



Secured eUSB

Secured eUSB lets you take control.

Take control of USB security

The wide-spread use of USB flash drives is a major issue for business leaders. How do you protect sensitive data when it is so easy to copy onto a USB device?

Secured eUSB lets you take control. Secured eUSB is a comprehensive, easy-to-use solution for USB security that incorporates all the functionality necessary to safeguard your intellectual property and comply with data protection laws and regulations. Secured eUSB provides strong encryption, centralized control of security policies, password policies and

user access rights, and extensive data content reporting, enabling you to deploy and control USB security across your entire network. With Secured eUSB you can be confident that the data on all USB flash drives in the organization is secured and that you have full visibility of data movement.

Benefits

Encrypt any USB drive, use it anywhere

It doesn't matter what USB flash drives your employees buy, Secured eUSB can encrypt any brand and will secure storage of up to 64 GB. A secured USB flash drive can be used in any Windows-based computer as all the software required for operating it is on the drive. No need to install a license – all you need is the password.

Fast encryption

The encryption of your removable media is extremely fast – a 16GB flash drive takes less than one minute to secure.

Easy to use – no training required

Secured eUSB is easy to use, fast to deploy and fits in with everyday workflows. So, having removable media encryption policies in place

won't slow anyone down. Removable media encryption is quick and simple, just a click of a button and input of a password. Users are guided through each step of the process.

Using secured devices is just as easy – users simply drag and drop files and folders to encrypt them on the secured device; and documents can be opened and edited as usual with Microsoft applications.

Regulatory compliance

Strong AES256 encryption complies with Sarbanes Oxley, GLB Act, HIPAA HITEC, FTC Red Flag Rules. The SEP management console enables IT managers to deploy a consistent removable media security policy across all users in the organization and enforce compliance. The SEP provides a full audit trail of data movement and user actions.

Fast to deploy and fits in with everyday workflows

Enable users to take responsibility for USB security

The Simple Encryption Platform (SEP) allows IT to centrally manage and enforce removable media security policies – create custom environments, define roles and permissions for groups and users, and then deploy this across the entire network. Users can then define who can access their encrypted USB flash drive, and what they can do with a document: eg. read only, or read/write.

Kill Pill Anti-theft system

If a user has lost or misplaced a USB flash drive IT can issue a 'lockout' command to block access to the device – administrators can unlock the device if required. If a secured USB drive is stolen or an employee leaves the company without returning their USB flash drives, the 'Kill Pill' command will completely wipe the flash drive clean to ensure complete data protection. This will even work over the Internet.

Track who owns each device

For each secured USB flash drive, the system automatically assigns ownership to an Active Directory user. IT can therefore track usage of USB flash drives and do data loss reports if a flash drive is lost or stolen. If a user is to leave the organization, IT can quickly identify which USB flash drives the user owns and ask for them to be returned.

The highest security standards

Secured eUSB creates a secure working environment. The user can open/create any Microsoft file within the secure working area of the USB drive and make changes without ever moving documents to an insecure environment. Any temporary files created by Microsoft during the editing process are wiped. A secured Recycle Bin travels with the device to ensure that data is not moved to an unsecured recycle bin and can be restored if necessary.

Users can then define who can access their encrypted USB flash drive

Key Features

- USB encryption can be implemented quickly and easily, no complex infrastructure is required.
- Administration overheads are minimized as users are guided through the USB encryption process.
- Built-in features provide basic Helpdesk support.
- Advanced technology ensures the highest levels of security.
- Central management tools allow you to deploy and enforce security policies.
- Automatic data content reporting provides a full audit trail to ensure regulatory compliance.
- Anti-theft systems lock down lost or stolen USB devices to prevent data loss



Cryptzone solutions mitigate information security risks in the key areas of Policy Compliance, Content Security, Secure Access and Endpoint Security.

International Headquarters

Cryptzone Group AB
Drakegatan 7,
SE-412 50 Gothenburg,
Sweden

www.cryptzone.com
info@cryptzone.com

Regional Offices

Sweden
Tel: +46 (0)31 773 86 00

United States
Tel: +1.949.279.6177

United Kingdom
Tel: +44 (0)370 013 1600

Partner information:

For more information go to
www.cryptzone.com/partners