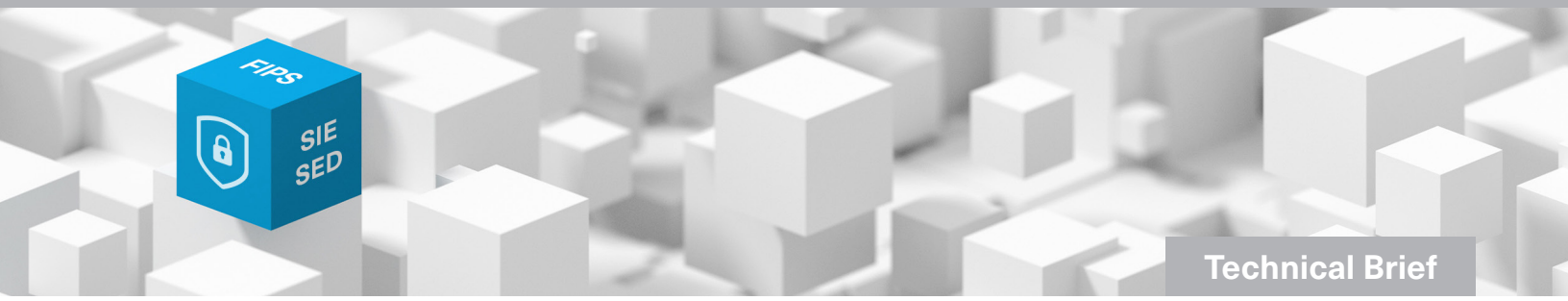
KIOXIA



Technical Brief

Data Security in Enterprise and Data Center SSDs

Understanding the Value of Drive Encryption and the Available Options

Data security within a data center includes the mechanisms, processes and tools that are put in place by an organization to protect themselves from the unwanted activities of unauthorized users and hackers, such as cyberattacks and data breaches. Despite being a very important facet of a company's IT operation, data security may not always get the full attention it requires, mostly because it can be expensive and difficult to deploy, requires ongoing management and maintenance, and can burden system performance. However, an organization that does not have a data security plan in place can suffer costly consequences if it is attacked or breached.

From a data storage perspective, there are a few efficient and powerful security options designed into enterprise and data center storage drives to help prevent against data loss and theft. Understanding these options and how drive encryption is used to protect data is the focus of this tech brief.

Data Breaches

The intentional or unintentional access of secure, private and/or confidential information to an untrusted environment is regarded as a data breach[1] and can potentially cost companies millions of dollars[2] to resolve[3], impact millions of individuals and damage consumer trust. These results can cost an organization significantly more than the cost of security equipment, deployment and support. Since there is not one security measure on its own that can mitigate data breaches, companies need to take a multifaceted approach, including at the drive level where encrypted SSDs are key to this support.

Encrypted SSDs include Sanitize Instant Erase[4] (SIE) drives, Self-Encrypting Drives[5] (SEDs) and Federal Information Processing Standard (FIPS)-certified drives. These security options are available from KIOXIA for enterprise and data center requirements and include the CM6 Series PCIe® 4.0 enterprise NVMe® SSDs, PM6 Series 24G enterprise SAS-4 SSDs and CD6 Series PCIe 4.0 data center NVMe SSDs.

As security vulnerabilities can occur from a variety of circumstances, a lost or stolen drive is as vulnerable as well. Earlier in 2021, a European cloud infrastructure and Platform-as-a-Service provider had one of its SSDs stolen from the back of an unlocked truck while in transit[6]. The SSD was sold online and it contained some unencrypted customer data, including source code and Secure Shell (SSH) keys of an Italian Virtual Private Service (VPS) provider. After the purchaser tracked down the drive's owner, the drive was returned safely and no data was further exposed. This example had a happy ending, and recovering the SSD helped authorities in their investigation. However, the end result could have been significantly worse. Lost or stolen devices increased the average data breach cost in 2020 by an average of $192,455[2].

SSD Security Options

Encryption is the key capability featured in the three SSD security options (SIE drives, SEDs and FIPS-certified drives) which rely on a Media Encryption Key (MEK) as part of the encryption/decryption processes. Encryption occurs on all user data sent to the AES[7]-256 cryptographic module within the drive, enabling data to be encrypted and stored on the drive. Performing encryption on the drive itself reduces the probability of unauthorized users being able to steal the MEK and decrypt the data.

When encryption is performed, the act does not change the probability of the key being stolen as the ability to compromise a key is a function of password strength. An added benefit to using KIOXIA encryption-enabled SSDs is that no performance loss occurs to the system that the drive resides in. While the three security options have encryption capabilities, there are some differences in how they work and protect data.

