries, several key factors need to be considered to gauge the effectiveness of those signatures, such as:

- How is threat intelligence being collected?
- How are signatures created?
- How quickly are they created?
- What types of signatures?
- How many external sources are being leveraged?
- How efficient or effective are the signatures?

These are critical questions in determining the security service's width, breadth, and timing as part of an NGFW. And because IT is different from OT/ICS, the above considerations need to be asked and evaluated in the context of dedicated OT/ICS threat research and analysis. The uniqueness of ICS systems dictates that the teams supporting ICS security services are ICS professionals.

How are patches and updates handled on your critical control systems assets?
Select the most applicable method.

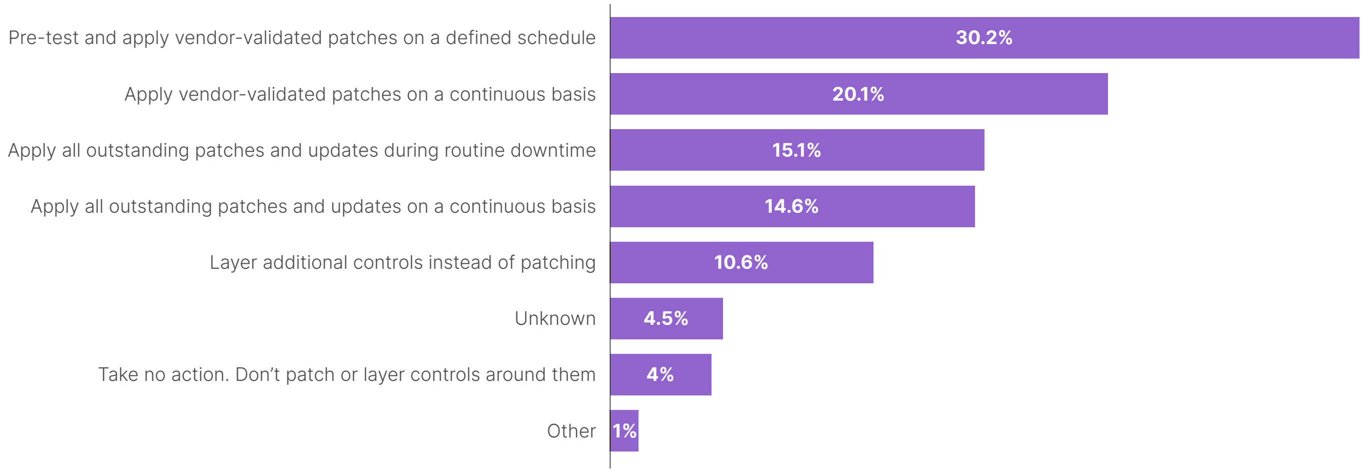

Figure 2: Handling of patches and updates[4]

A Final Consideration

The ability of the security service to identify, validate, and deploy signatures for zero-day vulnerabilities is vital. Zero-day vulnerabilities are undiscovered threats found via research or as a result of post-attack analysis. Until discovered, these vulnerabilities are used by attackers to penetrate secure networks. Thus, the discovery, management, and creation of signature libraries are essential for providing continuous real-time protection of ICS networks.

Conclusion

Industrial control systems, including manufacturing, critical infrastructure, SCADA (supervisory control and data acquisition), and DCSs (distributed control systems), are a growing target for cybercriminals. Standard IT security principles can be used to defend OT networks, but devices, software, and research must be purpose-built and maintained by dedicated OT vendors and professionals. Advanced ICS controls such as NGFWs and robust ICS/OT research teams are critical considerations in providing additional security.

[1] 2022 State of Operational Technology and Cybersecurity Report, Fortinet, June 21, 2022.

[2] Survey Results Reveal Resilience of Industrial Organizations in Face of Ongoing Disruptions, The Claroty Team, February 3, 2022.

[3] Dean Parsons, A SANS 2022 Survey: OT/ICS Cybersecurity, SANS, October 2022.

[4] Ibid.

www.fortinet.com

December 7, 2022 12:34 PM

1837816-0-0-EN