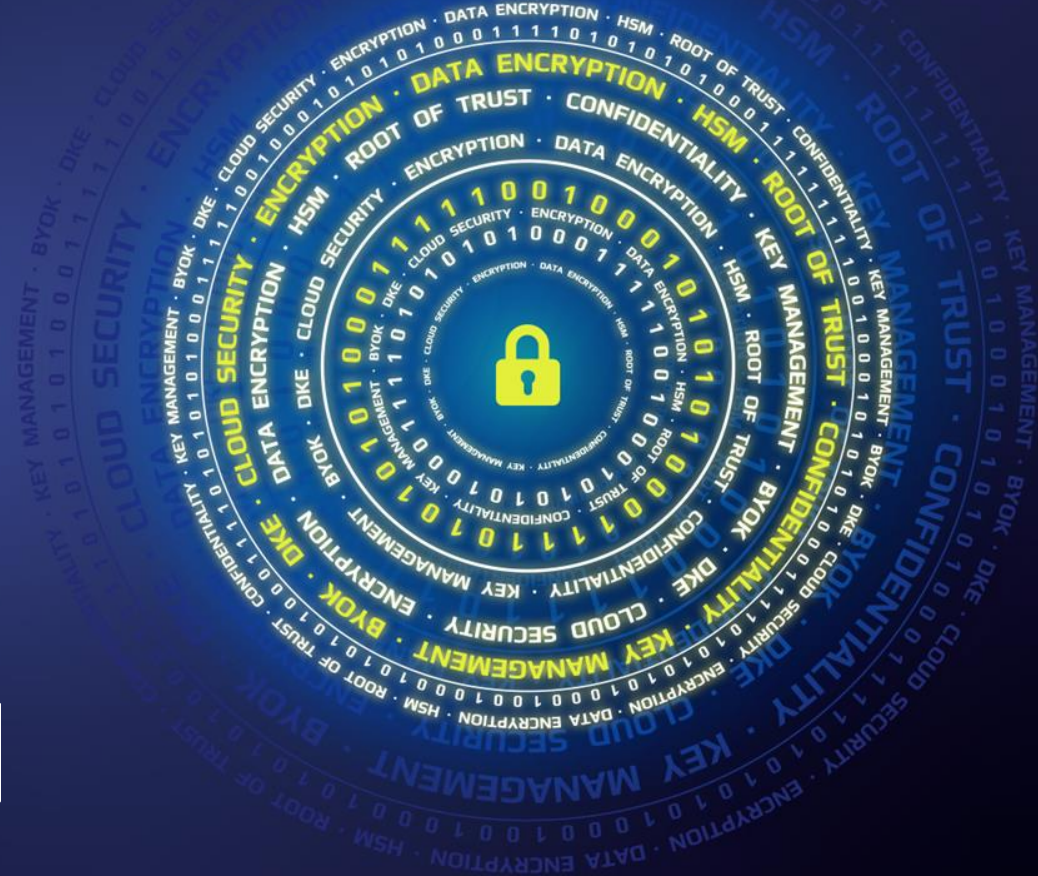
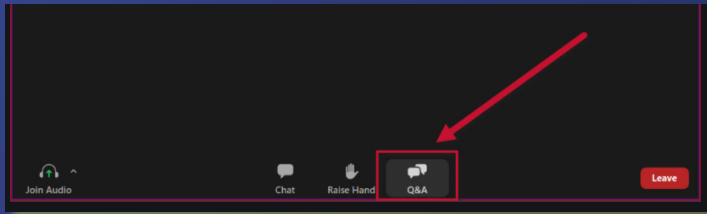
