2021 Industry Spotlight: Healthcare

Cyber-attacks targeting the healthcare industry have been prolific over the past year. Operating at full capacity while combatting fast-moving threats such as ransomware, many organizations have turned to self-learning Cyber AI to detect and autonomously interrupt attacks at machine speed.

At a Glance

- ✔ Protects over 280 healthcare organizations globally
- ✔ Self-learning AI technology which detects novel and sophisticated threats
- ✔ Autonomously stops fast-moving attacks in seconds
- ✔ Up to 92% reduction in triage time

Combatting Fast-Moving Attacks and Zero-Day Vulnerabilities

Cyber-criminals have been quick to capitalize on the upheaval of the past year. The WHO have reported a five-fold increase in attacks since the start of the pandemic, while the FBI have warned of an "imminent cyber-crime threat to hospitals and healthcare providers".

Of particular concern is ransomware. In September 2020, over 250 United Health Services hospitals were left debilitated for two weeks following an attack, with ambulances diverted, appointments postponed, and test results delayed. In the same month, the first fatality as a direct result of a cyber-attack was declared in Germany. With such devastating consequences, healthcare organizations simply cannot afford downtime – a fact cyber-criminals know and exploit.

Tasked with defending the digital systems and data that frontline workers rely on, security teams face a growing challenge. With digital infrastructure spanning everything from SaaS applications and email platforms, to MRI machines and remote patient monitoring devices, organizations' digital environments and the security stacks designed to defend them have never been more fragmented.

In addition, IoT devices implemented to improve efficiency and patient outcomes are often unsecured and unencrypted – and frequently outside of the security team's awareness. The US Food and Drug Administration (FDA) has recalled 86% of medical IoT devices more than ten times, due to critical zero-day vulnerabilities. Such flaws are an ideal launching point for stealthy infiltration.

As attackers continue to innovate, organizations must leverage self-learning AI to autonomously detect and respond to advanced and never-before-seen cyber-threats.

> "Autonomous Response is the future for defending against fast-moving and unpredictable threats, before they do damage."
>
> Craig York, CTO, Milton Keynes Hospital

Autonomously Defending Healthcare Organizations

Relied on by some of the world's most innovative and forward-thinking healthcare organizations, Darktrace Cyber AI defends the entire digital ecosystem. As a self-learning technology, the AI is able to identify and respond to machine-speed attacks and insider threats in real time – without relying on prior attack data.

Inspired by the human immune system, Darktrace works by learning the digital DNA of every user and device in a organization, and all the connections between them. Such an understanding of 'self' enables the AI to spot the most subtle signals of emerging threat and react immediately to neutralize the malicious activity. Operative across cloud, SaaS, medical IoT, email, endpoint devices, and the traditional network, Darktrace is able to defend organizations' sensitive patient data and digital systems wherever they are located.

In today's new era of threat, Darktrace's ability to autonomously stop machine-speed cyber-threats is invaluable, particularly in the event of DDoS attacks and ransomware. By taking swift and targeted action, Autonomous Response interrupts emerging threats without disrupting normal activity. Only highly unusual and suspicious device and employee behavior is inhibited – meaning that life-saving patient treatment can continue as usual, while the full range of cyber-criminal activity is swiftly neutralized.

Threat Find: Detecting Maze Ransomware Before Encryption

Darktrace Cyber AI autonomously detected a case of Maze ransomware targeting a healthcare organization, alerting the security team before the damage was done.

The attack began with network scanning activity and enumeration, with admin level credentials, unusual RDP activities, and multiple Kerberos authentication attempts all following. Darktrace then saw the attacker uploading a domain controller, before batch files were written to multiple file shares.

An infected device then proceeded to connect to mazedecrypt[.] top, before a TOR browser bundle was downloaded and a large volume of sensitive data from the R&D subnet was uploaded to a rare domain.

Darktrace's AI detected each stage of this attack, raising multiple high-fidelity alerts to the security team which enabled them to stop the threat before encryption began.

> "With Darktrace's complete visibility, early threat detection, and smart prioritization of anomalies, we are well-positioned to fight back against even the subtlest cyber-attack."

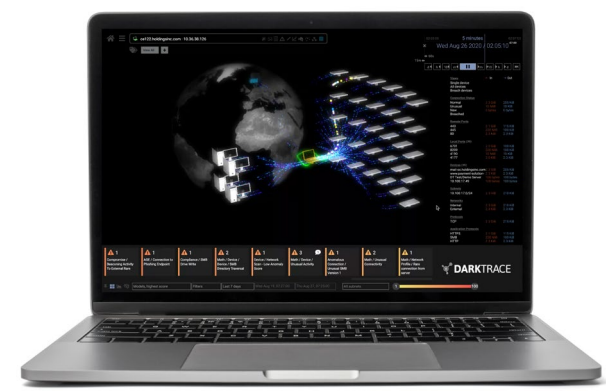
Brian Thomas, CIO, Swope Health Services

Threats by Numbers

$7.13 million is the average cost of a healthcare data breach.

4,000+ ransomware attacks daily between 2016 and 2020.

The cost of cyber-crime in 2025 will be $10.5 trillion USD.



Darktrace Antigena autonomously neutralizes threats, surgically blocking malicious activity