



SEAhawk Product Features

Self-Encrypting Drive
Management



Encryption In Hardware

Today, data protection at a bare minimum means encrypting your data. While there are various ways to achieve this, at the base level, your hard drive should be completely encrypted. This is commonly called Full Disk Encryption (FDE).

Full Disk Encryption (FDE)

Nothing is easier for a user than to accept that everything on their computer is encrypted. They don't have to worry about which part of the hard drive is secure, and which part is not. There is no conscious decision to make as to whether a document is sensitive enough to be encrypted or not. Everything on the Disk is encrypted! By virtue of FDE, encryption is mandatory and enforceability comes naturally.

Why Software FDE is primed to be replaced

Traditionally, FDE has been manifested through software. While it fulfills its purpose, there are some issues that arise with software FDE. Software FDE impacts the system it is installed on. There are modifications to the boot sector and key parts of the operating system to ensure that everything is protected. If not done right, there are many ways in which users can be locked out of their data. This type of FDE also impacts system performance since the CPU is now also tasked with encrypting / decrypting all your files as they are accessed.

Hardware FDE

The future of FDE is having it done in the hardware. Self Encrypting Drives are coming into the market, providing all the benefits of Software FDE with none of its drawbacks. Encryption is done within the drive itself and does not impact your CPU. The encryption key contained within the drive is never released to the CPU or the Operating System. That, coupled with the fact that this hardware solution is much more resilient to attack, makes it a very secure solution.

Management

While Self Encrypting Drives are looking to be an excellent solution, there is one piece that's missing in order to make it viable in the market – Management. It really isn't much of a solution if a user forgets his or her password and cannot access their data. Who takes care of the key management and access recovery?

The CryptoMill Touch

With CryptoMill software, you never have to worry. SEAhawk integrates extremely well with all types of Self-Encrypting Drives currently on the market and provides seamless setup, multiple user support, centralized access recovery and much more!. Data Protection CAN be this easy.



More Information

Hardware FDE Benefits

Hardware FDE provides complete data protection with no overhead.

The complete drive is encrypted. The encryption occurs within the hard drive itself, so your main CPU doesn't have to do waste it's time doing anything extra.

All cryptographic operations also occur within the disk. The encryption key never leaves the drive. This creates a very secure, enclosed environment.

Always-on encryption makes it easy to repurpose your drives and offers secure end of life for your storage.

Hardware FDE does not require software that changes the GINA or invasive software, which means a cleaner Operating System environment.

SEAhawk Capabilities

- Secure authentication environment unlocks drive at startup
- Authentication Management (setup users, passwords)
- Password Reset for Data Access Recovery
- Fast secure erase
- Hardware-based Random Number Generator helps provide better security for your sensitive data.

SEAhawk Benefits

- Simplified key management. No key servers, PKI
- User private data with SEAhawk virtual disks
- Protection on all mobile storage devices
- Simple policy management lets you secure your environment easily and Trust Boundaries contain your data and prevent data leaks.
- Works off-line and does not need to be connected to a server to be fully functional
- Recovery
 - Data always accessible by the Enterprise
 - Challenge-response for Single-User versions



CryptoMill Technologies provides innovative data security solutions for enterprises, professionals and individuals.

Loss or theft of information can have a devastating adverse impact on businesses and reputations. CryptoMill's SEAhawk is a Mobile Data Protection line of security products that provide comprehensive security solution for data within your organization

SEAhawk not only provides advanced virtual storage disks with robust encryption for mission critical and sensitive data but also prevents unauthorized access to storage media containing the data. All SEAhawk enabled computer systems have their data protected by encryption using government-grade encryption.

Contact

CryptoMill Technologies Ltd.
Suite 2000, 372 Bay Street, Toronto,
Ontario, M5H 3W9

T: (416) 241 4333
F: (416) 241 4333
e: info@cryptomill.com

Mailing Address:
P.O. Box 9, 31 Adelaide St. E., Toronto,
Ontario, M5C 2H8

While this information is presented in good faith and believed to be accurate, CryptoMill Technologies disclaims the implied warranties of merchantability and fitness for a particular purpose and makes no express warranties except as may be stated in its written agreement with and for its customer.

In no event is CryptoMill liable to anyone for any indirect, special or consequential damages. The information and specifications in this document are subject to change without notice.