THALES

CipherTrust Data Security Platform

Thales CipherTrust Data Security Platform is een uniforme oplossing voor gegevensbescherming en stelt organisaties in staat hun meest gevoelige data – ongeacht de locatie – te detecteren, beschermen en controleren. Het CipherTrust Data Security Platform verbetert de bescherming van gevoelige gegevens door middel van sterke toegangscontroles en gecentraliseerd sleutelbeheer. Dit platform helpt organisaties bij het oplossen van hedendaagse uitdagingen zoals de adoptie van een multi-cloudstrategie, de steeds veranderende privacyregelgeving en het toenemende risico op gegevensinbreuken door interne en externe dreigingen.

The CipherTrust Data Security Platform bestaat uit drie onderdelen. Discover richt zicht op het vraagstuk waar gevoelige informatie zich bevindt, Protect betekend het daadwerkelijk beschermen van deze gevoelige informatie en Control staat voor sleutelbeheer en de controle hierop. Alle drie de onderdelen worden hieronder verder behandeld.

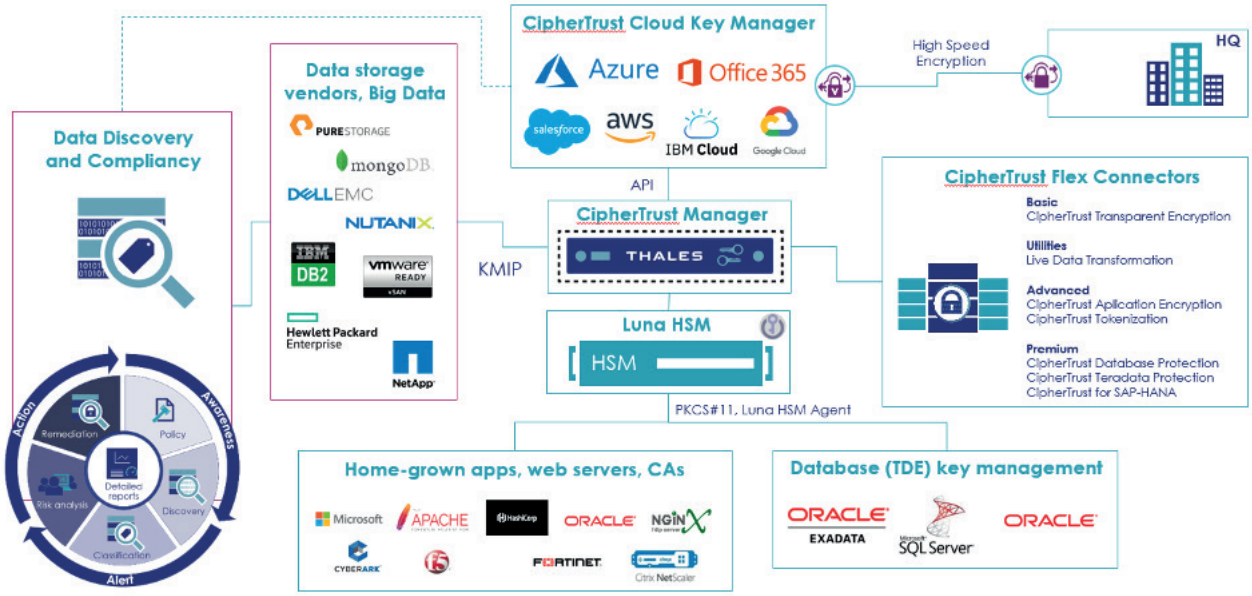
Discover

Organisaties hebben over het algemeen twee redenen om data te beschermen. 1: Security - vertrouwelijke informatie, bijvoorbeeld intellectual property, mag niet zomaar 'op straat' komen te liggen en dient goed beschermt te worden. Naast toegangscontrole op de data is beveiliging van de data van groot belang. En 2: Compliancy - veel organisaties moeten vanuit de overheid of andere instanties voldoen aan richtlijnen die zijn opgesteld voor de bescherming van bijvoorbeeld persoonsgegevens. GDPR is binnen Europa een goed voorbeeld. De uitdaging die veel organisaties vervolgens hebben is, waar bevindt zich deze data die volgens die richtlijnen beschermd moet worden? Organisaties beschikken over veel data en het is ondoenlijk om dit handmatig te bepalen. Met Thales Data Discovery and Classification kan op een veel snellere manier bepaald worden of een bepaalde data store informatie bevat die bijvoorbeeld volgens de GDPR richtlijnen beschermd zou moeten worden.

