

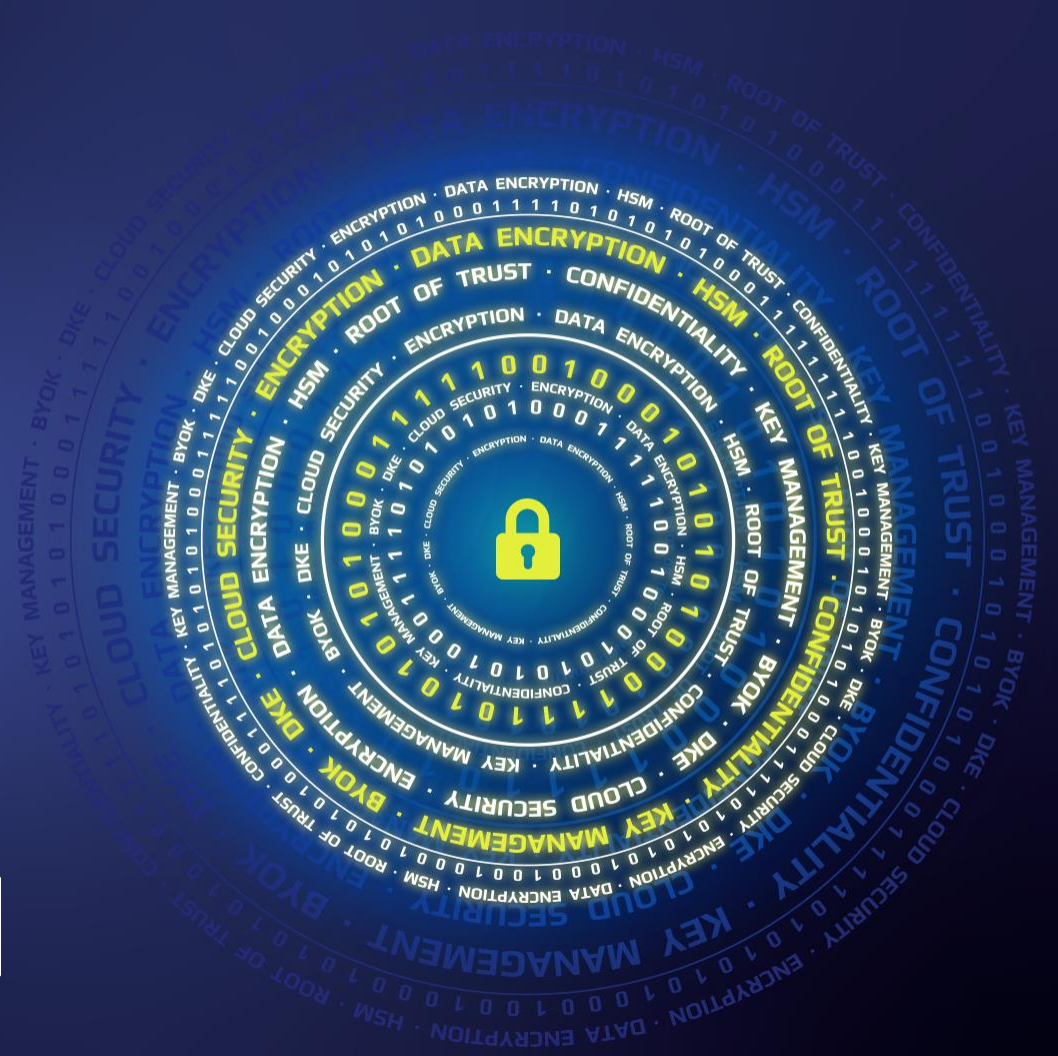
CryptoPanel

edycja #4

za chwilę zaczynamy...



