

Lancashire Care NHS Foundation Trust

Lancashire Care NHS Foundation Trust
Selects Sanctuary for Data Stored on Devices



Overview

Lancashire Care NHS Foundation Trust was formed in April 2002 to provide mental health and substance misuse services to adults of all ages across Lancashire. The Trust's vision is *'to be the provider of choice for mental health and substance misuse services in Lancashire'* and to this end it now employs over 3, 500 staff delivering services across many locations.

Over the last five years the Trust has invested to establish a modern and versatile information and communication technology infrastructure that will enable a flexible workforce and support the provision of better services in the years to come. More recently achieving foundation status has now become Lancashire Care NHS Foundation Trust.

The Trust has appointed Alan Boardman to the role of IM&T Security Systems Engineer and within that role fulfils the duties of the data security officer. Boardman is also responsible for meeting requirements of the Information Governance Toolkit.

The Challenge

As Data Security Officer for Lancashire Care NHS Foundation Trust, Boardman reports that his directive was to ensure that all USB memory sticks used by employees of the Trust were encrypted. This way, Boardman could be certain that even if a USB stick was lost or stolen, the data would be protected. He comments that drug company representatives often dropped off branded USB memory sticks to Trust employees and that it was difficult to control the types of devices that were being connected to such a disparate network. "These USB devices can store a tremendous amount of data, but they are so easy to lose," says Boardman. "We required USB

sticks to be encrypted so that if any are lost, the data is remains secure." Boardman researched the market to find a solution that would block all use of USB devices on the network unless they were of an approved type and encryption could be enforced.

"Initially I looked at open source solutions such as TrueCrypt, but this was not a system with central management, nor could I enforce encryption. We needed a data protection solution that would automatically enforce encryption."

The Lumension Security Solution

After looking at all the available products on the market, Boardman whittled the selection down to three products: DeviceWall; DeviceLock and Sanctuary Device Control.

Lumension's Sanctuary Device Control enables IT managers to create a "whitelist" of approved devices that are allowed to connect to their network. Everything else is blocked from running on that network by default. The software is granular enough to drill down to a particular serial number of a device to a named employee that allows the employee to use that device for work purposes. So an employee will be enabled to use that device, while all others will be blocked. Similarly, if that employee tries to connect a device that is not on the whitelist, this will be blocked by Sanctuary Device Control. Any authorised data storage can be logged by Sanctuary Device Control, so that the IT department always has a record of data downloaded to and from removable USB storage devices.

Boardman continues: "DeviceWall didn't allow the Trust to control removable storage devices in the way that we wanted to do it. DeviceLock had

no encryption at the time of evaluation. It allowed temporary whitelisting of devices, but it could only white list a particular class not a type of device model. In comparison, Lumension's Sanctuary Device Control offers you much more granularity, so you can white list a particular device model or even a serial number of a device."

Boardman selected Sanctuary Device Control and prepared to roll it out across the Trust in early 2008.

Following a number of high profile cases where government departments and banks had lost CDs containing sensitive consumer data, Boardman reports that many of the staff members at Lancashire Care NHS Foundation Trust were already aware of the risks to data from removable storage media. In addition, Prime Minister Gordon Brown had called for an update to the Information Governance regulations stating that all sensitive data in transit has to be encrypted and marked "Confidential".

However, before implementing Sanctuary Device Control across the Trust's network, Boardman undertook a staff education campaign to ensure that everyone was aware of the new security policy enforcement procedure. He placed advertisement banners on the front page of the Trust's Intranet and loaded data security articles onto the Lancashire Care NHS Foundation Trust's Intranet to educate staff on the importance of enforcing the USB device control measures. Global emails along with links on desktop wallpaper, ServiceDesk voice messages and a printed magazine article were utilised to bolster this. He followed this up with an amnesty on all the USB sticks that had been discovered to have been connected to the network before Sanctuary Device Control was installed. Once these rogue devices had been collected, the staff at the Trust was issued with an officially sanctioned USB memory stick for storing work data. No other USB memory sticks would be allowed to run on the network.

"We decided to standardise on one brand of USB memory stick. We screenprinted all of the sanctioned USB sticks with the Trust's head office postal code and PO Box number and marked them 'Confidential' so that if anyone found a stick they would know who to return it to, with the data encrypted via Sanctuary Device Control to avoid it being read. Each USB memory stick also has a unique engraved number"

During the staff education campaign, each line manager within the Trust was asked to order the official USB memory sticks through the amnesty so that Boardman and his team knew who had requested memory sticks and for whom. "We use an ITIL compliant service desk system and each USB memory stick with a unique number was assigned to a user as an asset within the system," explains Boardman.