Protect

Weten wat er beschermd moet worden is de volgende stap in het beveiligen van data. Deze stap kan uit de Discover fase komen, maar kan natuurlijk ook bepaald worden door beleid van de klant en kennis over de eigen omgeving. In deze fase wordt CipherTrust Manager ingezet voor Enterprise Key Management en de diverse oplossingen (connectoren) voor encryptie, tokenization en Cloud Key Management.
Door gebruik te maken van CipherTrust Manager is de organisatie in staat om diverse vraagstukken die betrekking hebben op beveiliging van data en het gerelateerde Key Management in te vullen met het CipherTrust Data Security portfolio; CipherTrust Manager is het hart van dit portfolio. Centraal beheer van sleutels en diverse encryptie oplossingen zal de organisatie helpen om haar doelstellingen met betrekking tot data beveiligen beter onder controle te krijgen en hiermee een centrale dienst te hebben van waaruit Key Management voor de gehele organisatie geregeld en gecontroleerd kan worden. Dit laatste is met name belangrijk voor externe Auditors. Zoals gezegd biedt CipherTrust Manager verschillende encryptie en tokenization oplossingen die in de toekomst ingezet kunnen worden. Deze oplossingen (connectoren) zullen in een volgend hoofdstuk verder behandeld worden.

Control
Als we spreken over control kan dit van twee kanten worden bekeken. In de eerste plaats is er (gecentraliseerd) controle over sleutelbeheer, encryption en tokenization policies. Het CipherTrust Manager Platform is naast de Enterprise Key Manager ook de policy manager voor de diverse connectoren die beschikbaar zijn voor het platform voor encryptie en tokenization. Op de tweede plaats is controle van belang over wie er toegang heeft tot de omgeving en waarvoor deze persoon geautoriseerd is. Daarnaast biedt de oplossing ook controle in de vorm van audit logging.
Het CipherTrust Data Security platform is hieronder als high level design weergegeven. In het hart staat CipherTrust Manager dat als hardware appliance en/of virtuele appliance ingezet kan worden. Dit kan ook een combinatie zijn (of in de toekomst worden) door bijvoorbeeld in een eigen datacenter een hardware appliance te plaatsen (al dan niet redundant uitgevoerd) en in een later stadium bij een geselecteerd Cloud Provider een virtuele appliance aan het cluster toe te voegen. Door CipherTrust Manager aan een Luna HSM te koppelen is de oplossing FIPS 140-2 Level 3 gecertificeerd. Zonder de Root-Of-Trust van de Luna HSM is de hardware appliance momenteel FIPS 140-2 Level 2 in progress bij NIST en de virtual appliance FIPS 140-2 Level 1 in progress.



Figuur – High Level Design CipherTrust Data Security platform

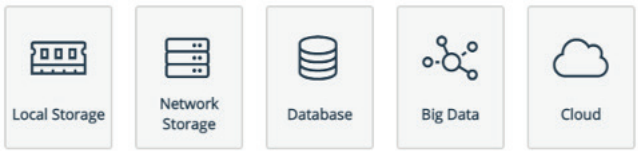
CipherTrust Manager
CipherTrust Manager vormt de basis voor het Data Security Platform. Vanuit deze basis is een organisatie in staat om centraal beheer te doen van (encryptie) sleutels en policies voor alle producten binnen het CipherTrust Data Security Platform. CipherTrust Manager vereenvoudigd het beheer van de diverse encryptiesleutels die binnen de organisatie worden gebruikt. Het genereren van de sleutel, roteren, archiveren en verwijderen van de sleutel zijn hier voorbeelden van. Vervolgens kunnen eigenaren van de sleutels via role-based access gekoppeld worden aan specifieke gebruikers en/of gebruikersgroepen waarbij een Microsoft Active Directory infrastructuur een veelgebruikte LDAP koppeling is.
Naast sleutelbeheer biedt CipherTrust Manager ook koppelingen naar leveranciers die zelf aan versleuteling van data doen en enkel een encryptie sleutel nodig hebben. Deze koppelingen vallen veelal onder Data Storage. Dit wordt hieronder verder behandeld.
Een groeiende vorm van sleutelbeheer is Key Vaults die bij Cloud Providers worden aangeboden. Deze vorm van sleutelbeheer wordt veelal Bring Your Own Key (BYOK) genoemd en valt binnen het CipherTrust Data Security Platform onder de connector CipherTrust Cloud Key Manager. Deze zal verderop in het document behandeld worden.
De verschillende encryptie en tokenization oplossingen vallen binnen de Flex Connectors en kunnen op basis van behoefte van de klant aangeschaft en ingezet worden. De meest voorkomende connectoren zullen hieronder verder aan bod komen.
Al bovenstaande oplossingen richten zich met name op Data-at-Rest. Naast bescherming voor deze

