SOLUTION BRIEF

Fortinet Security Fabric Integrates OT Security to Unlock Automation and Minimize Complexity

Executive Summary

As operational technology (OT) environments merge with the overall IT infrastructure, more CISOs are taking on responsibility for OT security. Reducing the complexity of securing the merged information technology (IT) and OT infrastructures can significantly improve the CISO's ability to ensure the uptime and availability of OT systems. The Fortinet Security Fabric is a proven solution for CISOs who prioritize clarity, cost-efficiency, and accountability in their security operations. A broad, integrated, and automated framework, the Fortinet Security Fabric provides end-to-end visibility and centralized management to protect OT environments without disrupting critical operations. In addition, automated security analytics and reporting make it easier to demonstrate that OT systems comply with new and evolving regulations and security requirements.

Integration for More Cost-effective Security Coverage

It is estimated that enterprises use an average of 75 different security products.[1] At the same time, in 77% of organizations, these point products are not completely integrated, leaving gaps in security effectiveness.[2]

To help CISOs close these gaps while simplifying their security operations, the Fortinet Security Fabric offers a unified framework that encompasses networks, applications, devices, and endpoints. The Fortinet Security Fabric protects the entire corporate network and reaches across multiple cloud services and the wide area network, to all the edges of the network where wired and wireless OT devices operate. It includes prebuilt application programming interfaces (APIs) for more than 70 Security Fabric-ready partners and REST APIs that enable security organizations to easily and quickly integrate non-Fabric-ready security solutions into the Fortinet Security Fabric architecture.

CISOs and their teams struggle to deal with the complexity of aggregating and reconciling multiple threat feeds. This consumes valuable staff time and slows responses to vulnerabilities and attacks. The Fortinet Security Fabric resolves this complexity by delivering an integrated, continuous feed of threat intelligence that is used to automatically update trusted signatures of the most comment industrial control (ICS) and supervisory control and data acquisition (SCADA) protocols.

The entire Fortinet Security Fabric is visible and controllable from a single pane of glass. This is not a hub-and-spoke platform solution, but a truly interconnected architecture. Every element of the Fortinet Security Fabric communicates with each of the other pieces, automating workflows and threat-intelligence sharing. This minimizes the amount of time overstretched security teams spend on manual processes while shaving threat, intrusion, and breach responses.

Benefits of the Fortinet Security Fabric for OT

- Streamlines security management by integrating disparate security elements
- Minimizes the time and impact of maintaining OT in a safe and available state
- Facilitates compliance reporting through end-to-end visibility and extensive automation
- Helps CISOs better understand and communicate security posture to corporate stakeholders

Customer Experience

A leading North American oil and gas company needed full network access visibility, control, and response to protect 5,000 ICS endpoints across 200 locations. By leveraging the Fortinet Security Fabric, the company avoided the cost of allocating IT staff to manually maintain and update these geographically dispersed systems.

Automated Discovery and Access Control for OT

The first step in securing OT is knowing what devices are connected to the network, what runs on them, and who is using them (if applicable). FortiNAC network access control automates the processes of OT device discovery, profiling, and tagging. This saves staff time and reduces manual configuration errors. Through a variety of protocols, such as Simple Network Management Protocol (SNMP), Command Line Interface (CLI), syslogs, Remote Authentication Dial-In User Service (RADIUS), and various APIs, FortiNAC gathers data from more than 2,000 types of wired and wireless network devices.

The wealth of information that FortiNAC collects during the profiling process enables the creation of tags that reflect business logic, such as the type of device (e.g., a camera, a bring-your-own-device [BYOD] device, or a printer) and the business unit it serves. FortiNAC passes these tags through the Fortinet Security Fabric to FortiGate next-generation firewalls (NGFWs), which use them to perform intent-based segmentation of the internal network and to define access policies. FortiNAC applies these policies to control OT device access, while continually monitoring for new device connections and deviant behavior of existing devices. Upon detecting any deviations, it can immediately change the device's access permissions pending further inspection.

