KIOXIA

Performance Brief

Deliver Encryption Protection without a Performance Hit in HPE® ProLiant® DL360 Gen11 Servers with KIOXIA CD8P Series Data Center NVMe® SSDs

Introduction

Data encryption has been used for decades in data centers to protect both data in transit and data-at-rest. As users generate data continuously, data collection also continues to grow. This abundance of data comes from many different devices, such as desktops, laptops, tablets, smartphones and IoT devices (e.g., robots, drones, machines, surveillance cameras, etc.), whether on-premises or at-the-edge of the network.

The business value of collected data makes it more important than ever for companies to protect what they have captured, especially with technologies like artificial intelligence (AI) that can help maximize data value. Additionally, more companies are encrypting the data stored in their data centers to help protect their business-critical and sensitive data-at-rest.

With each new generation of hardware and software, coupled with the exponential growth of data, it is critical for encryption methods to keep pace with technological advances since, historically, encryption degrades performance. The ideal encryption solution delivers similar performance as if encryption is disabled. The ability to protect data through encryption without experiencing performance degradation is the basis of this performance brief.

Data Encryption Performance Issues

Data encryption is the process of taking digital data and translating it into an unreadable format so that users with a 'secret key' or password are the only ones that can access or read it. Being a calculation-intensive operation, encryption has typically been limited in use because of the amount of time and CPU cycles which can be lost when encrypting and/or decrypting data. These limitations may cause reduced system and application-level performance challenges that not only affect the applications themselves, but also the customer experience.

To reduce the CPU cycles used for encryption, SSD manufacturers created devices that support encryption protocols inside of the drive itself. These drives are called Self-encrypting Drives[1] (SEDs). A KIOXIA SED SSD implements on-board crypto-processers and uses an AES[2]-256 cryptographic module, as well as a media encryption key, to encrypt plain-text data. This process ensures that data-at-rest is encrypted at a hardware layer to prevent unauthorized access.

This performance brief presents test results that determined if encryption leads to a performance hit. The KIOXIA Innovation Lab conducted database throughput tests on an HPE ProLiant DL360 Gen11 server, with and without encryption enabled. The server was deployed with four 3.84 terabyte[3] (TB) KIOXIA CD8P-R Series PCIe® 5.0 Data Center NVMe SSDs that support the TCG-Opal[4] specification for SED SSDs. During the initial server boot-up, SSD-based encryption was enabled through the BIOS on each drive. Windows Storage Spaces™ was then utilized to create a storage pool with the hardware encrypted drives. A virtual device (using mirror spaces) and a logical volume were created. The tests utilized an operational, high-performance Microsoft® SQL Server™ database workload based on TPROC-C[5] benchmarks created by HammerDB[6] test software.

The test results show that an HPE ProLiant DL360 Gen11 server, deployed with KIOXIA CD8P-R Series SSDs, effectively delivered similar database performance of more than 2.4 million transactions per minute (TPM), whether encryption was enabled or not. CPU utilization was also similar, with or without encryption enabled, which validated that the CPU resources (at approximately 78% utilization) were not impacted when encryption was enabled.

Test Results Snapshot

Four KIOXIA CD8P-R Series SSDs were tested, with and without encryption enabled, in an HPE® ProLiant® DL360 Gen11 server, with the following results:

-

Transactions per Minute

2,413,135 TPM

Without Encryption

vs.

2,459,593 TPM

With SSD-based Encryption

Encryption without a performance hit!!!

CPU Utilization

77.81%

Without Encryption

vs.

