Protecting Hospital Infrastructures From Computer-Speed Cyber-Attacks

Using Cyber AI to augment security teams in the healthcare sector

Ransomware by Numbers

- 50% increase in ransomware attacks across Q3 2020
- Ransomware attacks on healthcare will grow by 5 times by 2021
- 62% of hospital administrators feel inadequately trained to mitigate cyber risks

Darktrace Defends

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

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

The escalation of cyber-crime against hospitals and medical facilities in 2020 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.

In the past 3 months of 2020 alone, the percentage of US healthcare organizations targeted by ransomware has almost doubled, rising from 2.3% to 4%. In September, over 250 United Health Services hospitals were left debilitated for two weeks after a ransomware attack hit, while 6 hospitals were incapacitated by the variant 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.

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

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 the 'pattern of life' of the hospital or facility's networks and technologies. 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 'pattern of life'.

> "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**

As well as detecting such novel threats or 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 networks are made possible, with 24/7 Autonomous Response that stops the spread of fast-moving threats as they happen.

Case Study: Catching 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 had left the office for the weekend, Antigena Network 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 Antigena Network, 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.

More Ransomware Case Studies

Zero-Day Ransomware Blog

WastedLocker Ransomware Blog

Maze Ransomware Blog

To find out how Darktrace can defend your hospital, start your free trial today!

About Darktrace

Darktrace is the world's leading cyber AI company and the creator of **Autonomous Response technology**. Its self-learning AI is modeled on the **human immune system** and used by over 4,000 organizations to protect against threats to the **cloud**, **email**, **IoT**, **networks** and **industrial systems**.

The company has over 1,300 employees and headquarters in San Francisco and Cambridge, UK. Every 3 seconds, Darktrace AI fights back against a cyber-threat, preventing it from causing damage.