Milton Keynes University Hospital

At a Glance

- 24/7 Autonomous Response supports lean security team
- Major vulnerabilities detected and remediated with Self-Learning AI
- AI defenses avoid alert fatigue and business disruption

Milton Keynes University Hospital
NHS Foundation Trust

Founded in 1984, Milton Keynes University Hospital serves the citizens of Milton Keynes, Buckingham, Bedford, and Northampton. It also performs important research and development work, and offers a training program for undergraduate medical students.

Preventing digital downtime in a crucial industry

In the healthcare sector, digital downtime needs to be avoided at all costs. The US Department of Health and Human Services' HIPAA Breach Reporting Tool shows a record number of major health data breaches in 2021, and studies have laid bare the links between cyber disruption and increased patient stay lengths, medical procedure complications, and – according to CISA's findings – mortality rates. Medical staff and their patients are increasingly reliant on digital systems, and security teams in turn must employ robust cyber defenses to maintain the integrity of the IT and OT infrastructure underpinning modern hospitals.

The Conti ransomware attack in 2021 on the Irish healthcare system served as a wake-up call in the industry. It was the largest attack against a health service computer system on record, and it took four months to bring all computer servers back online. By then, the disruption to healthcare professionals and patients had been immense. Avoiding disasters of this scale in future needs to be a priority.

Craig York, CTO at Milton Keynes University Hospital NHS Foundation Trust, recognized the need for a forward-thinking approach to cyber security which could keep pace with increasingly sophisticated attacks. Putting patient care at the top of the agenda, York sought a technology which fights back against threats as they emerge, taking autonomous action to protect sensitive data and defend the integrity of the hospital's systems. He needed a self-sufficient solution that would learn and improve by itself, and automate the process of threat investigation, presenting his lean security team with clear findings and actionable insights.

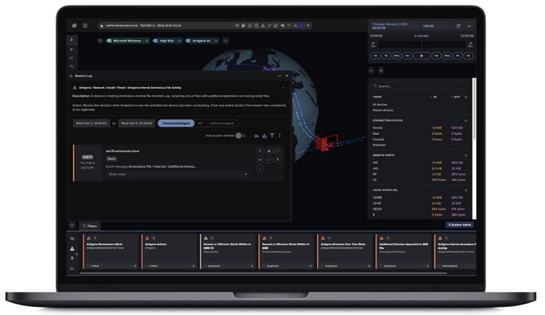
Milton Keynes University Hospital

AI protects the entire hospital environment

Milton Keynes University Hospital protect themselves from these attacks by deploying Darktrace's Self-Learning AI and Autonomous Response technologies.

The AI works by learning the 'pattern of life' for every user and device in the hospital's digital environment. This understanding of what 'normal' looks like enables it to detect even the most subtle deviations indicative of threat – from low and slow attacks to novel ransomware strains. Thus, unlike traditional tools which spot known attacks, Darktrace's unique approach catches sophisticated zero-day threats before they do damage. And, with Autonomous Response, Darktrace's AI fights back at machine speed to neutralize malicious behavior whenever it emerges.

Self-Learning AI correlates activity across network, cloud, SaaS, email, and endpoint environments to stop threats wherever they arise. Because this technology works 24/7, and can take action without human intervention with Autonomous Response, the hospital's systems are protected continually even when security teams are unavailable or out of office.



Darktrace's findings and autonomous actions are shown in the Threat Visualizer

Uplifting a stretched security team

The value of Darktrace's technology was instantly recognized by the team at Milton Keynes University Hospital for both its ability to identify novel threats and vulnerabilities and its function as a force multiplier – augmenting the capabilities of the existing security professionals.

For Craig York, this technology has been a game-changer. "Having Darktrace's AI watching over your network is really just another pair of eyes, one that never sleeps and which takes action in seconds to protect every digital asset you have."

With his lean security team, York has found Darktrace's ability to fight back on its behalf invaluable. And as attacks increasingly occur at machine speed, having a tool which neutralizes these threats seconds after they arise ensures the integrity of hospital systems and, crucially, prevents downtime.

Darktrace's AI shines a light into hard-to-track places, giving Milton Keynes Hospital's security team visibility into its entire dynamic workforce. The team has gone from fire-fighting and alert fatigue, to being able to plan digital transformation projects, increase adoption of state-of-the-art technology, and trial innovative medical technological developments.

In the event of an attack, Darktrace's AI surgically intervenes and interrupts the illegitimate activity alone, allowing normal business practices to continue as normal. This means that even an infected device can continue to undertake its usual business operations while the threat is stopped, with no disruption to the company workflow.

> "I am confident that we will be in a much better place to fend off another serious cyber-attack on the NHS with Darktrace at work."
>
> Craig York, CTO, Milton Keynes Hospital