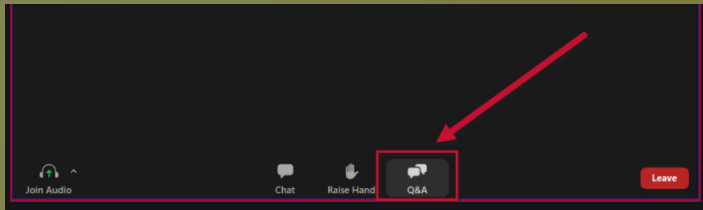
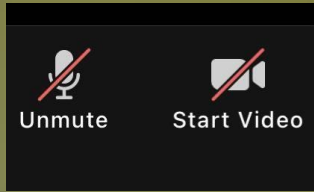
CryptoPanel



THALES



CryptoPanel



CryptoPanel

edycja #4

Zabezpieczanie maszyn wirtualnych i danych w nich przechowywanych w systemach wirtualizacji - na przykładzie VMware - z zachowaniem kontroli nad kluczami szyfrującymi przez użytkownika



CryptoPanel

dziś dyskutują



Artur Holeczek

Partner Account Manager /
Product Manager
artur.holeczek@clico.pl
mob. +48 667 699 444



Piotr Majek

Security Specialist
piotr.majek@clico.pl
mob. +48 663 994 996



CryptoPanel



problem



CryptoPanel



rozwiązanie



Rozwiązanie – szyfrowanie w VMware w integracji z CipherTrust Manager za pomocą KMIP ...i nie tylko



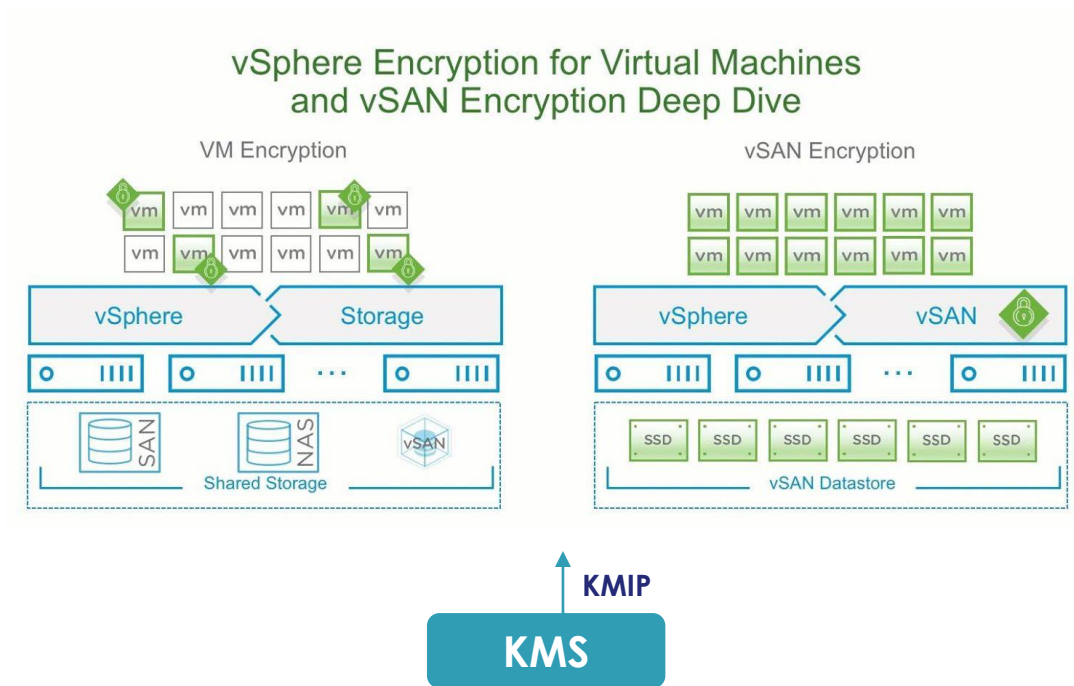
Rozwiązanie - propozycja

- Wdrożenie ochrony danych za pomocą szyfrowania na zasobach serwerowych z jednoczesnym zachowanie kontroli nad kluczami szyfrującymi – > spełnienie wymagań zgodności z regulacjami
- VMware: Wdrożenie szyfrowania całych maszyn wirtualnych. vSAN jak opcja lub druga faza
- Zapewnienie skalowalność z jednoczesnym zapewnieniem wysokiej dostępności



