Solution Brief

Secure Edge Data with Multi-Layer Encryption through HPE Edgeline and Thales TCT CipherTrust k160

thalestct.com

THALES
Building a future we can all trust

The HPE Edgeline EL8000 Converged Edge System brings high-performance computing to the edge of networks, where large volumes of data are being generated but compute capability to get quick insights has traditionally been very limited. The rugged Size, Weight, and Power (SWaP) optimized design of the HPE EL8000 delivers new efficiency and creates new business models in domains across the Federal government.

Secure Edge Data with Multi-Layer Encryption

Encrypted data stored within HPE EL8000 deployments is best protected through a multi-layer approach to encryption. Users can integrate and deploy the Thales Trusted Cyber Technologies (TCT) CipherTrust k160 and CipherTrust Transparent Encryption with HPE EL8000 for a FIPS 140 Level 2 multi-layer encryption solution to protect mission critical data at the edge.

Secure and Manage Cryptographic Keys at the Edge with CipherTrust k160

CipherTrust k160 is a compact cryptographic key management platform that protects and manages cryptographic keys and associated policies used to encrypt the most sensitive data-at-rest.

CipherTrust k160 can be deployed within an HPE EL8000 chassis. It protects and manages the self-encrypting drives keys via HPE iLO within EL8000. When CipherTrust k160 is deployed, an HPE EL8000 server is restricted from booting until the key manager provides its keys.

CipherTrust k160 includes a FIPS 140 certified token or a high assurance cryptographic token as its hardware root of trust. The token hardware security module (HSM) operates as a secure root of trust by encrypting all sensitive objects (e.g. keys, certificates, etc.) in CipherTrust k160 with keys that are generated by, and reside in, the token HSM. The removable token HSM provides an easy-to-use method to support common key management scenarios such as rapid key delivery disablement, key destruction, cryptographic erase, and time of use restrictions. By simply removing the detachable token you can keep mission-critical data safe, whether in the most hazardous environment or a remote branch office.

Features & Benefits

- Removable Token HSM: The token HSM is a secure root of trust for key generation, secure key storage, and encryption/decryption. Removal of the token provides a rapid means to block key delivery to the cryptographic endpoint.
- Full Key Lifecycle Management and Automated Operations: CipherTrust k160 simplifies management of encryption keys across their entire lifecycle, including secure key generation, backup/restore, clustering, deactivation, and deletion. It makes automated, policy-driven operations easy to perform, and generates alarms for events of interest.
- Centralized Administration and Access Control: Unifies key management operations with role-based access control and provides full audit log review. Authenticates and authorizes administrators and key users using existing AD and LDAP credentials.
- Secrets Management: Provides the ability to create and manage secret and opaque objects for usage on the platform.
- Multi-tenancy Support: Provides capabilities required to create multiple domains with separation of duties to support large organizations with distributed locations or multiple companies hosted by Managed Service Providers (MSP).
- Developer Friendly REST APIs: Offers new REST interfaces, in addition to KMIP and NAE-XML APIs, allows customers to remotely generate and manage keys as well as off-load cryptographic operations from clients to the CipherTrust k160 appliance.
- Flexible HA Clustering and Intelligent Key Sharing: Provide the option of clustering physical and / or virtual appliances together to assure high availability as well as increased encryption transaction throughput.
- Robust Auditing and Reporting: Includes tracking of all key state changes, administrator access, and policy changes in multiple log formats (RFC-5424, CEF, LEEF) for easy integration with SIEM tools. In addition, customers can generate pre-configured/customizable email alerts. Audit trails are securely stored and signed for non-repudiation.

CipherTrust Transparent Encryption

Thales TCT's CipherTrust Transparent Encryption can be deployed with CipherTrust k160 to deliver data-at-rest encryption with centralized key management, privileged user access control and detailed data access audit logging. CipherTrust Transparent Encryption adds a second layer of encryption to HPE EL8000 environments.

CipherTrust Transparent deployment is simple, scalable and fast, with agents installed at operating file-system or device layer, and encryption and decryption is transparent to all applications that run above it. CipherTrust Transparent Encryption is designed to meet data security compliance and best practice requirements with minimal disruption, effort, and cost. Implementation of the server encryption software is seamless keeping both business and operational processes working without changes even during deployment and roll out.

CipherTrust Transparent Encryption works in conjunction with CipherTrust k160, which centralizes encryption key and policy management.

Benefits & Features

- Define Granular Access Controls: Role-based access policies control who, what, where, when and how data can be accessed. Access controls are available for system level users and groups as well as LDAP, Active Directory, Hadoop and Container users and groups. Easily implement privileged user access controls to enable administrators to work as usual, but protect against users and groups that are potential threats to data

- High-Performance Hardware Accelerated Encryption: Transparent Encryption only employs strong, standards-based encryption protocols, such as the Advanced Encryption Standard (AES) for data encryption and elliptic curve cryptography (ECC) for key exchange. The endpoint agent is FIPS 140 Level 1 validated, and uses the encryption capabilities available in modern CPUs to minimize encryption overhead. A distributed agent-based deployment model eliminates the bottlenecks and latency that plague legacy proxy-based encryption solutions.

- Comprehensive Security Intelligence: Identify and stop threats faster with detailed data access audit logs that not only satisfy compliance and forensic reporting requirements, but also enable data security analytics. Pre-built integration and dashboards that make it easy to find denied-access attempts to protected data are available for major system vendors.

- Zero-Downtime Data Transformation: Eliminate the downtime required for initial encryption operations by adding the Live Data Transformation option. This patented technology allows for databases or files to be encrypted or re-keyed with a new encryption key while the data is in use without taking applications off-line. There is no other data encryption solution that offers this unique capability.

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