SEAhawk
CryptoMill
Cybersecurity Solution

SEAhawk

CryptoMill Cybersecurity Solutions

www.cryptomill.com

ENGLISH/ INGLÉS/ ANGLAIS

OVERVIEW

SEAhawk is an endpoint and removable storage security solution for desktop PCs and laptops running the Microsoft® Windows™ operating system.

Device agnostic, SEAhawk is a policy-based solution with Zero-Overhead Key Management, providing protection for data at rest and in motion.

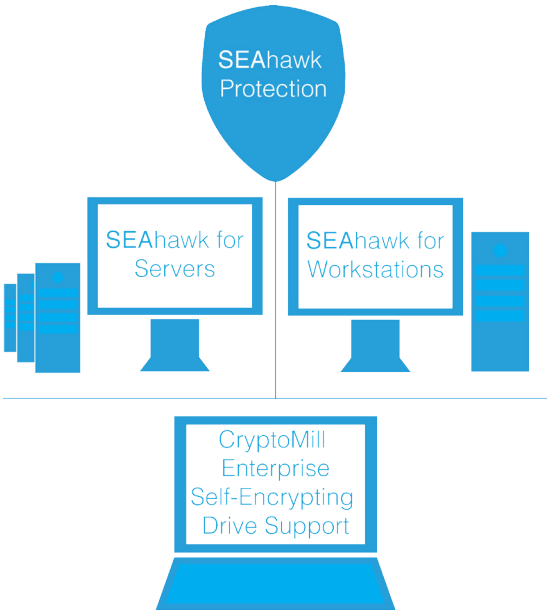
Key features of SEAhawk include Intelligent Device Access Management, Private Virtual Disk, Email File Protection and Self-Encrypting Drive Management.

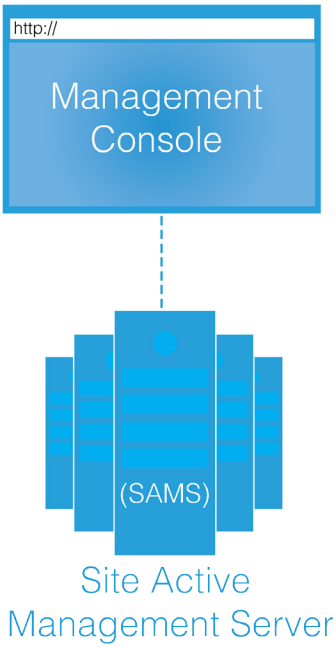
Highlights

- Data Protection and Trust Boundaries using strong encryption
- Policy-based control of removable storage media
- Secure data sharing with colleagues
- Facilitates secure data backup and recovery in case of disaster

SEAhawk combines Intelligent Device Access Management and Data Encryption in a single, seamless security solution for all storage devices.

CryptoMill Enterprise Security





FEATURES

Features	Benefits
Trust Boundaries Information is secured and accessed only within organizational perimeters.	Mitigates internal data breaches – intentional or accidental.
Intelligent Device Access Management Prevents copying of sensitive data to unencrypted USB drives and removable media.	USB drives, iPhones, Blackberrys and other storage devices can be used safely.
Private Virtual Disks Area defined on the hard drive for encrypted storage.	User Data Privacy. Protects against loss or theft of PC.
Management of Self Encrypting HDDs User Management, Secure Erase, Password / Access Recovery.	Complete data protection with zero performance impact.
Software FDE (Full Disk Encryption) Baseline, foolproof data protection.	Complete protection for your system drive.
Email File Protector Point and Click File Encryption.	Keep your information safe while sending it to authorized third parties or clients.

Trust Boundaries
A Trust Boundary is a set of Enterprise PCs and storage which may share protected data.

Examples of Trust Boundaries:
- Entire enterprise (simplest case)
- Business Units / Project Teams
- Executive / General Staff
- Groups which must legally be separated

Trust Boundaries transcend geography and network topology. Protected media cannot be decrypted outside of the Trust Boundary – *even if the sharing password is disclosed.*

SEAhawk Trust Boundaries prevent internal data breaches to unauthorized parties and insider data leaks to competitors.

Intelligent Device Access Management
SEAhawk employs Intelligent Device Access Management on access to removable storage devices like USB flash drives, iPod®s and CD/DVD. Based on SEAhawk policy settings, a user's ability to use these devices can be restricted to Read-Only or Blocked access.

Intelligent Device Access Management distinguishes between secure media and non-secure media. As a result, a user's SEAhawk policy can be set to permit full read/write access to secure media, while only

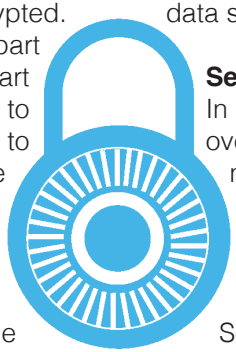
FEATURES

allowing read access to non-secure media – or, blocking it completely.