78.04%

With SSD-based Encryption

Encryption with similar CPU utilization

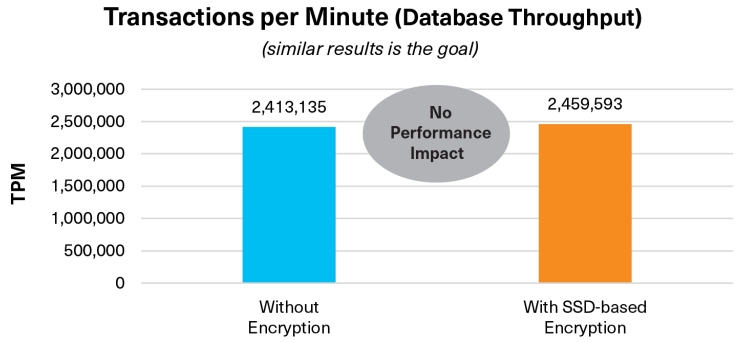
The test results include a description of each workload test, a graphical depiction of the test results and an analysis. Appendix A covers the hardware and software test configuration. Appendix B covers the configuration set-up and test procedures.

Test Results

The test results provide a data center scenario showcasing the effects that encryption has on database throughput performance when running a Microsoft® SQL Server™ database using comparable equipment and performing queries against it. In this test configuration, an HPE® ProLiant® server utilized four KIOXIA CD8P-R Series SSDs when running the database application to demonstrate performance of a system with and without data encryption. CPU utilization was also gathered while running the queries against the database to determine the effect that encryption has on it. The test results include the following:

Transactions per Minute (TPM)

In an online transaction processing (OLTP) database environment, TPM is a measure of how many transactions in the TPROC-C transaction profile are being executed per minute. HammerDB software, executing the TPROC-C transaction profile, randomly performs transaction types such as new orders, payments, order status, deliveries and stock levels. This benchmark simulates an OLTP environment where there are a large number of users that conduct simple, yet short transactions, and require sub-second response times that return relatively few records. For this test, the results are in TPM, and similar results were the goal. Data was aggregated through multiple test runs and delivered a performance deviation of 1.9%.

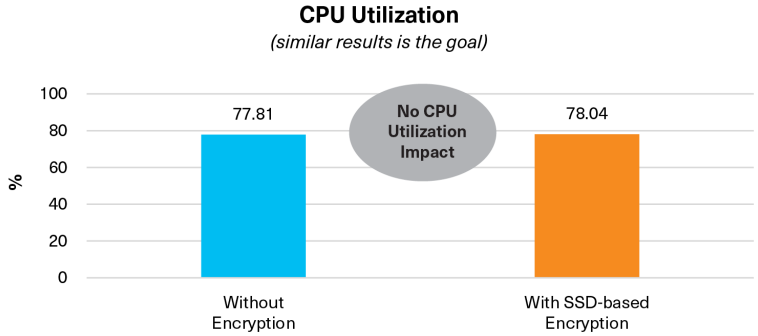


KIOXIA CD8P-R Series Tests: SQL Server™ TPROC-C Workload	Without Encryption	With SSD-basedEncryption
Transactions per Minute	2,413,135	2,459,593
Performance Deviation	-	1.9%

As the TPROC-C transaction profile was executed randomly, run to run database throughput performance varied depending on how many of which transaction happens to be selected to perform against the database. The margin of deviation when measuring TPM, with or without encryption, was 1.9%, which implies no discernable difference in application level performance between the two encryption approaches.

CPU Utilization

In general, CPU utilization represents a percentage of the total amount of computing tasks that are handled by the CPU, and provides another estimation of system performance. Some forms of encryption require CPU cycles to encrypt and decrypt data on the storage media itself, which can lead to a performance impact. CPU utilization was monitored to measure if the CPU resources were incurring any extra processing for encryption, which should be handled in hardware at the SSD level. The SSD-based configuration from HPE, deployed with KIOXIA CD8P-R Series SSDs, enabled the server CPU resources to be utilized for compute tasks, versus encryption. For this test, the results are in percentage (%) of use, and similar utilization results was the goal.



