Why You Should Choose Destroy
Over Other Products

Accreditation

Destroy and Destroy Lite have undergone rigorous testing and has been accepted into the Australasian Information Security Evaluation Program (AISEP). They are the only products of their type to be listed on both the Australian Government's Evaluated Products List and the Common Criteria Evaluated Products List, the international standard for Information Technology.

Destroy and Destroy Lite are rated to a security level of EAL2+. No other competing product has been independently tested and evaluated to this level, so the end user of any "shareware" type product has no guarantee that the product will work as intended.

Destroy and Destroy Lite meet and exceed the Australian Government's Australian Communications-Electronic Instructions 33 (ACSI 33) Handbook 6, Media Security standards for hard disk wiping, in that it performs a pass of binary zeros which is then verified and binary ones which again is then verified (repeated three times for Destroy) and a final pass of random characters. Few competing products meet this essential standard.

Destroy and Destroy Lite meet and exceed the US Department of Defense three pass overwrite, and Destroy meets the German standard of seven overwrites.

Destroy's Security Benefits

Some of the other data erasure products on the market do not perform a passes of binary zeros and binary ones, but simply write random characters to the hard drive.

The general concept behind overwriting is to flip the magnetic value of each byte back and forth creating a layered overwrite effect. Writing a series of binary zeros and binary ones achieves the deepest overwrite effect as these values are the minimum and maximum magnetic values respectively.

By only writing random characters, the write is unpredictable and the depth of overwrite is effectively just scratching the surface. There is no guarantee that the appropriate magnetic flipping occurs, thus a significantly poorer overwrite is achieved.

Using Magnetic Force Microscopy (MFM) and Scanning Probe Microscopy (SPM) it is possible to recover data from an overwritten hard disk, even the recovery of the contents of an entire hard disk after a single overwrite is possible. There are several thousand SPM devices in the field and an SPM can be built for as little as USD $1,400. This must be considered when releasing computers containing confidential information where the information has value.

A six pass overwrite of binary zeros and binary ones which are verified has been deemed by the Federal Government's Defence Signals Directorate to suit up to a protected class of network (exceeds in confidence networks) which suits most organisations.

The multi-pass overwrite of alternating values (such as zero and one) is also the standard required by defence agencies around the world, with the number of overwrites varying depending on the security level of the recorded data. Programs that only perform random passes do not conform to ACSI 33 or international IT security standards.

It is also impossible to perform a full verify on random characters. This means programs that only perform random passes cannot verify that the data has been completely overwritten, and therefore again do not comply with ACSI 33 standards.

Many competing products also rely on the Bios or reported settings to determine the size of the hard drive to be wiped. This can be a problem if the Bios settings are incorrect or if the hard drive has been configured to downgrade the size of the drive. Additionally many drives have hidden tracks that are not reported in the Bios. Therefore if the Bios settings are incorrect, and a drive has hidden sectors, then a product that relies on these settings would not necessarily overwrite the entire hard disk, and critical data may still be retrieved from the disk.

Destroy on the other hand does NOT rely on the Bios or reported settings of the drive. On start-up Destroy scans each hard drive to identify the actual physical size of each disk. As Destroy does not rely on Bios settings, it will also detect any tracks beyond the reported maximum, then confirms these values and overwrites the drives based on the actual found settings. This means you can be sure that the entire drive has been overwritten.

In addition, other competing products have a switch that allows the operator of the program to select whether they want to perform a single, three, or seven pass wipe. This introduces a significant security risk because there is no way of knowing that a drive has been overwritten to your required number of overwrites. Destroy does not have a switch asking the end operator to select the number of passes it wants to perform, but comes on separate media so you can always be sure that you have run a seven pass wipe if you have used Destroy, or a three pass wipe for Destroy Lite, and a single pass for Destroy Ultra Lite.

How Destroy's Performance Differs

Destroy has built-in auto correction technology where even problematic hard disks can be corrected and still be securely overwritten.

Some other data erasure products on the marketplace require you to download special drivers to erase data from a SCSI hard drive. Destroy does not require any additional software or hard disk drivers to wipe SCSI drives, but can detect whether your disk is SCSI or IDE and will overwrite the drive regardless. Destroy can also be run on servers, including servers which have been raid configured.

Destroy is also easily distributed and can be emailed to allow operators to run the program locally where multiple offices exist. Destroy can also run without any user intervention as there is an auto-executing version of Destroy. You simply boot the machine with Destroy and it runs automatically. No screen or keyboard is required. This speeds up the process to commence the program significantly.

Licensing & Distribution

Our licensing allows you to overwrite all licensed machines as often as required during the license term. This means you can wipe the machines not only at the time of disposal, but when relocating PCs, or prior to sending them out for maintenance, if you have a new staff member coming on board that will be utilising an old PC, or even downgrading the security of the PC. Some other products limit you to the number of actual wipes the program performs. For example if you purchase a 100 license you are limited to only running the program 100 times.

Other competing products only provide a license to an identified number of users. These users generally have to be employees of the agency or organisation. With Destroy, we license the organisation to cover their entire computer fleet not just the end operator, so if utilising outsourcers to perform the data erasure process, or if employing contractors, you are never in breach of a Destroy license.