SOLUTION BRIEF

FortiDeceptor Provides Proactive Intrusion Detection for Healthcare

Executive Summary

As healthcare IT infrastructures become increasingly complex and diverse, security leaders are concerned about maintaining resiliency in the face of cyber threats including ransomware, zero-day attacks that target legacy systems, and lateral attacks. These threats don't just affect IT networks; they can have an impact on interconnected operational technology (OT) networks as well.

Fortinet FortiDeceptor is designed to deceive, expose, and eliminate external and internal threats early in the attack kill chain and proactively block these threats before any significant damage occurs. FortiDeceptor can be used to simulate connected medical devices and OT environments.

For the eleventh year in a row, healthcare continued to incur the highest average breach costs at $9.23 million, an increase of 29.5% compared to 2020.[1]

Using Deception Technology in Healthcare

Healthcare IT environments are becoming increasingly complex and distributed, and organizations need a high-performance, secure network to ensure availability and to deliver uninterrupted, quality patient care.

The Internet of Things (IoT) is pervasive in the healthcare space. Millions of connected medical devices are in use, which represent millions of attack vectors for cyber criminals to target. Many of these devices also were not designed with cybersecurity in mind, which leaves them vulnerable to attack. Cyber criminals are aware of these vulnerabilities and use these devices to enter the network and expand, increasing the number of positions from which they can steal data.

IoT devices are particularly vulnerable to attacker tools that propagate through the network. Many IoT devices may have older embedded operating systems that are closed and not accessible to an IT team. These unpatched operating systems are highly vulnerable to an attacker's malware tools and can be used as a foothold to establish a backdoor into systems. Most endpoint security and internal cyber defense tools cannot be installed on these devices and cannot protect them. Security operations center teams have no visibility into an attacker's presence within these devices.

Deception is a leading cyber defense technology that can be used to secure IoT and connected devices in markets such as healthcare (medical devices), banking (automated teller machines), retail (retail and point-of-sale [POS] terminals), and manufacturing (industrial control systems—supervisory control and data acquisition [SCADA] components).

Deception technology can greatly enhance visibility, detecting lateral attacker movement to or from IoT devices. Almost any way an attacker moves within the network triggers a deception network trap.

Advanced Threat Deception for Your Healthcare System

Adding FortiDeceptor to a healthcare breach protection strategy helps shift defenses from reactive to proactive. It provides intrusion-based detection that is layered with contextual intelligence and automates the blocking of attacks against IT devices and OT system controls.

FortiDeceptor automatically lays out a layer of decoys and lures that help conceal sensitive and critical assets behind a fabricated deception surface, which confuses and redirects attackers while revealing their presence on the network. Using FortiDeceptor, organizations can:

- Deceive external and internal threats with decoys that are managed from a centralized location. It can deploy a deception surface of real Windows, Linux, virtual private network (VPN) server, medical IoT, and SCADA virtual machines with services that are indistinguishable from real production assets. These decoys serve as lures to catch attackers and uncover their activities.
- Expose hacker activity with early accurate detection and alerts that trace and correlate an attacker's tactics, tools, and procedures. It provides active notification using web UI, email, SNMP traps, logs, and events using FortiSIEM and FortiAnalyzer.
- Eliminate threats by automating threat response with FortiGate Next-Generation Firewalls (NGFWs), FortiNAC network access control, FortiSOAR security orchestration, automation, and response, and third-party security solutions through the Fortinet Security Fabric.

