POINT OF VIEW

Healthcare: The Future of AI-Driven Breach-Protection Technology

Executive Summary

Digital transformation across the healthcare and life sciences ecosystem the last decade has continued to grow. Advancements in digital patient experiences, workforce mobilization, cloud adoption, and the utilization of machine learning (ML) and artificial intelligence (AI) by clinical research scientists and physicians have helped create new therapies, new medications, and cure diseases. This transformation has also greatly expanded the potential attack surface of today's healthcare organizations. IT teams are now required to build and maintain a digital ecosystem that provides high performance, broad availability, and resiliency, all while maintaining the security and integrity of the vast clinical data stored on-premises and in cloud environments.

In today's climate, healthcare threats continue to evolve, advance, and increase in volume, especially the growing volume of ransomware. This new reality requires healthcare organizations to always remain a step ahead of their adversaries, and one way to do that is by utilizing AI-driven breach-protection technology. As overburdened security operations (SecOps) teams struggle with the increasing volume and sophistication of threats, AI is key to reducing the workload of threat investigation and ultimately accelerating threat mitigation.

AI is key to reducing the workload of threat investigation and ultimately accelerating threat mitigation.

Fortinet FortiAI

FortiAI represents the future of AI-driven breach-protection technology. Designed for short-staffed security operations center (SOC) teams to defend against various threats, it includes the identification of advanced persistent threats (APTs) through a trained Virtual Security Analyst who helps to identify, classify, and respond to malware, including those well camouflaged. FortiAI employs patent-pending Deep Neural Networks, based on advanced AI and Artificial Neural Network models, to provide sub-second investigation. This helps it to harness deep-learning technologies to assist in automated responses used to remediate different breeds of synthesized AI and non-AI-based threats.

Based on several years of FortiGuard Labs research, FortiAI reduces the "time to detect and respond" significantly to protect healthcare organizations. It directly addresses such issues as:

1. ***Shortage of Experienced SOC Analysts***
   Experience is the hardest thing to acquire in cybersecurity, especially in threat analysis, outbreak investigation, and malware research experience.
2. ***Breach Prevention***
   Without AI-driven capabilities, SecOps teams struggle to handle high volumes of traffic, identify malware, and discover anomalies hidden in the network.
3. ***Masqueraded Malware***
   IT teams also wrestle with discovering carefully crafted cyber threats designed to bypass existing security controls by camouflaging malware behaviors.
4. ***AI-powered Cyberattacks***
   Innovative threat actors are also increasingly disrupting cybersecurity through automated attacks designed to overwhelm or sneak past SOC defenses.

What It Does

FortiAI features a Virtual Security Analyst, powered by a Deep Neural Networks AI model that augments organizations' SecOps by mimicking an experienced security analyst to investigate threats and surface malware outbreaks.

It reduces malware detection and investigation time from minutes to providing a sub-second verdict.

Its mature AI applies 6 million+ malware features to achieve sub-second verdicts for day-one deployment, with the capability to learn new features.

On-premises learning reduces false positives by analyzing an organization's specific traffic and adapting to newly disguised threats.

It also scientifically analyzes zero days, including fileless threats, and classifies them into 20+ malware attack scenarios.

It can leverage the Fortinet Security Fabric by uniting with FortiGate devices to automatically quarantine attacks.

What Outcomes It Helps Drive

FortiAI responsibilities include:

Identifying and classifying attack scenarios: Determines malware attack scenarios with chain-on-infection and big-picture analysis

Investigating the source of an attack: Tracks the original source of infection with time stamps

Emulating as a FortiGuard malware analyst: Scientifically determines the type of malware based on evolving Neural Networks that constantly learn and mature over time and experience

Outbreak search: Searches networks for traces of malware outbreaks based on hashes and similar variants

Conclusion

FortiAI represents the future of AI-driven breach-protection technology, reducing the "time to detect and respond" significantly to better protect healthcare organizations.

Contact your Fortinet healthcare security expert to learn more.

Healthcare@fortinet.com

August 4, 2021 1:42 PM