Sizeable Healthcare Organization Within the United Kingdom's National Health Service (NHS)

NHS Trusts are healthcare organisations which operate within the National Health Services, providing crucial healthcare services to people within their respective geographical catchment areas

About the NHS Trust

10,000
Users

14K
Devices Secured

3.9M
Threats Prevented Weekly

Introduction

NHS Trusts are healthcare organisations which operate within the National Health Services, providing crucial healthcare services to people within their respective geographical catchment areas. In the UK there are currently more than 200 trusts, which employ around 800,000 of the NHS's 1.2 million total staff.

Iboss works with a number of healthcare organisations in the UK, helping to secure their critical information, and protect patient care. This includes one of the largest NHS Trusts in the UK, which employs more than 14,500 staff and provides specialist healthcare to over one million people a year in London. The Trust's hospitals have a long track record in research and education, influencing care and treatment nationally and worldwide. The Trust is also developing a growing range of integrated and digital care services alongside offering private healthcare in dedicated facilities on all of its sites.

The Challenge:

The healthcare industry continues to accelerate at pace in its digitalization, automation and Internet of Things (IoT) adoption. Latest figures predict the global IoT healthcare market to reach over $606 billion by 2028 as a greater number of medical devices are connected daily for tasks such as data collection, monitoring electronic health records and research purposes. The entire ecosystem of connected healthcare IoT systems also includes physical security like CCTV cameras or critical building management systems such as HVAC and lifts.

With digitalization comes big benefits from improved efficiency, reduced workloads, and greater flexibility for healthcare providers to operate wherever and whenever; all of which leads to better patient care. NHS Trust's now often have large remote workforces in operation.

To help defend against the rising risks associated with healthcare's new, digital infrastructures, it's also mandatory for any organization like NHS Trusts, which have access to NHS patient data and systems, to conduct a self-assessment using the Data Security and Protection Toolkit (DSPT), as set out by the NHS. Together, the assessment and toolkit provide assurance that such organizations practice good data security and handle personal information correctly by measuring their performance against the National Data Guardian's 10 data security standards.

However, interconnected healthcare environments can be extremely complex for Heads of IT to secure and manage. Connecting legacy medical operating systems to the network for the first time, often developed without cybersecurity in mind, presents unique security challenges. While connected environments bring network visibility issues and larger attack surfaces for cybercriminals to exploit.

UK healthcare organizations experience around 785 cyberattacks a week as healthcare systems and medical devices are often a potentially easy entry point for cybercriminals. One of the biggest and most dangerous risks to the sector is ransomware attacks, such as we saw with the 2017 WannaCry incident and the attack on NHS 111 in 2022. Cybercriminals are tempted by the rich, highly lucrative patient data as well as the opportunity to cause major disruption to patient care and critical infrastructure.

The Solution:

iboss creates and operates one of the largest multi award-winning cloud network security fabrics on earth. A scalable, global service which brings zero trust edge security to organizations for unrivalled network security and peace of mind, regardless of where users operate.

The Trust approached iboss in 2015, initially deploying the iboss on-premise, zero trust security solution for superior cybersecurity protection for its extensive range of on-site medical equipment, IoT devices and servers across all of its hospitals.

However, the Trust's IT security requirements have since evolved. Many of its growing workforce now require remote access to the hospital's IT network, which was accelerated further by the Covid-19 pandemic. In 2019 iboss introduced to the Trust a cloud network security solution, as well as adopting a zero-trust security system and operating model, putting the Trust in a strong position to handle the demands of the pandemic. -iboss now protects over 10,000 of the Trust's users with employees now able to work from anywhere with ultra-fast and secure connections to all cloud applications.

iboss helps the Trust meet the criteria of the DSPT and the National Data Guardian's 10 data security standards. The DSPT mandates the use of Protective Domain Name Service (PDNS), which is a cybersecurity service created by the NCSC to track and analyze Domain Name Service (DNS) queries and implement measures to mitigate threats.

