



# AINTREE UNIVERSITY HOSPITALS

delivers secure  
flexible working.



## The challenge

**Aintree University Hospitals NHS Foundation Trust**, based in Liverpool, comprises two main hospitals providing acute healthcare to a population of 330,000 in North Merseyside and surrounding areas.

**The Trust** wanted to enable flexible working for its remote and mobile staff whilst ensuring sensitive data was protected. Furthermore, the previous remote access solution used a secure token authentication process, which required a high level of maintenance and was costly to run.

**The Trust** required a cost effective, remote access solution which incorporated secure connectivity and strong authentication as standard, to provide strong security and ease of use for employees. In addition, they wanted to accommodate third party access if required; so the solution needed to be flexible in terms of access options and controls.

# Technologies used

- ◆ VPN Mobile Working / Remote Access
- ◆ Endpoint Security Solutions
- ◆ Fully Managed Network Services

# Key benefits

- ◆ Flexible, secure remote access
- ◆ Greater control over access rights
- ◆ Reduced IT costs
- ◆ Simple and easy to use

## The solution

The Trust chose Network Defence to implement a managed AppGate Security Server solution with Nordic Edge two-factor authentication. The solution allows secure access to the protected network from a remote device using authentication, encryption and access restriction.

The remote access solution uses advanced technology to deliver secure access control that outperforms old perimeter-based security models. It combines an application layer firewall with device security and a VPN in one solution that provides full control over corporate information.

The solution works in a similar way to SSL VPN solutions, but uses Secure Shell (SSH2) for securely accessing the protected network from a remote device. SSH2 is a recognised standard that is controlled by an IETF working group.

The remote access solution includes a range of software clients which provide users with an interface to the organisation. These clients range from installable clients for mobile devices, Microsoft Windows, Apple Mac OSX, Linux and Solaris operating systems to clientless solutions which only require Sun Java to be installed on the host system.

The managed service included as part of the solution guarantees remote access is available 24x7 and ensures the Trust's network and data are protected at all times. This allows the Trust's in-house IT resource to focus on delivering core business IT services.

Earlier this year Network Defence deployed over 500 SafeStick USB flash drives across the Trust to administration, clinical and non-clinical staff, who need to transfer data as part of their role. The USB data security solution ensures all data that is transferred using data sticks can only be read by users who have the correct password, helping to keep confidential data and sensitive information secure. The solution also helps reduce the number of service desk calls the IT department gets regarding issues with data storage.

"Keeping patient information and Trust data secure is of utmost importance, Network Defence has given us a solution which not only gives staff flexibility, but gives us a cost-effective way to keep sensitive information secure."

**Ward Priestman,**  
IT Director for Aintree University Hospitals NHS  
Foundation Trust

## The benefits

The managed AppGate Security Server solution implemented by Network Defence is easy to use and enables cost-effective flexible working for staff working off site or from home, with much higher security than before.

A key benefit of the solution is that it provides a robust level of remote access security; it controls user access to protected resources and its powerful and flexible authorisation database contains rules for what applications and services should be available to each user. This ensures the Trust has close management over access, giving them the ability to grant or restrict access rights depending on individual needs.

All users now have access to their emails from home, whilst clinical users are able to access clinical-based applications and can carry out other functions of their job remotely, such as prescribing medication. Additionally, the solution is able to accommodate third party access if required by the Trust.

Another significant benefit of the managed AppGate Security Server solution is the cost savings it brings to the Trust. The former remote access system cost the Trust approximately one thousand pounds per mobile user as it had to provide each user with a corporate laptop and a costly secure token authentication process. With the managed AppGate Security Server solution, employees can use their own personal computers, giving remote access at a fraction of the cost of the previous solution.

Ward Priestman, IT director at the Trust, said: "Keeping patient information and Trust data secure is of utmost importance and we are always looking for methods to maintain data security. Having worked previously with Network Defence, we know their expertise and knowledge ensures we get the solution that is right for us, so we approached them with the issue of finding an alternative remote access solution.

"Network Defence has given us a tailored solution, which gives us a cost-effective way to keep sensitive information secure. The new remote access solution means that we can now offer our employees a more flexible approach to working without worrying about whether our data is at risk."

The Trust's deployment of the secure remote access solution is part of their overall strategy to improve data security throughout the organisation, reduce IT costs and ease the burden of IT support on the Trust's IT department.



**Get protected!**  
Call our experts on  
**01925 272000**

[sales@networkdefence.com](mailto:sales@networkdefence.com)  
[www.networkdefence.com](http://www.networkdefence.com)