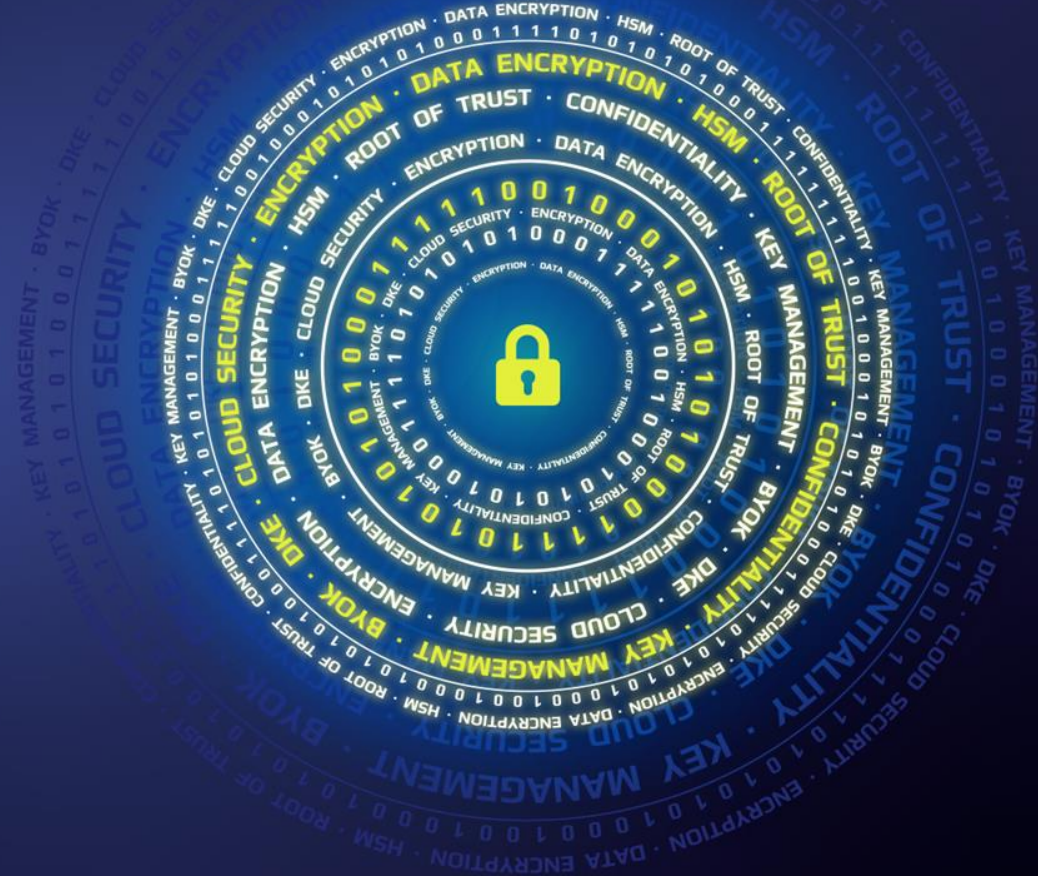
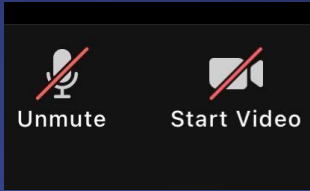