vorm van data biedt Thales ook een oplossing voor Data-in-Motion door specifieke verbindingen tussen locaties te versleutelen door middel van hardware- of virtual appliances voor bijvoorbeeld koppelingen naar Cloud omgevingen vanuit een eigen Private Cloud. Deze oplossing kan op OSI lagen twee, drie en vier versleuteling toepassen en op die manier een versleutelde verbinding opzetten tussen twee, of meerdere locaties. De performance die deze oplossing haalt gaat van 10Mb tot aan 100Gb zonder zichtbare vertraging.
Maar eerst de eerste en belangrijkste stap, Data Discovery en Compliance. De kennis die nodig is om te weten welke data onderhevig is aan compliance zal als eerste aan bod komen.

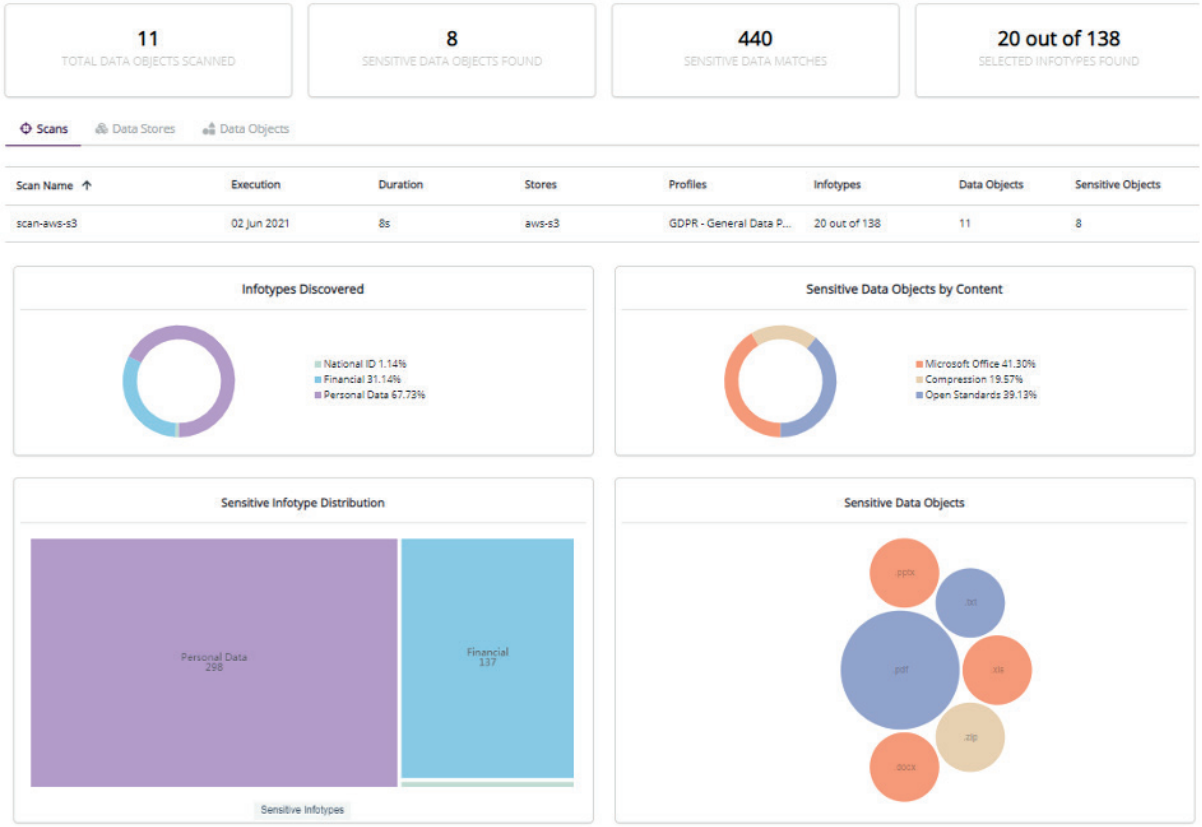
CipherTrust Connectors

Data Discovery

Data Discovery en Compliancy gaat over zoeken naar data die onderhevig is aan compliancy maatregelen. De oplossing, die vanuit de web interface van CipherTrust Manager beheerd wordt, kan op basis van een template, bijvoorbeeld voor GDPR, één of meerdere data stores onderzoeken op gegevens die onder de GDPR richtlijnen vallen. De rapportage die eruit voortkomt geeft aan in welke data store welk type data is gevonden en in welke hoeveelheid. De data stores die onderzocht kunnen worden zijn onder andere databases, fileservers op diverse platformen, storage devices, big data als ook Cloud storage.



