Datrium™

Blanket Encryption Datasheet

Datrium Benefits

- Only Converged Platform with FIPS 140-2 Cryptographic Certification
- In-use, in-flight, and at-rest encryption
- Full data reduction with encryption enabled
- BYOD economics
- Simple to deploy
- Virtually no performance overhead

Data Security: The Threats Are Rising

The frequency of data security breaches has risen 4X over the last ten years[1], and seven of the ten largest breaches ever occurred in the year 2016[2].

The key target in most security breaches is any and all sensitive data stored by the targeted company or government agency. Consequently, encryption of data as early in the lifecycle as possible has become a critical requirement for eliminating security risk in private, public, and hybrid cloud infrastructure.

Data encryption is a compliance requirement for many companies operating in the healthcare (HIPAA), credit card (PCI DSS), financial reporting (SOX) as well as most government agencies. With threats rising, the requirement to encrypt data everywhere – from host-tostorage, between hosts, and between sites – is becoming standard for any organization that values the privacy of its data and the data of its customers.

Current data encryption solutions force a variety of tradeoffs, which drive companies into a mix of secure and unsecure deployments, or worse make the trade-offs too expensive to consider data encryption at all. For example, leading arrays and hyperconverged systems only protect data at rest and do not protect against host or network intrusions. Guest operating systems and hypervisors offer encryption at the source, but at the expense of data reduction required by the economics of modern flash storage.

A Fundamentally New & Comprehensive Approach

Blanket Encryption is a 100% software-based solution that combines always-on efficient data reduction technology with high-speed encryption end-to-end, protecting data in-use at the host, in-flight across the network and at-rest on persistent storage. Most storage arrays and hyperconverged (HCI) offerings provide hardware-dependent, self-encrypting drive (SEDs) solutions, which can only protect data at-rest.

Datrium DVX is the only converged platform that has achieved FIPS 140-2 Cryptographic Certification, utilizing the AES-XTS-256 military grade crypto algorithm.

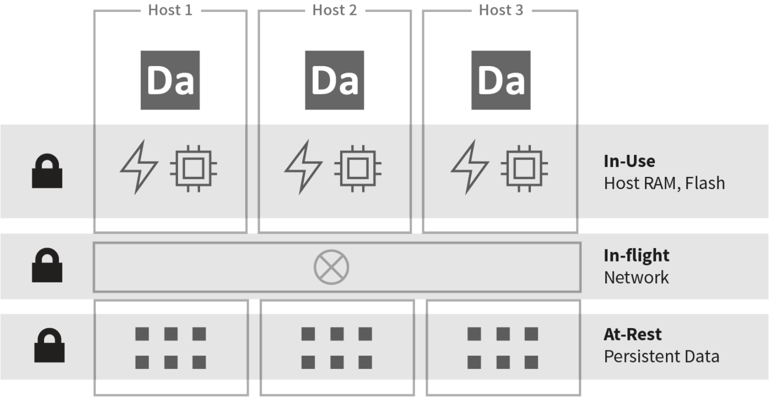
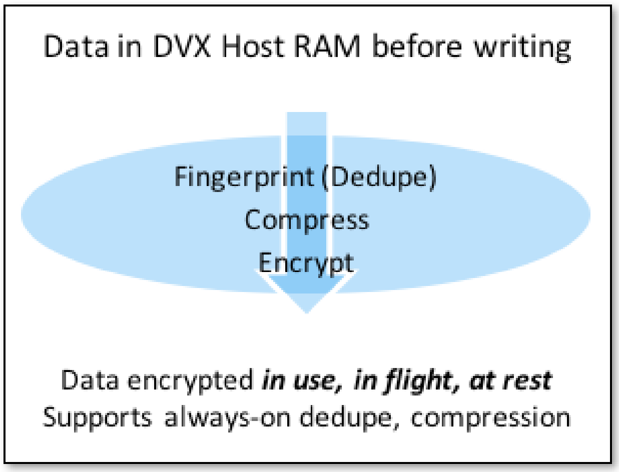


Figure 1: Industry First: FIPS 140-2 with End-to-End Encryption and Data Reduction

Blanket Encryption is the only data security solution that offers an in-flight encryption that is fully data efficient throughout the data lifecycle. Data is reduced, compressed and then encrypted as soon as it is created in the host RAM before it's written to the host flash or transmitted to the data server as fully encrypted.


Data in DVX Host RAM before writing
Fingerprint (Dedupe)
Compress
Encrypt
Data encrypted *in use, in flight, at rest*
Supports always-on dedupe, compression

While some app-based or OS-based encryption solutions offer an in-flight encryption capability, they eliminate all data reduction optimizations (storage or transfer over WAN) as they randomize the blocks before they can be data-reduced.

Simplicity and Agility

Blanket Encryption can be turned on/off at any time as desired by the customer. As a 100% software-based solution, customers have full hardware configuration freedom at Bring Your Own Device (BYOD) economics, and need not make any purchase choices upfront in order to enable encryption at a later time. With more conventional SED-based approaches, adding encryption requires the purchase of new arrays or hyperconverged systems, adding expense and silos across the private cloud environment.

DVX comes with an in-built key management service, so everything needed to turn on encryption comes standard.

Combined with a 100% software solution, customers get an integrated and cost-effective path towards data security. The internal key management service provides:

- Password & Key Rotation: security policy to change password & keys on a periodic basis.
- Lockdown Mode: an option that prompts for a passphrase upon a cold reboot before data can be accessed; useful during transportation or in case of full system theft.
- Secure Erase: wipes data so it cannot be accessed in case of part replacement or decommissioning.
- Security Officer Password: Support for fully functional second key to support security redundancy.

Server-Powered Performance

Blanket Encryption leverages the AES-NI instruction set available in all modern processors for speed, so it has virtually no impact on the VX's award-winning high performance. All data services (deduplication, compression, erasure coding, replication, snapshot and encryption) in the DVX scale in performance as hosts are added or enhanced. This means that the task of encrypting data is shared equally across all hosts in the cluster eliminating the controller-bound performance problems with software-based storage array approaches. This server-powered software-based approach virtually eliminates any performance impact of encryption.

Compromising on data security due to cost, flexibility, data efficiency, performance or residual security risks is now passé. With Datrium Blanket Encryption, an end-to-end, efficient, fast and always-secure infrastructure that addresses all the key threat scenarios above is achievable.

[1] http://www.businessinsider.com/biggest-hacks-of-all-time-chart-2016-12
[2] https://digitalguardian.com/blog/history-data-breaches