# Absolute Device Wipe

## Securely sanitize data across your endpoints

### THE NEED FOR SECURE AND VERIFIABLE DATA SANITIZATION

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 (70% of breaches today originate at the endpoint[1]), the need to take seamless protective action on a device to limit the risk of vulnerable data being leaked is of paramount importance.

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 purge 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.

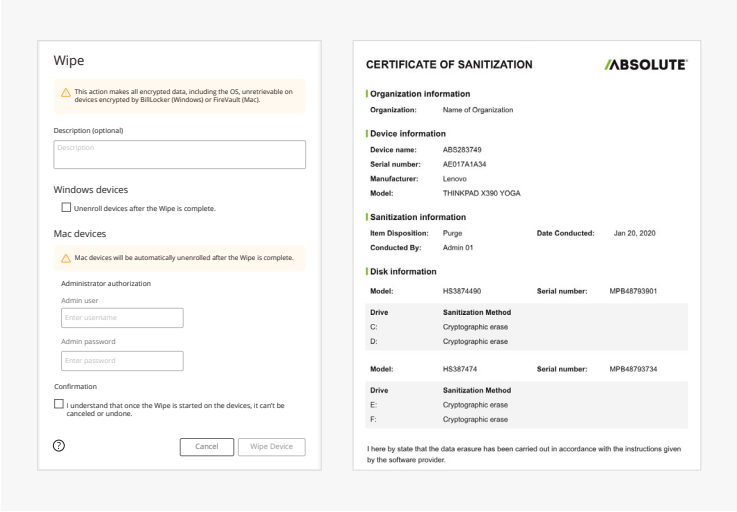
### SEAMLESS DEVICE DECOMISSIONING AND SENSITIVE DATA PROTECTION

- 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 intermediate key ensures all data is irretrievable and the SSD is reverted to its factory default state. 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 intermediate encryption key |
| **Supported Platforms** | **Mac:** Full wipe of encrypted Mac devices (FileVault)<br>**Windows:** Full wipe of any encrypted Windows devices (BitLocker) |




[1] IDC, 2016

## HOW IT WORKS

1. An authorized administrator selects specific devices and runs the Device Wipe action through the Absolute console.
2. The command percolates down to the endpoint at the next call in (occurs every 15 minutes).
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 key which protects the primary key
   - **c.** Child keys which provide access to the intermediate key. These child keys are protected by a Trusted Platform Module (TPM), PIN/password or a recovery key.
4. Absolute's crypto wipe breaks this encryption key framework by replacing and discarding the intermediate key, which then renders the child keys to be invalid.
   - **a.** 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 purge standards listed in NIST 800-88.