KIOXIA

Performance Brief

Next-Generation Dell EMC® PowerEdge™ Servers Deployed with KIOXIA Value SAS SSDs Deliver Encryption Protection without a Performance Hit

Data encryption has been used for decades in data center computing environments to protect both data-in-transit and data-at-rest. In these environments, there are two predominant storage factors: (1) clients generate data continuously; and (2) data collection continues to grow. This explosion in the amount of sensitive, and sometimes personal data that is generated and stored comes from many different devices such as desktops and laptops, smartphones and tablets, as well as IoT devices, whether on-premises or 'at-the-edge' of the data center network where data is captured and processed (i.e., robots, drones, machines, surveillance cameras, etc.). This data is sent to compute and storage systems in the data center for storage and further processing.

The sensitivity of this data makes it more important than ever for companies to protect what they've captured, both for short-term use and archival purposes, especially with technologies like artificial intelligence (AI) and machine learning (ML) that can help maximize the value of captured/archived data. Companies are relying more on encrypting stored data in their data centers for protecting business-critical and sensitive information from unauthorized parties and hackers.

With each new generation of hardware and software that is produced, in combination with the exponential growth of data, it is critical for encryption methods to keep pace with technological advances. An optimal solution is to provide encryption protection with data access speed that is comparable to data stored without encryption, which in turn delivers high system performance. The ability to protect data through encryption without degrading performance is the basis of this brief.

Data Encryption Performance Issues

Data encryption is the process of taking digital content (such as a document or an email message) and translating it into an unreadable format so that clients with a 'security key' or password are the only ones that can access it. This approach helps to protect the confidentiality of digital data stored on computer systems or that is transmitted over wireless networks and the Internet. For example, when a smartphone is used for a bank transaction or an online purchase, encryption protects the user information that is being transmitted over multiple networks to a remote server.

Being a compute-intensive operation, 'data-at-rest encryption' historically was not used as frequently as 'data-in-transit encryption' due to the amount of time and CPU cycles that were exhausted encrypting and decrypting data. These limitations, in some cases, caused reduced system and application-level performance that not only affected the applications themselves, but also the customer experience. To reduce CPU cycles used for encryption, storage manufacturers have created devices that support encryption protocols inside of the storage drive itself. These drives are called Self Encrypting Drives[1] (SEDs).

An SED-based SSD implements on-board crypto-processers and uses an AES[2]-256 cryptographic module and a media encryption key to encrypt plaintext data traversing to the SSD, to the media inside of the SSD itself. This process ensures that data-at-rest is encrypted at the hardware layer to prevent unauthorized access.

System and Application Test Scenario

Delivering a server or storage solution that provides data encryption inside of the drive without compromising SSD performance was a design goal for KIOXIA. To determine if encryption delivers a performance hit on its RM Series of value SAS enterprise SSDs, KIOXIA conducted a series of five tests, with varying megabytes per second (MB/s) throughput and input/output operations per second (IOPS) rates in a lab environment, with and without encryption enabled. The test configuration included the popular Dell EMC PowerEdge MX750c compute blade with dual Intel® Xeon® Gold 6330 CPUs and a KIOXIA RM6 Series value SAS SSD with Trusted Computing Group (TCG)-Enterprise[3] encryption support.

During the initial server boot-up, hardware level encryption was enabled through the BIOS on a Dell® PowerEdge RAID Card (PERC) Model H755 which enables the SSD to encrypt data. The 'logical volume' was created as an 'encrypted volume' to enable TCG-Enterprise encryption for the KIOXIA RM6 Series SSD, thereby creating a secured logical device.

The five tests were run through Flexible I/O (FIO) software[4] which is a tool that provides a broad spectrum of workload tests with results that deliver the actual raw performance of the drive itself. This included sequential read/write throughput tests and random read/write IOPS tests, often referred to as four-corner testing, as well as a mixed random IOPS test that emulates a general 70%/30% (read/write) ratio for a user application.

