

CREDANT Technologies delivers data security for 3,000 laptops in a major government department.

Last September, an outsourced IT team at one of the largest departments in the UK government received an urgent directive – data security for the department's laptops would have to be significantly increased. The team immediately began a review of IT software solutions for mobile data security.

Over a dozen IT security vendors were contacted as possible candidates for implementing the new security solution. CREDANT Technology was included because the company had been named a "Leader" in the 2007 Gartner "Magic Quadrant" for mobile data protection. This leadership position is based on the combination of a company's completeness of vision and its ability to execute that vision.

Meeting unique needs

Over a series of meetings, presentations and evaluations, CREDANT Mobile Guardian Enterprise Edition from CREDANT Technology was chosen as a finalist. This selection was based on a number of factors related to the unique needs of the government department.

First of all, the department needed a solution that would easily adapt to their existing IT infrastructure, operational procedures and user skill sets. They also wanted a solution that could be easily deployed to thousands of users.

With these needs in mind, the IT team was impressed with the broad platform support, scalability and easy implementation available with CREDANT. They were also impressed with CREDANT's centrally managed console for administration. They discovered that CREDANT is the only centrally managed solution for mobile data security, enabling organisations to both encrypt and secure data across multiple, diverse platforms from a single console.

Of course, security remained the single most important consideration. CREDANT addresses this by combining Policy-based Intelligent Encryption, enforcement, automatic device detection, authentication, auditing and reporting capabilities. Other security features include the automatic generation and escrow of the encryption keys at the server level, increasing security while supporting simple, immediate data recovery. Furthermore, CREDANT permits multiple users to securely share information on the same desktop or laptop, while still allowing individual users to access data permissible only to them – helping to guarantee that a local administrator cannot access data.

Equally significant to the IT team was the fact that CREDANT is not a sector-based solution, and therefore avoids the inherent restrictions and limitations common in those types of solutions. From its architecture to its interface, CREDANT can be adapted to a multitude of IT environments, organisational requirements and data security needs.

A winning solution

CREDANT was selected in February after a final, detailed evaluation. The selection was based on a variety of reasons, including the ability of CREDANT to interoperate within the existing infrastructure without the need to change, add or delete any processes or components. Other products often require the provisioning of multiple servers and laborious patch-management procedures.

After purchase, the CREDANT solution, including CREDANT Enterprise Server, was quickly implemented across the department. An average of 250 laptops per day were provided with CREDANT Shields. The CREDANT Shield



Don't Regret, Protect

resides on devices and they are considering extending coverage to include external media to enforce security policies even if the device is disconnected from the network. It enforces strong authentication, policy-based intelligent encryption and device and end-user controls so the data on devices is always protected.

This protection is reinforced by the CREDANT Local Gatekeeper. This component resides on desktops and notebooks to automatically detect, apply policy and control mobile devices that are connecting to and through the desktop or laptop.

In addition, the CREDANT Policy Proxy was implemented at the network level to provide secure distribution of policies and policy updates. The Policy Proxy also collects device inventory and reports the information back to the CREDANT Enterprise Server for audit-

ing and reporting.

Working together, these components have enabled the IT team to deploy a highly scalable solution that required virtually no changes to the department's existing IT infrastructures. The team has also been able to add data security with little or no impact to end user or IT productivity. Additionally, CREDANT provides automatic activity reports that record data access and offer proof of end-to-end data security.

As of today, more than 3,000 departmental laptops are being protected with CREDANT Shields. The department is pleased with their strengthened security, and the IT team is looking at new areas where CREDANT can be deployed to further enhance data protection for mobile devices.

As published in Government Technology Magazine, October 23, 2008.