

ProtectStar Data Shredder 2.0 ***Product Guide***

Safe deletion of confidential data



Secure deletion of sensitive data:

The new **ProtectStar™ Data Shredder 2.0** ushers in an intelligent generation of solutions for secure deletion of sensitive data.

This compact and user friendly software was designed with the data deletion needs of both business and private users, and allows all data to be deleted in such a way that it is completely beyond recovery, even for experts and government agencies.

When you use **ProtectStar™ Data Shredder 2.0** to delete data from a hard drive or storage device, you are ensuring that confidential information such as bank data, passwords and employee data can never fall into the wrong hands.

The **ProtectStar™ Secure Deletion Algorithm©**, which was specially developed by ProtectStar™ for **ProtectStar™ Data Shredder 2.0**, is one of the best such algorithms available today. It carries out 50 deletion processes with virtually no noticeable computer performance loss, and in a manner that complies with all international data security standards.



Product features:

- ✓ Secure data deletion based on government approved and military data security standards up to the confidential, secret and top secret security standard levels.
- ✓ Deletes confidential data from hard drives, memory sticks, memory cards and so on
- ✓ Integration of the powerful ProtectStar™ Secure Deletion Algorithm© allows for fail-safe data security
- ✓ Secure deletion of free storage space, as well as the Windows recycling bin, Internet cache, cookies, temporary system folders and so on.
- ✓ Allows for secure cutting and pasting of files and directories
- ✓ Fully integrated into the Windows Explorer context menu
- ✓ System partitions and individual system drives can be deleted securely in offline mode without a boot medium

- ✓ Detailed deletion log provides evidence of deletion
- ✓ Supports multicore processors
- ✓ Technical support
- ✓ Supports FAT, FAT32 and NTFS

Minimum requirements for the relevant operating system:

- ✓ Microsoft Windows 2000, XP and Vista
- ✓ Microsoft Windows 2000 Server, 2003 Server and 2008 Server
- ✓ Windows 7 ready
- ✓ 32 and 64 bit compatibility
- ✓ 15 MB of free disk space

Product features & functions

	ProtectStar™ Data Shredder 2.0 Freeware	ProtectStar™ Data Shredder 2.0 Professional	ProtectStar™ Data Shredder 2.0 Server
Secure deletion of files, directories and partitions	YES	YES	YES
Secure deletion of free disk space	YES	YES	YES
Allows for secure cutting and pasting of files and directories	YES	YES	YES
Deletion wizard	YES	YES	YES
Preinstalled standard deletion algorithms	DoD 5220.22-M E	YES	YES
Fully integrated with Windows Explorer	limited	YES	YES
Secure deletion methods such as BSI, DoD 5220.22-M ECE, and ProtectStar™ Secure Deletion Algorithm	X	YES	YES
Secure deletion of hard drives, partitions, memory sticks and SD cards	X	YES	YES
Secure deletion of Internet cache, cookies, temporary files and so on	X	YES	YES
Integrates the highly secure ProtectStar Secure Deletion Algorithm™	X	YES	YES
Allows for secure cutting and pasting of files and directories	X	YES	YES
Detailed deletion log provides evidence of deletion	X	YES	YES
Technical support	X	YES	YES
Windows Server enabled	X	X	YES

With **ProtectStar™ Data Shredder 2.0** users can choose the following different secure deletion methods:

ProtectStar™ Secure Deletion Algorithm© (50 cycles)

At first, all data will be overwritten for two times with a random value, afterwards with their complements, and finally again with the random value from the first pass.

After this all data will be overwritten for three times using the Department of Defense (DoD) 5220.22-M (E) standard afterwards with the random values, and finally again with the DoD 5220.22-M (E) standard.

At the end all data will be overwritten with the method from Peter Gutmann for 35-times by defined rules and another three defined rules from ProtectStar, Inc.

The ProtectStar™ Secure Deletion Algorithm© has in total sum 50 passes.

DoD 5220.22-M ECE (7 cycles)

The method is based on the January 1995 ,National Industrial Security Program Operating Manual' by the

U.S. Department of Defense (DoD). In this seven cycle variation (DoD 5220.22-M ECE), data is first overwritten three times with DoD 5220.22-M (E) Standards, then with a specific random value, and finally once again with DoD 5220.22-M (E).

