



CipherTrust Manager

2020년 6월 15일



- 데이터 보안 문제
- CipherTrust Manager 개요
- 고객 성공 사례
- 주요 차별화 요소
- 마이그레이션 전략

데이터 보안 문제

THALES





폭발적인 데이터 성장



데이터 유출 수 증가



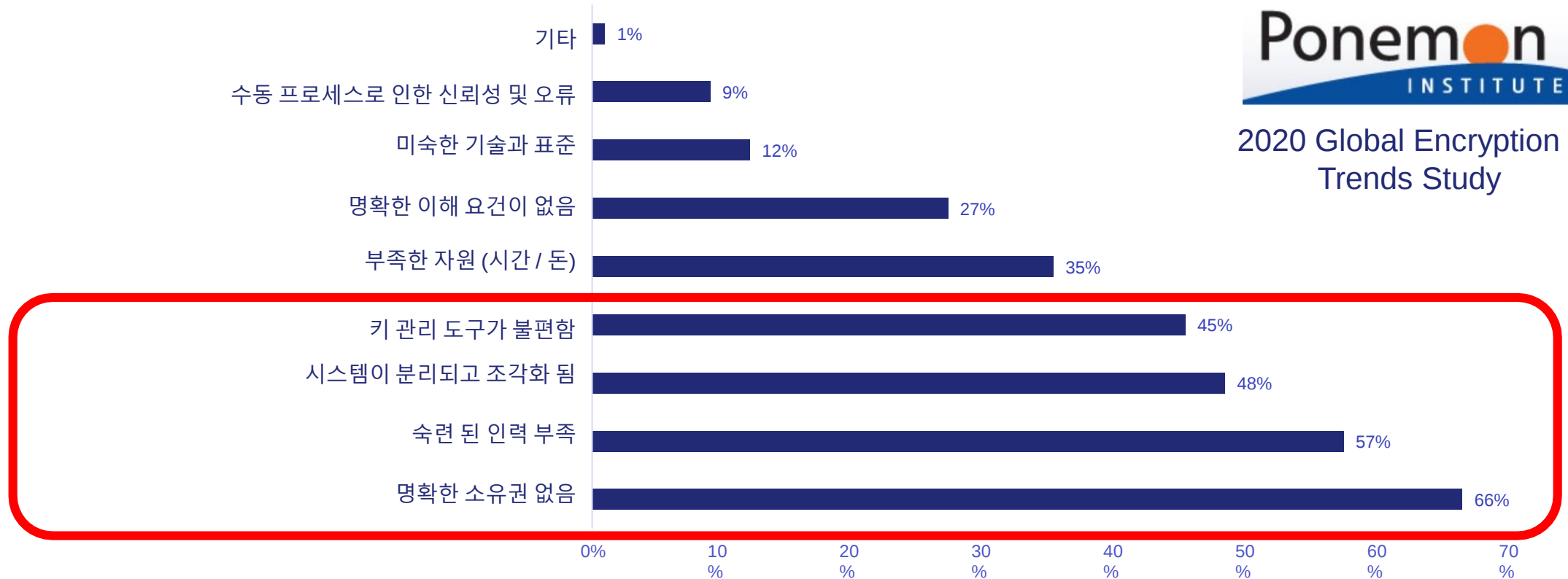
데이터 보호 복잡성



엄격한 개인 정보
보호 규정

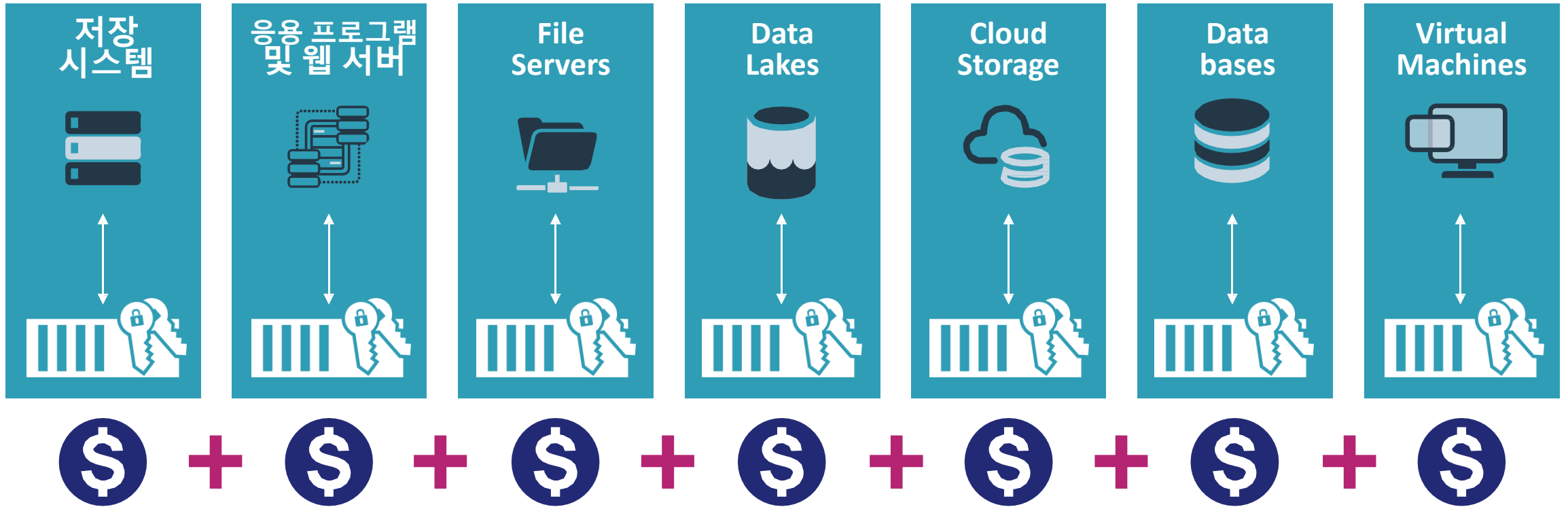
과제 : 조각난 키 관리 시스템

키 관리가 왜 그렇게 고통스러운 이유 ?



