When Are Encryption and Cryptographic Erasure Not Enough?

Should organizations rely solely on encryption and cryptographic erasure as a means of protecting data? In this document, we'll discover why the answer to that question is a resounding no. The ideal way to approach data protection, and specifically data sanitization, is to implement a multi-tiered, layered approach that goes beyond encryption alone.

Ask Yourself

"Can we rely 100% on data encryption to protect our data, brand and reputation?"

What is Encryption?

Encryption is the process of converting information or data into a code to prevent unauthorized access. Encryption is completed by using an algorithm to encode the data so that it can only be deciphered with an encryption key.

What is Crypto-Erase?

What is Cryptographic Erasure (CE)?

This wiping method uses the native command to call a cryptographic erasure, which erases the encryption key. While the encrypted data remains on the storage device itself, it is effectively impossible to decrypt, rendering the data unrecoverable.

Proper implementation of Cryptographic Erasure follows a 3-step process:

1. Find and overwrite crypto keys and password
2. Verify full encryption of media
3. Create tamper-proof report

Pros, Cons & Risks

Pros

- CE can take only a few seconds to complete.
- Proper implementation can render data unrecoverable.

Cons

- Self-encrypting drives can have implementation issues.
- Keys must be stored and managed – without secure storage and management, these keys are vulnerable to attack.
- Most CE does not provide any form of verification.

Risks

- Encryption has a "use by" shelf life. As cryptography advances rapidly, algorithms that were once considered "strong" can be broken.
- If encryption is not in place (but the organization thought it was) or, it's removed, turned off, flawed or broken, ALL of the organization's data on the device is then accessible.
- Executive travelers can be ordered to unlock encryption on laptops when crossing sensitive borders.

blancco

Encryption/Crypto Erase Gap Analysis

Ask yourself the following questions about your organization's relationship with encryption and cryptographic erasure to determine any areas that may need to be addressed.

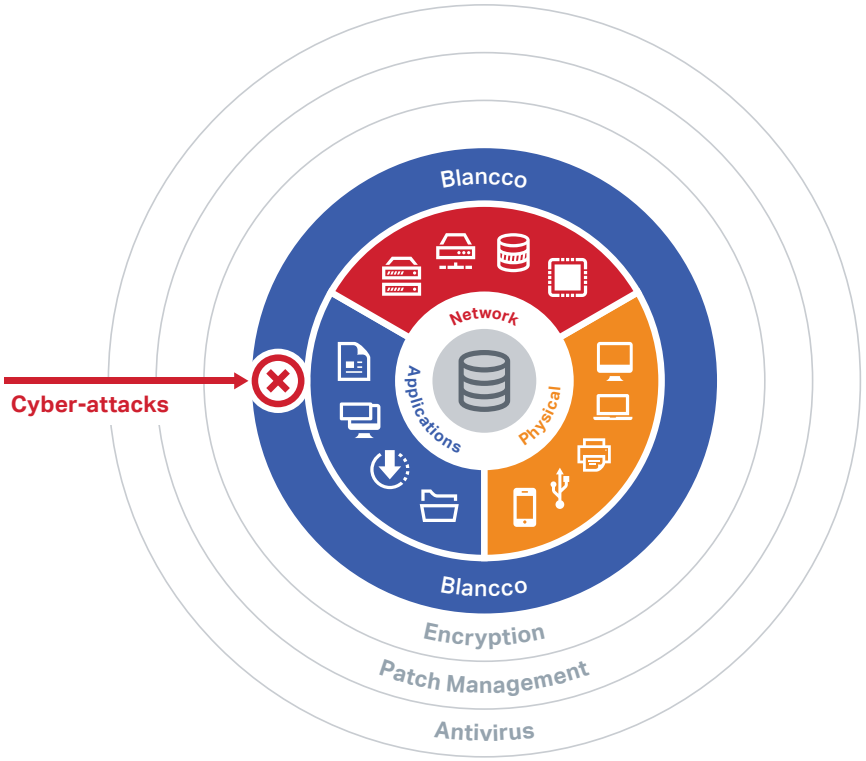
1. Where do you currently use encryption?
2. How do you manage and store your keys?
3. Do you:
   - verify that your CE was successful?
   - erase data on devices/severs/areas that cannot be encrypted?
   - manage encryption of your data in the cloud?
   - erase your files and folders?
4. Are you confident that your staff can effectively implement and manage cryptographic erasure methods?
5. Do you have a tight encryption key management process and policy? Is that policy being followed? Do you have documentation to prove that?
6. Are your key generation properties in line with specified NIST standards?
7. Do you know how your devices handle any errors encountered during the cryptographic erasure process?
8. Are your servers encrypted? How do you securely dispose of them?
9. Do you have an eDiscovery solution? What do you do with data it discovers is in the wrong place or has exceeded the time of your retention policy?

Taking a Layered Approach

Encryption isn't enough. Data erasure adds another layer to data security around your network, physical assets and applications. Why? Because if the data is erased, it can't be stolen. Encryption can prevent unauthorized access; however – it comes with risks.

Although Blancco supports encryption and cryptographic erasure within our solutions, we highly recommend that you provide an added layer of security via data erasure.

In a layered approach to data security, attacks that are missed by one defensive layer are defeated by another. **Data erasure represents a last line of defense in protecting your data.**



blancco

How Blannco Solutions Address Cryptographic Erasure

Blancco Drive Eraser

Because CE uses the native commands as defined by the manufacturer, it is only available if supported by the drive being erased.

Blancco Mobile Device Eraser

If a device has been previously encrypted, Mobile Cryptographic Erasure will erase the encryption key, rendering the data unrecoverable.

Blancco Differentiators

- ✔ Follows all three steps (remove key, verify, certify) for cryptographic erasure
- ✔ 100% tamper-proof report certifying the cryptographic erasure was a success

For more information on how to create a tiered data protection strategy that best fits your organization's data sanitization needs, contact us today.