Protecting Hospitals From Machine-Speed Attacks

Using Cyber AI to enhance and extend security teams in the healthcare sector.

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
- ✔ 92% reduction in time to triage
- ✔ No operational disruption

Penn Highlands Healthcare
Swope Health Services
PHOENIX group
Carle
Northfield Hospital + Clinics
Life Group

Ransomware on the Rise: Facing up to Computer-Speed Cyber-Attacks

The escalation of cyber-crime against hospitals and medical facilities is pushing security teams to their limit. Ransomware in particular is hitting hard, as criminals take advantage of overstretched staff – who are already struggling to support the frontline response to the pandemic – to disrupt digital systems and demand ransom money.

Over the past year, attacks targeting the healthcare sector have doubled, with the FBI, CISA, and HHS issuing warnings regarding the widespread threat. Last September, over 250 Untied Health Services hospitals were left debilitated for two weeks after a ransomware attack hit, while 6 hospitals were incapacitated by one strain alone – known as Ryuk – in October. As such, this is a threat that shows no signs of stopping.

The consequences of ransomware are not just financial. Disruption of IT systems is causing patients to be diverted to other hospitals, urgent surgeries to be postponed, and treatment options to be scaled back, with staff resorting to pen and paper.

With digital infrastructure in hospitals spanning everything from back-office networks and patient record systems, to connected medical devices and IoT equipment, such as WIFI connected MRI scanners and automated intravenous medication delivery, the challenge of defending critical data and building resilience is more daunting than ever.

Threats by Numbers

days average downtime from a ransomware attack.

ransomware attacks daily between 2016 and 2020.

average cost of a data breach in the healthcare sector.

"Autonomous Response is the future for defending against fast-moving and unpredictable threats, before they do damage. Darktrace fights backs on our behalf so we can focus on strategic tasks."

Craig York, CTO, Milton Keynes Hospital

Cyber AI: The Machine Fights Back

Relied on by over 280 healthcare organizations worldwide, Darktrace Cyber AI has become the de facto technology for defending against fast-moving attacks like ransomware.

Cyber AI is a self-learning technology that works by building an evolving understanding of what 'normal' looks like for a given hospital or facility's users, devices, and digital infrastructure. Unlike traditional approaches that pre-define what 'malicious' activity looks like, Cyber AI is able to detect novel cyber-threats inside the organization as their behavior falls outside of the normal patterns.

As well as detecting such novel threats and attacks, Darktrace Cyber AI can also autonomously respond, calculating the best action to take in the shortest period of time to neutralize the in-progress threat – before the damage is done.

As the pandemic persists, uninterrupted access to the systems and data that enable medical professionals to do their jobs must be a priority. With Cyber AI, self-defending digital ecosystems are made possible, with 24/7 Autonomous Response stopping the spread of fast-moving threats as they happen.

Stopping Ransomware Before Encryption

When ransomware hits, the last thing an organization wants is for their security team to be out-of-office. But in the case of one Darktrace customer, that's exactly what happened.

The initial compromise occurred when an employee accessed their personal emails from a corporate smartphone and was tricked into downloading a malicious file containing ransomware. Seconds later, the device began connecting to an external server on the Tor network and SMB encryption activities began. Within just nine seconds, Darktrace had detected the threat and had raised a prioritized alert signifying the need for immediate investigation of the rare behavior.

As the behavior persisted over the next few seconds, the AI revised its judgment on the severity of the threat. Thankfully, while the security team had left the office for the weekend, Darktrace Antigena was on and ready to defend. Darktrace's AI independently stopped the attack, interrupting all attempts to write encrypted files to network shares and preventing a single file from encryption.

Without Darktrace Antigena, the security team would have come back on Monday to an organization in chaos. Only Darktrace's deep, evolving understanding of your organization's DNA can offer such real-time detection and response to sophisticated ransomware attacks.

> "I sleep a lot better at night knowing I have AI protecting our organization and patient information."
>
> Tom Johnson, CIO, Penn Highlands Healthcare

> "Darktrace's ability to self-learn is game-changing, it has the unique ability to find potential threats that have never been seen before."
>
> Brian Thomas, CIO, Swope Health Services

Darktrace Antigena surgically stops ransomware in its tracks