응답자의 48 %가 격리 또는 단편화된 키 관리 시스템을 중요한 과제로 인식했습니다.

비즈니스 문제 : 너무 많은 키 저장소



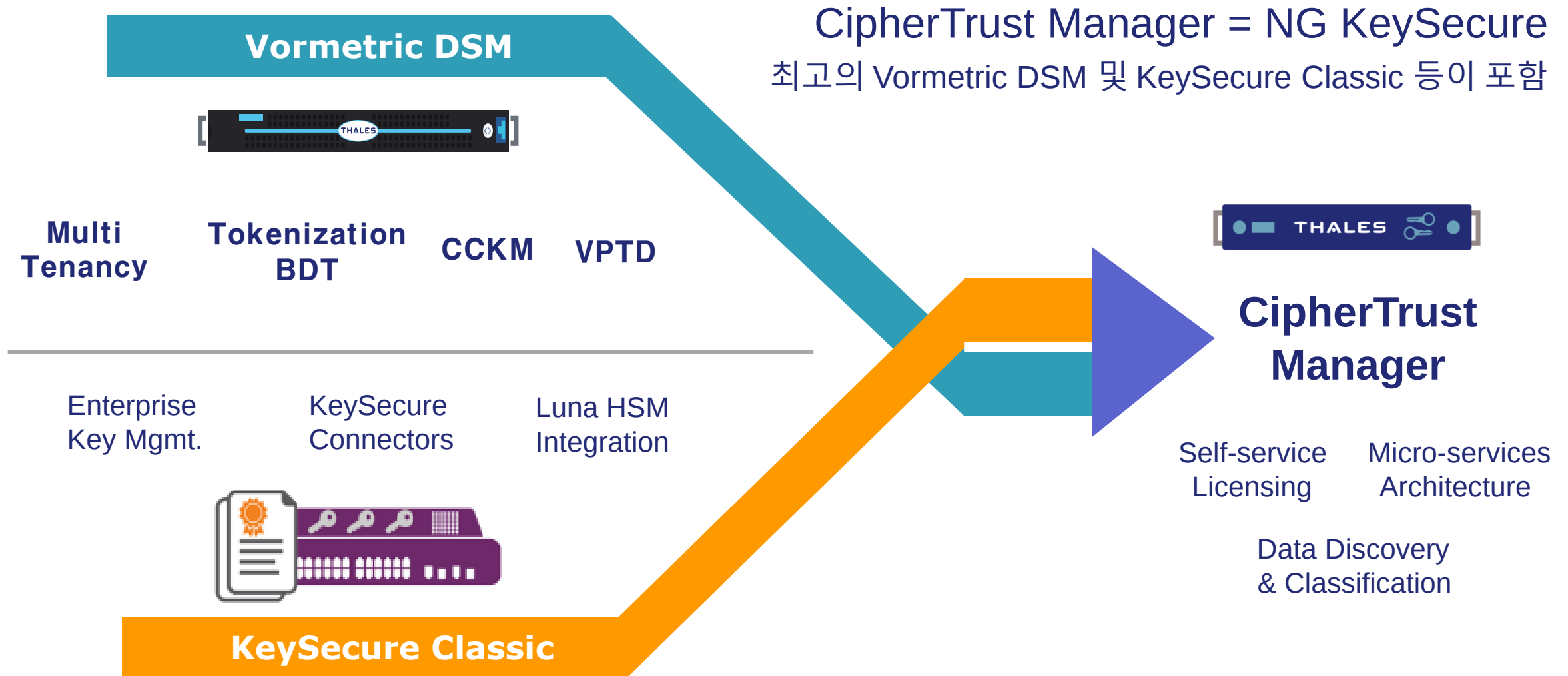
- 비용이 많이 들고 복잡한 관리
- 반복 가능한 프로세스 없음
- 감사 과제(Audit Challenge) 일관되지 않은 보안 정책 시행
- 금지된 데이터 및 비즈니스 워크 플로우 조각난 접근법 = 위험성 증가

CipherTrust Manager 개요

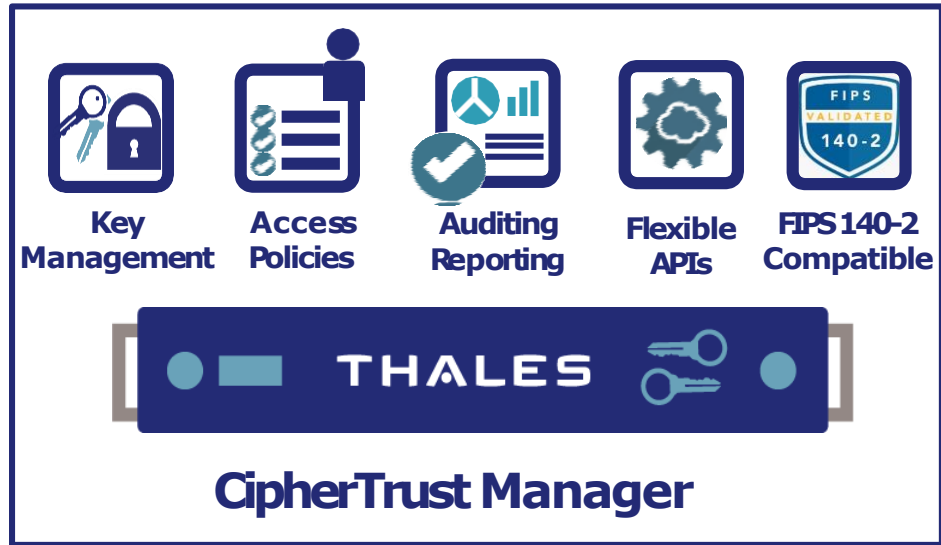
THALES



CipherTrust Manager : 차세대 키 관리



CipherTrust Manager(a.k.a Next Generation KeySecure)



