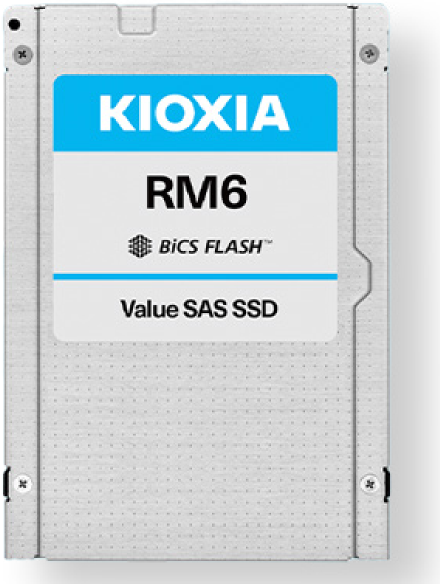
Technical Research Report

PROWESS

Life After SATA: KIOXIA Value SAS SEDs Protect Data with Encryption Without a Performance Hit

KIOXIA RM6 Series Value Serial-Attached SCSI (Value SAS) self-encrypting drives (SEDs) not only provide data protection and high-speed storage, but their superior price-performance over Serial ATA (SATA) removes the last hurdle to upgrading your data center.



Executive Summary

A best-practices security plan should include a way to safeguard confidential and sensitive data from physical theft. This is accomplished by encrypting data storage using hardware- or software-based full disk encryption. The results of Prowess Consulting workload testing indicate that self-encrypting drives (SEDs) built on value serial-attached SCSI (value SAS) technology can encrypt data without impacting storage performance or latency. Using results from a separate study, we concluded that value SAS SEDs perform better than traditional 6 gigabits per second Serial ATA (6 Gb/s SATA) drives and cost less than NVM Express™ (NVMe™) PCIe® drives.

Tasked with protecting your organization’s most valuable asset—its data—you have critical decisions to make. You need information that cuts through the gloom and doom and helps you make the most effective data storage choices possible. Read our analysis on the security and performance benefits that value SAS SEDs can give your data center. Learn why there is so much more to life after SATA.

Market and Technology Trends

Today's data center faces constant security threats, including the physical theft of storage drives. The probability of your data being physically stolen is relatively low, compared to the more prevalent theft of user credentials to gain access to secure data. However, a single drive going missing can have far-reaching and long-lasting consequences for your business. The loss of confidential or sensitive data can be devastating to revenue streams, user productivity, customer trust, partner relations, and legal compliance.

We recommend using full disk encryption to protect against data loss caused by physical theft. While this basic security feature does an excellent job of protecting your data, it can also impose a performance penalty on your data storage systems if not deployed properly.[1] Encrypted data can take longer to write and read from storage, which can result in increased application response times. Encryption operations can tie up the CPUs powering your application servers, stealing processing cycles from other workloads.

These considerations beg the question, what data storage technologies deliver both security and performance? And is it possible to get these benefits without breaking the bank? Our analyses indicate that there are storage solutions available that won't force you to choose between data encryption and business-critical application performance.

Methodology

Armed with these questions, Prowess Consulting designed a study examining storage technologies that offer data security and high performance, and that are also budget friendly. Our initial investigation indicated that SEDs could deliver hardware-level data encryption with effectively no performance hit. We focused our testing on value SAS SEDs because they deliver higher performance than traditional 6 Gb/s SATA drives, while costing less than PCIe/NVMe drives.[2,3]

We used the following hypothesis for testing: workloads using the SAS SED for data encryption would perform as well as unencrypted workloads and better than software-encrypted workloads.

We selected Linux® unified key setup (LUKS) as our file system software-based encryption method because of its popularity on Linux operating systems.[4] We measured throughput results as mean transactions per second for read-data and write-data. We measured latency results as mean response times for read-data only, because the Pepper-Box producer sampler does not track read-data latency. For full testing details, see the methodology report at https://prowessconsulting.com/project/kioxia-sas-value-ssd-security-encryption-performance.

