


SOLUTION BRIEF

Absolute Device Wipe

Securely sanitize data across
your endpoints

absolute.com



Endpoint devices today hold a treasure-trove of sensitive data such as personal information, health records, credit cards numbers, or specific customer details. Considering the endpoint is the primary source of most global security breaches (68% of breaches today originate at the endpoint¹), the need to take seamless protective action on a device to limit the risk of vulnerable data being leaked is of paramount importance.

1 Ponemon Institute, 2020 State of Endpoint Security Risk

ABSOLUTE[®]

⚠ This action makes all encrypted data, including the OS, unretrievable on devices encrypted by BitLocker (Windows) or FileVault (Mac).

Description (optional)

Windows devices
 Unenroll devices after the Wipe is complete.

Mac devices
⚠ Mac devices will be automatically unenrolled after the Wipe is complete.

Administrator authorization
 Admin user

 Admin password

Confirmation
 I understand that once the Wipe is started on the device canceled or undone.

ABSOLUTE

CERTIFICATE OF SANITIZATION

Organization information
 Organization: Name of Organization

Device information
 Device name: ABS283749
 Serial number: AE017A1A34
 Manufacturer: Lenovo
 Model: THINKPAD X390 YOGA

Sanitization information
 Item Disposition: Purge Date Conducted: Jan 20, 2020
 Conducted By: Admin 01

Disk information

Model:	HS3874490	Serial number:	MPB48793901
Drive	Sanitization Method		
C:	Cryptographic erase		
D:	Cryptographic erase		

Model:	HS387474	Serial number:	MPB48793734
Drive	Sanitization Method		
E:	Cryptographic erase		
F:	Cryptographic erase		

I hereby state that the data erasure has been carried out in accordance with the instructions given by the software provider.

The Need For Secure and Verifiable Data Sanitization

Devices routinely undergo data sanitization as part of general decommissioning or when they are either lost or stolen. The erasure must take place quickly and securely to alleviate the risk of sensitive data falling in the wrong hands and to align with industry media sanitization standards. Cryptographic Device Wipe, tied to Absolute’s undeletable tether at the BIOS of devices, is an innovative erasure method involving the removal of encryption keys to securely wipe an encrypted drive while obtaining a certification to prove sanitization for future audits.

Seamless Device Decommissioning and Sensitive Data Protection

- ✓ Remotely decommission (retire/reuse/resell) used devices, while conforming to the purge standards stated in **NIST Special Publication 800-88** (Guidelines for media sanitization) and HIPAA regulations.
- ✓ Protect sensitive data residing on devices that are either lost or stolen.

Cryptographic Device Wipe

Wipe devices encrypted through BitLocker (Windows) and FileVault (Mac) and obtain a certificate of sanitization for audits. Breaking the device’s encryption chain by replacing the child and intermediate keys ensures all data is irretrievable. The drive can be formatted for reuse once the wipe is complete.

