

Case Study: NPSA



The Challenge

The National Patients Safety Agency's (NPSA) mandate is to lead and contribute to improved, safe patient care by informing, supporting and influencing organisations and people working in the health sector.

They are an arm's Length Body of the Department of Health and through their three divisions cover the UK health service.

The NPSA needed to respond to a government directive to become far more responsive and flexible in assessing and releasing information relating to incidents within the health service. The NPSA decided that one way to do this would be to allow more of their users the ability to remotely access the network. If this was achieved their user base would be in a better position to meet this requirement.

The main challenge for the NPSA was to allow flexibility for their users in the ways in which they were able to access the network, whilst at the same time ensuring that sensitive data and network resources could not be compromised. The NPSA's end goal was to allow greater flexibility for the remote user's whilst ensuring that sensitive data could leave the network.

The reason this was a challenge was that the end point devices would not always be administered by the NPSA. As such any solution would need to be clientless in order to reduce the administrative roll out cost to the NPSA. The NPSA also wanted to allow multiple levels of network access depending on user group, how trusted or un-trusted the end point device was and how secure the device was determined to be.

Working in partnership with the NPSA, CNS needed to identify the number of different types of end points that were present in their user base and define the levels of access that should be granted based on defined criteria.

The Project

CNS specialises in assessing security risks and balancing these risks against the effects on the usability of the network and the ease of accessing critical data, as well as the cost of implementation. For the NPSA project considerations included:

CNS designed, configured and installed a highly resilient hardware solution deployed behind the existing firewall architecture. These were securely housed in a DMZ and were able to provide clientless connection requests, ensuring end user transparency. Once authentication and client integrity had been passed authorised users were then forwarded to a Terminal Service device.

The users were then able to log onto the NPSA network as if they were connected internally, thus ensuring that both data and user integrity/confidentiality was maintained and more importantly contained on NPSA internal networks.

The Results

Using its consultative approach, CNS was able to implement a secure system which has been able to deliver all of the initial requirements stated by the NPSA.

NPSA staff are now able to securely access the network from anywhere and the system has allowed for their level of security threat to be identified before access to the network is granted. For example the solution will automatically identify if the end point device is a corporate laptop and will check to ensure that OS patch levels and anti-virus settings are inline with corporate security policies. If they are not to correct levels the user is required to remediate before access is granted.

By configuring the solution to work with Terminal Services the NPSA now has the ability to ensure sensitive documentation cannot be removed from the network via the remote access solution or via web mail.

Steve Head, Head of ICT at the NPSA “We found CNS’s service to be of an excellent quality and their consultants extremely professional. As usual they completed the project on time and within budget. I would have no hesitation in using their services again or recommending them to others.”

About Convergent Network Solutions

CNS is a specialist security and networking consultancy, established in the City of London in 1999. The company is wholly owned by its employees and directors. CNS has built an excellent reputation for information security & networking consultancy & services to our customers across a variety of sectors on a global scale. CNS's customers vary in size from FTSE 100 and large public sector organisations to SMEs, but are united in the importance of digital information to their business, and in their desire for pragmatic, knowledgeable help in securing their systems and data, and in meeting their connectivity requirements.

Contact Details

For further information or to arrange interviews, please contact:

Shannon Simpson, Sales & Marketing Director, CNS

Tel: 020 7213 0999 Email: Shannon.simpson@convnet.co.uk