De rapportage geeft een grafisch overzicht welk type gevoelige data is gevonden en in welke datastore. Het rapport is clickable, dus er kan via een drill down specifiek worden ingezoomd naar de data source waar de gegevens werkelijk zijn gevonden. Hieronder een voorbeeld rapport.



Er wordt gezocht op basis van zogenaamde infotypes. Een infotype kan een creditcard nummer, een paspoortnummer, een email adres, etc. zijn. Deze infotypes zijn ook zelf te definieren, dus er kan specifiek naar organisatie-eigen informatie gezocht worden.

Data Storage
Zoals eerder vermeld ondersteunt CipherTrust Manager ook diverse leveranciers die zelf de encryptie verzorgen. Veelal zijn storage leveranciers zoals NetApp, Dell EMC, HP en PureStorage. Deze versleutelen de data zelf en hebben enkel een encryptie sleutel nodig. Deze communiceren via het KMIP protocol. KMIP is een standaard voor sleuteluitwisseling waarbij het storage device de KMIP client is en CipherTrust Manager de KMIP Server. Het grote voordeel van deze methode is ook weer controle op de te creëren sleutel en de sterkte ervan. Door CipherTrust Manager zijn deze eigenschappen van de encryptie sleutel te bepalen en te beheren.

Deze toepassing voor gebruik van CipherTrust Manager is vaak de eerste stap die organisaties nemen om sleutelbeheer onder controle te krijgen en vormt zo een goede start van Enterprise Key Management.

Cloud Key Manager
Met de Cloud migratie waar veel organisaties mee bezig zijn, wordt ook data in deze Cloud omgeving geplaatst. Bescherming van deze data is dan ook op de agenda gekomen vanwege bijvoorbeeld GDPR compliance regels en, meer recent, Schrems II. Veel applicaties die gebruik maken van deze data (SaaS, Paas), maken gebruik van encryptie middelen die de Cloud Provider biedt en gebruiken veelal encryptie sleutels die in de Key Vault is gegenereerd.

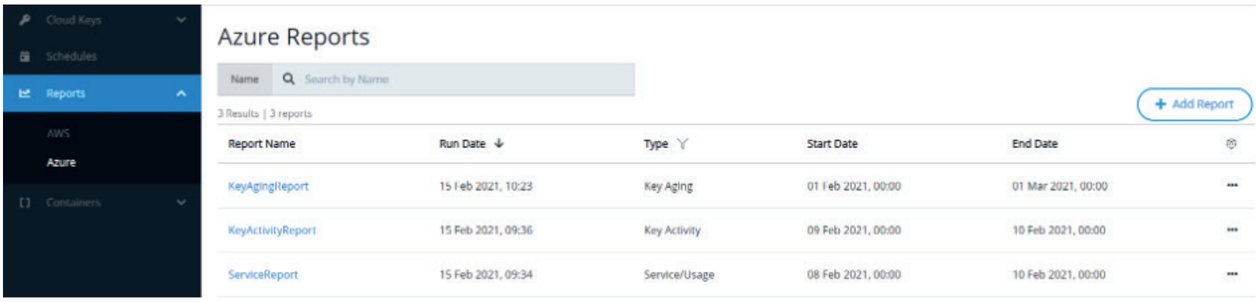
Bijkomend probleem is dat organisaties vaak eeen multi-cloud strategy erop nahouden en een Cloud Provider als Microsoft Azure meerdere Key Vaults kan bevatten met vele sleutels. Het probleem dat hierbij ontstaat is dat er geen overzicht meer is omdat de Cloud Providers geen adequate tooling beschikbaar stellen om correct beheer te kunnen doen over deze sleutels. Laat staan wanneer diensten worden afgenomen bij meerdere Cloud Providers.

Thales heeft hiervoor een oplossing in de vorm van CipherTrust Cloud Key Manager (CCKM). De klant heeft de keuze tussen een stand-alone oplossing of een oplossing die geïntegreerd is in het CipherTrust Manager platform. CipherTrust Cloud Key Manager maakt gebruik van een key source om sleutels aan te maken en in de Key Vault van de Cloud Provider te plaatsen. Deze Key source kan onder andere de Luna HSM zijn. Hieronder een additionele use-case om goed gebruik te kunnen maken van de Luna HSM oplossing.

