



# CASE STUDY

## NHS GREAT YARMOUTH AND WAVENEY

NHS Great Yarmouth and Waveney is a Primary Care Trust in East Anglia that wanted to improve security covering both its own PC network and also “unknown” PCs trying to access their network. The PCT has selected Sophos NAC Advanced software installed and supported by Foursys and is now able to enforce the security policies needed.

### Business Challenge

NHS Great Yarmouth and Waveney covers an area which is broadly aligned with Great Yarmouth Borough Council and Waveney District Council in East Anglia serving a population of approximately 230,000.

Whereas traditionally corporate networks have been fortresses protected from the outside world by firewalls, the age of flexible and remote working has presented a series of problems for those responsible for network security. This is combined with a growing need to allow visitors and staff to use their own hardware on the corporate network, and so the risk posed to an organisation’s security has never been greater.

After performing a risk assessment, the PCT highlighted two potential risk areas on their network. Firstly the risk posed by their own machines which could potentially deviate from their intended configuration, for example missing security software or patches.

Secondly and perhaps more significantly, unknown devices connecting posed a significant risk. Due to their physically dispersed network and the potential for “piggy backing” on to the network, the potential for unknown devices to connect to the network and obtain an IP address via DHCP was a real concern.

A solution was needed to reduce the risk to network security, both by limiting the network access of unknown devices, and ensuring that known devices met a baseline set of IT policies.

### Results

After assessing Sophos NAC Advanced via presentations and demonstrations provided by Foursys Ltd, it was clear to the PCT that it fitted their needs for a defence in depth model, providing a mechanism to control endpoint health and activity.

Sophos NAC Advanced has now been deployed to all PCs on the corporate network and to “guest PCs” seeking to access the network, enabling the PCT to enforce their security policies.

### Key Facts

<b>Organisation:</b>	NHS Great Yarmouth and Waveney
<b>Locaton:</b>	Beccles, Suffolk
<b>No of Users:</b>	1500
<b>Solutions:</b>	Sophos NAC Advanced

**Foursys Ltd** Specialists in Network Threat Protection

Stow Court Stow Road Quy Cambridge CB25 9AS

Tel(main): 01223 810910 Tel(technical): 01223 810911 Fax: 01223 810912 Email: sales@foursys.co.uk

Enhanced Support - Professional Services - Training

[www.foursys.co.uk](http://www.foursys.co.uk)



# Foursys

## **Solution – Sophos NAC Advanced**

After performing a successful evaluation of Sophos NAC Advanced, the PCT decided to proceed with a full implementation. Using four days of technical consultancy provided by Foursys Ltd, Sophos NAC Advanced with agent and DHCP enforcement was installed and deployed throughout the PCT's headquarters. Using the products flexible and phased deployment, the installation was successfully completed with no impact to end users.

Within days of the initial installation, the PCT had access to policy compliance information for their own hardware. This enabled them to remediate a number of issues before fully enabling NAC.

Upon completion of the project, the headquarters site was fully protected by Sophos NAC Advanced. The PCT hardware was 100% compliant with security policies defined within Sophos NAC, monitoring the status of AntiVirus software and ensuring that patches and service packs were up to date.

Any machines that deviate from this policy, for example where AntiVirus software is disabled, are now isolated from the network and remediated in order to reduce any potential risk.

Unknown devices connecting to the network are now isolated by NAC DHCP enforcement, and prevented from accessing internal systems. When authenticated with a guest logon, devices are assessed to ensure they pose no risk to the network, and then provided with filtered and logged Internet access.

## **Customer Feedback**

Andrew Brinded, IT Services Engineer for the PCT and technical lead for the implementation of Sophos NAC Advanced was impressed with the product and the way it was integrated by Foursys Ltd with the PCT's existing infrastructure.

"After dealing with Foursys with other projects we are confident in their abilities to deliver and support us. For a project as high risk as this we needed a company who are both knowledgeable and take every precaution during implementation to reduce the risk. I have been extremely happy with both the implementation and the support received from Foursys, due diligence was taken

during implementation and any issues experienced were dealt with swiftly, and the few issues which required escalation to the development teams at Sophos were made on our behalf by Foursys."

Andrew went on to explain how NAC has mitigated the risks initially identified.

"Since implementing Sophos NAC Advanced it has brought confidence to myself and my manager, and we now know (with a degree of certainty) that our endpoints are complying with our defined baseline policies. The key factor is that we also have the ability to ensure that an issue is immediately resolved."

"Sophos NAC provides the ability for us to say: 'If you don't comply with our policies, you get placed in a bubble and can only talk to a subset of the devices on our network' "

Andrew also added that although the PCT are very happy with the immediate benefits brought by Sophos NAC Advanced, he sees many additional uses for it moving forwards.

"Our currently configured policies are checking a few conditions, but we will look to expand further on this in the future. After having NAC fully active in our environment for some time now, we are planning to integrate NAC with 802.1x authentication for moving machines in and out of various VLAN's on our switches depending on their security posture."

Sophos NAC Advanced allows a phased deployment, enforcing varying policies for different users or sites. Whilst the PCT's headquarters is now fully enforced, remote sites can be deployed to in a report only mode, minimising impact to the end user.

"We will be starting several projects shortly, involving the majority of our GP sites and all of our community sites (over 50 sites). This will include the deployment of Sophos Anti-Virus, Sophos NAC and Utimaco SafeGuard".