Trusted Cyber Technologies

THALES
Building a future we can all trust

HPE 3PAR StoreServ and Thales CipherTrust Manager

Together, HPE 3PAR StoreServ Storage and Thales CipherTrust Manager reduce the cost and complexity of managing encryption keys across a distributed infrastructure with consistent security controls from a single point of deployment.

The Business Problem

A security breach can happen anytime, anywhere, and from both outside and inside company walls. The first line of defense against such breaches is to encrypt your data to both secure sensitive information and meet compliance mandates. For many companies, self-encrypting drives are the products of choice for use in storage environments because they mitigate risk by containing data while protecting it from unauthorized access. As the number of drives increase, however, so does the number of encryption keys, key stores, and access policies. This can significantly impact the administrative work required to manage the encryption deployments and the associated key lifecycles. To cost- effectively support such an environment and meet compliance, centralized enterprise key management must be part of the solution.

The Solution

Whenever encryption is used to protect data at rest, a strong key management system is essential for the control and preservation of the underlying cryptographic keys over the life of the data. HPE 3PAR StoreServ Storage integrates with Thales CipherTrust Manager to both reduce the cost and complexity of managing encryption keys across a distributed infrastructure with consistent security controls and automated key services from a single point of deployment.

Key Benefits

Centralize Management of Encryption Keys

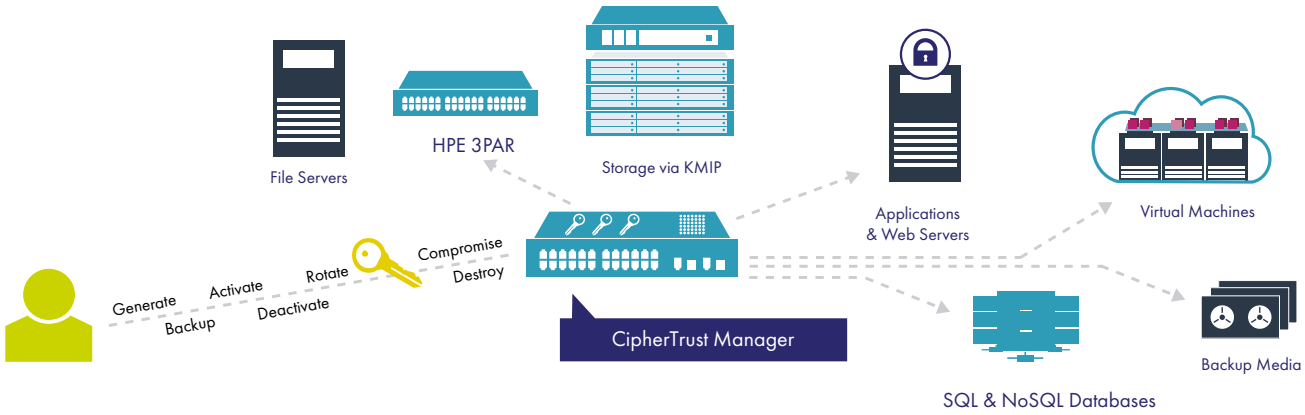
CipherTrust Manager centralizes and simplifies key management (e.g. key generation, escrow, recovery) for all HPE 3PAR self-encrypting drives and other KMIP-compatible encryption solutions while improving compliance and auditability.

Configure Data in High-Availability Schemes

Multiple CipherTrust Manager appliances can be clustered to to maintain encrypted data availability—even in geographically-dispersed data centers.

Separation of Duties

CipherTrust Manager supports segmented key ownership and management by individuals or group owners to protect sensitive material against unauthorized access from rogue staff.



HPE 3PAR StoreServ Storage

HPE 3PAR StoreServ Storage is an automated, multi-tenant storage environment that protects data at rest with encryption onto highly secure and scalable self-encrypting drives (SEDs). Data contained on these drives is protected against unauthorized access, including hardware theft, drive failure, or drive retirement. If sensitive data is stored on the HPE 3PAR StoreServ, it is recommended that users chose FIPS 140-2 Security Level 2-validated SEDs as well as a separate enterprise key management solution to centralize keys, maintain separation of duties, and satisfy compliance mandates.

Thales CipherTrust Manager

CipherTrust Manager is an encryption and key management appliance that centralizes control of disparate encryption solutions. CipherTrust Manager integrates with HPE 3PAR StorServ via the Key Management Interoperability Protocol (KMIP) to store the encryption keys for each self-encrypting drive. By consolidating the policy and key management of application servers, databases, and file servers, security administration is streamlined.

Centralized key management improves security by making key surveillance, rotation, and deletion easier as well as separating duties so that no single administrator is responsible for the entire environment. By unifying and centralizing policy management details, information is more readily accessible and demonstrating compliance with data governance requirements is easy.

CipherTrust Manager is available for sale to the U.S. Federal Government exclusively through Thales Trusted Cyber Technologies.

Benefits of CipherTrust Manager in HPE 3PAR Storage Environments

Maximize Security

CipherTrust Manager centralizes all of HPE 3PAR's key management activities, including key signing, role-based administration, and the backup, distribution, and destruction of encryption keys.

Increased Security and Compliance

Built-in auditing, logging, and alerting functions provide a non-repudiative audit trail facilitating regulatory compliance for the HPE 3PAR StorServe environment.

Reduce Costs

Automated services and a single point of management across a distributed infrastructure make it easy for enterprises to manage overhead and administrative duties costs across the storage environment.

Conclusion

Strong encryption with key ownership and management ensures that data is protected from internal and external security breaches. HPE and Thales combine to offer organizations the ability to secure data through encryption without making the management of the necessary encryption keys and policies unwieldy or difficult. This solution offers data protection without compromise. By properly securing enterprise data with FIPS 140-2 certified hardware, organizations can cost-effectively support their storage environment without increasing administrative duties or disrupting the user experience.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled. For more information, visit www.thalestct.com

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com