CryptoPanel



THALES  CLICO 

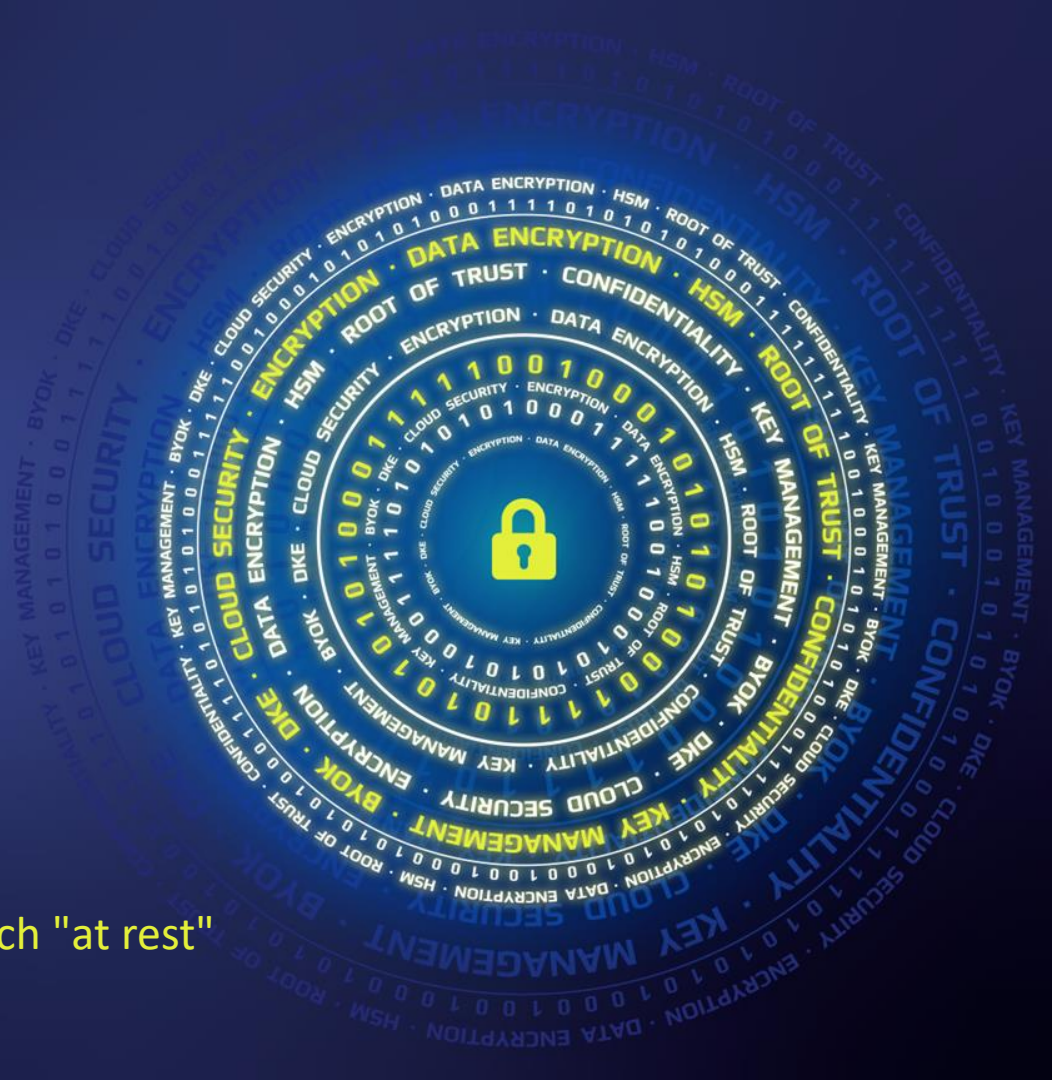
CryptoPanel



CryptoPanel

edycja #1

implementacja szyfrowania
w heterogenicznych środowiskach
bazodanowych jako skuteczny sposób
na zabezpieczanie przetwarzanych danych "at rest"



CryptoPanel

dziś dyskutują



Piotr Wróbel

Regional Sales Manager

Piotr.Wrobel@thalesgroup.com

mob. +48 669 88 99 76



Jarosław Ulczok

Pre-sales Consultant

jaroslaw.ulczok@thalesgroup.com

mob 603 056 667



CryptoPanel



problem



co nas boli...

- Posiadamy kilka kluczowych dla naszej działalności systemów dziedzinowych dostarczonych przez różnych dostawców
 - Systemy pracują na zróżnicowanym środowisku bazodanowym oraz są stale rozwijane zarówno funkcjonalnie jak i infrastrukturalnie
 - Dwa systemy pracują w środowisku Oracle z włączoną opcją Advanced Security i zaimplementowanym szyfrowaniem TDE – Transparent Data Encryption
 - Jeden z systemów pracuje w środowisku MS SQL również z włączonym szyfrowaniem TDE
 - Posiadamy jeszcze dwie aplikacje pracujące w środowisku PostgreSQL – nie szyfrujemy tych baz
 - Szyfrowanie danych przetwarzanych w naszych aplikacjach jest dla nas bardzo ważne
- ...że nie mamy zaszyfrowanych wszystkich kluczowych baz danych
 - ...że koszt utrzymania szyfrowania jest zbyt duży!!!
 - ...że podczas rozbudowy aplikacji, musimy indywidualnie podchodzić do każdego systemu bazodanowego, ze szczególnym uwzględnieniem TDE
 - ...że bardzo istotne dla nas szyfrowanie jest rozproszone, co uniemożliwia nam jego właściwą i należyłą kontrolę
 - ...że wdrażając kolejne aplikacje (a niedługo ruszy projekt nowego systemu ERP) nie wiemy tak naprawdę w jakim kierunku powinniśmy iść jeśli chodzi o szyfrowanie



