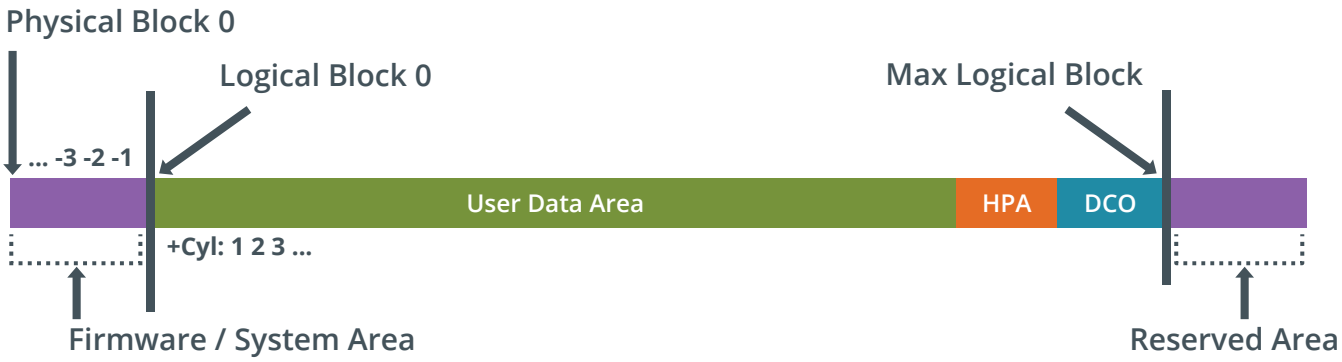
Does Your Data Sanitization Software Address The DCO Correctly?

www.WhiteCanyon.com | Sales@WhiteCanyon.com | 1 (801) 224-8900

THE PROBLEM: DCO LOCKING

DCO stands for Device Configuration Overlay. Computer system vendors often use various hard drive vendors when building their devices. By utilizing the DCO, the computer vendor can display the exact same available hard drive space on each device regardless of the actual hard drive capacity. In order to prevent a user from adjusting the hard drive capacity by removing the DCO, most computers will issue a lock on the DCO when the system is initially booted. This lock prevents any editing of the DCO settings. Since a locked DCO is not accessible to the user, it can potentially pose a threat to data security, if data has been stored on the DCO.

DCO controls are firmware based and require very specific command set with the hard drive in order to initially configure, edit or remove the configuration. Because of this, it is essential that the wiping tool is equipped to deal with a DCO by properly removing all locks and configurations before the wiping process. Dealing with the DCO improperly can result in potential data leakage and the misclassification of a "successfully" wiped hard drive.



Since the DCO are hidden areas of the hard drive, they are at risk to contain harmful and confidential information. Malware and viruses can copy confidential information to the DCO and potentially store sensitive data in these hidden areas of the hard drive.

As most data erasure software tools are unable to access and wipe the DCO, these hidden areas can present unique challenges for data security. Utilizing options such as factory reset or disk formatting will not effectively sanitize the DCO. Most software cannot detect the hidden areas of the drive, thus will perform the data erasure process without addressing this area of the drive. This gives the user a false assurance that their data has been securely erased.

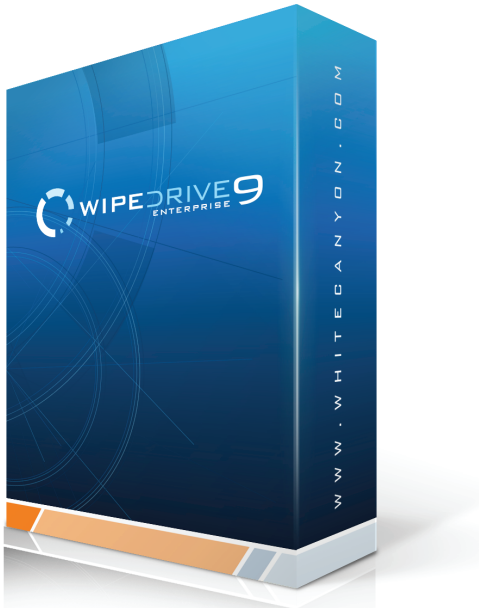
If malware or confidential data has been accidentally or maliciously copied to the DCO, it will remain there after a successful wipe. Because of this, it is crucial that the data erasure software implemented addresses the DCO on each drive.

THE WIPEDRIVE SOLUTION

Most data erasure software cannot detect the DCO, while others wipe the DCO and leave the hard drive unusable. This is not the case with WipeDrive.

WipeDrive addresses the DCO problem with these proprietary steps:

1. WipeDrive's proprietary software will unlock and remove the DCO.
2. WipeDrive then searches a list of hard drive manufacturer specifications to determine the size of the DCO and the area WipeDrive erased.
3. WipeDrive then compares the list to the DCO area it wiped and proves it securely purged all data from the drive.
4. WipeDrive then performs an audit of the drive to ensure the wipe was successful.



WipeDrive's proprietary data erasure software gives customers the peace of mind that comes with knowing that ALL their data is secure.

If you have any further questions about your data erasure needs, please contact our sales team 801.224.2952.