The Trust has also been able to use a number of iboss' other technology integrations for log analysis and tenant restrictions, to help improve its cybersecurity processes.

Mobile and managed devices that leave the premises, such as phones and laptops, as well as the Trust's wifi, are also protected by iboss to minimize the risk of potential breaches and data loss. While, the hospital's static, on-site medical and IoT equipment remains protected by extending the iboss policy enforcement points into the trusts private network.

Now every connected device, both within the hospital's premises and beyond, has advanced online protection under iboss' hybrid cybersecurity model, bringing peace of mind while freeing up more of the Trust's time to focus on patient care.

The Results

Thanks to iboss' infinite scalability, the Trust has always received purpose-built, unrivalled cybersecurity solutions and support in-line with its ever-changing IT needs, which protect the organization against modern day threats. Through some of the most difficult periods for the healthcare industry, iboss has been central to maintaining the security of the Trust, ensuring that teams can operate efficiently and securely in any environment.

For example, in 2017, the WannaCry ransomware attack crippled more than 300,000 machines in 150 countries, including 80 National Health Service hospitals in Britain. Yet, despite the size and scale of disruption to the wider NHS, the Trust was shielded from the attack thanks to iboss' proactive security measures, implemented ahead of and in response to WannaCry, and due to the security team's continued support throughout the incident.

Also, during the Covid-19 pandemic in 2020, the Trust was well placed to cope with the sudden shift to home working for many of its healthcare professionals due to its previous implementation and adoption of zero-trust operations. iboss' scalability and super-fast connection speeds meant healthcare teams could swiftly adapt to secure remote working and remain productive, while supporting the security needs of its ever-expanding remote workforce.

Highlights

- Having supported the Trust since 2015, **iboss' now protects over 10,000 of the Trust's users** with employees able to work from anywhere with ultra-fast and secure connections to all cloud applications
- The hospital's static, on-site medical and IoT equipment remains protected under **iboss' advanced, on-premise security architect**.
- Now every connected device, both within the hospital's premises and beyond, has advanced online protection under **iboss' hybrid cybersecurity model**, bringing peace of mind and improved cybersecurity for patients and workers.
- **iboss helps the Trust meet the criteria of the DPST** and the National Data Guardian's 10 data security standards.
- The Trust was shielded from the 2017 WannaCry ransomware attack thanks to **iboss' proactive security measures**, implemented before the attack, and its continuous support throughout.
- During the Covid-19 pandemic in 2020, thanks to its use of **iboss' scalable solution, which provides super-fast connection speeds and remote device online protection**, the Trust was well placed to accommodate the sudden shift to home working for many of its healthcare professionals during Covid-19.

About iboss

iboss is a cloud security company that enables organizations to reduce cyber risk by delivering a Zero Trust Secure Access Service Edge platform designed to protect resources and users in the modern distributed world. Applications, data, and services have moved to the cloud and are located everywhere, while users needing access to those resources are working from anywhere.

The iboss platform replaces legacy VPN, Proxies, and VDI with a consolidated service that improves security, increases the end-user experience, consolidates technology, and substantially reduces costs. Built on a containerized cloud architecture, iboss delivers security capabilities such as SWG, malware defense, Browser Isolation, CASB, and Data Loss Prevention to protect all resources via the cloud instantaneously and at scale. The iboss platform includes ZTNA to replace legacy VPN, Security Service Edge to replace legacy Proxies, and Browser Isolation to replace legacy VDI. This shifts the focus from protecting buildings to protecting people and resources wherever they are located. Leveraging a purpose-built cloud architecture backed by 230+ issued and pending patents and more than 100 points of presence globally, iboss processes over 150 billion transactions daily, blocking 4 billion threats per day. More than 4,000 global enterprises trust the iboss platform to support their modern workforces, including a large number of Fortune 50 companies. To learn more, visit https://www.iboss.com/