SOLUTION BRIEF

Achieving Full Transparency and Centralized Control in OT Environments

9 out of 10 OT organizations experienced at least one intrusion in the past year and 63% had three or more intrusions.[1]

Executive Summary

The integration of information technology (IT) and operational technology (OT) networks expands the OT attack surface and puts tremendous pressure on network operations to maintain security, uptime, and safety. OT now requires an integrated security infrastructure to provide visibility, control, and contextual awareness of users, devices, and applications—and the pathways they can offer to an ever-expanding array of internet-based threats. The Fortinet Security Fabric offers an end-to-end security architecture for OT environments. It delivers integrated, automated protection through segmentation, network access control (NAC), and security information and event management (SIEM).

The Need for Greater Visibility, Control, and Contextual Awareness

The OT attack surface is quickly expanding. Sensitive systems in critical infrastructure and industrial environments face new risks due to infrastructural changes such as serial OT connections being replaced with digital connections and rapid growth in the number of internet-connected systems and devices.

Despite all these challenges, network operations must maintain operational uptime and safety at all times. And when it comes to cybersecurity, OT environments have historically been neglected because, until recently, an air gap (complete separation from the IT network) kept these systems away from threats. Today, however, malware can attack OT systems through IT connections, which means OT systems are now vulnerable to typical IT exploits such as email phishing campaigns or stolen passwords.[2]

Prioritization of OT security has received a great deal of recent attention. But transposing traditional IT security strategies onto OT is not appropriate for the sensitive—often legacy—systems within these environments. To maintain secure and functional operations, organizations need three critical cybersecurity capabilities:

Visibility

Securing modern OT environments begins with establishing continuous visibility of every asset connected to the network, both wired and wireless. Security must keep track of all connected devices across the organization as they join, leave, or move from one location to another.

Control

To secure OT operations from potential IT-based threats, organizations must be able to apply and enforce access policies based on who and what is connected. Dynamic, role-based controls can group applications, link data, and limit access to specific groups in order to fortify OT defenses. This kind of intent-based segmentation provides fine-grained control that adjusts access based on continuously assessing the trust of devices and users.

Situational awareness

When an individual device in an OT environment is attacked, organizations need instantaneous alerts and contextual threat information to quickly understand what actions to take and where to look. OT security requires unified event correlation and risk management to help expedite analysis, automate responses, and accelerate remediation—especially considering the severe limits of staff resources at most organizations.

An Integrated Security Architecture for OT

The Fortinet Security Fabric connects different security solutions deployed across an OT environment into a coordinated security ecosystem. This integrated security architecture coordinates cyber defenses across an organization to enable end-to-end visibility, control, and situational awareness for protecting OT environments. If a connected device exhibits suspicious behavior, the Security Fabric has both the coverage and the capabilities to quickly spot and resolve the issue.

Within OT environments, the Security Fabric includes Fortinet solutions such as rugged FortiGate Next-Generation Firewalls (NGFWs), secure switching in FortiSwitch (wired) and FortiAP (wireless), FortiClient endpoint device protection, and FortiManager for transparent visibility and centralized management of all devices deployed across the organization.

The Fortinet Security Fabric also helps control access to critical systems without disturbing their operation. Traditionally, access controls assumed unchanging trust values for users, devices, and applications. But in reality, the trustworthiness of users and devices 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.

The leading forms of intrusion in OT organizations are malware (57%) and phishing (58%).[3]

A heavier workload (62%), unfilled positions (38%), and worker burnout (38%) are contributing to the cybersecurity skills gap.[4]

Specifically, Fortinet intent-based segmentation supports dynamic and granular access control that continuously monitors the user's trust level and adapts security policies in accordance. Critical IT assets are isolated to ensure quick detection and prevention of threats using analytics and automation. Powered by physical and virtual FortiGate NGFWs, intent-based segmentation provides end-to-end OT network control for both east-west and north-south traffic.

But security means nothing in OT if it interrupts the operation of critical systems in any way. Over its history, Fortinet has demonstrated its OT expertise through investment in a dedicated OT security architecture. Fortinet solutions are developed by subject-matter experts who understand the particular security and operational needs of these unique environments. The Security Fabric provides a complete architectural solution for end-to-end protection, versus the a la carte approach other vendors take with products and individual services that only address attack vectors one at a time.

Solutions for Deep OT Transparency

Endpoint protection solutions enhance the visibility and control of devices within OT environments. Four elements in the Fortinet Security Fabric play critical roles in endpoint protection.

FortiSIEM

Effective OT security requires both transparency and context to help network operations rapidly triage alerts, track devices, and remediate problems. FortiSIEM delivers multivendor SIEM for comprehensive visibility, correlation, automated responses, and remediation in a single solution to help unburden staff resources while improving breach detection.

