RAID Adapters 101: A Guide to Passive SED on Adaptec® Storage Adapters

New passive SED support for SAS and SATA devices is now available for Smart Storage adapters to protect data in use and at rest.

The importance of data security is rapidly increasing as the threat of cyber-attacks are becoming more common in data centers and the cloud computing industry. Data encryption is now a security requirement for the healthcare, finance and insurance industries with government mandates for security and privacy regarding data at rest.

Microchip's Adaptec® storage adapters offer two encryption capabilities. The first is Controller-Based Encrypton (CBE) and the second is Self-Encrypting Drive (SED) support. Controller-Based Encrypton (CBE) is a comprehensive encryption solution offered on most Adaptec RAID adapters, but we now also offer SED if your current system is not compatible with an Adaptec® maxCrypto™ CBE-enabled adapter or you need an HBA encryption solution. Our passive SED support for SAS and SATA devices is now available in most SmartRAID 3100 and SmartHBA 2100 models (in HBA Mode) and HBA 1100 models with Firmware version 4.11 and higher and will be available in most SmartRAID 3200 and SmartHBA 2200 models (in HBA Mode) and HBA 1200 models in the first quarter of calendar year 2022.

What Is a Self-Encrypting Drive?

A Self-Encrypting Drive (SED), is a hardware-based encryption method for HDDs and SSDs that automatically encrypts and decrypts the data independent of external encryption processors or operating systems. SEDs provide data at rest protection and alleviate cryptographic processing from the host CPU for little to no impact on latency and I/O performance.

How Does a Self-Encrypting Drive Work?

The encryption process is done using a unique and random Data Encryption Key (DEK) which the drive uses to both encrypt and decrypt the data. Whenever data is written to the drive, it first gets encrypted according to the DEK. Similarly, whenever

data is read from the drive, it first gets decrypted by the same DEK before being sent to the rest of the system. This hardware-based encryption provides additional security from cyberattacks because the key cannot be accessed from a software-level attack. The DEK is additionally useful because it can be managed by the user if it has become compromised and needs to be updated, or the data needs to be securely erased in which case the DEK can be deleted. In addition to the DEK, an Authentication Key, or AK, needs to be configured to ensure data at rest protection. This AK will lock the SED's encrypted data when the drives are powered off, preventing access to the drive data if they were stolen or accessed internally.

Passive SED on Adaptec adapters provides the Trusted Computing Group Security Protocol (TCG) needed to communicate and access the full feature set of any SED device. In Passive SED the adapter supports Level 0 discovery header to identify if it is a SED device, if the TCG security protocol is Enterprise or Opal and if the device is locked or unlocked. When the SED device is connected to a HBA or RAID adapter it is communicating to the operating system as an SCSI target only. It is not recommended to use SEDs in RAID volumes. Once connected, the OS uses a 3rd party utility to communicate using TCG security protocol with the SED via the physical SCSI passthrough interface of the Adaptec controller. Adaptec's Passive SED base code supports SAS and SATA interface versions of the TCG Security Protocol.

What Are the Benefits of an SED?

When considering purchasing a SED, consider the benefits below:

- SEDs have a negligible impact on performance speed and latency. The encryption process is completely integrated, so there is no need for other system components to step in and perform any heavy lifting.
- Besides CBE adapters, SEDs are one of the strongest security tools money can buy. They are independent of the operating system, so even if a hacker attacks a computer, it is nearly impossible to access the SED (and the encryption keys stored within) when the computer is turned off.
- Using an SED is simple- once paired with a 3rd party Encryption Key Management software. The software optimizes the SED's decryption and encryption functions, and the key management, relieving the user of any active SED management.
- SEDs are inexpensive to deploy and maintain. SEDs encrypt the moment they come off the assembly line. Management software does the rest, ensuring

that SEDs do their job without the need for human intervention, which saves time and money.

Conclusion

If an Adaptec maxCrypto™ CBE controller is not an option, but you are still looking to implement a strong protection against cyber-attacks on your business and/or customer data, SEDs are a great way to do so. Using SEDs isolates security data from software level attacks and minimizes human error in the security protocol. For more information about how the Adaptec storage adapters work with SEDs, please visit ask.adaptec.com.

Additional Resources

Learn more about our high-performance Adaptec® SmartRAID RAID Adapters and Adaptec® Host Bus Adapters (HBAs)

Contact Microchip's world-class Apps Engineering Support Team: https://ask.adaptec.com/app/ask

Search our knowledge base: https://ask.adaptec.com/app/home

Lisette Brown, Jan 7, 2022