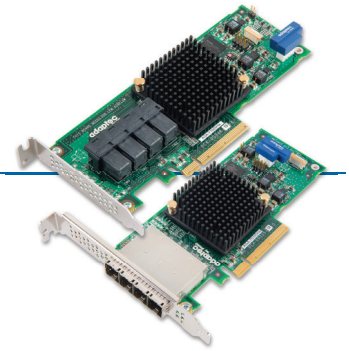
adaptec by PMC

maxCrypto TECHNICAL BRIEF

maxCrypto

Adaptec maxCrypto: Superior On-The-Fly Data Encryption at Line-Rate Speeds



Introduction

Data security has become one of the highest priorities for data centers and cloud computing environments as enterprises seek to safeguard customer information, classified company documentation and communications, financial records, employee payroll records, and other confidential data.

Data center managers face the challenge of safeguarding data while still meeting continually-increasing performance demands for large-scale applications such as web serving, file serving, databases, online transaction processing (OLTP), Microsoft Exchange Server, and high performance computing (HPC).

Threats to data security

Security efforts have traditionally focused on safeguarding data from Internet-based threats, but data centers can no longer ignore physical security threats presented by several common scenarios.

Storage drive disposal

When a storage device is retired, the data needs to be rendered inaccessible to dumpster-diving thieves. There are two ways to do this.

The first, data wiping, is a method of writing garbage data to the entire drive, thereby overwriting the useful data. The data being overwritten is typically a series of zeros, or various random patterns. Depending on the size and speed of the storage device, this process can take several hours. If an entire server is being retired, it can take days to wipe data from all of the connected drives. Additionally, different types of storage devices such as hard disk drives (HDDs) and solid state drives (SSDs) may require different tools and different methods of data wiping.

The second is to physically demolish the device with a hammer, shredder, or other tool of destruction. This can also be a time-consuming process and, if a thorough job is not done, can leave behind salvageable components that savvy thieves could glean data from.

Returning failed drives

Sensitive data should be removed from a storage device if the device has failed and needs to be returned to the vendor for replacement. This brings up the same challenges as the disposal scenario with the added twist of how to wipe data from a non-functioning device.

Theft

Firewalls and other network security tools do an admirable job of keeping data safe from hackers, but the threat of physical theft (an unauthorized person stealing a storage drive) remains.

An ideal solution for each situation above would be to manipulate the data on the drive itself, so that even if it were to be examined by somebody not authorized to view the data, the data would be unreadable or otherwise useless.

Data encryption

Encryption is a method of encoding information so that it can only be read by authorized parties. The information is scrambled using an encryption key and is unreadable to anybody who does not have the decryption key. There are two types of encryption: symmetric and asymmetric.

In symmetric cryptography, the same key is used for both encryption and decryption. If the key is compromised, the security is broken. Therefore, management of the encryption keys in this model is a critical and complex process.

Asymmetric cryptography uses one key for encryption and another for decryption. The encryption key can be made public through software implementation while the decryption key remains private in the hardware. This model provides a higher level of security than symmetrical cryptography.

Highlights

- **Adaptec maxCrypto data encryption for HDDs and SSDs**
- **Available on 6Gb/s Adaptec Series 7He family of HBAs**
  - One HBA encrypts multiple drives, reducing capital expenses and deployment complexity
  - Compatible with existing data center infrastructure and all brands of SAS and SATA HDDs and SSDs
  - Allows data centers to deploy uniform, scalable strategy across entire enterprise
- **On-the-fly hardware-based encryption**
  - Line-rate speeds with minimal impact on latency
  - Does not require key management software
  - Encryption key independent of the OS, eliminating threats from viruses and other attacks
- **Superior cryptography and functionality**
  - Industry-leading Infineon SLE95050 encryption device
  - 256-bit AES encryption
  - Advanced elliptic curve cryptography (ECC) logarithm
  - Asymmetric key authentication
- **Maintains disk data size and data structures**
  - No negative impact on usable disk capacity or on maintenance technologies

Adaptec maxCrypto: Superior On-The-Fly Data Encryption at Line-Rate Speeds

The encryption process can be software-based or hardware-based. While the CPU is responsible for powering software-based encryption, hardware-based encryption is a standalone chipset that can be located on the drive itself or on the Host Bus Adapter (HBA).

