Case Study

INFINIGATE
.... Adding Value to Distribution

Safend & NHS Wales:

Safend fits the bill and ensures data loss prevention at NHS Betsi

GIG CYMRU NHS WALES
Bwrdd Iechyd Prifysgol
Betsi Cadwaladr
University Health Board

safend
a SuperCom company

Overview

Organisation:	Betsi Cadwaladr University Health Board, Bangor – a National Health Services (NHS) Wales site.
Number of IT staff:	60
Number of users:	18,000 / 8,000 nodes
Key Challenges:	Time, budget, compliance with National Encryption Policy and impending GDPR.
Solution:	Safend Protector, Reporter and Auditor.
Benefits:	Greater visibility, control, compliance and no more USB-introduced viruses.

Background

The National Health Service (NHS) Wales is a publicly-funded service providing healthcare to more than three million residents. It is comprised of eight Health Boards, one of which is the Betsi Cadwaladr University Health Board in northern Wales. The Betsi site has 60 IT staff managing around 7,000 nodes and 18,000 users.

The major driving factor for Betsi seeking out a data loss prevention solution was the need to comply with policies surrounding data and encryption. Firstly, the National Encryption Policy in Wales had mandated that all organisations (particularly the NHS) ensure any electronic or mobile data must be encrypted. What's more, the impending changes to the General Data Protection Regulation (GDPR) in 2018 meant new regulations would soon apply.

The confidential nature of the information held by the NHS placed them under the microscope of the Information Commissioner's Office (ICO) and susceptible to fines they could not afford to pay. Data loss was simply not an option.

Business Challenges

The greatest challenge facing Betsi's IT team was money – tight budgets, ageing infrastructure and regular overspending. Keith Williams, Senior ICT Systems Engineer explains that the Betsi NHS region was recently the 4th most overspent NHS site in Wales with £30 million overspent.

On top of those concerns, the sensitive nature of patient health records means that data breaches within the NHS incur hefty fines from the ICO. Money that Keith believes could be better spent on the patients. This is a valid concern considering the Betsi site experienced between 50-100 viruses per week – 95% of which came from the use of USB devices. "We've been lucky we've had very few data breaches", he says.

Keith also cited time constraints as a challenge. He explains, "Although we have 60 people in the IT team, I'm the only person specialised in the IT security systems we have in place – antivirus, encryption etc. Any IT security function in the organisation comes to me."

Solution

With little time and money to become compliant with the encryption policies, Betsi began comparing suppliers. "We evaluated various Data Loss Prevention (DLP) solutions but it came down to McAfee and Safend", explains Keith. While the Betsi site already had McAfee data loss prevention software in place, to add the encryption feature would have been "prohibitively expensive and time consuming".

In terms of the deployment, Keith says McAfee was out of the question. "It would be me doing nothing else for 6 months", he explains. "With the amount of time and money we had, Safend was the best option".

The Safend Data Protection Suite (DPS) is a modular solution consisting of Auditor, Protector, Encryptor, Discoverer, Inspector and Reporter which can be combined through a single endpoint agent and deployed according to an organisation's requirements. The Betsi site opted for 8,000 Protector, Reporter and Auditor modules.

Figure 1 - Safend Data Protection Suite (DPS)

Safend Protector offers granular control to devices entering or leaving the organisation. It does this on a number of levels. It allows for the lock down of lesser used ports such as serial, mode, firmware ports etc. giving peace of mind that these cannot be exploited. Where ports are enabled, Safend DPS can detect and restrict devices or enforce encryption according to device type, model or unique serial number; here it is possible for Betsi to specifically allow devices or machines by their unique identity (medical equipment for example) whilst blocking everything else.

A key requirement for Betsi was the control of USB keys carrying data. With strong policy-based file encryption capabilities and built in compliance policies, Protector allows security administrators to either block all storage devices completely, permit read-only or encrypt all data. This gives Betsi the ability to enforce encryption on cheaper unencrypted USB keys and not only guarantee that the data on the move is still secure but it helps by reducing the cost of those keys in the first place. It does all this whilst setting a baseline for how data in motion is controlled.

This can all be achieved because Safend DPS allows for the creation of granular policies that can be applied to user groups or AD structures to enforce a DLP solution.