BSI Method (6 cycles)

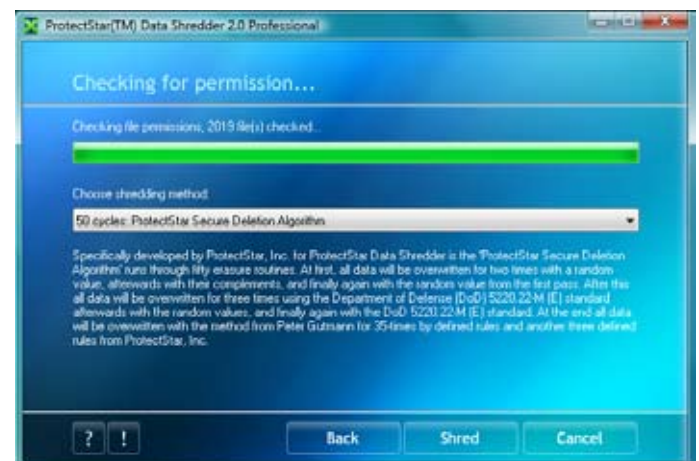
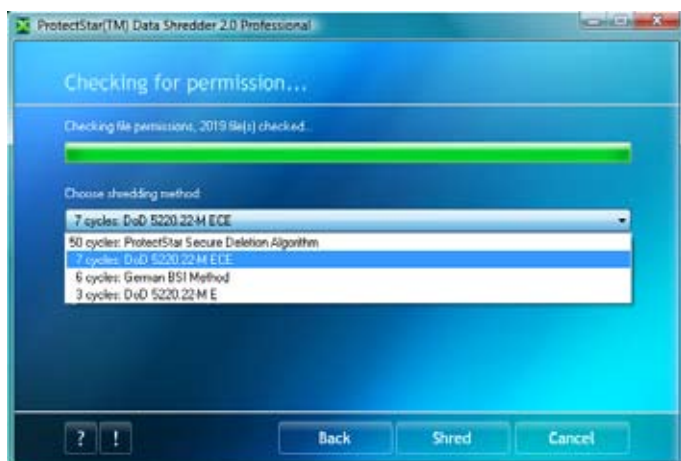
This method conforms to the standards of the German BSI as described in the ,BSI IT Baseline Protection Manual' (more information: www.bsi.de). Data are overwritten with a random value and then with this values compliment. This procedure is completed with new random values three times.

DoD 5220.22-M E (3 cycles)

The method for low security but for high execution speed is based on the.

January 1995 ,National Industry Security Program Operating Manual' from the U.S. Department of Defense (DoD 5220.22-M). The variation (DoD 5220.22-M E) offers 3 cycles in which the data are overwritten with first a set value, then its compliment, and then a random value.

Further information regarding secure data deletion with ProtectStar™ Data Shredder 2.0

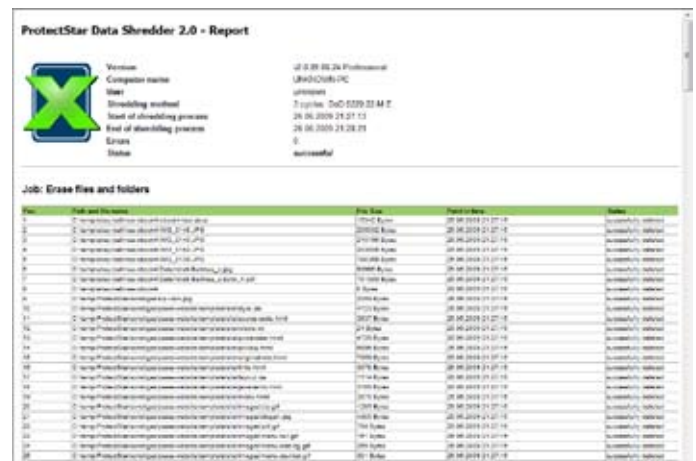


ProtectStar™ Data Shredder 2.0 – extended solution analyses

The table below lists the applications that were used to recover data that was securely deleted using the deletion algorithms that are integrated into **ProtectStar™ Data Shredder**.

	DoD 5220.22-M E 3 cycles	BSI Method 6 cycles	DoD 5220.22-M ECE 7 cycles	ProtectStar™ S.D.A. 50 cycles
ActiveUndelete v5.1	/	/	/	/
File Scavenger v3.0	/	/	/	/
FileRescue Professional v2.6	/	/	/	/
Flying FileRecoveryAngel v1.15	/	/	/	/
GetData Recover myfiles v3.9	/	/	/	/
MagicRecovery v3.2	/	/	/	/
Ontrack EasyRecovery PRO v6.0	/	/	/	/
PC Inspector File Recovery v4.0	/	/	/	/
R-Undelete v2.1	/	/	/	/

- + Data recoverable
- / Data not recoverable



Certifications

In a domain where confidence and security are key factors, **ProtectStar™ Data Shredder 2.0** provides a best-in-class deletion platform whose deletion method has been certified by the following organizations and individuals, among others:

- ✓ **National Security Agency (NSA)U.S.**
- ✓ **Departments of Defense (DoD)U.S.**
- ✓ **Department of Defence Sanitizing**
- ✓ **The National Computer Security Centre (NCSC-TG-025)**
- ✓ **Bundesamt für Sicherheit in der Informationstechnik (BSI)**
- ✓ **British HMG Infosec Standard No.5**
- ✓ **Bruce Schneier's AlgorithmusPeter Gutmann's Algorithmus**
- ✓ **Deutscher Standard VSITR**

