# Casper Secure™ Tech Edition

## Quick and Easy Disk Cloning and Imaging for the IT Professional

Casper Secure Tech Edition is the only disk imaging and cloning solution engineered specifically for IT technicians needing to upgrade, replace, back up, restore and re-image drives and hardware RAID arrays encrypted with Windows® BitLocker® or Symantec (PGP®) Drive Encryption.

Only Casper Secure keeps all data in its original encrypted state before, during, and after the disk imaging process, ensuring 100% compliance with data security directives.


## Benefits

### Only Drive Cloning and Imaging Solution Designed Specifically for Full Drive Encryption

- Casper Secure Tech Edition produces a fully encrypted copy of an encrypted drive in its original encrypted state without ever putting data at risk.
- Saves hours of valuable time by completely eliminating the arduous and lengthy decryption and re-encryption steps required with other drive imaging and cloning solutions.

### 100% Compliance with Existing Security Directives

- Casper Secure Tech Edition completely eliminates the security and compliance risks associated with other drive imaging and cloning software which clone, image and/or restore only unencrypted copies of a full drive encrypted drive.
- With Casper Secure, data is never placed in an unprotected state, ensuring 100% compliance with enterprise-wide security directives and HIPAA requirements.

### Rapid Backup, Re-imaging and Recovery

- Casper Secure eliminates the need to separately decrypt a drive prior to imaging or cloning, which means backups can be captured in a single step and safely stored in their original encrypted state.
- Casper Secure also eliminates the laborious data restoration and re-encryption steps required by other drive cloning and imaging solutions. A Casper Secure backup can be used as an immediate and permanent replacement for a failed drive, restored directly in its original encrypted state to a new drive, or used to quickly re-image an existing drive in its original encrypted state.

### Fast and Easy Drive Upgrades and Replacements

- Casper Secure makes it extraordinarily fast and easy to safely and securely replace an encrypted system drive with a larger drive or with a faster solid state drive.
- Casper Secure quickly duplicates an encrypted drive to another drive or restores an image to a new drive without requiring a separate and time consuming backup and restore and/or re-encrypt process.
- Automatic partition resizing and alignment ensure available space is maximized automatically when upgrading to larger capacity drives and optimum performance when migrating to solid state drives.

### Unparalleled Safety and Dependability

- Exclusive AccuClone™ and Automatic Copy Verification™ technologies bring dependability to a new level by automatically verifying the integrity of the image during the drive cloning and drive imaging processes.
- Engineered from the ground up to work with Windows BitLocker and Symantec (PGP) drive encryption technolgoies.

### Saves Time

- Upgrading an encrypted system drive to a larger or faster drive can be done in 1-2 hours rather than the 10 or more hours that other imaging solutions require.
- Re-imaging a system disk from a Casper Secure image file can be done in less than an hour rather than the customary 10 or more hours when using a different imaging solution.

Future Systems™ SOLUTIONS

# Casper Secure Tech Edition Data Sheet

## TECHNICAL HIGHLIGHTS

- Creates a complete image of an encrypted Windows system drive or hardware RAID array that maintains the original encryption of the drive or hardware RAID array.
- Produces a fully bootable copy of an encrypted Windows system drive or hardware RAID array that can boot and run directly from an external USB drive.[1] A bootable backup can also be used as a permanent replacement for the original encrypted drive.
- Creates a complete disk image file backup[2] of an encrypted drive or hardware RAID array that can be stored virtually anywhere, including on a network attached storage device or on a drive containing other data.
- Runs directly from within the Windows environment or from a bootable USB flash drive or CD/DVD.
- Easy-to-use wizards for copying, imaging, creating and removing encrypted and unencrypted drives.
- SmartStart™ wizard greatly simplifies the process of replacing a Windows system disk.
- SmartRelease™ technology automatically prepares a portable backup drive for safe release after a backup has been completed.
- Supports copying of larger drives to smaller drives.
- Copies an entire hard drive or selected partitions and volumes.
- Copies multi-boot Windows configurations.[3]
- Resizes partitions during cloning or image restoration for one-step migration to either larger or smaller drives.
- Automatic Copy Verification™ ensures copies are not corrupted by defective RAM, cables, disks, or controller interfaces.
- AccuClone™ technology ensures a true copy in shortest possible time with all encrypted data in its original encrypted state.
- SmartWrite™ technology ensures maximum performance and full use of computer while performing a backup within Windows.
- SmartAlert™ can send an email notification when a copy has been completed or when special attention is required.
- Advanced Power Management support automatically suspends, hibernates, or powers-off the computer when finished.
- Customizable startup environment created on a USB flash drive or CD/DVD provides options to add additional storage and network drivers, custom drivers, custom network settings, and more.
- Advanced disk management supports creating and removing encrypted and unencrypted partitions, changing the active partition, changing a drive letter assignment, replacing damaged or missing boot records on encrypted and unencrypted partitions, and more.
- Automatically detects and supports solid state and Advanced Format drives to ensure optimized alignment and performance.
- Supports all drives including SATA, mSATA, eSATA, ATA/IDE, SCSI, USB, Firewire, and hardware RAID arrays.

## SYSTEM REQUIREMENTS

- Supports all 32-bit and 64-bit editions of Windows® 10, Windows 8.1, Windows 8, Windows 7, Windows Vista®, Windows XP, Windows Server 2016, Windows Server 2012 and 2012 R2, Windows Server 2008 and 2008 R2, Windows Server 2003 and 2003 R2, Windows 2000 Professional, Windows ME, Windows 98SE, Windows 98, and Windows 95[4]
- Windows BitLocker Drive Encryption[5], Symantec Endpoint Encryption (SEE), Symantec Encryption Desktop (SED) version 10.x, or PGP Desktop version 9.6x or later[6]
- 10 GB available space for installation and Startup Disk creation
- 2 GB RAM (4 GB or more recommended)
- Windows 10 Assessment and Deployment Kit (ADK), Windows 8.x Assessment and Deployment Kit (ADK), or Windows 7 Automated Installation Kit (AIK)
- Internet connection for license activation and periodic license verification[7]

Future Systems™ SOLUTIONS

1) Booting from a USB hard drive requires a computer with BIOS/UEFI firmware support for booting from USB hard disk drive type (USB-HDD) devices. Not all computers support booting and running from USB hard disk drive type devices.
2) Virtual disk image file backups are supported only when running on Windows 7 and later or when booting and running from the Casper Tech Edition Startup Disk. The VHDX image file format is supported only when running on Windows 8 and later or when booting and running from a Casper Tech Edition Startup Disk created with the Windows 8.x ADK or later.
3) Multi-boot configurations, Windows 2000 and Windows ME/9x systems supported only when booting and running from the Casper Tech Edition Startup Disk.
4) Not designed for use with Windows NT or Windows Server for Itanium-Based Systems.
5) Windows BitLocker Drive Encryption is currently supported only for drives using software encryption that have been formatted with the NTFS file system. BitLocker hardware encrypted drives and BitLocker encrypted drives that are formatted with the FAT file system can be copied only in their unencrypted state.
6) Encrypted cloning and imaging is currently supported only for drives encrypted with software-based drive encryption. Self-encrypting drives (SED), including Opal compliant and Windows BitLocker eDrive compliant drives, may be copied in their encrypted state only when software encrypted.
7) Alternative licensing options available for secured runtime environments lacking Internet access. Contact Enterprise Sales for more information.



Revision 01709201