FORTINET

What Is an OT Security Platform?

Table of Contents

Executive Overview

Today, organizations must understand the similarities and differences between their information technology (IT) and operational technology (OT) networks and the measures needed to protect OT. OT technology controls processes that have safety and physical impacts, including equipment in manufacturing plants, power stations, pipelines, railways, and other cyber-physical systems (CPS). OT technology is critical to public safety and global economic health, so implementing advanced, unified security capabilities that are simple to deploy and manage is paramount.

Fortinet secures the interconnected IT and OT infrastructure while fully enabling integration through an OT security platform, which spans solutions and supports security automation across the entire security ecosystem.

Nearly 80% of professionals surveyed by Fortinet reported at least one cyber incident in their OT environment over the past year.[1]

IT and OT Network Convergence

OT networks include industrial control systems (ICSs) that control equipment in industrial sectors such as manufacturing, energy and utilities, and transportation. ICSs were deployed decades before IT networks and were at first analog and proprietary, with little or no connectivity to IT or external networks. This lack of connection, called the "air gap," between networks protected OT networks, and they were deemed "safe" because of their relative isolation.

As more processes were digitized, the traditional boundaries between IT and OT networks broke down. The Internet of Things, Industrial Internet of Things (IIoT), cloud computing, artificial intelligence, and other innovations converged IT and OT networks to optimize operations, improve safety and reliability, and deliver a competitive edge. These changes have transformed ICS into CPSs, an all-encompassing term from Gartner.[2]

The improved agility and efficiency that come from IT/OT convergence and CPS also come with increased risks to the business. The diminishing presence of the air gap between OT and IT networks means OT infrastructure is now subject to the threats typically faced in IT systems and OT-specific malware threats designed to damage or shut down critical systems. Attacks on OT systems can compromise industrial processes and equipment or critical infrastructure, which can lead to dire health and safety consequences if the systems are breached. As a result, OT and CPS networks have become attractive targets for nation-state advanced persistent threat groups looking to inflict maximum damage to an adversary. The security to protect IT/OT converged infrastructure must also transform to protect against evolving cyberthreats.

Real Cyberthreats to OT

Because OT has traditionally been isolated, cybersecurity is not top of mind at many organizations, and basic cybersecurity hygiene is not implemented within many OT environments. To adopt best practices, safety and cybersecurity must be systemic throughout an organization.

Nation-states can inflict global damage through spear phishing, compromised endpoints, and stolen credentials. The prevalence of these types of attacks underscores the necessity of two-factor authentication, employee security education, and continuous system monitoring for indicators of compromise.

Attackers are gaining expertise in penetrating OT networks. A successful attack can result in loss of intellectual property, trade secrets, and, in the worst cases, industrial sabotage. Attackers are developing, selling, and buying specialized toolsets designed to penetrate OT protocols and equipment.

The cultural gap between IT and OT generates safety and security risks within organizations. Organizations with connected IT and OT networks that are not properly divided with cybersecurity controls are especially susceptible to successful cyberattacks.

Segmentation is not commonplace within OT environments, and lack of segmentation particularly between IT and OT networks is often exploited. In addition, IT malware like ransomware and worms are making their way into OT networks and traversing laterally because there is no additional segmentation in the lower levels of the OT network to slow them down or prevent attacks on critical OT systems.

