CYBER DEFENSE FOR HEALTHCARE

The healthcare industry faces some of the steepest challenges when it comes to cyber security. With new internet-connected devices, troves of sensitive data, and often tight security budgets, healthcare firms are a frequent target for many of today's most insidious cyber-attacks.

Internet-connected medical devices have allowed healthcare companies to become more efficient, but they have also opened new avenues for attackers to enter the network. Given the amount of sensitive data that healthcare companies hold, data theft and ransomware have proven to be lucrative for criminals. The well-documented success of these attacks means that they will only continue to increase, both in the number of attacks and their sophistication.

> In the healthcare industry, Darktrace's technology has been proven to detect and respond to early-stage cyber-threats, including fast-moving ransomware, aggressive malware seeking to compromise credentials, and malicious insiders attempting to exfiltrate sensitive data.

With the extensive challenges facing the healthcare industry, a proactive stance on cyber security is needed.

The Enterprise Immune System

Darktrace's Enterprise Immune System has been widely adopted by healthcare companies looking to get ahead of an evolving threat landscape and proactively defend their sensitive information. Powered by unsupervised machine learning and AI algorithms, Darktrace's award-winning technology delivers on the promise of a self-learning and self-defending network.

Much the same way the human immune system learns 'self', the Enterprise Immune System learns the unique 'pattern of life' for every user and device on a network. It then employs powerful correlation techniques to identify deviations from 'normal' that indicate live, in-progress threats. This self-learning technology works without any prior knowledge of the network environment and or the threat landscape, and it does not rely on signatures or rules. Instead, Darktrace utilizes unsupervised machine learning to dynamically detect and fight back against previously unknown threats, all in real time.

Threats by Numbers

33% of all records compromised came from the healthcare industry

According to an industry report, over 33% of all records compromised are from the healthcare industry, the most of any industry vertical.

55% of incidents were carried out by an insider

Whether malicious or not, insiders represent a major security risk if not properly monitored. Phishing attacks consistently plague the industry, and even the best-trained employees can fall prey to well-disguised attacks.

Lost or stolen healthcare records cost **more than twice** the average for other industries

According to a study by the Ponemon Institute, lost or stolen healthcare records can cost up to $363 per record. This is 136% higher than the average cost of a stolen or lost record in other industries.

> Because Darktrace's AI technology doesn't look at yesterday's attack to predict that of tomorrow, it has the unique ability to find potential threats that have never been seen before.
>
> **Brian Thomas, CIO,**
> **Swope Health Services**

Growing Complexity and New Challenges

Physicians now carry multiple devices with them, including personal devices that may or may not have the appropriate security protocols. Work, personal, and medical devices ranging from imaging equipment to connected pacemakers, as well as connected objects like vending machines and air conditioning units, have given threat-actors a host of new and unexpected attack vectors.

> Healthcare organizations were the targets of 88% of all reported ransomware attacks across US industries in Fall 2016.

Despite this, experts suggest that cyber security has been under-resourced by medical institutions for years. They are now forced to play catch-up with a modern threat landscape dominated by sophisticated attacks which would have been unthinkable a decade ago.

As networks become increasingly complicated, with more and more connected devices in the growing Internet of Things, the healthcare industry can no longer afford to rely on legacy security tools to protect against the next generation of cyber-attacks.

A growing number of healthcare organizations have opted for a fundamentally different approach cyber defense: one that prioritizes real-time threat detection and responds to threats before they can do damage.

HUMAN LONGEVITY, INC.

Riverview Health

AVANIR pharmaceuticals

NORTHSIDE HOSPITAL

ICON HEALTH & FITNESS

SWOPE HEALTH SERVICES

NEKTAR

EPIC SCIENCES

Darktrace in Action

Data Exfiltratation

At a National Health Service trust in the UK, Darktrace detected a company device displaying signs of an insider attack. The device was uploading large amounts of data to external online storage, contacting a suspicious mailbox and failing to access data on an internal server. It was also regularly beaconing to a rare domain not accessed by any other internal devices.

Darktrace detected them as subtle deviations from normal behavior and understood that they were indicative of an ongoing internal attack that was attempting to exfiltrate company data.

Automated Credential Theft

The network of a healthcare provider was infected with a strain of malware designed to steal user credentials. The type of malware used was unlike anything on existing threat databases: security team could not respond quickly enough, and traditional defenses could not identify it. Darktrace's AI approach recognized the copied programs and the forced access of password managers as abnormal given its understanding of the normal activity of users and organizations.

Global Ransomware Campaign

On Friday 12th May 2017, the first reports came in that a ransomware known as WannaCry had hit organizations across the globe targeting a known exploit that had been identified and patched a few weeks earlier. The worm appeared to have used the EternalBlue SMB exploit to move laterally across the network and infect more devices, and tor nodes were used for Command and Control traffic.

The activity seen from infected devices was deemed very unusual, and inconsistent with the network's 'pattern of life'. On detecting the ransomware, Darktrace responds in real time by forcibly dropping suspect connections within the internal network and stopping its spread. This entirely autonomous response, generated by Darktrace Antigena, gave security teams the vital time to catch up before the data was lost or encrypted.

Contact Us

North America: +1 415 229 9100
Europe: +44 (0) 1223 394 124
Asia Pacific: +65 6248 4516

info@darktrace.com
darktrace.com