SOLUTION BRIEF

Fortinet Secures OT Networks Against Advanced Threats

Executive Summary

Fortinet solutions are designed to enable organizations to secure their operational technology (OT) networks and industrial control systems (ICS) while meeting the high-availability requirements of these environments. Fortinet solutions incorporate strategic security automation and deceptive technologies to expedite detection and remediation of threat actors operating within OT networks. Network segmentation and access control limit an attacker's ability to move laterally through the network, protecting uninfected devices while preserving system availability. OT-specific threat intelligence provided by FortiGuard Labs and Fortinet partners delivers the insight and context required to identify and remediate OT-specific threats.

Introduction

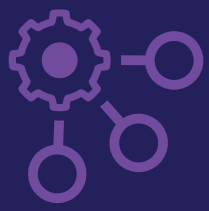
Advanced threat actors are increasingly attempting to gain access to high-value, critical OT systems. Unfortunately, these nonstandard—and often aging—systems are challenging to secure. The Fortinet Security Fabric, leveraging a shared operating system on all Fortinet solutions and an open application programming interface (API) ecosystem, provides full integration and single-pane-of-glass visibility and management of an organization's security infrastructure. Fortinet solutions, with the help of the Fortinet Security Fabric, enable OT network operators to minimize the time to identify, contain, and remediate advanced threats. Specific capabilities include automating threat response, deception technologies, minimizing lateral movement, and threat intelligence.

Automated Threat Response Maximizes OT Availability

OT environments have extremely high availability requirements. Fortinet solutions enable rapid and nondisruptive threat detection and response through strategic security automation, enabling rapid action but leaving the human in charge.

FortiAnalyzer automatically collects log data from across the OT network. It applies machine-learning analytics to the data to extract correlations and indicators of potential threats. This context enables rapid response to minimize the impact of an attacker on the network.

FortiSIEM accomplishes event management for the entire enterprise. By centralizing alert data in a single pane of glass, FortiSIEM provides analysts with full visibility into the current state of the network infrastructure. This supports rapid response to threats to the network.



Automation enables rapid threat detection and remediation, maximizing the availability of OT systems.

FortiSandbox activates suspicious objects in a simulated environment.

FortiDeceptor deceives attackers into compromising intent on a decoy virtual machine (VM).

FortiSOAR offers security orchestration, automation, and response. OT operators can automate processes for responding to common types of security incidents. Once a threat has been identified, automated responses can be initiated by the analyst to remediate the issue while minimizing the impact to operations and system availability.

The Fortinet Security Fabric enables integration of Fortinet solutions and over 350 third-party products. This integration enables these solutions to share threat intelligence and telemetry data and allows for coordinated response to threats across the OT network.

Fortinet also provides endpoint protection designed to meet the high-availability requirements of OT environments.

FortiEDR manages threats on infected endpoints by containing infections at the process level rather than terminating the affected processes. This enables infected systems to maintain operations without placing the rest of the network at risk. FortiEDR initiates automated responses to common threats, based upon playbooks to minimize the impact of security incidents. Additionally, FortiEDR's low memory and CPU requirements enable it to operate on the resource-constrained, aging, and end-of-life systems common in OT networks.

Deception Technologies Trap Advanced Threats

Advanced cyber threats employ sophisticated and targeted attacks to evade traditional threat-detection solutions. Fortinet deception solutions enable OT organizations to identify adversaries that have gained undetected access to their networks.

FortiSandbox emulates systems commonly found in OT network environments so that it can test suspicious objects in quarantine. This enables analysis of OT-specific malware and detection of adversaries operating within the OT network.

FortiDeceptor emulates OT control systems to trick attackers into engaging with these decoy systems. This enables OT network operations to identify internal threats within the network and extract intelligence about the adversary's tools and operations.

Preventing Lateral Movement in OT Networks

Lateral movement within an OT network enables threat actors to infect additional systems and sites connected to the same OT network. Fortinet solutions support internal network visibility, access controls, and policy enforcement to prevent lateral movement of threats through the network.

FortiGate next-generation firewalls (NGFWs) can be deployed within the OT network to create internal segmentation. A database of over 50 OT-specific protocols comprised of 1,750 commands enables FortiGate NGFWs to detect anomalous or malicious OT traffic and prevent a threat in one segment from spreading through the OT network.

Segmentation is a fundamental best practice for securing OT, as described in ISA/IEC-62443 (formerly ISA-99) security standards.[1]

Fortinet solutions easily adapt to OT network protocols, enabling them to identify anomalous or malicious commands sent to OT devices.

Fortinet is consistently recognized as a Leader in the Gartner Magic Quadrant for Enterprise Network Firewalls and achieved the best score in the NGFW Security Value Map from NSS Labs.

Integrated with the FortiGate NGFWs, the **FortiNAC** network access control solution continually monitors the network, automatically identifying all devices connected and attempting to connect to the OT network, and tests their compliance with the organization's security policies. Internal virtual local area networks (VLANs) control traffic flow within the network, limiting the ability of cyber threats to move laterally through the network.

FortiAuthenticator helps secure the lateral movement of both users and devices. It enables multi-factor user authentication and enforcement of role-based access controls. This minimizes the ability of a threat actor to use compromised user account credentials to gain access to OT systems. Through the use of certificates, it also ensures secure machine-to-machine communication.

Threat Intelligence Identifies OT-specific Threats

Fortinet invests continually in understanding and supporting OT-specific protocols, commands, systems, and threats. **FortiGuard Labs** automatically delivers OT-specific real-time threat intelligence directly to Fortinet solutions via the Fortinet Security Fabric.

FortiGuard threat intelligence enables FortiGate NGFWs to virtually patch OT systems against newly discovered vulnerabilities.

The **FortiAnalyzer** logging and reporting solution uses the indicators of compromise (IOCs) provided by FortiGuard Labs to automate contextual analysis. The IOC information includes context regarding the meaning of a particular indicator and its impact to network security, which helps reduce the burden associated with false-positive alerts.

FortiTester offers automated testing against the ATT&CK MITRE framework to simulate the post-compromise behavior of a cyber adversary on an enterprise network.

The Fortinet Fabric-Ready Partner Program is an ecosystem of security and network partners whose solutions integrate with the Fortinet Security Fabric. Intelligence sharing between FortiGuard Labs and these partners accelerates threat detection and response.

Conclusion

OT network operations analysts facing advanced cyber threats need OT security architectures that provide manageable defense in depth. The Fortinet Security Fabric meets this need with broad, integrated, and automated solutions that span OT and IT environments. These solutions enable detection and mitigation of advanced threats, robust analytics and reporting, and single-pane-of-glass visibility and management.

For more information, go to www.fortinet.com/contact to connect with a specialist near you.

Robust Threat Intelligence

FortiGuard Labs, the Fortinet threat intelligence organization, has been active for 15 years. In addition to identifying IT-specific threats, FortiGuard Labs also provides robust intelligence on threats specific to OT systems, and detects zero-day threats using artificial intelligence (AI) and machine learning (ML) techniques.

Fortinet published the industry's first threat report detailing cybersecurity threats and trends unique to OT environments.

[1] "ISA Standards: Numerical Order," International Society of Automation, accessed June 12, 2020.

July 22, 2020 12:11 PM

670238-0-0-EN

D:\Fortinet\Work\2020\July\072220\sb-ot-networks-advanced-threats