Trusted Cyber Technologies

THALES

Secure your Primera Storage System with KeySecure for Government

The Challenge

With the release of the Primera storage platform, Hewlett Packard Enterprise (HPE) raised the bar on high-end storage. Designed for mission-critical applications and large-scale consolidation for enterprises, Primera comes standard with a 100% data available guarantee. Its all-active, multi-node parallel architecture provides resilience and scaling with instant failover. And by utilizing Storage Class Memory and Non-Volatile Memory Express (NVMe), it's also built for speed.

For the security of data, Primera also offers an encryption option when the array is populated with FIPS 140-2 Level 2 Self-Encrypting Drives (SEDs). The SEDs are locked upon power-down or loss of power, and must be unlocked with an authentication key upon reboot. But where can this authentication key be securely stored? It's long been documented as a bad, or even forbidden, security practice to store this key on the same device with the encrypted data, and security-conscious government organizations know better than to do this.

KeySecure for Government, the Secure Key Management Solution

By implementing support for the Key Management Interoperability Protocol (KMIP) in Primera, HPE has provided the capability of using an external key manager that is specifically designed for the secure generation and storage of critical keys. The Thales Trusted Cyber Technologies'(TCT) KeySecure for Government key manager provides this necessary security for HPE's federal customers. As a KMIP-compliant and FIPS 140-2 Level 2 or 3 validated key manager, KeySecure generates and stores the authentication keys for Primera in a hardened, disparate appliance meeting government security mandates.

Additionally, by supporting the configuration of multiple key managers and a failover capability, Primera can also take full advantage of KeySecure for Government's fully-replicated and high-availability configuration. If the configured primary KeySecure for Government isn't available, Primera will automatically failover to other configured KeySecures, ensuring continuity and availability of data. With the integration of Primera and KeySecure for Government, your encrypted data will be available when you need it.

Thales TCT Key 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** - Thales 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.

HPE Primera Key Benefits

- **Artificial Intelligence Driven** - Powered by HPE's InfoSight predictive analytics platform
- **Always-on Availability** – HPE Peer Persistence provides continuous data availability storage for mission-critical apps.
- **Ease of Installation and Maintenance** – Primera sets up in minutes, tunes itself, and upgrades transparently.
- **Guaranteed Reliability** - Comes standard with a 100% data availability guarantee.
- **High Performance** – Primera is built with an all-active architecture built using Storage Class Memory and Non-Volatile Memory Express (NVMe).

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

About Hewlett Packard Enterprise

Hewlett Packard Enterprise is the global edge-to-cloud platform-as-a-service company that helps organizations accelerate outcomes by unlocking value from all of their data, everywhere. Built on decades of reimagining the future and innovating to advance the way people live and work, HPE delivers unique, open and intelligent technology solutions, with a consistent experience across all clouds and edges, to help customers develop new business models, engage in new ways, and increase operational performance. For more information, visit: www.hpe.com.