Product Brief

Self-Encrypting Drive Management for Lenovo

Enhanced Functionality for your Lenovo SEDs

- Intelligent Key Management
- Integrated Authentication Control
- OS-agnostic protection

The Case for **Self-Encrypting Drive** Management

Increasingly, IT managers are turning to self-encrypting drives (SEDs) as the most effective and cost-efficient way of protecting their company, its users, and data from the constant threat of a breach.

SEDs perform the encryption and decryption operations on the hardware itself, and offer a number of benefits over traditional software-based full disk encryption (FDE) technologies, such as eliminating the issues around performance and authentication inherent with some FDE solutions. Regardless of the additional protection offered by SEDs, it is still important for enterprises to consider deploying an SED management solution to manage them.

Common Attacks against SEDs

And, how to Protect Against Them

There has been an amazing effort over the past number of years to improve the security of SEDs. However, SEDs still have a critical shortcoming. Most notably, they are not designed to protect against data access after the storage device has been unlocked using a valid authentication credential. Once the data/media encryption key has been made available to the cryptographic engine to transparently encrypt and decrypt the data, the level of protection of the data is solely reliant on the operating environment. This protection is significantly weaker than a properly implemented encryption scheme.

Benefits Offered by SEDs

Smooth Integration

SEDs are typically purchased as a feature in new platforms from Lenovo. Once imaged as part of deployment, are readily available for use.

Assured Compliance

SEDs aboard Lenovo devices support the Opal specification of the Trusted Computing Group's Storage Working Group.

Better Performance

SEDs have integrated encryption hardware, resulting in minimal latency or performance impacts.

Stronger Security

SED security is independent of the OS, so software attacks on the OS, BIOS, etc. are not effective. SEDs are less vulnerable to alternative boot attacks like Evil Maid attack; or system memory attacks.

Increased Transparency

SEDs operate at the hardware level, making their encryption and authentication functions completely transparent to the system software, including the operating system.

Integrated Authentication

Encryption keys are generated in the SED controller, and they never leave the drive. To unlock the drive, the SED requires users to enter credentials at pre-boot. Authentication cannot be separated from the drive and is performed by the protected pre-boot OS only.

Four common attacks against SEDs that expose this weakness:

1. **The Hot Plug Attack –** attackers install a SATA data and power extension cable while the machine is in Sleep mode.
2. **The Forced Restart Attack –** attackers trigger a soft-reset and boot from an alternative OS on a USB memory stick.
3. **The Hot Unplug Attack –** attack exposed SATA data and power pins.
4. **The Key Capture Attack –** While in Sleep Mode (S3), attackers replace the SED with a tampered drive with custom firmware or sniff the SATA bus to get the password.

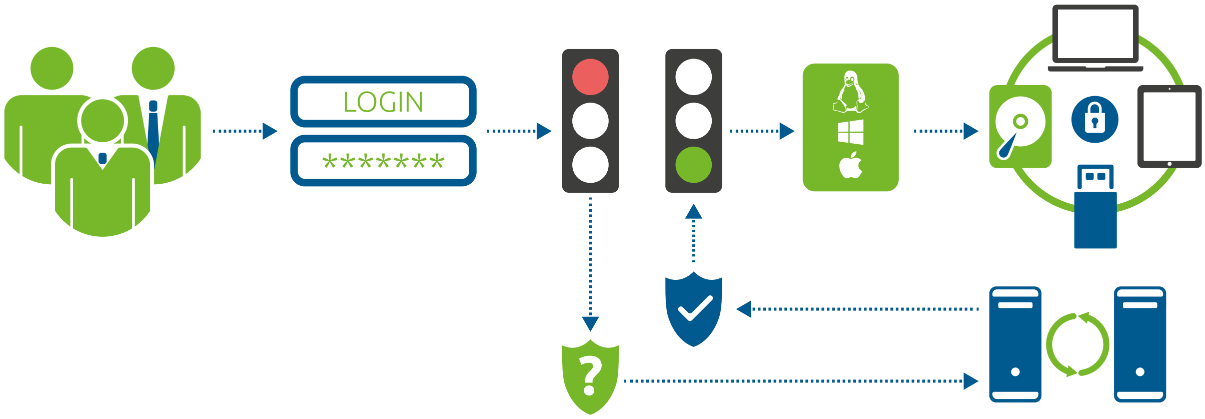
Encryption of any form doesn't provide confidentially without strong authentication, and management of it.

Encryption of any form doesn't provide confidentially without strong authentication, and management of it. That's why it is important to have a solution in place that can provide more robust authentication of users, and ensure that your data is safe from harm.

WinMagic, a Lenovo integrated partner, provides application-aware intelligent key management for everything encryption, with robust, manageable, and easy-to-use data security solutions.

SecureDoc, WinMagic's comprehensive and sophisticated encryption solution, manages data security across the enterprise - and is trusted by thousands of enterprises and government organizations worldwide. SecureDoc is the industry's leading full-disk encryption solution fully supporting Opal compliant SED's, and offers the broadest support for Trusted Computing Group (TCG) Opal and Enterprise compliant self-encrypting drives.

Check out WinMagic's SED Compatibility Certification Program



How it works

Automatic Deployment

When installing SecureDoc, the software will automatically recognize a supported SED, and can then make use of the hardware encryption.

Intelligent Key Management

SecureDoc Enterprise Server (SES) collects encryption key information from the self-encrypted drive, and provides the same central control, escrow, and protection that is used for SEDs.

Encryption is performed in dedicated drive hardware, offloading the encryption process from the computers CPU, and eliminating the need to store the encryption keys in the computer's memory.

Hardware encryption support is available on OPAL compliant SEDs with SecureDoc client installed on Windows, macOS, Linux and another other currently available operating systems.

Enhanced Functionality

SecureDoc adds much-needed authentication and enterprise manageability to SED's, making them highly secure and stable.

SecureDoc's unique features include:

- Policy & user control
- Password recovery/helpdesk capability
- Multi-factor authentication
- Port control
- Removable media encryption
- File/folder encryption
- Crypto erase

Additionally, the overall SecureDoc architecture has standard certificate support for PKCS#11, key labeling functionality and supports S3 sleep mode. The leveraged full feature design acts as an enhanced level of security over and above Opal.

The WinMagic Difference

User & Device based authentication

Utilizes wired and wireless pre-boot network authentication to enforce access controls and manage end point devices before the operating system loads.

Reduces the total cost of IT ownership: Cuts password reset time by 75% and PC staging time by 75%.

Cross-Enterprise, Multiplatform

Easy to use in multi-platform environments, supporting Windows, Mac and Linux.

Synchronizes user credentials across hardware platforms and device types. Should a password change on one device platform, SecureDoc's password propagation feature will apply that change to other devices.

Control of Keys in the Cloud

Keys to sensitive data are controlled by the enterprise, not the cloud service provider.

SecureDoc's CloudSync employs this mindset to ensure that if credentials to the cloud were ever hacked, your customer's data would be unreadable to the would-be attacker.

BitLocker Management

SecureDoc manages BitLocker with the benefits of lower IT costs and increased IT efficiency.

MBAM is a Windows only management solution. SecureDoc is platform agnostic, and capable of managing Windows, macOS, Linux and any other current available operating systems.