FortiClient

FortiClient provides security within OT environments for workstations and connected devices. It delivers critical endpoint protection such as antivirus, anti-malware, anti-exploit, web application firewall (WAF), and web filtering. It also includes a Fabric Agent for endpoint telemetry, connecting FortiClient to FortiGate NGFW security.

FortiEDR

FortiEDR provides transparent visibility across all endpoints. It has an intuitive user interface that gives organizations the ability to manage endpoint policies and remediate infections quickly and easily. In a single agent, FortiEDR combines next-generation antivirus (NGAV) protection, application communication control, virtual patching, and automated endpoint detection and response (EDR) for real-time blocking, threat hunting, and incident response.

FortiNAC

FortiNAC helps protect devices and systems in OT that may lack sufficient built-in security of their own, such as Internet of Things (IoT) and Industrial Internet of Things (IIoT) devices, programmable logic controllers (PLCs), as well as industrial control systems (ICS) and their supervisory control and data acquisition (SCADA) subset systems. In coordination with other Security Fabric solutions, FortiNAC helps secure highly distributed OT networks from threats by detecting endpoints with unpatched vulnerabilities.

For noncritical endpoints, FortiNAC can instantly and automatically remove them from the network until they are sufficiently patched. It can also automatically bring that endpoint back into the network from a central dashboard. In the event of a broad-scale, multivector attack such as a botnet attack or other emergency situation where access must be strictly limited for security reasons, FortiNAC has the ability to lock down the network and not allow new devices to join without manual approval.

Choose Security Designed for OT

Because of OT and IT convergence, network operations must now protect their delicate OT systems from a rising tide of internet-based threats. To support this evolution, the Fortinet Security Fabric provides a foundation of transparent visibility, policy-based controls, and immediate situational awareness that is specifically designed for OT environments.

The Fortinet Security Fabric delivers a unified, integrated security architecture that unlocks automation.

The Security Fabric integrates multiple technologies including segmentation, SIEM, NAC, endpoint protection, switching, and wireless to secure OT networks against pervasive IT-based threats. Network operations should evaluate their current OT security by asking a few basic questions. Does your OT security:

- Leverage an integrated security architecture that connects all parts of the security infrastructure into a cohesive, collective ecosystem?
- Provide greater visibility for OT network discovery to understand the current security posture?
- Discover and categorize IoT and IIoT devices according to associated risk factors like vulnerabilities, security ratings, and even utilization?
- Apply intent-based segmentation to increase resiliency of OT networks?
- Incorporate solutions such as SIEM and NAC to detect suspicious users and devices?
- Operationalize intelligence for real-time situational awareness without disrupting core operations?
- Enable simplified security management from a single pane of glass?
- Account for legacy, aging equipment cybersecurity to maintain uptime and availability requirements?

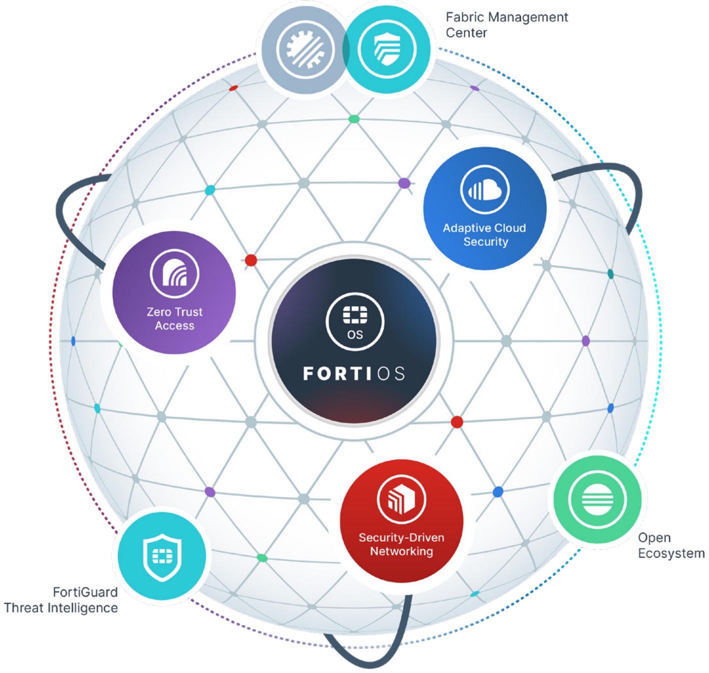

Figure 1: Fortinet Security Fabric diagram.

[1] "2021 State of Operational Technology and Cybersecurity Report," Fortinet, May 26, 2021.

[2] "Ransomware attacks on industrial control systems 2021," CyberTalk.org, June 15, 2021.

[3] "2021 State of Operational Technology and Cybersecurity Report," Fortinet, May 26, 2021.

[4] Hope Reese, "The cybersecurity skills gap persists for the fifth year running," TechRepublic, August 16, 2021.

www.fortinet.com

November 16, 2021 4:55 AM
360483-A-0-EN