

## Pointsec Mobile Data Protection

### Introduction

PointSec for PC secures desktop and laptop computers from unauthorized physical access, using both boot protection and 'strong' disk encryption (256 Bit AES). PointSec for PC provides the following security functions:

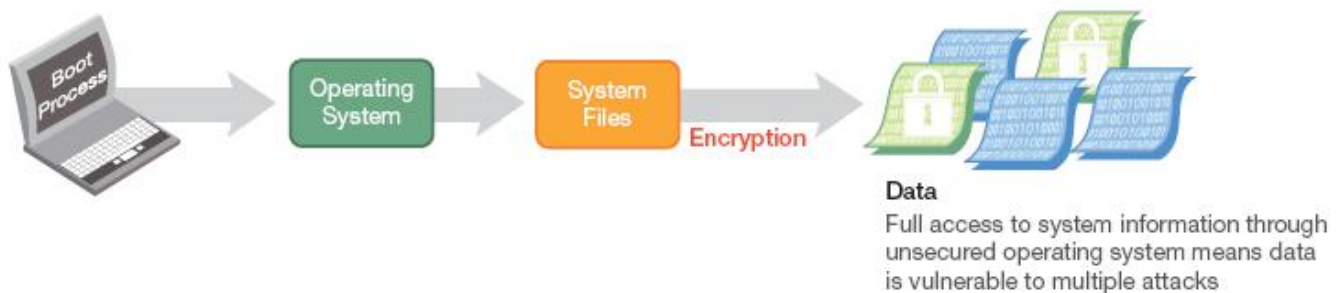
- n Strong user authentication
- n Secure Remote Help for users who have forgotten their passwords
- n Audit logging of events, i.e. successful and failed logon attempts

With PointSec for PC, all logical partitions / volumes are boot protected and encrypted. The careful integration of boot protection and automatic encryption provides a high degree of security with minimal impact on users. Boot protection prevents subversion of the operating system or the introduction of rogue programs while sector by sector encryption makes it impossible to copy individual files for brute force attacks. Full disk encryption secures the data even if the disk is removed and loaded into a controlled machine. This ensures security by enabling an organization to determine the security level instead of leaving it up to the user to see that the information is encrypted.

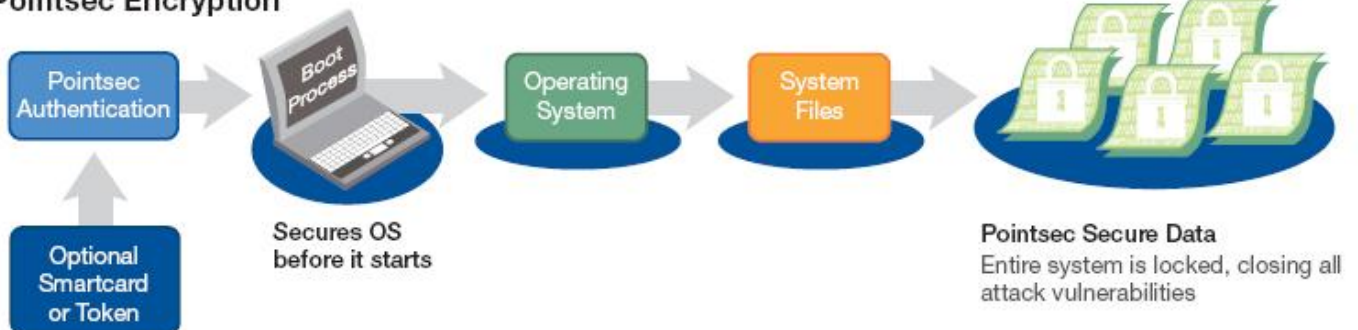
PointSec for PC uses full disk encryption to guarantee that unauthorized users cannot access or manipulate information on a protected computer, either from available files, erased files, or temporary files. PointSec for PC safeguards the operating system and the important system files (which often contain clues to passwords for Windows), shared devices, and the network.

#### Pointsec Encryption

##### Unprotected System or File and Folder Protection



##### Pointsec Encryption



## Minimum System Requirements

The following table is to be used as a guide to outline the minimum system requirements to run Pointsec for PC. Please note that the minimum requirements stated do not take into account running applications outside of the Operating System. Careful consideration must be given to purpose of the laptop (graphics, design, document processing etc) and scaled accordingly.

Operating System (32 bit)	Memory	Disk Space
Windows Vista	512MB Minimum *1GB Recommended	100MB of which 2MB must be free contiguous, free space
Windows XP Professional (SP3 recommended)	128MB Minimum *1GB Recommended	100MB of which 2MB must be free contiguous, free space
Windows XP Tablet Edition	256MB Minimum *1GB Recommended	100MB of which 2MB must be free contiguous, free space
Windows 2000 SP4	64MB Minimum *1GB Recommended	100MB of which 2MB must be free contiguous, free space

*\*Wherever possible the recommended specification should be followed.*

## Operating System Restrictions

Windows XP Home and Media Centre (all variants and Service Packs) are currently not supported. Apple Mcintosh computers are also **not** supported.

## Limitations

Software cannot be installed on Stripe or Volume sets (Hardware / Software RAID configuration is not supported)
Software cannot be installed on a Dynamic, Mounted or Hidden Volumes (Manufacturer Recovery Partitions)
Root directory is not compressed
No dual boot configurations
The hard disk is no more than 80% full
The use of disk utilities (Ghost, Partition Magic etc) is not supported. Any restructuring of the disk may result in a non bootable system. Pointsec will need to be removed should any work on the partition structure be required

## System Preparedness Checklist

Egton recommends that the following points are reviewed before sending your laptop in for configuration.

**p** A '**Full**' backup of **any** data (Office files, Accounting software etc) outside the Windows Operating System before the laptop is despatched to Egton. It is recommended that you also test that you can read and recover your backup set if there is a requirement to do so. This includes the ability to restore any associated applications.

**p** Remove **any** 'sensitive' data from the laptop before it is despatched. Sensitive data can be defined as personal information held on clients, customers or patients (bank account details, address details, medical records for example).

If the Operating System becomes unstable, Egton will restore it back to a known good configuration, which may involve formatting the hard disk.

**p** Unnecessary software should be uninstalled.

**p** Any BIOS anti-virus functionality has been disabled.

▶ Complete a 'Full' Windows Defrag. Please note that this could take some time depending on disk size and fragmentation state.

▶ Provide the local Administrator account password so that the encryption software can be installed\*.

▶ Laptop users must ensure that they include the power adapter when the laptop is sent in.

### Egton Support

Please contact Egton Support on **0845 125 5530** for any support enquires (including password reset).

\* The password should not be written down on paper and placed with the laptop.

No part of this document may be sold, hired, reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording and information storage and retrieval systems for any other purpose than the purchaser's use without the express written permission of EMIS. Every effort is made to ensure that your Egton documentation is up to date, but our commitment to constantly improve our software and systems means that there may have been changes since this document was produced.

• tel 0845 124 5245    • fax 0845 124 5246    • [mail@egton.net](mailto:mail@egton.net)    • [www.egton.net](http://www.egton.net)

Egton • Stafford House • Unit 2 Leathley Road Industrial Estate • Leathley Road • Hunslet • Leeds • LS10 1BG