NEW *Optimizations/new functions relative to the previous version*

- More intelligent:** The application's deletion wizard now helps users to delete the desired files, folders or partitions in a few easy steps
- More secure:** The new ProtectStar™ boot mode allows for secure deletion of entire partitions
- Quicker:** Up to 30 percent faster than the previous version
- Simpler:** New intuitive and self-explanatory user interface
- More comfortable:** Secure cutting and pasting of files, folders and directories is now easier than ever
- More complete:** The application's extended deletion log proves that the target data has been deleted and can be saved and printed out

And what's more, the new version of ProtectStar™ Data Shredder 2.0 is also

- ✓ available in a server Version
- ✓ Windows 64 bit enabled
- ✓ Windows 7 ready

Background Informationen:

Deletion doesn't always really mean deletion

More than 98 percent of computer users worldwide believe that the data on a hard drive or external storage device is always irretrievably deleted when the disk/device is reformatted. Such users also hold the unfortunately incorrect opinion that files deposited in the Windows recycling bin or the like can be deleted securely via the delete command and can thus be safeguarded against access by unauthorized persons.

But this is far from being the case, mainly because Microsoft Windows and other operating systems do not delete file data from a hard drive fully and irretrievably. What happens instead is that the name of the deleted file in the file allocation table (FAT) is assigned a special symbol. The symbol used in the FAT system is ASCII 229 (0xE5); for the NTFS file system a special attribute is added to the header of the deleted file.

This is basically like removing the table of contents from a book: although it's no longer possible to locate specific information in the book, it can of course still be read.

In the standard deletion procedure as described above, the purportedly deleted file is merely concealed from the user, and the cluster comprising the file is regarded by the system as "free." The actual file content and virtually the entire file name remain recoverable until data is again stored in this cluster – which means that the original file can be easily read, even by non-experts, with a few mouseclicks and the relevant software.

An introduction to data deletion

The only guaranteed way to definitively remove all data from a hard drive or storage device such as a memory stick is to overwrite this data by means of specially tested and recognized deletion methods.

Data that has been deleted in this manner can never be recovered by qualified specialists using the relevant software and methods.

Data is stored on a hard drive in binary sequences comprising 1 and 0 that are represented on various magnetized sections of the hard drive. Thus a 1 that has been written to a hard drive is also read as a 1 by the controller, and the same applies to a 0. However, if an existing 0 on a hard drive is overwritten by a 1, the result is not 1 but only 0.95.

By the same token, the result of overwriting a 1 with another 1 is not 1 but rather 1.05 or the like, owing to the heightened magnetism engendered by the overwrite. In practice this difference is irrelevant as the system will in any case interpret the values correctly. However, using specialized software and slightly modified hardware, the layer below the current data can be read if the exact values are taken; and thus the 0.95 value will be read as the 0 that was originally there. During this process, hard drive sector magnetization levels and traces of the original data are analyzed, and these traces are then recovered using microscopic magnetic processes.

Data should be overwritten not with standardized patterns such as 0000 but rather with patterns such as C1 (hexadecimal, the equivalent of the bit string 11000001). In a second procedure, a complementary pattern such as 3E (the equivalent of the bit string 00111110) should be used so as to ensure that each bit is modified at least once.

Hence the overwrite procedure should be realized a number of times, and preferably as often as possible, as this yields more satisfactory data security results. In other words, the principal that should be applied is this: the more often file data is overwritten, the more securely deleted it will be.

Contact & Copyright

Corporate Headquarter:

ProtectStar, Inc.
444 Brickell Avenue
Suite 51103
33131 Miami, FL
USA

Phone: +1 888 218 4123
Fax : +1 888 218 8505
e-Mail: info@protectstar.com
Web : www.protectstar.de

European Headquarter:

ProtectStar, Inc.
Daws House
33-35 Daws Lane
London NW7 4SD
UK

Phone: +44 20 8906 6651
Fax : +44 20 8906 6611
e-Mail: info@protectstar.com
Web : www.protectstar.de

Copyright by ProtectStar™, Inc.

Copyright by ProtectStar™, Inc. All rights reserved. All texts, pictures, graphics, etc. are subject to copyright and other laws for the protection of intellectual property. Especially the reprint, integration into online services, Internet and duplication (also in extracts) on data media such as CD-ROM, DVD-ROM etc., are admitted only with the prior written consent by ProtectStar™, Inc. They must neither be copied for commercial purposes nor for dissemination, nor must they be altered and used on other Web sites. Some texts, pictures, graphics, etc. of ProtectStar™, Inc. also contain material which are subject to the copyright of those who provided them to us.

The information is provided by ProtectStar™, Inc. without any assurance or guarantee of its correctness, be it express or implied.

Neither do we make any implied affirmations regarding the negotiability, the suitability for certain purposes or the nonviolation of laws and patents.