FORTINET

WHITE PAPER

Solving OT Security with the Fortinet Security Fabric

Executive Overview

Digitization of operational technology (OT) expands the attack surface and increases risk. Because OT networks consist of devices and systems that are different than those on information technology (IT) networks, traditional security approaches are inadequate in protecting them from the evolving threat landscape. The Fortinet Security Fabric addresses these unique requirements with a security architecture that provides transparent visibility across the entire attack surface and every security element. Additionally, the Security Fabric's integrated security approach unlocks automation capabilities for proactive prevention, detection, and response.

Securing OT Requires a Strategic Approach

With 74% of OT systems breached in just the past year, and half of those reporting three to 10 or more breaches,[1] it is clear that OT systems are inadequately protected. A recent study supports this conclusion, finding that OT companies simply do not have basic security controls in place. For example, 65% of OT companies lack role-based access control, 53% lack internal network segmentation, and 39% do not manage, monitor, or analyze security events.[2] Another survey finds that 82% of OT organizations acknowledge that they are unable to identify all the devices connected to their OT and IT networks.[3]

Given the greatly expanded attack surface brought on by the digitation of OT, it is critical that OT organizations deploy basic security. But this is just a starting point. They must also take a strategic, integrated security approach focused on stopping common attacks, as well as threats targeting OT-specific vulnerabilities.

"Since OT systems often use older technology and security operations that are frequently less developed, the attackers have a higher rate of success there."[4]

"With 74% of OT systems breached in just the past year, and half of those reporting three to 10 or more breaches, it is clear that OT systems are inadequately protected."

Fortinet Addresses the Unique Security Challenges of OT

OT networks and devices present many challenges, starting with the fact that Industrial-Internet-of-Things (IIoT) devices are inherently insecure. In addition, OT systems contain outdated hardware and software, and if they even have security, it is very likely outdated. Even the more up-to-date components of OT networks tend not to be patched regularly, as this may cause unacceptable system downtime.

The traditional approach of largely ignoring the security of OT systems is becoming very dangerous—very quickly. All attack surfaces throughout the OT network must be protected. The complexity, number, and myriad types of devices attached to increasingly distributed IT/OT networks make a holistic security fabric architecture the only viable solution.

To enable the necessary monitoring and protection of all OT devices, even those that are headless, Fortinet delivers:

- High-performance security and networking across the entire IT/OT infrastructure, including cloud deployments
- Shared threat intelligence between each of the security elements for fast response to known and unknown/zero-day threats
- Tight integration of Fortinet security solutions and Fabric-Ready Partners to close security gaps and enable visibility throughout the network

Key Security Fabric Capabilities for OT Security

The Fortinet Security Fabric enables OT organizations to meet these security challenges with a broad, integrated security platform. The Security Fabric scales to meet the expanding attack surface and sophistication of new threats by orchestrating and automating workflows, including threat-intelligence sharing. The different elements contained within the Security Fabric help organizations to address security challenges that are specific to OT environments in various ways:

Defining zones and conduits

Created by the International Society of Automation (ISA) and later renamed to align with the International Electrotechnical Commission (IEC) standard, ISA/IEC-62443 presents practical guidance to address the most pressing vulnerabilities of industrial control systems (ICS). The standard provides practical guidance, including how to segment OT networks with zones and conduits. Security zones are defined as "groups of physical or logical assets that share common security requirements, which have clearly defined borders (physical or logical)." Conduits, on the other hand, are the connections between these zones.[5]

The architectural model of zones and conduits greatly reduces the risk of intrusion and limits damage in the event of a breach. Specifically, once access is gained, it restricts an attacker's ability to move laterally across the network. Users or devices are authorized for a specific activity in a specific zone and are limited to functioning appropriately within that zone. FortiGate next-generation firewalls (NGFWs), which are the backbone of the Security Fabric, enable organizations to define and enforce zones and conduits. With FortiGate NGFWs, strict controls limit who and what can access each zone and conduit, based on the authenticated identity of the user or device.

"Network segmentation is one of the most effective architectural concepts for protecting OT environments."[6]

Fortinet intent-based segmentation, which is powered by FortiGate NGFWs, provides granular access control that continuously monitors trust levels and adapts security policies

Segmenting the network dynamically

Network segmentation must be dynamic because the trustworthiness of users, devices, and applications changes frequently. This may be due to normal changes in business operations or the result of developing threats.

Fortinet intent-based segmentation, which is powered by FortiGate NGFWs, provides granular access control that continuously monitors trust levels and adapts security policies accordingly. OT organizations can intelligently segment network and infrastructure assets regardless of their location, whether on-premises or in multiple clouds. High-performance, advanced security isolates critical assets to ensure quick detection and prevention of threats with the help of analytics and automation capabilities within the Fortinet Security Fabric. Access controls change automatically when trust levels change, which is determined by querying an external continuous trust assessment database.[7]

For traffic within an internal network, the aforementioned zone and conduit strategy and intent-based segmentation capabilities can be enforced by FortiGate internal segmentation firewalls (ISFWs).[8] Whereas perimeter firewalls are focused on defending a border, FortiGate ISFWs sit between two or more points on the internal network and analyze traffic packets. They provide:

- Authentication, user, and device controls
- Intrusion detection and prevention (IDS/IPS) of specific OT-targeted attacks
- Inspection and control for allowed and disallowed applications, including watching OT protocols
- Antivirus/anti-malware protection

Identifying attached devices and implementing role-based access

When it comes to protecting devices, knowledge is power. Security teams cannot protect what they cannot see. Since lack of visibility is cited by 82% of OT organizations as a challenge,[9] the majority of OT organizations have dangerous security gaps. Without an up-to-date inventory of devices and applications running on the network, effective security is impossible.