CryptoPanel

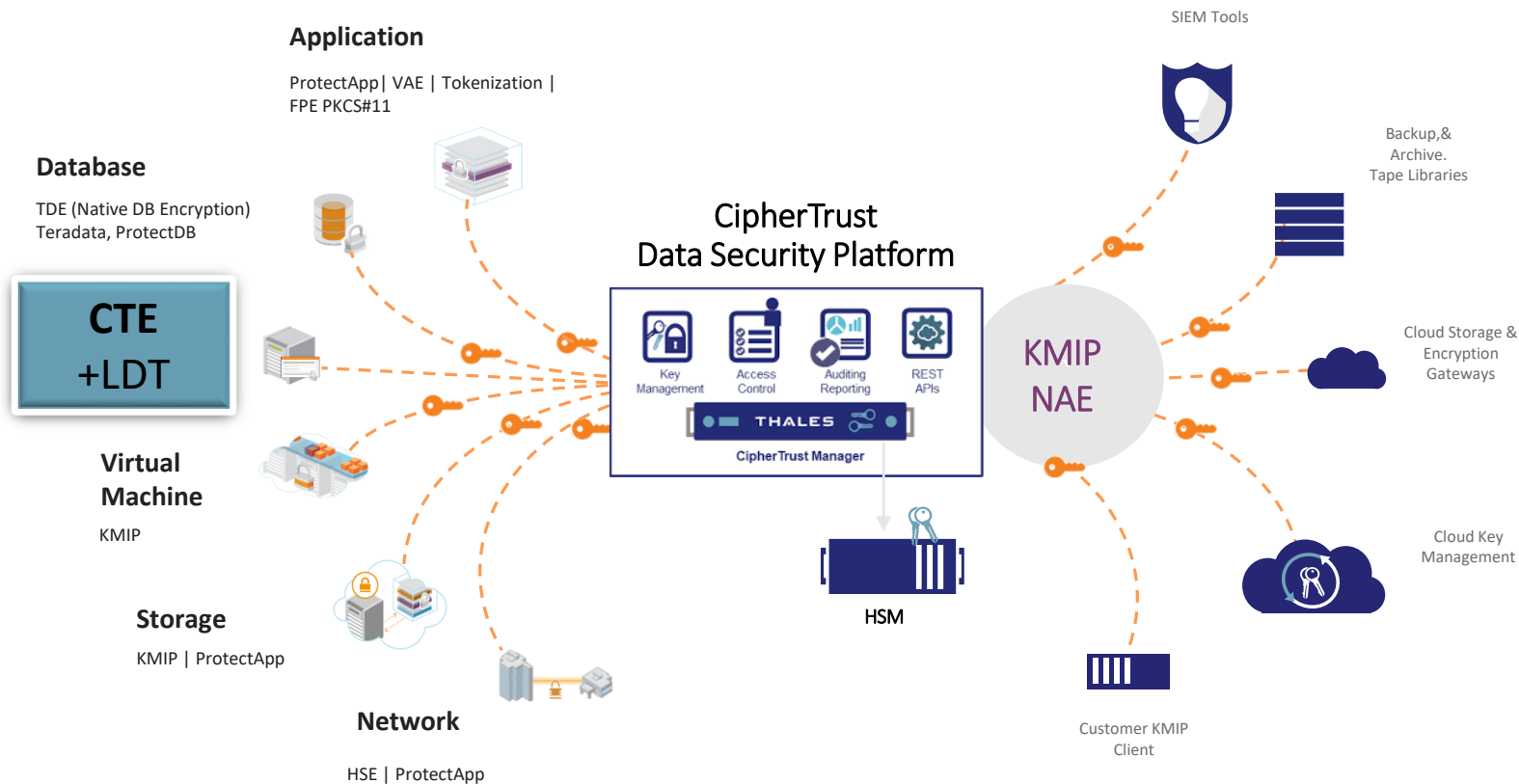


rozwiązanie



Rozwiązanie – CipherTrust Transparent Encryption
z Live Data Transformation

Enterprise Key Management Solution

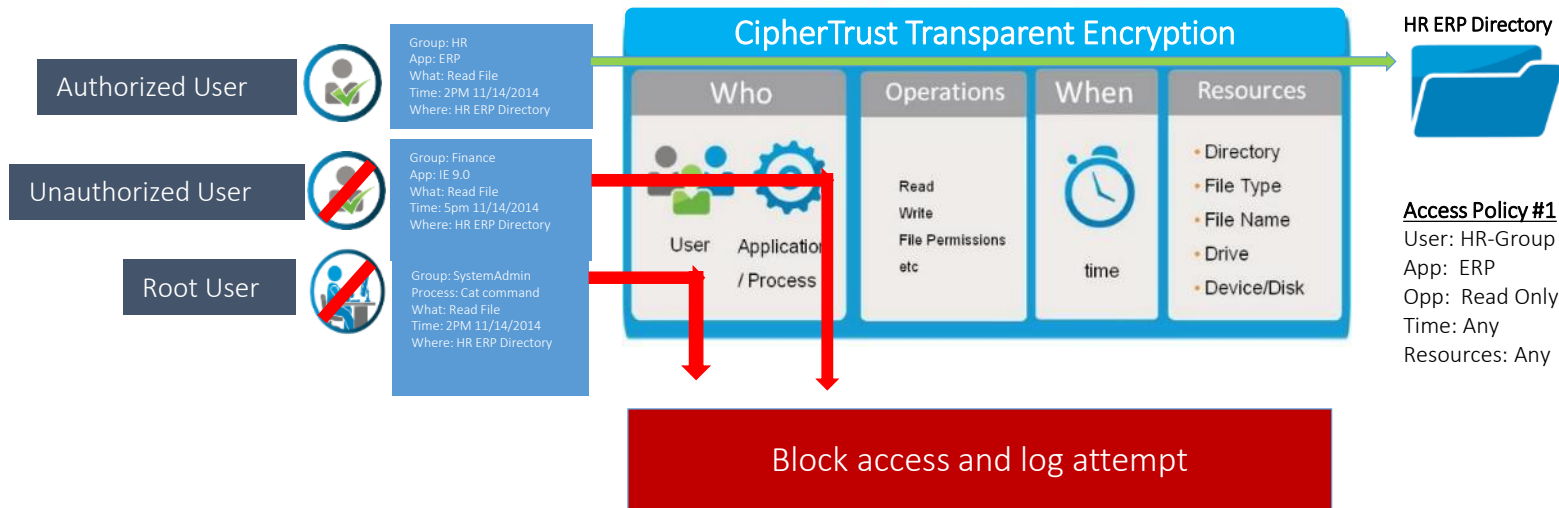


Rozwiązanie – CipherTrust Transparent Encryption z Live Data Transformation

- Traktujemy bazę danych jak plik,
- Ograniczymy przerwy w działaniu systemów (dzięki LDT. Patent!)
- 1 KMS – wiele integracji: do szyfrowania plików, macierzy, dysków, chmur.

