VIOLIN SYSTEMS

Security & Compliance

Violin Extreme Performance Storage Platforms

Data Security and Encryption Without Compromising Application Performance

HIGHLIGHTS

- **Encryption & Performance**
  - Built-in AES-XTS 256-bit data-at-rest encryption and passphrase protected authorized access
  - Hardware acceleration to deliver Millions of encrypted 4 KB IOPS with microsecond latency for applications accessing encrypted data
  - Always-on flash optimization with Violin's vRAID, wide striping and wear leveling algorithms

- **Standards**
  - FIPS-140-2 AES-XTS-256 (compliant)
  - HIPAA (Encryption and Decryption - 164.312(a)(2)(iv)) & 164.312(e)(2)(ii)) (compliant)

- **Selective Controls**
  - Easily dedupe, encrypt and compress data by LUN for better application optimization and data integrity. This functionality enables applications workload consolidation onto a single platform without compromising performance or efficiencies.

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.

Violin provides a software-based solution for encrypting data at rest for Violin extreme performance storage platforms and individual LUNs. Encryption at the storage platform level prevents unauthorized access. LUN-level encryption ensures even more flexible protection of sensitive data.

ENTERPRISE DATA SERVICES

Data Services are paramount for an enterprise-class storage. Resiliency, availability, flexibility, security and efficiency are table-stakes especially when data must be available to applications at all times, even during failure. In addition, functions of replication, snapshots, data reduction are required.

Concerto OS - At the core of Violin's architecture is 'Consistent Performance' enveloped and supported by powerful data services, we call this software Concerto. The Concerto OS platform drives the XVS, and FSP Systems. Powered by Violin Data Protection, Data Reduction and Flash Fabric Architecture engines, Concerto OS delivers consistent low latency and high IOPS, making Violin the right choice for primary storage. Violin's complete flash storage solution, designed from scratch, to deliver the best performance, storage efficiency, data redundancy and value. It is the first all flash storage solution that can store data at the same effective cost as enterprise disk arrays while providing the performance to be primary storage.

Concerto OS delivers consistent low latency with high IOPS with new levels of functionality and ease-of-use through enterprise class data services. It provides application consistent snapshots, replication, granular block level dedupe, and the best management in storage.

Concerto Encryption extends the data protection capabilities of the Violin storage platforms to provide high performance data-at-rest encryption across the entire array. Concerto 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-microsecond latencies for all access to encrypted data
- Always-on flash optimization for high performance and endurance

ENCRYPTION

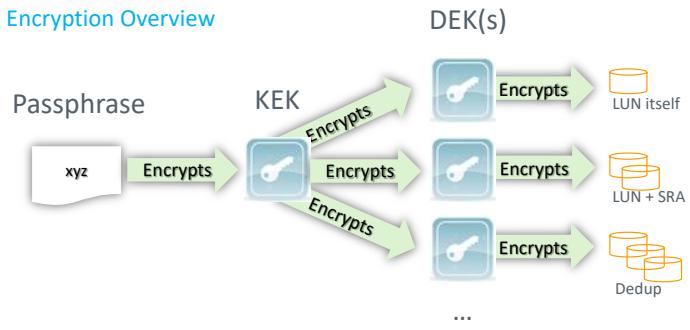
Protect Data from unauthorized access, and meet regulatory compliance

Violin enables encryption and creating encrypted LUNs using the Command Line Interface (CLI) or Violin Symphony management interface. Thin LUNs, thick LUNs and snapshots on standalone platforms and platforms (shelves) within a Violin XDR configuration are fully supported. With Concerto OS versions greater that 7.6.0, Violin offers data-at-rest encryption using OpenSSL FIPS 140-2 Object Module v2.0 validated cryptography. Encryption is supported on a per-LUN basis, meaning you have the flexibility to encrypt only specific LUNs. Each encrypted LUN is protected with its own key.

Encryption on the Violin storage platforms (both Memory Gateways) using the Concerto CLI. Once encryption is enabled, every LUN that you want to encrypt must be explicitly specified as being encrypted (except for dedupe LUNs). For dedupe LUNs, either all are encrypted, or none are encrypted. Concerto OS uses Secure Sockets Layer (SSL) and Transport Layer Security (TLS) cryptographic protocols with AES-128 (128-bit key), AES-256 (256-bit key), and RC-4 (128-bit key) algorithms to encrypt the data network connections between the host computer and the Storage Platforms. Secure Shell (SSH) protocol encrypts all traffic between the host computers and the Storage Platforms using AES-128 (128-bit key) and RC-4 (128-bit key) algorithms.

Data-at-rest encryption

Violin's 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. With 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. Concerto Encryption validates the passphrase every time the array is powered up and uses the passphrase to protect the encryption keys. Without the correct passphrase, Concerto locks out access to the array and all the data contained in the array.

Always-on Optimization

Always-on Optimization Violin Encryption seamlessly integrates with and complements the enterprise features. Violin Systems' 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 enabled per LUN 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 through CLI, WebUI as well as REST API, with no limitations or additional steps.

Key Management & LUN Flexibility

The 2-key mechanism used by Concerto 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, encrypted LUN's are not loaded until user loads then using the passphrase because encryption KEK is protected by the user-provided passphrase and serves as the master key for all the encrypted LUNs. 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, 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 Concerto 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.

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. Concerto enforces successful passphrase validation before the backed-up keys can be imported onto the array to re-enable access to encrypted data.

