



Aintree University Hospitals

Providing flexible and secure remote working for hospital staff

Healthcare/NHS | Secure Application Access & Business Continuity | AppGate



Background

Aintree University Hospitals NHS Foundation Trust, based in Liverpool, comprises two main hospitals providing acute and non-acute healthcare services 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.

Requirements

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.

Solution

The Trust chose AppGate from Cryptzone from certified partner Network Defence to implement a managed solution using the AppGate Network Security 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 control.

The AppGate solution uses advanced technology to deliver secure access control that outperforms the old perimeter-based security model. It combines an application layer firewall with device security and a VPN in one easy to use and cost effective solution, providing full control over user access to corporate information and resources.

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 recognized standard that is control by an IETF working group.

The remote access solution includes a range of software clients that provide users with an interface to the organization. These clients range from installable clients for mobile devices, Microsoft Windows, Apple Mac OSX, Linux and Solaris operating systems to clientless solutions that 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.

The managed AppGate security server solution 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 authorization 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

"Keeping patient information and Trust data secure is of utmost importance. 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."

Ward Priestman
IT Director
Aintree University Hospitals
NHS Foundation Trust



"Having worked previously with Network Defence, we know their expertise and knowledge ensures we get the solution that is right for us. They have given us a tailored solution, which gives us a cost-effective way to keep sensitive information secure."

as prescribing medication. Additionally, the solution is able to accommodate third party access if required by the Trust.

Another significant benefit of the AppGate security server solution is the cost savings it brings to the Trust. The former remote access system cost the Trust approximately £1000 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 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. We now have 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 organization, reduce IT costs and ease the burden of IT support on the Trust's IT department.

Benefits

Strong security

Secure encrypted communications end-to-end as standard.

Two-factor authentication

The AppGate security server supports a wide variety of two-factor authentication methods including Nordic Edge One-Time Passwords providing added security especially for 3rd party access.

Control of user access

Granular levels of control over which network resources each user can access.

Flexibility

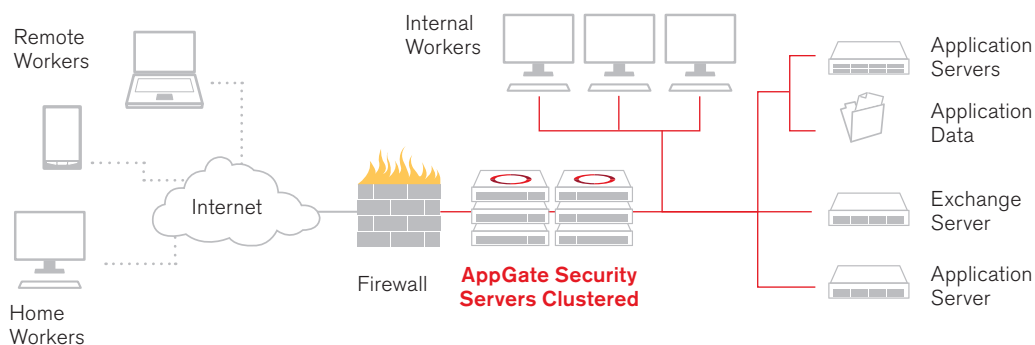
The AppGate system supports a wide range of client platforms so users can work remotely using any device – mobiles, laptops or home computers.

3rd party access

Network access for 3rd parties is easy to configure, control and monitor; 3rd parties can securely access applications without installing client software.

Cost savings

Nordic Edge one-time passwords remove the need to deploy and support physical tokens.




Microsoft Partner
 Gold Independent Software Vendor (ISV)

Cryptzone solutions mitigate information security risks in the key areas of Policy Compliance, Content Security, Secure Access and Endpoint Security.

International Headquarters

Cryptzone Group AB
 Drakegatan 7,
 SE-412 50 Gothenburg,
 Sweden

www.cryptzone.com
info@cryptzone.com

Regional Offices

Sweden
 Tel: +46 (0)31 773 86 00

United States
 Tel: +1.949.279.6177

United Kingdom
 Tel: +44 (0)370 013 1600

Partner information:

For more information go to
www.cryptzone.com/partners