The Pro and Cons of Opal Compliant Drives

Securing data-at-rest using hardware self-encrypting drives (SED) is becoming a popular option to keep information where it belongs. Data at rest is the term used for data in computer storage, such as files stored on a local hard drive, copies of the files store onsite and offsite on servers or backup drives. Contrarily, in flight data or data in motion is the term used to describe data as it is in transit. It is the process of the transferring of the data, such as date on the internet or data exiting the network via email, web, or other protocols.

Full-disk encryption (FDE) used to be a software-only proprietary solution. However, over the past couple of years, a hardware based hard drive standard has emerged in the form of Opal Security Subsystem Class, also known as Opal.

Developed by the Trusted Computing Group (TCG), a not-for-profit international standards organization, Opal is used for applying hardware-based encryption to hard drives (rotating media), solid state drives, and optical drives.

Hardware encryption has many advantages. For starters, it works with any OS. It also transfers the computational load of the encryption process to dedicated processors, cutting the stress on the host system's CPU. In addition, because the encryption/decryption keys are stored in the hard drive controller and never sit in the system's memory, cold-boot attacks don't work.

Many independent software vendors provide management of self-encrypting drives, both locally and remotely. Such vendors include Absolute Software, CryptoMill, McAfee, Secude, Softex, Sophos, Symantec, Wave Systems and WinMagic.

The primary driver for encrypting data at rest is compliance. As for types of data that are normally encrypted, studies show that the top three types are financial documents, employee records, and customer data.

The main reason to encrypt data-at-rest is to comply with state or federal data protection laws said 51 percent of the IT practitioners surveyed. The remaining 49 percent cited their organizations' need to comply with self-regulatory programs such as PCI DSS, ISO, NIST and others.

Here's a look at some pros and cons of SEDs:

Pro No. 1: Hardware based encryption is more secure than software based offerings since it cannot be corrupted or negated while software can. Hardware based security can more effectively restrict access from the outside, especially to unauthorized use. Additionally, dedicated hardware can have superior performance compared to software.

Pro No. 2: Hardware encryption does not have negative impact on the performance of systems. In fact, dedicated hardware can always out-perform software running on a general purpose OS-based platform.

Con No. 1: Management can be difficult since integrated management solutions are necessary to support Opal compliant drives.

Con No. 2: SEDs are not designed to protect data in flight. Since SEDs are focused on data at rest, in flight data will require an alternative solution.

Popular and successful techniques include transport layer security (TLS) and its predecessor secure sockets layer (SSL), cryptographic protocols.

To comply with Opal standards, all Advantech 2.5" & mSATA SQFlash product lines offer the option to support AES-256 encryption. The security controller which generates an AES (Advanced Encryption Standard) key is embedded in the drive and offers real-time data encryption before storing data into NAND flash. The data is fully hashed with the encryption key so in the event that the controller or firmware fails, the data stored in the NAND flash cannot be accessed.

Along with the encryption capabilities, SQFlash drives with AES also support another function called Flash Lock. This mechanism is used to lock the SQFlash module with a specific motherboard by enabling the drive to match a unique identifier in the BIOS of the motherboard. When this occurs, the SQFlash drive can only operate with the specific corresponding platform. This helps prevent data from being read or taken when SQFlash drive is connected to other computers or card readers. Due to the identifier Flash Lock requires a special version of BIOS.

To learn more, please contact your Advantech account manager or iot.inquiry.usa@advantech.com for details.