thalescpl.com

THALES

Vormetric Transparent Encryption

과제: 변화하는 환경과 증가하는 위협 전반에 노출된 민감 데이터의 보호

민감 데이터를 보호하는 데는 데이터센터 내부의 온프레미스 데이터베이스 및 파일을 보호하는 것 이상의 노력이 필요합니다. 오늘날 기업들은 통상 3개 이상의 IaaS 또는 PaaS 제공업체와 협력하여 50개 이상의 SaaS 애플리케이션, 빅데이터 환경, 컨테이너 기술, 그리고 자체 가상 환경 및 프라이빗 클라우드를 사용하고 있습니다.

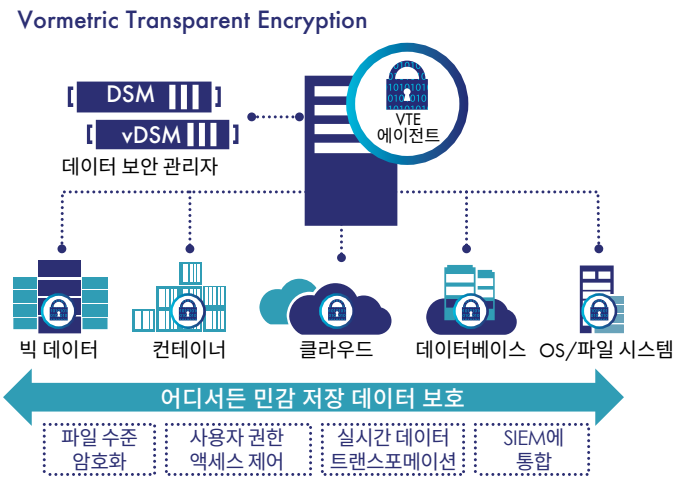
사이버 공격은 더욱 정교하고 강력해져, 문제를 더욱 복잡하게 만듭니다. 민감 정보 보호와 관련된 새로운 규제들이 시행되고 있으며, 기존의 규제는 더욱 엄격해지고 있습니다.

솔루션: Vormetric Transparent Encryption

Vormetric Transparent Encryption (VTE)은 중앙집중식 키 관리를 사용한 저장 데이터 암호화, 관리자 액세스 제어, 상세한 데이터 액세스 감사 기능을 제공함으로써, 데이터가 어디에 존재하든 기업이 데이터 보호를 위한 규제요건을 충족할 수 있도록 지원합니다. FIPS 140-2 레벨 인증을 받은 VTE 에이전트가 운영 파일 시스템이나 장치 계층에 설치되어, 이 계층 위에서 실행되는 모든 애플리케이션에 대해 투명한 암호화 및 복호화기능을 제공합니다. VTE는 데이터에 대한 액세스를 액세스 주체, 액세스 유형, 그리고 시간 등을 기준으로 제어할 수 있도록 지원하는 다양한 액세스 제어 옵션을 제공합니다.

저장되어 있는 모든 민감 데이터 보호

- 물리적 환경, 가상 환경, 클라우드 환경에서, 입증된 하드웨어 가속 암호화 솔루션을 사용하여 파일, 볼륨, 및 클라우드 스토리지를 암호화하고 액세스 제어 및 데이터 감사 기능을 제공함으로써 민감정보 보호를 위한 규제 요건을 충족합니다.
- 중앙집중식 키 관리, 암호화, 및 액세스 정책을 통해 멀티클라우드, 온프레미스는 물론 빅데이터와 컨테이너 환경에도 간단하고 신속하게 배포할 수 있습니다.
- 관리자가 평소처럼 작업할 수 있으면서도 데이터에 잠재적인 위협이 될 수 있는 사용자 및 그룹에 대해서는 따로 보호 조치를 실행하는, 관리자 액세스 제어를 손쉽게 구현할 수 있습니다.



- 위협 요소를 보다 신속하게 식별하고 차단하기 위해, 파일 액세스 활동에 전례 없는 통찰력을 제공하는 상세하고 작동 가능한 보안 이벤트 로그를 사용합니다.
- 업계에서 가장 광범위한 플랫폼 지원. Linux, UNIX 및 Windows 시스템은 물론, Amazon S3 및 Azure Files와 같은 클라우드 스토리지 환경의 정형 및 비정형 데이터를 보호합니다.
- Live Data Transformation 옵션을 추가하면 초기 암호화 및 암호키 교체 작업 시 발생할 수 있는 중단 시간을 없앨 수 있습니다. 이는 타사 데이터 암호화 솔루션에는 없는 탈레스만이 제공하는 기능입니다.

