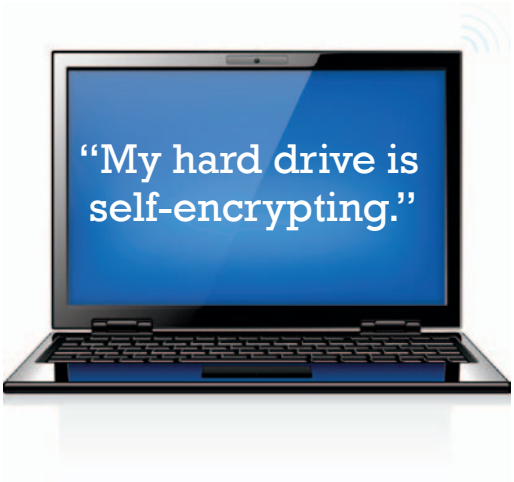
Absolute Secure Drive

PRODUCT DATASHEET

Asset Administration

Data & Device Security



Manage

Configure OPAL SEDs and manage authentication mechanisms including single-sign-on options.

Protect

Remote encryption key erase for cryptographic data wipe drive decommissioning or at PC end of life.

Recover

Easily restore credentials if the system crashes or an authentication device fails.

Many organizations rely on encryption to protect their sensitive corporate data. If a device containing company information is compromised, encryption is relied upon to protect the organization from data breaches and the negative publicity and impact to reputation that will follow.

But most encryption solutions present their own set of challenges:

- Traditional software applications are expensive
- Computer performance can be negatively impacted
- Management of encryption keys is a manual process, that consumes significant IT resources

Even if you get everything right, there is one point of failure beyond your control...the end user. If the user fails to store the documents in the appropriate volume or if they do not safeguard their encryption key, then encryption will provide you with no protection at all.

To combat this reality, computer manufacturers are building self-encrypting drives (SEDs) into their devices, providing a standardized, hardware-based method of encryption that will ship with the computer.

Self-Encrypting Drives & OPAL Specifications

SEDs that are built into new computers comply with the OPAL specifications – an industry standard released in early 2009 by the Trusted Computing Group. By encrypting the drive itself, rather than other components of the PC, the content of an OPAL SED is always encrypted, including the encryption keys.

Fig 1. *Computer manufacturers are building SEDs into new computers that comply with the OPAL specifications*

Absolute Secure Drive

With encryption built into computers, it is imperative that the organization take immediate control to ensure the encrypted hard drive (and the data it contains) is not compromised.

Absolute® Secure Drive supports the new OPAL SEDs, placing control of this encryption technology in the hands of the organization. IT Administrators can easily configure and set up OPAL SEDs on each computer. Then they can administer users, authentication methods, policies, and system maintenance through to end-of-life, all from a central administration console and much more cost effectively than traditional software-based encryption solutions.

Absolute®
SECURE DRIVE

Absolute Secure Drive

PRODUCT DATASHEET

Configuration & Management

Since the SED is built into the computer, it's important that your organization owns and controls the encrypted drive before anyone else can take control of it. With Absolute Secure Drive, IT Administrators can:

- Set up and configure OPAL SEDs using strong authentication with Windows login
- Easily deploy through integration with existing Active Directory/ADA M, and Novell eDirectory environments
- Configure SED security features accessible by multiple users and groups of users per OPAL specifications
- Manage multiple authentication devices and mechanisms to unlock the hard disk at pre-boot with SSO options
- Recover credentials in case the system crashes or if the authentication device malfunctions
- Decommission SEDs including at PC end-of-life with disk drive and data erase

Absolute Secure Drive supports S3 (sleep) mode resume without blue screening or crashing. Plus it includes a standard plug-in for the Microsoft Management Console.

Authentication & Access

IT Administrators can unlock OPAL SEDs with the pre-boot authentication module that runs in under 3 seconds from the secure Master Boot Record shadow area. Strong authentication mechanisms are supported (Windows passwords and fingerprint scanning) providing single sign-on capabilities so that users will no longer have to re-authenticate at GINA/CredProv login. IT Administrators can also perform emergency login and recovery as needed.

Linux-based pre-boot authentication means that Absolute Secure Drive is flexible and scalable. Other solutions do not support open source and are limited to text-based log-in with little customization.

Absolute Secure Drive includes a central administrative console where IT can easily configure and manage SEDs and users. Your organization will benefit from a significant reduction in the time IT spends on configuration, maintenance, and encryption key management.

Computrace Persistence

Absolute Secure Drive leverages Computrace BIOS persistence by allowing the Computrace Agent to self-heal onto the encrypted hard drive in the event that the asset is lost or stolen.

Absolute Software

Absolute Software specializes in software and services for the management and security of computers and mobile devices.

Computrace technology for endpoint security allows our customers to centrally track and secure their IT assets within a single cloud-based console. Capabilities include Asset Administration, Data & Device Security, Geotechnology, Theft Recovery, and a Service Guarantee.

Absolute Manage for endpoint management allows our customers to manage PC, Mac®, and iOS devices (iPhone®, iPod touch®, and iPad™). Capabilities include Application & License Management, Security, Change & Configuration Management, Automated Patch Management, Computer Imaging, Asset Inventory, and Power Management.

For more information about Absolute Software and our products visit www.absolute.com/products

Absolute®
SECURE DRIVE

"One of the primary benefits of SEDs is that the encryption is transparent once the drive is unlocked. The drive behaves normally and all transactions appear in clear text at the interface, which means that no operating system modifications or RAID management changes are required, except for unlocking at power-on. There is also no impact to system or drive performance, since all data is encrypted on the fly as it is written to the disk and decrypted as it is read from the disk, and this performance is scalable because each SED is responsible for its own encryption."

John Monroe
Gartner
July 13, 2010

www.absolute.com

System Requirements

- Windows® 7™ Ultimate, Home Premium, Professional (32 & 64-bit)
- Windows® Vista™ SP2 Ultimate, Home Basic, Home Premium, Business (32 & 64-bit)
- Windows® XP® Home SP2 (32-bit) & Professional SP2 (32 & 64-bit)
- Server
  - Windows server 2003, Windows server 2003 R2 (32 & 64-bit)
  - Windows server 2008, Windows server 2008 R2 (32 & 64-bit)
- Internet Explorer 6.0, or above
- At least 60 MB available hard disk space

OPAL hard drives from these vendors are supported:

- Hitachi
- Seagate (including Seagate Drive Trust)
- Toshiba
- Fujitsu-Toshiba
- Micron