Birmingham Community Healthcare NHS FT uncovers a network blind spot and eradicates ‘several hours of manual work per week’

The first step in protecting anything is knowing that an asset exists. It sounds simple. But how can you protect something if you don’t know you have it? With NHS networks growing ever more complex, gaining end-to-end network visibility is an increasing challenge. Find out how Birmingham Community Healthcare NHS Foundation Trust (BCHC) worked with ITHealth to reveal threats to its network it didn’t know existed and now manages its cyber security with greater confidence.

Customer

Birmingham Community Healthcare NHS Foundation Trust (BCHC)

Type of NHS Organisation

Community Health Trust.

Customer Since

2019.

Challenge

BCHC knew there had to be a better way of viewing and managing the security state of its sprawling IT infrastructure than manually piecing together disparate reports from multiple security appliances.

Solution

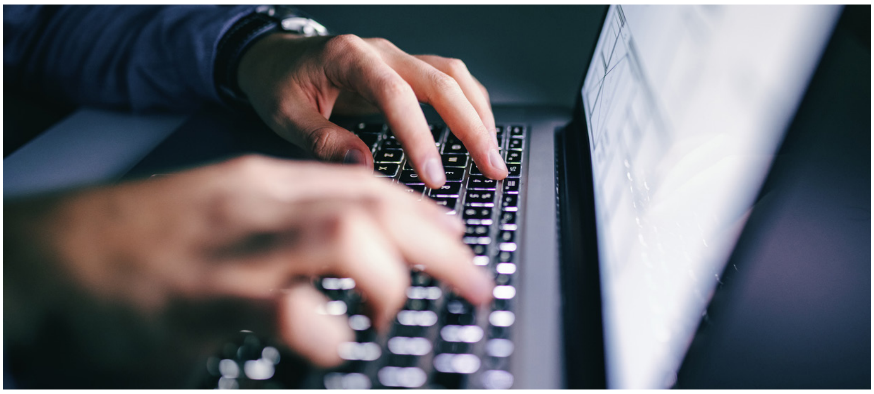
ITHealth’s Assurance Dashboard Solution provides an accessible, unified view of the Trust’s IT estate. BCHC now manage its network with greater confidence and rely on a trusted view of its assurance.

Birmingham Community Healthcare NHS Foundation Trust provides high quality community and specialist services within Birmingham and the West Midlands. It delivers over 100 clinical services, out in people's homes and in over 200 hospitals, health centres and clinics. It provides services for adults, children, people with learning disabilities, and those with rehabilitation needs, as well as dental services.

> "Our endpoint security appliances were all very capable, yet disparate in their reporting. Collation of the relevant data to get an overall picture of the network required manual intervention and so reporting took a lot of time and resource."
>
> GARY MULLINDER
> IT System Administrator
> Birmingham Community Healthcare
> NHS Foundation Trust

The Challenge

BCHC has a sprawling, complex IT estate with staff spread across hundreds of sites making security for the Trust a challenge. For its 2018/2019 cyber security programme, the Trust's endpoints had received multiple security applications to re-enforce the security stance – all very capable and able – yet *all* were disparate in their reporting mechanisms. Collation of the relevant data from each of the systems required manual intervention to produce the monthly Cyber Security Briefing and daily review reports on assurance and protection status. Although fit-for-purpose, it was an approach that was both time-consuming and resource reliant; it also left room for error. The Trust knew there had to be a better way of getting a holistic and more accurate view of the state of its network.



The Solution

ITHealth were already in discussions with BCHC about support for its Sophos solutions and migration to Sophos Central, and so proposed its Assurance Dashboard Solution. The Trust were impressed by the Dashboard's ability to provide a consolidated and dynamic risk-based view of different aspects of its network and so agreed to undertake a proof of concept.

Prior to the Dashboard, with its myriad of SAM's (software asset management systems) and monitoring tools, the Trust's IT team believed it was fully compliant on most things. For example, they believed they had eradicated all Windows XP machines and had no Server 2003 instances on their network (their client-based installed Software Asset Management application had told them this, so why would they doubt it). The ITHealth Assurance Dashboard proved otherwise. After an agentless scan of the network, one of the Dashboard's many reports identified an XP device. "We couldn't believe it", said Gary Mullinder, IT System Administrator. "We naturally thought it was incorrect."

Fortunately, as almost all of the data within the Dashboard is drillable, the Trust was able to pin down the rogue device as the Dashboard had provided the specific network switch, make, model and serial number – even what LCD monitor it plugged into. It was the classic scenario of a part-time employee using a machine for her part-time hours and then dutifully putting it away in a cupboard afterwards. Needless to say, the Trust resolved the issue immediately. "This particular machine didn't have the SAM client software installed, nor did it have Sophos AV and it was running on XP! I am pleased to say that it is the only one we encountered, but at the stage of our process maturity without the Dashboard we wouldn't have seen it for a long time", said Gary.

The Trust was also impressed by the Dashboard's ability to automate much of the management of NHS Digital CareCERTs. "The Assurance Dashboard's CareCERT automation has pretty much eradicated several hours of manual work per week", continued Gary. "The Dashboard scans the network following nearly all new CareCERT detail and highlights affected devices so we know exactly where to target remediation."

> "The Assurance Dashboard contradicted what we thought we knew about our network. We now manage our IT estate with much greater confidence."
>
> GARY MULLINDER
> IT System Administrator
> Birmingham Community Healthcare
> NHS Foundation Trust

> The level of reporting and additional functionality within the Assurance Dashboard is astounding. If you want to manage your IT estate with confidence, then you need this more than you realise."

GARY MULLINDER, IT System Administrator, Birmingham Community Healthcare NHS Foundation Trust

The Results

With the need to keep systems up to date and compliant, BCHC now rely heavily on the Assurance Dashboard for a truthful view of its network. Benefits for the Trust include:

- **Freed up IT resource** - Manual intervention to collate disparate reports is no longer needed nor is manual interrogation of the network necessary every time following CareCERT bulletins. The IT team can now focus on other important projects.
- **Streamlined cyber reporting** - The Dashboard gives the Trust one place to go for a wealth of near real-time reports on the state of its network – all of which are exportable. As the solution is supported by ITHealth, comprehensive monthly assurance reports - designed to be board-facing - are also provided which highlight key stats, figures, trends and more.
- **Simplified remediation and compliance** - Vulnerabilities and weaknesses within the IT estate are flagged in the Dashboard in almost real-time meaning issues can be addressed before they become a problem. The Dashboard's available reports also directly meet or support 81% of the evidence required for the DSPT (Data Security and Protection Toolkit).

> "The Assurance Dashboard relieves a lot of the effort associated with the DSPT. We will be using it heavily for our 2019/2020 submission."

GARY MULLINDER, IT System Administrator
Birmingham Community Healthcare NHS Foundation Trust

Find out more about ITHealth's Assurance Dashboard

Call: 0115 987 6339
Email: info@ithealth.co.uk
Visit: www.ithealth.co.uk

About ITHealth

ITHealth provide NHS organisations with proven and trusted IT security and access management solutions. Whether it's providing fast, reliable, and secure access for NHS mobile workers, or finding effective ways to reduce threats while improving productivity and clinical workflows, ITHealth's cost-effective solutions mean NHS systems and data are always secure, easy to access, and simple to manage.

Registered Office: ITHealth, 10 Churchill Park, Private Road, No 2, Colwick, Nottingham, NG4 2HF