Technical Brief

Microsemi Adaptec SmartStorage maxCrypto: Superior Data-at-Rest Encryption

July 2018

Microsemi

a Microchip company

Contents

Revision History

The revision history describes the changes that were implemented in the document. The changes are listed by revision, starting with the most current publication.

Revision 1.0

Revision 1.0 of this document was published in July 2018. This was the first publication.

Introduction

Data security has become one of the highest priorities for data centers and cloud computing environments as they seek to safeguard customer information, classified company documentation and communications, financial records, employee payroll records, and other confidential data. Solutions for data-at-rest encryption are now a security requirement in many market segments such as health care, finance, e-commerce, federal government branches, and insurance—representing a significant overall percentage of the deployed storage. In fact, government legislation is now in place mandating data security and privacy, such as the Health Insurance Portability and Accountability Act, Gramm–Leach–Bliley Act, Sarbanes–Oxley Act, and the European Union General Data Protection Regulation.

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), machine learning, and high-performance computing (HPC).

Threats to Data Security

McAfee estimated that the cost of cybercrime and data breaches was $600 billion in 2017 alone. Security policies need to safeguard data from both Internet-based threats and physical threats to data at rest.

Unauthorized Access or Theft

Firewalls and other network security tools do an admirable job of keeping data safe from hackers, but the threat of unauthorized access or physical theft remains.

Storage Drive Disposal

Whenever a storage device is removed from the data center—whether it is being returned to the vendor for replacement, resold, or recycled—the data it contains must be protected from unauthorized access.

Data wiping is one option for securing the drive outside of the data center, either with block writes or instant secure erase. Encryption techniques are another protection method—these are discussed in detail in the following section.

In cases where security is of the utmost importance, customers may choose to shred the device in addition to data wiping and encryption.

Data Encryption

Encryption is a method of encoding information so that it can only be read by using the proper key. The encryption process can be software-based or hardware-based. While the CPU is responsible for powering software-based encryption, hardware-based encryption is performed within a chip located on the drive itself or on the storage adapter.

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 using the host CPU.

Advantages of Software-Based Encryption

- Software applications are available for the major operating systems and work with all brands of HDDs and SSDs
- Can offer many advanced features such as data-in-place encryption and re-key support

Disadvantages of Software-Based Encryption

- Storage systems may experience added latency and I/O performance degradation
- Lacks a common implementation between versions of operating system (for example, Windows /Linux)
- Degrades the performance of other applications running on the main CPU

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, using a chip on the drive utilizing a symmetric key securely generated and stored on the device.

Advantages of SEDs

- Dedicated cryptographic hardware, yielding little to no impact to latency or I/O performance
- Transparent to the host operating system and host CPU
- Independent of the storage adapter in use

Disadvantages of SEDs

- Drives that support encryption must be purchased and deployed, requiring additional inventory complexity and possibly additional cost
- Securing existing storage infrastructure requires replacing all existing HDDs and SSDs with SEDs
- Current data must be transferred from existing non-encrypted drives to new SEDs (that is, there is no support for data-in place encryption)
- Datapath between the host operating system and the SED is in plaintext, allowing opportunities for data snooping

Hardware-Based Encryption-Enabled Storage Adapters

On an encryption-enabled storage adapter, the encryption/decryption process takes place independent of the CPU and OS, using a chip on the adapter instead of the drive.

Advantages of Encryption-Enabled Storage Adapters

- Dedicated cryptographic hardware, yielding little to no impact on latency or I/O performance
- Transparent to the host operating system and host CPU
- One adapter encrypts multiple drives, reducing capital expenses and deployment complexity
- Compatible with all brands of SAS and SATA HDDs and SSDs where a RAID volume is supported, spanning one or multiple drives
- Allows data centers to deploy a uniform, scalable encryption strategy across the entire enterprise
- Data is encrypted on the storage subsystem, avoiding data snooping on the adapter cache, attached cables, or expanders, all the way to the media of the drive
- Allows for selective encryption enablement and unique encryption keys per logical volume
- Support for data-in-place encryption while the volume remains accessible during the encryption process

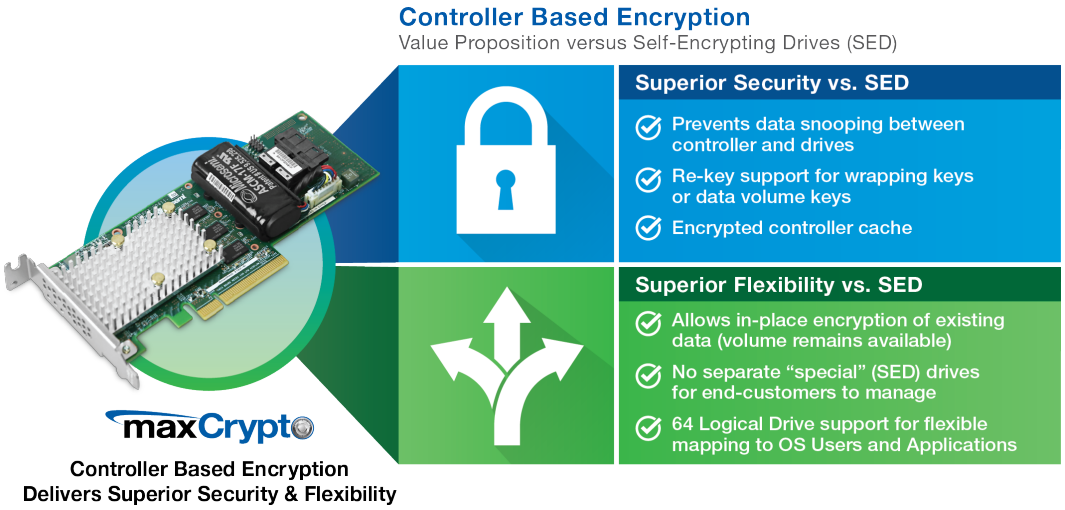
Disadvantages of Encryption-Enabled Storage Adapters