Private Virtual Disks
SEAhawk provides the option of using secure Virtual Disks – encrypted containers that store sensitive user data; this provides loss and theft protection.

SEAhawk Virtual Disks:
- appear to the operating system just like regular hard disks
- are secured using strong stan dardsbased encryption (AES) for maximum protection
- can be easily backed up and recovered without the need for additional security
- are securely bound to the organization

Management of Self Encrypting Drives (SEDs)
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 as to whether a document is sensitive enough to be encrypted or not. Everything on the Disk is encrypted! By the virtue of Full Disk Encryption, encryption is mandatory and enforceability comes naturally.



The future of FDE is to have it done in the hardware. Self Encrypting Drives provide 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 that is 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. While these SEDs 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?

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

Software FDE (Full Disk Encryption)
To support legacy devices that do not contain Self Encrypting Drives, CryptoMill offers software FDE to completely protect your system drive. It features the same Zero Overhead Key Management, bullet- proof Access Recovery and robust software encryption to keep your data safe.

Secure Erase
In the past, data was destroyed by overwriting every part of the storage medium with zeros, or random data patterns. This was called 'wiping' the storage medium. This process was very time consuming.

Secure erase works by erasing the key used to access encrypted data. All data is encrypted with a key. If you possess the key, you can decrypt the data. Throw away the key, and it's practically impossible to get to the data.

Wiping (or destroying) the encryption key is the best way to destroy encrypted data. It's fast (literally takes seconds!) and safe, as it works on the same encryption principles that

FEATURES

protect your data in the first place.

CryptoMill SEAhawk's Management Console lets you easily erase data from a central location. Your IT staff can easily select one or more fully encrypted computers to be secure erased. The next time any of those computers reboot or power-up, the data will be securely erased in seconds. All without anyone having to physically touch the machines.

Email File Protection
The E-mail File Protector provides convenient, easy protection for E-mail file attachments.

File encryption is as easy as 'Point and Click'. Simply right click on a file and select 'encrypt for email'. The user is then asked for a password to protect the file with. The file is then encrypted and can be attached to an email to send to a contact.

Should the receiving party not have SEAhawk installed, they can still decrypt the file using the stand alone File Decryptor application available through a free web download.

Decrypting an encrypted file is just as easy; right click the file and select "Decrypt File". Upon entering the right password, the file is decrypted and is ready for use.

Enterprise Data Accessibility
The Enterprise will always have access to its protected data. Even in the event of employee termination/absence, or forgotten passwords, access to encrypted media can be recovered through:

- Management Console (centralized media recovery)
- Over-the-phone secure challenge / response recovery

Easy for Users
- Authentication is provided using the user's Windows credentials (single sign-on option).
- Data protection runs transparently– no extra user action required

Management
CryptoMill's centralized Management Console is extremely easy to use and intuitive, ensuring that both administrative and help desk staff spend less time managing and configuring software, and more time doing what's important.

Workstations and laptops can be managed confidently and securely, so there is a high ROI based on less time required to manage a SEAhawk for Workstations secured environment.

Active Directory Integration
CryptoMill SEAhawk supports full integration with Active Directory. Administrators can assign Policies and Trust Boundaries and groups and OUs. Users in those groups will automatically be provisioned and will be able to sign in with their AD credentials at the SEAhawk pre-boot screen.

BENEFITS

Compliance

Today's organizations are facing the growing challenge of regulatory compliance. Throughout the world, governments are enacting legislation to regulate information management and security. At the root of these laws are the concepts of: data integrity, security, identity management and authorization. They are forced into the world of constantly changing information management requirements to comply with regulations and industry standards, such as the Sarbanes-Oxley Act, HIPAA, various countries' privacy laws and others.