He reports that the staff response to the deployment of Lumension's Sanctuary Device Control has been encouraging. "The media attention around the recent government department data security breaches really helped to drive the security message home. We have had lots of people approach us for advice on data security, which demonstrates that we have staff support for the new security measures, which is very positive."

The Benefits

The Trust's IT team can reset the password for them with a challenge/ response scenario. "There are a variety of removable storage media that we need to be able to monitor and control such as USB dictaphones and digital cameras," comments Boardman. "Sanctuary Device Control is really easy to implement: we just set up groups under each of the classes of device we want to control and then assign permissions to those classes. For example, USB printers is a class of devices. We can set up a rule so that everyone has access to a USB printer, but for another device such as a USB memory stick, we can set up a default rule so that no-one is allowed read/write access. In the case of our allowed USB memory stick, read write access is only allowed where the device is encrypted. We can also assign permission to individual people. So for example, another member of staff with different user privileges, using the same machine with the same USB device would not be able to connect that device."

According to Boardman, whitelisting is a more modern approach to securing data rather than creating an ever extending blacklist of devices that are not allowed. "Sanctuary Device Control allows us to enforce encryption across the Trust, because it allows us the flexibility to set up a policy that states that a particular type of USB memory stick can be used, but only if it's ours and only if it's encrypted. Sanctuary Device Control gives us the opportunity to shadow and log all usage of USB memory sticks for auditing and compliance purposes."

Boardman is also using Sanctuary Device Control to disable write access to floppy disks and control the use of CD/DVD writers across the Trust. Sanctuary Device Control has a feature that allows IT managers to discover every device that connect to their network in order to audit and control who has access to those devices and what types of files are on them.

He also cites the benefit of being able to use Sanctuary Device Control to turn off wireless networks whenever a wired connection is plugged into one of the Trust's machines. "This is really useful as the wireless connection could provide a bridge between insecure hotspots and I need to block that," says Boardman.

"We also used Device Control to find out which staff are still using floppy disks and wean them off. It is an archaic storage technology. We came across two people who were still using floppy disks and got two of my technicians to educate them on better and safer ways of storing their data."

Additional security measures put in place by Boardman included turning off the write function for DVDs and CDs by setting up a rule through Sanctuary Device Control that allows data to be read from these media, but not written to them. Currently, Sanctuary Device Control is being used to manage USB device use at 120 different sites and to manage a host of different disciplines.

Future Plans

Boardman is currently planning the roll out of Sanctuary Device Control across 8 or 9 Trusts and is waiting for the release of Lumension's Sanctuary Device Control 4.3 which will allow DVDs and CDs to be encrypted. He is also looking at other products that will allow the Trust to incorporate email encryption to secure communication with partners and suppliers. "We've always had data encryption as a policy and Sanctuary Device Control just enforces that policy. In that sense, Sanctuary Device Control is an enabler to the business. It enables you to put information

onto a USB memory stick and not worry unduly that it's going to be seen by the wrong person," concludes Boardman.

"I now don't have to worry about loss of reputation through someone losing a memory stick which may contain person identifiable data or corporate sensitive information. Now that I've installed Sanctuary Device Control I can sleep soundly knowing that's not going to happen."

About Lumension Security™, Inc.

Lumension Security, a company formed by the combination of PatchLink® Corporation and SecureWave® S.A., is a recognized, global security management company, providing unified protection and control of enterprise endpoints for more than 5,100 customers and 14 million nodes worldwide. Leveraging its proven Positive Security Model, Lumension enables organizations to effectively manage risk at the endpoint by delivering best-of-breed, policy-based solutions that simplify the entire security management lifecycle. This includes automated asset discovery, vulnerability assessment, remediation and validation; application and device control; extensive policy compliance reporting; and integration with leading network access control solutions. Headquartered in Scottsdale, Arizona, Lumension has offices worldwide, including Virginia, Florida, Luxembourg, the United Kingdom, Spain, Australia, Hong Kong and Singapore.



Lumension Security
15880 N. Greenway-Hayden Loop, Suite 100
Scottsdale, AZ 85260
480.970.1025 / www.lumension.com

©2008 Lumension Security. All rights reserved. Lumension Security, the Lumension Security logo, and the PatchLink and Sanctuary product names and logos are either registered trademarks or trademarks of Lumension Security. In addition, other companies' names and products mentioned in this document, if any, may be either registered trademarks or trademarks of their respective owners.