Our engineers configured a Dell™ PowerEdge™ R650 server using KIOXIA RM6 Series Value SAS SEDs for storage. (See Table 1 for details.) We set up this test system to emulate a high-throughput, low-latency Apache Kafka® platform, using the Pepper-Box plugin to represent 50% read-data/50% write storage. We ran three types of benchmarking tests on the same KIOXIA Value SAS SED system. Each benchmarking test changed one of the following encryption variables:

1. No encryption: workloads with the KIOXIA Value SAS SED built-in encryption disabled.
2. Hardware encryption: workloads with the KIOXIA Value SAS SED built-in encryption enabled.
3. File system encryption: workloads with the KIOXIA Value SAS SED built-in encryption disabled and using LUKS for data encryption.

Table 1 | One server configuration was used for all testing

Configuration	Dell™ PowerEdge™ R650
Model Name	Dell PowerEdge R650
CPU	Intel® Xeon® Silver 4314 processor
Storage Controller 1	Broadcom®/LSI Dell PowerEdge RAID Controller 11 (PERC 11) H755 Front
Data Disk	3.84 TB KIOXIA KRM6VRUG3T84 self-encrypting drive (SED)
Number of Disks	4
Storage Controller 2	Marvell Technology Group Ltd. Dell™ Boot Optimized Server Storage (BOSS)-S1
Boot Disk	2 x 480 GB Micron® MTFDDAV480TDS
Operating System (OS)	Ubuntu® 22.04.2 LTS
Apache Kafka® Version	2.12-3.2.3
Hardware Encryption	KIOXIA embedded encryption engine
File System Encryption	Linux® unified key setup (LUKS)

Results and Analysis

As mentioned previously, the potential risk of performance bottlenecks can mislead you into unnecessarily turning off data encryption. Our benchmarking results indicate that the KIOXIA Value SAS SED offers an encrypted storage solution that can liberate you from making an either/or choice between performance and security.

The KIOXIA Value SAS SED showed no significant performance difference between encryption turned on and encryption turned off. Compared to LUKS file system encryption, the KIOXIA Value SAS SED delivered up to:

- 5.29x faster encrypted read-storage latency
- 15% higher encrypted read-storage throughput
- 9% higher encrypted write-storage throughput

In a study comparing value SAS and SATA drives, price-performance analysis indicated that unencrypted value SAS drives could provide up to 43% better performance per dollar (US) than SATA drives.[2] In short, with value SAS SEDs, you can have it all: robust data protection, high-speed storage, and a price-performance that beats SATA.

Encryption Throughput for Write-Data and Read-Data Storage

Our testing results (Figure 1 and Table 2) showed no significant difference in storage throughput for the KIOXIA Value SAS SED, whether encryption was turned on or turned off. As expected, file system encryption processing imposed a performance penalty on storage throughput. Using the KIOXIA Value SAS SED's built-in hardware encryption resulted in up to 15% higher read throughput and 9% higher write throughput compared to LUKS file system data encryption with the hardware encryption turned off.

