BestCrypt
Suite ™

Complete Endpoint Data Protection
For Windows & Mac

PAINLESS ENCRYPTION + FORENSICALLY CLEAN WIPING

Encryption used on its own still leaves vulnerabilities for sensitive data to be recovered. In order to achieve truly complete data protection, an active combined system of precise encryption and wiping mitigates these risks.

BestCrypt Suite protects endpoint data throughout the lifecycle:

- **Painless Encryption with BestCrypt**
  - Volume Encryption
    for superior whole disk encryption
  - Container Encryption
    for selected files/folders
- **'Forensically Clean' Wiping with BCWipe**
  Unique strength to wipe selected files
  + data remanence beyond forensic recovery

Central management is available for Enterprise-class efficiency and control of all utilities.

MAIN FEATURES

Physical Threats Protection
Protect sensitive information on stolen computers and lost devices.

Virtual Threat Protection
Protect information on active, shared computers and network storages.

Secure Erasure
Securely erase all traces of unwanted files beyond forensic recovery.

Single Installation & Access
All-in-one access to BCWipe, BestCrypt Volume and Container Encryption.

Central Management
Remotely manage all encryption and wiping operations.

BENEFITS & ADVANTAGES

- Peace of mind for privacy
- Compliance with regulations
- Ongoing data protection
- Ransomware protection
- No backdoors

TECHNICAL SPECIFICATIONS

Whole Disk Encryption

- Encrypt every sector, including entire OS
- Encrypt all types of volumes residing on fixed and removable disks

Good Start, but...
With pre-boot authentication, BestCrypt Volume Encryption keeps your data safe while your computer is turned off. But once the 'front gate' is open and intruders can get inside, Volume Encryption (or any full disk encryption utility) is no longer protecting your private data.

Files & Folders Encryption

- Securely store files in encrypted, password protected containers on active computers
- Create and manage multiple containers
- Access encrypted files via virtual drives

Good Progress, but...
While files stored in encrypted containers are safely tucked away from intruders, recoverable traces may still exist out in the open. Hence, a good 'cleaner' is needed to remove the mess.

Files + Data Remanence Wiping

- Wipe files, folders, and compressed files
- Wipe Data Remanence, including free space, file slack space, swap files, MFT records, directory entries, NTFS log files and directory slack space
- Wipe browser history

DEPLOYMENT OPTIONS

Standalone Endpoints

Install, activate and manage BestCrypt Suite on standalone endpoints.
Best for smaller teams.

Central Management

Deploy and manage BestCrypt Suite from a central console.
Remotely set policies and manage user access control. Remotely recover encrypted data in case of emergency.
Wipe files remotely without end-user intervention and keep
track of all wiping activities with extensive log files and reports.
Best for larger teams.

NEED TO WIPE ENTIRE HARD DRIVES?

Use **BCWipe Total WipeOut** to securely erase hard drives at end of life:

- Decommission
- Dispose
- Sell
- Donate

www.jetico.com/bcwipe-total-wipeout

TOP SECURITY ORGANIZATIONS TRUST JETICO

Jetico

+358 50 339 6388 (EU)

202 742 2901 (US)

sales@jetico.com