VEXATA VX-DARE SYSTEM SECURITY WITH 256bit DATA @ REST ENCRYPTION

Comprehensive, Always-on Data Security with No Application Performance Impact

Data security remains a top priority for all organizations across many industry sectors and with the adoption of GDPR, eliminating the possibility of a data breach to protect corporate and customer data has never been more urgent. CIO's and CSO's are many times forced to implement security mechanisms that impact system performance or require complex key management schema's. Vexata has addressed this challenge directly with a data at rest encryption solution that conforms to the highest security standards, does not impact application performance and involves no complex encryption key management.

VX-DARE is a high performance, AES-256 bit Data At Rest Encryption included within the Vexata Operating System (VX-OS) and included natively within the Vexata VX-100F and VX-100M Scalable Storage Systems. When encryption mode is selected for each Drive Group (DG), all user data is encrypted using the NIST/FIPS approved AES-256-XTS based block ciphers. The Data Encryption Key (DEK) used to encrypt the data is generated internally (once during system initialization) within the hardware and never leaves the hardware/cypto-graphic boundary. The encryption is data path accelerated and hence does not incur any performance penalties. This keeps data secure at all times to protect against theft or even during drive replacement or routine hardware maintenance.

VX-DARE automates key management using a Local Key Manager (LKM). LKM automates generation and management of Authentication Key (AK); One AK is generated per array/system and is required to unlock the access to the data upon system bootup. Authentication Key (AK) is protected by encrypting with auto-generated random "Secure Secret" (48 Bytes). Local Key manager stores the encrypted authentication key (EAK) on the Enterprise Storage Modules (ESM). Local Key manager also protects the "Secure Secret" by splitting it into multiple (16) fragments (called Secret Fragments) and distributed/stored in redundant format in all available ESMs. This ensures that the "Secure Secret" can be reconstructed in case of 2 ESM failures and "Secure Secret" can not be reconstructed from a single ESM thus providing protection against ESM theft or single drive theft.

VX-DARE framework is compliant with the Key Management Interoperability Protocol (KMIP), enabling integration with organizations that utilize external key manager for regulatory compliance. VX-DARE can be integrated with organic or in-organic KMIP client SDK libraries and can support any centralized KMIP compliant External Key Manager.

VX-DARE provides the following benefits:

Comprehensive System Security

- Protection against drive, ESM (Enterprise Storage Module) theft
- Protection when decommissioning or maintenance of ESM's or NVMe drives
- Encryption is implemented as a system level, does not require Self-Encrypting Drives (SEDs)

Power, Performance and Simplicity

- No performance, throughput or system scaling impact and no change to the useable capacity of the system
- No application changes or re-configuration; VX-DARE is always-ON
- Simplicity of automated key management when used with Local Key Manager
- Integration with KMIP compliant external key management systems
- Support for all supported storage media, NVMe SSDs, Storage Class memory and Intel Optane

ABOUT VEXATA:
Vexata is the leader in active data management solutions. Vexata's unique breakthrough enterprise offerings enable transformative performance and scale from database and analytics applications. With unparalleled ability to consume the latest in media like NVMe Flash and now with Intel Optane™ SSDs, Vexata systems deploy simply and seamlessly into existing storage environments. Learn more at www.vexata.com