

Implementing End-Point Security



The Project Plan Whitepaper

emereo

*Protecting Your Organisation
Without Inhibiting Your People*

Protect 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 to prevent the unauthorised removal of data in organisations.

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.

Like most IT projects no one wants to be saddled with long lead times and no pragmatic response to really protecting your organisation without hindering the productive working behaviour of staff.

The purpose of this whitepaper is to prove the methodology which will allow rapid realisation of an IT security policy through enabling technology. However, as covered in this document, people's working behaviour will positively shape the scope of this project.

Emereo|EPS (End-Point Security) is the enabling solution which has already been delivered to many UK organisations: from law firms to local government and healthcare to manufacturing. Emereo|EPS helps to realise a workable security policy and provide the means to lock and control all end-point devices. 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 forensic investigations into these events are undertaken. Understanding the threat is the first step Emereo takes to help you deploy 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.

Data Theft - Criminals will 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.

Compliance – Emereo|EPS is often deployed as a solution where the key objective is to satisfy strict compliance needs. Here understanding the scale of the threat is only the first part of the requirement where the primary need will be reporting upon data security status in order to demonstrate compliance. To this end Emereo has satisfied the demands of standards such as Government Connect Code of Connection (CoCo), e-health, Data Protection Act, PCI and Sarbanes Oxley.

Protecting Your Organisation

- 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.....



Project Goals

Emereo realise that data security and the need to intelligently control mobile devices, such as USB drives, is of paramount importance for those wishing to avoid data loss and theft. Emereo|EPS provides very granular control over the use of peripheral devices. Significantly permissions can be granted or denied in order to determine which devices users or groups are allowed to use.

This type of questioning is often where an implementation project for DriveLock begins as it encourages the debate between Corporate Governance and IT Governance:

- Best Practice for Managing People
- Best Practice for Data Security
- Best Practice for Managing Information
- Best Practice for Protecting Customers

Regardless of which stakeholders truly sponsor the project (the business or IT) the implementation will be quick, easy to configure and user intuitive.

An organisation's security policy can be fully enabled in days.

Project Approach

At the beginning of any project, regardless of its scale, Emereo's consultants aim to provide a more informed picture of how data is used. A discrete audit examines usage, storage and access rights, as a result Emereo can quickly demonstrate a real and actionable understanding of what risk factors truly exist.

But risk is only one factor because many breaches, in fact according to **Computing November 2008**, 56% of employees leak data unintentionally, so the audit also examines working practices. As good as it is to achieve an IT security policy which protects your organisation it will soon become counter-productive if staff find it increasingly difficult to work.



Without doubt in all instances with data and information secure the opportunity for better decision making can be derived.

So its no surprise that for all the implementations Emereo has completed every organisations' security policies have been 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. Others may just need to be able to prove that access to critical information sources is controlled in order to satisfy compliance with an industry standard or requirement.

To that end any project initiated by Emereo breaks naturally into 3 phases:

- **Understand the Data and Resources**
- **Engage, Enable and Empower People**
- **Optimise Processes and Technology**



Project Scope and Implementation

Understand the Data and Resources – The first phase of any end-point security project Emereo undertakes is to consult with the organisation to understand how they think their data and corporate information is managed and used.

- What data exists, where and in what form
- Why data exists and what purpose does it serve
- What are the foreseeable future uses
- Who uses the data, how are they using it and how it is being shared amongst colleagues and 3rd parties

This last point throws up many grey areas, Government use a plethora of 'agencies' and it is not uncommon in private sector organisations for the Marketing department to share customer information with mailing houses and research companies. In fact looking at how an organisation interacts with its partners and suppliers can immediately reveal holes the organisation never knew they had in their information management processes.

Consequently it will come as no surprise that Emereo utilises an array of skills to understand how data is used and is moved. A device usage report is generated to illustrate people's reliance on storage devices, often to legitimately do their job; a USB memory stick is many peoples preferred means of taking work home to do. As conscientious as this may be for many, a lost memory stick can sometimes be a window of opportunity for others to gain competitive advantage.

The device usage report provides an accurate view of both peoples' preferred working behaviour as well as their inappropriate use of devices to download or introduce files, such as MP3s, onto the corporate network and increase the threat of Malware and viruses.

Getting the balance between legitimate working practices and mis-use of corporate resources is something the device usage report will only highlight, while Emereo's use of focus groups will provide a level of consultation with key workers to ensure their daily use of IT is no more inhibited than the time it takes to unlock and lock an encrypted USB device.

Once this level of findings and research is completed it will be presented to management for analysis and discussion with the aim of drafting a realistic IT security policy.

As a bi-product of this discussion Emereo has run Risk Awareness Campaigns (RAC) as a way of PR'ing the introduction of a policy which although designed not to inhibit employees working practices, may be met with suspicion. The RAC simply highlights the threats and risks facing the company in such a way to validate the introduction of both the policy and enabling technology to protect the individual against the unscrupulous acts of others.

