

Cirquent Consulting – IT Consultancy

Organization

Cirquent GmbH

Locations

Munich (headquarters) + offices in Hamburg, Cologne, Frankfurt, and Ettlingen plus subsidiaries in Austria, Switzerland, and the U.K.

Workforce

Around 11,750

IT infrastructure

1,250 notebook + desktop PCs – 94.3% of which have Windows XP as the operating system (as at: end of 2009)

IT Security solution

SafeGuard Device Encryption (hard drive encryption)



About the customer

Cirquent is one of Germany's leading IT consultancies. With its headquarters in Munich and further offices in Hamburg, Cologne, Frankfurt, and Ettlingen plus subsidiaries in Austria, Switzerland, and the U.K., Cirquent prides itself on being a reliable partner to its customers. And to ensure that this reliability extends to matters of security, Cirquent consultants lead by example: using SafeGuard Device Encryption von Sophos, they encrypt the hard drives in their own notebooks, which are used to store and process large amounts of sensitive, business-critical information for a range of big-name customers.



Cirquent's requirements

Around 90 percent of Cirquent's 11,750 consultants work with notebooks and other mobile devices. It was therefore essential for the technology consultancy firm to secure the often business-critical and highly valuable information stored on these computers against theft, loss, and espionage. To address this need, Miguel Heinrich, CISO (Chief Information Security Officer) at Cirquent ordered the rapid introduction of hard drive encryption. „And some of our customers, especially those operating in the automotive sector, also explicitly demanded encryption of the notebook hard drives used by Cirquent consultants working on certain consultancy projects,“ says Markus Höfl, IT Infrastructure Consultant at Cirquent. In addition to notebooks, it was also necessary to encrypt the internal hard drives of desktop PCs to prevent the data being accessed by third parties once these computers reached the end of their IT lifecycle and were retired from the company.

The shortlist drawn up by the company included the IT security solutions Safeboot from McAfee, BitLocker Drive Encryption from Microsoft, and SafeGuard Device Encryption from Sophos. With the support of the IT service provider five(9)s, a longstanding Cirquent solution partner for client management, Markus Höfl compared and analyzed the three software products in line with the following criteria and requirements.

“Using hard drive encryption to protect its valuable know-how against theft, loss, and espionage was an essential requirement for technology consultancy Cirquent. And some of our customers, especially those operating in the automotive sector, also explicitly demanded encryption of the notebook hard drives used by Cirquent consultants working on certain consultancy projects.”

Markus Höfl, IT Infrastructure Consultant at Cirquent

The solution had to

- ▶ operate independently of the hardware used (hard drives, device types, and models) - with a focus on the operating systems Windows XP, Vista, and Windows 7
- ▶ support central, role-based administration - worldwide and across multiple Windows domains
- ▶ enable access to encrypted devices even in offline mode
- ▶ be capable of recovering the encrypted data centrally and be auditable
- ▶ allow integration with a PKI with single-sign-on function that was to be implemented later
- ▶ and, finally, the software needed to be capable of being installed on around 80 percent of workstations within a three-month period.

Since 94.3% of all Cirquent consultants work with Windows XP, the BitLocker solution, developed for Windows Vista and Windows Server 2008, did not meet the company's requirements. Rolling out Vista/Windows 7 would have complicated the project objective, which was to encrypt all available PCs in the second half of 2009.

Out of the two remaining alternatives, the Sophos solution not only met all requirements, but was also already being used successfully at one of Cirquent's shareholders, the Japanese IT company NTT Data. The IT consultancy therefore decided to implement SafeGuard Device Encryption.

The Sophos solution

SafeGuard Device Encryption prevents unauthorized access to mobile and stationary terminals through simple, transparent encryption of the entire hard drive and removable media.

If the terminal enters the wrong hands, the data remains inaccessible to unauthorized individuals, even if the hard drive is dismantled. SafeGuard Device Encryption is a functional module of SafeGuard Enterprise, the central Sophos solution for managing data security - even in mixed IT environments. SafeGuard Device Encryption is administered using the central console in the SafeGuard Management Center. Its implementation went according to plan and proceeded without incident.

The central administration function includes the following features:

- ▶ Consistent, central specification and monitoring of security policies: Monitoring of compliance with security policies for user authentication and encryption for both end users and user groups.
- ▶ Key management: Creation, distribution, backup, reallocation, and recovery of keys and certificates. Thanks to intelligent key management (key ring function), users and administrators can easily use data across different groups and devices.
- ▶ Reporting and auditing: Client activities and security statuses are logged and saved centrally. Internal security policies determine the type and content of the logs.
- ▶ Recovery of data/passwords and forensics: Compatible with standard recovery and forensics software available in the market. Efficient emergency mechanisms such as the challenge/response procedure for forgotten passwords

“SafeGuard Device Encryption not only meets our requirements 100%, but also integrates very well with existing applications.”

Markus Höfl, IT Infrastructure Consultant at Cirquent

Conclusion: Implementation proceeded according to plan, on time, and without incident.

Within just eleven weeks, Cirquent had installed the encryption software on 1,250 computers on time and during ongoing operation (see graphic for client installation progress). According Markus Höfl, who had been in charge of the project, significantly less than one percent of notebooks experienced technical problems in the form of total failures.

On the whole, the IT expert is extremely satisfied with the installation process and the security solution itself.

Communication with the IT service provider five(9)s and the rollout documentation were also ideal. Together, Sophos and five(9)s support the consultancy firm by issuing information about issues such as compatibility problems and by providing the necessary updates, patches, and upgrades.

United Kingdom Sales:
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales:
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia & New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Boston, USA | Oxford, UK
© Copyright 2012. Sophos Ltd. All rights reserved.
All trademarks are the property of their respective owners.

Sophos Customer Success Story 11.10v1.dEN

SOPHOS