

Secure Device and Application Management



*Prevent Data Loss, Theft
and Unauthorised Access*

Security Policy Enablement

End Point Security To Go

Secure Your Organisation Against Data Loss, Theft and Unauthorised Intrusion

The loss of data and information is often the focus for IT security, sharply centred on the control of the devices, systems and services that prevent the unauthorised removal of data in organisations like yours. The issues you face are two-fold; how to design and realise a security policy which is applicable to the user community you serve, and how to easily enforce the policy through enabling technology.

Emereo|EPS (End-Point Security) is a solution which helps you realise a workable security policy and provides the means to lock and control all end-point devices, e-mail and internet access. Data theft and loss and unwanted intrusion can and does cause significant security issues and often the threat occurs with the end-points across the infrastructure.

The fall-out will dictate that critical services, applications and information become unavailable to your user community as investigations into these events are undertaken. Understanding the threat is the first step Emereo takes to help you shape a security policy applicable to your operational needs.

To enable the policy Emereo deploys DriveLock™ to place controls on devices and applications, in fact anywhere that critical information resides electronically; from barring USB devices to hard-disk encryption and control of e-mail and internet access (see Emereo|PSM product information) provided by WebRoot.

Data Theft - Criminals can copy large amounts of data to mobile storage devices; favourite targets of data thieves include research data, personal data and credit card information. Emereo|EPS gives complete control over who can copy what, to and from USB sticks and other mobile storage devices.

Data Disclosure - Countless USB sticks are lost each day and many laptops too, the data may be easy to replace but Information disclosure is often costly. Emereo|EPS encrypts data on USB sticks, other storage devices and laptops to safeguard your data.

Unauthorised Intrusion - Uncontrolled peripherals can obtain access to corporate networks. Mobile devices can also spread viruses and malware. Emereo|EPS can protect your network by giving you total control over the use of all ports on computers in your network.

System Instability - Troubleshooting problems caused by the uncontrolled use of peripheral devices becomes time-consuming and expensive. Emereo|EPS ensures only approved devices are connected to the computers on your network.

Access Control – E-mail and the internet can still be the open door unauthorised users need to push/pull data out of your organisation. Emereo|PSM (Perimeter Security Management) provides the controls you need to restrict behaviour all the way down to specific file types and provide an audit for forensic use.

Compliance – Emereo|EPS is deployed as a solution where the key objective is to satisfy your desired outcome. Put simply this could just be understanding the scale of the threat so a security policy can be authored and enabled or to demonstrate how secure management information is and how compliant your IT is with the demands of standards such as ISO27001 and GSI.

Secure Your Organisation Today!

- 25 million lost child benefit records
- 3 million UK learner driver records go missing
- 26,000 retail staff warned that their personal data is at risk following the theft of a laptop containing pension information
- FSA hits Building Society with a £1m fine following the theft of a laptop
- A lost disk holding confidential data on 62,000 mortgage customers was not encrypted

And many more.....

DriveLock To Go

Full Control Over All Devices, Ports and Applications

Emereo chose DriveLock as part of its EPS Solution because many organisations around the world today consider it to be the industry standard for controlling the use of ports and attached devices on computers across their network.

DriveLock allows you to control all of your company's critical data and information. More than this with DriveLock installed security breaches are instantly transparent and you take action before its too late.

- HMS Devonport/Babcock Marine ·
- Vodafone · Macroberts · Exxon Mobil ·
- Getronics Pink Roccade · Brunner Mond ·
- Coventry PCT · Munich Airport ·

Always Cutting Edge

DriveLock's product development is driven by real-world experience, customer requirements and the need for greater compliance and governance with legislation, standards and best practice.

