Case Study

Care UK Plc protects data and meets NHS legislation with Becrypt security solutions

Leading independent provider of health and social care implements robust data security solutions with centralised management.

Care UK is a leading independent provider of health and social care. Working in close partnership with local authorities, Primary Care Trusts (PCTs) and Strategic Health Authorities (SHA), the company provides tailor-made service solutions, including residential, community, specialist, primary and secondary care. It operates over 50 nursing and residential homes for older people and provides over 120,000 hours of care and support every week to people in their own homes.

In the health sector, Care UK is the largest operator of NHS independent sector treatment centres in the UK and is active across a wide spectrum of care services. It operates GP practices; NHS Walk-in Centres; GP out-of-hours services and some prison health services as well as highly innovative Clinical Assessment and Treatment Services (CATS).

Securing data to protect patient and company assets

In order to enhance security measures and to safeguard patient, company and employee data, Care UK has chosen to implement the Becrypt data security solution. To work alongside the NHS it is essential to comply with appropriate legislation for data protection.

Care UK has rolled out Becrypt DISK Protect and Enterprise Manager across its laptop estate. The next phase of the project will be to replace a host of inherited solutions and to standardise on Becrypt's security suite for all mobile devices.

According to Owain Jones, IM&T Project Manager at Care UK; "Over recent years the business has grown with acquisitions

that the company has made. This has meant that our hardware estate has increased considerably and we wanted to implement a new security solution that would enhance and further safeguard data against accidental loss and theft.

Care UK trialled three security solutions, selecting Becrypt DISK Protect solution for its ease of use, both to the user and for the IT team. The team set about rolling DISK Protect out to over 50 key worker laptops, with the intention to increase this to another 500 laptops over subsequent months using the central management capabilities provided by Becrypt Enterprise Manager.

Smooth rollout and management
"We chose Becrypt's solution as a proven Full Disk Encryption (FDE) solution that is FIPS compliant. We liked the look and feel of Becrypt's DISK Protect. It is extremely easy to use and totally transparent to the user. This has proven to be the case – when we rolled it out, the calls to the help desk were very few."

FIPS accreditation has helped Care UK to meet government data security compliance requirements. The organisation is required to protect patient identifiable data (PID), which can now be easily managed using DISK Protect.

Initially DISK Protect has been installed on each machine separately with dual factor authentication using Active Directory. In future it will be rolled out automatically from Becrypt Enterprise Manager with single sign on, in order to make it as transparent to the user as possible.

"The central control uses Active Directory to package installations making it very easy to distribute on new laptops," explained Jones. "After we have installed DISK Protect the encryption overhead is such that there is no noticeable degradation in

Becrypt help Care UK Plc to:

• Ensure data confidentially through disk and device management

• Provide endpoint control for policy enforcement

• Meet data security regulation

laptop performance. We don't even need to make users aware of it – the transparency is fantastic."

Secure systems architecture

The Becrypt solution plays a significant part in Care UK's overall systems architecture for information security, governance, compliance, ISO27001 and IGSOC (Information Governance Statement of Compliance). IGSOC is the document that defines the minimum standards and processes that an organisation must comply with before being able to connect to CFH systems.

Since the company has implemented DISK Protect, it has been reviewing the suite of Becrypt security solutions. While DISK Protect provides full disk encryption with Enterprise Manager at the back end, the company is also implementing Connect Protect for full USB port control, as well as Trusted Client for secure remote working and Becrypt Media Client and Removable Media Module for safeguarding data stored or transported on portable media such as USB sticks, CDs and DVDs.

Currently the central control enables distribution of DISK Protect via a group policy and provides a full audit of security breaches. Changes can be implemented across all machines centrally – such as changing password formats to increase security, or enabling or disabling USB ports.

The IT team is also able to assign multiple logins to machines, enabling hardware resource to be shared securely.

"With a full suite of security products we can manage our data security from all aspects," explained Jones. "We can sign our own devices and make sure that only our secure USB sticks are able to connect with our machines, so that external parties cannot use USB sticks on our computers. The reporting capabilities are great – we can monitor everything from a central location".

"We have such a distributed environment with excellent company connections, that the functionality we have for centralised control is great. It gives us a very robust solution even without the compliancy directives. We have full control and administration over passwords and data security."

The scalability of the solution is an important factor for Care UK, enabling it to deliver the functionality across PDAs and other hardware platforms.

"With Becrypt solutions we are assured that we have data confidentiality through disk and device management. It allows us endpoint control for policy enforcement to meet all data security regulations," said Jones.