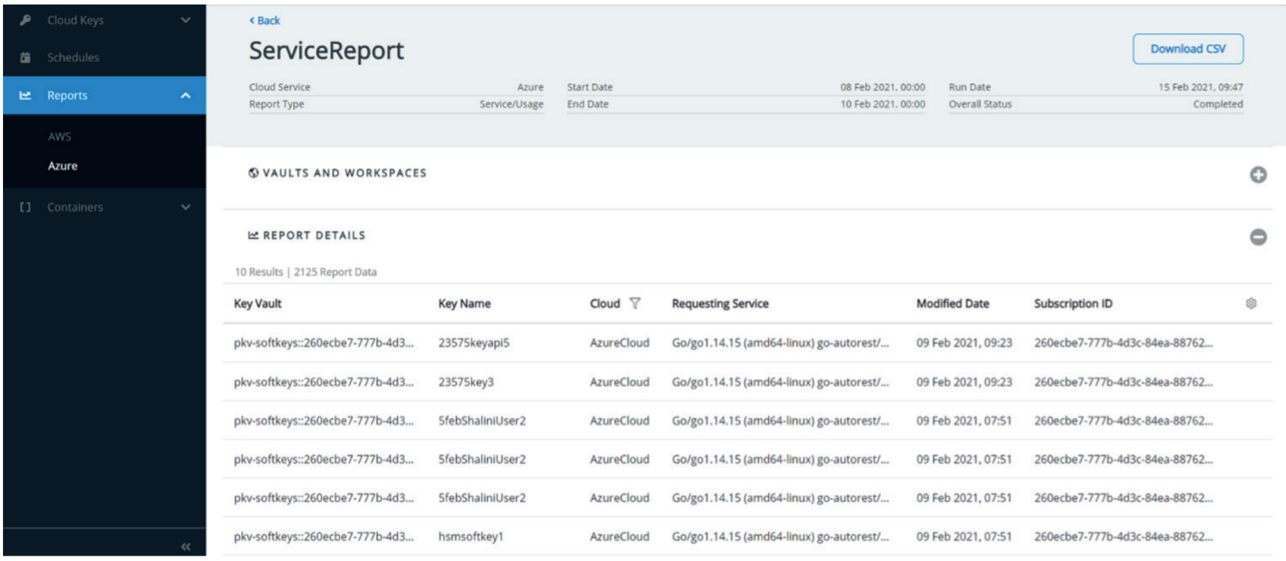
Het CipherTrust Cloud Key Management platform maakt gecentraliseerd sleutelbeheer mogelijk voor één of meerdere key vaults bij één of meerdere Cloud Providers. De op dit moment ondersteunde Cloud Providers worden hieronder weergegeven, additionele Cloud Providers staan op de roadmap en zullen in de toekomst worden toegevoegd.

- *Microsoft Azure*
- *Microsoft Azure Stack*
- *Microsoft Azure GovCloud*
- *Microsoft Azure China*
- *Microsoft Azure Germany*
- *Google Cloud*
- *Amazon Web Services (AWS)*
- *AWS GovCloud*
- *AWS China*
- *IMB Cloud*
- *Salesforce.com*
- *Salesforce Sandbox*

CipherTrust Cloud Key Manager biedt gecentraliseerd sleutelbeheer voor een (multi-) Cloud omgeving. Dus het genereren van sleutels, synchroniseren met de Cloud Key Vault, (automatisch) roteren van sleutels, (automatisch) een back-up maken van de sleutels en via rapportages gebruik inzichtelijk maken en het uiteindelijk centraal kunnen verwijderen van sleutels.
Hieronder twee voorbeelden van rapporten die mogelijk zijn. Beide rapporten zijn voorbeelden van Microsoft Azure Key Vaults.