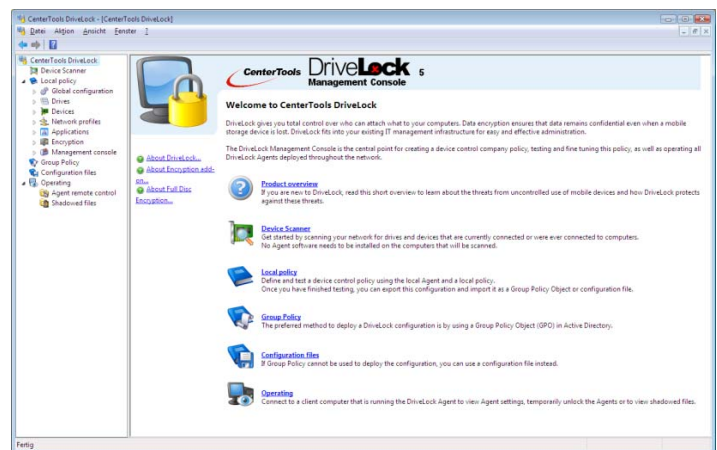
We realise that every organisation's security policies will be different. Some will concentrate on restricting the use of mobile devices and storage, while others will aim to exert more granular control upon users and applications. And for some there will be the need to prove that access to critical information sources is controlled in order to satisfy compliance with ISO 27001 or Sarbanes Oxley to name just two common standards.



Consequently DriveLock's features and configuration options are designed to achieve bullet-proof data security while maintaining ease-of-use and minimising resource requirements. With these goals in mind, Emereo constantly aims to improve existing customer configurations.

Intelligent Security to go:

- ✓ Full Disk Encryption
- ✓ Encryption for Windows Mobile
- ✓ Security Reporting Centre
- ✓ Audit and File Shadowing
- ✓ Device Scanner
- ✓ Encryption of Mobile Devices
- ✓ Network Profiles
- ✓ Application Launch Filter
- ✓ Uses Active Directory for fast deployment



In-House Security

Emereo|EPS Lets IT Professionals Do Their Job Securely

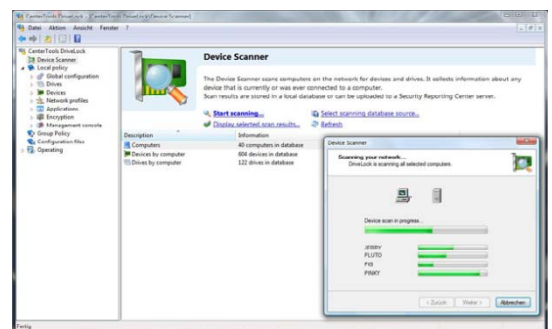
Many Companies trust Emereo to provide solutions which keep their infrastructure and information readily available to those that need it. We provide intelligent solutions that resolve issues simply, make tasks and processes much easier and automate routine administration task.



Emereo realise that data security and the need to intelligently control mobile devices, such as USB, is of paramount importance for those wishing to avoid data loss and theft. Emereo|EPS, powered by DriveLock, gives you very granular control over the use of peripheral devices. You can grant or deny permissions that define which devices users or groups are allowed to use. Best of all it is quick to implement, easy to configure and user intuitive. Your organisation's security policy can be fully enabled in days.

Device Scanner

The Device Scanner creates an inventory of all devices that are currently or have ever been attached to the computers in your network. You can easily use the Device Scanner to test, amend and create your security policy. This policy sets the tone for how Emereo's consulting services will configure DriveLock to effectively control the use of mobile devices and restrict access to key applications.



Network Profiles

DriveLock immediately recognises when a computer is connected to a different network, and applies the settings you have configured for this network. Each drive, device or application white-list rule can be set to apply to one or more network profiles, to correspond with specific networks. You can use network profiles to prevent connections to unapproved networks.

Also, you can determine which devices or applications can be used while a computer is connected to your corporate network or while working remotely. To prevent network intrusions you can automatically disable wireless connections when a computer is connected to your corporate network.

DriveLock is the perfect fit for the mobile professionals in your organisation. DriveLock will simplify mobile computing by automatically configuring browser and default printer settings when moving between networks.



In-House Security

Emereo|EPS – Security for all Seasons

Emereo Solutions has a growing reputation across the UK for working across all customer types. Consequently DriveLock has been deployed in small and large organisations covering most sectors from Healthcare to Central Government from Law Firms to Manufacturing Companies.



