

Sussex Health Informatics Service

HEALTHCARE

Sussex Health Informatics Service (HIS) manages the IT services for eleven National Health Service (NHS) trusts throughout the county. Its deployment of a new consolidated security suite from Sophos has helped tighten the security of its 25,000 user network from the email gateway to the endpoint computers, while the easy-to-use management features have eased pressure on IT resources.



Business challenge

Set up in 2004, Sussex HIS provides IT services for all the healthcare providers that make up Sussex's NHS trusts. Having inherited nine separate IT departments, its first challenge was to consolidate all operations onto one centrally managed network.

In 2007, the organisation turned its attention to unifying its IT security defences. Previously, each trust had chosen its own security solutions, but the overhead of managing products from McAfee, Symantec and Trend was causing a headache for Sussex HIS's staff. With each vendor classifying malware using

different criteria, there had also been a risk that some threats could slip through the net.

Alongside Civica, which provides managed IT services to public sector organisations, Sussex HIS embarked on a tendering process, comparing solutions offered by the world's major security vendors. They investigated how each solution could adapt to support Sussex HIS's operational needs, as well as assessing each solution's ease of management and ability to block malware, spam and potentially unwanted applications. The quality of after-sales support was also an important criterion.

Key facts

Organisation

Sussex Health Informatics Service

Headquarters

Sussex, UK

Number of users

25,000

Solutions

Endpoint Security and Control
Email Security and Control

"The technical superiority of the Sophos solution means we can ensure the integrity of all 11 trusts with just a mouse click."

*Steve Orman,
Technical Director,
Sussex HIS*

TECHNOLOGY SOLUTION

To simplify the management of the NHS trusts' IT security defences, Sussex HIS opted to install Sophos's best-of-breed technology across the whole of its 25,000 user network. According to Steve Reynolds, managing director, Civica, "Sophos was the clear favourite, offering the best implementation and support package, as well as taking on board Sussex HIS's complex needs." Crucially, Sophos enabled Sussex HIS to migrate over to the new solution gradually, which minimised upheaval to users and IT staff alike and was vital to the project's success.

Sophos's consolidated security suite combines two of the company's flagship solutions: Sophos Endpoint Security and Control and Sophos Email Security and Control.

The cross-platform endpoint protection is deployed on each and every desktop computer, laptop and server used by Sussex's eleven NHS trusts. Comprising anti-malware protection and Sophos Client Firewall, it is enabling Sussex HIS to block viruses, worms, spyware, adware, hack attacks and potentially unwanted applications from entering the network, all in a single scan.

It will also allow Sussex HIS to prevent NHS staff from installing unauthorised software applications such as Instant Messaging tools, voice over IP applications, streaming video and games. These applications are troublesome for Sussex HIS to manage, pose a threat to employee productivity and can expose the trusts to new malware attacks.



Sophos's automated management console provides a single point from which to deploy, update and report on the security status of all the various computers and devices connected to the network. For the first time, Sussex HIS has full visibility of the security of the entire network and, with fewer clicks required to perform each task, the amount of time needed to manage network-wide security is greatly diminished.

Sophos Email Security and Control delivers an extra layer of security for the NHS trusts. By scanning all inbound, outbound and internal messages at the email gateway, this solution is preventing email-borne malware, spam and phishing attacks from ever reaching staff inboxes.

With such a large network to secure, it is vital that Sussex HIS can close all potential avenues of attack. The organisation's new security defences rely on Sophos Behavioral Genotype® protection, which is able to proactively spot, quarantine and block any suspicious-looking code, in order to stop zero-day attacks. To provide further assurance, Sophos is on hand 24 hours a day, seven days a week, in case Sussex HIS needs assistance securing its network.

BUSINESS RESULTS

Sophos's consolidated, simple-to-use security solutions allow Sussex HIS to commit more resources to its everyday activities.

Steve Orman, technical director at Sussex HIS says, "We're delighted with the solution from Sophos and Civica, which exactly matches our operational requirements. Consolidating the IT security of eleven trusts is a tall order. However, Sophos has risen to the challenge and we can now ensure the integrity of our whole network with literally just one click of the mouse."

He is also confident that the new defences are best placed to protect the 25,000 user network from attack and concludes, "As a public sector organisation – funded by taxpayers – we undertook a rigorous tendering process to ensure we selected the best solution, at the best price. Furthermore, Sophos's flexible approach accommodated our requirements and enabled us to implement the new solution according to our time scale."

To find out how Sophos products can help protect your organisation, visit www.sophos.com/products