



FinallySecure Enterprise

End-point Data Protection

The use of portable computers is exploding and laptops are becoming cheap and replaceable. Unfortunately, data within these laptops are not. Companies must implement an effective Full Disk Encryption solution without compromising the business workflow.

By 2009, IDC predicts that over 45% of all PCs in the world will be laptops! According to a 2008 study sponsored by Dell, 15,648 laptops per week are lost by business travelers in US and European airports?²

A single stolen laptop can cost a company over \$4,556.00, but that does not include the value of the lost or stolen data.

The average cost of lost records containing personal information is \$197 per record with an average loss of 31,979 records. A data breach is estimated to be a net loss of \$6.3 million³.

Rapidly changing government data regulations also needs to be addressed. Regulations such as HIPAA, PCI DSS, and Sarbanes-Oxley require robust electronic data protection management. Such laws require protection of credit card information, health records, and financial records.

The cost of lawsuits and legislative compliance related fines can be substantial simply due to lost, stolen, or even just unprotected data. Companies should also be wary of irreversible damage to corporate reputation because of data breaches.

Software-FDE alone is not enough

- > High CPU demand from continuous hard drive encryption slows workflow
- > Initial hard drive encryption can take hours
- > Repurposing an encrypted drive can take several more hours
- > Upgrading the operating system can be difficult or impossible

Hardware-FDE alone is not enough

- > Older laptops cannot be protected if companies aren't willing to replace the hard drives in them
- > Alone, this solution cannot extend to file and folder, messaging, or digital signature encryption
- > Hardware encryption algorithms do not allow customers to select between a variety of algorithms and may be limited in key length

The Case for End-Point FDE

FinallySecure provides total data-at-rest protection with Pre-Boot Authentication by combining hardware- and software-based technologies. FinallySecure offers companies a migration path from single user to enterprise and software-only to hardware-based FDE.

1 IDC Worldwide Quarterly PC Tracker, Dec 2007
2 Ponemon Institute, Airport Insecurity, Jun 2008
3 Ponemon Institute, Annual Cost of a Data Breach, Nov 2007



SECUDE IT Security GmbH
Sales, Service & Solution Center
Goebelstrasse 21
64293 Darmstadt
Germany

Tel : +49 6151 828 97 0
Fax : +49 6151 828 97 26
info@secude.com



Ease of Use

Protection & Performance

FinallySecure offers the only solution in the world that works with both software and hardware FDE technologies. With hardware-FDE, encryption is done on-the-fly with a dedicated chip embedded onto the HDD itself and not the CPU.

Central Management

Many companies do not encrypt because of impracticality for both end-users and IT administrators. FinallySecure provides centralized management with remote configuration, remote decommissioning, an intuitive interface, and synchronization with Microsoft Active Directory™.

Adaptability

A Path to End-point Protection

Many companies will not replace HDDs in existing computers. Only a hybrid software and hardware FDE solution will allow companies to adopt cutting-edge hard drive FDE technology and still protect legacy computers under one single management system.

Integrated Data Protection

Hard drive encryption alone cannot guarantee the integrity of data transmitted across computers. Companies need a hard drive encryption solution that seamlessly integrates with file and folder, messaging, and digital signature encryption technologies. This solution is designed to blend seamlessly with other data protection applications provided by SECUDE.

Security

FIPS 197 Certified

Many companies and government organizations have limited data protection choices due to stringent certification standards. Some hardware-based FDE hard drives have received FIPS 197 certification for their integrated AES encryption engine making a combined solution designed for even the most discriminating standards.

Pre Boot Authentication

Without authentication, encryption is useless. FinallySecure provides both encryption and authentication. PBA enables encryption of the entire hard drive from temporary files to the operating system itself. FinallySecure utilizes a Linux pre-boot partition to authenticate and authorize users before booting to the operating system.

Cryptographic Secure Erase

Hardware-based encryption allows instant secure erasure of confidential and proprietary information stored on the HDD. By removing the key used for encryption, all of the data is irrevocably lost, making it easy to redeploy or retire the HDDs.

Remote Decommissioning

Employees often leave the company without returning his or her laptop. The FinallySecure Management Console can erase that hard drive remotely or just temporarily decommission it.



Features:

Operating System:

- Microsoft Windows 2000 (ver. 8.x)/XP SP2&3/Vista

Encryption Standards:

- AES (128, 256)
- DES
- 3 DES
- Blowfish

Authentication Method:

- Username/password
- X.509v3

Smart Card Support:

- PKCS#11 Helpdesk Support (login screen)

Central Management Single Sign-On to OS Encryption of USB devices.

SECUDE IT Security GmbH
Sales, Service & Solution Center
Goebelstrasse 21
64293 Darmstadt
Germany

Tel : +49 6151 828 97 0
Fax : +49 6151 828 97 26
info@secude.com

