THALES

Building a future we can all trust

Bringing Security to High Performance Computing: Using Thales Enterprise Key Management for Panasas PanFS Encryption

PANASAS®

The Challenge

Whether used to understand complex climate and weather forces or analyze defense and military intelligence data, high performance computing (HPC) systems store and manage massive volumes of data. HPC data is often sensitive and needs to be protected from unauthorized access - both from within the organization and without.

The best way to protect HPC data is to encrypt it. However, encrypting large volumes of data can generate large numbers of encryption keys, key stores and access policies. This creates a significant administrative burden to manage both the encryption and the associated key lifecycles.

Fortunately, Panasas and Thales have teamed together to offer customers a secure option for HPC systems.

The Solution

Panasas® PanFS® on ActiveStor®

Panasas PanFS, a scale-out parallel file system, provides unprecedented bandwidth and scalability, accelerating throughput for data-intensive applications. Its excellent mixed-workload processing offers fast, nimble system performance, and its low-touch administration means one IT administrator can easily manage petabytes of storage.
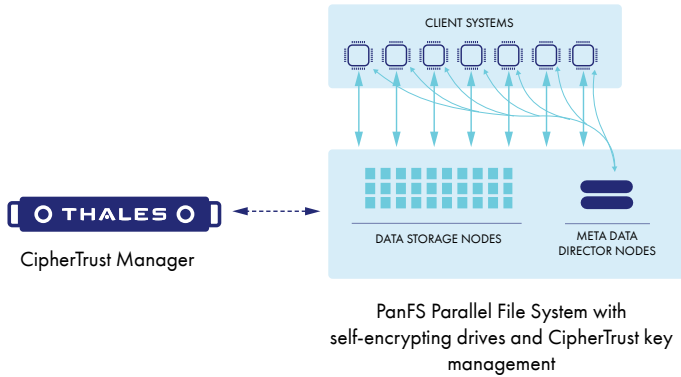
In order to protect sensitive data at rest, Panasas PanFS, when deployed on Panasas ActiveStor platforms, delivers superior encryption with zero degradation in performance, making it suitable for critical applications.

Thales CipherTrust Manager

It is paramount for organizations to properly manage and secure the encryption keys for their sensitive data. Panasas PanFS integrates with Thales CipherTrust Manager for enterprise encryption key management in order to mitigate the threat of unauthorized access to encrypted data.

Thales' CipherTrust key management platform provides robust encryption key security and rich administration features to satisfy compliance requirements and ensure best practice security. Panasas PanFS self-encrypting drives stores its keys externally in CipherTrust Manager where it is managed for its entire lifecycle. Centralizing key storage and management improves security by making surveillance, rotation, and deletion easier. Policy and role based access control features allow organizations to separate duties so that no single administrator is responsible for both data and the keys securing that data. Additionally, unifying and centralizing policy management, logging, and auditing makes information more readily accessible when demonstrating regulatory compliance.

CipherTrust Manager

PanFS Parallel File System with self-encrypting drives and CipherTrust key management

About Panasas

Panasas delivers high-performance computing (HPC) data storage solutions that support industry and research innovation around the world. Whether it's building the next Dreamliner, winning a Formula One race, creating mind-bending visual effects, curing disease, or modeling climate change, the world's leading companies trust Panasas to support their most innovative HPC projects. For more information, visit www.panasas.com.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

Key Benefits

Centralized, Streamlined Encryption Key Administration

If organizations aren't mindful, using vendor provided encryption can quickly lead to a collection of security silos. CipherTrust Manager consolidates Panasas encryption keys into an easy to use management platform where organizations administer them (e.g. key generation, escrow, recovery) with keys from a wide variety of encryption solutions including: the Thales Data Security Portfolio, self-encrypting drives, tape archives, Storage Area Networks, Cloud Service Provided encryption, and an ever growing list of vendors supporting the OASIS Key Management Interoperability Protocol (KMIP) standard.

Logging, Auditing, and Reporting For Compliance

CipherTrust Manager records detailed key and access information in centralized logs to simplify auditing and reporting access to data and encryption keys. Tracking this information from a centralized location gives organizations increased security around their data and the ability to readily demonstrate compliance with such regulatory obligations as PCI DSS, HIPAA, and GDPR.

Maximum Key Security with Tamper-proof Hardware.

CipherTrust Manager is available with a FIPS 140-2 Level 3 compliant hardware security module (HSM) with a full U.S. supply chain as a root of trust. HSMs offer both logical and physical security for encryption keys to ensure that they are protected from a wide array of attack vectors.