cpl.thalesgroup.com

THALES

탈레스는 인도네시아의 선도적 금융 기술 및 서비스 제공업체의 PCI 규제 준수 지원

요약

인도네시아의 한 선도적 금융 기술 및 서비스 제공업체는 고객과 안전하게 데이터를 교환하기 위해 PCI-DSS(지불 카드 산업 데이터 보안 표준)를 준수하는 데이터 보호 솔루션이 필요했습니다.

기업 소개

24년간 연구 및 분석 소프트웨어를 개발해 온 인도네시아의 선도적 금융 기술 및 서비스 제공업체. 이 기업은 자본 및 자금 시장에 대한 전문 지식과 소프트웨어 개발을 결합한 제품을 제공하여 소매 투자자 및 부문별 전문가와 같이 다양한 사용자를 지원합니다.

또한, 청구서 결제 집계, 전자 결제 플랫폼, 온라인 결제 솔루션이라는 세 가지 사업 분야를 운영하고 있습니다.

비즈니스 요구 사항

이 기업은 지불 카드 산업 규제(PCI-DSS)를 준수하고 전자 상거래, 은행 및 보험 분야에서 고객과 안전하게 데이터를 교환할 수 있는 데이터 보호 솔루션이 필요합니다. 감사자는 데이터 보호를 위한 PCI-DSS의 암호화 및 키 관리 요건을 충족할 수 있도록 FIPS(연방정보처리표준) 140-2 인증을 의무화하고 있습니다.

선도적인 금융 기술 기업이기 때문에 고객이 인증 및 금융 서비스를 준수하는 것은 중요합니다. 규제를 준수하지 못하면 보안 사고로 이어질 수 있으며, 이로 인해 데이터 유출과 막대한 벌금이 부과되고 브랜드 평판이 손상되며 전체 비즈니스가 위험에 처할 수 있습니다.

가장 중요한 것은 더 많은 파트너가 서비스에 참여하고 민감한 재무 데이터를 분석, 처리함에 따라 확대·확장할 수 있는 솔루션이 고객에게 필요하다는 것입니다.

PCI 데이터 보안 표준을 준수하지 못할 경우 일어날 수 있는 문제

PCI 보안 표준위원회에 따르면 규제를 준수하지 않는 기업은 다음과 같은 결과에 직면할 수 있습니다.

- 판매 감소
- 새 지불 카드 재발급 비용
- 사기로 인한 손실
- 법적 비용, 합의 및 판결
- 지불 카드 가맹 취소
- 실직(CISO, CIO, CEO 및 해당 전문직)
- 폐업

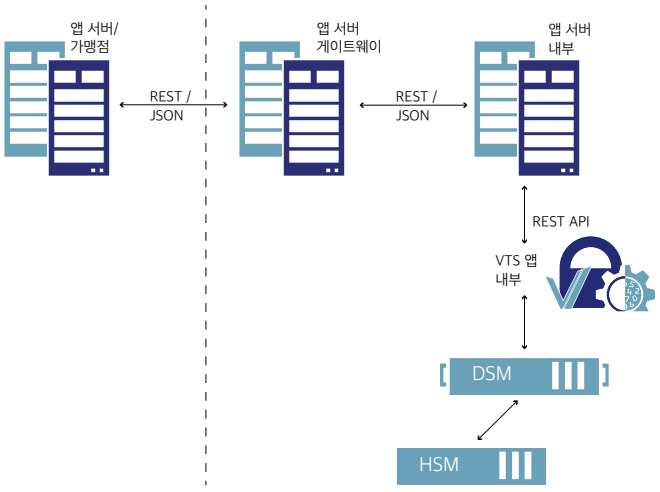
또한, 포네몬 연구소의 2019년 "데이터 유출 비용" 보고서에 따르면 데이터 유출의 평균 비용은 건 당 $150입니다.

솔루션

1단계에서의 요건은 고객 애플리케이션 내의 데이터에 암호화 서비스를 제공하는 솔루션을 배포하는 것입니다. 탈레스는 애플리케이션이 Rest API를 사용하여 암호화 서비스를 호출할 수 있는 CTS(CipherTrust Token Server) 사용을 제안합니다.

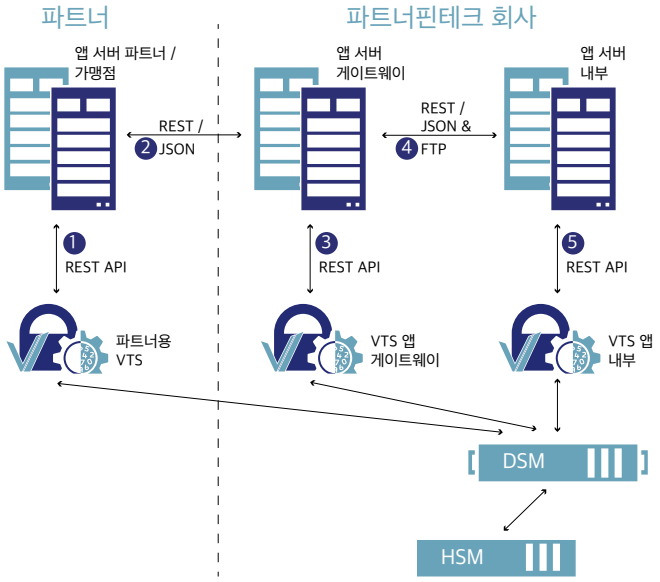
암호화에 사용되는 키는 탈레스 CipherTrust 데이터 보안 관리자(DSM) 내에서 안전하게 관리, 보호받습니다.

솔루션을 FIPS 140-2 레벨 3으로 검증해야 하는 감사자 요건의 일환으로, 고객은 DSM의 ROT(신뢰 기반)로 기존에 이용하던 탈레스 Luna 범용 하드웨어 보안 모듈(GP HSM)을 활용합니다.



배포 1단계

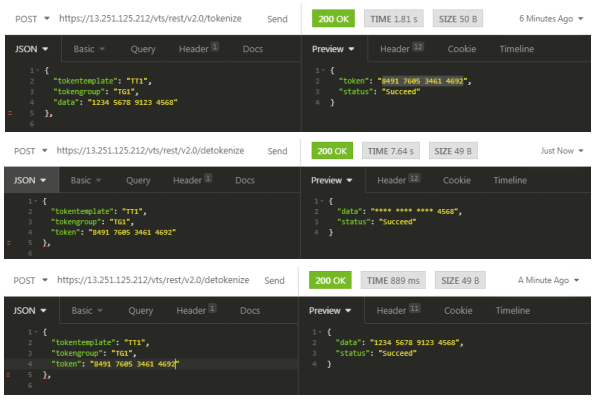
제안 솔루션을 모두 적용하면 게이트웨이 서버와 사내 서버 간에 FTP를 통해 전송하기 전에 비정형 데이터를 암호화할 수 있습니다.



전체 토큰화 아키텍처

1. 토큰화 단계: 파트너는 데이터 전송 전에 데이터를 토큰화합니다.
2. 게이트웨이 서버 전송: 파트너는 토큰화 데이터를 핀테크 고객 게이트웨이 서버로 전송합니다.
3. 역토큰화: 핀테크 고객의 게이트웨이 서버는 내부 처리를 위해 데이터를 역토큰화합니다.
4. 내부 서버 전송: 처리된 데이터를 내부 서버로 전송하기 전에 암호화합니다.
5. 데이터 분석 단계: Finnet 내부 서버가 분석, 처리 및 저장 목적으로 메시지를 해독합니다.

* 모든 'Vormetric' 및 'Keysecure' 명칭은 2020년 9월부터 'CipherTrust'로 변경됩니다.



다양한 토큰화 단계

규제 준수 요건 충족

규제 준수 상태 유지는 금융 기술 부문에서 고객과의 신뢰를 구축하고 유지하는 데 있어 중요한 비즈니스 요건입니다. 규제 준수는 일회성 연례행사가 아닙니다. 규제 준수를 따르고 유지하는 것은 PCI 모범 사례에 따라 규제 요건을 지속적으로 충족하는 비즈니스 과제로 생각해야 합니다.

Vormetric Data Security Manager 사용

Vormetric Data Security Manager(DSM)는 모든 Vormetric Data Security Platform 제품을 위한 중앙 집중식 공용 관리 환경입니다. 정책 제어와 암호키의 보안 관리 및 저장 기능을 제공하며 웹 기반 콘솔과 CLI, SOAP 및 REST API를 포함합니다.

토큰화 솔루션 활용

Vormetric Data Security manager는 금융 서비스를 지원하는 토큰화 솔루션을 갖추고 있으며, 증가하는 데이터 유출 및 사기 사례에 대응하기 위해 가장 많이 찾는 솔루션입니다. 토큰화는 데이터를 민감하지 않은 데이터로 대체하여 도난당한 경우에도 데이터를 사용할 수 없게 만들어 데이터에 대한 보안을 제공합니다. 인식 불가능한 토큰화 데이터 형식을 생성하며 이는 소스 데이터의 형식을 유지합니다.

금융 서비스 부문에서 자금 세탁 방지 이니셔티브는 개인 식별 정보(PII)에 대한 개인정보 보호 및 보안을 유지하면서 데이터를 분석해야 합니다.

토큰화된 데이터는 데이터베이스 스키마를 변경하지 않고 원본 데이터 대신 사용할 수 있으므로 기존 애플리케이션과 시스템을 유지하고자 하는 조직에 큰 이점이 됩니다.

탈레스 Vormetric Data Security Platform, 사용하기 쉬운 종합 저장 데이터 보안 솔루션

HSM 소개

하드웨어 보안 모듈

탈레스는 오늘날 시장에서 가장 성능이 뛰어나고 가장 안전하며 통합하기 가장 쉬운 업계 최고의 하드웨어 보안 모듈(HSM) 제품군을 제공합니다. FIPS 140-2 레벨 3 인증을 받은 고보증성 침해 방지 장치에서 데이터와 디지털 ID를 암호화하는 마스터키를 보호하여 트러스트 앵커 역할을 담당합니다. 탈레스는 목적별로 다음과 같은 유형의 HSM을 제공합니다.

범용 HSM

Luna HSM은 네트워크 어플라이언스, 임베디드 PCIe 모듈 및 휴대용 USB 등 다양한 폼팩터로 제공됩니다. 광범위한 애플리케이션과 쉽게 통합되어 일반 암호화 작업 속도를 높이고 암호키 수명 주기를 보호하며 전체 암호화 인프라에서 RoT(신뢰 기반) 역할을 담당합니다. Crypto Command Center는 온프레미스나 가상 환경, 또는 하이브리드 클라우드 환경에서 여러 Luna HSM 암호화 리소스를 중앙에서 모니터링하고 관리하는 데 사용할 수 있습니다.

탈레스 소개

귀하의 데이터를 보호하는 기업들은 탈레스를 통해 자신들의 데이터를 보호합니다. 데이터 보안에 대해 중요한 결정을 내려야 하는 순간이 증가하고 있습니다. 암호화 전략을 수립하거나, 클라우드로 데이터를 이전하거나, 규제 준수 요구사항을 충족시켜야 하는 모든 순간에 탈레스를 믿고 찾아주십시오. 탈레스는 귀하의 안전한 디지털 트랜스포메이션을 지원합니다.

결단이 필요한 순간을 위한 결정적인 솔루션.