Posted on 07 May 2024 by Karen Kelvie in CipherTrust Data Discovery and Classification, CipherTrust Data Discovery and Classification, CipherTrust Manager

Thales CipherTrust 2.15 now available

We are pleased to announce the official release of 2.15.0 CipherTrust Manager (CM), CipherTrust Cloud Key Management (CCKM) and CipherTrust Data Discovery and Classification (DDC).

New Features and Enhancements

Below are highlights from this release. See the full Release Notes here.

CipherTrust Manager (CM) v2.15.0

- Enables External CA support for Client Certificate of Luna Network HSM – Root of Trust
    - For organizations requiring use of corporate Certificate Authority, until now CipherTrust Manager (CM) only recognized Luna self-signed CAs for Luna Client Cert. CipherTrust Manager v2.15.0 allows such organizations to use their corporate Certificate Authority for Luna Client Cert.
- Introduces Key Check Value (KCV) support for symmetric keys to verify key material imported from different payment systems
    - For organizations using symmetric keys across different systems, it is crucial to verify the same key material is used, without exposing the value of the key. CipherTrust Manager v2.15.0 introduces Key Check Value (KCV) to help with integrity and key value check without exposure of key value.
- Brings more administrative operations under quorum (multiple approvers) protection
    - For organizations who want to increase their security with expanded quorum (multiple approvers) protection. CipherTrust Manager v2.15.0 introduces quorum protection coverage for the following operations:
        - Key Management
            - Archive Key
            - Recover Key (from archive)
            - Revoke Key
            - Reactivate Key
        - Changes in LDAP configuration (The source of truth for your identity should not be easily reconfigured.)
        - Download of Backups
- Improves ability for administrators to troubleshoot network traffic and flows, by providing tcpdump option

CipherTrust Manager Cloud Key Management (CCKM) v2.15.0

- Supports both asymmetric and symmetric key types in AWS BYOK for key upload, import and rotate via the API
    - For organizations requesting the ability to use asymmetric keys in addition to symmetric keys
- Introduces alternative key source for OCI EKMS (HYOK) – Luna Network HSM

        - For organizations who require an external Luna Network HSM as a key source for use with OCI EKMS
        - An alternative to using CipherTrust Manager as a key source
    - Introduces the ability to export and download the key list metadata from the AWS, Azure, Google, Oracle, and SAP cloud consoles as a CSV file, and removes the 100 key limit per page
        - For organizations that want to export and download the entire filtered or unfiltered cloud key list and KMS container (AWS Accounts, Azure Keys Vaults, Google Key Rings, etc.) metadata available on CCKM
    - Removes the limit of 100 keys per export and download on the first page of the search results for: AWS, GCP and Azure
        - For organizations that want to export and download the metadata of more than 100 keys in a single export per cloud
    - Users can now manage GCP key permissions directly from CCKM
        - For organizations requesting the ability to manage and view GCP key permissions directly from CCKM versus the GCP console
    - Enhancements to CCKM Cloud Key Discovery feature: 2 new report options + an important KMS Container management feature*
        - Reports options: Discover Only, Discover and Add
        - KMS Containers: CCKM console now displays the date the containers were added for management

    - The CCKM Cloud Key Discovery capability quickly helps customers gain visibility into the number of Azure Key Vaults and Google Key Rings in their environment. It's a useful tool that can be used during a free trial or PoC to determine how many licenses are required in addition to how many keys exist in the environment. Additionally, customers can schedule the discovery function on a regular basis to automate continuous discovery and management of new KSM Containers (i.e., Azure Key Vaults & Google Key Rings).

For a description of the additional features in this release, please see Release Notes.

For additional detail, read the full announcement at the Data Protection Technical Blog.

CipherTrust Cloud Key Management PB – Sept '23

CM Product Brief –Sept '23

CDSP Product Brief – June '23

CDSP Datasheet –Oct '23

—

CipherTrust Data Discovery & Classification (DDC) v2.15.0

DDC v2.15.0 introduces scan enhancements and secrets discovery support for over 30 secret types.

Scan enhancements

- Partial database scanning for relational databases: This feature gives customers the option to save time and computing resources when scanning large databases. Using advanced configuration, customers can define the number of rows to scan per each database. The selected rows depend on the database type, in general sorted by primary key in descending order.
- List of columns containing sensitive data available via API: This feature helps customers pinpoint columns within a database that contain sensitive data. Supported databases include: Microsoft SQL, MySQL, Oracle Database, PostgreSQL, SAP HANA, Teradata.
- Data object metadata in reports: After running a scan, metadata from the operating system and application is now shown on the Data Objects tab to provide more information about data structure as well as data ownership and access.
    - For structured data, metadata parameters include the name of the table, key source, key columns name, number of scanned rows, and catalog name.
    - For unstructured data, metadata parameters are shown from the operating system—like owner and modification date—and other parameters from the application managing the file—like creator name, creation date, modifier name, and modification date.
    - A filter has been added to the Data Objects report that allows customers to show all files related to a specific owner.

For more detail and supported databases, see Thales Docs.

Support for secrets discovery

Beginning with the v2.13.1 release, Thales expanded the capability of DDC to include secrets discovery with support for over 20 infotypes—including AES Key, Auth Secrets, and SSH keys. With the v2.15 release, 12 new secret types have been added: RSA Keys, PGP Keys, ECC Keys, and Asymmetric Keys, and database credentials for Oracle, MySQL, DB2, MongoDB, Microsoft SQL, PostgreSQL, Redis and Maria.

Secrets discovery complements CipherTrust Secrets Management powered by Akeyless to help customers discover and centrally manage secrets to reduce the risk of exposed secrets and improve security posture.

The full list of infotypes supported by DDC is available on Thales Docs.