Vormetric Data Security Platform
데이터 시트

Vormetric Data Security Platform

데이터 유출사고가 끊임없이 발생하여 경각심을 높이고 있는 가운데 데이터 보안 규제는 점점 엄중해지고 있습니다. 오늘날 기업들은 보다 다양한 환경, 시스템, 애플리케이션, 프로세스 등을 고려한 사용자 전반에 걸친 데이터 보안을 강화해야 합니다. 탈레스의 Vormetric Data Security Platform을 사용하면 기업 전체의 저장 데이터에 대한 보안을 효율적으로 관리할 수 있습니다.

Vormetric Data Security Platform은 확장이 가능할 뿐 아니라 기존의 인프라에 효과적으로 연동되는 일련의 제품으로 구성되어있습니다. 또한, 효율적인 중앙 집중형 암호키 및 정책 관리 기능을 제공합니다. 이런 기능을 통해 보안 팀은 관리에 투입되는 노력과 TCO를 절감하면서 데이터 보안 정책, 규제 준수 및 모범사례를
따를 수 있습니다.

본 플랫폼은 데이터베이스, 파일 및 컨테이너에 대한 보호 및 액세스 제어기능을 제공하며 클라우드, 가상화, 빅데이터 및 물리적 환경의 자산 및 데이터를 보호합니다. 확장가능하고 경제적인 데이터 보안 플랫폼을 통해 사용자는 시급한 데이터 규제 준수 요구사항을 충족시키면서 향후 보안에 관련된 도전과제나 규제에 대비할 수 있습니다. 확장이 가능한 본 데이터 보안 플랫폼을 사용할 경우 현재 일어나는 긴급한 요구사항에 보다 손쉽게 대응할 수 있을 뿐 아니라, 향후에 일어날 수 있는 보안 이슈 및 규제에 신속하게 대응할 수 있도록 지원합니다.

기능

- 파일, 데이터베이스 및 컨테이너에 대한 투명한 암호화
- 애플리케이션 계층 암호화
- 토큰화
- 동적 및 정적 데이터 마스킹
- FIPS 140-2, CC 인증 키 관리
- 클라우드 키 관리
- 관리자 액세스 컨트롤
- 접근 감사 로깅
- 배치 데이터 암호화 및 토큰화

지원 환경 및 기술

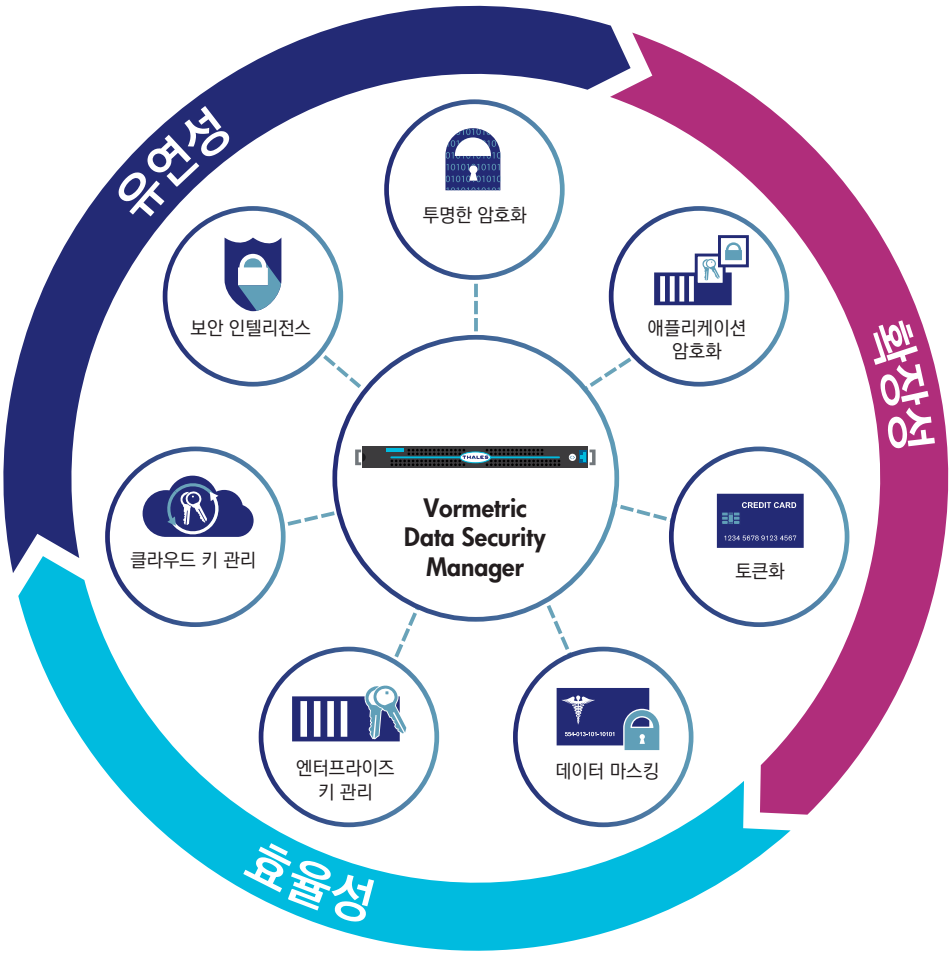
- IaaS, PaaS 및 SaaS: Amazon Web Services, Google Cloud Platform, Microsoft Azure, Salesforce, Microsoft Office365 및 PCF: Pivotal Cloud Foundry 내의 MySQL 데이터베이스
- 운영체제: Linux, Windows 및 Unix
- 빅데이터: Hadoop, NoSQL, SAP HANA 및 Teradata
- 컨테이너: Docker, Red Hat OpenShift
- 데이터베이스: IBM DB2, Microsoft SQL Server, MongoDB, MySQL, NoSQL, Oracle, Sybase 및 기타
- 모든 스토리지 환경

플랫폼의 장점

- 중앙 집중화된 저장 데이터 보안 정책
- Vormetric Data Security Platform 및 타사 암호화 제품의 키 관리
- 물리적, 가상화, 클라우드 및 빅데이터 환경 전반에서 일관적인 보안 및 규제 준수 제공
- 사전 정의된 SIEM 대시보드를 통해 상세하고 대응 가능한 파일 액세스 분석 정보 제공
- 유연성 및 확장성을 통해 추가적인 사용 사례에 대한 신속한 지원 가능
- 호환되는 HSM장비를 통해 데이터 암호키 제공
- FIPS 140-2 레벨 3 인증을 받은 HSM을 통해 높은 신뢰도 제공

규제 준수

- PCI DSS
- GDPR
- HIPAA/HITECH
- NIST 800-53
- FISMA
- 대한민국 개인정보 보호법
- 각 지역별 데이터 레지던시 및 개인 정보 보호 규제



보안 및 규제 준수의 강화

유연하고 확장 가능한 솔루션을 활용하여, 보안 팀은 기업전반에서 사용 사례를 광범위하게 활용하고 민감 데이터를 보호할 수 있습니다. 본 플랫폼은 광범위한 보안 및 개인정보 보호 요건에 대응할 수 있도록 설계되었습니다. 여기에는 PCI DSS, GDPR,HIPAA FISMA, 대한민국 개인정보보호법 및 각 국의 데이터 보안 규제가 포함됩니다. Vormetric Data Security Platform은 외부 위협에 대처하고 내부자 오용을 방지하며 지속적인 제어를 확립할 수 있는 강력한 기능을 제공합니다. 데이터가 클라우드나 외부 공급업체의 인프라에 저장된 경우에도 동일한 기능을 제공합니다.

운영 및 리소스 효율성 극대화

Vormetric Data Security Platform은 보다 쉽고 효율적으로 보안 관리를 할 수 있도록 지원합니다. 본 플랫폼은 직관적인 웹 기반 인터페이스, CLI 인터페이스는 물론 REST, SOAP, Java, .NET 및 C 언어 API를 지원합니다. 본 제품을 통해 기업은 저장 데이터에 대한 보안을 신속하고 일관성 있게 적용할 수 있으므로, IT 운영효율성과 생산성을 극대화할 수 있습니다. 뿐만 아니라 암호화 성능이 우수하므로 서버 리소스를 효율적으로 사용할 수 있고, 결과적으로 서비스에 필요한 인프라를 줄일 수 있습니다.

TCO 절감

Vormetric Data Security Platform은 저장 데이터에 대한 보안 과정을 단순화하고 비용을 절감시킵니다. 이 플랫폼은 IT팀과 보안 팀이 전사의 데이터를 일관적이고 반복적인 방식으로 신속하게 보호할 수 있도록 지원합니다. 또한, Vormetric Data Security Platform을 통해 일관성 있고 중앙화된 관리가 가능하므로 다수의 독립형 제품을 사용할 필요가 없습니다.

플랫폼 제품

Vormetric Data Security Platform에는 다음과 같은 제품들이 제공됩니다:

Vormetric Data Security Manager: 모든 Vormetric Data Security Platform 제품을 위한 중앙 집중화된 공용관리 환경을 제공합니다. 정책 제어는 물론 암호키의 안전한 관리 및 저장기능을 제공합니다. 웹 기반 콘솔, CLI, SOAP 및 REST API가 포함됩니다. FIPS 140-2 및 CC인증을 받은 가상 및 물리적 어플라이언스로 제공됩니다.

Vormetric Transparent Encryption: 서버 상에 소프트웨어 에이전트 형태로 설치되어 파일 시스템 또는 볼륨 계층에서 실행되는 제품입니다. 로컬 스토리지 및 클라우드 스토리지에 저장되어 있는 비정형 및 정형 데이터를 보호합니다.데이터센터, 클라우드 및 하이브리드 클라우드를 모두 지원하며 하드웨어 가속암호화 기능, 접근 통제 기능 및 데이터 액세스 감사 기능을 제공합니다. 다음과 같은 확장 및 추가 프로그램들이 있습니다:

- 컨테이너 보안: 도커(Docker™) 및 오픈쉬프트(OpenShift™) 컨테이너의 내부에서 실행되므로 다른 컨테이너와 프로세스, 심지어 호스트 운영시스템도 민감 데이터에 접근할 수 없게 만들 수 있습니다. 암호화, 접근통제 및 데이터 액세스 로그를 컨테이너 단위로 적용하는 기능을 제공합니다.
- Live Data Transformation: 파일 및 데이터베이스에 대해 애플리케이션 및 업무 중단 없이 암호화를 제공합니다. 주기적인 암호키 변경 기능도 제공합니다.
- Vormetric Transparent Encryption for Efficient Storage: 중복 제거 및 압축과 같은 핵심적인 스토리지 효율성을 유지하는 한편 데이터를 암호화하여 스토리지 시스템에 저장되는 데이터에 높은 수준의 보안을 제공합니다. 스토리지 효율성을 유지하면서도 최상의 데이터 보호 기능을 제공하는, 업계 최초의 솔루션입니다!
- Vormetric Transparent Encryption for SAP HANA: SAP HANA 환경에서 고급 저장 데이터 암호화, 액세스 컨트롤, 키 관리 및 데이터 액세스 감사 로깅을 제공합니다

Vormetric Tokenization with Dynamic Data Masking: Vormetric Tokenization 데이터베이스의 주요 필드를 보호하기 위한 포맷 보존 암호화(FPE)와 정책 기반의 동적 데이터 마스킹을 통한 디스플레이 보안을 손쉽게 구현할 수 있습니다.

Vormetric Application Encryption: 미국 국립표준 기술 연구소(NIST)의 표준인 AES 암호화와 형태 보존 암호화 (FPE)를 기존 애플리케이션에 손쉽게 추가할 수 있도록 지원합니다. 고성능 암호화 및 키 관리를 위한 표준 기반 API를 제공합니다.

Vormetric Batch Data Transformation: 데이터베이스의 민감한 컬럼 데이터를 보다 쉽고 빠르게 마스킹, 토큰화 또는 암호화할 수 있도록 지원합니다. Vormetric Tokenization 또는 Vormetric Application Encryption을 적용하기 전에 사용 가능합니다. 정적 데이터 마스킹 기능을 제공합니다.

Vormetric Key Management. Vormetric Data Security Platform 제품, TDE 및 KMIP 호환 제품 및 저장 인증서를 위한 키 관리 및 안전한 중앙 키 저장소를 제공합니다.

CipherTrust Cloud Key Manager: Salesforce, Microsoft Azure 및 AWS를 위한 암호키 관리 기능은 자신의 네이티브 환경 밖에서 암호키 전체 수명주기를 관리하기 위해 규제 준수 및 모범 사례를 충족해야 하는 기업의 니즈를 충족시킵니다. 기업이 암호화 전문가가 될 필요가 없습니다. 개인 클라우드 또는 온프레미스 배포 가능

Vormetric Protection for Teradata Database: 테라데이터 환경에서 저장 데이터를 위해 강력한 보안 기능을 빠르고 효율적으로 구현할 수 있도록 지원합니다. 테라데이터 데이터베이스의 특정 컬럼에 대한 암호화 및 사용자별 접근 통제 기능을 제공합니다.

Vormetric Security Intelligence: 관리자 계정의 접근을 포함, 파일 접근 활동에 대해 감사에 사용 가능한 세부적인 기록을 제공하는 상세 로그를 생성합니다. 보안 정보와 이벤트 관리 (SIEM) 시스템과의 통합 기능을 제공합니다. 규제 준수 보고를 간소화하고 위협 탐지를 가속화할 수 있도록, 사전에 패키지화된 대시보드와 보고서를 제공합니다.

Vormetric Data Security Manager

Vormetric Data Security Manager(DSM)는 모든 Vormetric Data Security Platform 제품에 대한 중앙 집중 관리 기능을 제공합니다. DSM을 사용하면 규정준수 요구사항 및 규제 요건을 효율적으로 충족시키고 업계 모범사례를 따를 수 있으며 배포 및 규제 사항이 변화해도 쉽게 대응할 수 있습니다. DSM 및 관련 제품은 LDAP, 액티브 디렉터리, OS 사용자 계정, 하둡 및 컨테이너 환경과 같은 사용자 및 그룹 관리 시스템과 통합되므로 보안 정책 관리 및 배포에 최적의 솔루션을 제공합니다.

강력한 보안과 안정성을 갖춘 FIPS 인증 시스템

가용성과 보안을 극대화하기 위해, DSM에는 고가용성 유지를 위한 어플라이언스 클러스터링 기능과 이중화 컴포넌트가 포함되어 있습니다. 한 명의 관리자가 데이터 보안 활동, 암호키 또는 관리에 대한 모든 통제력을 갖지 않도록 강력한 임무 분리 정책이 시행됩니다. 이외에도, DSM은 관리자에 대해 2팩터 인증을 지원합니다.

유연한 구현 옵션

DSM은 FIPS 140-2 레벨 1 가상 어플라이언스 뿐만 아니라 FIPS 140-2 레벨 2 인증을 받은 V6000과 FIPS 140-2 레벨 3 인증을 받은 V6100의 두 가지 하드웨어 어플라이언스로 제공됩니다. 하나는 FIPS 140-2 레벨 2 인증 V6000, 또 하나는 FIPS 140-2 레벨 3 인증 V6100입니다. 가상 어플라이언스는 VMware, Hyper-V, KVM,Amazon Web Services 및 Azure 에서 사용 가능합니다.

호환되는 HSM을 연동시키면 가상 또는 V6000 하드웨어 어플라이언스 DSM에 대해 FIPS 140-2 레벨 3 인증 RoT를 제공할 수도 있습니다.

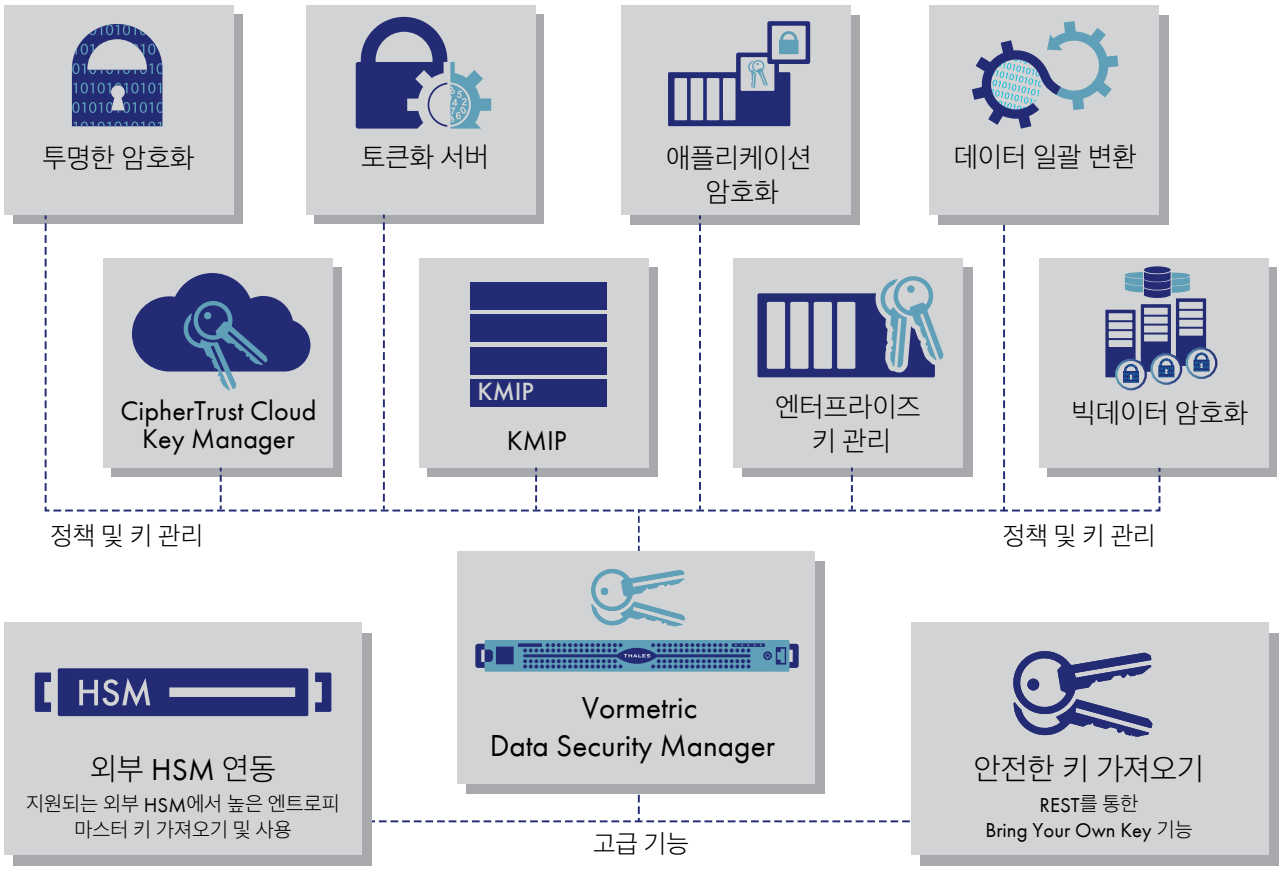
주요 기능

- 단일한 콘솔에서 모든 플랫폼 정책과 키 관리
- 멀티 테넌시 지원
- 10,000개 이상 에이전트 환경에서 검증된 확장성
- 고가용성을 위한 클러스터링
- 툴킷 및 프로그래밍 인터페이스
- 기존의 인증 인프라와 손쉬운 연동
- RESTful API 지원
- 멀티팩터 인증 및 HSM 내장 옵션
- 원격 관리

기술 사양

플랫폼 옵션:

- FIPS 140-2 레벨 1 가상 어플라이언스(호환되는 HSM 연동시 FIPS 140-2 레벨 3 RoT제공)
- FIPS 140-2 레벨 2 하드웨어 어플라이언스(호환되는 HSM 연동 시 FIPS 140-2 레벨 3 RoT제공)
- FIPS 140-2 레벨 3 하드웨어 어플라이언스(HSM 내장)
- 가상 어플라이언스는 Vmware, Hyper-V, KVM, Amazon Web Service, Azure와 호환됨



하이브리드 기업 전체에 걸친 통합 관리

DSM은 Vormetric Data Security Platform, IBM Security Guardium Data Encryption, 마이크로소프트 SQL TDE, 오라클 TDE 및 KMIP 호환 암호화 제품에서 생성된 키 등 이종 암호키에 대한 중앙화된 관리를 제공하여 비용을 절감시킵니다. DSM에는 암호키 및 정책 관리 그리고 전사적인 감사를 지원하는 직관적인 웹 기반 콘솔과 API가 포함되어 있습니다. 이 제품은 또한 중앙화된 로그 수집을 지원합니다.

DSM 사양

하드웨어 사양

섀시	1U 랙 장착 가능:43.18cm x 52.07cm x 4.5cm(폭x길이x높이)
중량	V6000: 21.5lbs (9.8kg); V6100: 22lbs (10kg)
메모리	16GB
하드 디스크	듀얼 SAS RAID 1 미국 FIPS 표준 봉인
직렬 포트	1
이더넷	2x1Gb
IPMI	1x10/100Mb
전원공급장치	착탈식 80+인증(100VAC-240VAC/50-60Hz) 400W 2개
섀시 침입 탐지	지원 환경 및 기술 상단 커버에 미국 FIPS 표준 봉인 제공
최대 BTU	최대 410 BTU
작동 온도	10°~35°C (50°~95°F)
비작동 온도	-40°~70°C (-40°~158°F)
작동 상대 습도	8%~90%(비응축)
비작동 상대 습도	5%~95%(비응축)
안전 기관 승인	FCC, UL, BIS 인증서
FIPS 140-2 레벨 3	V6100 모델, 호환되는 HSM 연동 시 V6100 또는 가상 어플라이언스 형태의 DSM에 FIPS 140-2 레벨 3 RoT 제공 가능
HSM 원격 관리	V6100만 해당; 옵션으로 제공되는 원격 관리자 툴 키트 필요

소프트웨어 사양

관리용 인터페이스	보안 웹, CLI, REST
관리 도메인 수	1,000+
API 지원	PKCS #11, Microsoft Extensible Key Management (EKM), SOAP, REST
보안 인증	사용자ID/비밀번호, RSA 멀티 팩터 인증(옵션)
클러스터링 지원	포함
백업	수동 및 예약 보안 백업. M-of-N 키 복원.
네트워크 관리	SNMP, NTP, Syslog-TCP
Syslog 형식	CEF, LEEF, RFC 5424
인증 및 유효성 검사	FIPS 140-2 레벨 1, FIPS 140-2 레벨 2, FIPS 140-2 레벨 3 CC인증(ESM PP PM V2.1)

가상 기계 최소 사양—가상 어플라이언스 기준 권고 사항

CPU 수	2
RAM(GB)	4
하드디스크(GB)	100GB
씬 프로비저닝 지원	지원

Vormetric Transparent Encryption

Vormetric Transparent Encryption은 저장 데이터에 대한 암호화, 사용자 접근 권한 통제 및 보안 인텔리전스 로그 수집 기능을 제공합니다. 본 솔루션은 가상화 및 물리적 환경, 빅데이터, 도커 및 클라우드 환경에 존재하는 정형 및 비정형 데이터 보안을 유지할 수 있습니다.

이 솔루션이 제공하는 투명한 암호화 방식은 애플리케이션, 인프라 또는 업무 절차를 변경하지 않고 암호화를 구현할 수 있도록 지원합니다. 암호키를 적용하기만 하는 다른 솔루션과 달리, Vormetric Transparent Encryption은 사용자와 프로세스의 무단 접근을 방지하는 정책을 적용하고 관련 액세스 로그를 지속적으로 수집합니다. 최소한의 노력과 비용으로 무중단 구축이 가능하므로 구축단계는 물론 이후 운영 단계에서도 비즈니스 업무 및 운영 절차를 변경할 필요가 없습니다.

암호화 및 접근 관리에 대한 규제준수 요건 충족

암호화, 액세스 제어 및 데이터 액세스로깅은 PCI DSS, HIPAA/Hitech, GDPR 등 거의 모든 규제 및 데이터 개인정보 보호표준을 준수하기 위해 필요한 기본 요구사항입니다. Vormetric Transparent Encryption은 운영프로세스 또는 비즈니스프로세스 변경 없이 규제 준수에 필요한 모든 기능을 제공합니다.

확장 가능한 암호화

Vormetric Transparent Encryption은 서버의 파일 시스템 계층 또는 볼륨 계층에서 실행되는 에이전트입니다. 이 에이전트는 Windows, Linux 및 Unix를 포함한 광범위한 플랫폼을 지원하며, 또한 도입된 스토리지 기술에 상관없이 물리적, 가상, 클라우드 및 빅데이터 환경에서 사용될 수 있습니다. 관리자들은 Vormetric Data Security Manager(DSM)를 통해 정책과 키 관리 등 모든 관리 작업을 수행할 수 있습니다.

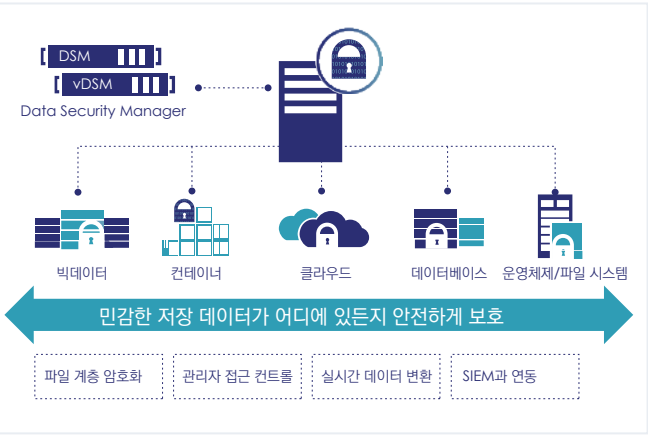
암호화를 서버상에서 수행할 수 있으므로, 프록시 방식 레거시 솔루션의 골칫거리라 할 수 있는 병목 현상이 없습니다. 또한, Intel AES-NI, IBM POWER9 등 최신 CPU에 내장된 암호화 하드웨어 모듈을 활용함으로써 성능과 확장성이 한층 향상됩니다.

주요 장점

- 다양한 플랫폼과 환경을 지원하는 암호화를 통해 규제준수 및 모범사례 요구사항 충족
- 쉬운 구현: 애플리케이션 수정 불필요
- 시스템 관리자 권한을 가진 내부자의 오용에 대한 강력한 방어 구축

주요 기능

- 업계에서 가장 광범위한 플랫폼 지원: Windows, Linux 및 Unix 운영체제
- 고성능 암호화: 호스트 CPU에 내장된 하드웨어 암호화 기능 사용 - Intel 및 AMD AES-NI 및 POWER9 AES 암호화
- Suite B 프로토콜 지원
- 사용자, 애플리케이션 및 프로세스에 의한 모든 허용, 차단 및 제한된 접근 시도 로그 기록
- 역할 기반의 접근 정책으로 누가, 무엇을, 어디서, 언제, 어떻게 접근할지 통제 가능
- 관리자가 데이터 내용을 복호하지 않고 관리 작업 수행 가능
- 확장 기능: 컨테이너 수준 암호화, 고성능 스토리지 암호화, 무중단 데이터 암호화 기능



Vormetric Transparent Encryption은 데이터의 위치에 위치에 관계 없이 모든 데이터를 보호할 수 있습니다.

세분화된 사용자 접근 제어

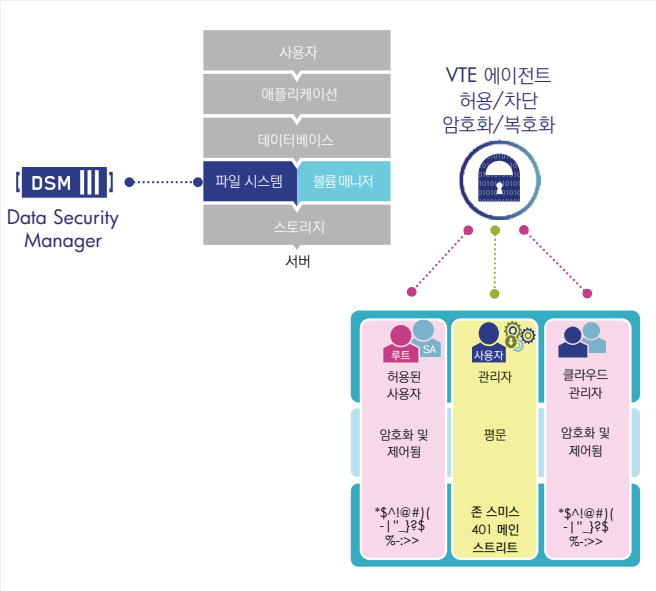
외부 공격 및 오용으로부터 데이터를 보호하기 위해 세부적인 최소 권한 사용자 접근 정책을 시행합니다. 시스템, LDAP/Active Directory, Hadoop 및 컨테이너의 사용자/그룹별로 특정 정책을 고유하게 적용할 수 있습니다. 프로세스, 파일유형, 시간 등 다른 조건으로 액세스 정책을 설정할 수도 있습니다.

쉽고 빠른 설치

Vormetric Transparent Encryption 에이전트는 파일시스템 또는 볼륨레벨에서 동작하며 Linux, Unix, Window 파일시스템 및 Amazon S3 및 Azure와 같은 클라우드 저장소를 지원합니다. 설치를 위해 응용프로그램, 사용자 워크플로우, 운영방법, 운영프로세스를 변경 할 필요가 없습니다.

클라우드 데이터 보호

암호화 대상이 온프레미스, 클라우드, 또는 하이브리드 환경에 분산된 경우에도 암호키 및 액세스 정책을 고객 데이터센터에서 관리할 수 있습니다.



관리자 계정 액세스 통제

기술 사양

암호화 알고리즘

- AES, 3DES, ARIA

유료 확장 기능

- 무중단 데이터 암호화
- 실시간 데이터 변환
- 고효율 스토리지

플랫폼 지원

- Microsoft: Windows Server 2019, 2016 및 2012
- Linux: Red Hat Enterprise Linux (RHEL), SuSE Linux Enterprise Server, Ubuntu, Amazon Linux
- UNIX: IBM AIX*

데이터베이스 지원

- IBM DB2, Microsoft SQL Server, Microsoft Exchange Data Availability Group (DAG), MySQL, NoSQL, Oracle, Sybase 및 기타

애플리케이션 지원

- Documentum, SAP, SharePoint, 사용자 개발 애플리케이션등 모든 애플리케이션에 투명하게 적용

빅데이터 지원

- Hadoop: Cloudera, Hortonworks, IBM
- NoSQL: Couchbase, DataStax, MongoDB
- SAP HANA
- Teradata

암호화 하드웨어 가속

- AMD 및 Intel AES-NI
- IBM POWER9 암호화 코프로세서

에이전트 인증서

- FIPS 140-2 레벨 1

컨테이너 지원

- Docker, Red Hat OpenShift

클라우드 지원

- AWS: EBS, EFS, S3, S3I, S3 Glacier
- AZURE: Disk Storage, Azure Files
- PCF: Pivotal Cloud Foundry 내의 MySQL 데이터베이스

** IBM AIX는 Vormetric Transparent Encryption, 버전 5.3 에이전트로만 지원 가능*

Live Data Transformation

저장 데이터의 암호화 구축 시 가장 어려운 문제 중 하나는 기존 데이터를 암호화 하거나 이미 암호화된 데이터의 암호키를 변경하는 것입니다. 기존에는 이를 위해 계획된 다운타임이나 인력에 의한 데이터 복제 및 동기화 작업이 요구되었습니다. Vormetric Transparent Encryption의 추가기능인 Live Data Transformation은 이러한 장애물을 제거하여 암호화 및 암호키 변경에 전례 없는 가동 시간과 관리 효율성을 제공합니다.

무중단 암호화 및키 교체

Live Data Transformation은 다음과 같은 주요 기능을 제공합니다:

무중단 암호화 구현 이 솔루션은 관리자들이 다운타임 없이 사용자, 애플리케이션 또는 작업의 흐름에 지장을 주지 않고 데이터를 암호화할 수 있도록 지원합니다. 암호화가 진행되는 동안, 사용자와 프로세스는 여느 때처럼 데이터베이스나 파일시스템을 사용할 수 있습니다.

보안 수준 향상 많은 규제를 준수하기 위해서는 정기적인 키 변경 작업이 요구됩니다. Live Data Transformation은 이러한 요구사항을 신속하고 효율적으로 충족시킬 수 있습니다. 본 솔루션은 데이터를 복제하거나 관련된 애플리케이션의 구동을 중단하지 않고 키를 변경할 수 있도록 지원합니다.

지능적인 리소스 관리 대규모 데이터 세트의 암호화에는 많은 시간과 상당량의 CPU 리소스가 필요합니다. Live Data Transformation은 정교한 CPU 관리 기능을 제공하여 관리자들이 암호화와 다른 비즈니스 운영을 위한 리소스 수요 사이에 균형을 유지할 수 있도록 지원합니다. 예를 들어, 관리자는 근무 시간 중에는 암호화로 시스템 CPU의 10%만 소비하도록 하고, 야간 및 주말에는 암호화로 CPU의 70%를 사용하도록 리소스 관리 규칙을 정의할 수 있습니다.

백업 및 아카이브 버전화 Live Data Transformation의 암호키 버전 관리 기능은 이전 암호키로 암호화된 데이터도 신속하게 복원할 수 있도록 지원합니다. 데이터 복구작업 시, Vormetric Data Security Manager로부터 아카이브된 암호키가 복구되어 자동으로 이전 데이터세트에 적용됩니다. 복구된 데이터는 현재의 암호키로 암호화됩니다.

주요 장점

- 다운타임 및 추가 스토리지 없이 암호화 구현
- 암호화 구현 및 유지관리와 관련된 비용 절감
- 암호화가 서비스 가용성에 미치는 영향 극소화
- 무중단 키 변경을 통해 보안 및 규제 준수 강화
- 이전 키로 암호화된 데이터를 신속하게 복구

기술 사양

운영체제 지원

- Microsoft: Windows Server 2019, 2016 및 2012
- Linux: Red Hat Enterprise Linux(RHEL) 6, 7 및 8, SuSE Linux Enterprise Server 11, 12 및 15

클러스터 지원

- Microsoft Cluster: File Cluster, SQL Server Cluster

데이터베이스 지원

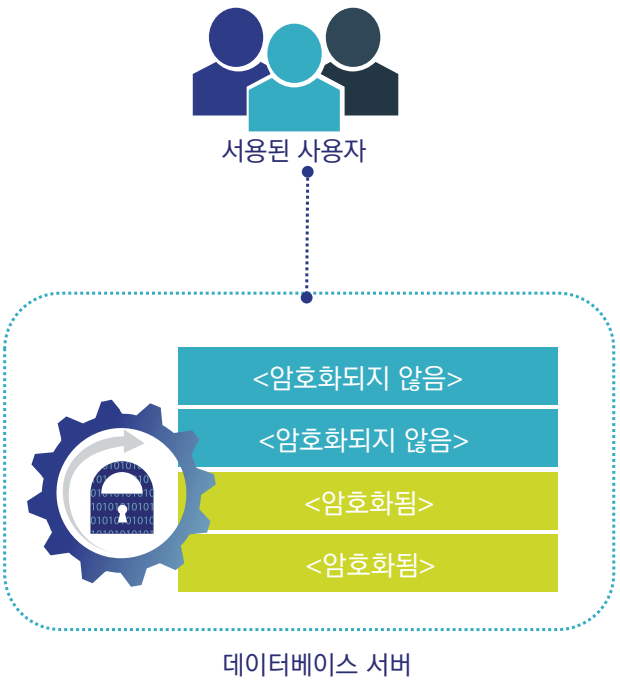
- IBM DB2, IBM Informix, Microsoft SQL Server, Oracle, Sybase 및 기타

빅데이터 지원

- Cassandra, CouchBase, Hadoop, MongoDB, SAP HANA

백업/복제 지원

- DB2 backup, NetBackup, NetWorker, NTBackup, Oracle Recovery Manager(RMAN), Windows Server Volume Shadow Copy Service(VSS)

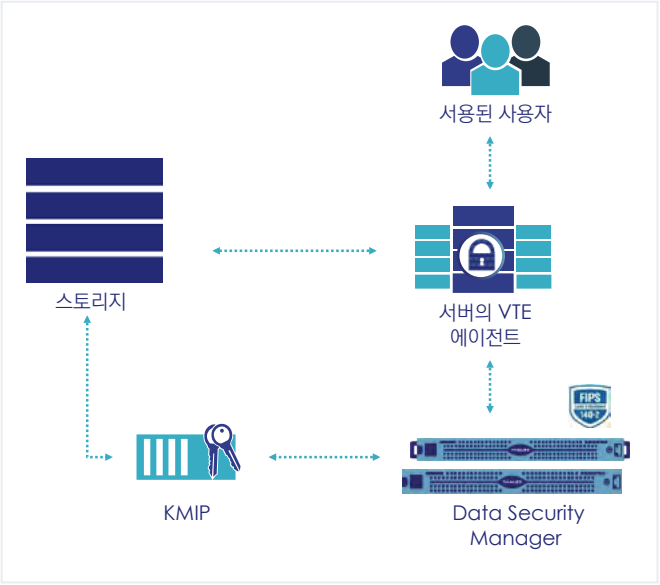


Vormetric Transparent Encryption 확장 및 추가 프로그램

Vormetric Transparent Encryption

VTE for Efficient Storage를 사용하면 더 이상 데이터 보안과 스토리지 효율성 중에서 하나를 선택할 필요가 없습니다. 둘 다 가질 수 있기 때문입니다! 이 솔루션은 중복 제거 및 압축과 같은 핵심적인 스토리지 효율성을 유지하는 한편 데이터를 암호화하여 궁극적으로 기업 스토리지 시스템에 저장되는 데이터에 높은 수준의 보안을 제공합니다. VTE for Efficient Storage는 스토리지 효율성을 유지하면서도 최상의 데이터 보호 기능을 제공하는, 업계 최초의 솔루션입니다:

Vormetric Transparent Encryption과 스토리지 어레이 간의 보안 키 공유 기술을 사용하여, VTE를 실행하는 호스트의 암호화된 데이터를 스토리지 솔루션이 분석하고 압축 및 중복 제거한 다음 데이터를 암호화한 상태로 어레이에 안전하게 저장할 수 있도록 지원합니다. 데이터 저장 및 보안에 있어 최상의 선택이 될 것입니다.



Vormetric Transparent Encryption

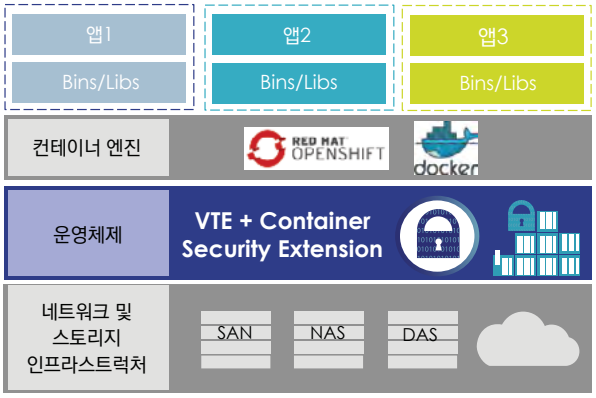
Vormetric Transparent Encryption for SAP HANA

Vormetric Transparent Encryption은 SAP HANA 데이터를 엄격한 보안, 데이터 거버넌스 및 규제 준수 조건 충족과 함께 보호하는 검증된 접근 방식을 제공합니다. SAP HANA 시스템, 데이터베이스 및 하드웨어 인프라를 변경할 필요없이 신속하게 솔루션을 구현할 수 있습니다. 이 솔루션을 통해 기업은 SAP HANA 데이터 및 로그 볼륨을 암호화하고 강력한 거버넌스 및 책임 분리를 설정할 수 있습니다.

Vormetric Transparent Encryption Container Security

Vormetric Container Security는 정책 기반의 Vormetric Transparent Encryption 파일 계층 암호화, 접근 관리, 데이터 접근 감사 로깅 기능을 Docker 및 OpenShift 컨테이너 환경까지 확대할 수 있습니다. 이 솔루션을 사용하면 사용자는 이미지변경 없이 컨테이너 이미지 내부에 저장되는 데이터를 파일 계층에서 암호화할 수 있을 뿐 아니라 접근제어도 가능합니다.

이 솔루션은 규제 준수, 규제 및 모범 사례 요구 사항을 준수하는 데 필요한 상세한 가시성과 제어기능을 제공합니다. 세분화된 데이터 접근 정책은 컨테이너 환경 내에서뿐만 아니라 기본 시스템 계층에서 관리자가 접근제어를 할 수 있도록 지원합니다. 정책에는 민감 데이터에 접근할 수 있는 사람, 대상, 장소, 시기 및 방법이 포함됩니다.



컨테이너 계층 암호화

컨테이너 보안 기술 사양

플랫폼/환경 지원

- Docker 및 Red Hat OpenShift
- Red Hat Enterprise Linux, 8.x
- 물리적 시스템, 가상 기계 및 AWS EC2 인스턴스 상에서 작동

Vormetric Security Intelligence

Vormetric Security Intelligence는 사전 연동된 주요 SIEM 솔루션과의 연동을 통해 보안 이벤트로그를 제공하여 파일 액세스 활동에 대한 전례없는 통찰을 제공합니다. Vormetric Transparent Encryption 및 Vormetric Data Security Manager로 이용할 수 있는 데이터 액세스 감사 로깅 기능에 기반한 이 정보는, Vormetric Transparent Encryption 에이전트가 구성되어있는 곳이면 어디서나 무단 액세스 시도뿐만 아니라 인증된 데이터 액세스에 대해서도 모든 세부 정보를 담을 수 있습니다. DSM의 정보에는 보안 관리자의 조치도 포함되어 있는데, 이는 규제 준수 감사 목적에 필요한 또 다른 항목입니다.

이 로그는 SIEM 시스템에서 사용되는 공용 형식으로 제공되며, DSM에서 중앙 집중형으로 수집되고, 당사 SIEM 파트너와 함께 사전 구축된 대시보드를 통해 고객은 즉시 효과를 볼 수 있습니다. 대시보드에는 무단 접근 시도가 표시되기 때문에 무단 접근 시도에 대한 즉각적인 경고가 가능합니다.

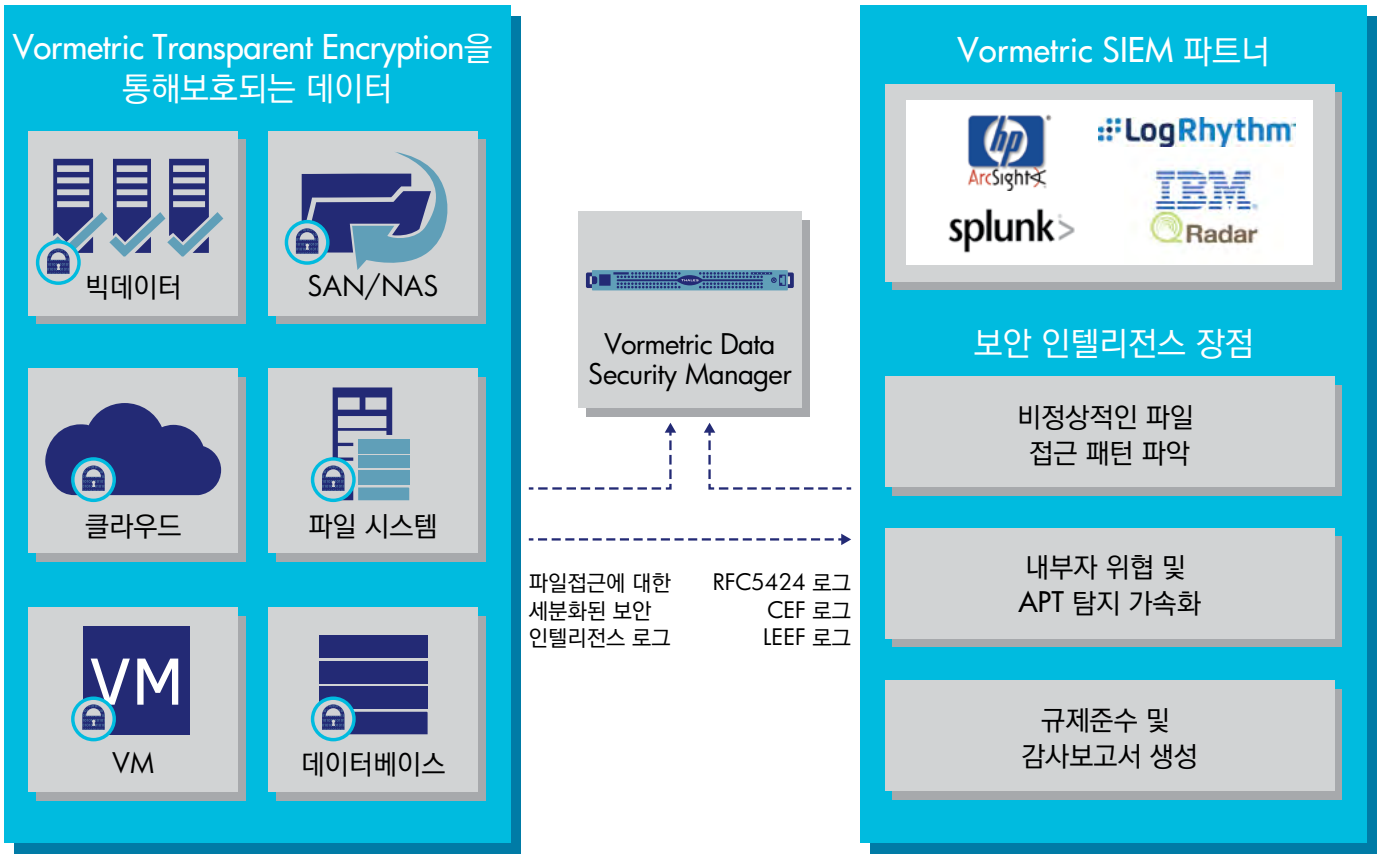
생성된 데이터 세트를 기반으로 민감 데이터에 접근하는 사용자 및 애플리케이션에 따른 접근 패턴의 기준을 작성할 수도 있습니다. 작성된 접근 패턴 기준은 위협이 될 수도 있는 비정상적인 접근 패턴을 식별할 수 있도록 지원합니다.

주요 기능

- 무단 액세스를 시도하는 잠재적인 멀웨어 또는 악의적 내부자 탐지
- 악성 코드(또는 악의적 내부 사용자)에 의한 데이터 도난 징후를 보여주는, 보호된 데이터에 대한 비정상적인 사용자 접근 패턴 파악
- 멀웨어에 의한 프로세스 병합 선택 징후를 보여주는 비정상적 사용 패턴과 비교 대조하여 보호된 데이터에 대한 프로세스 접근 모니터링
- 권한 없는 사용자의 Vormetric Data Security Management 어플라이언스에 대한 공격 파악

SIEM 파트너 연동

- FireEye Threat Prevention Platform
- Micro Focus ArcSight
- IBM Security QRadar SIEM
- Informatica Secure@Source
- McAfee ESM
- LogRhythm Security Intelligence Platform
- SolarWinds
- Splunk



Vormetric Tokenization with Dynamic Data Masking

Vormetric Tokenization with Dynamic Data Masking은 GDPR 및 PCI-DSS과 같은 보안 정책 및 데이터 규제를 준수하는 데 투입되는 비용과 노력을 절감시킬 수 있도록 지원합니다. 민감한 자산이 데이터 센터, 빅데이터 환경, 클라우드 등 어디에 있든지 관계없이 이를 보호하고 익명화할 수 있습니다.

간소화된 토큰화

Vormetric Tokenization은 민감 데이터 보호를 위한 형태 보존 암호화 또는 랜덤 토큰화 기능을 제공합니다. 정책 기반의 동적 데이터 마스킹으로 사용 중인 데이터를 보호합니다. 중앙 집중형 관리 및 서비스와 함께 RESTful API를 사용하여 필드 당 한 줄의 코드로 토큰화를 구현할 수 있습니다. 중앙 집중형 토큰화 서버 관리 및 구성에는 그래픽 사용자 인터페이스로 편리하게 토큰화 구성 워크플로우를 파악할 수 있는 운영 대시보드가 포함되어 있습니다.

동적 데이터 마스킹. AD 또는 LDAP 서버에 의해 제어되는 사용자 식별에 기반하여 특정 필드의 마스킹 범위를 전적 또는 부분적으로 선택하여 정책이 결정됩니다.

예를 들어, 고객서비스 담당자는 신용카드 번호의 마지막 4자리 숫자만 조회할 수 있고, 고객서비스 관리자는 신용카드 번호 전체를 조회할 수 있도록 정책을 수립할 수 있습니다.

무중단. 형태 보존 토큰화는 데이터베이스 스키마를 변경하지 않고도 주요 데이터를 보호할 수 있도록 지원합니다.

기술 사양

토큰화 기능:

- 비가역 옵션이 포함된 형태 보존 암호화 토큰(FF1 또는 FF3, 문자/숫자)
- 랜덤 토큰(영숫자/숫자, 데이터 길이 최대 128K)
- 데이터 토큰화
- FPE 및 랜덤 토큰 모두 Luhn 검사를 통과하도록 구성 가능

동적 데이터 마스킹 기능:

- 정책 기반, 노출되는 표시할 왼쪽/오른쪽 문자 수 (마스크 문자 사용자 정의 가능)

설치 가능 형태 및 옵션:

- Open Virtualization Format (.OVA) 및 International Organization for Standardization (.iso)
- Microsoft Hyper-V VHD
- Amazon Machine Image(.ami)
- Microsoft Azure Marketplace
- Google Cloud Platform

시스템 요구사항:

- 최소 하드웨어: 4 CPU 코어, 16-32 GB RAM
- 최소 디스크: 80GB

애플리케이션 연동:

- RESTful API

인증 연동:

- Lightweight Directory Access Protocol(LDAP)
- Active Directory(AD)
- 클라이언트 인증서
- OAuth2

성능:

- RAM 16GB의 32코어 서버(듀얼 소켓 Xeon E5-2630v3)에서 각 토큰 서버(다중 스레드 및 배치(또는 벡터) 모드 사용)당, 초당 백만 개 이상의 신용카드 크기 데이터 토큰화 트랜잭션 처리

Vormetric Application Encryption

Vormetric Application Encryption은 암호키 관리, 서명 및 암호화 서비스를 제공하여 파일, 데이터베이스 필드, 빅데이터 및 IaaS 환경의 데이터를 포괄적으로 보호합니다. 이 솔루션은 PKCS#11 표준 기반으로, FIPS 140-2 레벨-1 인증을 받았으며 실용적인 활용사례를 기반으로한 확장사례들을 기준으로 문서화시켰습니다. Vormetric Application Encryption은 맞춤형 데이터 보안 솔루션의 개발을 가속화합니다.

암호화 구현 간소화

Vormetric Application Encryption 솔루션은 애플리케이션에 키 관리 및 암호화 기능을 추가하는 절차를 간소화시킵니다. 개발자는 PKCS#11 라이브러리와 연결된 RESTful API나, C 또는 Java 기반 API를 사용하여 맞춤형 데이터 보안 솔루션에 표준기반 키 관리 및 데이터 암호화 서비스를 구현할 수 있습니다.

안전한 클라우드, 데이터베이스 및 빅데이터

애플리케이션 계층에서 특정 필드를 암호화해서 민감한 데이터가 데이터베이스, 빅데이터, 클라우드 환경에 저장되기 전에 보호하도록 요구하는 모든 규제를 준수할 수 있습니다.

기술 사양

암호화 알고리즘

- AES, 3DES, HMAC-SHA, HMAC MD5, RSA, FPE FF1/FF3

지원 환경:

- 웹 서비스를 지원하는 모든 서버의 RESTful API; Vormetric Tokenization Server 필요
- Microsoft Crypto Next Generation(CNG) 용 KSP(Key Services Provider)

운영체제 및 언어/바인딩 지원:

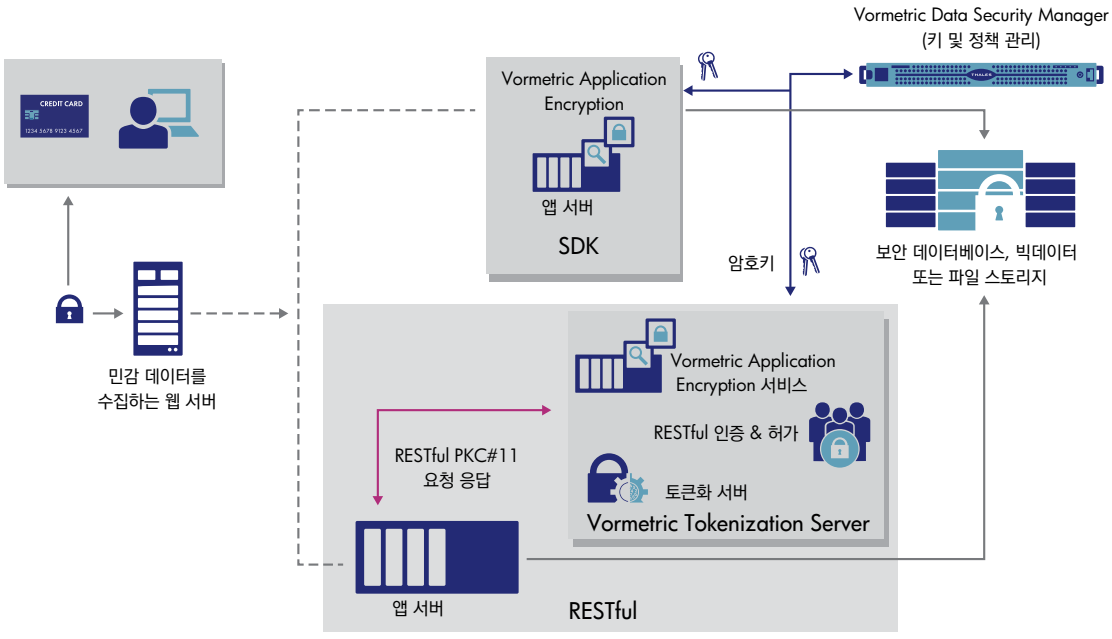
- Windows Server 2008/2012/2016: C, .NET, Oracle/Sun JDK
- Linux: C, Oracle/Sun JDK

보안 계층

- 권한 분리
- 호스트 등록 및 호스트 수준 PIN
- 애플리케이션 계층 키 접근
- RESTful 사용자 ID 및 비밀번호 또는 클라이언트 인증서
- RESTful 키 사용 및 운영 제어

인증:

- FIPS 140-2 레벨 1



Vormetric Application Encryption 선택사항: SDK 또는 RESTful

Vormetric Batch Data Transformation

Vormetric Batch Data Transformation은 데이터 웨어하우스, 온프레미스 및 클라우드 환경상의 빅데이터, 개발팀이나 아웃소싱 데이터 분석회사를 위한 데이터 변환을 안전하고 신속하며 효율적으로 수행할 수 있는 정적 데이터 마스킹 기능을 제공합니다.

유연한 데이터 마스킹

Vormetric Batch Data Transformation은 Vormetric Application Encryption과 Vormetric Tokenization with Dynamic Data Masking 둘 모두를 지원합니다. Vormetric Application Encryption의 경우 로컬에 설치된 에이전트를 활용하여 암호화 및 키 관리를 수행하고, Vormetric Tokenization Server의 경우 서버를 통해 토큰화 및 데이터 마스킹 서비스를 실행합니다.

디지털 트랜스포메이션을 위한 보안

변환 옵션에는 파일 또는 지원되는 데이터베이스에 대한 암호화 또는 토큰화가 포함됩니다. 사용 사례:

- 빠른 암호키 변경
- 빅데이터 소비자, 개발팀 또는 외주업체와의 안전한 데이터베이스/데이터 추출 공유
- 안전한 클라우드 마이그레이션을 위한 데이터 준비
- 토큰화 또는 애플리케이션 계층 암호화를 적용하기 위한 초기 암호화

주요 장점

- 유연한 보안으로 새로운 데이터 사용 가능
- Vormetric Application Encryption을 기반으로 하는 동적 데이터 마스킹 또는 맞춤형 애플리케이션을 통해 Vormetric Tokenization 구현 가속화
- Vormetric Data Security Platform에 대한 기존 투자의 활용 및 확장

기술 사양

데이터 변환 옵션:

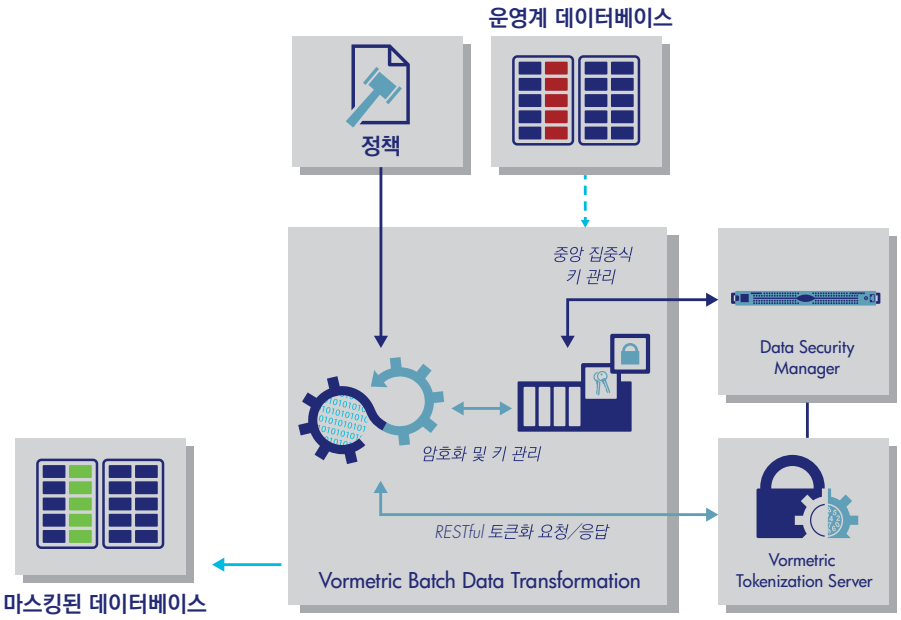
- 토큰화: 형태 보존 FF1/FF3, 랜덤 토큰화 데이터
  암호화: AES, FF1/FF3
- 알파벳 및 숫자 형태 보존

정책 파일 옵션:

- 개별 컬럼 별 변환 방식 설정 - 암호화, 토큰화, 토큰화 해제 및 키변환
- 애플리케이션 변경 없이 손쉽게 암호화 적용
- 유연한 키 관리 옵션 - 키를 DSM 또는 서버에 저장, 다중 암호키 지원

하드웨어 및 운영체제 요건:

- 최소 4코어 프로세서 및 16GB RAM
- Java Runtime Environment(JRE)
- Windows
- Linux - RedHat, CentOS, Ubuntu 및 SUSE



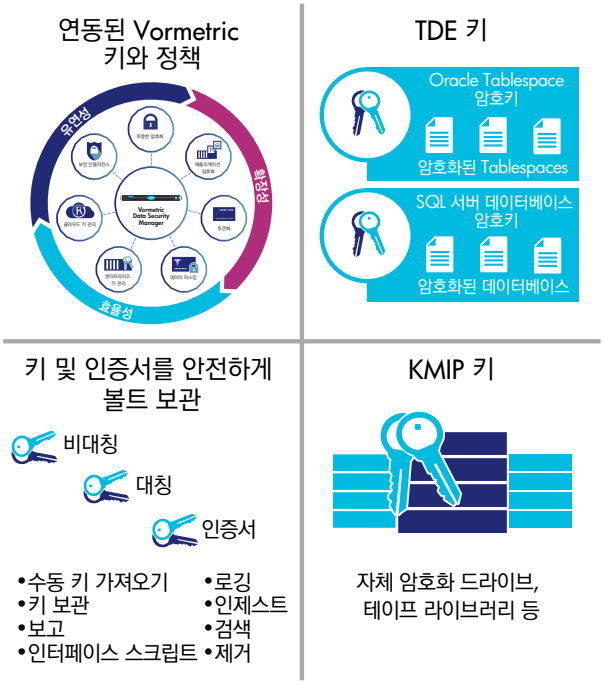
Vormetric Key Management

Vormetric Key Management를 사용하면 모든 Vormetric Data Security Platform 제품군의 암호키를 포함하여 IBM Security Guardium Data Encryption, Microsoft SQL TDE, Oracle TDE , KMIP 호환 암호화 제품을 포함한 타사 제품의 암호키와 인증서를 중앙에서 안전하게 저장하고 관리할 수 있습니다. 본 제품을 사용하면 통합 키 관리가 가능해져 다양한 시스템에서 일관적인 정책 구현을 촉진할 수 있을 뿐 아니라, 교육 및 유지보수 비용을 절감할 수 있습니다.

키 관리 및 전자인증서 보관 간소화

암호화를 사용하는 애플리케이션과 디바이스의 수가 늘어나면서, 키 관리 시스템의 수도 더불어 증가하고 있습니다. 이렇듯 나날이 증가하는 키 관리 시스템들로 인해 암호화된 환경에서 높은 수준의 가용성을 유지하는 것이 한층 더 복잡해졌을 뿐 아니라 비용도 많이 소요됩니다. 또한 이러한 각양각색의 키 관리 시스템들은 중요한 인증서들을 미보호 상태로 남겨놓아 해커들의 손쉬운 공격 목표가 됩니다. 인증서들이 제대로 관리되지 않으면, 인증서 만료로 인해 핵심 서비스들이 예상치 못하게 중단되는 사태가 발생할 수 있습니다.

Vormetric Key Management는 키 관리 기능을 확장하여, Vormetric Data Security Platform 솔루션은 물론 타사 제품의 키와 인증서를 보다 효과적으로 관리할 수 있도록 지원합니다. 또한 CipherTrust Cloud Key Manager를 사용하면 클라우드 공급업체들이 제공하는 BYOK를 구현할 수 있을 뿐 아니라 키 수명주기 전반에서 완벽하게 암호키를 통제할 수 있습니다.



강력하고 감사 가능한 통제 구축

Vormetric Key Management는 Vormetric Data Security Manager(DSM)를 활용하여 키를 생성하고 저장합니다. DSM은 FIPS 140-2 레벨 1 인증을 받은 가상 어플라이언스 및 FIPS 140-2 레벨 2 인증을 받은 하드웨어 어플라이언스 V6000, 그리고 HSM 카드가 내장되어 FIPS 140-2 레벨 3 인증을 받은 하드웨어 어플라이언스 V6100 세 가지 형태로 제공됩니다. 또한 클라우드 환경에서의 키 관리를 위해 DSM의 VM 버전이 Amazon Web Service 및 Microsoft Azure 마켓플레이스에서 제공됩니다.

주요 장점

- 인증서 및 암호키의 안전한 저장
- 만기가 다가오는 인증서 및 키에 대한 사전통지
- 상태 및 특징정보를 담은 보고서 제공 및 감사지원

기술 사양

보안 객체 관리

- X.509 인증서
- 대칭 및 비대칭 암호키

관리:

- 보안 웹, CLI, API
- 디지털 인증서 및 벌크 암호키 가져오기
- 가져오기에 대한 검증
- 스크립트

검색, 경고 및 보고서의 키 및 인증서 형식

- 대칭 암호키 알고리즘: 3DES, AES128, AES256, ARIA128, ARIA256
- 비대칭 암호키 알고리즘: RSA1024, RSA2048, RSA4096
- 디지털 인증서(X.509): DER, PEM, PKCS#7, PKCS#8, PKCS#12

타사 암호화

- Microsoft SQL TDE, Oracle TDE, IBM Security Guardium Data Encryption, KMIP 클라이언트
- 파트너 사례: Nutanix, Linoma, NetApp, Cisco, MongoDB, DataStax, Huawei

API 지원

- PKCS#11, Microsoft 확장 가능 키 관리(EKM), OASIS KMIP

키 가용성 및 이중화

- 자동화된 백업을 통해 다수의 어플라이언스에 걸쳐 안전한 키 복제

CipherTrust Cloud Key Manager

많은 클라우드 서비스 업체가 자체적으로 저장 데이터 암호화 기능을 제공하고 있습니다. 하지만 이러한 기능은 암호키가 클라우드 서비스 사업자로부터 분리되어 원격에서 저장되고 관리되어야 한다는 규제 준수 요구사항을 충족시키지 못합니다. BYOK서비스 및 API로 이런 요구사항을 충족시킬 수 있습니다.

고객에 의한 키 운영

고객이 BYOK 기반으로 키를 관리하면 암호키의 생성부터 회수에 이르는 모든 키 관리 과정을 고객이 통제할 수 있습니다. CipherTrust Cloud Key Manager는 BYOK API를 활용하여 암호키의 전체 수명주기를 고객이 중앙 집중적으로 관리할 수 있도록 해주므로 키 관리의 복잡성과 운영비용을 줄일 수 있습니다.

강력한 암호키 보안

고객 키 제어를 위해서는 안전한 키 생성 및 저장이 필요합니다. CipherTrust Cloud Key Manager는 Vormetric Data Security Manager 또는 지원되는 HSM을 활용하여 암호키를 생성하고 저장하므로
보안이 강화됩니다.

IT효율성 향상 및 규제준수 도구

단일 브라우저 창에서 여러 클라우드 공급자를 위한 중앙 집중식 키 관리, 자동화된 키 교체, 연합 로그인 및 기본 클라우드 키 관리 기능을 결합시킬 경우 IT 효율성이 향상됩니다. CipherTrsut Cloud Key Manager의 클라우드 관련 로그 및 사전 패키지화된 보고기능을 통해 규제준수를 위한 보고서를 신속하게 작성할 수 있습니다.

기업 니즈에 맞춘 구현 선택

CipherTrust Cloud Key Manager는 보안 및 구현 요구 사항을 보다 편리하게 충족할 수 있도록 여러 유형의 구현 옵션을 제공합니다.

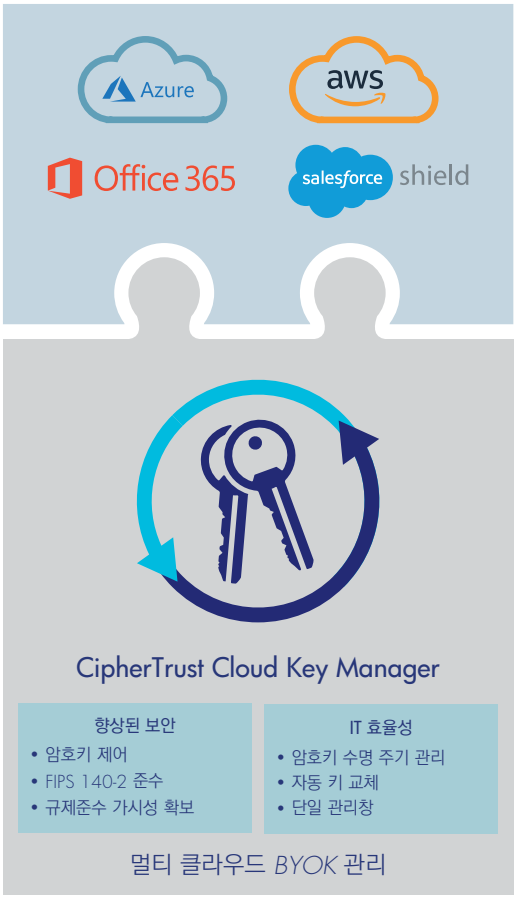
- 모든 소프트웨어는 FIPS 140-2 레벨 1 인증 키 보안과 함께 사용할 수 있습니다. CipherTrust Cloud Key Manager Virtual Appliance와 가상 Data Security Manager 모두 Amazon Web Services 및 Microsoft Azure에서 인스턴스화하거나 VMware를 활용하는 모든 퍼블릭 및 프라이빗 클라우드에 구현할 수 있습니다.
- FIPS 140-2 레벨 3 또는 2가 필요한 고객은 기존의 Vormetric Data Security Manager 어플라이언스나 지원 HSM을 온프레미스 또는 호스팅된 데이터 센터에 배포하거나 활용할 수 있습니다.

주요 장점

- 고객이 직접 키를 관리하는 "Bring Your Own Key" 서비스의 가치를 클라우드 암호키 운영에도 활용하십시오. 수명주기 제어에는 기본 또는 "만료" 일정을 기반으로 하는 자동 키 교체, 지원 클라우드에 대한 클라우드 네이티브 키 관리, 그리고 완전한 동적 키 메타 데이터 관리가 포함됩니다.
- 최대 FIPS 140-2 레벨 3의 검증된 키 생성 및 저장으로 가장 엄격한 데이터 보호 법규 준수
- 여러 클라우드 환경에서 중앙 집중형 키 관리로 IT 효율성 향상

클라우드 환경 지원

- IaaS 및 PaaS: Microsoft Azure, Azure China 및 Germany National Cloud, Microsoft Azure Stack, Amazon Web Services
- SaaS: Microsoft Office365, Salesforce.com, Salesforce Sandbox



Vormetric Protection for Teradata Database

테라데이터 환경에 있는 대용량 데이터를 통합함으로써, 기업은 전례 없는 통찰력과 전략적 가치를 확보할 수 있습니다. 그러나, 이러한 데이터 통합은 또한 전례 없는 위험을 야기할 수 있습니다. 이러한 환경에서 적절한 보호책이 구축되지 않은 상태로 데이터를 처리하면, 민감 정보가 관리자 계정에 의해 의도치 않게 노출이 되거나 악의적인 내부자 또는 외부 공격자에 의해 탈취될 수 있습니다. Vormetric은 기업들이 이러한 위험에 대처할 수 있도록 지원합니다. Vormetric Protection for Teradata Database는 테라데이타 환경에서 강력한 저장 데이터 보안 기능을 빠르고 효율적으로 구현할 수 있도록 지원합니다.

구조 변경과 비용을 최소화하면서 보안강화

Vormetric Protection for Teradata Database는 테라데이타 데이터베이스의 특정 필드와 컬럼에 대한 암호화가 가능하며 민감한 기록의 보안과정을 간소화시킵니다. 이 솔루션은 형식이나 필드 스키마를 변경하지 않고 민감한 기록을 암호화할 수 있도록 NIST 인증된 형태 보존 암호화(FPE) 기능을 제공합니다. 이는 관련된 애플리케이션과 워크플로우에 미치는 영향을 최소화할 뿐만아니라, 기존의 암호화 솔루션과 달리 스토리지를 증설할 필요도 없습니다. 이 솔루션은 또한 동적 데이터 마스킹을 지원하므로 사용자 별로 다른 수준의 복호화 및 데이터 마스킹을 제공할 수 있습니다. Teradata Appliance for Hadoop에 Vormetric Transparent Encryption 에이전트를 설치하면 Teradata 빅데이터까지 보호 영역을 확장할 수도 있습니다.

주요 장점

- 빅데이터 분석 기능에 영향을 주지 않고 보안 강화
- 관리자 오용 및 사이버 공격으로부터 데이터 보호
- 신속한 구현

주요 기능

- 고성능 실현 및 테라데이터 노드 수에 따라 확장 가능한 고성능 암호화
- 형태 보존 암호화를 활용하여 암호화에 따른 스토리지 증설과 업무 중단 최소화
- 암호화, 토큰화, 동적 데이터 마스킹 및 복호화를 위한 사용자 정의 함수(UDF)를 기존 SQL 코드에 손쉽게 통합
- 고객이 컬럼마다 다른 키를 사용할 수 있도록 지원
- ASCII 텍스트, Unicode 등 다국어 지원
- 테라데이터 인증 암호화 솔루션

기술 사양

암호화 알고리즘

- AES, FPE (FF1, FF3)

지원 플랫폼:

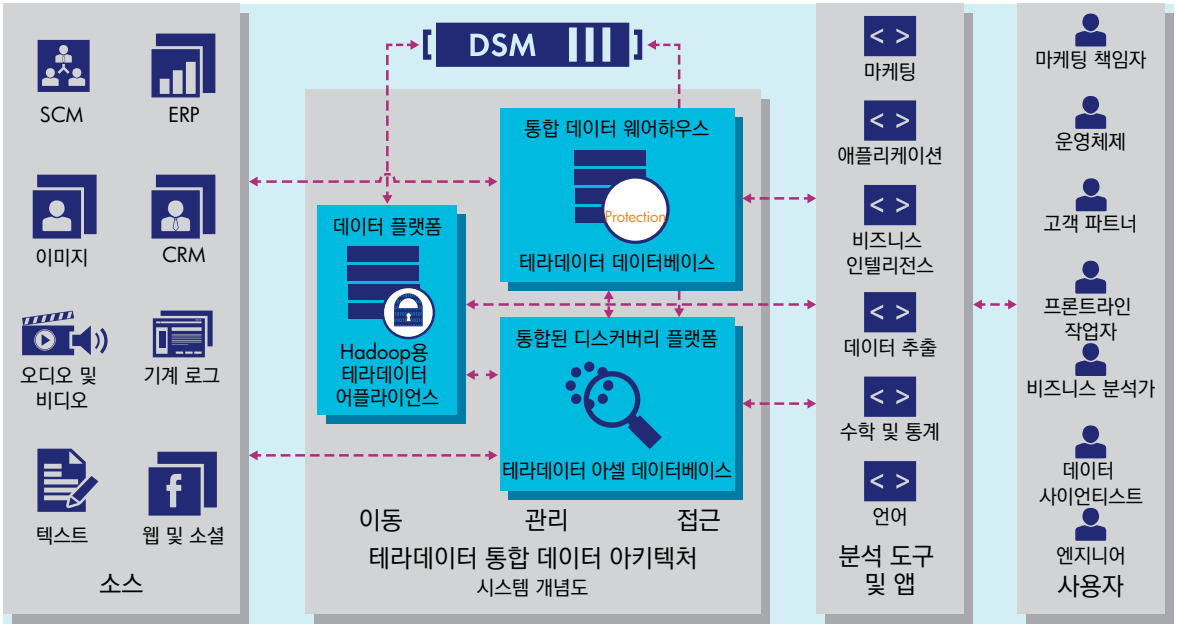
- 테라데이터 데이터베이스, 버전 16.20 및 그 이하(SLES 및 제품 버전에 따라)

운영체제:

- SUSE Linux Enterprise Server(SLES), 버전 10 또는 11

컬럼별 최대 길이:

- ASCII: 16KB
- 유니코드 UDF: 8KB



암호화 구현 및 사용 간소화

이 솔루션은 개발자들이 암호화 및 키 관리 작업 수행 시 구현할 수 있는 문서화된 표준 기반의 애플리케이션 프로그래밍 인터페이스(API)와 사용자 정의 함수(UDF)를 제공하여 복잡성을 감소시킵니다. 이 솔루션은 사용자들이 설정 가능한 프로파일을 간단하게 구성하여 암호화 및 복호화 요청을 제출할 수 있도록 지원하는데, 설정 옵션에서 암호화 알고리즘으로 표준 AES 또는 FPE를 선택할 수 있습니다.

중앙 집중식 키 및 정책 관리 실현

Vormetric Protection for Teradata Database는 FIPS 인증을 받은 암호키 관리 어플라이언스인 Vormetric Data Security Manager(DSM)와 완벽하게 연동됩니다. DSM은 본 솔루션 및 Vormetric Data Security Platform 솔루션, 타사의 암호화 제품의 키와 접근정책을 중앙에서 관리할 수 있도록 지원합니다.

THALES

대한민국

서울특별시 용산구 한남동 독서당로 98 여선교회관 6층

전화: 82.2.3278.8202 | 팩스: +82.2.3278.8290

이메일: krsales.cpl@thalesgroup.com

> cpl.thalesgroup.com <