- 역할 기반 액세스 정책으로 키를 중앙에서 관리
- 여러 로그 형식 및 customizable alert를 통한 향상된 감사(Audit) 및 보고(Report)
- 관리 기능을 자동화하고 프로그래밍 방식의 암호화를 허용하는 REST API
- 각각 FIPS 인증 HSM 옵션이있는 가상 또는 하드웨어 어플라이언스로 사용 가능
- 모든 Thales Data Security 제품에 대한 통합 관리 (Management) 및 관리(administration)
- 최고의 파트너 에코 시스템

CipherTrust Manager를 선택하는 이유

단순화된 관리



- Thales Data Discovery 및 Data Protection 커넥터용 통합 콘솔
- 더 나은 가시성 및 제어를 위한 셀프 서비스 라이선싱
- 자동화를 위한 개발자 친화적인 REST API

클라우드 지원 향상



- 가상 어플라이언스의 클러스터링으로 Cloud 중단에 대한 안전 장치 제공
- 여러 클라우드 공급자 지원
- 중앙 집중식 멀티 클라우드 BYOK 관리 지원

보안 및 암호화



- Multi-tenancy 지원
- 암호화 가속을 위한 내장 HSM 옵션
- HA 클러스터링이 있는 Network HSM(Luna 7)
- 주요 Cloud Provider를 위한 Cloud HSM (as-a- service) 옵션

Appliance Improvements



- High-speed interfaces 2x10G/2x1GB NICs
- 향상된 대역폭을 위한 NIC Bonding
- PED를 통한 강력한 인증

CipherTrust Appliance Specifications



CipherTrust Manager
Physical Appliances

특 징	k470	k570
최대 키 저장 수	1,000,000	1,000,000
최대 동시 세션 수	1000	1000
Network Interface Card (NIC) 옵션	• 4x1GB interfaces • 2x1GB / 2x10GB optional NICs • NIC bonding support	
FIPS140-2 인증	• Level 2 chassis	• Level 2 chassis • Level 3 w/ built-in HSM



CipherTrust Manager
Virtual Appliances

특 징	k170v	k470v
최대 키 저장 수	25,000	1,000,000
최대 동시 세션 수	100	1000
시스템 요구 사항	• HD: 100GB • RAM: 4-8 GB • NICs: 1 -2 • CPUs: 2 또는 그 이상	• HD: > 200GB • RAM: > 16 GB • NICs :2 또는 그 이상 • CPUs:4 또는 그 이상
FIPS140-2 인증	• Level 1 virtual appliance • Level 3 w/ external HSM	

CipherTrust 로 더 많은 것을 할 수 있습니다 !

KS “Connector” Coverage



SafeNet
ProtectFile



SafeNet
ProtectDB



SafeNet
ProtectAPP



SafeNet
Tokenization



ProtectV™



KMIP 1.4
Support



TDE/EKM



Data
Discovery

DSM “Agent” Coverage



Vormetric
Tokenization
Service



KMIP
Clients



CipherTrust
Cloud Key
Manager



Vormetric
Protection for
Teradata

진행중.... Q3 20 배포



Application Encryption
VAE+ProtectApp



Transparent Encryption (file/folder/etc.)
VTE (Migration 2021)

파트너 에코시스템 – FY 20 Plan

성장하는 파트너 에코시스템

2020년 상반기 인증 완료

2020년 하반기 예정

KMIP



PKCS #11



NAE-XML REST



THALES

고객 성공 사례

THALES



주요 EMEA 금융 서비스 제공 업체의 Cipher Trust Migration

고객사 개요:

응용 프로그램 및 스토리지를 보호해야 하는 유럽 (지역 및 국제 플레이어)의 주요 금융 서비스 제공 업체. 그들은 제공하는 확장 성과 유연성을 활용하기 위해 CipherTrust 플랫폼으로 마이그레이션했습니다.



주요 요구 사항

- KMIP 지원 : HCI 및 물리적 스토리지 (vSAN 등)를 보호하기 위해 KMIP를 활용할 수 있는 기능 요구
- HSM as Root of Trust: 더 높은 수준의 보안 및 키 엔트로피 제공
- 기존 시스템 지원 : 기 사용중인 Oracle TDE 지원

솔루션

- Agents: ProtectApp, ProtectFile, KMIP, Oracle TDE
- 장비 : K570, K170V
- 2020년 상반기에 DPOD과의 Integration 예정

Thales만의 차별점

- K570 어플라이언스는 2x10GB / 2x1GB 및 FIPS 인증 Luna 제공
- KMIP 및 NAE-XML과 함께 사용 가능한 REST API
- 물리적 및 가상 어플라이언스를 클러스터링하는 기능

고객사 개요 :

선도적인 클라우드 기반 IT 서비스 회사는 IT 서비스 관리 및 IT 운영 관리 공급자로 시작하여 최근 workflow 자동화로 확장되었습니다. 전 세계 6,200여 기업 고객이 IT 서비스를 사용합니다.