“A compelling reason for Brunner Mond was the speed and ease with which Emereo Solutions deployed DriveLock to help us realise a usable security policy.” **Martin Murgatroyd, Head of IT, Brunner Mond.**

Application Launch Filter

Protect your network against zero day exploits and Trojan Horse programmes by allowing only authorised applications to be used. Prevent some users from running applications on certain computers, such as Terminal Servers, or while connected to a specific network.

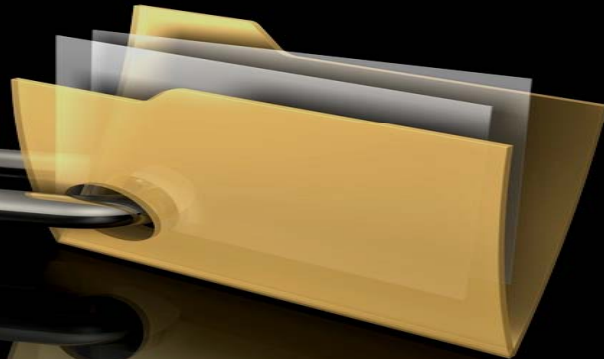
The terminal server edition of DriveLock allows the controlled use of external drives attached to thin clients in your Terminal Server environment (Windows and Citrix).

The easy configuration of the Application Launch Filter combine to make it an invaluable tool for making your network more secure.

File Filtering

Because you need to control what can be copied to or from removable media. DriveLock will allow or block the copying of files according to your rules. File types are identified according to their content And not just only as file extensions.

You can choose from the many file types that DriveLock has identified or, for instances of proprietary or bespoke applications, you can create your own definition and extend this through a custom DLL.



Encryption of Removable Drivers

Accidental disclosure of sensitive data due to lost or stolen storage devices can be very costly. DriveLock can give you peace-of-mind by automatically and transparently encrypting data that is copied to removable drives. When you need to ensure that only encrypted data is stored on these devices DriveLock can enforce encryption and monitor data transfers for compliance reporting.

For employees needing to work with corporate data at home or share files with someone else, the Mobile Encryption Application allows access to encrypted information, even on computers where DriveLock is not installed and without the need for local administration rights.

Full Control Security

Full Disk Encryption

Data lost on laptops continues to be the bane of many organisations across the public and private sectors. DriveLock can fully encrypt all hard disks (including temporary and paging files) right down to the system partition.

Once deployed a secure pre-boot authentication process with a single sign-on for Windows combine ease-of-use with added security. Authentication process restricts access to any part of the hard drive. Full data recovery can be expedited with an emergency logon. Monitoring of encryption status can be facilitated using DriveLock's Secure Reporting Centre.



DriveLock Full Disk Encryption uses technology recognised as being certified to Common Criteria EAL4 by the National Technical Authority for Information Assurance or CESG and has FIPS 140-2 certified encryption algorithms.

Windows Mobile Encryption

Increasingly there is a need to encrypt data on Windows Mobile (Pocket PC 2003, Windows Mobile 5 and Windows Mobile 6) handheld devices and Smartphones.

DriveLock creates encrypted containers which can be used on a Windows Mobile device as well as desktop computers and laptops. Appearing as virtual storage cards, encrypted data can be securely synchronised between the mobile device and PC.

When it is necessary to completely restrict access use DriveLock to also lock the appropriate ports which may be used to connect mobile devices.



Secure Reporting Centre (SRC)

More than just reporting. DriveLock SRC is the system's engine offering both a means to manage compliance issues as well as ensuring that elements such as Full Disk Encryption have been correctly distributed. SRC will consolidate network-wide information about device activity and data transfers.

Choose from standard report formats or create your own from the auditing data. Dynamic report creation, flexible filtering and sophisticated grouping functionality combine to let you find the information you're looking for within seconds. Once you have created a report, you can print it, export the data for further analysis or even send the report to someone else via e-mail.