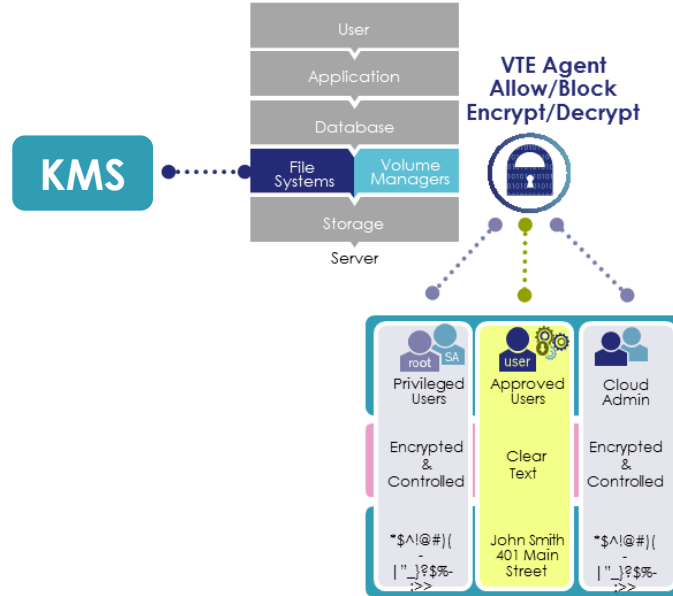
Rozwiązanie – co możemy zrobić? 2 opcje

1. VM Encryption (KMIP)
2. vSAN Encryption (KMIP)



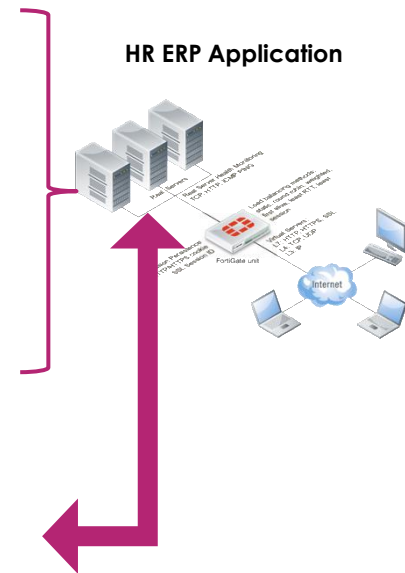
Rozwiązanie – co możemy zrobić?

1. CTE Transparent Encryption z kontrolą dostępu



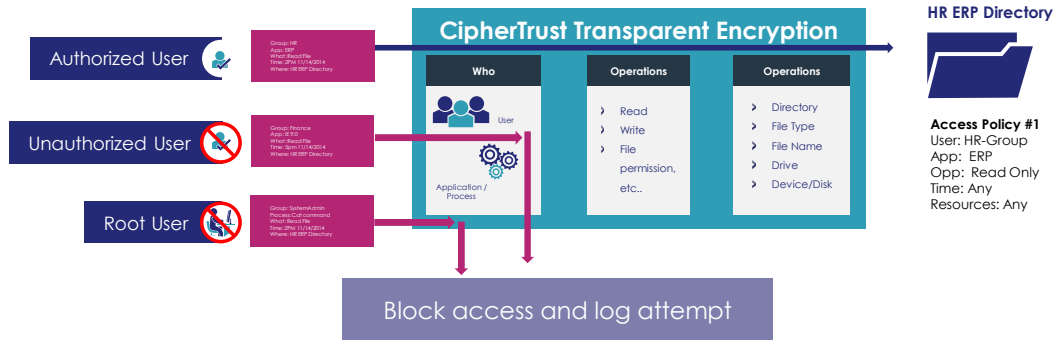
CTE – tylko tam gdzie dane wrażliwe

#	Resource	User	Process	Action	Effects
1	..\<share>/*.pdf	Authorized User	Database	Read/Write	Permit, Encrypt/Decrypt
2	..\<share>/*.pdf	Administrators	Whitelisted management process	Metadata Only	Permit, Audit
3	..\<share>/*.pdf	*	*	*	Deny, Audit