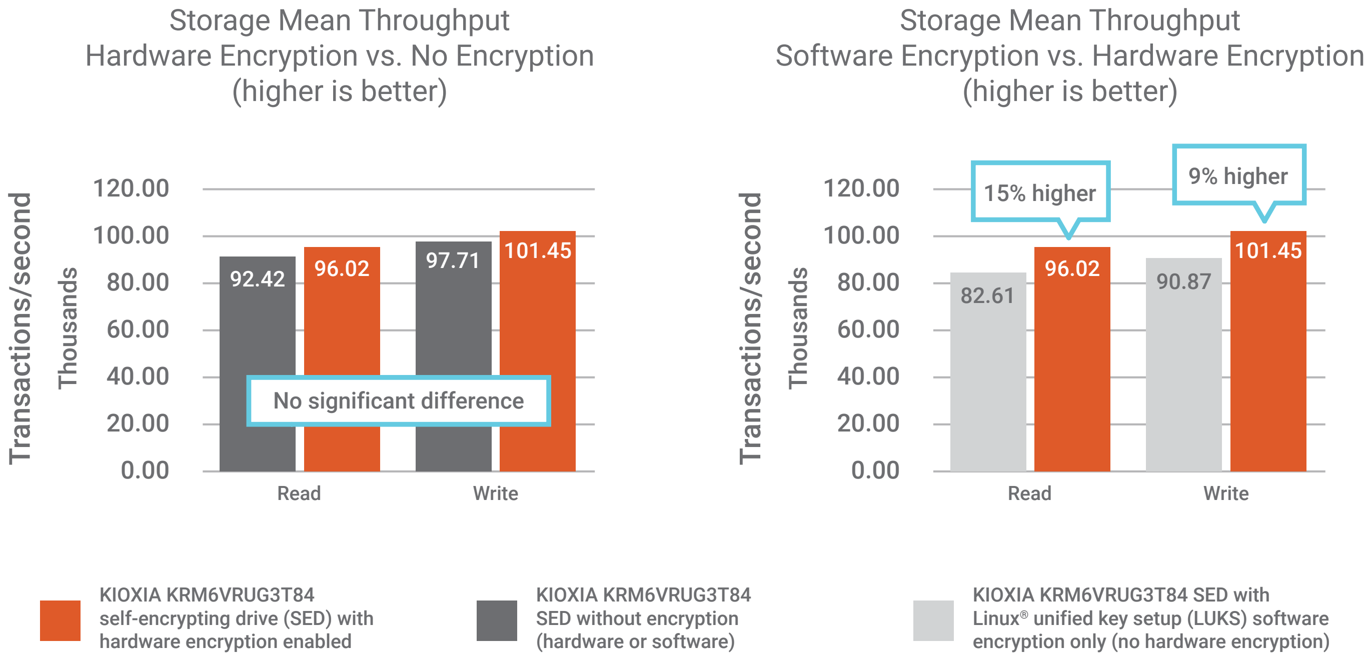


Figure 1 | The KIOXIA Value SAS SED encryption mean throughput for read data and write data is equivalent to no encryption and higher than LUKS encryption

Table 2 | KIOXIA Value SAS SED encryption throughput for read data and write data

Encryption Type	Data Type	Transactions per Second (mean)	Difference
KIOXIA Value SAS SED Hardware encryption	Read	96,018.85	• Up to 15% higher than Linux® unified key setup (LUKS) file system encryption • On par with no encryption
	Write	101,449.37	• Up to 9% higher than LUKS file system encryption • On par with no encryption
KIOXIA Value SAS SED LUKS file system software encryption	Read	82,607.32	
	Write	90,866.76	
KIOXIA Value SAS SED No hardware or software encryption	Read	92,420.61	
	Write	97,707.27	

Here is one example of how an organization can benefit from securing its data without taking a performance hit. The payment card industry data security standard (PCI DSS) requires online merchants to use data encryption to store customer credit card information. These merchants can face substantial fines should they fail to use data encryption when storing confidential information.[5] Our results indicate that online merchants could process up to 15% more secure transactions using hardware encryption instead of software encryption. And more transactions per second translates into higher profit margins.

Encryption Latency for Write-Data Storage

As shown in Figure 2 and Table 3, the difference in encrypted storage latency performance is even more marked. Write workloads using KIOXIA Value SAS SED hardware encryption had a 5.29x faster response time than LUKS file system software-encrypted workloads.

