ThinkSystem CM5-R Entry NVMe PCIe 3.0 x4 SED SSDs

Product Guide

The ThinkSystem CM5-R Entry NVMe solid-state drives (SSDs) are high-performance self-encrypting drives (SEDs) that adhere to the Trusted Computing Group Opal Security Subsystem Class cryptographic standard (TCG Opal SSC). They use Kioxia (formerly Toshiba) NAND flash memory technology with a PCIe 3.0 x4 NVMe interface to provide an high-performance solution for secure read-intensive workloads.

The ThinkSystem CM5-R Entry NVMe solid-state drives is shown in the following figure.

Figure 1. ThinkSystem CM5-R Entry NVMe PCIe 3.0 x4 SED SSD

Did you know?

Self-encrypting drives (SEDs) provide benefits by encrypting data on-the-fly at the drive level with no performance impact, by providing instant secure erasure thereby making the data no longer readable, and by enabling auto-locking to secure active data if a drive is misplaced or stolen from a system while in use. These features are essential for many businesses, especially those storing customer data.

NVMe (Non-Volatile Memory Express) is a technology that overcomes SAS/SATA SSD performance limitations by optimizing hardware and software to take full advantage of flash technology. The use of NVMe drives means data is transferred more efficiently from the processor to the drives compared to the legacy Advance Host Controller Interface (AHCI) stack, thereby reducing latency and overhead. These SSDs connect directly to the processor via the PCIe bus, further reducing latency and TCO.

Part number information

The following table lists the ThinkSystem part numbers.

Table 1. ThinkSystem ordering information

Part number	Feature	Description
4XB7A14060	B6K4	ThinkSystem U.2 CM5-R 3.84TB Entry NVMe PCIe 3.0 x4 Hot Swap SSD SED

The benefits of drive encryption

Self-encrypting drives (SEDs) provide benefits in three main ways:

- By encrypting data on-the-fly at the drive level with no performance impact
- By providing instant secure erasure (cryptographic erasure, thereby making the data no longer readable)
- By enabling auto-locking to secure active data if a drive is misplaced or stolen from a system while in use

The following sections describe the benefits in more details.

Automatic encryption

It is vital that a company keep its data secure. With the threat of data loss due to physical theft or improper inventory practices, it is important that the data be encrypted. However, challenges with performance, scalability, and complexity have led IT departments to push back against security policies that require the use of encryption. In addition, encryption has been viewed as risky by those unfamiliar with key management, a process for ensuring a company can always decrypt its own data. Self-encrypting drives comprehensively resolve these issues, making encryption both easy and affordable.

When the self-encrypting drive is in normal use, its owner need not maintain authentication keys (otherwise known as credentials or passwords) in order to access the data on the drive. The self-encrypting drive will encrypt data being written to the drive and decrypt data being read from it, all without requiring an authentication key from the owner.

Drive retirement and disposal

When hard drives are retired and moved outside the physically protected data center into the hands of others, the data on those drives is put at significant risk. IT departments retire drives for a variety of reasons, including:

- Returning drives for warranty, repair, or expired lease agreements
- Removal and disposal of drives
- Repurposing drives for other storage duties

Nearly all drives eventually leave the data center and their owner's control. Corporate data resides on such drives, and when most leave the data center, the data they contain is still readable. Even data that has been striped across many drives in a RAID array is vulnerable to data theft because just a typical single stripe in today’s high-capacity arrays is large enough to expose for example, hundreds of names and bank account numbers.

In an effort to avoid data breaches and the ensuing customer notifications required by data privacy laws, companies use different methods to erase the data on retired drives before they leave the premises and potentially fall into the wrong hands. Current retirement practices that are designed to make data unreadable rely on significant human involvement in the process, and are thus subject to both technical and human failure.

The drawbacks of today's drive retirement practices include the following:

- Overwriting drive data is expensive, tying up valuable system resources for days. No notification of completion is generated by the drive, and overwriting won't cover reallocated sectors, leaving that data exposed.
- Methods that include degaussing or physically shredding a drive are expensive. It is difficult to ensure the degauss strength is optimized for the drive type, potentially leaving readable data on the drive. Physically shredding the drive is environmentally hazardous, and neither practice allows the drive to be returned for warranty or expired lease.
- Some companies have concluded the only way to securely retire drives is to keep them in their control, storing them indefinitely in warehouses. But this is not truly secure because a large volume of drives coupled with human involvement inevitably leads to some drives being lost or stolen.
- Professional disposal services is an expensive option and includes the cost of reconciling the services as well as internal reports and auditing. Transporting of the drives also has the potential of putting the data at risk.