Information Management

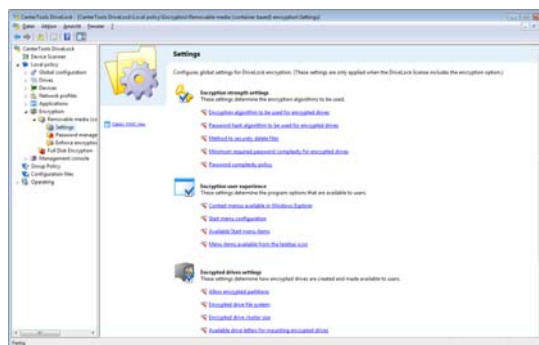
Emereo|EPS – Intelligent Control

DriveLock easily integrates with your existing IT infrastructure by utilising Active Directory Group Policy (DriveLock also fully supports Novell and other environments). Client deployment uses existing software distribution mechanisms. Training and support costs remain low for a high return on investment.



DriveLock – Features At A Glance

- >> Dynamically locks removable devices: USB Flash drives, floppy disks, CD-ROM, scanners, cameras, network adapters, Blackberry, Palm, Windows Mobile, Smartphones, modems and many more.
- >> Dynamically locks most types of port: USB, 1394/Firewire, Bluetooth, infrared, PCMCIA serial (COM) and parallel (LPT).
- >> Wizard for creating encrypted CDs and DVDs.
- >> Configurable whitelists for device types and models.
- >> Allow storage devices based on serial numbers.
- >> Access granted for specific users and/or groups.
- >> Integrates with Active Directory Group Policy. Supports Novell eDirectory and ZENworks.
- >> Policy enforcement based on user log-on.
- >> Allows and denies copying of specified file types.
- >> Audit of files that are read from or written to removable drives.
- >> Separate read/write permissions for removable drives.
- >> Drive access rules based on size and encryption status.
- >> 256-bit encryption for data on mobile devices or hard disks.
- >> Automatic and transparent encryption of data copied to mobile devices.
- >> Access to encrypted drives and files from computers without DriveLock.
- >> Use blacklists and whitelists to ensure users only run approved applications.
- >> Disables network adapters when user attempts to connect to an unapproved network.
- >> Auditing keeps complete record of device and application usage.
- >> Customised reports on device and application usage.
- >> Multiple alerting mechanisms for DriveLock events.
- >> File shadowing keeps full record of the content of files that are copied to or from removable drives.
- >> No servers required to deploy policies.
- >> Easy configuration using Microsoft Management Console (MMC) snap-in.
- >> Alternate configuration using UNC-Path, HTTP or FTP.
- >> Administrators can temporarily suspend device restrictions.
- >> Remote identification of devices connected to clients.
- >> Quick policy deployment using templates.
- >> Protection against tampering or de-installation.
- >> Customisable taskbar notification with HTML text.
- >> Encryption enforcement.



emereo

About Emereo Solutions

Emereo Solutions (UK) Limited (formerly AdRem Software UK) was founded in 2004 as a privately held company. Its installed base serves a diverse range of customer types base from Central and Local Government, the NHS, Education, Finance Services, Law firms and many more organisations where the goal is making IT effective and available. Emereo's solutions have been deployed on over 15,000 servers across the UK and Ireland.

Emereo provides rapidly-deployed software solutions for infrastructure management covering network management and monitoring, network behaviour analysis, end-point security and IT service management. Our solutions help organisations secure greater resilience of their enterprise networks so IT can provide better services to the business and operations it supports.

Best-of-Breed products adhere to ITIL and COBIT best practices and ensure compliance with initiatives such as Sarbanes Oxley, FSA, GSI, e-Health and e-Government. The Company's products deliver efficient and effective solutions without prohibitive costs and extended consulting times traditionally associated with enterprise solutions.



making | IT | available

Emereo Solutions (UK) Limited
6 Rickett Street
London SW6 1RU

Telephone: 0871 717 7294
Facsimile: 020 7385 7183

www.emereo.eu

©2008 Emereo Solutions (UK) Limited
This document is written by Emereo Solutions and represents the views and opinions of the Company regarding its content, as of the date the document was issued. The information contained in this document is subject to change without notice.

Emereo Solutions encourages the reader to evaluate all products personally.
Emereo and Emereo|EPS are trademarks or registered trademarks of Emereo Solutions (UK) Limited.
DriveLock is a registered trademarks of CenterTools GmbH
All other product and brand names are trademarks or registered trademarks of their respective owners.

First Published October 2008