DARKTRACE

INDUSTRY SPOTLIGHT

Cyber Defense for Healthcare & Pharma

In recent years, the healthcare industry has been increasingly targeted by advanced cyber-attacks. Confidential records and financial data, along with life-critical medical systems, make the sector a target for fast-moving threats, like ransomware, used by opportunistic threat actors looking for financial gain.

The industry's rapid adoption of connected IoT devices - which are not always designed with security in mind - has also expanded the attack surface. Internet-connected medical devices have allowed healthcare companies to become more efficient, but they have also opened new avenues for attackers to compromise the network.

Indeed, physicians now carry multiple devices with them, including personal devices that may or may not have 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.

Over the next decade, analysts are anticipating cyber-threat to cross from the digital to the physical world, with ransomware attacks designed to target medical IoT devices. With these more advanced attacks on the horizon, the stakes have never been higher when securing healthcare organizations.

Despite this, experts suggest that cyber security has been regarded as an afterthought by many 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.

A growing number of organizations have opted for a fundamentally different approach to cyber defense: one that prioritizes real-time threat detection and responds to threats before they can do damage. Darktrace is the industry leader of this new approach, using its cutting-edge AI technology that can autonomously respond to novel threats as they arise.

ICON · NEKTAR · MetroPath · Human Longevity, Inc. · Riverview Health · Swope Health Services · CordenPharma · Wockhardt · Penn Highlands Healthcare · Avanir Pharmaceuticals · SCRAM Systems · QTultrasound · The Farrer Park Company · Epic Sciences · NCH North Country Healthcare · Littleton Regional Healthcare

> 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**

Threats By Numbers

55% of incidents were carried out by someone with insider access

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.

DARKTRACE

CASE STUDY

MetroPath

Background

Founded in 1913, Metropolitan Pathologists (MetroPath) is the oldest private pathology lab in the state of Colorado. A physician-owned organization, MetroPath performs a full range of diagnostic testing services for hospitals, medical clinics, and surgery centers throughout the region. Given the demands of its daily operations, MetroPath's corporate network has become increasingly integrated, with its physicians and staff constantly engaging with digitized lab equipment, IoT devices, medical records, and sensitive billing data governed by stringent HIPAA regulations.

Challenge

Alarmed by the healthcare industry's changing risk profile, MetroPath wanted to enhance its IT systems with a proactive security technology. The company's IT team was concerned that its legacy tools did not provide complete visibility of its entire network infrastructure. Further, the rule-based defenses were incapable of identifying never-before-seen threats, the 'unknown unknowns' that security teams fear. Without a 24/7 security operations center, MetroPath lacked the resources to neutralize these attacks should they occur outside working hours. Facing a threat landscape characterized by stealth and sophistication, it knew that early threat detection and complete visibility would be critical to safeguarding sensitive patient records.

> Once we plugged Darktrace in, we started finding threats that completely bypassed our legacy systems.
>
> **Jimmy Gelhaar, Director of IT, MetroPath**

Solution

To address these concerns, MetroPath deployed Darktrace into the heart of its network for a four-week Proof of Value (POV). After a one-hour installation, Darktrace began self-learning about every user and device on the network to develop a distinctive sense of 'self' - what was normal for the network, and what was not.

After being deployed in MetroPath's network for just under two weeks, Darktrace demonstrated this nuanced understanding of 'self' when it discovered strange activity taking place in the middle of the night. A computer was making unknown data transfers to devices in Russia. Darktrace was able to instantly alert the security team, as the time, size, and destination of the data transfer deviated from the network's expected 'pattern of life'. MetroPath instantly took the computer offline, and the situation was mitigated before any damage could be done.

"Once we plugged Darktrace in, we started finding threats that completely bypassed our legacy systems," commented Jimmy Gelhaar, IT Director at MetroPath. "Darktrace's AI technology has proven instrumental in providing visibility of devices we didn't even know we had on our network. Armed with the Enterprise Immune System, we can now detect and mitigate in-progress attacks on all of our internet-connected devices, in real time, before they cause any damage."