Why is Certification Important

CERTIFICATION VS. COMPLIANCE

There is a significant difference between software claiming to comply with standards and the National Security Agency (NSA) certifying compliance. We don't believe our customers should have to verify that our software does what we claim, so we are Certified by NIAP to EAL 4, higher than any other software wiping tool (see http://www.niap-ccevs.org/st/vid10395/). This certification took over a year and cost literally hundreds of thousands of dollars, but they verify that WipeDrive works the way it is designed.

When you see wiping software that claims to "comply" with standards, all it means is that they believe they comply but there is no outside body that has independently verified and authenticated that they comply.

RISK VS. COST OF AVOIDING RISK

We recognize that there is a trade off between risk and the cost of avoiding risk. But many of our larger customers, like the DoD, Air Force and DHS, don't have the option of accepting any level of risk. Our software is designed with their input to address their needs so all our customers benefit.

We start with each of the published standards (HIPPA, Sarbanes-Oxley, SOX, GLB, PCI, NIST 800-88) as a minimum security level. Working with our most risk-averse customers we have added features that allow both operational efficiency and increased security (such as remote wiping, digitally signed audit logs and fully scripting the wipe process to eliminate human error, faster wiping speed).

WHAT DOES THE NIAP EAL4 CERTIFICATION MEAN?

The National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) have established a program under the National Information Assurance Partnership (NIAP) to evaluate IT product conformance to international standards. The program is officially known as the NIAP Common Criteria Evaluation and Validation Scheme for IT Security (CCEVS).

Part of the EAL4 standard is a line by line source code audit. The purpose of the audit is to certify not only that the software works as intended but also that there are no security holes, malicious or otherwise. Software EAL3 and below do not include this review and therefore the user cannot be assured that there aren't any unseen security holes.

THE CONCLUSION BY THE NATIONAL SECURITY AGENCY

After over a year of testing by the National Security Agency (NSA) and Booz Allen Hamilton, an international independent Consulting Firm, (www.boozallen.com) the conclusion of WipeDrive's performance is:

> "WipeDrive is a disk sanitizing tool that permanently erases all data from hard drives and other data storage devices. This includes but is not exclusive to: HPA partitions, DCO partitions, remapped sectors, operating systems, programs, and user files. This data is permanently destroyed as to make any type of forensic data recovery impossible."

The NSA report further states that WipeDrive provides

"Data destruction in accordance with US DoD 5220.22-M. WipeDrive complies with all of the following disk wipe standards:

- US DoD 5220.22-M
- Standard single pass overwrite
- US Army AR380-19
- US Air Force System Security Instruction 5020
- US Navy Staff Office Publication P-5329-26
- US National Computer Security Center TG-025
- Australian Defense Signals Directorate ACSI-33 (X0-PD)
- Australian Defense Signals Directorate ACSI-33 (X1-P-PD)
- Canadian RCMP TSSIT OPS-II Standard Wipe
- CIS GOST P50739-95
- GB HMG Infosec Standard #5 Baseline
- GB HMG Infosec Standard #5 Enhanced
- German VSITR

POTENTIAL RISKS OF NON CERTIFIED WIPING SOFTWARE

Standards, like HIPPA, Sarbanes-Oxley, SOX, GLB, PCI, NIST 800-88, contain one common, overriding standard: that the all drive data must be overwritten. KillDisk and free drive deletion software clearly falls short of this basic goal.

HPOS AND DCOS

Some wiping software does not remove HPAs (Host Protected Areas) and DCOs (Drive Configuration Overlays) this means that the data in these partitions won't be overwritten. Also the possibility exists of someone creating a hidden partition on the drive. Not wiping these hidden partitions is both a security risk and a compliance issue.

WipeDrive securely overwrites these hidden partitions. The NIAP certification states that neither Host Protected Areas (HPA) and Device Configuration Overlays (DCO) remain after WipeDrive has completed. Testing the removal these hidden partitions was a key element of the WipeDrive Security Target.

HANDLING OF UNWRITEABLE SECTORS

Per NIST/800-88 "Overwriting cannot be used for media that are damaged or not writeable. "[SP 800-36].

Sectors on a hard drive that become damaged are remapped to another physical location on the drive and may not be addressable and therefore cannot be overwritten. If that occurs those sectors will not be overwritten with some software and data will remain. This data can be relatively easy to recover forensically and could contain information previously stored on the drive.

WipeDrive will use the ATA Secure Erase command to overwrite remapped sectors. If WipeDrive encounters a remapped sector and it is unable to overwrite the sector, then it will continue to overwrite the remainder of the drive and give the User a warning that certain sectors could not be overwritten. The user can then decide if the drive needs to be physically destroyed.

Per the NIAP report on testing this feature "This test attempts to create a device that has been marked with faulty sectors and feed it into WhiteCanyon for wiping. WhiteCanyon should be able to successfully erase all data surrounding the faulty sectors and should flag them as faulty appropriately."

VULNERABILITY RESULTS

The NIAP testing also concluded, "The testing staff, upon completion of the vulnerability testing process, were able to verify that all tested areas of potential vulnerability contained no actual vulnerabilities."

No user of can be expected to review the security level of their wiping software as thoroughly as the NSA did. Using non-certified wiping software means that the user must rely on the marketing claims of the software developer.

For companies entrusted with their own private data, as well as customers and user's data, trusting marketing claims isn't enough. We believe these companies should only use software that has been certified to the highest standards.