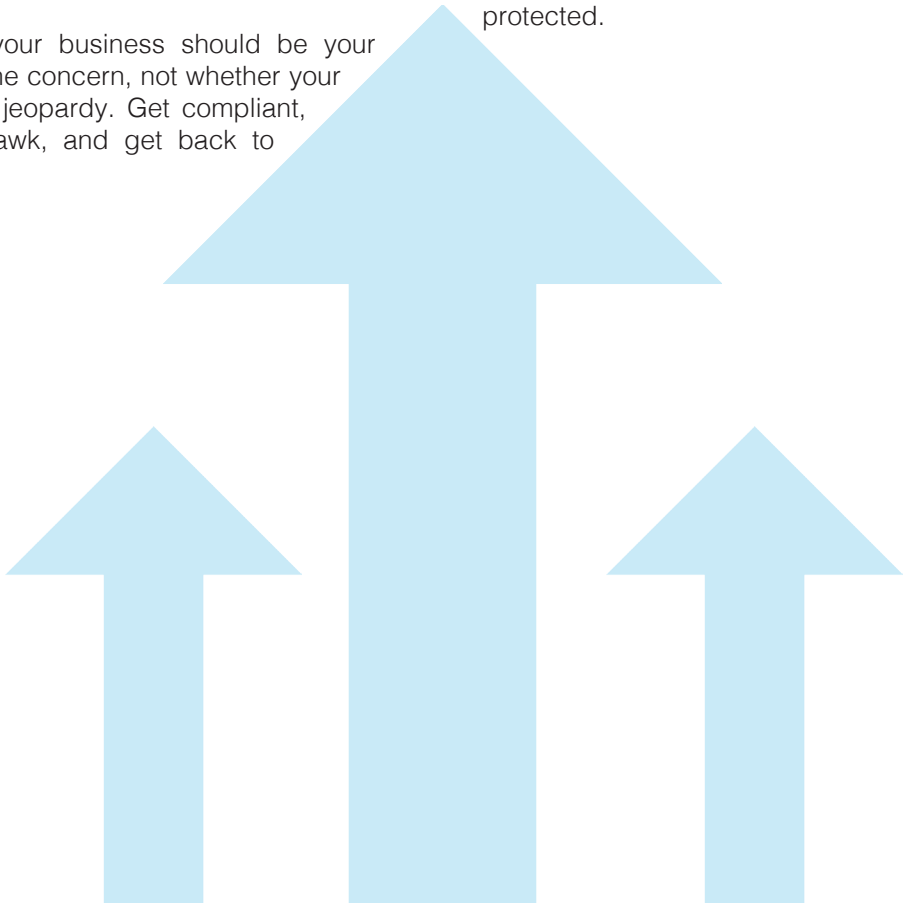
Growing your business should be your number one concern, not whether your data is in jeopardy. Get compliant, get SEAhawk, and get back to business.

Reputation

Your corporate reputation is a prized, highly vulnerable asset and it needs to be protected. Security Breaches are one of the leading causes of reputation risk.

Failure to comply with regulations poses the biggest threat to reputation. Maintaining a good reputation strengthens market position and increases shareholder value.

With SEAhawk for Workstations, your corporate endpoints and your reputation are protected.



SPECIFICATIONS

Product Specifications
SEAhawk provides data protection for:
• Supplementary (non-boot) drives – full disk encryption.
• Virtual Disks – virtual disks are fully encrypted.

Storage options:
• Direct-attached storage (DAS) – PATA, SATA, SCSI, SAS, USB, Firewire (IEEE 1394)
• IP-based storage: iSCSI
• SEAhawk Virtual Disks on local storage, or on network file servers.

Encryption Ciphers:
• AES (256-bit, or 128-bit) – CBC mode •Triple DES (3DES) – CBC mode

These values may be subject to workstation memory and processing limitations.

Server System Requirements
SAMS has the following system requirements:

• Microsoft® Windows Server 2008 R2
- 1 gigahertz (GHz) or faster processor
- 1 gigabyte (GB) RAM
- 200 MB available hard disk space

• Microsoft® Windows 2012 R2
- 1.4 gigahertz (GHz) or faster processor
- 2 gigabyte (GB) (64-bit) RAM
- 200 MB available hard disk space

Workstation System Requirements
SEAhawk has the following system requirements:

• Microsoft® Windows 7 (Home Premium, Professional, Ultimate)
- 1 gigahertz (GHz) or faster processor
- 1 gigabyte (GB) RAM
- 100 MB available hard disk space

• Microsoft® Windows 8
- 1 gigahertz (GHz) or faster processor
- 1 gigabyte (GB) (32-bit) or 2 GB (64-bit) RAM
- 100 MB available hard disk space

• Microsoft® Windows 10
- 1 gigahertz (GHz) or faster processor
- 1 gigabyte (GB) (32-bit) or 2 GB (64-bit) RAM
- 100 MB available hard disk space

SEAhawk for Workstations requires a temporary connection to a CryptoMill Site Active Management Server (SAMS).

SEAhawk

CryptoMill

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

Loss or theft of information can have a devastating impact on businesses and reputations. CryptoMill's SEAhawk is an endpoint and removable storage device protection solution that provides comprehensive security 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 Cybersecurity Solutions
Suite 301, 100 Front Street East,
Toronto, Ontario, Canada, M5A 1E1
Toll free: (855) 441 4333
T: (416) 241 4333
F: (416) 241 4333
E: info@cryptomill.com

Sales Contact
E: sales@cryptomill.com

connect with us

YouTube:
http://www.youtube.com/user/CryptoMillTech

Facebook:
https://www.facebook.com/Cryptomill

Twitter:
https://twitter.com/cryptomill

LinkedIn:
http://www.linkedin.com/company/cryptomill-technologies