South Lon
and Maud
NHS Foundation

# SLAM NHS Foundation Trust turns to

Saving costs and boos

## About the Customer

**5,000**

Network users at one time

**Hybrid Workforce**

9,500

**Previous Security**

Legacy VPN and squid proxy system

# Introduction

South London and Maudsley (SLAM) NHS Foundation Trust is a leader in health and wellbeing locally, nationally and globally, providing the widest range of NHS mental health services in the UK. The Trust has four hospitals, Bethlem Royal, Lambeth, Lewisham and Maudsley, and provides outpatient treatment and care from a number of other hospital sites nearby, serving a local population of 1.3 million people in South London, as well as providing specialist services for children and adults across the UK. Each year, healthcare centres linked to the Trust provide inpatient care for over 5,000 people and treat more than 40,000 patients in the Lambeth, Southwark, Lewisham and Croydon communities.

# SLAM NHS Foundation Trust's Challenge

Prior to working with iboss, a zero trust security and digital infrastructure specialist, SLAM NHS Foundation Trust relied on a legacy Virtual Private Network (VPN) with multiple vendor solutions to help enable the shift to remote working. These solutions had reached the end of their natural lifecycle or were deemed no longer fit for purpose. Stuart MacLellan, Chief Technology Officer at SLAM NHS Foundation Trust said: "We had a complicated legacy infrastructure around our on-premise proxy servers which were used for login and monitoring of web activity. This was not fit for purpose, especially with a dispersed, hybrid workforce of 9,500. Users were not getting the best experience when accessing the network via our previous clunky system and old proxy servers and, as a result, we would get user complaints around issues such as a lack of network response or it not facilitating the user's request, which then required a lot of management for the IT team. This was an area we needed to remove from our workload and so we decided to look at our security options." Additionally, the Trust faced challenges in meeting the rigorous compliance requirements set out in the Cyber Assessment Framework (CAF) and the Data Security and Protection Toolkit (DSPT).

These frameworks are critical for maintaining operational integrity and protecting sensitive data, yet the Trust's legacy systems lacked the necessary visibility and reporting capabilities to streamline compliance processes. Budget constraints added another layer of complexity. As a public sector organisation, SLAM NHS required a solution that not only met its technical and operational needs but also aligned with its financial limitations.

# SLAM NHS Foundation Trust's iboss solution

With 5,000 users on the network at any given time logging on daily from central and remote locations and devices, the Trust needed to modernise and consolidate its cybersecurity system to keep laptops, PCs, and servers secure. It needed a scalable solution that could accommodate fluctuating user demands while working within the confines of the Trust's budgets. On the recommendation of another partner, the Trust turned to iboss and its Consolidated SaaS Network and Security Service, which formed part of the Trust's journey to a zero-trust architecture.

To spread costs and meet specific technical needs, iboss began a phased deployment and implementation at SLAM NHS Foundation Trust. This began with its Zero Trust Core license package, an easy to use, cloud-based web proxy solution that mitigates risks from threat actors by monitoring and blocking malicious action before it can impact the Trust's network. Users are also prevented from accessing certain websites, searching for particular terms, and blocked from logging on from specific global regions to minimise risk.

By using iboss' consolidated platform, the Trust has cut the cost and the complexity of relying on multiple vendors and on-premise appliances, and improved the overall user experience, enabling the IT team's time to focus on strategy rather than firefighting user issues. iboss also provides a 24/7 mission critical support service for continuous assistance, ensuring that the Trust's tech team receive timely help for any technical challenges.

The second phase of the project replaced a legacy VPN with Zero Trust Network Access (ZTNA), giving the Trust additional security features, granular reporting and controls, plus comprehensive data protection and automated log forwarding to its (SIEM) platform, enabling the organisation to maintain DSPT (Data Security and Protection Toolkit) compliance. Stuart continues: "We looked at a number of enterprise wide (ZTNA, SASE and SSE) vendors and found iboss was perfect to help meet our limited budgets. The system gives us granular reporting and greater visibility on user activity so we can spot potential threats in a timelier manner compared to traditional proxies. This also means we can now push forward with the DSPT and CAF side of things."

# Key results for South London and Maudsley NHS Foundation Trust:

- Reduced vendor swell and complexity on the SLAM NHS environment
- Reduced risk of vulnerabilities
- Improved security compliance and visibility
- Improved proxy service performance
- Elimination on proxy downtime
- Improved user experience and efficiency of systems
- Cost-effective, scalable solution which aligns with regulatory NHS requirements

# Highlights:

- The Trust had been relying on multiple legacy solutions across various areas of its cybersecurity stack, many of which had reached the end of their lifecycle
- This created a need for modernisation and consolidation, which led the security team at SLAM NHS Foundation Trust to iboss
- With a hybrid workforce, the Trust needed a solution which could scale up and down at ease, while also providing unrivalled network security for all staff, regardless of their point of access
- Through the iboss platform, the Trust has reduced vendor swell, saved costs, improved user experience and productivity by replacing the problems of the VPN legacy system with a consolidated solution
- The platform provides advanced security features, including VPN replacement (ZTNA) and comprehensive data protection, ensuring robust defence against threats
- The Trust's hybrid workforce is now protected at all times, in all locations and on any network

## About iboss

With over 4,000 customers, including the largest government, financial, insurance, energy, and technology organizations, iboss provides users direct and secure access to cloud applications from wherever they work. iboss transitions organizations from protecting in-office workers to protecting the modern work-from-anywhere workforce while providing fast, secure, and direct connections to cloud applications to increase productivity and protect organizations from malware and data loss. A Gartner Magic Quadrant "Visionary", and backed by 230+ issued and pending patents, iboss processes and secures over 150 billion daily network transactions globally and has built the largest containerized cloud security fabric. The iboss Government Cloud Platform enables agencies to modernize their architecture, by reducing the dependency or eliminating the need for traditional network security appliances that are no longer effective at protecting today's hybrid workforce. Jumpstart your SASE transformation and experience the future of cloud security today at http://www.iboss.com.