A description of the test criteria, set-up, execution procedures, results, and analysis are presented below. The test results demonstrate the probable effects that encryption has on 4-corner performance (plus a 70/30 mix) when running raw FIO workloads with an RM6 Series SSD and comparable equipment.

Test Criteria

The hardware and software equipment used for the five encryption tests included:

- **Dell EMC MX750c Server:** One (1) dual socket server with two (2) Intel Xeon Gold 6330 processors, featuring 28 processing cores, 2.0 GHz frequency, and 512 gigabytes[5] (GB) of DDR4 RAM
- **Operating System:** CentOS™ Stream (Kernel 4.18.0-315.el8.x86_64)
- **Application:** FIO v3.19
- **Test Software:** Synthetic tests run through FIO v3.19 test software
- **SAS RAID Card:** Dell PERC H755
- **Storage Device** (Table 1)**:** One (1) KIOXIA RM6 Series value SAS SSD with 1.92 terabyte[5] (TB) capacities and following specs:

Specifications	RM6 Series
Interface	12Gb/s SAS
Capacity	1.92TB
Form Factor	2.5-inch[6] (15mm)
NAND Flash Type	BiCS FLASH™ 3D flash memory
Drive Writes per Day[7] (DWPD)	3 (5 years)
Power	9W

Table 1: KIOXIA RM6 Series SSD specifications and set-up parameters

Set-up & Test Procedures

Set-up: The test system was configured using the hardware and software equipment outlined above. An unsecured RAID 0 set was created on the Dell H755 PERC using one RM6 Series SSD with the SED option. RAID 0 was selected since it is the only RAID set that can be used with a singular drive so that the RM Series SSD can be presented to the OS through the Dell PERC H755. Once the RM6 Series SSD array was initialized, the RAID 0 set appeared as a regular logical device to the OS.

Test Procedures: The MX750c server was set up with CentOS Stream and FIO test software. Two tests were set up and run in succession on the same server to compare RM6 Series SSD performance – one with TCG-Enterprise encryption enabled and one with encryption disabled. The tests consisted of running the FIO synthetic benchmarks across one RM6 Series SSD as specified above covering the common 4-corners of testing, as well as a 70/30 mixed read/write split as follows:

Test Order	Throughput or IOPS	Type of Test	Block Size
Test #1	Throughput	100% Sequential Read	128 kilobyte[5] (KB)
Test #2	Throughput	100% Sequential Write	128KB
Test #3	IOPS	100% Random Read	4KB
Test #4	IOPS	100% Random Write	4KB
Test #5	IOPS	70%/30% Random R/W	4KB

For each of these five tests, CPU utilization was also measured to determine if encryption when enabled taxes the CPU more versus when encryption is disabled.

Utilizing FIO software, the first set of five tests were run ***with encryption disabled***. The RM6 Series SSD was placed into the RAID 0 set and the five tests and associated CPU utilization was conducted with encryption disabled. See Test Results section.

The second set of five tests were run ***with encryption enabled***. To begin, the RAID 0 set was destroyed and a secure RAID 0 set based on the TCG-Enterprise specification was created. The RM6 Series SSD was placed into the secure RAID 0 set and the same five tests were conducted with encryption enabled. See Test Results section.

Test Results

The objective of these tests was to showcase how the FIO test runs on the Dell MX750c system provide the same level of performance whether data was encrypted or unencrypted. All five workload tests were run using FIO test software with the throughput, IOPS and CPU utilization recorded. The drive performed nearly identical on all tests regardless of whether encryption was enabled or disabled.

