

Encryption Protection without a Performance Hit with KIOXIA CM7 Series SSDs in a Dell™ PowerEdge™ R6615 Server

Introduction

Protecting sensitive business data through robust data security measures is essential for maintaining trust, compliance and operational continuity in any organization. Almost all data is protected in transit at the network layer by network encryption methods. However, data at rest is often not encrypted due to the resource constraints of the encryption and decryption processes.

Data encryption is the process of taking digital data and translating it into an unreadable format so that only users with a key can access the data if removed from the system. KIOXIA SSDs with a Self-Encrypting Drive¹ (SED) option implement on-board crypto processors and use an AES²-256 cryptographic module and encryption key to encrypt raw binary data. This process ensures data encryption at the hardware layer to prevent unauthorized access.

There is a misconception that enabling the encryption key on an SSD with the SED option will lead to a reduction in drive performance. However, as it relates to KIOXIA SSDs with the SED option, encryption is built into the drives, enabling data to flow through the encryption logic whether the encryption key is enabled or not. As a result, enabling the encryption key has no performance impact on KIOXIA SSDs with the SED option. The ability to protect data through encryption without experiencing performance degradation is the basis of this performance brief.

Dell Technologies™ offers ways to enable the encryption key for an SSD with the SED option and includes integrated Dell Remote Access Controller (iDRAC) Local Key Management (iLKM) that helps protect data if a drive is removed from a system and OpenManage™ Secure Enterprise Key Management (SEKM) that helps protect data if an entire server is taken down. Both the iLKM and SEKM provide an authentication key to the SSD with the SED option that enables access to the data on the drive.

When a KIOXIA CM7-R Series SSD with the SED option is deployed in a Dell PowerEdge R6615 server, there is no performance impact on the drive as it is always encrypted.

This performance brief presents a test comparison to demonstrate that encryption does not lead to a performance hit. Flexible I/O (fio) tests were conducted on a Dell PowerEdge R6615 server, with and without encryption enabled. The server was deployed with one 3.84 terabyte³ (TB) KIOXIA CM7-R Series PCIe® 5.0 enterprise NVMe™ SSD that supports the TCG-Opal⁴ specification for the SED option.

There were five fio workloads (100% sequential read and write, 100% random read and write, and mixed random) to record metrics for input/output operations per second (IOPS), throughput and read/write latency.

The test results show that a Dell PowerEdge R6615 server deployed with a KIOXIA CM7-R Series SSD, delivered similar IOPS, throughput and latency performance whether encryption was enabled or not. The metrics were based on three test runs of 5 minutes each and the average result was recorded. For the IOPS test, over 2.8 million IOPS was recorded for the 100% random read workload.

The test results include a description of each workload test, a graphical depiction of the test results and an analysis. Appendix A covers the hardware and software test configuration. Appendix B covers the configuration setup and test procedures.

Test Results Snapshot

One KIOXIA CM7-R Series SSD was tested, with and without encryption enabled, in a Dell PowerEdge R6615 server, with the following results:

Average IOPS

Workload	Encryption Disabled	Encryption Enabled
100% RanWrite	328,481 IOPS	327,883 IOPS
70%/30% Random	680,126 IOPS	677,485 IOPS
100% RanRead	2,873,302 IOPS	2,870,487 IOPS

Average Throughput

Workload	Encryption Disabled	Encryption Enabled
100% SeqRead	14.1 GB/s	14.3 GB/s
100% SeqWrite	7.4 GB/s	7.5 GB/s

Average Read Latency

Workload	Encryption Disabled	Encryption Enabled
100% SeqRead	0.62 ms	0.61 ms
70%/30% Random	0.80 ms	0.80 ms
100% RanRead	0.35 ms	0.35 ms