주요 요구 사항

- 현재 Thales KS Classic K460 사용 중
- 기존 SaaS 고객에 대한 서비스 무중단하의 키관리 확장이 필요
- REST API를 사용하여 주요 수명주기 관리를 자동화해야 함
- 새로운 플랫폼에서 레거시 NAE-XML 인터페이스 지원

솔루션

- ProtectApp (Enterprise Site License)
- 50대의 K570 (전 세계 지사에 설치)
- 12대의 K170V (application 개발용)

Thales만의 차별점

- KMIP 및 NAE-XML 클라이언트를 위한 REST API
- 더 빠른 2x10GB / 2x1GB 인터페이스를 제공하는 K570
- 물리적 및 가상 어플라이언스를 클러스터링하는 기능

1개월만에 차세대 플랫폼으로 웹 결제 애플리케이션 전환

고객사 개요 :

지능형 여행 애플리케이션을 위한 업계 최고의 결제 및 정보 솔루션 통합 서비스.
미국, 영국 및 호주에서 대중 교통 이용의 60 % 이상이 큐빅을 사용하여 가져옵니다.



주요 요구 사항

- 중앙 집중 서비스 : 사업부 전체의 암호화 및 키 관리 서비스를 표준화하여 애플리케이션의 자체 키 격납고 사용 방지.
- 보안 및 규정 준수 : 정형 및 비정형 PII (고객 / 직원) 데이터 및 지적 재산 보호.PCI DSS Compliance 달성

솔루션

- 웹 서비스를 포함한 ProtectApp
- 4대의 Azure상의 K170V (2/2 prod/test 분리)

Thales만의 차별점

- 중앙 집중 식 확장 가능 및 표준 기반 키 관리 제공
- 여러 분산 형 포인트 제품을 교체하여 운영 효율성 향상
- 에이전트 / 커넥터는 새로운 사용 사례 및 새로운 클라우드 배포 (Google)를 지원하기 위해 광범위한 적용 범위와 옵션을 제공

고객사 개요 :

약 220 만 명의 직원을 보유한 세계 최대 소매 업체. 미국에서 5,160 개 이상의 매장 운영



주요 요구 사항

> POS 데이터 암호화

신용 카드를 긁으면 공개 키를 사용하여 암호화된 다음 지정된 데이터 센터로 전송

거래를 완료하기 위해 신용 카드가 해독되고 토큰화 됨

소비자 데이터는 다양한 비즈니스 개발에 사용됩니다

솔루션

- > 암호화, 데이터 센터의 PCI 처리를 **Agents:** 상점용 앱 레벨 위한 토큰화
- > **Appliances:** 사용 중인 physical 및 virtual appliance

Thales만의 차별점

- > 신용 카드 번호 암호화로 PCI 준수 가능
- > 중앙 집중식, 확장 가능 및 표준 기반 키 관리로 효율성 향상
- > CipherTrust는 데이터 수신 즉시 웹 애플리케이션 계층에서 통합하여 데이터를 보호 할 수 있습니다

