Violin MEMORY

vMOS Encryption

Violin Memory Operating System (vMOS) delivers data encryption at the speed of memory. Meet stringent data protection standards without compromising application performance.

Highlights

Data Encryption at the Speed of Memory

- Built-in AES-XTS 256-bit data-at-rest encryption and passphrase protected authorized access
- Hardware acceleration to deliver up to 1 Million encrypted 4 KB IOPS and sub-millisecond latencies for applications accessing encrypted data
- Always-on flash optimization with Violin Memory's vRAID, wide striping and wear leveling algorithms

Compliance regulations require businesses to protect all personally identifiable information, such as customer data and healthcare information, from any unauthorized access. Data needs to be protected all through the storage life cycle – during regular use of the storage and also when the storage is serviced, repurposed or returned. Storage administrators face the challenge of complying with these regulations while simultaneously ensuring low administrative overhead in managing the storage and enabling high-speed access to data for all applications and consumers.

Comprehensive Flash Storage Management

The Violin Memory Operating System (vMOS) delivers the industry's leading flash optimized storage management solution. vMOS empowers administrators to monitor, manage, and configure Violin flash Memory Arrays anywhere, anytime, with full visibility into all components of the array.

vMOS Encryption extends the data protection capabilities of the Violin Memory flash Arrays to provide high performance data-at-rest encryption across the entire array. vMOS Encryption works seamlessly in the data path to encrypt all writes before the data is written to flash and to decrypt the data that is being read off flash, providing:

- Built-in data-at-rest encryption for complete data protection
- Passphrase protection for reliable access authorization
- Sub-millisecond latencies for all access to encrypted data
- Always-on flash optimization for high performance and endurance

Built-in Data-at-Rest Encryption

vMOS Encryption uses AES-XTS 256-bit algorithm, as outlined in the IEEE 1619 encryption standard and as required by most leading compliance regulations such as HIPAA and FIPS. vMOS uses a combination of two encryption keys to encrypt every write before it is written to Violin Intelligent Memory Modules (VIMM). The data on the VIMM cannot be decrypted without the encryption keys – this protects the data from any unintended access in the event of a VIMM reuse or theft.

Administrators have the flexibility to enable passphrase protection to prevent any unauthorized access to the array. vMOS Encryption validates the passphrase every time the array is powered up and uses the passphrase to protect the encryption keys. Without the correct passphrase, vMOS locks out access to the array and all the data contained in the array.

©2013 Violin Memory, Inc. All rights reserved. These products and technologies are protected by U.S. and international copyright and intellectual property laws.
Violin Memory is a registered trademark of Violin Memory, Inc. in the United States and/or other jurisdictions.

Hardware-Accelerated Data Protection

vMOS Encryption does not impact array or application performance. The Violin Memory 6000 series encryption-ready arrays are powered by high-performance internal Memory Gateways. The higher computing power of these gateways, coupled with all the performance capabilities of the Violin flash Memory arrays, delivers up to 1 Million encrypted 4 KB IOPS and provides sub-millisecond latencies to applications – even with encryption enabled.

Always-on Flash Optimization

vMOS Encryption seamlessly integrates with and complements vMOS key features. Violin Memory's patented vRAID algorithm for reliability, multi-level wide striping for performance, and automatic self-healing capabilities for availability are all available for encryption-enabled arrays, as well. Data encryption is always on and is transparent to all the data accesses above and all the flash operations below, supporting the complete set of storage administration operations offered by Violin Memory through CLI, WebUI as well as REST API, with no limitations or additional steps.

Key Highlights

The 2-key mechanism used by vMOS Encryption enables easy and effective re-purposing of individual LUNs in an encryption enabled array. When the array is powered up for the first time and encryption is enabled, an encryption key is automatically generated. This key is protected by the user-provided passphrase and serves as the master key for the array. Discarding the master key effectively destroys access to all data in the array, thereby enabling effective repurposing of the array without risking any unintended access to the data after array reuse.

Once encryption is enabled on the array, all the LUNs created in this array are required to be enabled for encryption. Each LUN has its own automatically generated unique encryption key, which in turn is, protected by the array's master key. The LUN-specific keys are generated, stored and managed internally by vMOS with no administrative intervention. When a LUN needs to be re-used or moved to a different business unit, discarding the key effectively destroys access to all the data stored in this LUN.

vMOS Encryption is supported with 6000 series Fiber Channel connected Flash Memory arrays, custom built with special purpose high performance internal Memory Gateways (MG2). All encryption-powered arrays are equipped with simplified key management, providing the ability to export all the encryption keys to an external location for safekeeping and backup. vMOS enforces successful passphrase validation before the backed up keys can be imported onto the array to re-enable access to encrypted data.

Violin Memory, Inc.
4555 Great America Parkway, Santa Clara, CA 94054 USA
Tel: 1-650-396-1500 • Fax: 1-650-396-1543
www.violin-memory.com