KIOXIA CD8P-R Series Tests: SQL Server TPROC-C Workload	Without Encryption	With SSD-based Encryption
CPU Utilization	77.81%	78.04%
Usage Deviation	-	0.2%

The test results demonstrate that CPU utilization was similar, yielding 77.81% utilization without encryption and 78.04% utilization with encryption. The margin of deviation, with or without encryption, was 0.2%, which implies no discernable difference in CPU usage between the two encryption approaches. The SSD-based encryption configuration from HPE®, deployed with KIOXIA CD8P-R Series SSDs, enabled the ProLiant® DL360 Gen11 server CPUs to be utilized for compute tasks, instead of encryption.

Analysis

The test results validated that KIOXIA CD8P-R Series SSDs enabled the HPE ProLiant DL360 Gen11 server to deliver similar database throughput performance whether encryption was enabled or not. This particular PCIe® 5.0 and NVMe™ server and storage configuration was able to deliver more than 2.4 million TPM, without any database throughput degradation, regardless of the encryption method. As a result, systems and applications that use SSDs based on the TCG-Opal standard can utilize the CPU resources for performance and processing tasks, rather than encryption-related tasks.

The test results also validated that there was almost no deviation in CPU utilization during the testing process, which further demonstrated that the CPU was not required to process any extra workloads for encryption.

Summary

Encryption in today's data centers is as important as ever for securing captured data from attacks and hackers, however, encryption has typically degraded application and system performance. The test results demonstrated an encrypted solution that did not impact application or system performance and featured the HPE ProLiant DL360 Gen11 PCIe 5.0-enabled server deployed with KIOXIA CD8P-R Series SSDs. This solution effectively delivered similar database throughput performance, whether encryption was enabled or disabled.

CPU utilization was also similar, with or without encryption enabled, which validated that the CPU resources (at approximately 78% utilization) were not impacted when encryption was enabled.

Based on these tests, the HPE ProLiant DL360 Gen 11 server and KIOXIA CD8P-R Series SSD storage solution delivered encryption protection without a performance hit!!!

KIOXIA CD8P-R Series SSD Product Info

The KIOXIA CD8P Series SSD product line is data center-class and compliant with the PCIe® 5.0 specification and the NVMe™ 2.0 protocol. These SSDs are available in 2.5-inch[7] and Enterprise and Datacenter Standard Form Factor (EDSFF) E3.S form factors.

For this performance brief, the KIOXIA CD8P-R Series E3.S SSD was used with 1 DWPD[8] of endurance and a 3.84 TB[3] capacity. The product series supports up to 30.72 TB capacity in the 2.5-inch format and up to 15.36 TB capacity in the E3.S format and has the following performance specifications[9] (in single port (1x4) mode):

Sequential Read: *up to 12,000 megabytes per second (MB/s); includes the 15.36 TB model*
Sequential Write: *up to 5,500 MB/s; up to 5,300 MB/s for the 15.36 TB model*
Random Read: *up to 2,000,000 input/output operations per second (IOPS); includes the 15.36 TB model*
Random Write: *up to 200,000 IOPS; includes the 15.36 TB model*

KIOXIA CD8P Series SSDs are also available for higher endurance mixed-use applications and include 3 DWPD endurance and capacities up to 12.8 TB.

Additional KIOXIA CD8P Series SSD information is available here.

KIOXIA CD8P Series E3.S SSD[10]

Appendix A

Hardware/Software Test Configuration

Server Information	
Model	HPE® ProLiant® DL360 Gen11
No. of Servers	1
No. of CPU Sockets	2
CPU	Intel® Xeon® Gold 6426Y
No. of CPU Cores	32
CPU Frequency	2.5 GHz
Total Memory	352 GB[3] DDR5 DRAM
Memory Frequency	DDR5-4800

Operating System Information	
Operating System	Windows Server® 2025 Datacenter
Version	24H2

Database Information	
Database	Microsoft® SQL Server™ 2022
Version	16.0.1000.6
MaxDOP[11]	8
Maximum Server Memory	32,768 MB