Over 1/3 of Companies, where technology has enabled a robust security policy, have seen increases in staff satisfaction due to greater mobile working capabilities

Gartner

Engage, Empower and Enable – The next phase doesn't see any less consultancy with the organisation and its people. Having established a draft IT security policy it then becomes necessary to establish the best way to involve as many people in the deployment. An IT security 'task force' is often pulled together, run by IT but using a cross-functional mix of employees, to participate in a pilot exercise.

This will help to test the scope of the technology and enable a realistic project plan to be produced which is both user and information centric. In short publish a project initiation plan which is both acceptable to the people and achievable with technology.

Optimise Process and Enable Technology – Emereo then moves into the implementation cycle of the project (more of which is covered in the next section). Critical to this and running in parallel will be the overall appraisal of all data and information management processes and procedures (from access rights, use of SaaS to back-ups), Emereo will make recommendations to possible changes.

- HMS Devonport/Babcock Marine - Vodafone - Macroberts LLP - Exxon Mobil - Pink Roccade - Brunner Mond - Coventry PCT - Munich Airport - Broadland District Council - Brodies LLP - Origo - Frontier Economics - Dundas & Wilson LLP - and many more



Implementation Timescales

The following timescales are based upon Emereo's experience of implementing DriveLock in a variety of customers, where organisations such as Coventry PCT and Babcock have thousands of PC users but Frontier Economics have only 100.

Typically most phases are expedited on-site although where specific or customised documentation is concerned the Emereo consultant may choose to author this 'back-at-base'.

At every phase of the implementation Emereo encourages full involvement of at least one dedicated customer representative

(System Administrator and/or IT Project Manager). Seeking to expedite a full transfer of knowledge only helps to resolve future problems and issues and allows any configuration changes to be made internally and securely.

The product element of Emereo|EPS will ordinarily provide drive and device locking, file filtering and shadow copies, network profiles, auditing and central management with the Security Reporting Centre (SRC). Drive Lock Classic Encryption secures all removable drives and Windows Mobile devices.

	Less 150 PCs		150 – 600 PCs		600 PCs Plus	
Phase/Activity	Time	Phase Total	Time	Phase Total	Time	Phase Total
Information & Resources		1 Day		1 Day		7 Days
1. Device Usage Report	½ Day		½ Day		1 Day	
2. Focus Groups & Research	½ Day		½ Day		5 Days	
3. Management Consultation					1 Day	
Engage, Enable, Empower				2 Days		3 Days
1. IT Security Policy			1 Day		1 Days	
2. Project Management & Scope (including Documentation)			1 Day		2 Days	
Optimise Processes & Technology		2 Days		3 Days		7 Days
1. Audit and Improve Procedures and Processes					1 Day	
2. Implementation (Classic DriveLock only)	1 Day		2 Days		4 Days	
3. Training (including user Documentation)	1 Day		1 Day		2 Days	
Total		3 Days		6 Days		17 Days



Project Management

Emereo has been providing consultancy in the UK and Eire since 2004 and have built a model of services based upon best practice that acknowledges the role IT must play in supporting the core business activities of its organisation.

ITIL/COBIT – Emereo embed appropriate processes from both frameworks into every project plan as the end-goal for any IT project has to be driven by the fundamentals of IT service management and the improvement of delivery to the customer.

ISO/IEC 27001/2 – Emereo utilises this code of practice for Information Security Management by working within a range of specific security controls.

PRINCE2 – is the structured approach to project management which Emereo uses. It provides Emereo with a method for managing IT security projects within a clearly defined framework. It enables Emereo to coordinate people and activities in a project, how to design and supervise the project, and what to do if the project has to be adjusted if it doesn't develop as planned.

The combination of these best practice areas allows compliance to industry standards to become a realisable outcome of any project Emereo undertakes.

Other Considerations

This whitepaper explains the steps organisations would take to achieve a solid IT security baseline which 'internally' will go a significant way to eradicating the threat of data loss and the risk of unwanted intrusion and malware.

But that's not to say there will not be other considerations which may extend the project plan by a day or so:

Terminal Services - 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).

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.

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

Once deployed a secure pre-boot authentication process with a single sign-on for Windows combines 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 Security Reporting Centre.

Integration Points – The DriveLock Security Centre analyses all user, system and network events relating to data use and movement, regardless of need and intent. The analysis helps pinpoint areas of risk and allows forensic resolution to threats. However integration with a network management solution, such as Emereo|NMS powered by NetCrunch, and/or a helpdesk system, will enhance the visibility of security problems by compiling SNMP events into an e-mail handshake. It ensures support groups are not just alerted, but their activity in terms of response and fix times is also tracked so, if necessary, the problem can be escalated.

Emereo would also encourage any organisation to look at how e-mail and internet access can be used as a back-door for data theft. Emereo recommends WebRoot to eradicate this form of threat.



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.

- ✓ 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

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.

“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.**



About Emereo Solutions

Emereo Solutions (UK) Limited was founded in 2004 as a privately held company. Its installed base serves a diverse range of customer types 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.



*Protecting Your Organisation
Without Inhibiting Your People*

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 2009