Visibility is often achieved with active scanning. However, active scanning of network assets is not allowed in many OT environments, as it can disrupt operations. In contrast, however, the Fortinet FortiNAC network access control (NAC) enables passive scanning of network traffic. FortiNAC identifies network users and devices. It then implements appropriate role-based network access policies to protect critical data and sensitive assets. If desired, FortiNAC can also lock down ports to only authorized devices. Plus, for additional control of what devices are being added to the network, any device added to the network can be required to be approved by authorized staff.

FortiNAC uses dynamic role-based network access control to create network segments by grouping applications and like data together, and limiting access to a specific group of users. Further, if a device is compromised, the Security Fabric can trigger an alert that is enforced not only by FortiNAC but also by each of the security elements across the security architecture. This enables rapid, automated threat containment, which results in the quarantining of devices in real time.

Enabling transparency and centralized controls

Once firewalls divide an OT network into zones and conduits, analyzing network traffic for threats is a requisite. This can be achieved by integrating information from the core elements of the Fortinet Security Fabric.

FortiSIEM (security information and event management) automatically discovers everything attached to a network and builds a configuration management database (CMDB). It also builds an auditable traffic record used for proactive risk mitigation. FortiSIEM unites IT and OT data for complete security visibility. This automated correlation is used to open incident tickets for investigation and even automate response and remediation.

FortiManager provides a dashboard view showing up-to-the-minute Security Fabric status, as well as a unified perspective that serves both security operations center (SOC) and network operations center (NOC) teams. SOC teams can see the scope of security alerts and issues, and the NOC team can see if any performance degradations are the result of a security incident. With this insight, the operations team is more likely to understand and readily consent to security team requests to reconfigure or quarantine assets. FortiManager also enables management of firewalls and other security tools from a single location.

FortiAnalyzer automates log management and real-time threat analysis. It leverages an indicators of compromise (IOCs) service from FortiGuard Labs consisting of a daily package of approximately 500,000 IOCs gleaned from a variety of sources around the globe. This helps to identify any communications with servers that have been shown to be malicious. Detected incidents within FortiAnalyzer, combined with detailed evidence and forensics, enable network administrators to determine a resolution as well as trigger automatic changes to device configurations.

Requiring access authentication and control

Multi-factor authentication makes it much more difficult for cyber criminals to use stolen credentials, and yet more than half of OT organizations currently lack this critical protection.[10]

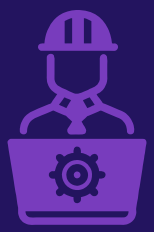
FortiAuthenticator provides services that are key in creating effective security policy, strengthening security with role-based access (ensuring only the right person at the right time can access the OT environment). It also simplifies and centralizes the management and storage of user identity information and applies granular control of access to each zone and conduit, providing integration with Active Directory (AD), RADIUS, LDAP, 802.1X wireless authentication, certificate management, and single sign-on (SSO).

FortiToken multi-factor authentication further helps enforce appropriate access by requiring users to have a software or hardware token in addition to username and password. Even if a cyber criminal has stolen credentials, they should not also have the token and therefore are unable to gain access.

Stopping insider threats

A disgruntled employee has the potential to cause great harm if they decide to attack an OT environment, especially critical infrastructure. Insider security compromises, whether malicious or accidental, occur in very different manners than external attacks. Protecting against them, therefore, requires a very different approach.

FortiInsight is a unique data security and threat detection solution that identifies, responds to, and manages risky behaviors that put business-critical data and OT environments at risk. A hosted solution, FortiInsight leverages user and entity behavior analytics (UEBA) to add additional user-level safeguards against insider threats by detecting behavioral anomalies that might signal a threat.



"When it comes to industrial control systems and operational technology (OT) environments, the insider threat has never been greater or more concerning."[11]

Why Fortinet for OT Security

The Fortinet Security Fabric combines top-rated security and management solutions to deliver the security controls and visibility required resulting from the digitization of OT. With a broad portfolio of network and content security products, plus Fabric-Ready Partners, the entire attack surface is covered by a single security platform. With tight integration, full visibility can be achieved to close security gaps, and threat intelligence can be shared to deliver automated prevention, detection, and response.

In addition to Fortinet's unique Security Fabric approach, OT organizations benefit from Fortinet's vast IT/OT security experience and proven security effectiveness.

[1] "State of Operational Technology and Cybersecurity Report," Fortinet, March 15, 2019.

[2] Ibid.

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

[4] "Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems," Fortinet, May 16, 2019.

[5] "Zones and conduits, protecting our industrial network," INCIBE, June 21, 2018.

[6] Keith Stouffer, et al., "Guide to Industrial Control Systems (ICS) Security," NIST, May 2015.

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

[8] "Protecting Your Network from the Inside-Out: Internal Segmentation Firewall (ISFW)," Fortinet, December 2016.

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

[10] "State of Operational Technology and Cybersecurity Report," Fortinet, March 15, 2019.

[11] Michael Rothschild, "PERSPECTIVE: 3 Ways to Help Secure Industrial Operations from Insider Threats ," Homeland Security Today, November 13, 2018.

September 19, 2019 9:35 AM