통합 관리

중요한 데이터를 검색
분류 및 보호하는 단일 창

클라우드 배포 옵션

VMware, AWS, Azure,
Google Cloud 및
기타 클라우드 지원

FIPS 140-2 지원

HSM이 내장 된 FIPS 140-2
레벨 3 호환 물리적
어플라이언스로 사용 가능

최고의 파트너 생태계

주요 엔터프라이즈, 스토리지,
서버 및 SaaS 공급 업체와 통합

개발자 친화 API

키 관리 및 암호화 작업을
자동화하는데
사용할 수 있는 REST API

고급기능

더 나은 가시성 및 제어
및 Multi-tenancy 지원을 위한
셀프 서비스 라이선싱

CipherTrust Manager의 주요 차별성

THALES

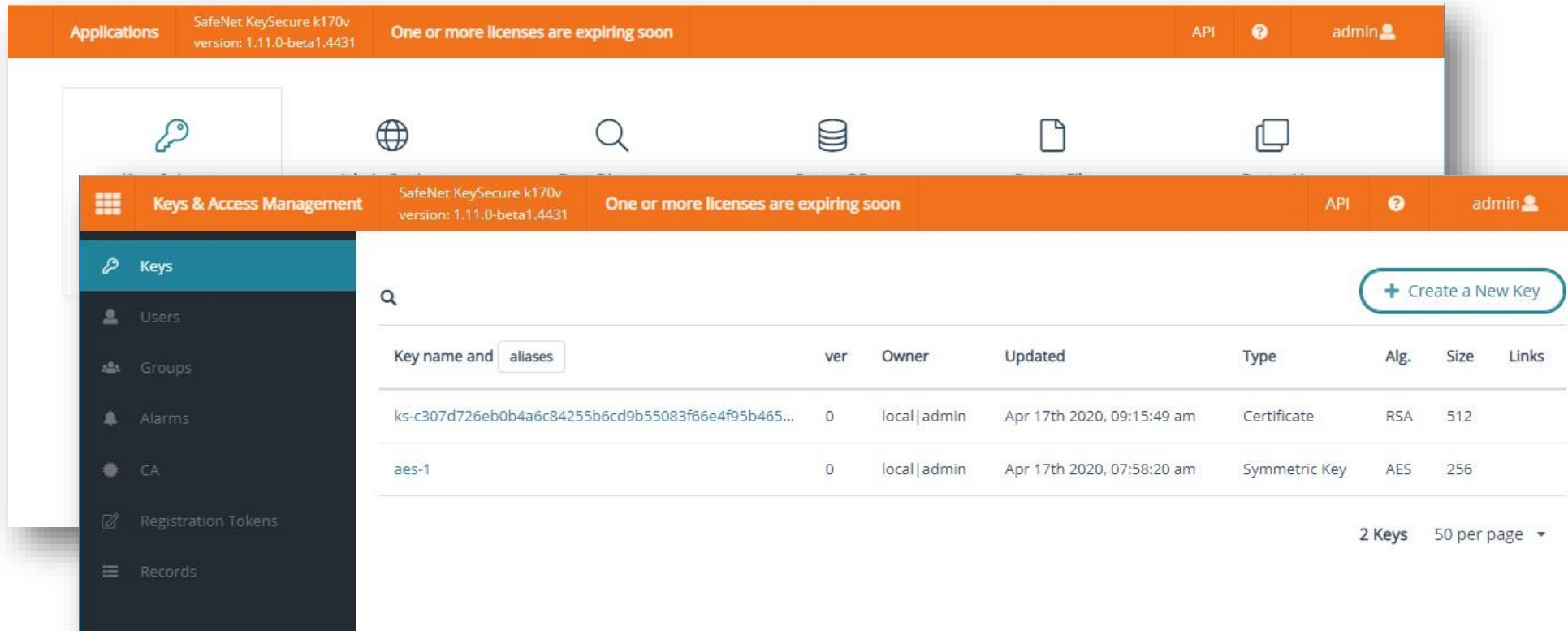


- 새로운 **GUI**를 통한 단순화 된 관리
- 더 나은 가시성 및 제어를 위한 셀프 서비스 라이선싱
- 확장된 **HSM** 옵션
- 업무 분리를 통한 **Multi-tenancy** 지원
- 개발자 친화적인 **REST API**
- **Cloud**지원 향상
- 향상된 모니터링 및 레포팅 기능

새로운 GUI로 관리의 단순화

일반적으로 사용되는 기능에 대해 간단하며 사용하기 쉬운 환경을 제공합니다

- 업무 분리를 통한 주요 수명주기 관리 및 세분화 된 액세스 정책
- Thales Data Discovery 및 Data Protection 커넥터 관리를 위한 통합 콘솔



더 나은 가시성 및 제어를 위한 셀프 서비스 라이선싱

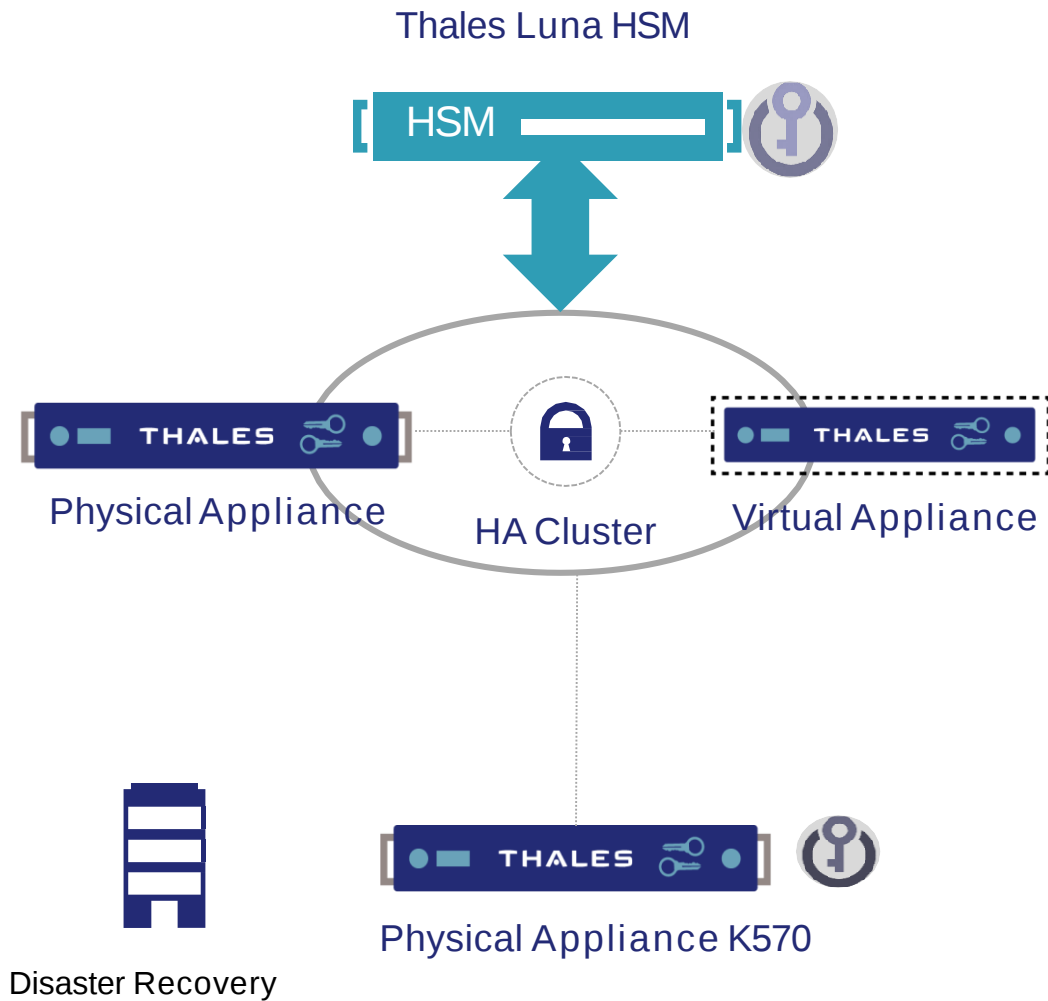
새로운 라이선싱 엔진은 단순화된 **self-service UI**를 제공합니다.