- Requires purchasing an encryption-enabled storage adapter
- Requires the use of a RAID volume to store data as currently implemented by Smart Storage

Adaptec Smart Storage maxCrypto

Available on the SmartRAID 3162-8i/e version of the Smart Storage series of storage adapters, maxCrypto hardware encryption delivers data protection with little to no impact on latency or I/O performance. Leveraging the SmartROC 3100 RAID-on-Chip (RoC) controller, the Smart Storage maxCrypto solution allows data centers to deploy a uniform, scalable encryption strategy across the enterprise.

maxCrypto Highlights



Controller Based Encryption
Delivers Superior Security & Flexibility

Highlights

- Adaptec maxCrypto data encryption for HDDs and SSDs when configured for a RAID volume for data storage
- Available on the SmartRAID 3162-8i/e
  - Efficient—one adapter encrypts multiple drives, reducing capital expenses and deployment complexity
  - Flexible—compatible with all brands of SAS and SATA HDDs and SSDs, and can be enabled on any type of RAID volume
  - Uniform security policy—allows data centers to deploy a single, scalable encryption strategy across the entire enterprise
  - Highly secure—encrypted data path from the adapter to the drive media
  - Multi-tenant security—unique encryption keys per logical volume
  - Line-rate speeds with minimal impact on latency or performance
  - Does not require separate key management software
- Superior cryptography
  - 256-bit XTS-AES encryption
  - Tweak value per LBA (encryption key is altered per LBA making the encryption very difficult to break)
  - Disk capacity remains unaltered

Enabling maxCrypto

Enabling maxCrypto encryption for one or more logical volumes attached to the adapter is easy Using the security administrative role of maxCrypto, the encryption functionality is enabled by entering a master passphrase. Logical volumes can then be created with encryption enabled or disabled utilizing the Smart Storage management tools. Per the security policy of the data center, the same master key passphrase can be used for all adapters in the data center or, alternatively, unique passphrases may be used. Migrating encrypted drives from one adapter to another is as easy as re-entering the matching master passphrase in the replacement adapter.

Once enabled, the encrypted data is inaccessible without the matching master passphrase and a maxCrypto-enabled adapter. Because it operates automatically (in the background), maxCrypto does not interfere with day-to-day storage operations such as drive replacement and logical drive creation or common tasks associated with storage administration.

Conclusion

Data centers face a growing responsibility to safeguard sensitive data such as customer identities, company communications, and financial records. Data-at-rest on drive media is open to compromise when appropriate safeguards are not observed. By encrypting data-at-rest, a data center can ensure that unauthorized parties will not be able to read the data when drives are removed (either intentionally or unintentionally).

Software encryption comes at the expense of valuable CPU resources. Self-encrypting drives offer a high-performance hardware-based solution but require significant operational overhead and do not provide the security and flexibility of controller-based encryption.

maxCrypto hardware-based encryption is available on the SmartRAID 3162-8i/e and delivers the highest levels of data protection 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 data center.

Ordering Information

SmartRAID 3100 Series	Part Number	Raid Levels	Host Interface	SAS /SATA Ports	Cache	Cache Width	Cache Backup	maxCrypto
SmartRAID-3162-8i/e	2299600-R	0, 1 ,5, 6, 10, 50, 60, 1 ADM, 10 ADM	8-Lane PCIe Gen 3	8 internal	2 GB DDR4/ 2100 MHz	64-bit	Yes, onboard	Yes, controller-based encryption

Microsemi Headquarters
One Enterprise, Aliso Viejo,
CA 92656 USA
Within the USA: +1 (800) 713-4113
Outside the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996
Email: sales.support@microsemi.com
www.microsemi.com

Microsemi, a wholly owned subsidiary of Microchip Technology Inc. (Nasdaq: MCHP), offers a comprehensive portfolio of semiconductor and system solutions for aerospace & defense, communications, data center and industrial markets. Products include high-performance and radiation-hardened analog mixed-signal integrated circuits, FPGAs, SoCs and ASICs; power management products; timing and synchronization devices and precise time solutions, setting the world's standard for time; voice processing devices; RF solutions; discrete components; enterprise storage and communication solutions; security technologies and scalable anti-tamper products; Ethernet solutions; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Microsemi is headquartered in Aliso Viejo, California, and has approximately 4,800 employees globally. Learn more at www microsemi.com.

ESC-2181400