SIE Drives

SSDs with this security option use encryption to make data unreadable when they are erased and taken out of commission or repurposed. Data is automatically encrypted when written to an SSD, and then decrypted when sent to the host. The encryption does not require host management. When an SSD is to be decommissioned or repurposed, IT personnel/user can issue a Sanitize command, rendering the data unreadable in less than a second.

The SSD uses the MEK and the AES 256-bit cryptographic module to encrypt the data as it is written, and just the MEK to decrypt data as it is read. When a 'Secure Erase' or 'Sanitize' command is issued, the MEK is deleted and a new one is made. Since the previous MEK was used to encrypt the data on the drive, there is no way now to decrypt the data, and the data is considered inaccessible.

Encrypted data within an SSD is not protected from unauthorized users being able to access the data-at-rest. This is due to the host having no involvement, management or access to the MEK because it is internally generated, stored, discarded and refreshed by the SSD itself. Therefore, a higher level of security is required and provided by SEDs.

Self-Encrypting Drives

Similar to an SIE drive, an SED uses the MEK to encrypt data within the drive itself. User data is sent to the drive, which uses an AES-256 cryptographic module to encrypt data and store it securely. However, an SED provides an additional layer of protection requiring an authentication step before the drive can be accessed. Encryption/decryption requires a password-protected alphanumeric key. Once accessed, data written to and retrieved from the SSD is continuously encrypted/decrypted, protecting user data.

Host-side authentication can be used by assigning an Authentication Key (AK) to each authorized user. This key is required to lock/unlock access to the user's drive data prior to being processed through the AES cryptographic module. This process requires security commands as defined by the Trusted Command Group[8] (TCG) which dictate the management, activation and provisioning of user data. The specifications include data structures and mechanisms for managing and configuring the authentication credentials and access controls.

For SAS SSDs (KIOXIA PM6 Series), the command set is TCG-Enterprise
For NVMe® SSDs (KIOXIA CM6 / CD6 Series), the command set is TCG Opal

SEDs are designed for most applications and regulations that require data-at-rest to be encrypted. Without the password-protected alphanumeric key employed, and SED behaves like an SIE drive.

FIPS-Certified Drives

The last security option is FIPS 140-2, or the Federal Information Processing Standard 140 publication series 2, developed by the National Institute of Standards and Technology (NIST). It is the standard which specifies 'Security Requirements for Cryptographic Modules.'

IMPORTANT NOTES:

1. The last date to submit for FIPS 140-2 certification is September 22, 2021. After that date, no additional FIPS 140-2 submissions will be allowed and vendors must submit for FIPS 140-3 certification instead. NIST will complete all of the FIPS 140-2 submissions in the queue.

2. A FIPS 140-2 certified product does not need to be resubmitted for FIPS 140-3 certification as the FIPS 140-2 certificate is valid for 5 years. However, all FIPS 140-2 certificates will be retired on September 22, 2026. Vendors should resubmit for FIPS 140-3 certification before that date.

The certification process is rigorous and tests the security of the SSD's cryptographic module through NIST's Cryptographic Module Validation Program[9] (CMVP). The tests are conducted by a third party NIST-accredited lab. There are four levels[10] of the FIPS 140-2 standard - Level 1 is low-level software security – Level 4 is high-level security that includes secure key management, tamper proof seals, etc.

To achieve FIPS 140-2 certification (or FIPS 140-3 certification), the SSD must undergo a review and validation of a number of items: (1) the cryptographic module specification and documentation; (2) the key management responsibilities including generation, entry, output, storage and destruction of the keys; (3) the cryptographic module implementation, design assurance and mitigation. Storage providers typically work with the NIST-accredited lab which independently tests SSD cryptographic modules and who submit the results and proper documentation to NIST for review.

Once NIST has reviewed the validation data and documentation, and the drive proves to be in compliance to the standard, it would be certified as FIPS 140-2 Level 2 compliant. The certification means that the cryptographic modules for this series of drives have been validated by the CMVP. This process can be lengthy and a good reason why FIPS-certified drives are difficult to find when a new SSD is launched by a storage provider.

SIE Drives	Self-Encrypting Drives	FIPS 140-2-Certified Drives
Enables Cryptographic Erase to quickly facilitate making data unreadable when an SSD is taken out of commission or repurposed.	*Encrypts/decrypts data written to and retrieved from an SSD via a password-protected alphanumeric key, (continuously encrypting and decrypting the data).*	*Validates that an SSD's cryptographic module is in compliance with the FIPS 140-2 standard developed by NIST through its rigorous CMVP certification process.*

Security Option Disclaimers

Though deploying enterprise and data center drives with security options is a great added step to protect data-at-rest, it is important for users to set their respective authentication keys. Having a strong password or passphrase is critical as that is the primary mechanism used to unlock the MEK. Setting AKs mean if a drive finds its way out of the data center and into unauthorized user hands, the data on the drive is useless as the AES-256 cryptographic module is nearly impossible to break.