- ▶ Thales Data Protection 커넥터 라이선스 사용률에 대한 향상된 가시성 및 제어
- ▶ Thales License Portal에서 쉽게 활성화

The screenshot displays the 'Admin Settings' interface for Thales KeySecure. The top navigation bar includes 'Admin Settings', 'SafeNet KeySecure k170v version: 1.11.0-beta1.4540', a warning 'One or more licenses are expiring soon', and user information 'API', '?', and 'admin'. The left sidebar lists various settings categories: Licensing, System, Notifications, Policies, Identity Providers, Backups, Domains, and Logs. The main content area is titled 'Server Licenses' and contains two sections: 'Key Manager Lock Code' and 'Connector Lock Code', each with a text input field and a 'Copy' button. Below these is the 'Add A New License' section, featuring a 'License String' input field and an 'Add' button. At the bottom, the 'Installed Licenses' section contains a table with the following data:

Feature	State	Type	Start	Ends	Total Clients	Used Clients
DDC_DATA_ALLOWANCE	active	trial	Tuesday, February 11th 2020	Wednesday, July 1st 2020	2	...
KMIP	active	trial	Tuesday, September 24th 2019	Sunday, August 30th 2020	N/A	N/A

확장된 HSM 옵션



Hardware Security Module

- FIPS 140-2 Level 3 HSM카드에 master key 저장
- RoT(root of trust) 역할
- FIPS 인증 RNG를 통해 더 나은 키 엔트로피를 제공하는데 HSM을 사용

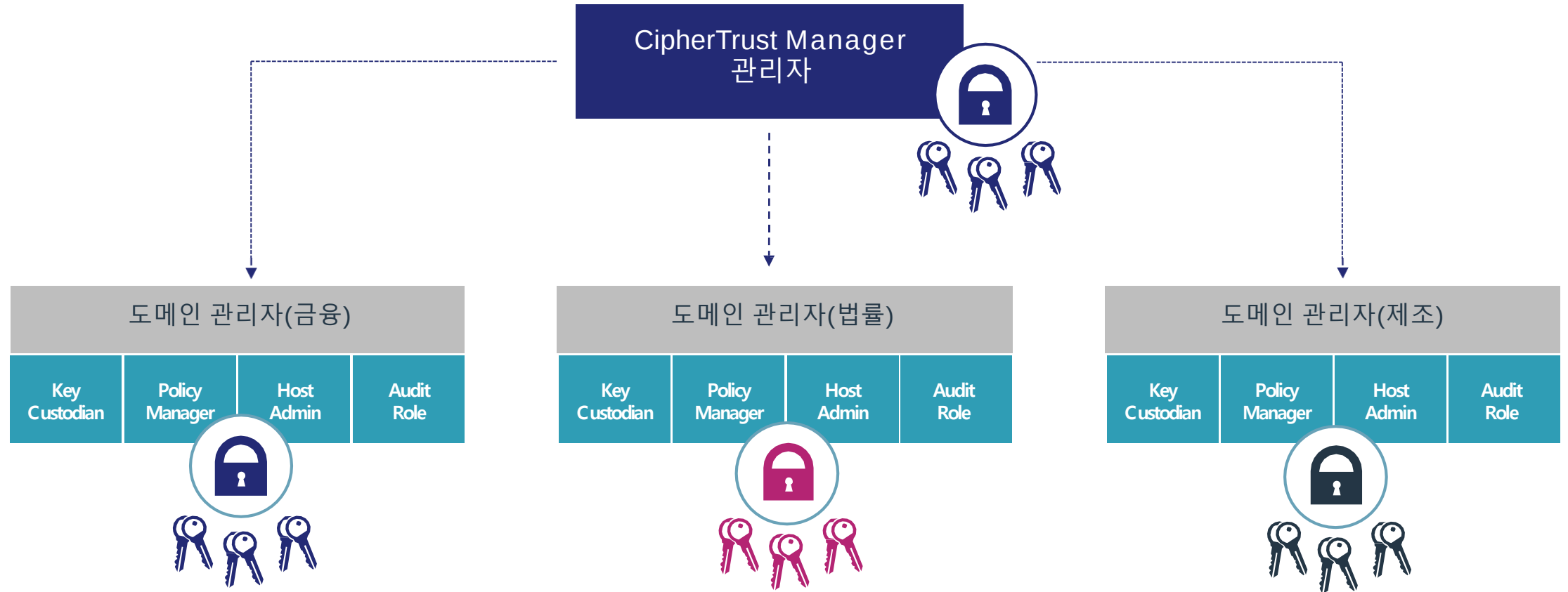
CipherTrust Manager K470 장비는 다음의 HSM과 integration이 될 수 있습니다

- Luna HSM 5, 6 and 7 (network attached)
- DPoD (Cloud HSM)
- AWS Cloud HSM
- Azure Dedicated HSM
- IBM Cloud HSM

CipherTrust Manager K570 장비

- Built-in HSM Card
- FIPS 140-2 Level 3 certified appliance

강력한 역할 분리를 통한 Multi-Tenancy 지원



위치, 사업부 또는 회사 이름으로
도메인을 만들 수 있습니다

키 관리, 보안 제어, 암호화 및
감사를 위한 역할 분리

개발자용 REASTAPI와 Micro-services 구조

개발자용 Native REST 인터페이스로 키관리 운영을 자동화할 수 있습니다.

- CipherTrust Manager는 애자일 개발을 위한 micro-services 아키텍처가 빌트인 되어져 있습니다. 개발 학
- 습 곡선을 완화하는 REST API 놀이터

The screenshot displays the THALES REASTAPI interface, which is a web-based API explorer. The interface is divided into several sections:

- THALES** logo and navigation tabs: **CLI Guide**, **API Guide**, and an **Authenticate** button.
- Keys** section: A sidebar on the left lists various API endpoints and their methods (e.g., `/v1/vault/keys2/` with `List - get`, `Create - post`, etc.).
- Keys** main content area: Contains descriptive text about cryptographic keys and a sample JSON response for a key resource. The text explains that keys can be symmetric or asymmetric, have a `meta` attribute, and include identifiers like `uuid`, `uri`, and `muid`.
- API Call** section: A form for executing an API call. It shows the `List - get` method for the `/v1/vault/keys2` endpoint. Below the form, there are input fields for query parameters: `skip` (integer), `limit` (integer), `fields` (string), and `metaContains` (string).