Self-encrypting drives eliminate the need to overwrite, destroy, or store retired drives. When the drive is to be retired, it can be cryptographically erased, a process that is nearly instantaneous regardless of the capacity of the drive.

Instant secure erase

The self-encrypting drive provides instant data encryption key destruction via cryptographic erasure. When it is time to retire or repurpose the drive, the owner sends a command to the drive to perform a cryptographic erasure. Cryptographic erasure simply replaces the encryption key inside the encrypted drive, making it impossible to ever decrypt the data encrypted with the deleted key.

Self-encrypting drives reduce IT operating expenses by reducing asset control challenges and disposal costs. Data security with self-encrypting drives helps ensure compliance with privacy regulations without hindering IT efficiency. So called "Safe Harbor" clauses in government regulations allow companies to not have to notify customers of occurrences of data theft if that data was encrypted and therefore unreadable.

Furthermore, self-encrypting drives simplify decommissioning and preserve hardware value for returns and repurposing by:

- Eliminating the need to overwrite or destroy the drive
- Securing warranty returns and expired lease returns
- Enabling drives to be repurposed securely

Auto-locking

Insider theft or misplacement is a growing concern for businesses of all sizes; in addition, managers of branch offices and small businesses without strong physical security face greater vulnerability to external theft. Self-encrypting drives include a feature called auto-lock mode to help secure active data against theft.

Using a self-encrypting drive when auto-lock mode is enabled simply requires securing the drive with an authentication key. When secured in this manner, the drive's data encryption key is locked whenever the drive is powered down. In other words, the moment the self-encrypting drive is switched off or unplugged, it automatically locks down the drive's data.

When the self-encrypting drive is then powered back on, it requires authentication before being able to unlock its encryption key and read any data on the drive, thus protecting against misplacement and theft.

While using self-encrypting drives just for the instant secure erase is an extremely efficient and effective means to help securely retire a drive, using self-encrypting drives in auto-lock mode provides even more advantages. From the moment the drive or system is removed from the data center (with or without authorization), the drive is locked. No advance thought or action is required from the data center administrator to protect the data. This helps prevent a breach should the drive be mishandled and helps secure the data against the threat of insider or outside theft.

Features

The ThinkSystem CM5-R Entry NVMe SED SSDs have the following features:

- Industry standard 2.5-inch form factor
- Compliant with TCG Storage Security Subsystem Class Opal Version 2.01 Revision 1
- Kioxia (formerly Toshiba) 64-layer BiCS FLASH 3D TLC memory technology
- Suitable for read-intensive workloads with an endurance of less than 1 full drive write per day (DWPD) for 5 years
- Direct PCIe 3.0 x4 connection for each NVMe drive, resulting in up to 4 GBps overall throughput.
- Advanced Encrypting Standard (AES) 256-bit encryption
- Supports Sanitize Cryptographic Erase
- Power loss protection and end-to-end data protection

SSDs have a huge but finite number of program/erase (P/E) cycles, which affect how long they can perform write operations and thus their life expectancy. Entry SSDs typically have a better cost per read IOPS ratio but lower endurance and performance compared to Mainstream and Performance SSDs. SSD write endurance is typically measured by the number of program/erase cycles that the drive can incur over its lifetime, which is listed as total bytes written (TBW) in the device specification.

The TBW value that is assigned to a solid-state device is the total bytes of written data that a drive can be guaranteed to complete. Reaching this limit does not cause the drive to immediately fail; the TBW simply denotes the maximum number of writes that can be guaranteed. A solid-state device does *not* fail upon reaching the specified TBW. However, at some point after surpassing the TBW value (and based on manufacturing variance margins), the drive reaches the end-of-life point, at which time the drive goes into read-only mode. Because of such behavior, careful planning must be done to use SSDs in the application environments to ensure that the TBW of the drive is not exceeded before the required life expectancy.

