SOLUTION BRIEF

Fortinet Provides Zero-day Protection in OT Environments

Executive Summary

Information technology (IT) networks have a wide assortment of security technologies to protect organizations against advanced threats. However, industries that utilize operational technology (OT) systems have many fewer options for cybersecurity defenses. Even more concerning, OT breaches in critical infrastructure (e.g., hydroelectric dams, nuclear power plants, oil and gas pipelines) can have serious consequences that impact the environment and human lives. Network operations analysts need purpose-built security tools for their OT-based systems that are capable of discovering previously unknown malware and attacks without disrupting the potentially sensitive nature of their operations. FortiSandbox and FortiDeceptor support comprehensive OT security—including intelligence sharing for protection against zero-day threats.

About 74% of OT organizations have experienced a malware intrusion in the past 12 months, causing damages to productivity, revenue, brand trust, intellectual property, and physical safety.[1]

OT Environments Are Increasingly Targeted for Attacks

OT environments may include human-machine interfaces (HMI), industrial control systems (ICS) that run equipment or machinery for critical infrastructure, as well as the supervisory control and data acquisition (SCADA) subset systems that provide a graphical user interface for ICS. In many cases, maintaining the continuous uptime of these systems without any disruptions is a requisite for OT network operations teams.

Some of the same threats that target IT networks can be repurposed for attacks against OT as well. For example, a cryptomining infection recently managed to spread to half of all OT workstations at a major international airport in Europe as a result of increasing convergence with IT systems.[2] Unfortunately, network operations analysts for OT environments have not solved some critical issues that their counterparts in IT environments have—such as lateral (east-west) movement of intrusions. To make matters worse, nation-states are increasingly targeting OT-based systems and use sophisticated techniques (e.g., agile development, polymorphism) that make it more difficult to identify, detect, and remediate attacks.

While purpose-built OT security tools—such as segmentation and border protection with SCADA/ICS signatures—offer some basic protections, these defenses are insufficient when it comes to detection and protection against previously unknown (also known as "zero-day") threats.

Zero-day threats need special security attention. Suspicious objects must be detected and safely inspected. Indicators of compromise (IOCs) must be discovered. Then, the aggregated threat intelligence must be pushed to the broader security architecture. To achieve this in OT, network operations analysts need a two-part solution:

- Sandboxing capabilities that inspect objects for malicious intent, including anomalous communications to ICS
- Deception decoys deployed in-network that pose as IP-specific devices—such as a Siemens programmable logic controller (PLC)—in order to trick threats into revealing themselves

Sandboxing and deception solutions complement each other in detecting zero-day threats. To fulfill their role in the kill chain, each must then share detected threat intelligence with an integrated next-generation firewall (NGFW). The NGFW enforces internal network controls (via segmentation) and updates broader OT defenses to block any previously unknown forms of attack.

	FortiSandbox	FortiDeceptor
Goal	Deceive **suspicious object** to run in a simulated environment	Deceive an **attacker** into compromising a decoy VM
Attack Life Cycle/Cyber Kill Chain (Earliest Response)	**Mid-stage:** Blocks exploitation and installation of unknown malware stage	**Early stage:** Redirects reconnaissance and blocks pre-breach attempts
Detection	Captures **malware behavior** to alert on malicious intent	Captures **attacker's behavior** to alert on malicious intent
Response	Share IOCs to provide real-time protection **during breach attempt**	Share IOCs to provide real-time protection **before breach attempt**

Figure 1: Better together—Fortinet sandboxing and deception solutions offer holistic breach protection.

A lack of cybersecurity contributes to risk in OT-based environments—78% of organizations have only partial centralized visibility; 65% lack role-based access control; more than half do not use internal network segmentation.[3]

In 2020, experts predict more attacks against critical infrastructure: botnets mounting distributed denial-of-service (DDoS) attacks against OT networks; attacks on manufacturing systems that use cloud services; supply chain attacks where third-party vendors are compromised as springboards for threat actors to target critical sectors.[4]

Fortinet Solutions for Sandboxing and Deception

Fortinet offers network operations analysts a zero-day threat "tripwire" for detecting and sharing intelligence in real time to prevent attacks in OT environments. These inherently passive technologies are purpose-built for OT environments to avoid disruption to sensitive systems.

FortiSandbox malware protection

As the only vendor that incorporates a SCADA/ICS simulator in the sandboxing process, Fortinet offers malware protection that is unique in the industry. FortiSandbox provides the ability to detect malware-based behavior when malicious code tries to communicate with a SCADA/ICS device. FortiSandbox then generates intelligence to block malicious communication and malware across the broader OT environment via FortiGate NGFWs.