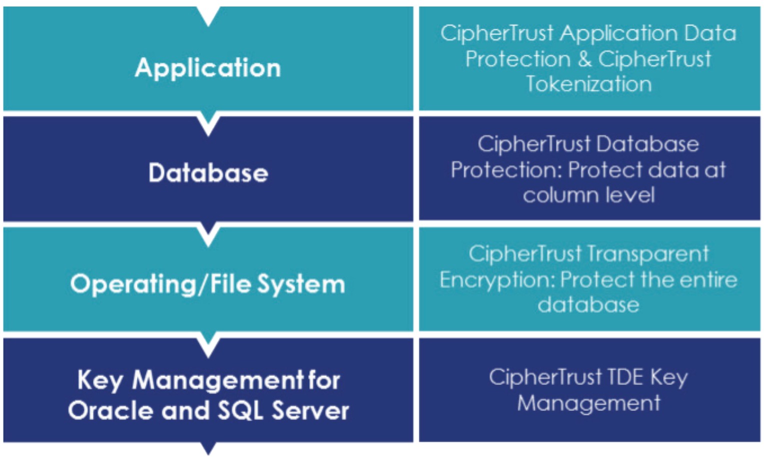


Figuur – CCKM rapport voorbeelden Azure



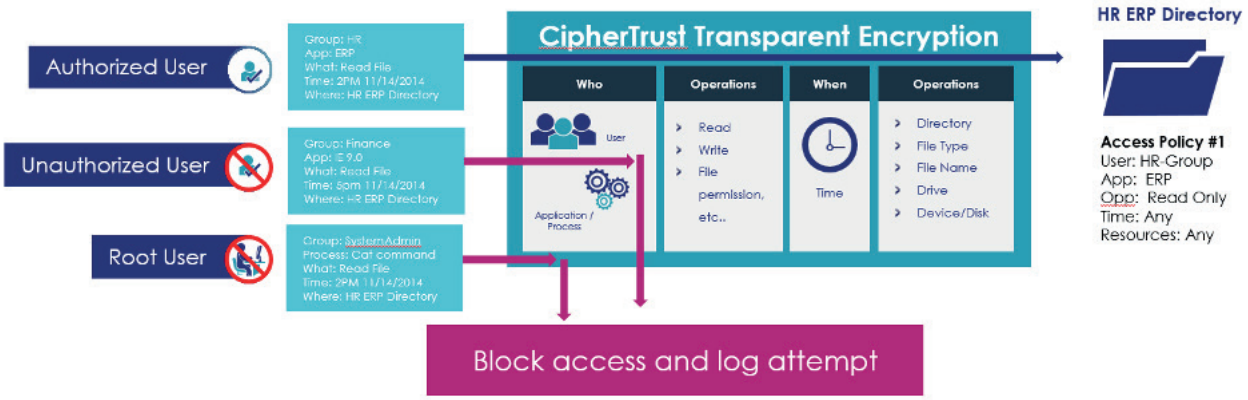
Figuur – CCKM rapport Azure Service/Usage Report

Flex Connectors
Thales biedt met het CipherTrust Manager platform verschillende connectoren die op licentie basis aangeschaft kunnen worden en naar gelang de use-case worden ingezet binnen de organisatie. Al deze connectoren worden vanuit dezelfde CipherTrust Manager interface geconfigureerd en beheerd. De meest voorkomende connectoren worden hieronder besproken.



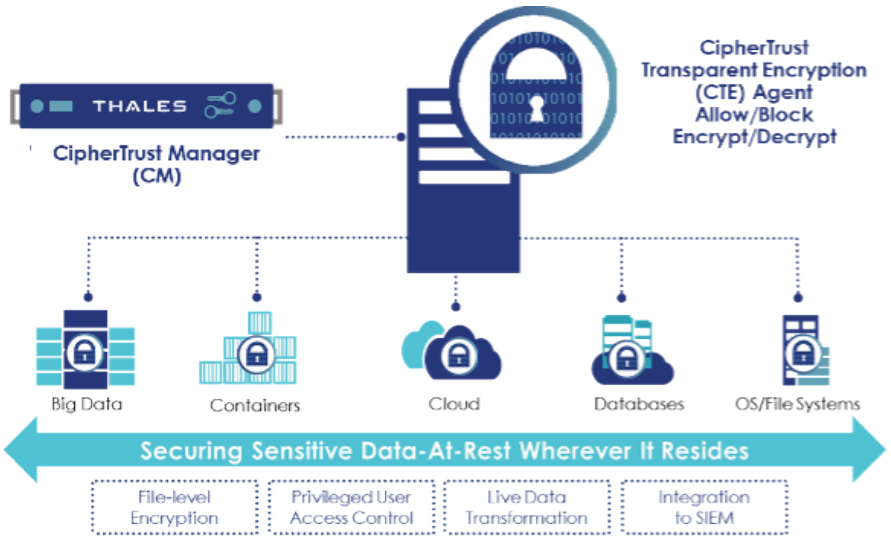
Figuur – CipherTrust Connectors

CipherTrust Transparent Encryption
CipherTrust Transparent Encrypion (CTE) is een agent die geïnstalleerd wordt binnen een server omgeving. Verschillende besturingssystemen worden hierbij ondersteunt. Het idee is dat bepaalde bestanden en folders versleuteld worden maar voor de gebruiker van deze bestanden zichtbaar blijven. Een voorbeeld is de HR afdeling. Deze afdeling heeft veel vertrouwelijke documenten die beveiligd opgeslagen moeten worden. Ook beheerders van de server omgeving zouden hier niet bij moeten kunnen. Dit is waar CTE onder andere voor bedoeld is. De policy kan zo ingesteld worden dat de HR afdeling transparant bij de documenten kan. De beheer afdeling kan ook bij de documenten, maar krijgen in de policy geen toegang tot de encryptie sleutel. Dit betekend dat ze de bestanden kunnen openen, maar enkel versleutelde content zien. Hieronder een grafische weergave van dit proces:



Figuur – CTE Bestandstoegang regels

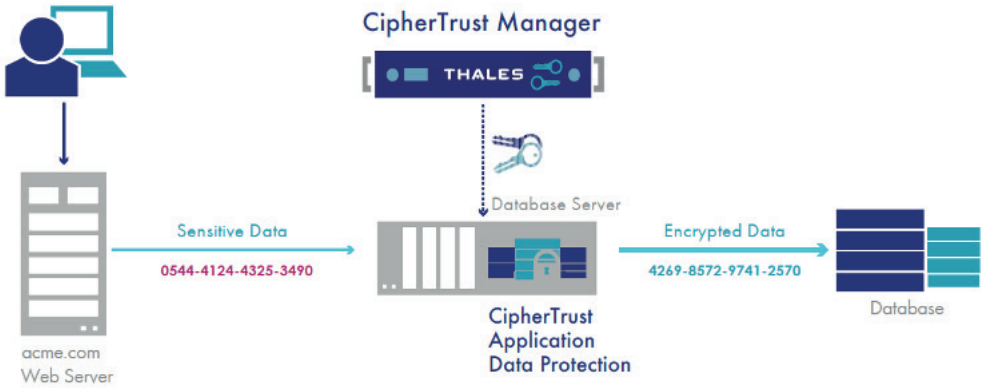
Naast documenten kan CTE ook ingezet worden voor de beveiliging van databases, Big Data omgevingen, Containers en binnen Cloud omgevingen.



Figuur – CTE implementatie mogelijkheden

CipherTrust Database Protection
Naast CipherTrust Transparent Encryption (CTE) om database bestanden te beschermen, bestaat ook de mogelijkheid om binnen een database specifieke kolommen te versleutelen. Met CipherTrust Database Protection (CDP) is het mogelijk om enkel die kolommen te versleutelen waar gevoelige informatie wordt opgeslagen. Waar CTE bedoeld is om de bestanden die het database platform gebruikt te versleutelen kan CDP binnen de database versleuteling toepassen.

De oplossing is bedoeld om:
- Encryptie transparant, op kolom niveau, binnen databases toe te passen;
- Door goed gedefinieerde toegangscontrole ervoor te zorgen dat enkel geauthoriseerde gebruikers en applicaties toegang krijgen tot de gevoelige data;
- Het voorkomen dat database beheerders (DBAs) zich als andere gebruikers voordoen om zo toegang te krijgen tot de gevoelige data.



Figuur – CipherTrust Database Protection

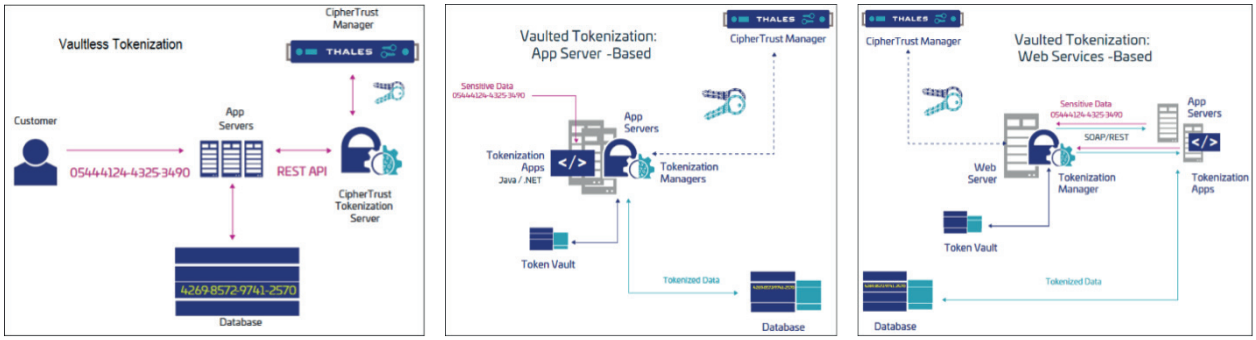
Doordat de CDP oplossing zich richt op specifieke database kolommen, kan CDP snel en op een efficiënte manier data versleutelen en ontsleutelen, eventueel met behoud van het formaat. De oplossing is Cloud-friendly waardoor deze ook binnen een Cloud imgeving ingezet kan worden.