Technical specifications

The following table presents technical specifications for the ThinkSystem CM5-R Entry NVMe SSDs.

Table 2. Technical specifications

Feature	960 GB drive	1.92 TB drive	3.84 TB drive	7.68 TB drive
Kioxia model	KCM5DRUG960G	KCM5DRUG1T92	KCM5DRUG3T84	KCM5DRUG7T68
Host interface	PCIe 3.0 x4	PCIe 3.0 x4	PCIe 3.0 x4	PCIe 3.0 x4
Capacity	960 GB	1.92 TB	3.84 TB	7.68 TB
SED encryption	TCG Opal	TCG Opal	TCG Opal	TCG Opal
Endurance (total bytes written)	1752 TB	3504 TB	7008 TB	14,016 TB
Endurance (drive writes per day for 5 years)	1.0 DWPD	1.0 DWPD	1.0 DWPD	1.0 DWPD
Data reliability (UBER)	< 1 in 10^{17} bits read	< 1 in 10^{17} bits read	< 1 in 10^{17} bits read	< 1 in 10^{17} bits read
MTBF	2,500,000 hours	2,500,000 hours	2,500,000 hours	2,500,000 hours
IOPS reads (4 KB blocks)	370,000	650,000	750,000	770,000
IOPS writes (4 KB blocks)	50,000	65,000	70,000	80,000
Sequential read rate (128 KB blocks)	3100 MBps	3100 MBps	3200 MBps	3200 MBps
Sequential write rate (128 KB blocks)	1200 MBps	2350 MBps	2900 MBps	2900 MBps
Latency (random read)	110 µs	110 µs	110 µs	110 µs
Latency (random write)	30 µs	30 µs	30 µs	30 µs
Power consumption (typical)	11W	13W	15W	16W

Server support

The following tables list the ThinkSystem servers that are compatible.

Table 3. Server support (Part 1 of 2)

Part Number	Description	Edge		1S Intel V2			2S Intel V2				AMD				Dense V2				4S V2		8S
		SE350 (7Z46 / 7D1X)	SE450 (7D8T)	ST50 V2 (7D8K / 7D8J)	ST250 V2 (7D8G / 7D8F)	SR250 V2 (7D7R / 7D7Q)	ST650 V2 (7Z75 / 7Z74)	SR630 V2 (7Z70 / 7Z71)	SR650 V2 (7Z72 / 7Z73)	SR670 V2 (7Z22 / 7Z23)	SR635 (7Y98 / 7Y99)	SR655 (7Y00 / 7Z01)	SR645 (7D2Y / 7D2X)	SR665 (7D2W / 7D2V)	SD630 V2 (7D1K)	SD650 V2 (7D1M)	SD650-N V2 (7D1N)	SN550 V2 (7Z69)	SR850 V2 (7D31 / 7D32)	SR860 V2 (7Z59 / 7Z60)	SR950 (7X11 / 7X12)
4XB7A14060	ThinkSystem U.2 CM5-R 3.84TB Entry NVMe PCIe 3.0 x4 Hot Swap SSD SED	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N

Table 4. Server support (Part 2 of 2)

Part Number	Description	1S Intel V1				2S Intel V1								Dense V1				4S V1		
		ST50 (7Y48 / 7Y50)	ST250 (7Y45 / 7Y46)	SR150 (7Y54)	SR250 (7Y52 / 7Y51)	ST550 (7X09 / 7X10)	SR530 (7X07 / 7X08)	SR550 (7X03 / 7X04)	SR570 (7Y02 / 7Y03)	SR590 (7X98 / 7X99)	SR630 (7X01 / 7X02)	SR650 (7X05 / 7X06)	SR670 (7Y36 / 7Y37)	SD530 (7X21)	SD650 (7X58)	SN550 (7X16)	SN850 (7X15)	SR850 (7X18 / 7X19)	SR850P (7D2F / 2D2G)	SR860 (7X69 / 7X70)
4XB7A14060	ThinkSystem U.2 CM5-R 3.84TB Entry NVMe PCIe 3.0 x4 Hot Swap SSD SED	N	N	N	N	N	N	N	N	N	N	Y	N	Y	N	N	N	N	N	N

Storage controller support

NVMe PCIe SSDs require a NVMe drive backplane and some form of PCIe connection to processors. PCIe connections can take the form of either an adapter (PCIe Interposer or PCIe extender/switch adapter) or simply a cable that connects to an onboard NVMe connector.