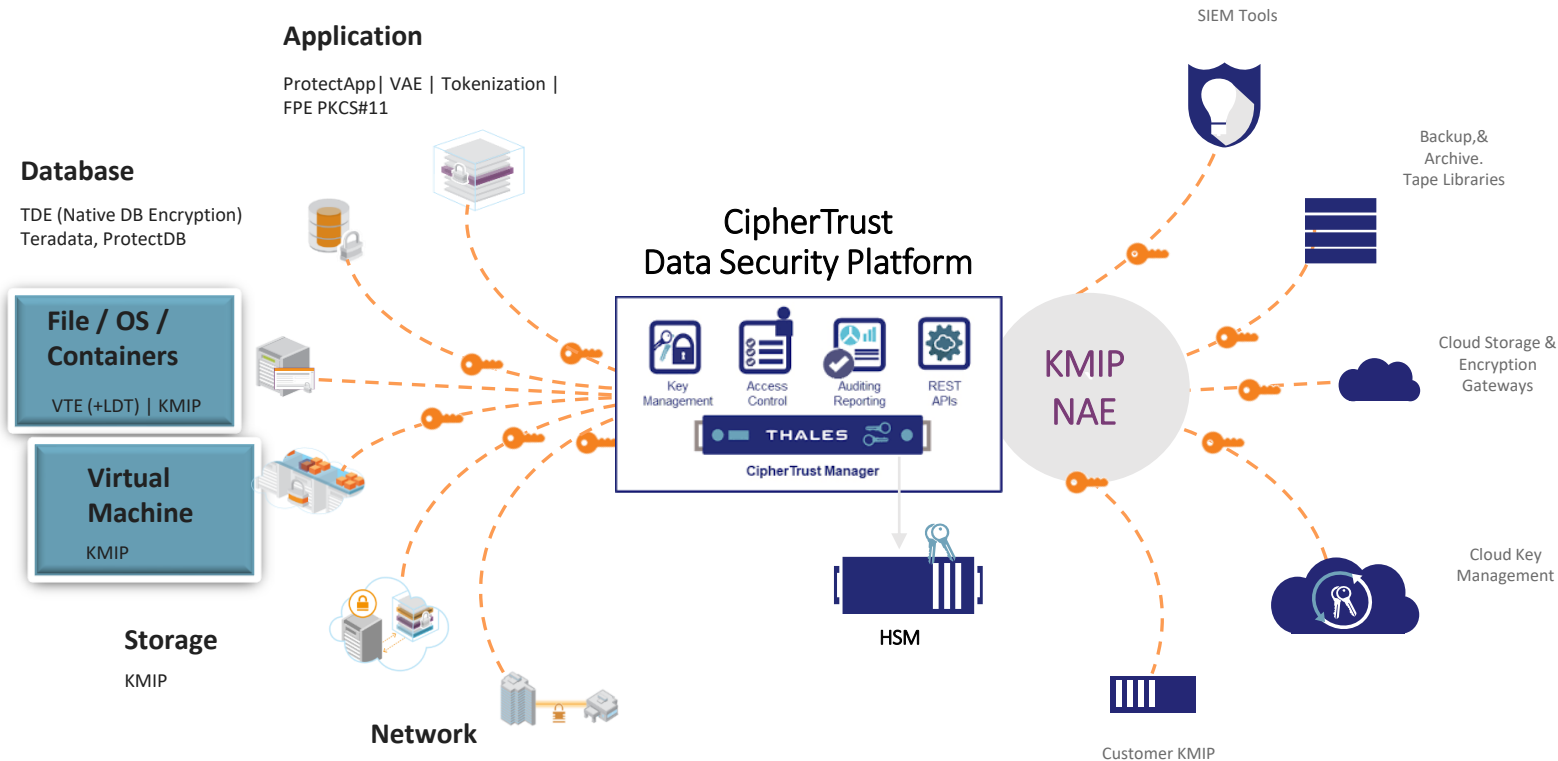
Simple “Set It & Forget It” Policies ENFORCE Intended Application Architecture & Access To Data

- Complete Audit of data transactions
- Secured Logs
- Chain of Custody Insured
- Targets OIC/SOC Operations



File access policies can be very granular. User access can be controlled by application, allowed operations, time and the file or resource they attempt to access.

Enterprise Key Management Solution



Rozwiązanie – CipherTrust w integracji po KMIP

- Wykorzystujemy standard przemysłowy – szeroki zakres współdziałania
- Łatwość integracji
- Z definicji: wysoka dostępność



Dlaczego KMIP?

