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 organization 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 works in partnership with local GPs and other NHS Foundation Trusts.

The healthcare sector has become an increasing target for cyber criminals looking to generate revenue through advanced attacks.

Client Profile

A **healthcare delivery** organization operating **3 facilities** across the UK and managing a **staff of 5,000**

Challenges faced

- Thousands of endpoints across multiple sites
- Limited staff and resources
- Complying with CIS, NIST, and other security standards
- Budgetary restrictions
- No centralized configuration security visibility or enablement

Case Study

Mid Cheshire Hospitals NHS Foundation Trust

GYTPOL

Mid Cheshire Hospitals NHS Foundation Trust

The Business Need

Cyber criminals target healthcare organizations 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 is easy to use and quick to work, providing the ability to auto-remediate misconfigurations with the push of a button. For Mid Cheshire, those rapid response capabilities and assured effectiveness proved an excellent match for the fast-paced and evolving threat landscape in which they operate. 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 Trusted Advisor

Recognized as industry thought leaders, Next Generation Security (NGS) researches the cyber-security landscape and technology vendors to advise its clients on the best solutions for their needs. Having a long-standing and very productive relationship with NGS, Mid Cheshire turned to the consultancy to discuss their challenges.

GYPTOL quickly stood out in that conversation as the best solution to the problem at hand. Key factors included GYTPOL's ability to validate existing security policies, automatically detect policy violations, and enable push-button remote remediation at any scale and with no risk of disruption.

The 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.

The 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

The Results

Mid Cheshire NHS Foundation Trust found great value in GYTPOL, particularly due to the quick, easy deployment and almost instant results. This reduced the demands on the IT department and saved engineering resources.

In the UK, all organizations that have access to NHS patient data and systems must use the Data Security and Protection Toolkit (DSPT) to demonstrate good data security practices. With GYTPOL's hardening enablement and on-demand audit trails, the platform proved extremely valuable for compliance demonstrations purposes. Commenting on this fact, Matt Palmer, Head of Digital and Information Services at Mid Cheshire notes that "GYTPOL gives us a benchmark score on desktop builds according to Centre for Internet Security standards; a key audit requirement for us".

Immediately upon deployment, GYTPOL discovered a number of group policies that were not been applied as designed. These rogue configurations were previously went unnoticed, expanding the attack surface and adding significant operating risk to the organization. On this, Mr Palmer notes that "the misconfiguration visibility provided by GYTPOL highlights key group policy errors and raises a broad spectrum of exploitable security issues."

This, together with the guidance and remediation provided in the system, helped the organization measure their security progress and realize a rapid return on their investment.