Disk Imaging and Pointsec™ for PC

Overview

When deploying hardware or software some organizations utilize disk-imaging software applications, such as Symantec Ghost, to replicate a standardized workstation or laptop configuration. Pointsec fully supports disk-imaging software. However, the timing of the imaging is important due to the Pointsec key generation process.

Disk imaging software creates a copy or image of a standardized hard disk that can be deployed to the masses through LAN, WAN or multimedia. The result is imaged-workstations that have the same software installed and is configured as the original workstation. Using imaging software, administrators can deploy or restore an operating system image or application onto a PC in minutes and then configure individual user settings and profiles to customize the PC.

This process of disk imaging saves large organizations time, money and resources. Essentially, it enables them to install and configure one workstation and then copy it to thousands of machines.

Pointsec Generates a Unique Key for Each Partition

In order to provide the highest possible level of security, Pointsec generates unique encryption keys at installation for each partition on the primary hard disk. In an enterprise deployment each partition the hard disk will use a unique encryption key for encryption and decryption. A unique encryption key on each partition ensures hardened security should an encryption key become compromised on a specific partition. In such a case, only one partition on the disk is affected while all other partitions and disks within the enterprise remain secure.

This document explains how to image a partition or hard disk properly so that unique encryption keys are created for each partition in a deployment.

Pointsec for PC and Low Level Installation

In general, installing Pointsec is comprised of two phases. The first phase installs all Windows-dependent components and the second phase creates a unique encryption key for each partition as well as modifies the boot record to ensure boot protection through authentication.

In the first phase, Pointsec installs the Graphical User Interface (GUI) which consists of the administrative program, disk monitoring tools, profile and software update services as well as segregating the contiguous space for the local user database. During this phase, the installation also issues the command to install the low level driver upon reboot.

In phase two, the PC is automatically or manually shutdown and rebooted, Pointsec marks the partitions and starts the generation of the unique encryption keys necessary to access the partitions. To ensure the generation of unique keys for every partition on every disk, the procedures described in the next section must be used when involving Pointsec in the imaging process.

Disk Imaging Procedure with Pointsec for PC

In order to achieve maximum security every partition in the organization must have a unique encryption key. Therefore, we must image the master workstation at the correct point in time. That point in time occurs before phase two of the installation.

1. Install Pointsec as the last application on the machine that is to be imaged as your "gold or standard" image.
    a. To reduce the number of images you maintain use Sysprep to create one master image to install Windows 2000 on destination computers with different mass storage controllers. If you are using sysprep with the automatic computer name generation switch, install Pointsec as the last application before booting through a network bootable diskette to create the image.
2. When phase one of the installation is complete, Pointsec may prompt for a reboot – Answer NO

NOTE: If you are installing Pointsec with a silent profile, the Pointsec installation does not prompt for reboot.

3. Reboot the machine from a DOS bootable floppy so that the imaging software can be run.

NOTE: If you are using 32 bit imaging software you are not required to reboot before starting imaging.

When a freshly imaged workstation is started, the second phase of the Pointsec installation will be initiated and unique encryption key will be generated for each partition.

Points to Consider When Using Disk Imaging and Pointsec

Taking the Disk Image at the Correct Stage

The image of the 'original' workstation must be taken at the correct stage in the installation process. If this is not done correctly, Pointsec will not function properly. Furthermore, the controls Pointsec uses for ensuring a secure system may also be violated during the imaging process.

Imaging a NTFS Partition

If Pointsec is installed on a partition that is using the NFTS file system, the image needs to be taken from the 'original' disk, and loaded on the 'clone' disk using a sector-by sector image copy. Be aware that with sector by sector encryption, the image will match the size of the hard drive being imaged.

Difficult to Associate Recovery Files to Imaged Machines

When Pointsec creates the recovery file, it uses the computer name as the first part of the name for the recovery file (e.g. <computer_name>_R.pvr). When installing Pointsec on several workstations using disk imaging, all of the workstations will have the same computer name and the same recovery search path for the recovery file.

Pointsec handles duplicate recovery files by appending unique identifiers to the end of the recovery file name, changing the _ (underscore) at the end of the filename to first 0-9, and then A-Z. The problem occurs when there is a need to identify which recovery file belongs to which machine.

The most common resolution to this issue may be to utilize software such a Sysprep.

Risk that Pointsec Will Have No Way of Naming the Recovery (.pvr) File

When Pointsec creates recovery files for workstations with identical computer names, a variable character at the end of the recovery file is used to differentiate them. The following characters are used, 0-9 and A-Z. In total, Pointsec has 35 different ways of naming a recovery file for a specific computer name on the network. Sysprep can be used with the automatic computer name generation switch to resolve this issue. If the computer name is renamed after the Pointsec Volume Recovery File (pvr) file is created, a new pvr file with the new computer name is created at the recovery file location after sysprep is run. The old computer name_R.pvr files can and should be deleted.

Recovery Search Path Is Set to the Network in the Image

When setting up the Pointsec profile, the search path could be set to the network to enable backup and safe storage of these files for recovery purposes. If the image is restored to the workstation while the workstation is not connected to the network, the recovery file will not be created and encryption will not start. The best resolution to this issue may be to use a temporary search path or writing the recovery files to a local drive and manually transporting file to a secure data repository.

Quick Reference Guide

- Pointsec should be installed as the last application in the image in order to ensure that unique encryption keys are created on each partition.

- Use sysprep to prepare the image for large scale deployments.

- Machine should be rebooted after Pointsec installation and imaged from a DOS bootable floppy.

- If using NTFS, use sector by sector imaging for Pointsec installation to properly install.

- When installing Pointsec be aware of location Pointsec Volume Recovery File (PVR) is written.

NOTE: For more detail instructions on deploying Pointsec for PC with Ghost software, please contact your Professional Service representative.