Average Write Latency

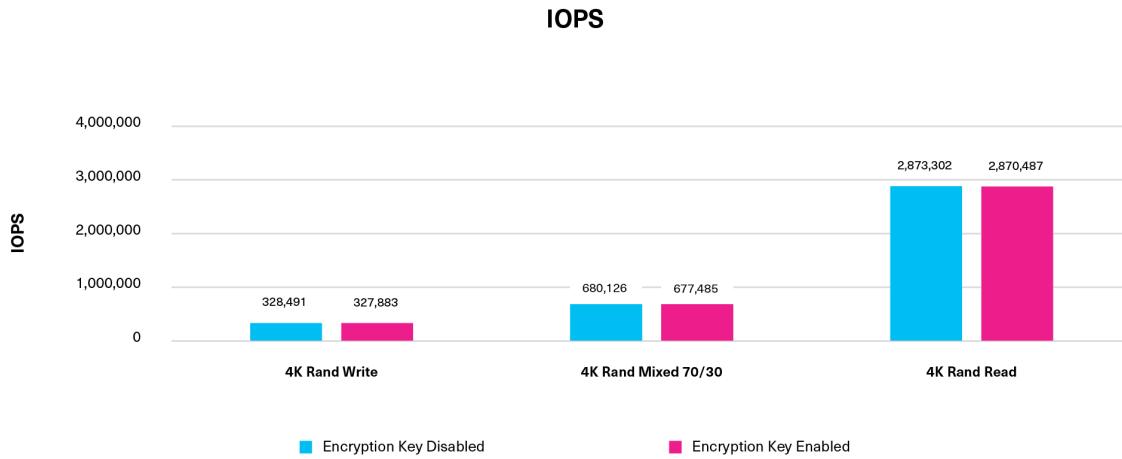
Workload	Encryption Disabled	Encryption Enabled
100% SeqRead	1.18 ms	1.17 ms
70%/30% Random	0.19 ms	0.19 ms
100% RanRead	3.15 ms	3.16 ms

Encryption without a performance hit!!!

Test Results⁵

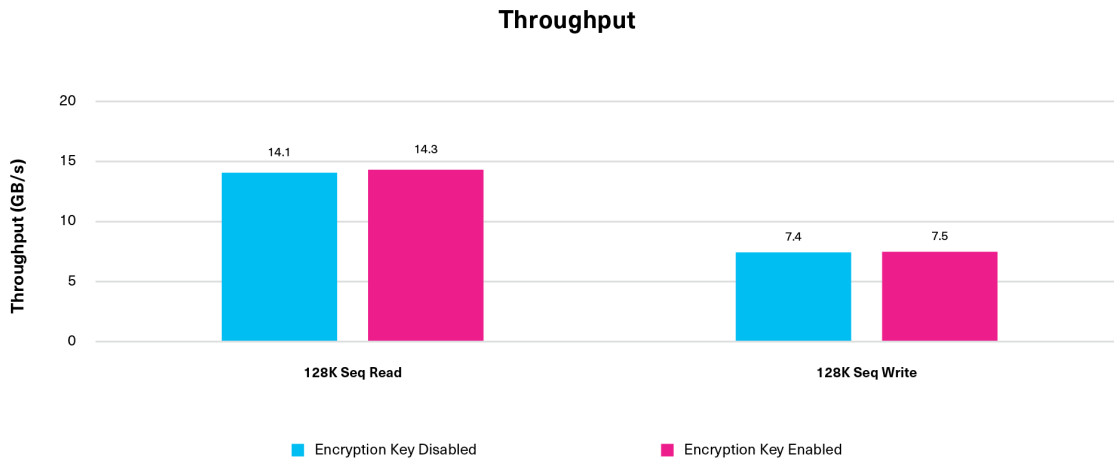
Test 1: IOPS

This test measured the number of IOPS that the KIOXIA CM7-R Series SSD and Dell™ PowerEdge™ R6615 server configuration completed and included 4K 100% random write, 4K random 70% read / 30% write and 4K 100% random read workloads. The metrics were based on three test runs of 5 minutes each and the average result was recorded. The results are in IOPS, and similar results are the objective:



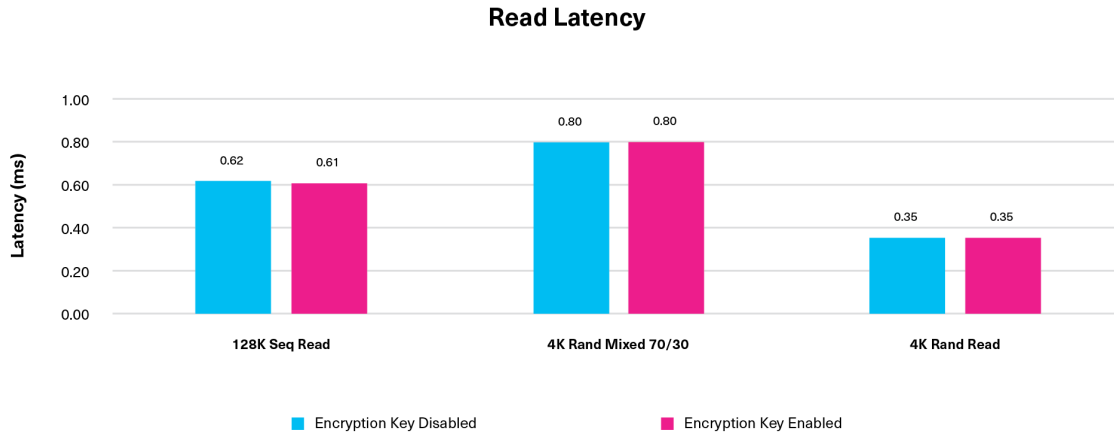
Test 2: Throughput

This test measured the amount of data transferred per second to and from the SSDs and included 128K 100% sequential read and 128K 100% sequential write workloads. The metrics were based on three test runs of 5 minutes each and the average result was recorded. The results are in gigabytes per second (GB/s), and similar results are the objective:



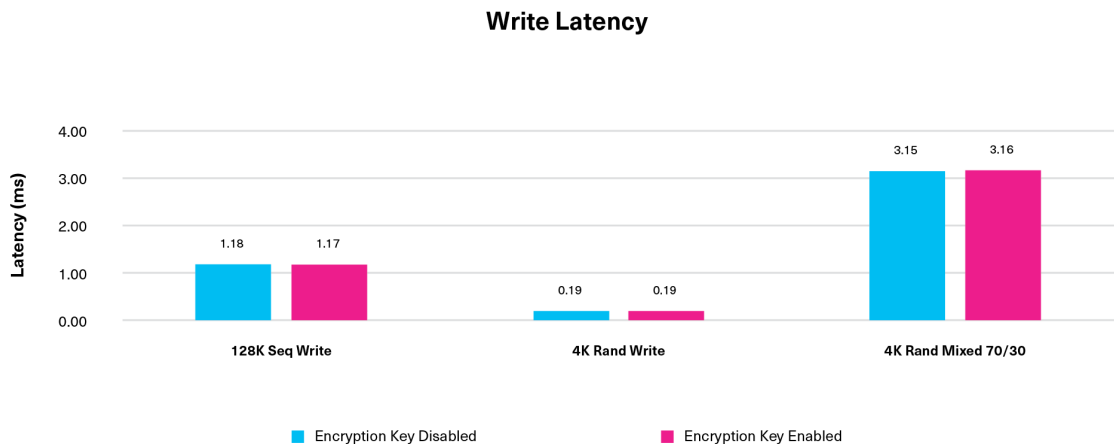
Test 3: Read Latency

This test measured the time it took to perform a read operation. It included the average time it took for fio to not only issue the read operation, but also the time it took to complete the operation and receive a 'successfully completed' acknowledgement. The workloads included 128K 100% sequential read, 4K random 70% read / 30% write and 4K 100% random read. The metrics were based on three test runs of 5 minutes each and the average result was recorded. The results are in milliseconds (ms), and similar results are the objective:



Test 4: Write Latency

This test measured the time it took to perform a write operation. It included the average time it took for fio to not only issue the write operation, but also the time it took to complete the operation and receive a 'successfully completed' acknowledgement. The workloads included 128K 100% sequential write, 4K 100% random write and 4K random 70% read / 30% write. The metrics were based on three test runs of 5 minutes each and the average result was recorded. The results are in milliseconds (ms), and similar results are the objective:



Analysis

The test results validated that a KIOXIA CM7-R Series SSD with the SED option enabled the Dell™ PowerEdge™ R6615 server to deliver similar IOPS, throughput and latency performance whether the encryption key was enabled or not. Over 2.8 million IOPS was delivered by this PCIe® 5.0/NVMe™ 2.0 server/storage configuration with the encryption key enabled and disabled. Moving the KIOXIA CM7-R Series SSD to another system while it was locked by the encryption key, provided validation that the key was working properly. Without the encryption key to unlock it, the KIOXIA CM7-R Series SSD was unable to be accessed.

Summary

Encryption in today's data centers is as important as ever for securing data from attacks and hackers but has typically degraded application and system performance. The test results demonstrated that a KIOXIA CM7-R Series SSD, with encryption built into the drive, enabled data to flow through the encryption logic unimpeded whether the encryption key was enabled or not. As a result, enabling the encryption key had no performance impact on the SSD when deployed in a Dell™ PowerEdge™ R6615 server. This solution effectively delivered similar performance whether the encryption key was enabled or disabled. Based on these tests, this server/storage solution delivered encryption protection without a performance hit.

KIOXIA CM7 Series SSD Product Info

KIOXIA CM7 Series enterprise NVMe™ SSDs support E3.S and 2.5-inch form factors and are compliant with the PCIe® 5.0 and NVMe 2.0 specifications. These SSDs are available in two configurations: KIOXIA CM7-R Series for read-intensive applications (1 DWPD⁹), up to 30.72 TB capacities) and KIOXIA CM7-V Series for higher endurance, mixed-use applications (3 DWPD, up to 12.8 TB capacities). Additional features include a dual-port design for high availability applications, flash die failure protection and security options⁷. Additional KIOXIA CM7 Series SSD information is available [here](#).



KIOXIA CM7 Series SSDs⁹

Appendix A

Hardware/Software Test Configuration

Server Information	
Model	Dell™ PowerEdge™ R6615
No. of Servers	1
CPU Information	
No. of CPU Sockets	1
CPU	AMD EPYC™ 9454P
No. of CPU Cores	48
CPU Frequency	2.75 gigahertz (GHz)
Memory Information	
Memory Type	DDR5 DRAM
Total Memory	128 gigabytes ³ (GB)
Memory Frequency	DDR5-4800
SSD Information	
Model	KIOXIA CM7-R Series
Interface	PCIe® 5.0 x4
Protocol	NVMe™ 2.0
No. of Drives	1
Form Factor	E3.S
Capacity	3.84 TB
DWPD	1 (5 years)
Power Consumption	25 W
Operating System Information	
Operating System	Ubuntu®
OS Version	24.04
Test Software Information	
Test Software	fio
Version	3.41

Appendix B

Configuration Setup/Test Procedures

Configuration Setup

One Dell™ PowerEdge™ R6615 server was set up with an Ubuntu® 24.04.3 LTS operating system.

One 3.84 TB KIOXIA CM7-R Series SSD in an E3.S form factor with the SED option was installed into the server.

fiio v3.41 test software was installed onto the server.

Test Procedures

fiio tests were run with the encryption key disabled for IOPS, throughput and read/write latency:

- *Up to five workloads were used and included:*
 - 128k 100% sequential read
 - 128k 100% sequential write
 - 4k 100% random read
 - 4k 100% random write
 - 4k random 70% read/30% write
- *Each workload was tested three times in 5-minute durations to determine an average result.*

To run fiio tests with the encryption key enabled, iLKM needs to be enabled and the secure drive option needs to be selected by following these steps:

- *To enable the iLKM log into the iDRAC, go to iDRAC Settings, Services, iDRAC Key Management and enable iLKM.*
- *To enable the encryption key for the KIOXIA CM7-R Series SSD:*
 - Connect to the iDRAC
 - Go to iDRAC Settings, select Services, and then select iDRAC Key Management
 - In iDRAC Key Management, enable iLKM
 - Go back to iDRAC Settings, select Storage, and then select Physical Disks
 - Select 'action' on the drive to enable the encryption key
 - Select Secure Drive

Once the iDRAC Key Management Settings were made, the fiio tests were then run with the encryption key enabled for IOPS, throughput and read/write latency:

- *The same workloads and testing process when the encryption key was disabled were used.*

The results of the IOPS, throughput and read/write tests were recorded and compared to the results when encryption was disabled.