		Encryption Disabled		Encryption Enabled	
Performance Test	**Test Metrics**	**Results**	**CPU Utilization**	**Results**	**CPU Utilization**
100% Sequential Read *Sustained, 128KB, QD16*	Throughput (MB/s)	877.50	0.56%	877.83	0.58%
100% Sequential Write *Sustained, 128KB, QD16*	Throughput (MB/s)	732.83	0.56%	728.00	0.58%
100% Random Read *Sustained, 4KB, QD32*	IOPS	162,758	0.97%	162,758	0.90%
100% Random Write *Sustained, 4KB, QD32*	IOPS	65,622	0.55%	65,701	0.67%
70%/30% Random Mixed *Sustained, 4KB, QD32*	IOPS	118,455 (R) +50,752 (W) 169,207	1.05%	119,165 (R) +51,083 (W) 170,248	1.07%

Sequential Read/Write

Sequential read/write operations read and write data of a specific size that is ordered one after the other from a logical block address (LBA) perspective. The sequential read/write performance is regarded as data throughput and specified in MB/s.

Random Read/Write/Mixed

Random read/write/mixed operations read and write data of a specific size that is ordered randomly from a logical block address (LBA) perspective. The random read/write/mixed performance is specified in IOPS.

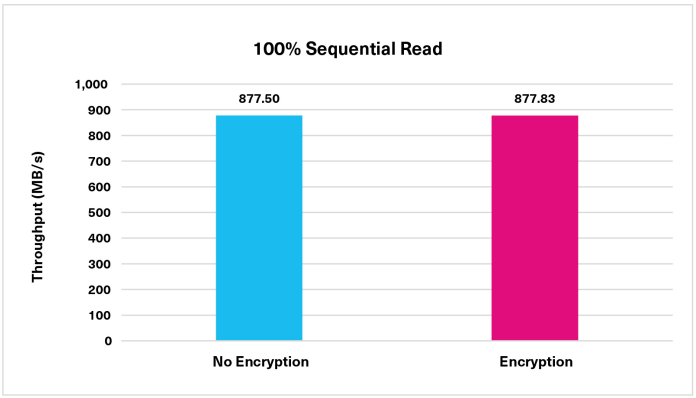
CPU Utilization

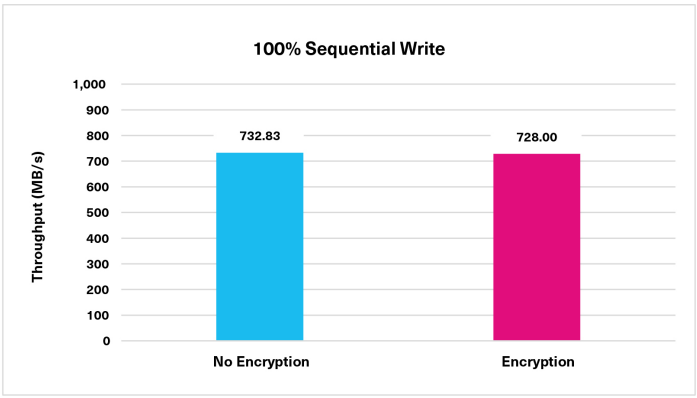
CPU utilization represents a percentage of the total amount of available CPU cycles being used for a given workload. Some forms of encryption require CPU cycles to encrypt and decrypt data on the storage media itself which can have an adverse effect on performance. For each of the five performance tests conducted, CPU utilization was measured to ensure that the Intel Xeon CPU was not incurring any extra processing for encryption – these tasks are handled in hardware at the RAID controller and SSD levels.

The results for each of the five performance tests:

Tests 1 & 2: 100% Sequential Read / Write

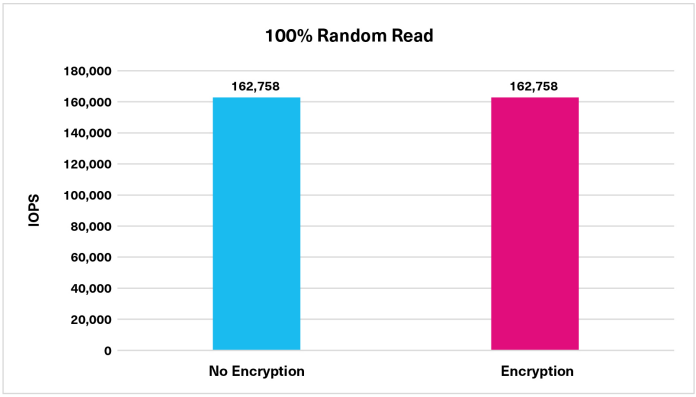
RM6 Series: FIO Sequential Workload Tests	No Encryption	With Encryption
100% Sequential Read (in MB/s)	877.50	877.83
Performance Difference	-	**0.0%**
100% Sequential Write (in MB/s)	732.83	728.00
Performance Difference	-	**-0.6%**

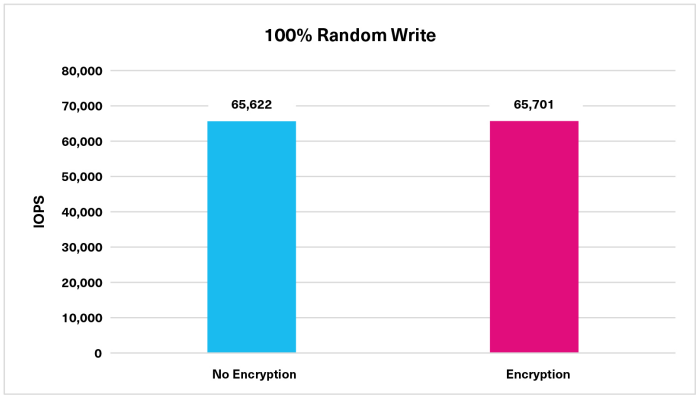




Tests 3 & 4: 100% Random Read/Write

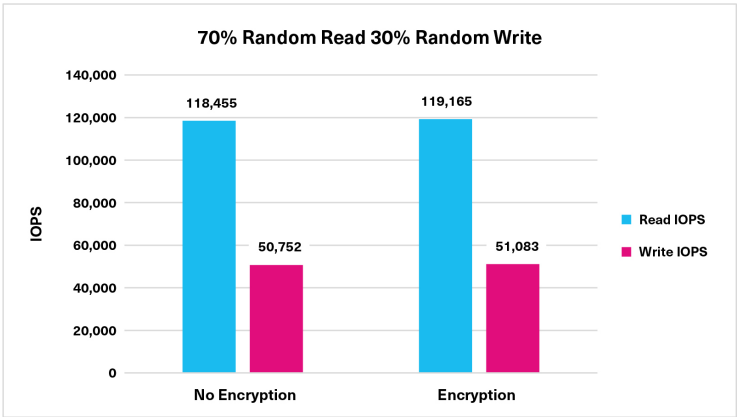
RM6 Series: FIO Random Workload Tests	No Encryption	With Encryption
100% Random Read (in IOPS)	162,758	162,758
Performance Difference	-	**0.0%**
100% Random Write (in IOPS)	65,622	65,701
Performance Difference	-	**+0.1%**





Test #5: 70%/30% Random Mixed

RM6-Series Tests: FIO Workload	No Encryption	With Encryption
70% Read Random Mixed (in IOPS)	118,455	119,165
30% Write Random Mixed (in IOPS)	50,752	51,083
Total Random Mixed (in IOPS)	169,207	170,248
Performance Difference	-	**+0.6%**



Test Analysis

The test results validate that the KIOXIA RM6 Series SSD enabled the Dell MX750c compute blade to deliver nearly identical throughput and IOPS performance whether encryption was enabled or not. This particular 12Gb/s SAS server configuration was able to deliver up to 877MB/s and up to 732MB/s for 100% sequential read and write operations, respectively, without any throughput-related performance degradation regardless of whether encryption was enabled or disabled.

