cpl.thalesgroup.com

THALES

Thales — portfolio rozwiązań do ochrony danych

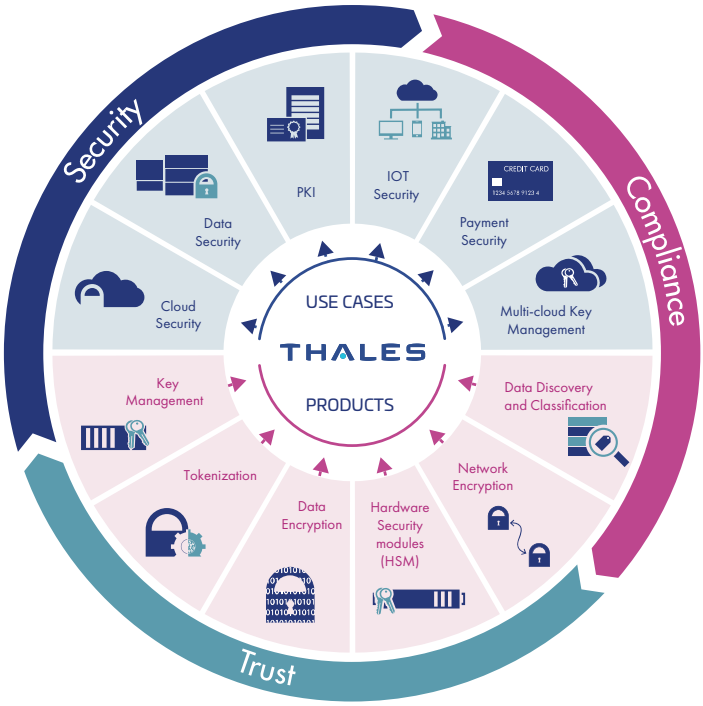
Thales — portfolio rozwiązań do ochrony danych

Przypadki naruszenia bezpieczeństwa zdarzają się dziś z niepokojącą regularnością. Co więcej, wymagania dotyczące zgodności z przepisami stają się coraz bardziej rygorystyczne, dlatego firmy muszą wykrywać i chronić wrażliwe dane w środowiskach lokalnych, hybrydowych i wielochmurowych.

Doskonałe portfolio produktów do ochrony danych firmy Thales pozwala organizacjom na zabezpieczanie danych w spoczynku i w ruchu na skalę całego ekosystemu IT. Pozwala także zapewnić, aby klucze do tych danych były zawsze chronione i pozostawały wyłącznie pod kontrolą właściciela. Nasza oferta upraszcza ochronę danych, zwiększa efektywność operacyjną i skraca czas uzyskiwania zgodności z przepisami. Niezależnie od tego, gdzie znajdują się dane, Thales jest w stanie zapewnić, aby były one bezpieczne. Do tego celu służy szeroka gama sprawdzonych, czołowych na skalę całego rynku produktów i rozwiązań do wdrażania w centrach danych, przez dostawców usług przetwarzania w chmurze (CSP), dostawców usług zarządzanych (MSP) lub w formie usług opartych na chmurze, zarządzanych bezpośrednio przez firmę Thales.

Zalety produktów firmy Thales do ochrony danych:

- **Ochrona danych w spoczynku** za pomocą platformy CipherTrust Data Security Platform; wykrywanie, ochrona i kontrolo-wanie wrażliwych danych organizacji w dowolnym miejscu dzięki nowej generacji rozwiązań do ujednoliconej ochrony danych
- **Ochrona danych w ruchu** za pomocą dedykowanych fizycznych oraz wirtualnych wysokowydajnych szyfratorów sieciowych; ochrona poufnych danych, wideo i dźwięku w czasie rzeczywistym – podczas przesyłu między centrami przetwarzania danych lub oddziałami firmy, a także lokalizacjami do przechowywania kopii zapasowych i odzyskiwania danych po awarii oraz w chmurze
- **Bezpieczne zarządzanie kluczami szyfrującymi** – z podziałem obowiązków i przez cały cykl życia kluczy – za pomocą platformy CipherTrust Data Security Platform lub usług CipherTrust Key Broker dostępnych w ramach platformy Data Protection on Demand (DPoD)
- **Kontrola funkcji kryptograficznych** za pomocą modułów Luna Network Hardware Security Module (HSM) i Luna Cloud HSM, która pozwala na bezpieczne zarządzanie, przetwarzanie i przechowywanie kluczy kryptograficznych bezpiecznych, odpornych na manipulacje urządzeniach z certyfikatem FIPS 140-2, dostępnych jako sprzęt w siedzibie firmy, w chmurze jako usługa DPoD lub na oba sposoby – jako rozwiązanie hybrydowe
- **Skuteczna ochrona transakcji** w środowiskach przetwarzania płatności detalicznych, obsługa aplikacji płatniczych i przetwarzania kodów PIN za pomocą payShield HSM do obsługi płatności
- **Bezpieczne udostępnianie plików** użytkownikom wewnętrznym i zewnętrznym z możliwością ich zapisywania, udostępniania i synchronizowania w chmurze i w siedzibie firmy za pomocą SureDrop – rozwiązania klasy korporacyjnej, które wykorzystuje zabezpieczenia klasy obronnej



Najważniejsze korzyści

- **Większa zgodność i bezpieczeństwo**
  Produkty i rozwiązania firmy Thales do ochrony danych spełniają wymagania szeregu przepisów dotyczących bezpieczeństwa i prywatności, takich jak electronic IDentification, Authentication and trust Services (eIDAS), Payment Card Industry Data Security Standard (PCI DSS), Ogólne rozporządzenie o ochronie danych (RODO), Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA), a także regionalnych przepisów dotyczących ochrony danych i prywatności.
- **Optymalizacja wydajności personelu i zasobów**
  Firma Thales zapewnia najszersze wsparcie przypadków użycia zabezpieczeń danych w branży dzięki produktom zaprojektowanym z myślą współpracy, pojedynczej linii globalnego wsparcia, doświadczeniu w ochronie przed ewoluującymi zagrożeniami i największemu ekosystemowi partnerów w branży ochrony danych. Thales koncentruje się na łatwości użytkowania, interfejsach API do automatyzacji i zarządzaniu responsywnym, co pozwala zapewnić, aby zespoły mogły szybko wdrożyć zabezpieczenia w firmie i monitorować je. Co więcej, nasz specjalistyczny personel serwisowy oraz ekosystem partnerów jest dostępny na etapach projektowania, wdrażania i szkoleń, aby zapewnić szybkie i niezawodne wdrożenie przy jak najmniejszym nakładzie czasu pracowników.
- **Mniejszy całkowity koszt posiadania**
  Portfolio firmy Thales to kompleksowy zestaw produktów i rozwiązań do ochrony danych, które pozwalają na łatwe skalowanie i rozszerzanie na nowe przypadki użycia oraz są połączone z udokumentowanym doświadczeniem w zabezpieczaniu nowych i tradycyjnych technologii. Dzięki Thales można zabezpieczyć inwestycje na przyszłość przy jednoczesnym obniżeniu kosztów operacyjnych i nakładów kapitałowych.

Ochrona danych w stanie spoczynku

Platforma CipherTrust Data Security ujednolica wykrywanie, klasyfikowanie i ochronę danych oraz bezprecedensową szczegółową kontrolę dostępu i scentralizowane zarządzanie kluczami. Takie podejście skutkuje zmniejszeniem ilości zasobów przeznaczonych na operacje związane z bezpieczeństwem danych i wszechobecnymi kontrolami zgodności z przepisami oraz znacznie ogranicza ryzyko na skalę całej firmy. Platforma obejmuje następujące składniki:

CipherTrust Manager
CipherTrust Manager, centralny element platformy, to znakomite rozwiązanie do zarządzania kluczami. Umożliwia przedsiębiorstwom centralne zarządzanie kluczami szyfrowania, szczegółową kontrolę dostępu i konfigurowanie reguł bezpieczeństwa. Zarządza zadaniami związanymi z całym cyklem życia kluczy, od tworzenia, poprzez rotację, importowanie i eksportowanie, aż po ich niszczenie. Zapewnia mechanizmy kontroli i reguły dostępu do kluczy oparte na rolach. Umożliwia efektywne przeprowadzanie audytów i tworzenie raportów. Udostępnia interfejsy REST API łatwe w obsłudze dla programistów. Rozwiązanie pozwala na scentralizowane zarządzanie kluczami szyfrowania i regułami w odniesieniu do konektorów ochrony danych, które omawiamy poniżej. CipherTrust Manager jest dostępny zarówno w formie wirtualnej, jak i fizycznej. Obie z nich są zgodne ze standardem FIPS 140-2 do poziomu 3, co pozwala na bezpieczne przechowywanie kluczy przy podwyższonym poziomie zaufania.

CipherTrust Data Discovery and Classification
CipherTrust Data Discovery and Classification lokalizuje wrażliwe dane, zarówno te ustrukturyzowane, jak i nieustrukturyzowane, w chmurze, systemach Big Data i tradycyjnych magazynach danych. Jedna aplikacja umożliwia poznanie wrażliwych danych i związanego z nimi ryzyka, co pozwala na podejmowanie lepszych decyzji dotyczących usuwania luk w zabezpieczeniach, określania priorytetów działań naprawczych oraz zabezpieczania transformacji chmury i udostępniania danych stronom trzecim. Rozwiązanie usprawnia przepływ pracy na wszystkich etapach: od konfigurowania reguł, przez wykrywanie i klasyfikację, po analizę ryzyka i tworzenie raportów. Dzięki temu pomaga w wyeliminowaniu tzw. martwych stref bezpieczeństwa i uproszczeniu procesów.

CipherTrust Transparent Encryption
Rozwiązanie CipherTrust Transparent Encryption umożliwia szyfrowanie danych w spoczynku, kontrolowanie dostępu użytkowników uprzywilejowanych oraz tworzenie szczegółowych dzienników kontroli dostępu do danych. Dostępne konektory chronią dane w plikach, woluminach i bazach danych, w systemach operacyjnych Windows, AIX i Linux na serwerach fizycznych i wirtualnych, w chmurach i systemach Big Data. Rozszerzenie Live Data Transformation umożliwia szyfrowanie i zmiany kluczy bez powodowania przestojów. Ponadto dzienniki i raporty zawierające dane analityczne dotyczące bezpieczeństwa upraszczają raportowanie zgodności z przepisami i przyspieszają wykrywanie zagrożeń, wykorzystując najlepsze systemy zarządzania informacjami i zdarzeniami dotyczącymi bezpieczeństwa (SIEM).

CipherTrust Application Data Protection
Rozwiązanie CipherTrust Application Data Protection udostępnia funkcje kryptograficzne, takie jak zarządzanie kluczami, składanie podpisów, tworzenie skrótów i szyfrowanie za pośrednictwem interfejsów API. Dzięki temu programiści mogą łatwo zabezpieczać dane na serwerze aplikacji lub węźle systemu Big Data. Do rozwiązania dołączone są przykładowe aplikacje. CipherTrust Application Data Protection przyspiesza tworzenie niestandardowych rozwiązań do ochrony danych i sprawia, że programiści nie muszą już się zajmować złożonymi procedurami zarządzania kluczami. Wprowadza silne odseparowanie obowiązków na podstawie reguł zarządzania kluczami. Za reguły te odpowiada tylko dział bezpieczeństwa.

CipherTrust Tokenization
Rozwiązanie CipherTrust Tokenization jest oferowane w wersji ze skarbcem (vaulted) i bez skarbca (vaultless). Pomaga firmom w dostosowaniu się do standardów ochrony danych, takich jak PCI-DSS, w sposób prostszy i mniej kosztowny. Wersja bez skarbca obejmuje oparte na regułach dynamiczne maskowanie danych, natomiast opcja ze skarbcem udostępnia dodatkowe interfejsy API dopasowane do danego środowiska. Obie wersje ułatwiają dodawanie funkcji tokenizacji do aplikacji za pośrednictwem interfejsów RESTful API.

CipherTrust Database Protection
Rozwiązania CipherTrust Database Protection umożliwiają integrację szyfrowania wrażliwych pól bazy danych z bezpiecznym i scentralizowanym zarządzaniem kluczami, bez konieczności wprowadzania zmian w aplikacjach bazy danych. Rozwiązania CipherTrust Database Protection obsługują bazy danych Oracle, Microsoft SQL Server oraz IBM DB2 i Teradata.

CipherTrust Enterprise Key Management
CipherTrust Key Management to wydajne, oparte na standardach rozwiązania do zarządzania kluczami szyfrowania w całym przedsiębiorstwie. Zapewniają one bezpieczeństwo kluczy i upraszczają procesy administracyjne związane z zarządzaniem nimi. Klucze są zawsze udostępniane na potrzeby autoryzowanych usług szyfrowania. Rozwiązania CipherTrust Key Management obsługują różne przypadki użycia:

- **CipherTrust Cloud Key Manager** upraszcza zarządzanie kluczami w modelu BYOK (ang. bring your own key), w którym pracownicy używają swoich prywatnych kluczy szyfrowania w systemach przedsiębiorstwa, na platformach Amazon Web Services, Microsoft Azure, Salesforce i IBM Cloud. Umożliwia kompleksowe zarządzanie cyklem życia kluczy w chmurze oraz automatyzację tego procesu. Zwiększa wydajność zespołów odpowiedzialnych za bezpieczeństwo i upraszcza zarządzanie kluczami w chmurze.
- **CipherTrust TDE Key Management** obsługuje wiele rozwiązań bazodanowych, takich jak Oracle, Microsoft SQL i Microsoft Always Encrypted.
- **CipherTrust KMIP Server** centralizuje zarządzanie klientami KMIP, co obejmuje pełne szyfrowanie dysku (FDE), systemy Big Data, bazę danych IBM DB2, archiwa taśm, szyfrowanie w środowiskach VMware vSphere i vSAN i inne.

Ochrona danych w ruchu

Firma Thales oferuje szybkie szyfratory (HSE), które odpowiadają za szyfrowanie danych w ruchu niezależne od sieci (warstwy 2, 3 i 4). Takie podejście pozwala chronić dane podczas ich transferu pomiędzy lokalizacjami lub z siedziby firmy do chmury i z powrotem. Nasze rozwiązania HSE pozwalają klientom lepiej chronić dane, wideo, głos i metadane przed podsłuchiwaniem, inwigilacją oraz jawnym i ukrytym przechwytywaniem — a wszystko to z zachowaniem przystępnych kosztów i bez negatywnego wpływu na wydajność. Produkty HSE firmy Thales są dostępne zarówno jako urządzenia fizyczne, jak i wirtualne. Obsługują szerokie spektrum prędkości sieci — od 10 Mb/s do 100 Gb/s — a dostępne platformy obejmują urządzenia zarówno jedno-, jak i wieloportowe.

- **Seria CN** to sprzętowe urządzenia sieciowe, które zapewniają niezależne od warstwy sieciowej (warstwy 2, 3 i 4) szyfrowanie danych w ruchu. Te szyfratory sprzętowe noszą certyfikaty zgodnościze standardem FIPS 140-2 Level 3 oraz Common Criteria EAL 2 i 4+.
- **Seria CV** to silnie zabezpieczone urządzenie wirtualne, które zapewnia silne szyfrowanie danych w ruchu w szybkich sieciach WAN operatorów i łączach SD-WAN. Do tego celu wykorzystuje technologię Network Function Virilization (NFV).

Sprzętowe moduły bezpieczeństwa

Moduły HSM firmy Thales to urządzenia zdolne zapewnić wysoki poziom bezpieczeństwa, zweryfikowane zgodnie ze standardem FIPS 140-2 Level 3, i odporne na manipulacje. Pozwalają osiągnąć zgodność z przepisami i skalowalność, aby sprostać potrzebom przypadków użycia, które wymagają dużej wydajności w newralgicznych środowiskach. Moduły zabezpieczają klucze na potrzeby danych w spoczynku i w ruchu, dzięki czemu pełnią funkcję punktów zaufania, które chronią klucze główne — szyfrujące dane, tożsamości cyfrowe i transakcje. Firma Thales oferuje następujące rodzaje specjalnie zaprojektowanych modułów HSM:

- **Luna General Purpose HSM** (ogólniego przeznaczenia) są podstawą zaufania całego ekosystemu organizacji, w tym urządzeń, tożsamości i transakcji. Moduły Luna HSM zapewniają integralność kluczy kryptograficznych i funkcji, chroniąc je za pomocą różnych form produktów — urządzeń sieciowych, wbudowanych kart PCIe lub przenośnych urządzeń USB. Szeroka gama interfejsów API, doskonała wydajność i setki gotowych aplikacji partnerów technologicznych do ochrony cykli życia i operacji związanych z kluczami kryptograficznymi pozwalają uprosić rozwój i integrację. Rozwiązanie Crypto Command Center — scentralizowana platforma, która zapewnia funkcje monitorowania, raportowania, udostępniania i ostrzegania na żądanie w ciągu kilku minut — pozwala ponadto na łatwe zarządzanie zasobami kryptograficznymi Luna HSM i ich monitorowanie.
- **Moduły Payment HSM** (płatnicze) zapewniają pakiet funkcji związanych z ochroną płatności, w tym przetwarzanie transakcji, ochronę danych wrażliwych, wydawanie poświadczeń na potrzeby płatności, akceptację kart mobilnych i tokenizację płatności. Moduły payShield HSM firmy Thales są stosowane w całym globalnym ekosystemie płatniczym przez emitentów, dostawców usług, nabywców, podmioty przetwarzające i sieci płatnicze. Najnowszy model, payShield 10K, otrzymał szereg globalnych i regionalnych certyfikatów bezpieczeństwa, w tym PCI HSM v3, FIPS 140-2 Level 3 i AusPayNet.

Data Protection on Demand

Nagradzana platforma Thales Data Protection on Demand (DPoD) to rozwiązanie oparte na chmurze, które udostępnia szeroką gamę usług takich jak Luna Cloud HSM, CipherTrust Cloud Key Management oraz payShield Cloud Payment za pomocą prostego w obsłudze interfejsu graficznego w przeglądarce. Dzięki temu ochrona danych staje się prostsza, bardziej ekonomiczna i łatwiejsza w zarządzaniu, ponieważ nie ma sprzętu, który trzeba kupić, wdrożyć i utrzymywać. Wystarczy kliknąć, aby w kilka minut wdrożyć pożądaną ochronę, uruchomić usługi, dodać reguły bezpieczeństwa lub otrzymać raporty dotyczące użytkowania. DPoD to również idealna platforma dla dostawców zarządzanych usług zabezpieczeń, którzy chcą zapewnić swoim klientom bezkonkurencyjne rozwiązania do ochrony danych jako usługi, w połączeniu z innymi usługami bezpieczeństwa i przetwarzania w chmurze.

Usługi Luna Cloud HSM
DPoD udostępnia na żądanie szeroki zakres usług HSM opartych na chmurze, dzięki czemu pozwala klientom przechowywać klucze kryptograficzne używane do szyfrowania danych w chmurze i zarządzać nimi, zachowując jednocześnie nad nimi pełną kontrolę. Rynek DPoD oferuje usługi Cloud HSM dostosowane do szerokiej gamy przypadków użycia i integracji w środowiskach chmurowych, hybrydowych i lokalnych.

Usługi CipherTrust Cloud Key Management
Usługi Key Broker w platformie DPoD zapewniają funkcjonalność BYOK (ang. bring your own key) jako usługę opartą na chmurze. DPoD zapewnia prostą i bezpieczną kontrolę nad kluczami i powiązanymi zbiorami reguł bezpieczeństwa na potrzeby szyfrowania w środowiskach IaaS i PaaS dostawców usług przetwarzania w chmurze oraz dostawców SaaS.

Bezpieczne współdzielenie plików

Kultura pracy z dowolnego miejsca i współpracy z dowolnymi osobami jest coraz bardziej powszechna. Niezależnie od tego, gdzie i jak pracują członkowie organizacji, zawsze istnieje potrzeba udostępniania i synchronizowania plików — zarówno wewnętrznie, jak i zewnętrznie. Mimo że samo umożliwienie takiej współpracy może wydawać się najważniejsze, na pierwszym miejscu zawsze powinno być bezpieczeństwo danych. W przeciwnym razie ryzyko braku zgodności z przepisami i potencjalnego naruszenia bezpieczeństwa danych staje się poważnym problemem. SureDrop to rozwiązanie klasy korporacyjnej do bezpiecznego współdzielenia plików i współpracy w chmurze lub w siedzibie firmy, które zapewnia kompleksowe szyfrowanie danych. SureDrop zaprojektowano z myślą o organizacjach, które dysponują silnymi regułami bezpieczeństwa dotyczącymi przechowywania plików, ale nadal potrzebują zalet związanych z wydajnością, jakie daje w pełni funkcjonalne rozwiązanie do współdzielenia plików.

Informacje o firmie Thales

Ludzie, którym powierzasz ochronę swojej prywatności, polegają na Thales, aby chronić swoje dane. Jeśli chodzi o bezpieczeństwo danych, organizacje stają w obliczu coraz większej liczby „decydujących momentów". Niezależnie od tego, czy takim momentem jest budowanie strategii szyfrowania, przejście do chmury, czy spełnienie wymogów zgodności, możesz polegać na Thales, aby zabezpieczyć swoją cyfrową transformację.

Decydująca technologia ma znaczenie w decydujących momentach.

THALES

Informacje kontaktowe

Wszystkie lokalizacje biur i informacje kontaktowe można znaleźć na stronie cpl.thalesgroup.com/contact-us

> cpl.thalesgroup.com <