Solution Brief
Intel® Xeon® processor E5 v3 Family
Big Data Security

Strong Security with High Performance for Real-Time, Big Data Deployments

Intel, Vormetric, and MongoDB* deliver enterprise-class data security—with breakthrough performance—for the world's most popular NoSQL database.

Security versus performance—that's the tradeoff many businesses have had to make when deploying big data applications. Strong data encryption is essential to protect sensitive data, but cryptographic algorithms place heavy loads on servers and can significantly slow application response times, especially in new big data deployments.

Vormetric, MongoDB, and Intel offer a solution to this challenge. Vormetric Data Security provides enterprise-class support for data security and compliance. It also takes full advantage of hardware-assisted security technologies that are built into the Intel® Xeon® processor E5-2600 v3 family. With this solution, you can implement strong data security without slowing performance. In fact, you are likely to find that your applications perform even better with encryption than without.

Strong Security and Compliance for Low-Risk Innovation

Vormetric Data Security provides encryption, key management, configurable security policies, and fine-grained data access controls, so you can enforce data security and compliance. The platform also provides efficient, centralized management, and captures information that security intelligence and event management (SIEM) solutions can use to detect advanced threats. You can even provide IT staff (or cloud service providers) with full access to your systems and applications, without allowing them to access your data, your keys, or your security policies. You remain in full control of your data.

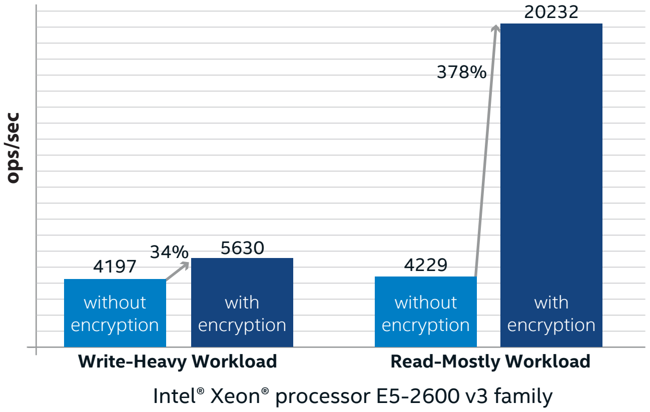
Hardware Assistance for Better, Faster Encryption

The Intel® Xeon® processor E5-2600 v3 family includes Intel® Data Protection Technology with Advanced Encryption Standard New Instructions (AES-NI) and Secure Key. These technologies are fully supported in Vormetric Data Security.

- **AES-NI** accelerates AES encryption and has been optimized for even faster throughput and lower latency on the Intel Xeon processor E5 v3 family. This processor family also includes new instructions for accelerating other cryptographic algorithms, including RSA, SHA, and ECC.
- **Secure Key** improves the quality of security keys by providing a hardware-based random number generator (RNG). This fast, scalable RNG eliminates the security gaps associated with traditional, software-based RNGs.

Faster Performance with Encryption for MongoDB

(operations/sec)



Encrypting data using Vormetric Data Security actually improved performance for MongoDB running on the Intel Xeon processor E5 v3 Family versus the same workload running without encryption.

Faster Performance with Encryption

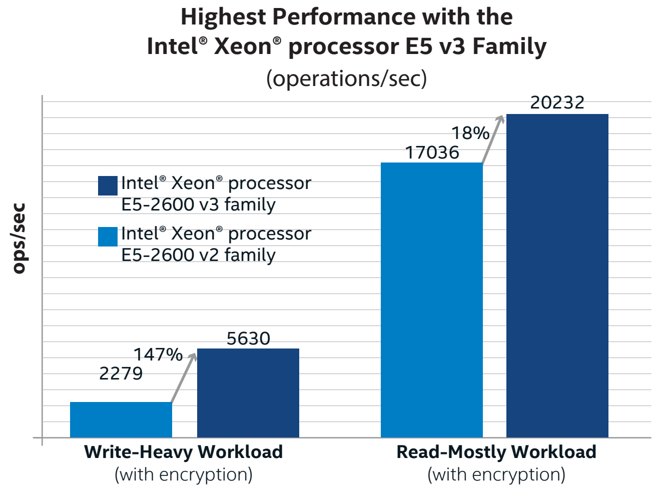
Vormetric and Intel collaborated with MongoDB to measure performance with and without encryption using MongoDB running on a two-socket server powered by the Intel Xeon processor E5 v3 family. Two different workloads were used.

- **Write-Heavy Workload** (50 percent reads/50 percent writes). Corresponds to applications, such as session stores, that record significant amounts of data.
- **Read-Mostly Workload** (95 percent reads/5 percent writes). Corresponds to applications, such as photo tagging, that record only small amounts of data.

The performance results showed that encrypting the data actually improved database performance by up to 34 percent for the write-heavy workload and by up to 378 percent for the read-mostly workload.[1]

These large gains are due to Intel AES-NI, along with Vormetric optimizations to the Linux kernel that improve read performance when using the Vormetric layered file system. The optimizations eliminate non-essential work, while preserving correct functionality. They also improve efficiency for "read ahead" operations, which identify and load data for upcoming sequential reads.

MongoDB, Vormetric, and Intel ran additional tests to determine the performance benefits of using servers powered by the Intel Xeon processor E5 v3 family versus previous-generation servers based on the Intel Xeon processor E5 v2 family. The results showed that the newer server improved encrypted database performance by up to 147 percent for the write-heavy workload and by up to 18 percent for the read-mostly workload.



Running MongoDB with Vormetric data encryption on the Intel Xeon processor E5 v3 family delivers substantially higher performance versus the previous-generation Intel Xeon processor E5-2600 v2.[1]

Based on these results, you can use Vormetric Data Security with MongoDB and the Intel Xeon processor E5 v3 family to secure your big data, while actually improving performance across a range of workloads. You can also expect substantially higher performance for your secured big data solution using the Intel Xeon processor E5 v3 family rather than previous-generation server platforms.

Learn More

- Vormetric Data Security: **www.vormetric.com**
- Intel Xeon processor E5 v3 family: **www.intel.com/content/www/us/en/processors/xeon/xeon-processor-e5-family.html**
- MongoDB NoSQL Database: **www.mongodb.com**

Vormetric mongoDB

Software and workloads used in performance tests may have been optimized for performance only on Intel® microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products.

[1] Source: MongoDB, Vormetric, Intel performance tests, August 2014. Throughput with and without Vormetric Transparent Data Encryption was measured using the Yahoo Cloud Serving Benchmark (YCSB) on two different systems. The baseline system was an Intel production server with 2 x Intel® Xeon® processor E5-2670 v2 (2.5 GHz). The new system was an Intel production server with 2 x Intel® Xeon® processor E5-2697 v3 (2.6 GHz). Both systems had identical configurations: 64GB memory, Raid-0 (128 K Stripe size; write policy: write through; I/O policy: Cached) with 4 x 800 GB Solid State Drives, EXT4 filesystem, Red Hat Enterprise Linux 6.5.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics ofany features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request. Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order. Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel's Web site at www.intel.com.

*Other names and brands may be claimed as the property of others. Printed in USA 0814/KE/MESH/PDF ♻ Please Recycle 331106-001US