Industry Spotlight: Healthcare

DARKTRACE

At a glance:

- Protects over 390 healthcare organizations globally
- Self-Learning AI which detects novel and sophisticated threats
- Autonomously stops fast-moving attacks in seconds
- Up to 92% reduction in triage time

Cyber-attacks targeting the healthcare industry have been prolific in recent years. Operating at full capacity while combatting fast-moving threats such as ransomware, many organizations have turned to Self-Learning AI to detect and autonomously interrupt attacks at machine speed.

/ Industry Challenges

The WHO have reported a five-fold increase in attacks since the beginning of 2020, while the FBI have warned of an "imminent cyber-crime threat to hospitals and healthcare providers".

In 2021, Ireland's Health Service Executive (HSE) became the target of a Conti ransomware attack, causing IT systems nationwide to be shut down. The most significant attack on a health service system, the breach caused hundreds of confidential patient records as well as corporate documents to be published. Requiring four months to fully recover, HSE sustained numerous damages. 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

/ The Cyber AI Loop

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

It works by learning the 'pattern of life' of every user and device in an organization and the connections between them. As well as helping to pre-empt attackers and harden defenses, this understanding of 'self' enables the AI to spot the subtlest signals of emerging threats 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 cybercriminal activity is swiftly neutralized.

> 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

/ Attack Case Study: Maze Ransomware

Darktrace's Self-Learning AI autonomously detected a case of Maze ransomware targeting a healthcare organization, alerting the security team before the damage was done.

The attacker began engaging in network scanning activity and enumeration to escalate access within the Research and Development subnet. Darktrace's AI detected a successful compromise of admin level credentials, unusual RDP activities and multiple Kerberos authentication attempts. The attacker was then observed making uploads to a domain controller, before batch files were written to multiple file shares, which were used for encryption.

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. If the organization had enabled RESPOND, Darktrace's Autonomous Response capability, it would have taken targeted action to contain the attack in the early stages.

Figure 1: Darktrace RESPOND autonomously neutralizes threats, surgically blocking malicious activity

About Darktrace

Darktrace (DARK.L), a global leader in cyber security artificial intelligence, delivers complete AI-powered solutions in its mission to free the world of cyber disruption. Its technology continuously learns and updates its knowledge of 'you' for an organization and applies that understanding to achieve an optimal state of cyber security. It is delivering the first ever Cyber AI Loop, fueling a continuous end-to-end security capability that can autonomously prevent, detect, and respond to novel, in-progress threats in real time. Darktrace employs over 2,200 people around the world and protects over 8,100 organizations globally from advanced cyber-threats.

Scan to LEARN MORE