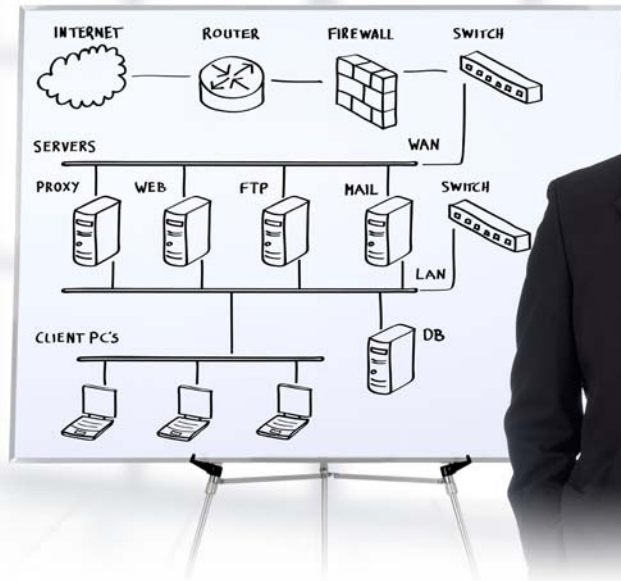




Wave Systems' EMBASSY® software for managing self-encrypting hard drives provides unrivaled data security for VEGA's laptops and minimizes administrative tasks.



VEGA Deutschland

Industry
Engineering & Consulting Services

Benefits Summary

- Full-disk encryption (FDE) in minutes
- Lower setup and support costs
- Centralized management of remote laptop encryption features
- Zero-impact on system performance or application software
- Proof of compliance with data protection regulations

A little over thirty years ago, VEGA Deutschland began offering satellite operations support for the European Space Agency. Since then, it's cultivated a reputation for consistently spot-on systems and software expertise, as well as impeccably professional integrity and discretion when it comes to handling sensitive client data.

Today, VEGA's reputation has earned them clients in multiple European markets, from defense and aerospace to high finance and the public sector. Unwilling to rest on its laurels, VEGA continues to seek leading-edge technologies to ensure the security and privacy of its client's most sensitive business information.

THE CHALLENGE:

Provide full-disk encryption (FDE) to secure confidential and classified information stored on 300 laptops distributed throughout Europe.

VEGA's outstanding reputation for handling sensitive client data took over thirty years to build. Yet even a suspected data security breach from a lost or stolen laptop could collapse that hard-earned reputation over night.

With more than 300 consultants operating at client sites across Europe, VEGA cannot take chances when it comes to protecting the information stored on its laptop hard drives. Such data encompasses confidential timelines, budgets and strategic details for its clients in aerospace, finance and government, as well as competitive or personal information about VEGA's own operations and employees.

A lost laptop or data breach would not only hurt VEGA's professional image, it could impose an immediate financial impact. In some cases, a loss of client data through negligence could even lead to legal prosecution and imprisonment.

Christian Schmidt, VEGA's Information Security Operations Manager, recognized he needed a full-disk encryption (FDE) solution to minimize exposure to such risks. The question was: What type of FDE provided the most confidence?

His research indicated that software-based solutions didn't deliver that confidence. Software solutions are vulnerable to known published attacks and therefore, Schmidt felt, could be bypassed by "smart kids on the street."

Plus, software solutions are costly to setup and maintain. By Schmidt's calculations, installing FDE software takes about eight hours per laptop. Two of those hours would require direct IT staff member involvement, while the other six signify how long the software would take to encrypt the contents of the hard drive. Meanwhile, that meant the laptop's owner — one of VEGA's highly skilled consultants — would be inactive for eight hours. Once Schmidt figured in the comparatively minor costs of travel, he estimated that software-based encryption of a single laptop would cost in the neighborhood of €1,500 (US \$2,000).