Software-based encryption

Software-based encryption is managed by the operating system, using an application to encrypt and decrypt data as it is read from or written to the drives.

Advantages of software-based encryption

- Usually the most affordable option for data encryption
- Software applications are available for the major operating systems and work with most brands of HDDs and SSDs

Disadvantages of software-based encryption

- Since the encryption/decryption processes take place at the CPU level, storage systems experience added latency
- The OS that is running the software encryption is vulnerable to viruses, crashes and other threats

Hardware-based Self-Encrypting Drive (SED)

On a self-encrypted SSD or HDD, the encryption/decryption process takes place independent of the CPU and OS through the use of a chipset that includes an encryption/decryption key.

Advantages of SEDs

- The encryption key is independent of the OS, eliminating threats from viruses and other attacks
- Dedicated hardware performs the encryption process and does not cause a noticeable impact on latency or I/O performance

Disadvantages of SEDs

- New SEDs must be purchased (usually at a higher cost than non-SEDs) and deployed
- Securing entire system requires replacing all existing HDDs and SSDs with SEDs
- Limited options currently available from HDD and SSD vendors
- Current data must be transferred from existing non-encrypted drives to new SEDs
- Managing multiple SEDs requires an integrated key management software solution
- Some SEDs contain a nonremovable key, leaving data vulnerable if the drive is disposed of or returned to the vendor

Hardware-based encryption-enabled HBAs

As in the SED scenario, encryption-enabled HBAs have an onboard chipset that performs the encryption/decryption process.

Advantages of encryption-enabled HBAs

- The encryption key is independent of the OS, eliminating threats from viruses and other attacks
- Dedicated hardware performs the encryption process and does not cause a noticeable impact on latency or I/O performance
- Compatible with a data center's existing infrastructure and all brands of HDDs and SSDs, eliminating the need to replace current drives with one vendor's SEDs
- One HBA can encrypt many drives, reducing capital expenses (CapEx) and deployment complexity
- HBAs typically have a longer lifespan than HDDs and SSDs and do not need to be replaced as often, further reducing CapEx
- Does not require integrated key management software

Disadvantages of encryption-enabled HBAs:

- Requires replacement of existing HBAs with encryption-enabled HBAs
- Enabling encryption erases a drive. If it is desirable to retain existing data on a drive, a backup must be performed before enabling encryption.

Adaptec maxCrypto

Available on 6Gb/s Adaptec Series 7He family of Host Bus Adapters (HBAs), Adaptec maxCrypto hardware encryption delivers the highest levels of on-the-fly data encryption/decryption at line-rate speeds with minimal impact on latency.

Adaptec maxCrypto features an industry-leading Infineon SLE95050 encryption device using an advanced elliptic curve cryptography (ECC) logarithm and asymmetric key authentication for superior cryptography and functionality. It does not require key management software, which allows data centers to deploy a uniform, scalable encryption strategy across the enterprise.

Since maxCrypto is HBA-based, it is compatible with existing storage infrastructures and eliminates the need for new HDDs or SSDs. The Adaptec 7He, however, does not encrypt data on tape or other non-direct access devices. The HBA will support tape if the encryption key is removed. Also, multi-lun support for RBOD is not yet available, but encryption will work on lun0 of an RBOD and all other direct access devices.

Adaptec maxCrypto does not change the size of a disk's data, nor does it change data structures, so there is no negative impact on usable disk capacity or on maintenance technologies such as dedupe.