The FortiDeceptor deception workflow

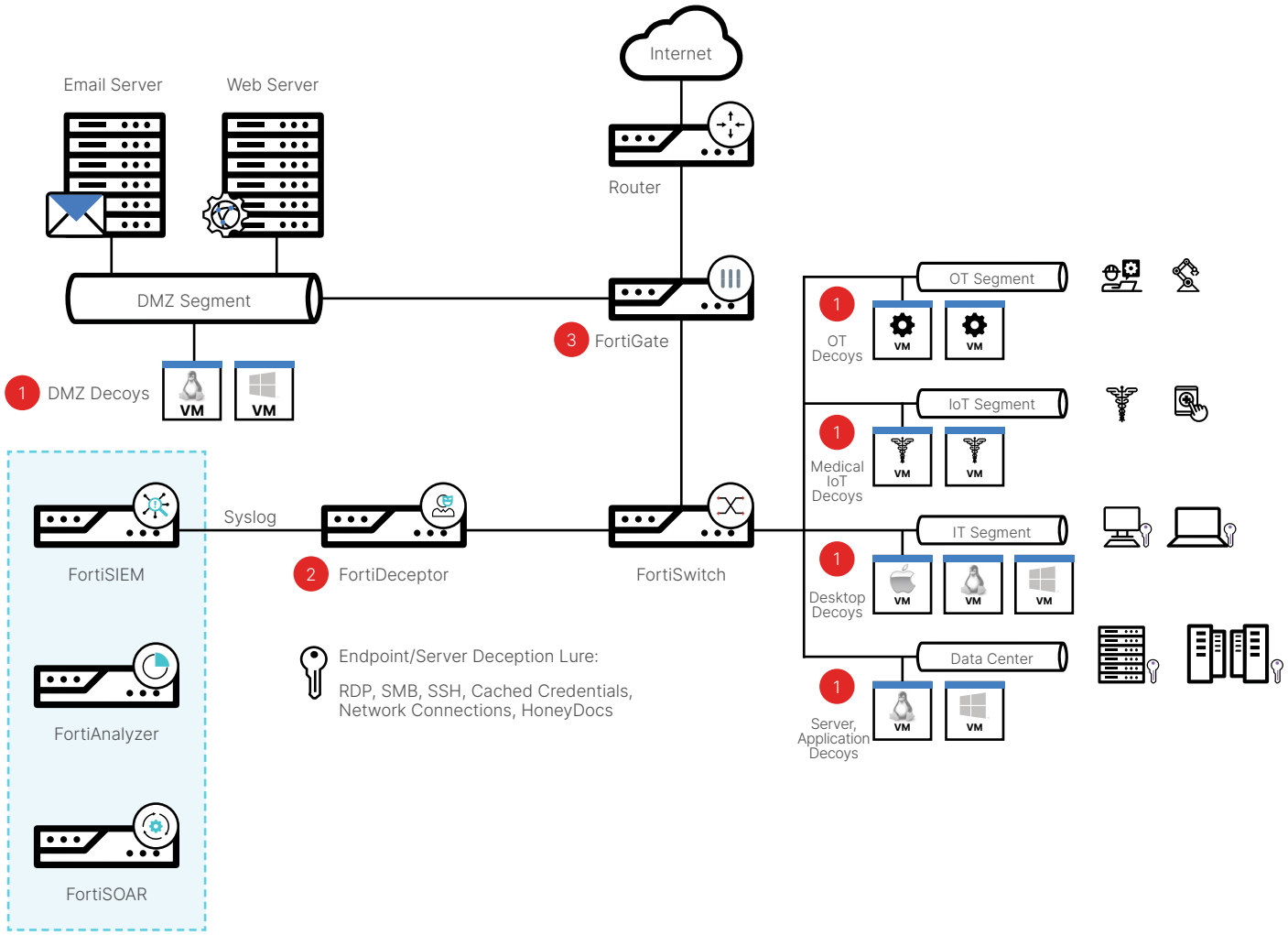

Figure 1: The three phases of the FortiDeceptor deception workflow.

1. FortiDeceptor deploys decoys with different operating systems equipped with lures (such as RDP, SMB, Credentials, HoneyDocs) that appear indistinguishable from real IT and OT assets and are highly interactive.

2. FortiDeceptor acts as an early warning system that exposes an attacker's malicious intent and tracks lateral movement, which translates to real-time alerts sent to FortiDeceptor, FortiAnalyzer, and FortiSIEM for review and validation. FortiDeceptor applies analytics powered by FortiGuard Labs, FortiSandbox, and VirusTotal intelligence, to a consolidated set of security events and correlates them to the campaigns with a timeline of activities.

3. FortiDeceptor allows security analysts to manually investigate and apply manual remediation or automatically block attacks based on severity before actual damage occurs through its integration with FortiGate NGFWs, FortiNAC, and FortiSOAR.

Conclusion

In healthcare, the odds are tipped in favor of cyber adversaries, but FortiDeceptor helps level the playing field by automating the creation of dynamic decoys that are dispersed throughout the healthcare IT environment. Because attackers are unable to determine which assets are fake and which are real, their time advantage is reduced or eliminated. When cyber criminals can't make the distinction between real and fake assets, they are forced to waste time on fake assets while inadvertently alerting a security administrator to their presence.

Even if attackers become aware of the deception, they need to immediately exercise caution as they look for tripwires embedded in the fake environment. They are forced to alter their tactics in ways that increase their chances of being detected by the security team. In the end, attackers are either trapped by the illusion created by FortiDeceptor or forced to abandon their goals. Either way, it is a win for a healthcare cybersecurity team.

To learn more about using FortiDeceptor in healthcare, contact your Fortinet healthcare security expert at healthcare@fortinet.com.

[1] "Cost of a Data Breach Report 2021," IBM and Ponemon Institute, July 2021.

October 28, 2021 5:31 AM
1331229-0-0-EN