The sample JSON response for a key resource is as follows:

```
{
  "id": "d22042eb-b527-48fe-b2d6-...",
  "uri": "kylo:kylo:vault:keys:rus...",
  "account": "kylo:kylo:admin:acc...",
  "application": "ncryptify:gema...",
  "devAccount": "ncryptify:gema...",
  "createdAt": "2016-12-01T19:57:...",
  "name": "mykey",
  "updatedAt": "2016-12-01T19:57:...",
  "usage": "any",
  "meta": {
    ...
  }
}
```



CipherTrust Manager는 여러 클라우드 호스팅 옵션을 제공하며 다음에서 기본 가상 머신으로 실행됩니다

- VMware
- AWS
- Microsoft Azure
- OpenStack
- Hyper-V
- Google
- More public / private clouds coming soon

CCKM (Cipher Trust Cloud Key Manager)지원



여러 클라우드 서비스에서 키 관리 간소화

IaaS and PaaS

- Microsoft Azure
- Microsoft Azure Stack
- Microsoft China and Germany National Clouds
- Amazon Web Services
- IBM Cloud

SaaS

- Microsoft Office365
- Salesforce.com
- Salesforce Sandbox

■ syslog 및 Alert를 Security Operations Centers / SIEM에 보내는 기능

- ▶ 여러 포맷의 Audit record 생성 (RFC-5424, CEF, LEEF)
- ▶ 사전 구성 및 사용자 정의 가능한 이메일 Alert 생성 (SNMP v1, v2c, v3)

The screenshot displays the 'Alarm Configuration - Create Key' window. It includes fields for 'Severity' (set to 'Info'), 'Name' (with a placeholder 'Enter an alarm configuration name'), and 'Description'. Below these are radio buttons for 'Conditions', with 'Basic Trigger Conditions' selected. The 'Condition Editor' section shows a rule being built: 'When' is 'details.name', 'Operator' is '==', and 'Value' is 'input must be string'. A note specifies that input only accepts letters or a combination of letters and numbers. To the right, the 'Conditions Preview' shows a list of conditions: 'details.name == Testkey1', 'details.size == 256', 'details.algorithm == AES', 'details.usageMask == 12', 'details.objectType == Symmetric Key', 'message == Create Key', 'service == minerva', 'success == true', 'username == admin', 'client_ip == 174.114.113.184', and 'source == keysecure'. Each condition has a delete button. At the bottom are 'Cancel' and 'Save' buttons.

Alarm Configuration - Create Key

Severity: Info

Name: Enter an alarm configuration name

Description:

Conditions: ☒ Basic Trigger Conditions ☐ Advanced Trigger Conditions

Condition Editor

When: details.name

Operator: ==

Value: input must be string

Note: Input only accepts letters or a combination of letters and numbers (e.g. Thales or Thales123)

Conditions Preview

```
details.name == Testkey1
details.size == 256
details.algorithm == AES
details.usageMask == 12
details.objectType == Symmetric Key
message == Create Key
service == minerva
success == true
username == admin
client_ip == 174.114.113.184
source == keysecure
```