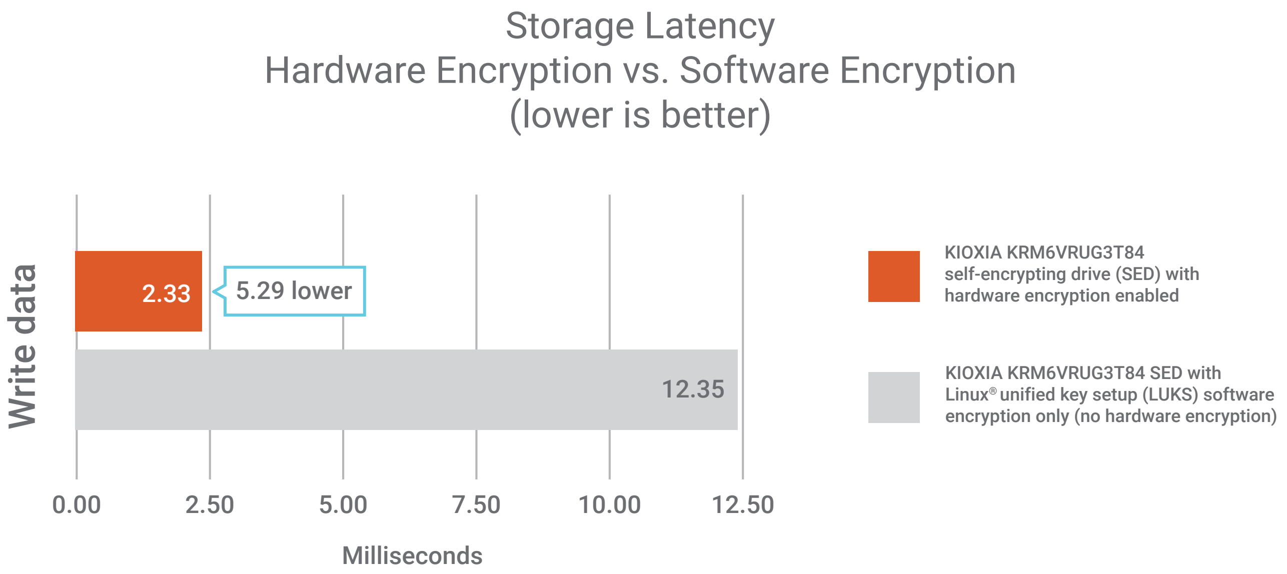


Figure 2 | KIOXIA Value SAS SED latency for write data using encryption is lower than LUKS encryption

Table 3. Encryption latency (average) for write data

Encryption Type	Milliseconds	Difference
KIOXIA SED hardware encryption	2.33	Up to 5.29x faster than Linux® unified key setup (LUKS) file system encryption
LUKS file system encryption	12.35	

Reaping the Benefits of High-Speed, Encrypted Data Storage

Value SAS drives give you an upgrade option that can pay for itself in higher performance/dollar. In a separate study comparing unencrypted value SAS and SATA drives, a KIOXIA Value SAS drive delivered up to 43% better price-performance than a traditional SATA drive.[2]

Using value SAS SEDs to encrypt data instead of using a file system such as LUKS benefits your applications in a couple of ways. First, hardware encryption can deliver better than 5x faster storage response, which lowers application response time. Using the value SAS SED to handle data encryption also helps free up CPU cycles for other workloads.

The ability to boost the performance of read-encryption and write-encryption can help you implement location-independent data protection across your network for a variety of usages, including information security and privacy compliance, user authentication, data integrity, and improved consumer trust.[6]

It is evident from the damages that *are* being reported that an extra layer of data protection could help prevent your organization from being bankrupted by the loss of your data.[7]

Conclusion

If finding secure data storage is on your to-do list, we suggest that you review the evidence presented in this report. The results of our workload testing indicate that value SAS SEDs can encrypt data without impacting performance. We also like the fact that value SAS SEDs outperform traditional 6 Gb/s SATA drives and cost less than NVMe PCIe drives.

If you have been hesitant to upgrade your SATA storage because of cost concerns, we recommend taking a look at KIOXIA's value SAS SEDs for data centers. As our test results indicate, the KIOXIA RM6 Series Value SAS SED offers a budget-friendly storage solution that won't make you choose between data protection and storage performance.

Learn More

Learn more about KIOXIA Value SAS SEDs at www.lifeaftersata.com.

[1] Sybase. "How database encryption and obfuscation affect performance." 2009. https://infocenter.sybase.com/help/index.jsp?topic=/com.sybase.help.sqlanywhere.11.0.1/uladmin_en11/ul-tuning-s-5258672.html.

[2] Prowess Consulting. "A Big Step Up from SATA: Testing KIOXIA RM6 Series Value SAS SSDs." 2023. https://prowessconsulting.com/wp-content/uploads/2023/05/220148-kioxia-sas-value-ssd-outperforms-sata-technical-research-report.pdf.

[3] Prices quoted for server configurations using 1.92 TB storage and provided by Dell Technologies as of March 30, 2023. SATA: US $63,849. SAS: US $65,824. PCIe/NVMe: US $67,902.

[4] It's FOSS. "Linux Jargon Buster: What is LUKS Encryption?" March 2023. https://itsfoss.com/luks/.

[5] Investopedia. "What Is Encryption? How It Works, Types, and Benefits." July 2022. www.investopedia.com/terms/e/encryption.asp#toc-benefits-of-encryption.

[6] Lepide. "5 Benefits of Using Encryption Technology for Data Protection." September 2022. www.lepide.com/blog/5-benefits-of-using-encryption-technology-for-data-protection/.

[7] Cybercrime Magazine. "60 Percent Of Small Companies Close Within 6 Months Of Being Hacked." January 2019. https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/.

The analysis in this document was done by Prowess Consulting and commissioned by KIOXIA.

Results have been simulated and are provided for informational purposes only. Any difference in system hardware or software design or configuration may affect actual performance.