Test Software Information	
Load Generator	HammerDB
Version	4.12
No. of Warehouses	1,000
No. of Virtual Users	64

SSD Information	
Model	KIOXIA CD8P-R Series
Interface	PCIe® 5.0 x4
Protocol	NVMe™ 2.0
No. of Drives	4
Form Factor	EDSFF E3.S
Capacity	3.84 TB
DWPD	1 (5 years)
Power Consumption	19 W

Appendix B

Configuration Set-up/Test Procedures

Configuration Set-up

An HPE® ProLiant® DL360 Gen11 server was set-up with four 3.84 TB KIOXIA CD8P-R Series E3.S SSDs with the SED option and the drives were installed into the server.

A Windows Server® 2025 Datacenter operating system was installed.

Both an unsecured and secured Windows Storage Spaces™ mirror spaces set was used on a storage pool consisting of the four KIOXIA CD8P-R Series SSDs.

The mirror spaces were set-up with a Microsoft® Windows® NT file system (NTFS) on top of a logical volume.

The Microsoft SQL Server™ application was then installed and limited to 32 GB of memory.

A TPROC-C database was then loaded using HammerDB test software. Tests were then run to gather database throughput and CPU utilization.

Test Procedures

The four KIOXIA CD8P-R Series SSDs were placed into a Windows Storage Spaces mirror spaces set and the first test was conducted with encryption disabled. The TPROC-C workload utilized HammerDB software to run the test.

The results of the database throughput and CPU utilization tests were recorded when encryption was disabled.

In preparation of conducting the second test with encryption enabled, the previous Microsoft SQL Server instance, logical volume, virtual disk and storage pool were removed, and the server was rebooted into the server BIOS.

Each KIOXIA CD8P-R Series SSD was then enabled for SSD-based encryption in the BIOS using a local key manager.

A new storage pool, mirror set, virtual disk, logical volume with an NTFS file system, and a Microsoft SQL Server instance were created based on the drives being encrypted using the TCG-Opal specification.

The TPROC-C workload was run using HammerDB test software and the same test was conducted with encryption enabled. The objective of this test was to showcase how the application and system provide the same level of performance whether data was encrypted or not.

The results of the database throughput and CPU utilization tests were recorded when encryption was enabled 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 often referred to as TCG-Opal.

[5] TPROC-C is the OLTP workload implemented in HammerDB derived from the TPC-C™ specification with modification to make running HammerDB straightforward and cost-effective on any of the supported database environments. The HammerDB TPROC-C workload is an open source workload derived from the TPC-C Benchmark Standard and as such is not comparable to published TPC-C results, as the results comply with a subset rather than the full TPC-C Benchmark Standard. TPROC-C means Transaction Processing Benchmark derived from the TPC "C" specification.

[6] HammerDB is benchmarking and load testing software that is used to test popular databases. It simulates the stored workloads of multiple virtual users against specific databases to identify transactional scenarios and derive meaningful information about the data environment, such as performance comparisons.

[7] 2.5-inch indicates the form factor of the SSD and not the drive's physical size.

[8] 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.

[9] The KIOXIA CD8P-R Series E3.S SSD performance specifications provided by Kioxia Corporation are accurate as of this publication. Specifications are subject to change. Read and write speed may vary depending on the host device, read and write conditions, and the file size.

[10] The product image shown is a representation of the design model and not an accurate product depiction.

[11] Maximum degree of parallelism.

TRADEMARKS:

Intel and Xeon are trademarks of Intel Corporation or its subsidiaries. HPE and ProLiant are registered trademarks of Hewlett-Packard Enterprise Company and/or its affiliates. Microsoft, Windows, Windows Server, Windows Storage Spaces and SQL Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. 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. TPC-C is a trademark of the Transaction Processing Performance Council. Trusted Computing Group is a registered trademark of Trusted Computing Group. 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.