Another consideration was that software-based FDE could potentially interfere with the home-grown software that VEGA consultants run on their laptops. Although, most leading independent software vendors test for compatibility with

commonly available programs, Schmidt wasn't confident that software-based FDE would be compatible with VEGA's proprietary code on day one — or on any subsequent occasion — as they would have no assurance that future versions of their software would behave without conflict.

Overall, Schmidt's research led him to conclude that software-based FDE posed unacceptable administrative, logistical and performance costs, and still failed to sufficiently protect VEGA's laptops from a data breach.

THE SOLUTION:

Seagate self-encrypting hard drives managed with Wave System's EMBASSY Trusted Drive Manager and EMBASSY Remote Administration Server (ERAS).

The clear alternative was hardware-based FDE, which Schmidt learned about through VEGA's preferred PC provider, Dell Inc. Dell works closely with Seagate — a pioneer of self-encrypting drives — and Wave Systems, a leading provider of encryption management software to offer customers turnkey solutions for data security.

In VEGA's case, that solution took the form of a Dell Latitude™ E-Series laptop incorporating Seagate's Momentus 7200 series of self-encrypting hard drives. Management of the Seagate drive relied on Wave's EMBASSY software.

While self-encrypting drives are the best choice, a complete data protection solution requires more than just encryption. It also requires policy-based access controls, centralized management and proof of compliance. Wave's EMBASSY software provides these essential capabilities and more.

Wave's Trusted Drive Manager, a client application that activates the on-board security features of Seagate's encrypting drives, provides authentication that is stronger than Windows®, and enables a secure erase feature that allows for the safe retirement or disposal of machines and drives. The technology immediately enforces policy-based access controls when the PC is powered on. Its support of single sign-on to Windows provides a friendly and familiar user experience. In addition, integration with Windows password update allows the drive access policies to be automatically updated with Windows, ensuring compliance to company password policies.

VEGA's distributed deployment of hundreds of self-encrypting drives required centralized administration of users, credentials and access rights, all of which are provided by EMBASSY Remote Administration Server (ERAS). With ERAS native integration with existing directory structures and policy distribution mechanisms, assigning users and policies can be performed within the directory framework — dramatically simplifying deployment.

THE BENEFITS:

Quick to install, simple to administer and virtually impossible to penetrate data security. Plus, the ability to remotely deploy and administer security solutions from a central location.

From a purely logistical perspective, Schmidt found Wave's solutions were radically simpler to install and administrate compared to software-based FDE alternatives he researched.

"All you have to do is connect the laptop to the network, lock onto the console, initialize it and you're on to the next laptop. It takes five minutes," he said. Also, because it eliminates the time and expense of software encryption, Wave's simple solution encourages completion of security administration tasks to occur on a more regular basis.

There were additional benefits for VEGA's end-users — its highly traveled engineers and consultants. First, hardware-based FDE operates independently of a laptop's computing resources and operating system. So, it neither slows down the machine, nor generates conflicts with software applications.

Plus, because Wave's technology supports Windows® single sign-on and password synchronization, end users need remember only one password to secure both the contents of a laptop's hard drive and its active Windows profile. That simplifies the task of securing VEGA laptops, since the firm requires its consultants to change their passwords every ninety days. Fewer passwords to remember means fewer help desk calls, Schmidt said, which further reduces his department costs.

Finally, and most importantly, hardware-based FDE powered by Wave protects all of the data stored on VEGA's laptops. The decryption key is protected by hardware, making it impervious to software attacks such as malware and rootkits. Wave's software securely stores user access control policies in a protected area of the hard drive, ensuring only authorized users have access to protected data.

In addition, Wave's ERAS software creates secure audit logs including specific drive security profiles to further aid compliance both with the firm's internal policies and international data security regulations, such as those established under ISO/IEC 27002. The ISO/IEC framework identifies full-disk encryption as an important means of ensuring confidentiality of information stored on laptops.

"Data is important and its protection should be taken seriously," said Schmidt. "If implementing information security is difficult, then it often won't be done. With Wave Systems we found a solution that was easy to implement, and which provided a good return on investment."