thalestct.com

THALES

Protect Your Cohesity Keys with KeySecure for Government

The Challenge

Many government storage administrators are faced with the challenge of protecting an increasing number of applications, while reducing costs and better utilizing public cloud resources. Legacy data protection solutions were not designed with today's complex environments in mind. Data protection typically consists of a complex patchwork of different products for target storage, backup software, media servers, proxies, replication, and disaster recovery. Cohesity provides the only web-scale platform that was designed from the ground up to consolidate this secondary data into one easily managed solution. Its simplicity consolidates backups, files, objects, test & development resources, and analytics in one hyperconverged solution for maximum speed and flexibility.

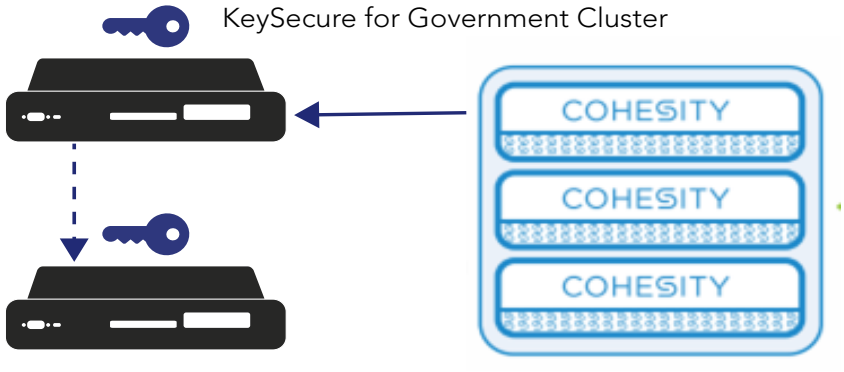
With a full understanding of the daunting risks associated with storing secondary data, Cohesity also designed in security from the ground up. The Cohesity file system provides full data-at-rest encryption using the FIPS-approved AES-256 encryption algorithm. Implementing a two-level key hierarchy, Cohesity uses Data Encryption Keys (DEKs) to encrypt and decrypt the data, and secures the DEKs with higher level Key Encryption Keys (KEKs). Storing these KEKs securely is paramount to the protection of the stored data, but how can these critical keys be stored securely? Storing them locally with the data is like locking a door and leaving the key in the lock.

The Solution

Cohesity implemented support for the Key Management Interoperability Protocol (KMIP) in their secondary storage solution. By supporting KMIP, Cohesity enables their federal customers to use Thales Trusted Cyber Technologies' (TCT) KMIP-compliant KeySecure for Government key manager to serve as the hardened guardian of the Key Encrypting Keys. As a dedicated and disparate key manager, KeySecure for Government satisfies the requirement many federal agencies must meet that states keys must be stored on a different system than the encrypted data.

KeySecure for Government is available as both a hardware appliance and as a virtual platform that runs on either VMware or AWS with an optional Hardware Security Module. The hardware appliances are certified to FIPS 140-2 Level 2 or 3, depending on selected options, and the virtual platform certified to Level 1, 2 or 3, depending on the same.

With TCT's Key Secure for Government, agencies can enjoy the benefits of Cohesity's comprehensive, converged secondary storage solution, while meeting the stringent security requirements for a dedicated, centralized, and hardened key management device approved for government use.



Integration Benefits

Robust, Redundant Clustering

Multiple KeySecure for Governments can be clustered to provide redundant configurations with fully replicated data.

Hardware Root of Trust

Depending on configuration, KeySecure for Government can protect keys and cryptographic operations with either an internal or network-attached HSM validated to comply with FIPS 140- 2 Level 2 or Level 3.

Virtual Version Available

A virtual version of KeySecure for Government is available that is validated to FIPS 140-2 Level 1 as a stand-alone software solution, or it can optionally use a network-attached HSM for a hardware root of trust if a higher level of certification is needed.

Multi-Tenancy Support

Multi-tenancy for administrators is supported to ensure that administrators can only manage the keys within their purview.

Secure Auditing and Logging

Detailed logging and audit tracking of all key activity, administrator access and policy changes. Audit trails are securely stored and signed for non- repudiation and can be consumed by leading 3rd party SIEM tools.

A Trusted U.S.-based Source

TCT develops, sells, manufactures, and supports our core data security solutions solely within the boundaries of the U.S., thus providing a completely trusted U.S.- based source

About Cohesity

Cohesity makes your data work for you by consolidating secondary storage silos onto a hyperconverged, web-scale data platform that spans both private and public clouds. Enterprise customers begin by radically streamlining their backup and data protection, then converge file and object services, test/dev instances, and analytic functions to provide a global data store. Cohesity counts many Global 1000 companies and federal agencies among its rapidly growing customer base and was named to Forbes' "Next Billion-Dollar Startups 2017," LinkedIn's "Startups: The 50 Industry Disruptors You Need to Know Now," and CRN's "2017 Emerging Vendors in Storage" lists.

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.

Contact Us: 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