Automated Analysis and Reporting Facilitate Compliance

Pulling logs and reconciling them for compliance and audit tracking and reporting is a significant burden for time-strapped IT teams. Organizations can improve compliance and reporting efficiencies with capabilities built into the operating system that runs on all Fortinet Security Fabric elements. These capabilities align with Payment Card Industry Data Security Standard (PCI DSS) and other regulations. They also help CISOs ensure that their OT devices are compliant with Federal Information Processing Standard (FIPS) 140-2 and Common Criteria Evaluation Assurance Levels (EALs) 4–7.

Additionally, the Fortinet Security Fabric includes elements for security analysis and security information and event management (SIEM). These work together to collect, organize, and correlate data from security devices across IT and OT networks, helping to break down the silos between these operational areas. Mapping the network topology in real time, the SIEM elements track and record security events as they occur, so logs are kept up to date, even when IT teams are shorthanded.

Almost two-thirds of CISOs indicate their threat-intelligence activities and processes are difficult to manage.[3]

FortiNAC can control more than 2,000 wired and wireless network devices. Fortinet is developing APIs for additional products.

"Because we deal in the management and control of critical resources, we needed granular access to firewalls and other security tools to build and maintain a single, unified security posture. That's why we started working with Fortinet."

– Richard Hannah, Vice President of Information Services, Gibson Energy

The Security Rating Service, which is delivered through the Fortinet Security Fabric, quantifies security performance, evaluates the organization's security posture against industry benchmarks, and recommends improvements according to industry best practices.[4] Presented on a dashboard on the central security management console, the Security Rating Service helps CISOs communicate both visually and numerically to a variety of corporate stakeholders the security information that interests them. For example, CISOs can show adherence of OT devices to enterprise security policies, as well as their up-todate industry and regulatory compliance status, based on the latest available information, which is fed through the Security Fabric.

Fortinet: Proven OT Security

For more than a decade, Fortinet cybersecurity has been protecting OT environments in sectors such as energy, defense, manufacturing, food, and transportation. The Fortinet Security Fabric integrates these OT security solutions with best-of-breed threat protection for corporate IT environments that extend from the data center, to the cloud, to the network perimeter. This integration, coupled with automation and built-in support for industry standards, minimizes the complexity and reduces the operational expense (OpEx) of OT security management, when compared to point security solutions in siloed IT and OT environments. With the Fortinet Security Fabric, CISOs have an efficient, nondisruptive way to ensure that the OT environment is protected and compliant.

Fortinet Leadership Evidence: NSS Labs and Gartner

- NSS Labs has given Fortinet solutions "Recommended" ratings across nine different groups of security products.[5]
- Fortinet has been named a Leader in Enterprise Network Firewalls in Gartner's 2018 Magic Quadrant,[6] and as a Leader in Gartner's unified threat management (SMB Multifunction Firewalls) Magic Quadrant.

[1] Kacy Zurkus, "Defense in depth: Stop spending, start consolidating," CSO Online, March 14, 2016.

[2] Patrick E. Spencer, "Cyber Resilience Rises to the Forefront in 2019, According to New Scalar Security Study," Scalar Security Blog Post, February 20, 2019.

[3] Sam Friedman, "Taking cyber risk management to the next level: Lessons learned from the front lines at financial institutions," Deloitte, accessed May 20, 2019.

[4] "Proactive, Actionable Risk Management with the Fortinet Security Rating Service," Fortinet, February 14, 2019.

[5] "Independent Validation of Fortinet Solutions, NSS Labs Real-World Group Tests," Fortinet, April 2019.

[6] "2018 Gartner Magic Quadrant Reports," Fortinet, accessed May 10, 2019.

[7] Ibid.

FORTINET

www.fortinet.com

May 12, 2021 2:43 AM

D:\Fortinet\2021 Rebranded templates\Solution Briefs\May\Refresh\Security Fabric integrates ot security\sb-fortinet-security-fabric-integrates-ot-security-5122021\sb-fortinet-security-fabric-integrates-ot-security-5122021

391455-A-0-EN