Hewlett Packard Enterprise

Data Sheet

HPE SecureStorage

Protecting Sensitive Data-at-Rest

Benefits

- Full data-at-rest protection from physical loss
- Secures Linux volumes on premises and in the cloud
- Meets compliance and audit requirements for logging, authentication, authorization and stateless key management
- Delivers infrastructure to enable an easy step to data-centric encryption and tokenization with HPE SecureData
- Eliminates the need for key storage, management and protection of keys and enables use of existing policy and access controls
- Enables storage encryption with data-centric security, central policy controls and key management for heterogeneous environments

In an era of complex privacy laws and compliance requirements, keeping sensitive data secure in a data storage environment is a high priority for IT departments. Sensitive data can contain customers' personal data, partner information and intellectual property. Lost or stolen data, especially customer information, can result in loss of trust, brand damage and competitive disadvantage.

Enterprises are storing and accumulating large volumes of sensitive information in Hadoop and cloud applications, where the data is often replicated and stored in multiple areas and accessible to a wide range of business systems, users and partners. Hadoop and cloud are inherently insecure and pose many unique challenges to properly securing data within these environments. Enterprises need to make certain that sensitive data is encrypted so it is protected at rest, especially with the reduced physical and logical access controls of many environments. Encryption at the storage level protects physical, virtual and cloud-based Linux volumes while enforcing security policies surrounding data access.

Fully securing the enterprise environment is essential to mitigate potentially huge data vulnerabilities. High performance data-at-rest protection with volume encryption combined with stateless key management is critical in securing large volumes of sensitive data for unwanted access and distribution.

HPE SecureStorage

HPE SecureStorage protects sensitive data-at-rest. HPE SecureStorage uses the native Linux dm-crypt along with HPE Stateless Key Management to protect data stored on Linux volumes. Also included is support for Transparent Data Encryption (TDE) in Hadoop, enabling granular access control for data-at-rest.

HPE SecureStorage protects against data loss in the case of media theft removal and hardware repair which often occurs in Hadoop, and large data stores due to frequent disk repairs and swap-outs. HPE SecureStorage provides a secure way to maintain control of the data by incorporating stateless key management in which the key is never persisted or written to the disk. Encryption keys are derived as needed, and all key requests are logged. This protects against unauthorized authentication of the key request to personnel who may have physically obtained the disk from being able to read any data from it. This is a useful control when there are frequent disk repairs and swap-outs and even in the event of an unwanted theft. HPE SecureStorage with HPE Stateless Key Management enables consistent data

HPE Stateless Key Management: Transparent, Dynamic, Role-based

HPE Stateless Key Management securely and mathematically derives any key, as required by an application, once that application and its users have been properly authenticated and authorized against a centrally managed policy. HPE Stateless Key Management reduces IT costs and eases the IT administrative burden by:

- Eliminating the need for a key database, as well as the corresponding hardware, software and IT processes required to protect the database continuously or the need to replicate or back up keys from site to site.
- Easily recovering archived data because keys can always be recovered.
- Automating supervisory or legal e-discovery requirements through simple application APIs, both native and via web services.
- Maximizing the re-use of access policy infrastructure by integrating easily with identity and access management frameworks and dynamically enforcing data-level access to data fields or partial fields, by policy, as roles changes.

ownership and control while meeting compliance and audit requirements. Data-at-rest stored in volumes is protected and only authorized machines can access it.

For customers electing to initially use only the HPE SecureStorage data-at-rest option, HPE Security - Data Security also provides the ability to grow your capability and expand your protection in the future with HPE SecureData and HPE SecureData Suite for Hadoop. HPE SecureData is a comprehensive end-to-end data protection framework that secures data as it is captured, processed, and stored across a variety of devices, operating systems, databases and applications. HPE SecureData is comprised of industry-standard, next generation HPE Format-Preserving Encryption (FPE), HPE Secure Stateless Tokenization (SST) and HPE Stateless Key Management technologies.

How HPE SecureStorage Works

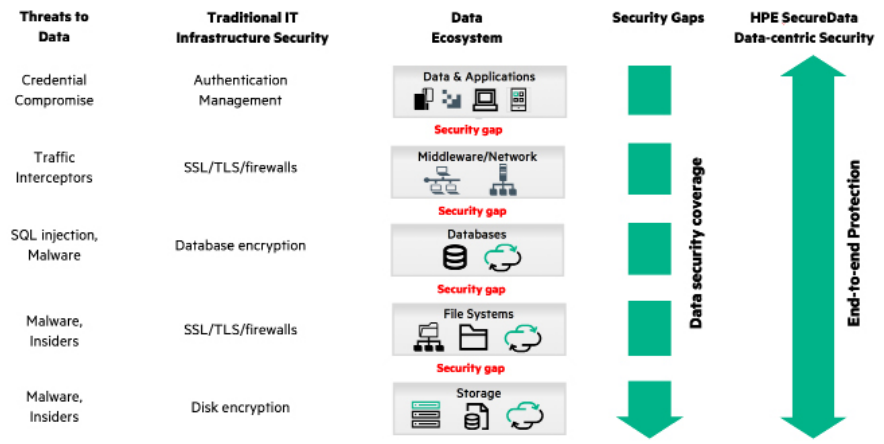
HPE SecureStorage protects data stored on Linux volumes when used in the data-center or cloud environments, including Enterprise Linux servers, and Hadoop. For HDFS (Hadoop Distributed File System), HPE SecureStorage can replace the key management service (KMS) provided in Hadoop, with the HPE Stateless Key Management solution. This Stateless Key Management solution provides a complete set of capabilities for authentication, authorization, and event logging.

HPE SecureStorage is a solution for managing data encrypted by dm-crypt through HPE Stateless Key Management. In a system without HPE SecureStorage, the keys used by dm-crypt are stored in a file local to the disk. HPE SecureStorage lets you avoid the risk of storing the keys with the disk by deriving keys from the HPE SecureData Key Server. This key is used by dm-crypt to decrypt the partition at volume mount time. Although no key is ever stored on disk, encryption and decryption can still occur without any user interaction.

HPE SecureStorage also helps centralize control of machines that are authorized to access data on protected volumes. Enterprises can control and manage data access based on the machine. The advantage of HPE SecureStorage volume-level encryption versus other tools is that it uses the same key servers and encryption infrastructure as HPE SecureData, enabling simplified and consistent key management across the organization.

HPE SecureStorage can be installed in the following storage volumes running:

• Ubuntu 12.04 LTS • RedHat 6.2 • CentOS 6.2 • SuSE 12



For more information:

voltage.com

http://hpe.com/software/datasecurity

Hewlett Packard Enterprise

4AA6-0208ENW, November, 2015