Case Study

Mid Cheshire Hospitals NHS Foundation Trust

GYTPOL

Mid Cheshire Hospitals NHS Foundation Trust

Company Overview

Mid Cheshire Hospitals NHS Foundation Trust is an award-winning organisation that delivers high quality, safe, cost effective and sustainable healthcare services to the people and communities of Cheshire, and beyond. As an NHS Trust, Mid Cheshire is a key provider of community services and work in partnership with local GPs and numerous other NHS Foundation Trusts.

The healthcare sector has increasingly become a target for cyber criminals looking to generate revenue through advanced attacks. COVID and remote working has provided these hackers with new opportunities to exploit the healthcare industry, highlighting the increased pressure to protect all data and gain ultimate visibility. Back in 2017, WannaCry ransomware, exploiting SMBVI vulnerability tore across the globe, afflicting over 200,00 computers in over 150 countries and resulting in over 6,900 NHS appointments being cancelled.

Client Profile

Industry – Healthcare

Location – Three sites across Cheshire:

- Leighton Hospital
- Victoria Infirmary
- Elmhurst Intermediate Care

No. of Employees – 5000

Challenges faced

- Thousands of endpoints across multiple sites
- Limited resource and staff
- Meeting compliance for CIS, NIST and other security standards
- Budgetary restrictions
- No centralised visibility or assurance for secure configuration of devices

Case Study

Mid Cheshire Hospitals
NHS Foundation Trust

GYTPOL

Mid Cheshire Hospitals NHS Foundation Trust

Business Need

Cyber criminals target healthcare organisations because of the sensitive patient data they hold and the vulnerabilities that can be exploited. As we have learnt with previous cyber-attacks against the NHS, suffering a data breach or losing access to their technology can be detrimental to the running of a trust. There are many victims when the NHS is targeted, along with reputation and financial implications.

Complex challenges needn't require complex solutions- Gytpol are the only technology provider to easily auto-remediate, with instant results which is ideal for the fast-paced nature of the healthcare industry. Like many organisations, the ever-evolving threat environment creates pressure on stretched IT departments to adapt and research new technologies to fit their requirements. Working within the public domain also means NHS Trusts must meet CIS and NIST compliance, along with other security standards, which requires experienced IT professionals.

The Solution

Recognised as thought leaders in the industry, Next Generation Security (NGS) researches the cyber-security landscape and technology vendors to provide the best solutions. As our experts have worked with Mid Cheshire for over a decade, the IT department engaged with NGS to discuss their challenges. Deploying Gyptol Validator proved to be the best fit for their organisation due to its ability of ensuring validation of existing policies and continuous detection and remediation of security misconfigurations of devices, even remote ones, with zero impact.

Problem

Difficulty in having full visibility of devices and continuous validation that endpoints were securely configured to meet compliance. Additionally, stretched IT resource and budgetary restrictions caused pressure to research new technologies.

Solution

Gytpol offer a one-click remediation along with the option to auto-remediate all other endpoints meeting the same criteria. If for any reason the remediation needs to be reversed, the roll-back option is a simple button press.

Case Study

Mid Cheshire Hospitals
NHS Foundation Trust

GYTPOL

Mid Cheshire Hospitals NHS Foundation Trust

Results

Mid Cheshire NHS Foundation Trust found great value in Gytpol Validator's capabilities, particularly due to the quick and easy deployment and almost instant results. This reduced the demanding workload for the IT department and saved on engineer resource. Matt Palmer, Head of Digital and Information Services at Mid Cheshire notes Gytpol Validator "providing a benchmark score on desktop builds for the Centre for Internet Security, a key audit requirement with a built-in check". All organisations that have access to NHS patient data and systems must use the Data Security and Protection Toolkit (DSPT) to provide assurance that they are practising good data security, which Gytpol provide information to help with the submission.

For Mid Cheshire NHS Foundation Trust, Gytpol Validator discovered group policies that had not been applied but were originally believed to have been. Matt notes that the visibility of misconfigurations provided through the Validator highlighted any group policy errors and captured a broad spectrum of exploitable security issues with intuitive in-app guidance. Mid Cheshire experienced quick results and saw a rapid return on investment through deploying the tool, along with NGS's support and guidance.