

SOLUTION BRIEF

Fortinet Dissolves OT Complexity Through Integration and Automation

Executive Overview

The convergence of information technology (IT) and operational technology (OT) has caused security deployments to become much more complex due to the broad addition of isolated point security products. This complexity presents new opportunities for threats to exploit. The Fortinet Security Fabric offers network operations analysts purpose-built protection that simplifies infrastructure while improving OT defenses. The integrated Security Fabric architecture supports comprehensive visibility and control across OT environments while streamlining burdensome tasks associated with compliance auditing and reporting.

Convergence with IT Makes OT Environments More Complex

Greater connectivity with IT and growing OT infrastructural complexity put OT systems at greater risk from internet-based threats. However, security integration converts the complex deployment of disparate products into a cohesive defensive architecture that shares information in real time and provides instant contextual analysis of potential issues across the organization.

This is where the **Fortinet Security Fabric** architecture is the linchpin, providing broad, integrated, and automated protection for OT environments. If a connected OT device exhibits suspicious behavior, the Security Fabric has both the coverage and the capabilities to quickly identify the problem along with the critical information and tools that network operations analysts need to quickly remedy the issue.

The Security Fabric lays a foundation for unified visibility and control at the device level to help network operations teams understand their organizations' overall security posture. It includes automated workflows for compliance auditing and reporting to reduce the burden on limited staff resources. Most importantly, Fortinet offers security that is purpose-built for OT—so that organizations can repel all orders of advanced threats without disturbing sensitive OT systems.

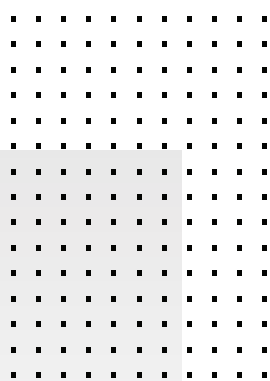
End-to-End Visibility and Control for OT Environments

The foundation of the Fortinet Security Fabric includes **FortiGate** next-generation firewalls (NGFWs), secure switching in **FortiSwitch** (wired) and **FortiAP** (wireless), and **FortiManager** for transparency and centralized management of all devices deployed across the organization. These components provide the foundation of connected security across OT environments—while extending visibility and control via specialized Fabric-connected solutions. The following are some of the core capabilities:

Access management for users

Multi-factor authentication makes the successful use of stolen credentials more difficult,² and yet more than half of OT organizations currently lack this critical protection.³ **FortiAuthenticator** provides services that are key in creating effective security policy, strengthening security by ensuring only the right person at the right time can access the OT environment.

FortiToken multi-factor authentication further helps enforce role-based access. It also supports third-party guest management for wired and wireless network protection. And with **FortiInsight** user and entity behavior analytics (UEBA), organizations can add additional user-level safeguards against insider threats by detecting behavioral anomalies that might signal a threat.



You cannot protect what you cannot see. 82% of organizations are not able to identify all the devices connected to their network.¹



Intent-based segmentation controls

The Fortinet Security Fabric also supports intent-based segmentation to control both east-west (lateral) and north-south (vertical) access to OT systems based on defined business needs—who, what, and where. It uses firewall policies to help network operations analysts limit internal access to sensitive systems by continuously assessing the trust level of users and devices in OT environments.

Device-level control and endpoint protection

The Fortinet network access control (NAC) solution—**FortiNAC**—helps to protect devices and systems in OT that may lack sufficient built-in security of their own.

These include Internet-of-Things (IoT)/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 components, FortiNAC helps secure highly distributed OT networks from threats by all devices on the network. With the latest release (version 8.6), FortiNAC can use all integrated FortiGate NGFWs as a traffic sensor and do passive identification and anomaly detection. Native integration between Fortinet intent-based segmentation and FortiNAC allows for business rules to be extended to device access controls.

Automation and Compliance

Compliance management often involves manual processes done by multiple full-time staff over several months each year. An integrated OT security architecture enables automation in many areas—including compliance auditing and reporting.

FortiAnalyzer automates compliance tracking and reporting of industry regulations and security standards, which is integrated at the network operations layer, for greater workflow efficiency. FortiAnalyzer natively provides the capability of evaluating the network environment against best practices to measure compliance risks. Network operations teams then apply and enforce controls on the network to protect against cyber threats. FortiAnalyzer offers an in-depth analysis of network operations to determine the scope of risk in the attack surface and then identify where immediate response is required. Prebuilt reporting tools provide easy-to-schedule delivery of reports.

FortiAnalyzer can also feed data to security information and event management (SIEM) solutions, such as Fortinet **FortiSIEM**, that are integrated into the Security Fabric. This further enhances compliance capabilities through improved visibility (tracking all devices across the infrastructure in real time) and also context (what devices represent an actual threat) to reduce the noise and false positives that multiple security tools can create.

Choose Security Designed for OT

Fortinet offers OT organizations a robust portfolio of security solutions that are part of the Fortinet Security Fabric. The latter simplifies OT security through transparent visibility across the organization, advanced controls for devices and users, and automated compliance management capabilities. At the same time, it secures delicate OT systems without disruption to maximize operational uptime. By combining purpose-built solutions (e.g., NGFW, segmentation, NAC, UEBA, SIEM) into a cohesive security ecosystem, the Security Fabric can protect OT environments against pervasive IT-based threats.

¹ Jeff Goldman, "IoT Security Fail: 82 Percent of Companies Can't Identify All Network-Connected Devices," eSecurity Planet, November 8, 2017.

² "State of Operational Technology and Cybersecurity Report," Fortinet, March 2019.

³ Ibid.

⁴ Samantha Regan, et al., "Comply & Demand: 2018 Compliance Risk Study," Accenture, March 2018.

Compliance technologies that help better visualize risk are a top spending priority for enterprises—both over the next 12 months (57%) and within the next three years (51%).⁴



www.fortinet.com