Granularna kontrola dostępu

Zasady dostępu do plików uwzględniające procesy i użytkowników

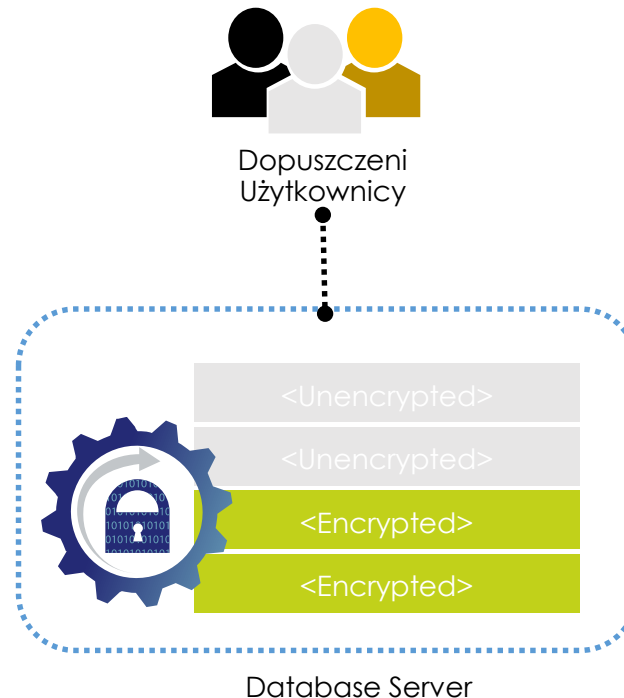


File access policies can be very granular. User access can be controlled by application, allowed operations, time and the file or resource they attempt to access.

1			key_op	permit,applykey	No
▼ <input type="checkbox"/> 2			f_rd_att,f_rd_sec,d...	permit,audit	Yes ...
			Action(s): read file attribute read file security read directory read directory security		
▼ <input type="checkbox"/> 3		sql	all_ops	permit,audit,applykey	Yes ...
		Process Set: sql sqlservr.exe			
▼ <input type="checkbox"/> 4	Administrators		all_ops	permit,audit	Yes ...
		User Set: Administrators Administrator			
▼ <input type="checkbox"/> 5			all_ops	deny,audit	Yes ...
			Action(s): all operations		

Live Data Transformation: robi różnicę!

- Wdrażanie szyfrowania bez przestojułów
 - Zastosuj szyfrowanie i kontrolę dostępu bez przełączania aplikacji w tryb *offline*;
 - Wdrożenie bez przestojułów;
 - Rotacja kluczy bez przestojułów.



Rozszerzenia do CTE



CTE Live Data Transformation

Wdrożenie ograniczające przerwy do minimum



CTE Container Security

Szyfrowanie danych przechowywanych w kontenerach



CTE for SAP HANA

Szyfrowanie danych i logów baz SAP HANA



CTE for Efficient Storage

Maksymalna ochrona przy zachowaniu wydajności platformy



CTE for Teradata

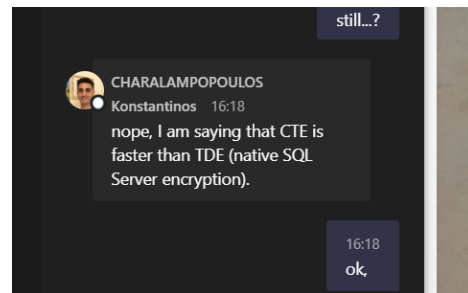
Wysokowydajne rozwiązanie dla baz Teradata

Dlaczego CTE?

- Łatwość wdrożenia ochrony danych w spoczynku,
- Możliwość realizacji HYOE w zasobach chmurowych,
- Pozwala uzyskać zgodność z regulacjami dotyczącymi szyfrowania i kontroli dostępu i rotacji kluczy,
- Live Data Transformation – ochrona bez trybu offline,
- Certyfikowane integracje,

Tego nie znajdziecie w dokumentacji

- CTE pozwala chronić w zasadzie dowolne (pliki) bazy danych (mamy testy/wdrożenia: z Oracle, MS SQL, DB2, MySQL, MariaDB, MongoDB, ...)
- CTE obciąża silnika bazy mniej niż TDE ...ale to jednak inne technologie
- Testy z prawdziwego wdrożenia - 4 bazy Oracle Enterprise po kilka terabajtów każda...



” Tak, testy wykonane w pierwszej fazie oceniamy pozytywnie. Włączenie szyfrowania na bazie praktycznie nie miało wpływu na czas wykonywania obciążających operacji wykonywanych przez pojedynczego użytkownika, nie było również widać istotnych różnic w obciążeniu procesorów / operacji IO w czasie wykonywania tych operacji. To co chcemy jeszcze zweryfikować to zachowanie innej bazy pod obciążeniem wynikającym z równoległej pracy użytkowników symulowanej jmeterem. I tu jesteśmy w trakcie przygotowania scenariuszy testów automatycznych.

”

CryptoPanel



podsumowanie



CryptoPanel