- Łatwość wdrożenia ochrony danych w spoczynku,
- Możliwość realizacji HYOK w zasobach chmurowych,
- Pozwala uzyskać zgodność z regulacjami dotyczącymi szyfrowania i kontroli dostępu i rotacji kluczy,
- Certyfikowane integracje (VMware, Dell, Nutanix, NetApp).



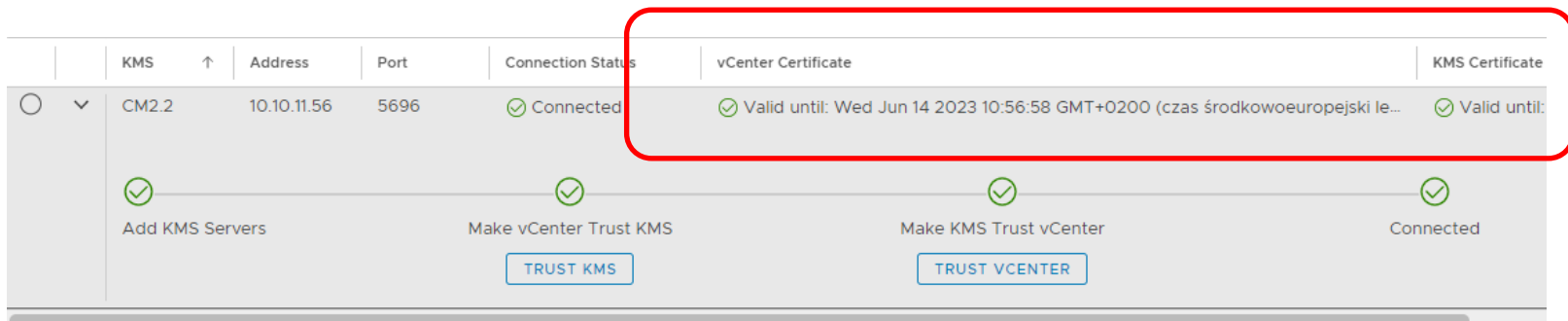
A co z licencjonowaniem ?

- Podstawa – CipherTrust Manager (14k Euro)
- Konektory:
 - Flex Ability (KMIP) – 450 Euro
 - Flex Basic (CTE) – 4480 Euro



Nauczki, czyli *lessons learned* #2/2

- 1. Ustanowienie zaufania vCenter-KMS oparte jest na certyfikatach. Wszystkie certyfikaty kiedyś wygasają – bądź przygotowany! Wpisz do kalendarza, ustaw alarmy, ...



- Odebranie dostępu do klucza w KMS powoduje niemożliwość uruchomienia VM. Co z ochroną uruchomionej VM? CTE!
- Zapewnij backup KMS! Przećwicz jego odtwarzanie! To teraz twój najważniejszy zasób 😊



VM Encryption – co daje

■ Brak modyfikacji w Guest OS.

■ Agnostyczny VM'owo ;)

- Guest OS
- Wersja VM

■ Niezależne od typu datastore

- NFS, iSCSI, VMFS, vSAN

■ Co jest szyfrowane?:

- VMDK
- Pliki VM
- *Pliki core dump hosta*

■ Guest **nie ma** dostępu do kluczy szyfrujących

■ **Tylko** posiadający klucz pochodzący z KMS **ma dostęp** do danych na VM!

■ KMS Keys (KEK) nie znajdują się na vCenter

■ **Klienci** są odpowiedzialni za zarządzanie cyklem życia kluczy!



CryptoPanel



Podsumowanie

Podsumowanie

- Szyfrowanie w środowisku VMware zwiększa bezpieczeństwo danych,
- Odpowiednie procedury szyfrowania pozwalają na obniżenie kosztów poprzez outsourcing,
- Możliwe wdrożenie polityk dostępu bazujących na użytkownikach maszyn wirtualnych.



CryptoPanel



Materiały

▮ Oprogramowanie do pobrania lub wersja ewaluacyjna...

- Bardzo prosimy o kontakt z nami!

▮ Dokumentacja...

- CipherTrust Manger: <https://www.thalesdocs.com/ctp/cm/latest/>
- Podręcznik Integracji KMS-vCenter: <https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.virtualsan.doc/GUID-1583A645-07EE-4D26-8698-080283694635.html>

▮ Zapraszamy także na... Kolejny CryptoPanel!