CipherTrust Tokenization
Naast beveiliging door middel van encryption is tokenization ook een veel gebruikte oplossing om data te beschermen. Met tokenization wordt de data niet versleuteld, maar 'vertaald' naar een token. Hier kan bijvoorbeeld ook het formaat van de data behouden worden. Dus een opgeslagen creditcard nummer kan via een token worden vertaald naar een formaat dat lijkt op het oorspronkelijke creditcard nummer, maar deze niet meer is.

Figuur – Concept tokenization

Tokenization wordt veel ingezet omdat dit de kosten en moeite die nodig zijn om te voldoen aan interne policies en externe regelgevingen zoals GDPR en PCI-DSS verminderd. Omdat de gevoelige data is veranderd in een token, valt de betreffende omgeving die het opslaat veelal niet meer onder deze regelgevingen.

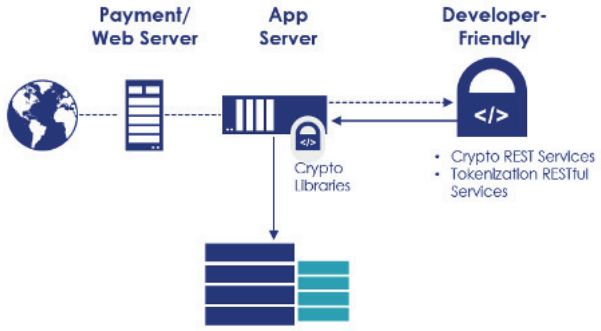
Er bestaan twee vormen van tokenization, namelijk Vaultless tokenization and Vaulted tokenization. Vaultless tokenization vindt direct vanuit de applicatie plaats en zal via een REST API de vertaalslag maken van gevoelige data naar een token. Vaulted tokenization gaat een stap verder en kan een specifiek formaat van het token maken dat voorziet in de behoefte van de klant of applicatie. Vaulted tokenization biedt het hoogste beveiliginsniveau voor de meest gevoelige data.



Figuur – Verschillende vormen van tokenization

CipherTrust Tokenization kan gevoelige data op een veilige manier anonimiseren, waar deze data zich ook bevindt. Dit kan in eigen Private Cloud omgevingen zijn, big data environments en Public Cloud omgevingen.

CipherTrust Application Data Protection
De CipherTrust Application Data Protection suite stelt applicatie ontwikkelaars in staat om direct vanuit de applicatie crypto operaties uit te voeren op data. De ontwikkelaar kan via API's sleutelbeheer, signing, hashing en encryptie services uitvoeren op de verhandelde data. Direct vanuit de applicatie versleuteling toe passen op data is de meest veilige manier van data opslag.



Figuur – Encryptie op Applicatie niveau

CipherTrust Data Security Platform
Al met al kan geconcludeerd worden dat de oplossingen die Thales biedt op het gebied van sleutelbeheer (Enterprise Key Management) en Encryptie toepassingen in zowel Private Cloud omgevingen als Public Cloud omgevingen, of een combinatie ervan, uniek zijn in de markt. Thales is de enige leverancier die van een data discovery tot aan een daadwerkelijke encryptie oplossing kan aanbieden dat beheerd wordt vanuit hetzelde management platform.
De flexibiliteit die daarmee wordt geboden kan ook als uniek worden ervaren. Of de behoefte nu ligt bij fysieke appliances, virtuele appliance, of een combinatie ervan; met het Thales portfolio kan dit ingevuld worden. De oplossing kan tot aan FIPS 140-2 level 3 gecertificeerd zijn.
De Thales CipherTrust oplossingen zorgen ervoor dat de transitie naar een Public Cloud Provider veilig kan. Hierbij wordt gevoelige data versleuteld, kunnen sleutels centraal beheerd worden en kan op regelmatige basis onderzocht worden of data nog steeds voldoet aan de regels die gesteld zijn door zowel interne auditors als externe regelgeving.

De combinatie met de Luna HSM maakt de oplossing toekomst bestendig. Het CipherTrust Manager platform kan gebruikt worden voor de diverse uitdagingen die elke organisatie heeft op het gebied van Enterprise Key Management en Encryptie toepassingen. Als deze gecombineerd wordt met de Luna HSM oplossing, die op zichzelf ook weer gebruikt kan worden voor verschillende toepassingen, wordt er direct voldaan aan de FIPS 140-2 level 3 en Common Critieria EAL4+ (eIDAS). De omgeving kan naar behoefte in de toekomst uitgebreid worden als bijvoorbeeld performance eisen veranderen en via licenties kunnen connectoren worden toegevoegd om een specifieke toepassing te beveiligen.