blancco

Is a Low Level Format Enough to Guarantee Data Sanitization?

Historically, many organizations have used various forms of formatting (low level format, deep format, full format, etc.) as their process for removing data during asset decommissioning. This has resulted in both process inefficiencies and severe data breaches.

Formatting can go by many names, such as low level format, deep format or full format. This summary will outline why none of these formatting options can be the foundation of a secure decommissioning process.

Note that you will also find several OEM alternatives to formatting that are referred to as "erasure." These methods also have limitations and do not meet the guidelines for true data erasure, which features a chosen erasure standard, verification and certification.

What is Formatting?

In modern operating systems, there are typically two options for formatting: a format and a quick format. Quick format is not an erasure solution because it only removes the index, but a full format attempts to overwrite the diskspace visible to the OS with zeroes. If everything goes perfectly, then the one round of overwriting with zeroes will remove data to a large extent. However, the reality and level of detail that you need to consider is a bit more complex.

The key issue with formatting is that there is no way to confirm that the data is gone. Verification and certification (as shown in this example report) are key for security and auditing purposes.

Data Erasure Report

blancco

[illegible]

Issues that Arise with Formatting

- It is often unknown if the Windows format has managed to detect the disk size correctly. This is especially true if the disk has HPA or DCO areas. In these cases, it is likely that only part of the disk gets overwritten.
- There is no verification with a format, so if something goes wrong with the process, there is no way to know it. For example, an operator may choose a quick format instead of a deep format based on misunderstandings or time pressure. Another common issue? Interruptions. When you process more than one computer, it's likely that one or more of the machines will turn off from loss of power or being accidentally unplugged at some point.
- With a proper erasure software the (digitally- signed) erasure report creates an audit trail. With it organizations can show that they have done their part in safekeeping data correctly. A format does not provide this type of auditable verification.
- Many modern computers come with solid-state drives (SSDs), and to safely overwrite those, a special SSD overwriting method is needed. SSDs have overprovisioned areas which will be untouched if formatting is used as a data destruction method.
- Formatting does not identify bad sectors on hard drives, opening a potential security risk. When organizations use software-based data erasure (overwriting), they can determine how many of their hard drives have been erased successfully—and which of these erased drives contain bad sectors. Those with bad sectors are typically sent for physical destruction to avoid potential security risks.
- Formatting can be very time-consuming. It is not a process that you can easily scale and run automatically in a production flow. Additionally, if you are formatting servers or desktops with more than one drive, these drives cannot be processed in parallel.

More Information About OEM 'Erasure' Solutions

Generally, OEM erasure (formatting) solutions won't offer the industry standard erasure methods, such as DoD 5220.22M or NIST. Either there is no option to select an erasure method, or if there are choices, the overwriting methods are vaguely named (e.g. "fast method"). OEM erasure solutions are not certified and do not comply with known data erasure standards.

Second, it's often difficult to start OEM erasure software. In some cases, the right option must be found and selected from the BIOS; in others, the software may be hidden in the recovery partition, etc. This means that person erasing the computer with OEM solution needs to use unnecessary time trying to find OEM solution.

Third, formatting can be interrupted due to many reasons, such as power failure, machine failure, manual shutdown, etc. In such a case if technician decides to just send that hard drive for further processing, then there is a risk of data leakage. There is no way to determine how many how and how many formats are interrupted on a large scale. And with no verification or certification of the process, the issue of security is further complicated.

OEM solutions may be good enough for average consumer that is simply looking to erase hi/s her personal computer before selling it or donating it. However, when an organization, such as an electronics recycling center, is dealing with hundreds or thousands of computers, using an OEM erasure solution is more trouble than it is worth.

Why Blancco Data Erasure Solutions?

With secure data erasure from Blancco, you can be confident that data is erased completely and permanently, with no chance of recovery. Here are some additional benefits available through Blancco data erasure solutions.

Key Benefits:

- With Blancco software, performing an erasure is a straight-forward and user-friendly process.
- Blancco is the only company with a patented SSD erasure method. Additionally, Blancco is globally certified and third-party tested by several top organizations.
- Blancco software provides many different commands (including crypto erase) to securely erase any drive and prevent data recovery using laboratory techniques.
- Verification and certification are a part of every erasure process.
- Blancco provides customers with information about bad sectors so they can make informed decisions about physical destruction.
- Blancco Management Console provides a central view of the data sanitization process, so you can ensure it's adhering to set policies set forth in your organization.
- Full integration with your asset management system provides real-time monitoring of how many assets are erased versus how many are decommissioned.

The conclusion for enterprises and governments around the world when taking these facts and practical implications into account is that deep format cannot be approved in best practice data sanitization policies and asset decommissioning processes. It is simply not secure enough to guarantee complete, permanent erasure of sensitive data.

For more information about the differences between formatting and Blancco data erasure solutions, contact your local sales representative today.