DARKTRACE

DATA SHEET

Cyber AI for the Public Sector

Hundreds of public sector organisations around the world rely on cyber AI to protect against the most advanced cyber-attacks, including ransomware and other automated attacks. When security teams are outpaced, the machine fights back.

Held to **Ransom**

Some of the most significant ransomware attacks of the past year were waged against public sector infrastructure, which resulted in critical data encrypted, and vital services crippled.

These recent spates of ransomware have brought to the fore the vulnerabilities that connected infrastructure and public services face in the wake of increasingly sophisticated and fast-moving threats. Ransomware campaigns are designed to specifically identify and exploit the weaknesses of their targets, and spread across networks in a matter of seconds. Their speed and sophistication give security teams almost no time to react before the damage is done.

Governments and policy-makers are recognising the importance of advanced solutions for the entirety of their digital environments, and are relying on cyber AI and Autonomous Response technology to safeguard the critical infrastructure of cities and its public sector services.

NHS West Suffolk NHS Foundation Trust

NHS West Suffolk Clinical Commissioning Group

NHS University Hospitals of Derby and Burton NHS Foundation Trust

NHS Milton Keynes University Hospital NHS Foundation Trust

NHS Royal Free London NHS Foundation Trust

NHS The Hillingdon Hospitals NHS Foundation Trust

Darktrace Cyber AI:

- Protects **more than 100** public sector organisations and **18 UK NHS hospital trusts**
- Responds to an emerging threat **every 3 seconds** worldwide
- Installs in **just 1 hour**

> Autonomous Response is the future for defending against fast-moving and unpredictable threats, before they do damage. 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, Associate Director of IT, Milton Keynes University Hospital Trust

The Machine **Fights Back**

Darktrace's award-winning cyber AI is trusted by hundreds of cities and providers of critical national infrastructure in the UK and around the globe, including the smart city of Las Vegas.

Darktrace technology is able to not only identify but also respond to cyber-attacks such as ransomware – before they encrypt files, and ultimately, disable public services.

Modeled on the human immune system, Darktrace AI autonomously learns what is normal for each digital environment without relying on rules or signatures. The technology forms an ever-evolving understanding of an organisation's unique digital estate, allowing it to identify and respond to malicious activity the moment it transpires – even novel threats previously unknown to the security community.

Using a unique technology known as 'Autonomous Response', recognised by Gartner as the future of cyber defense, Darktrace Antigena fights back in real time – neutralising ransomware in its tracks within seconds.

Case Study

Milton Keynes Hospital

Milton Keynes University Hospital (MKUH) has over 500 patient beds and employs more than 4,000 staff, providing a full range of hospital services and specialist care. As a member of the regional Sustainability and Transformation Plan, MKUH is part of a healthcare ecosystem where hospitals are enhanced with shared databases. Alongside increased privacy and data security concerns, MKUH were also vulnerable to cyber-attacks because of chronic under-investment in cyber defense infrastructure.

For MKUH, the WannaCry virus in May 2017 highlighted cyber security as a critical patient safety issue that required urgent solutions. This cyber-attack disrupted services at 61 NHS organisations and forced the UK's healthcare system to turn away patients.

To defend against more sophisticated future ransomware attacks, MKUH deployed Darktrace's Enterprise Immune System. With its unique understanding of a digital 'pattern of life', Darktrace AI now safeguards the hospital's critical services and patient databases, detecting emerging cyber-threats in real time, and at machine-speed.

Proof of Value: 30 Day Trial

Discover how Autonomous Response can supercharge your cyber defense by starting your 30-day free trial. As part of a Darktrace Proof of Value (POV), you will benefit from a dedicated Darktrace Cyber Technologist and access to our award-winning interface, the Threat Visualizer.

- Installs in 1 hour
- Access to the Threat Visualizer
- Threats and findings reported within a week
- 100% visibility of your digital environment

> Darktrace Antigena is the only automated cyber defense technology on the market that is capable of fighting the most important battles for us.
>
> **Michael Sherwood, CIO,**
> **City of Las Vegas**

Fighting back against: **Ransomware**

Traditional security tools that use rules and signatures to stop cyber-threats at the border are now ill-equipped to defend against automated ransomware attacks and other zero-day threats. As more sophisticated malware strains have emerged, human teams are now outpaced in their ability to neutralise threats.

However, with the detection and Autonomous Response capabilities of Darktrace's self-learning AI, identifying and stopping novel ransomware attacks and other zero-day threats is now routine. Due to ransomware's highly anomalous behaviour that deviates from the digital 'pattern of life', Darktrace's cyber AI will detect attacks within seconds of threatening behaviour appearing on the network.

As soon as anomalous connections are made to external servers, Darktrace Antigena is activated and will interrupt SMB encryption attempts of shared files - instantaneously preventing attacks spreading beyond patient zero.