IBM SKLM Key Management support

To effectively manage a large deployment of SEDs in Lenovo servers, IBM Security Key Lifecycle Manager (SKLM) offers a centralized key management solution. Certain Lenovo servers support Features on Demand (FoD) license upgrades that enable SKLM support.

The following table lists the part numbers and feature codes to enable SKLM support in the management processor of the server.

Table 5. FoD upgrades for SKLM support

Part number	Feature code	Description
Security Key Lifecycle Manager - FoD (United States, Canada, Asia Pacific, and Japan)		
00D9998	A5U1	SKLM for System x/ThinkSystem w/SEDs - FoD per Install w/1Yr S&S
00D9999	AS6C	SKLM for System x/ThinkSystem w/SEDs - FoD per Install w/3Yr S&S
Security Key Lifecycle Manager - FoD (Latin America, Europe, Middle East, and Africa)		
00FP648	A5U1	SKLM for System x/ThinkSystem w/SEDs - FoD per Install w/1Yr S&S
00FP649	AS6C	SKLM for System x/ThinkSystem w/SEDs - FoD per Install w/3Yr S&S

The IBM Security Key Lifecycle Manager software is available from Lenovo using the ordering information listed in the following table.

Table 6. IBM Security Key Lifecycle Manager licenses

Part number	Description
7S0A007FWW	IBM Security Key Lifecycle Manager Basic Edition Install License + SW Subscription & Support 12 Months
7S0A007HWW	IBM Security Key Lifecycle Manager For Raw Decimal Terabyte Storage Resource Value Unit License + SW Subscription & Support 12 Months
7S0A007KWW	IBM Security Key Lifecycle Manager For Raw Decimal Petabyte Storage Resource Value Unit License + SW Subscription & Support 12 Months
7S0A007MWW	IBM Security Key Lifecycle Manager For Usable Decimal Terabyte Storage Resource Value Unit License + SW Subscription & Support 12 Months
7S0A007PWW	IBM Security Key Lifecycle Manager For Usable Decimal Petabyte Storage Resource Value Unit License + SW Subscription & Support 12 Months

The following tables list the ThinkSystem servers that are compatible.

Table 7. IBM SKLM Key Management support (Part 1 of 2)

		Edge		1S Intel V2			2S Intel V2				AMD				Dense V2				4S V2		8S
Part Number	Description	SE350 (7Z46 / 7D1X)	SE450 (7D8T)	ST50 V2 (7D8K / 7D8J)	ST250 V2 (7D8G / 7D8F)	SR250 V2 (7D7R / 7D7Q)	ST650 V2 (7Z75 / 7Z74)	SR630 V2 (7Z70 / 7Z71)	SR650 V2 (7Z72 / 7Z73)	SR670 V2 (7Z22 / 7Z23)	SR635 (7Y98 / 7Y99)	SR655 (7Y00 / 7Z01)	SR645 (7D2Y / 7D2X)	SR665 (7D2W / 7D2V)	SD630 V2 (7D1K)	SD650 V2 (7D1M)	SD650-N V2 (7D1N)	SN550 V2 (7Z69)	SR850 V2 (7D31 / 7D32)	SR860 V2 (7Z59 / 7Z60)	SR950 (7X11 / 7X12)
A5U1	SKLM for System x w/SEDs - FoD per Install w/1Yr S&S	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	N	N	Y	Y	Y	Y
AS6C	SKLM for System x w/SEDs - FoD per Install w/3Yr S&S	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	N	N	Y	Y	Y	Y

Table 8. IBM SKLM Key Management support (Part 2 of 2)