The consequences of an OT breach can be catastrophic and widespread. A single stolen password allowed for a successful ransomware attack against Colonial Pipeline, disrupting fuel supplies to the entire southeastern United States. As CISA states, the breach was a "watershed moment in the short but turbulent history of cybersecurity. On May 7, 2021, a ransomware attack on Colonial Pipeline captured headlines around the world with pictures of snaking lines of cars at gas stations across the eastern seaboard and panicked Americans filling bags with fuel, fearful of not being able to get to work or get their kids to school. This was the moment when the vulnerability of our highly connected society became a nationwide reality and a kitchen table issue."[3]

Gartner states: "Overall interest in CPS security (and particularly OT security) is growing as seen not only in Gartner surveys but also in Gartner client inquiry trends. This is driven by threat actors (in some cases, with nation-state involvement) increasingly targeting critical infrastructures and industrial systems, as well as by enterprises' attack surface expanding due to digital transformation initiatives. Meanwhile, compliance requirements have also been increasing, such as those related to the planned EU's NIS2 Directive and Cyber Resilience Act and the U.S.'s updated NIST Cybersecurity Framework."[4]

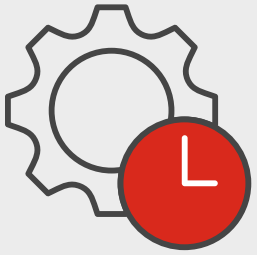
OT Security Platform: An Extension of the Fortinet Security Fabric

The Fortinet OT Security Platform is an extension of the Fortinet Security Fabric. It is specifically engineered to protect the unique network, communication and devices found in CPS. The OT Security Platform provides network visibility in an OT environment by authenticating and classifying IT, OT, and IIoT devices. Unlike other security solutions, it does this passively through deep packet inspection without active scanning because many OT networks are particularly sensitive and scanning can have a negative effect.

The Fortinet OT Security Platform can identify devices and inspect over 70 of the most common OT protocols, such as Modbus, PROFINET, OPC and more. Many OT devices use these protocols to communicate with one another. Because the Fortinet OT Security Platform supports these protocols, firewalls can see the devices and the network traffic occurring within the devices and protect the operating parameters that control the OT devices. This capability is part of the Fortinet OT Security Service, which also supports “virtual” patching of many OT devices, even devices from vendors that are no longer in business. OT devices can be sensitive, and organizations often are cautious about making changes or disrupting devices because of the risk of causing an operational outage. Still, with Fortinet virtual patching, OT organizations can identify and prevent OT device vulnerabilities.

The integrated OT Security Platform centralizes the correlation of intelligence between security devices and segments. The OT Security Platform can quickly identify anomalous behavior and alert the network operations center or security operations center, improving response.

The OT Security Platform can also automatically wall off potentially compromised devices to contain incidents and respond in a coordinated way. It can also be configured to monitor, detect, and alert without affecting production.



Organizations measure their success in several ways. But “response time to security incidents/return-to-service time” was the top answer overall, and nearly half (46%) of respondents ranked this as a top three success factor in a recent Fortinet survey.[5]

A Unified Solution for IT/OT Environments

Securing an OT environment can seem daunting, but mitigating risks can be accomplished incrementally. Securing any environment is a journey, and it is important to have a destination in mind. In this case, the destination should be an environment optimized to respond to threats across IT and OT.

Deploying best-in-class point security solutions to solve different security challenges is common practice. However, point security solutions often are not integrated and work in silos. As a result, security can become complex, difficult to manage, and prone to gaps. Point solutions also leave asset owners saddled with technical debt. As vendors release upgrades, organizations must make sure their integrations continue to perform as expected. However, a unified platform-based solution like the Fortinet OT Security Platform can simplify management and reduce complexity.

[1] Fortinet, State of Operational Technology and Cybersecurity Report, 2024.

[2] Gartner, Emerging Tech: Top Factors Driving Cyber-Physical Systems Security Growth, Ruggero Contu & Katell Thielemann, April 14, 2024.

[3] Jen Easterly, CISA, The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years, May 7, 2023

[4] Gartner, Emerging Tech: Top Factors Driving Cyber-Physical Systems Security Growth, Ruggero Contu & Katell Thielemann, April 14, 2024.

[5] Fortinet, State of Operational Technology and Cybersecurity Report, 2024.

FORTINET

www.fortinet.com

Copyright © 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

September 16, 2024 7:30 PM / 2857009-0-0-EN