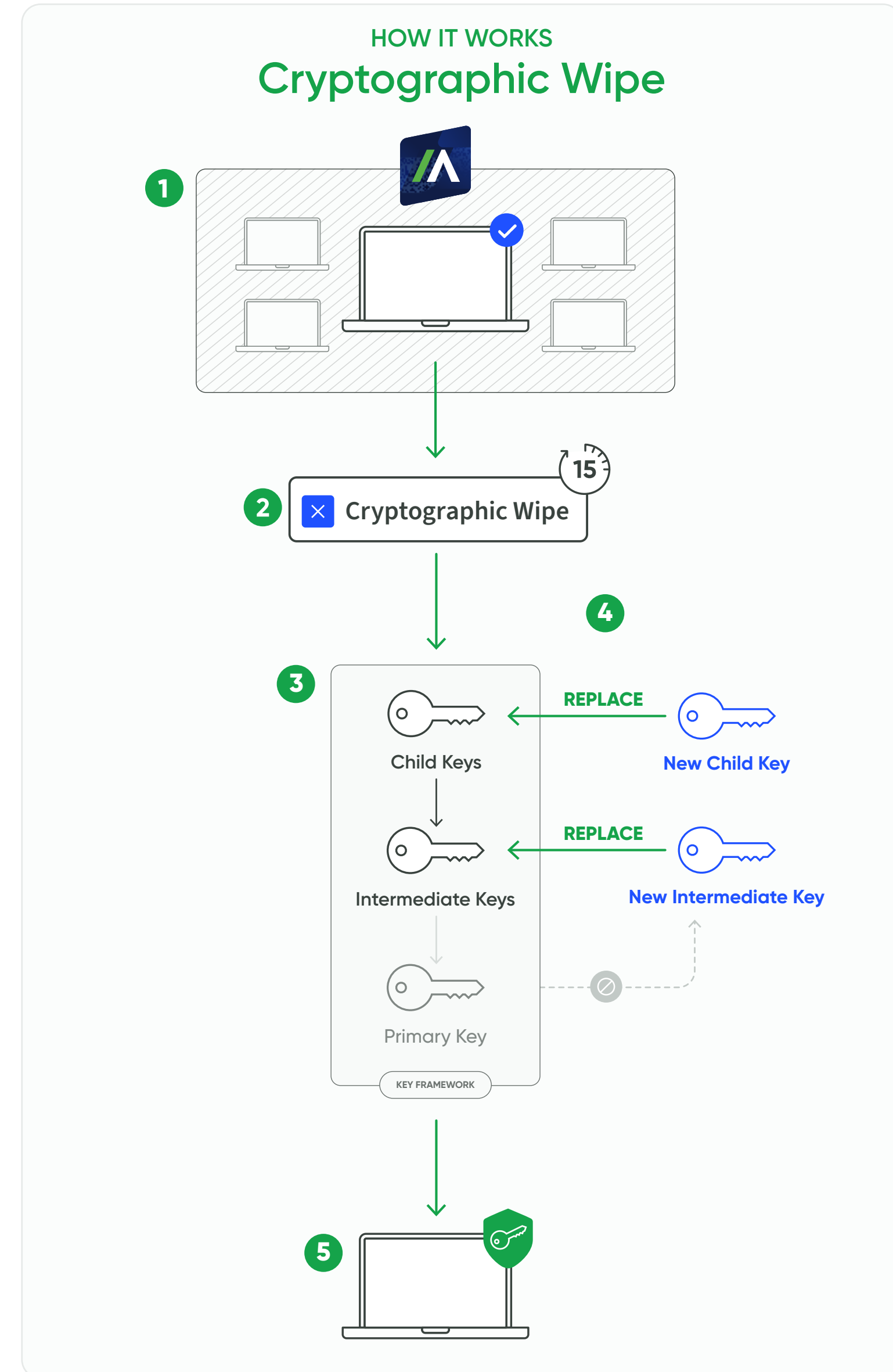
- ✓ **Need** Wipe all data on encrypted devices for decommissioning or to protect sensitive data on a missing device
- ✓ **How** Wipes data by breaking the *encryption chain* on devices
- ✓ **Speed** Fast, as the focus is just to replace the child and intermediate encryption keys
- ✓ **Supported Platforms**
 - › Mac: Full wipe of encrypted Mac devices (FileVault)
 - › Windows: Full wipe of any encrypted Windows devices (BitLocker)



How It Works

1. An authorized administrator selects specific devices to be wiped through the Absolute Console.
2. The administrator then runs the Device Wipe action.
 - > The command percolates down to the endpoint at the next call-in*.
3. The device's drive is encrypted through a three-layered hierarchical key framework as described below.
 - a. Primary key which protects the drive
 - b. Intermediate keys which protect the primary key
 - c. Child keys which provide access to the intermediate keys. These child keys are protected by a Trusted Platform Module (TPM), PIN/password or a recovery key.
4. Absolute Cryptographic Wipe generates a new recovery key by replacing the existing Child keys with new ones. As a result, all associated Intermediate keys are replaced as well.
5. This then results in the drive still being encrypted without any keys in existence that can unlock it. The destruction of data on the drive then satisfies media sanitization standards listed in [NIST SP 800-88](#).

*With an Absolute Resilience license, the Device Wipe command percolates down to the endpoint in an accelerated manner (i.e. a couple of minutes). With Absolute Visibility and Control, this process may take up to 15 minutes.





ABSOLUTE[®]

Trusted by more than 18,000 customers, Absolute Software is the only provider of self-healing, intelligent security solutions. Embedded in more than 600 million devices, Absolute is the only platform offering a permanent digital connection that intelligently and dynamically applies visibility, control and self-healing capabilities to endpoints, applications, and network connections – helping customers to strengthen cyber resilience against the escalating threat of ransomware and malicious attacks.

[Request a Demo](#)