In addition, the same configuration was able to deliver up to 162,758 IOPS and 65,701 IOPS for 100% random read and write operations, respectively, without any IOPS-related performance degradation regardless of whether encryption was enabled or disabled.

Lastly, the 70/30 random workload that emulates another typical user application was able to deliver up to 170,248 of total combined read/write IOPS without any IOPS-related performance degradation regardless of whether encryption was enabled or disabled.

As a result, systems and applications that use SSDs incorporating encryption that is compliant with the TCG-Enterprise standard can encrypt data-at-rest without a performance hit. Regardless of whether hardware encryption was enabled or disabled, there was almost no deviation of the drive performance across all five tests run during the testing process.

RM6 Series SSD Overview

The RM6 Series is KIOXIA's 2nd generation value SAS SSD product line that delivers improved performance over previous RM Series generations. The series features larger 7.68TB capacities, single-port interfaces, 1 DWPD for read-intensive applications (RM6-R Series) and 3 DWPD for mixed use applications (RM6-V Series), up to a 9-watt power envelopes, and a host of security options – all of which are geared to support a wide variety of workload requirements.

The RM6 Series SSD architecture has encryption built into the data path; as the drive is reading and writing from NAND flash memory, the encryption or decryption is performed in a way that it has no material impact to performance[8].

Summary

Encryption has become more important than ever to secure data. An ideal encryption solution does not impact application or system performance. The test results presented validate that a PowerEdge MX750c compute sled with a KIOXIA RM6 Series SSD effectively delivered nearly identical 4-corner performance and 70/30 mixed read/write random performance while providing the added security of encryption. As data usage scales over time, performance will not typically be impacted by encryption no matter how much data is being transmitted (to and from the SSD), and users would not experience any difference in performance.

CPU utilization was also comparable with or without encryption enabled as the Dell PERC H755 SAS RAID card fully offloaded encryption management from the CPU and validated that the Intel Xeon CPU was not materially impacted when encryption was enabled or disabled.

Bottom line: The Dell EMC and KIOXIA server solution delivered encryption protection without a performance hit.

RM6 Series SSDs
12Gb/s SAS

High-Performance[9]
SeqRead = up to 840MB/s
RanRead = up to 160K IOPS
SeqWrite = up to 710MB/s
RanWrite+ up to 50K IOPS

Configurable Flexibility
1 and 3 DWPD options
960GB – 7,680GB capacities

Notes:

[1] Self-Encrypting Drives 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] Developed by the Trusted Computing Group (TCG), a not-for-profit international standards organization, the TCG-Enterprise standard is targeted for fixed media storage devices in high-performance systems where high capacity, fast data access and the utmost in reliability are required, and supports the higher performing SAS bus type.

[4] Flexible I/O (FIO) is a free and open source disk I/O tool used both for benchmark and stress/hardware verification. The software displays a variety of I/O performance results, including complete I/O latencies and percentiles.

[5] Definition of capacity - KIOXIA Corporation defines a kilobyte (KB) as 1,000 bytes, 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 = 230 bits = 1,073,741,824 bits, 1GB = 230 bytes = 1,073,741,824 bytes and 1TB = 240 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.

[6] 2.5-inch indicates the form factor of the SSD and not the drive's physical size.

[7] 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.

[8] Variances in individual test queries may occur in normal test runs. Average performance over time was consistent for encryption enabled and encryption disabled.

[9] Read and write speed may vary depending on the host device, read and write conditions, and the file size.

Trademarks:

CentOS is a trademark of Red Hat, Inc. in the United States and other countries. Dell, Dell EMC and PowerEdge are either registered trademarks or trademarks of Dell Inc. Intel and Xeon are registered trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries. All company names, product names and service names may be the trademarks of their respective companies.

Disclaimers:

 Information in this performance brief, including product specifications, tested content, and assessments are current and believed to be accurate as of the date that the document was published, but is subject to change without prior notice. Technical and application information contained here is subject to the most recent applicable KIOXIA product specifications.