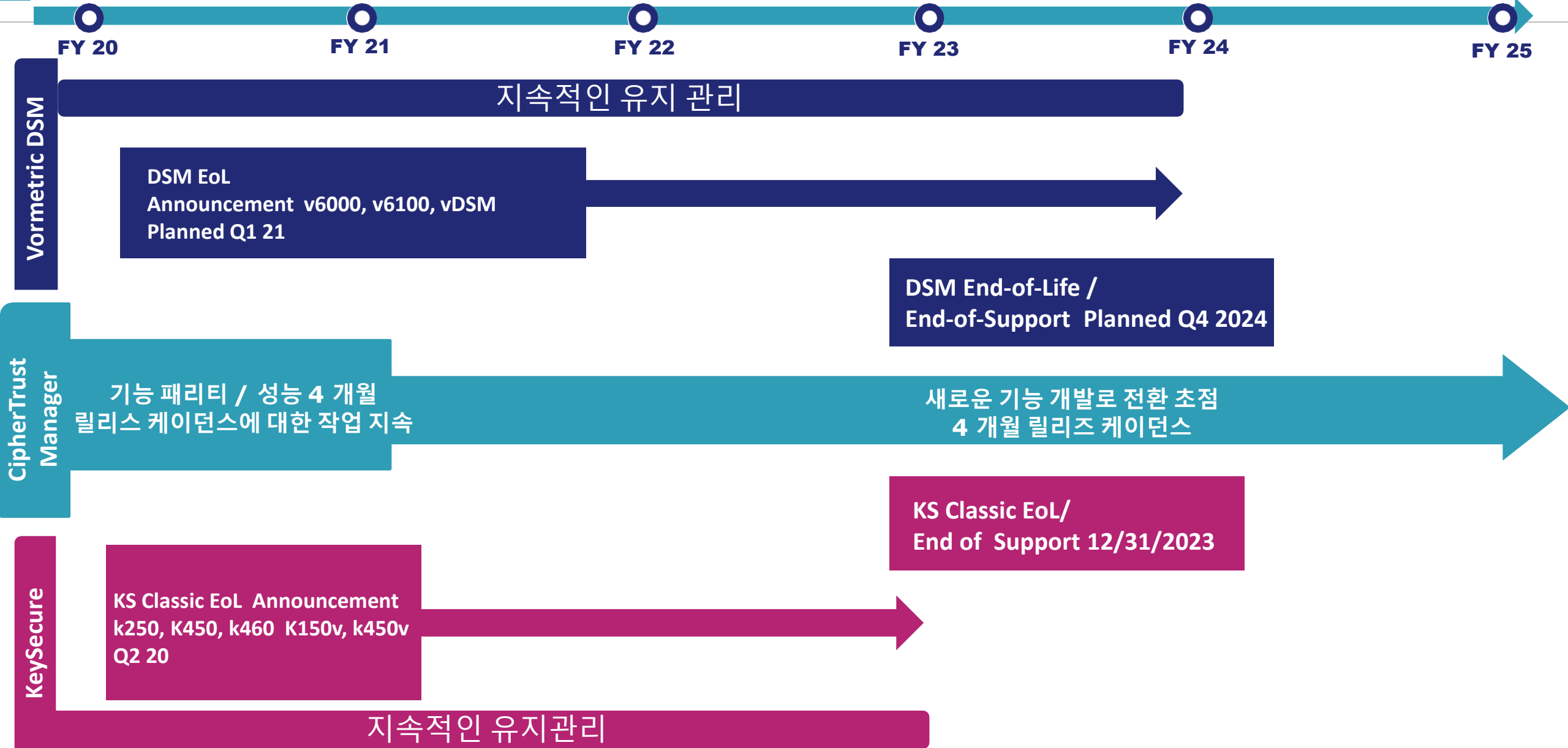
Cancel Save

KeySecure Classic의 마이그레이션 전략

THALES



Support Timeline : Vormetric DSM과 KeySecure Classic



기존 KeySecure Classic 고객을 위한 투자 보호

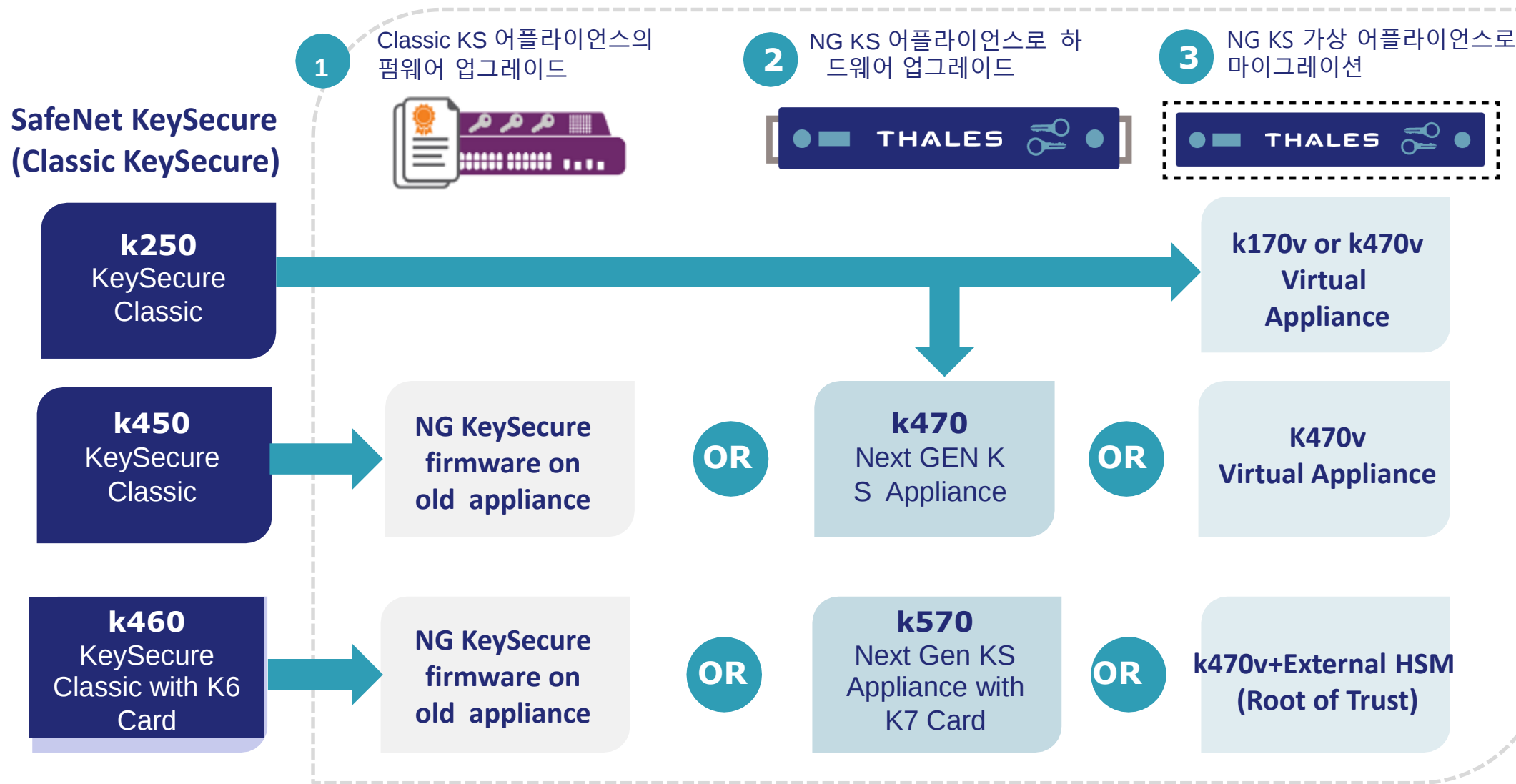
Migration
인센티브\$

적합한 마이그레이션
경로 선택

Thales 지원

Physical KeySecure 마이그레이션 옵션기존 Gemalto 고객용

NextGen KeySecure 으로 마이그레이션하는 옵션



감사합니다

Thank you

Gracias مكل اركش

धन्यवाद Merci

Danke 謝謝

ありがとうございました