Keith explains that the Safend DPS allows the IT team to enforce those security controls while still providing data availability to those who are authorised to access it. "The controls on the endpoint encourage users to use email instead of USB drives as it's our preferred method of file transfer. The solution offers greater control, it allows us to authorise certain people in certain functions to be able to access different information" he says.

This is supported by the regulatory compliance and security log summaries of the Reporter module, as well as the comprehensive endpoint visibility and risk detection of the Auditor module.

Figure 2 - A key requirement for Betsi was the control of USB keys carrying data

Benefits

Aside from the price, Keith found the ease of deployment as being a key benefit. Considering his time constraints, a lengthy deployment was unfavourable. “The actual deployment of the solution was absolutely easy. We deployed it via Microsoft System Centre Configuration Manager (SCCM)”, he says.

Compliance with the National Encryption Policy became a concern of the past and key areas of the GDPR were addressed, with Keith putting full trust in the solution. “We have to maintain security in accordance with the GDPR and Safend DPS will 100% help us to become compliant”, Keith says. This can be attributed to the Safend Reporter module which is designed as a compliance reporting solution. It answers to PII, UK Data Protection Act (DPA) and other stringent requirements, providing in depth compliance reports and security log summaries.

Figure 3 - The implementation of Safend DPS has also helped to make NHS Wales become compliant with the incoming EU GDPR

Safend provides tamperproof logging of all activities occurring with devices that are connected to the endpoint including all files that are downloaded to or read from these devices. It is possible to create an audit policy that can take a complete snapshot of the actual files that are being transferred and securely store them for review by an authorised controller. With roles-based permission allowing staff to see exactly what has occurred.

The reporting module can be used to provide scheduled or one-off reports on the state of the deployment and how effectively the policy is being enforced. This can give management the visibility to show compliance or risk mitigation when needed.

> *“We have to maintain security in accordance with the GDPR and the Safend DPS will 100% help us to become compliant.”*
>
> - Keith Williams, Senior ICT Systems Engineer, NHS Wales

One unexpected benefit for Betsi was the protection from malware. “Antivirus wise, 95% viruses coming through were coming from USB drives. It has since dropped to 0 because of the file control function – which allows you to designate which types of files are allowed to or from storage devices,” Keith says.

“We block executable and script files and that has taken us down from 50-100 viruses a week to 0,” Keith says. “The Safend solution has well and truly paid for itself in just the malware prevention alone”.

Keith says he has a very good rapport with Infinigate and finds them to be very responsive in providing solutions to the issues faced at Betsi. “They are like friends,” he says. He reports that thanks to the Safend / Infinigate solution, they now use fewer USB drives and no longer have the worry of the data commissioner’s fines.

> *“The Safend solution has well and truly paid for itself in just the malware prevention alone.”*
>
> - Keith Williams, Senior ICT Systems Engineer, NHS Wales

W: www.infinigate.co.uk | T: 0207 593 3290 | E: marketing@infinigate.co.uk

About Safend

Safend is a leading provider of endpoint data protection software. Their products protect against corporate data loss by offering comprehensive data encryption, port control, device control, content inspection, ensuring compliance with regulatory data security, and privacy standards. Safend's products encrypts CD/DVDs, removable storage devices, as well as internal and external hard drives. Safend provide granular port and device control over physical, wireless, and removable media devices. Additionally, they provide control over sensitive data transferred over endpoint and network channels. With more than 3,000 customers worldwide and 3 million licenses sold, Safend's software is deployed by multinational enterprises, government agencies, healthcare organizations, and small to mid-size companies across the globe.

safend
A SuperCom company

www.safend.com

About Infinigate UK

Infinigate is a leading Value Added Distributor (VAD) of IT security solutions in Europe and a Safend Platinum Partner. The company was founded in 1996 and has today 8 subsidiaries. Infinigate offers state-of-the-art IT-Security solutions through its European partner network (VARs, integrators, consulting companies, etc.) to secure and protect IT networks and data.

INFINIGATE
.... Adding Value to Distribution

www.infinigate.co.uk

W: www.infinigate.co.uk | T: 0207 593 3290 | E: marketing@infinigate.co.uk