In a server with several SEDs, it could be difficult to keep track of individual AKs unless a key manager is used. Some server providers make individual AK tracking easy by providing comprehensive security key management options that are paired with hardware-based integration which takes the guesswork and confusion out of SED deployment when protecting data-at-rest.

The security options supported within a drive can vary by storage provider, intended industry and the specific product category itself and may not be available in all countries due to export and local regulations. **Even more important**, security on a drive ***does not*** guarantee that a breach will be prevented especially if there are failures in security protocols. However, taking a multi-level security approach, including at the drive level where encrypted SSDs are key, can only happen if the storage provider offers drives with security options.

Security Benefits at the System/Application Level

SIE drives, SEDs and FIPS-certified drives provide different capabilities to combat data theft and loss, and carry their own respective advantages;

- *SIE drives provide the benefit of fast and secure erase*
- *SEDs provide the benefit of a password-protected authentication key for enhanced security*
- *FIPS 140-2-certified drives provide assurances that cryptographic modules meet the specifications established by the United States government*

The three classes of security options available within KIOXIA SSDs encrypt all of the data that is sent to and received from the drive using secure onboard crypto-processors that have no performance impact to host systems. SSDs with these levels of security offer advanced data protection for organizations.

KIOXIA SSD Security Options

SSD security options are available for KIOXIA'S CM6 Series, PM6 Series and CD6 Series SSDs and support these key product specifications:

CM6 Series SSDs

PCIe 4.0 and NVMe 1.4 Specification Compliant

High-Performance

SeqRead = up to 6,900 MB/s
RanRead = up to 1.4M IOPS
SeqWrite = up to 4,200 MB/s
RanWrite = up to 350K IOPS

Endurance and Capacities

1 and 3 DWPD options
800 GB - 30,720 GB capacities

PM6 Series SSDs

24G SAS, SAS-4 Specification Compliant

High-Performance

SeqRead = up to 4,150 MB/s
RanRead = up to 595K IOPS
SeqWrite = up to 3,700 MB/s
RanWrite = up to 466K IOPS

Endurance and Capacities

1, 3 and 10 DWPD options
400 GB – 30,720 GB capacities

CD6 Series SSDs

PCIe 4.0 and NVMe 1.4 Specification Compliant

High-Performance

SeqRead = up to 6,200 MB/s
RanRead = up to 1.0M IOPS
SeqWrite = up to 4,000 MB/s
RanWrite = up to 250K IOPS

Endurance and Capacities

1 and 3 DWPD options
800 GB – 15,360 GB capacities

Summary

An organization that does not properly secure its data-at-rest can experience data breaches that can be very expensive to resolve and can adversely affect customer confidence and trust. Built within KIOXIA enterprise and data center SSDs is encryption support of user data that protects data-at-rest in cases of unauthorized access and includes SIE drives, SEDs and FIPS-certified drives. Each has their own capabilities and advantages to combat data theft and loss.

NOTES:

[1] In 2020, there were 3,950 reported data breaches. Source: Verizon, '2021 Data Breach Investigations Report (DBIR),' https://www.verizon.com/business/resources/reports/dbir/

[2] The average cost of each data breach reported in 2020 was approximately $3.86 million. Source: IBM - 'The Cost of a Data Breach Report 2020,' https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

[3] One of the most expensive data breaches recorded cost more than $500 million. Source: Federal Trade Commission (FTC) – 'Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach,' July 2019, https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related

[4] Sanitize Instant Erase (SIE) drives are compatible with the Sanitize device feature set, which is the standard prescribed by NVM Express, Inc. first introduced in the NVMe v1.3 specification, and improved in the NVMe v1.4 specification, and by the T10 (SAS) and T13 (SATA) committees of the American National Standards Institute (ANSI).

[5] In support of the SED (TCG-Opal/Ruby) security option, there are a limited number of features that are not supported.

[6] Source: The Register – 'SSD belonging to Euro-Cloud Scaleway was stolen from back of a truck, then turned up on YouTube,' Simon Sharwood author, published July 27, 2021, https://www.theregister.com/2021/07/27/stolen_scaleway_ssd_recovered/

[7] The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology in 2001.

[8] The Trusted Computing Group (TCG) is a not-for-profit international standards organization that applies hardware-based encryption to solid state drives.

[9] More information on the NIST Cryptographic Module Validation Program is available at: https://csrc.nist.gov/projects/cryptographic-module-validation-program

[10] More information on the NIST Cryptographic Security Requirements is available at: https://csrc.nist.gov/publications/detail/fips/140/2/final

TRADEMARKS:

DISCLAIMERS: