



Health insurance giant immunizes against data theft.

devicewall[®]

BUSINESS DRIVER

Protect against identity theft and data loss of personal, medical and financial information
FSA security recommendations

INDUSTRY SECTOR

Health Insurance

NETWORK TYPE

Decentralized over five sites in two countries

WHY DEVICEWALL

Quick to install and easy deployment, active directory

BUSINESS BENEFITS

Reduced risk of internal IT security breaches

With the FSA highlighting the risk of data theft in the financial sector and more devices than ever entering the workplace, one of the UK's leading health insurance providers HSA turned to DeviceWall to help defend against the threats of identity theft and data loss.

Introduction

With a history dating back nearly 100 years, the HSA Group provides health cash plans and private medical insurance for over two million members in the UK and Ireland. Over the last five years, a major program of expansion and computerization has led to radical changes in the way the company does business, with a greater reliance on IT systems and electronic records.

During 2005 and early 2006, HSA undertook a major project to integrate IT systems across its sister companies, covering eight buildings and five sites in the UK and Ireland. Each company had different IT infrastructures and a different approach to data security. However, common to all the companies within the group was the need to protect the personal health, medical treatment and financial records of their many members.

A new threat to data security

With USB, Firewire and other fast data connections now standard on most PCs, HSA grew concerned that there was an increasing danger that small, cheap portable storage devices could be used to either remove sensitive information from the network or introduce unwanted content onto company PCs.

Kevin Quinn, operations manager at HSA explained: "We were already familiar with using USB sticks within the IT team. We quickly recognized how easy it was to use one of these devices to take data from the network and out of the building without anyone noticing."

At the same time, the Financial Services Authority (FSA) issued a set of security recommendations for regulated organizations in the UK, which warned of a trend among criminal gangs to seek employment in financial firms solely to get access to customer data. Although currently only a guide, HSA took the advice to heart and began considering how to combat the threat of data loss and identity theft.

With 1,000 desktops and laptops, a large call centre and sensitive customer data moving in and out of each office, a consistent approach to security was needed. Usability was key to successfully managing access to portable storage devices. While HSA wanted to automatically block the unauthorized use of all types of devices, from CD-ROM drives and iPods, to digital cameras and PDAs, it was important that they could also support the legitimate use of these devices by appropriate employees.

What's more, with staff often having access to multiple PCs, it was important that HSA assign the right security privileges to individual employees, not PCs



devicewall[®]

"DeviceWall has provided us with an easy, low-cost way to prevent the unauthorized use of portable storage devices by computer users, and thus avoid a potentially crippling security breach."

Controlling access

It was at this time that Quinn was introduced to DeviceWall from Centennial Software. He downloaded the software and initially installed it on a small number of machines within his department. After using DeviceWall for a month, it was clear that deploying across the ever-growing network would be easy and the functionality gave him the flexibility he needed to match security with business productivity.

DeviceWall enables organizations to secure the network against the risks presented by portable storage devices by preventing the unauthorized local and wireless connection of unwanted devices to company-owned PCs. The software makes it easy to create and enforce a security policy that determines which employees in the company should be able to access different types of device.

"Within DeviceWall, we've created user groups based on the Active Directory user information already set up for each employee – allowing us to automatically assign different rights to appropriate employee groups. And because each employee takes their security rights with them wherever they go, we know that mobile staff working remotely are just as secure as those inside the building," continued Quinn.

Each site took just a single day to install. "My biggest concern was how the users would take to the new security measures," said Quinn. "However, by using the configurable dialogs within DeviceWall, combined with active user education on the security issues we face as a company, the reaction has been very good. It certainly helps that DeviceWall makes it easy for administrators to grant temporary access rights to a user who has a specific need to access a blocked device."

Legitimate use

Quinn's team had a few surprises as the roll-out progressed. For example, when they set up the permissions at headquarters, the team soon received calls from the senior executives asking why their PDAs would no longer synchronize.

"The company had never sanctioned the use of PDAs, yet obviously their use was already quite widespread. Luckily, DeviceWall made it easy for us to set up a 'senior managers' group and allow the appropriate people to access their PDAs – all within a couple of minutes from receiving the first call," said Quinn.

A major reason for choosing DeviceWall was the ability to avoid a blanket lockdown on all portable devices. Training staff, for example, are heavily reliant on using portable storage devices to deliver training courses across the Group's offices.

"With trainers allocated to a group set up in DeviceWall, these individuals are able to have access to the files they need to take on the road. This is cheaper and presents far fewer risks than equipping the team with laptop computers," said Quinn.

Likewise, the IT team at HSA can work on any PC in the company and use all the connections they need to transfer data and software without having to give access to all the users of that machine.

Completing the roll-out

Looking forward, Quinn is eager to implement some of the latest DeviceWall features, including the ability to remotely monitor all types of device connection across the HSA network.

"Although HSA had never suffered a security breach where customer data had been stolen, I wasn't prepared to gamble that it wouldn't happen in the future," concluded Quinn. "DeviceWall has provided us with an easy, low-cost way to prevent the unauthorized use of portable storage devices by computer users, and thus avoid a potentially crippling security breach."



CENTENNIAL
software

www.centennial-software.com

UK	+44 (0)1793 836200
USA	+1 503-238-7455
Australia	+61 2 9973 4151
Germany	+49 (0) 6047 6281
SA	+27 (0) 83 604 0 603