FORTINET softwerx

OT Network Security Starts with Visibility

Greater Transparency for Industrial and Critical Infrastructure Networks

Table of Contents

Executive Overview

Operational technology (OT) systems control industrial and critical infrastructure in sectors such as energy, utilities, manufacturing, communications, transportation, and defense. As all industries increasingly adopt a wide spectrum of new digital technologies, OT networks are increasingly intersecting with internet-connected information technology (IT) networks. This overlap means that the ever-expanding IT attack surface now exposes previously isolated OT systems to the full assortment of IT-based threats. Because traditional security strategies were not designed for the unique and sensitive needs of OT, network operations analysts must seek out protection that provides visibility, control, and situational awareness across these environments.

01: Defending an Expanding OT Network Attack Surface

Until recently, the best way to protect OT networks was to keep them completely isolated from IT—a process known as "air gapping." But today, nearly three-quarters of businesses report at least basic connections between IT and OT.[1] This convergence eliminates the de facto security of the air gap against common internet-borne threats.

In the face of defending OT against an infinitely more expansive attack surface and a rising tide of sophisticated threats, network operations analysts are under tremendous pressure to simultaneously maintain security, operational uptime, and safety in these environments. As a result, they must rethink how their OT networks are secured.

Three-quarters of businesses report at least basic connections between their IT and OT environments.

97%

of organizations acknowledge security challenges because of the convergence of traditional IT and OT. [2]

02: Finding a New Solution for OT Security

In light of OT and IT convergence, an evolved and effective OT security posture requires some specialized considerations. Attempts to address risk by simply deploying off-the-shelf firewalls, sandboxes, and intrusion prevention systems into OT environments present unacceptable, disruptive, and uncertain outcomes. OT security tools need to be purpose-built to align with the protocols, communications, and services that are native to these delicate environments.

Rather than bolting isolated point solutions onto the network to cover newly exposed defensive gaps, organizations need to design security into the most basic levels of OT environments to address the bigger picture. The various parts of the organization's security infrastructure need to work together as a cohesive and coordinated system.

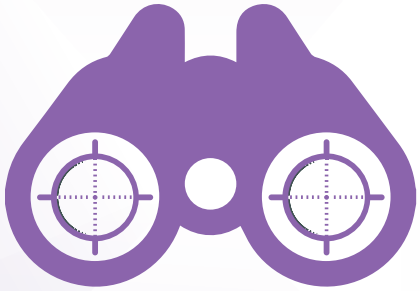
An integrated, segmented, and layered security architecture offers one such approach. This type of end-to-end security enables protection beyond merely locking down a connected HVAC system that shows signs of compromise. Integrated security can provide transparent visibility of all devices, real-time analytics for contextual awareness as well as policy-based controls that ensure device or system integrity while safeguarding the other critical parts of an OT environment.

About two-thirds (65%) of OT companies lack role-based access control, giving attackers greater freedom to move within their OT environments.[3]

03: Visibility Across the Attack Surface

Today, ensuring reliable OT operations requires maintaining continuous visibility of every device (both wired and wireless) within the environment as devices join, leave, or move from one location to another. It is now very common for a broad assortment of wireless and Internet-of-Things (IoT) devices (such as smart environmental controls) to be deployed in OT environments. However, since these technologies connect to an outside IT network for additional capabilities, they offer a potential backdoor for threats to attack vulnerable OT systems.

An integrated security architecture can support transparent, centralized visibility of the entire OT environment. To help enable this kind of interlinked protection, the security architecture should include prebuilt application programming interface (API) connections and open REST APIs. Organizations, as a result, can connect existing security solutions to the security ecosystem. Establishing visibility may also include the adoption of solutions such as **network access controls (NACs)** to help with passive inventory and management of IoT devices as well as other endpoints (without disrupting sensitive OT systems).



You cannot protect what you cannot see. 82% of organizations are not able to identify all the devices connected to their network.[4]

04: Control Access, Security Updates, and More

Control in OT entails baselining normal traffic and predefining approved functions that yield recognition and real-time responses to any behavior that is out of scope. Fortunately, device behaviors within an OT environment tend to be static and within a predictable range, so anomalous behaviors are more likely to be immediately apparent and identified than in traditional IT environments.

Control solutions should include switching, segmentation of the network (north-south and east-west), and micro-segmentation of assets on the network. Being able to force traffic from primitive devices through a next-generation firewall solution is another critical capability needed within OT environments.

Organizations must be able to apply and enforce access policies based on who and what is connected to the network. Dynamic, role-based controls establish segments within the network that group applications, link data, and limit access to specific groups to fortify OT security. This type of fine-grained control is sometimes referred to as **intent-based segmentation**—adjusting access control based on continuous trust assessment.[5]

In the past, access controls assumed static trust values for users, devices, and applications. But trustworthiness can fluctuate due to normal changes in business operations or as a result of emerging threats. Intent-based segmentation links access control to continuously updated trust levels based on information acquired from both internal and external sources.

Intent-based segmentation establishes "where, how, and what" to control device and user access to assets based on established business needs.

05: Situational Awareness

Network operations analysts may receive thousands of security alerts each day. After notification of suspicious activity on a specific IP address, it may take hours of investigation to manually track down the location of a suspect device and all the other relevant information surrounding the event to determine whether this is an actual attack or just an anomaly. Limited staffing resources only compound these problems.

When an individual device in an OT environment is attacked, organizations need instantaneous alerts and contextual threat information in order to quickly understand what precise actions to take. A solution that provides security information and event management (SIEM) capabilities can provide unified event correlation and risk management to help expedite analysis, automate responses, and accelerate remediation.

If a suspicious device trying to access the network is detected, an integrated NAC solution can send automated threat notifications to the network operations analyst for review, along with relevant, real-time contextual information about the event to enhance the fidelity of the alert. This helps network operations analysts quickly locate and resolve threats—reducing containment time from days to seconds.

Nearly two-thirds (64%) of OT leaders say that keeping pace with change is their biggest challenge, and almost half (45%) are limited by a shortage of skilled labor.[6]

06: Greater Transparency for Industrial and Critical Infrastructure Networks

Protecting the expanding attack surface of OT without disrupting sensitive systems presents challenges. While the convergence of OT and IT offers great benefits, it also introduces new risks that may be unfamiliar to network operations analysts and security teams.

Organizations must be able to ensure they know everyone and everything connecting to their infrastructure at all times. OT now requires comprehensive transparency—visibility of everything connected to the OT network at all times. They need centralized management and compensating controls (e.g., SIEM, NAC) as well as endpoint protection and network segmentation. And they need an integrated security architecture that connects the various solutions into a cohesive, defensive architecture that can help protect OT from a full spectrum of IT-based threats.

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

[2] Ibid.

[3] "State of Operational Technology and Cybersecurity Report," Fortinet, March 2019.

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

[5] "A Network Operations Guide for Intent-based Segmentation," Fortinet, February 5, 2019.

[6] "State of Operational Technology and Cybersecurity Report," Fortinet, March 2019.

www.softwerx.com www.fortinet.com

360444-0-0-EN

May 15, 2019 11:52 AM

eb-network-operations-analyst