DARKTRACE

CASE STUDY

Metropolitan Pathologists

MetroPath

Overview

Industry

- Healthcare

Challenge

- Small security team
- Needed to protect sensitive medical and financial records
- Perimeter defenses provided incomplete visibility of internal network activity
- Attack surface amplified by IoT devices

Results

- Comprehensive visibility of every device on the network, including IoT
- Unprecedented awareness of 'normal' network activity
- Self-learning technology safeguards crucial medical information
- Dynamically updating 'pattern of life' helps reduce false positives and cut through the noise

Business 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.

> Darktrace's AI technology has proven instrumental in providing visibility of devices we didn't even know we had on our network.
>
> **Jimmy Gelhaar,**
> **Director of IT, MetroPath**

Challenge

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 top target for fast-moving threats, like ransomware, from 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. 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 approaches did not provide complete visibility of its entire network infrastructure. Further, the rules-based defenses were incapable of identifying never-before-seen threats, the 'unknown unknowns'. Without a 24/7 security operations center, MetroPath lacked the resources to neutralize these attacks should they occur post-working hours. Moving forward in 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.

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 belonged on the network, and what didn't. Powered by unsupervised machine learning and AI algorithms, Darktrace can detect subtle and stealthy deviations from this 'normal' network activity, spotting and stopping anomalous threats in real time, before they can do any damage.

Darktrace presents its understanding of the 'pattern of life' via the intuitive 3D Threat Visualizer, which provides complete visibility of MetroPath's entire network infrastructure, including IoT and rogue devices. It ranks each threat by its deviation from 'normal' activity, limiting alert fatigue and enabling MetroPath's team to prioritize the most pressing threats.

After being deployed in MetroPath's network for just under two weeks, Darktrace demonstrated its nuanced understanding when it discovered strange activity taking place in the middle of the night. A computer was making an 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 Gelhaar. "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 it causes any damage."

> Healthcare facilities are one of the biggest targets of cyber-attacks today. Without better network visibility, we knew we'd be sitting ducks just waiting for the next attacker to strike.
>
> **Jimmy Gelhaar,**
> **Director of IT, MetroPath**

Benefits

With Darktrace, MetroPath has renewed confidence in its security stack's ability to fight back against in-progress threats, as well as having an unprecedented awareness of its internal network activity. Because it doesn't rely on any prior assumptions, it is uniquely capable of identifying never-before-seen threats enabling MetroPath to stay abreast of a sophisticated threat landscape. Further, with Antigena, MetroPath is now capable of autonomously fighting back against these sophisticated cyber-attacks at any hour of the day – giving the time advantage back to the small security team.

Armed with Darktrace's platform and 3D Threat Visualizer, MetroPath is confident that its security solution will ensure that it stays ahead of healthcare industry's rapidly-evolving threat landscape. Given the platform's self-learning approach, Darktrace is equipped to handle tomorrow's most sophisticated cyber-attacks, however unpredictable they may be.

"As a healthcare organization, we are prime targets for threat-actors," commented Jimmy Gelhaar. "We needed a way to proactively ensure our patient data was safeguarded, especially as we enter a 'WannaCry' era of threats. Darktrace's AI technology helps us ensure that we have full awareness of what's happening on our network, in real time, allowing us to stay on top of a fast-moving threat landscape."

Contact Us

North America: +1 415 229 9100
Europe: +44 (0) 1223 394 100
Asia Pacific: +65 6804 5010

info@darktrace.com
darktrace.com