Adaptec maxCrypto encryption key use-cases

Each maxCrypto key is manufactured with a unique encryption key. Adaptec 7He HBAs are equipped with a clip-in socket similar to the one used in cell phones for media storage.

Adaptec maxCrypto: Superior On-The-Fly Data Encryption at Line-Rate Speeds

The act of physically inserting or detecting the key into the slot triggers the encryption. All attached drives share the same encryption state — either they are all encrypted or none of them is. The HBA BIOS indicates whether encryption is enabled or disabled so encryption status can be confirmed without physically inspecting the HBA to verify that the key is installed.

The table below illustrates the results of inserting, removing, and replacing the maxCrypto key in various scenarios.

Since the data on maxCrypto-encrypted HDDs and SSDs is useless without the key, maxCrypto addresses the physical security threats mentioned earlier in this paper: a retired drive can be disposed of without a lengthy data-wiping process, and a failed drive can be returned to the manufacturer without fear of the data being compromised. Even if a drive is stolen, the thief will only gain a piece of hardware — not the valuable data stored on it.

Conclusion

Data centers face a growing responsibility to safeguard sensitive data such as customer identities, company communications, and financial records. They must look beyond Internet-based threats and also consider physical security risks to their HDDs and SDDs.

Data can be compromised when a data center returns a failed drive to a vendor, retires a drive without undertaking a lengthy data wiping process, or leaves a drive vulnerable to thievery. By encrypting data as it is stored, a data center can ensure that unauthorized parties will not be able to read the data, even if they possess the drive on which the data is stored.

Software encryption is a cost-sensitive solution but causes performance issues and is vulnerable to viruses and OS crashes. Self-encrypting drives (SEDs) offer a high-performance hardware-based solution but require significant capital investment and management.

Locating the encryption process on the HBA offers the benefits of hardware-based encryption with a lower capital investment and easier management than SEDs.

Adaptec maxCrypto integrates hardware-based encryption with 6Gb/s Adaptec Series 7He family of Host Bus Adapters (HBAs) to deliver the highest levels of data encryption/decryption with minimal impact on latency. It integrates seamlessly into existing storage infrastructures and allows data centers to deploy a uniform, scalable encryption strategy across the entire enterprise.

Original State	Data Encrypted?	Action	Result
HBA with no maxCrypto key	No	Insert maxCrypto key	Existing data deleted*, new data is encrypted
HBA with no maxCrypto key	No	Replace HBA with no maxCrypto key	Data not encrypted
HBA with no maxCrypto key	No	Replace HBA with maxCrypto key	Existing data deleted*, new data is encrypted
HBA with no maxCrypto key	No	Replace with 3rd Party HBA	Data not encrypted
HBA with maxCrypto key	Yes	Remove maxCrypto key	Existing data deleted*, new data not encrypted
HBA with maxCrypto key	Yes	maxCrypto key failure	Existing data deleted*, new data not encrypted
HBA with maxCrypto key	Yes	Replace key with new maxCrypto key	Existing data deleted*, new data is encrypted
HBA with maxCrypto key	Yes	Replace HBA with existing maxCrypto key	Data remains intact and encrypted
HBA with maxCrypto key	Yes	Replace HBA with maxCrypto key	Existing data deleted*, new data is encrypted
HBA with maxCrypto key	Yes	Replace with 3rd-party HBA	Existing data deleted*, new data not encrypted

** After user confirmation*

adaptec by PMC

PMC-Sierra, Inc.
1380 Bordeaux Dr.
Sunnyvale, CA 94089 USA
Tel: +1 (408) 239-8000

World Wide Web: www.adaptec.com
Pre-Sales Support: **US and Canada:** 1 (800) 442-7274 or (408) 957-7274 or adaptecsales@pmcs.com
UK: +44 1276 854 528 or uk_sales@pmcs.com
Australia: +61-2-90116787
Germany: +49-89-45640621 or adaptecsales.germany@pmcs.com
Singapore: +65-92351044

TB_maxCrypto_071013_US Information subject to change.