As an integrated part of the Fortinet Security Fabric architecture, FortiSandbox uses three forms of threat intelligence for automated breach detection and prevention. It uses global intelligence about emerging threats around the world via FortiGuard Labs researchers. It also shares local intelligence with both Fortinet and non-Fortinet products across the security infrastructure for real-time situational awareness across the organization. Finally, FortiSandbox applies true artificial intelligence (AI) capabilities—including both static and behavioral analysis—to improve detection efficacy of zero-day threats.

As FortiSandbox employs AI capabilities throughout the entire sandboxing process, this differentiates the solution from other sandboxing solutions: Most sandbox vendors have yet to implement any form of AI, and other solutions that claim to use AI techniques often only apply static analysis. But effective sandboxing AI requires both static and dynamic operations to successfully spot some types of advanced threats.

Certified performance and protection

NSS Labs' Breach Prevention System (BPS) tests focus on detection and blocking of advanced malware, exploits, and evasions. It emphasizes the importance of an automated response cycle (prevent-detect-mitigate) across a number of threat vectors that include web, email, and endpoint exposures. The Fortinet integrated BPS solution (consisting of FortiSandbox, FortiGate, and FortiClient) achieved an overall "Security Effectiveness" of 97.8% and offered the lowest three-year total cost of ownership (TCO) in NSS Labs testing, along with a "Recommended" rating.[5]

FortiSandbox has also been validated and recommended in other respected tests such as ICSA Labs ATD certification[6] and NSS Labs Breach Detection System tests.[7]

FortiDeceptor attack reconnaissance for OT

While FortiSandbox tricks suspicious objects (such as malware) into running within a simulated environment, the Fortinet FortiDeceptor solution deceives attackers into compromising a decoy posing as an OT device. FortiDeceptor provides the ability to detect malicious behavior when an attacker touches a SCADA/ICS decoy. Fortinet is the only vendor offering deception technology with decoys that can simulate both OT (SCADA/ICS devices) and IT (servers, endpoints, IoT devices). FortiDeceptor then sends intelligence to FortiGate NGFWs in order to block the origins of the intrusion—sharing IOCs in real time to disrupt the earliest stage of the attack life cycle.

Malware attacks specifically designed for ICS and SCADA systems continue to appear—and safety systems are now a target.[8]

Top-tier OT organizations are 68% more likely than bottom-tier organizations to manage and monitor security events and perform event analysis, reducing risk from a breach by minimizing the time to detection.[11]

The time from an attacker's first action in an event chain to the initial compromise of an asset is typically measured in minutes, while the time to discovery is more likely to be months.[9] The current time it takes to identify and contain a single breach is an average of 279 days.[10] During this window of exposure, extensive and irreparable financial and reputation damage can occur, not to mention physical safety in the case of hydroelectric dams, nuclear power plants, and oil and gas pipelines, among others. To avoid this situation, network operations analysts can use FortiDeceptor to deploy a network of OT-specific lures to redirect attackers away from valuable assets. This greatly reduces the risk of breaches resulting from unknown threats. FortiDeceptor then analyzes any threat activity and shares information via the Fortinet Security Fabric across all security components to protect the broader OT environment.

Purpose-built Tools for OT Threat Intelligence

Network operations analysts have had limited tools for securing OT environments (including critical infrastructure) against the latest malware and attack strategies. When it comes to detecting and repelling zero-day threats and maintaining critical uptime of systems, Fortinet is uniquely positioned to address the complex intersection of IT and OT environments. Fortinet unifies and automates OT protection against known and unknown threats by integrating sandboxing (FortiSandbox) and deception (FortiDeceptor) solutions with other Fortinet and non-Fortinet security products.

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

[2] Tara Seals, "Major Airport Malware Attack Shines a Light on OT Security," Threatpost, October 18, 2019.

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

[4] Bruce Sussman, "15 Cyber Threat Predictions for 2020," SecureWorld, December 12, 2019.

[5] Jessica Williams, et al., "Breach Prevention Systems Report: Fortinet FortiGate 500E + FortiClient + FortiSandbox," NSS Labs, August 7, 2019.

[6] "Q4 2019 Advanced Threat Defense (ATD) Testing Report," ICSA Labs, January 8, 2020.

[7] "Breach Detection Systems Report: Fortinet FortiSandbox-2000E," NSS Labs, October 19, 2017.

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

[9] "2019 Data Breach Investigations Report," Verizon, 2019.

[10] "2019 Cost of a Data Breach Report," Ponemon Institute and IBM Security, July 2019.

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

February 14, 2020 10:35 AM

560486-0-0-EN

D:\Fortinet\Work\2020\February\021420\sb-zero-day-protection