NOTES:

¹ Self-Encrypting Drives (SEDs) encrypt all data to SSDs and decrypt all data from SSDs, via an alphanumeric key (or password protection) to prevent data theft. It continuously scrambles and descrambles data written to and retrieved from SSDs.

² 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.

³ Definition of capacity – KIOXIA Corporation defines a megabyte (MB) as 1,000,000 bytes, a gigabyte (GB) as 1,000,000,000 bytes and a terabyte (TB) as 1,000,000,000,000 bytes. A computer operating system, however, reports storage capacity using powers of 2 for the definition of 1Gbit = 2^{30} bits = 1,073,741,824 bits, 1GB = 2^{30} bytes = 1,073,741,824 bytes and 1TB = 2^{40} bytes = 1,099,511,627,776 bytes and therefore shows less storage capacity. Available storage capacity (including examples of various media files) will vary based on file size, formatting, settings, software and operating system, and/or pre-installed software applications, or media content. Actual formatted capacity may vary.

⁴ Developed by the Trusted Computing Group[®] (TCG), a not-for-profit international standards organization, the Opal specification is used for applying hardware-based encryption to solid state drives and is often referred to as TCG-Opal. The KIOXIA CM7 Series optional SED model supports TCG Opal and Ruby SSCs and has a few unsupported features of TCG Opal SSC.

⁵ Read and write speed may vary depending on the various factors such as host devices, software (drivers, OS, etc.) and read/ write conditions.

⁶ DWPD: Drive Write(s) Per Day: One full drive write per day means the drive can be written and re-written to full capacity once a day, every day, for the specified lifetime. Actual results may vary due to system configuration, usage, and other factors.

⁷ Optional security feature compliant drives are not available in all countries due to export and local regulations.

⁸ The product images shown are representations of design models and not accurate product depictions.

TRADEMARKS:

AMD EPYC and combinations thereof are trademarks of Advanced Micro Devices, Inc. Dell, Dell Technologies, OpenManage and PowerEdge are trademarks of Dell Inc. or its subsidiaries. NVMe is a registered or unregistered trademark of NVM Express, Inc. in the United States and other countries. PCIe is a registered trademark of PCI-SIG. Trusted Computing Group is a registered trademark of Trusted Computing Group. Ubuntu is a registered trademark of Canonical Ltd. All other company names, product names and service names may be trademarks or registered trademarks of third-party companies.

DISCLAIMERS:

KIOXIA America, Inc. may make changes to specifications and product descriptions at any time. The information presented in this performance brief is for informational purposes only and may contain technical inaccuracies, omissions and typographical errors. Any performance tests and ratings are measured using systems that reflect the approximate performance of KIOXIA America, Inc. products as measured by those tests. Any differences in software or hardware configuration may affect actual performance, and KIOXIA America, Inc. does not control the design or implementation of third-party benchmarks or websites referenced in this document. The information contained herein is subject to change and may render inaccuracies for many reasons, including but not limited to any changes in product and/or roadmap, component and hardware revision changes, new model and/or product releases, software changes, firmware changes, or the like. KIOXIA America, Inc. assumes no obligation to update or otherwise correct or revise this information.

KIOXIA America, Inc. makes no representations or warranties with respect to the contents herein and assumes no responsibility for any inaccuracies, errors or omissions that may appear in this information.

KIOXIA America, Inc. specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. In no event will KIOXIA America, Inc. be liable to any person for any direct, indirect, special or other consequential damages arising from the use of any information contained herein, even if KIOXIA America, Inc. are advised of the possibility of such damages.

© 2026 KIOXIA America, Inc. All rights reserved.