Part Number	Description	1S Intel V1				2S Intel V1								Dense V1				4S V1		
		ST50 (7Y48 / 7Y50)	ST250 (7Y45 / 7Y46)	SR150 (7Y54)	SR250 (7Y52 / 7Y51)	ST550 (7X09 / 7X10)	SR530 (7X07 / 7X08)	SR550 (7X03 / 7X04)	SR570 (7Y02 / 7Y03)	SR590 (7X98 / 7X99)	SR630 (7X01 / 7X02)	SR650 (7X05 / 7X06)	SR670 (7Y36 / 7Y37)	SD530 (7X21)	SD650 (7X58)	SN550 (7X16)	SN850 (7X15)	SR850 (7X18 / 7X19)	SR850P (7D2F / 2D2G)	SR860 (7X69 / 7X70)
A5U1	SKLM for System x w/SEDs - FoD per Install w/1Yr S&S	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	Y	Y	Y
AS6C	SKLM for System x w/SEDs - FoD per Install w/3Yr S&S	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N	Y	Y	Y

Warranty

The ThinkSystem CM5-R Entry NVMe SED SSDs carry a one-year, customer-replaceable unit (CRU) limited warranty. When the SSDs are installed in a supported server, these drives assume the system's base warranty and any warranty upgrades.

Solid State Memory cells have an intrinsic, finite number of program/erase cycles that each cell can incur. As a result, each solid state device has a maximum amount of program/erase cycles to which it can be subjected. The warranty for Lenovo solid state drives (SSDs) is limited to drives that have not reached the maximum guaranteed number of program/erase cycles, as documented in the Official Published Specifications for the SSD product. A drive that reaches this limit may fail to operate according to its Specifications.

Physical specifications

The drives have the following physical specifications (approximate, without the tray):

- Height: 15 mm (0.6 in.)
- Width: 70 mm (2.8 in.)
- Depth: 100 mm (4.0 in.)
- Weight: 130 g (5.3 oz)

Operating environment

The SSDs are supported in the following environment:

- Operating temperature: 0 to 60°C (32 to 140°F)
- Non-operating temperature: -40 to 85°C (-40 to 185°F)
- Relative humidity: 5 to 95% (non-condensing)
- Shock, operating: 1,000 G (Max) at 0.5 ms duration
- Vibration, operating: 2.17 G_{RMS} (5-800 Hz)

Agency approvals

The SSDs conform to the following regulations:

- Underwriters Laboratories: UL60950-1
- Canada: CAN/CSA-C22.2 No.60950-1
- TUV: EN 60950-1
- BSMI (Taiwan): CNS 13438 (CISPR Pub. 22 Class B): D33003
- MSIP: KN22, KN24 (CISPR Pub. 22 Class B)
- Australia/New Zealand: AS/NZS CISPR32:2015 Class B
- Canada: ICES-003 Issue 6 Class B
- EMC: EN55022 (2010) Class B
- EMC: EN55024 (2010)
- RoHS 2011/65/EU: EN50581 (2012) Category 3

Related publications and links

For more information, see the following documents:

- Lenovo ThinkSystem storage options product web page
  https://lenovopress.com/lp0761-storage-options-for-thinksystem-servers
- Implementing NVMe Drives on Lenovo Servers
  https://lenovopress.com/lp0508-implementing-nvme-drives-on-lenovo-servers
- Toshiba CM5-R SSDs product page:
  https://business.toshiba-memory.com/en-us/product/storage-products/enterprise-ssd/cm5-r-1dwpd-series.html

Related product families

Product families related to this document are the following:

- Security Key Lifecycle Manager
- Drives

Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service. Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
8001 Development Drive
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION ”AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary. Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk. Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

This document, LP1172, was created or updated on June 5, 2021.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:
  https://lenovopress.lenovo.com/LP1172
- Send your comments in an e-mail to:
  comments@lenovopress.com

This document is available online at https://lenovopress.lenovo.com/LP1172.

Trademarks

Lenovo and the Lenovo logo are trademarks or registered trademarks of Lenovo in the United States, other countries, or both. A current list of Lenovo trademarks is available on the Web at https://www.lenovo.com/us/en/legal/copytrade/.

The following terms are trademarks of Lenovo in the United States, other countries, or both:
Lenovo®
System x®
ThinkSystem®

The following terms are trademarks of other companies:

Intel® is a trademark of Intel Corporation or its subsidiaries.

Other company, product, or service names may be trademarks or service marks of others.