DBAN vs. Certified Data Erasure: Which is Right for Your Organization?

When it comes to choosing a data sanitization method for your hard disk drives (HDDs) and other IT assets, there are three questions to consider.

- ✔ Does it meet the minimum threshold for your risk tolerance?
- ✔ Does it achieve data sanitization?
- ✔ Does it meet your organization's needs to meet industry-specific guidelines and data protection regulations?

1. Determine Risk Tolerance

First, you must understand the level of risk your organization is willing to allow based on government and industry regulations or internal policies with which you must comply. You must also understand the types of data residing on your drives and the level of sensitivity associated with that data.

For a personal computer that's accessed infrequently and only used to store music, the risk associated with remnant data is much lower than a computer that's used by a HR Director who stores personal employee information.

Data protection guidelines vary across industries, but HIPAA and EU GDPR are two that refer to to the protection of an individual's information and carry heavy fines (4% of annual global turnover or €20 Million for EU GDPR) if improperly erased. Most guidelines and regulations also require an auditable trail for your IT assets.

	DBAN	Blancco
Product Features		
Supported Erasure Standards	6	22+
Erasure Reporting	✖ No certificate or guarantee	✔ Digitally Signed Report (XML & PDF)
Certifications, Approvals and Compliance		
DoD 5222.2M, NIST 800-88	✖	✔
Third-Party Certifications and Approvals	✖	Common Criteria, NATO CESG, 6+ others

blancco

2. Achieve Data Sanitization

Data erasure is one of the three methods that achieve data santization, but the erasure software chosen must allow for three steps:

	DBAN	Blancco
1. Selection of a specific standard, based on your industry and organization's unique compliance needs	✔	✔
2. Verification that the overwriting methodology has been successful and removed data across the entire device, or Target Data (if specifically called)	✖	✔
3. Production of a tamper-proof certificate containing information that the erasure has been successful and written to all sectors of the device, along with data about the device and standard used	✖	✔

3. Address all Requirements

The method of data sanitization used should be capable of addressing most of your data storage devices. From faster and smaller SSDs, to mobile devices and files and folders, you need to ensure the software chosen can support current technology trends, scale for the future and provide a unified and centralized data erasure solution.

So what data removal method is best for your organization? If you use DBAN, wiping your drives is free today, but it could leave your organization open to risk tomorrow.

	DBAN	Blancco
Erasure		
HDD Compatible	✔	✔
Secure SSD Erasure	✖	✔
Remapped Sectors and Hidden Areas	✖	✔ Patented SSD process
Erasure when data is on-network	✖	✔
Erasure for Removable Media, LUNs, Mobile Devices and Virtual Machines	✖	✔

blancco

	DBAN	Blancco
Functionality		
Delivery Methods	CD	CD, USB, MSI, PXE
Supported HDD Connectors	ATA, SATA, SCSI	ATA, SATA, SCSI, SAS, FIBRE CHANNEL, USB
RAID Dismantling	✖	✔
HW and Smart Tests	✖	✔
User Authentication	✖	✔
License Harvesting	✖	✔
UEFI Support	✖	✔
Support		
Global Technical Support	✖	✔
Regular Software Updates	✖	✔

Why Blancco?

For 20 years, Blancco has offered solutions that support compliance with data protection and privacy regulations such as the new General Data Protection Regulation (EU GDPR), HIPAA, PCI DSS and more. We support the need for heavily-regulated industries to stay compliant with these regulations with data erasure solutions that satisfy (and often exceed) those requirements.

Experience the Blancco difference. Request a free trial of Blancco Drive Eraser for enterprise organizations today.

For more information about Blancco Technology Group, please visit our website at www.blancco.com.