주요 장점

투명한 데이터 보호. 애플리케이션, 인프라스트럭처, 시스템 관리 작업, 업무 절차 등을 변경하지 않고 파일 수준의 암호화를 적용하여 허가받지 않은 사용자 및 프로세스의 무단 액세스로부터 민감정보를 보호하는 한편, 모든 액세스에 대한 상세한 감사 로그를 생성합니다.

쉽고 원활한 배포. Vormetric Transparent Encryption 에이전트는 서버의 파일 시스템 또는 볼륨 수준에 설치되며 로컬 디스크는 물론 Amazon S3 및 Azure Files와 같은 클라우드 스토리지 환경 역시 지원합니다.

세분화된 액세스 제어 정의. 외부 공격 및 관리자의 오용으로부터 데이터를 보호할 수 있도록 세분화된 최소 권한 사용자 액세스 정책을 적용합니다. 시스템, LDAP/Active Directory, Hadoop 및 컨테이너의 사용자/그룹별로 특정 정책을 고유하게 적용할 수 있습니다. 제어기준에는 프로세스, 파일 유형, 날짜/시간 등 이 포함됩니다.

고성능 하드웨어 가속 암호화. Vormetric Transparent Encryption의 데이터 암호화는 AES, 키 교환을 위해서는 ECC와 같은 강력한 표준 기반의 암호화 프로토콜만을 적용합니다. 최신 CPU가 제공하는 AES 하드웨어 암호화 기능을 사용하여 암호화 오버헤드를 최소화합니다.

포괄적인 보안 인텔리전스. 규제준수 요건을 충족시킬 뿐만 아니라, 데이터 보안 분석을 가능하게 하는 상세한 데이터 액세스 감사 로그로 위협을 더 신속하게 식별 및 차단합니다. 메이저급 SIEM 솔루션을 위한 사전 내장된 통합 및 대시보드를 제공하므로 보호 데이터에 대한 거부된 접근 시도를 손쉽게 확인할 수 있습니다.

가장 광범위한 시스템 및 환경 지원. 에이전트는 Windows, Linux, 및 UNIX 기반의 다양한 플랫폼에서 구동 가능하며, 기반 스토리지 기술에 관계없이 물리적, 가상, 클라우드, 컨테이너 빅데이터 등 광범위한 환경에서 사용할 수 있습니다.

고급 보안

무중단 데이터 변환. Live Data Transformation 옵션을 이용하면 초기 암호화 및 암호키 교체 작업 시 요구되는 중단 시간을 제거할 수 있습니다.

이 특허 기술은 애플리케이션을 오프라인으로 전환하지 않고도 데이터를 계속 사용하면서 데이터 베이스 또는 파일을 암호화하거나 새로운 암호키로 교체할 수 있도록 지원합니다.

컨테이너 지원. Vormetric Container Security 에서는 정책 기반 파일 수준 암호화, 액세스 제어, 데이터 액세스 감사 로깅 기능을 확대하여 컨테이너 환경까지 적용할 수 있습니다. 이 솔루션으로 컨테이너 사용자를 기준으로 컨테이너 이미지 내부에 저장되는 데이터에 대한 파일 수준 암호화 및 액세스 제어를 실현할 수 있습니다.

자동 배포 및 유지 보수. Vormetric Orchestrator는 대규모 설치가 필요한 환경에서 간편하게 Vormetric Transparent Encryption을 배포하고 유지보수를 진행할 수 있도록 지원하는 자동화 기능을 제공합니다.

빅데이터를 위한 고급 액세스 제어(Hadoop). 데이터가 Hadoop 환경에서 구현된 경우, Hadoop 사용자 및 그룹에 대한 액세스 제어기능을 제공합니다.

SAP HANA 인증. Vormetric Transparent Encryption은 SAP로부터 데이터 암호화, 키 관리, 관리자 액세스 제어, 세분화된 파일 액세스 감사 로그를 제공할 수 있는 HANA v2.0 인증을 받았습니다.

솔루션 아키텍쳐

Vormetric Transparent Encryption 에이전트 및 Vormetric Data Security Manager (DSM) 어플라이언스로 구성되어 있습니다. DSM을 통해 중앙에서 키 및 정책을 관리합니다. DSM은 FIPS 140-2 레벨 1, 2 또는 3 인증을 받았으며 고객은 이 하드웨어 중에서 자신의 환경에 맞는 어플라이언스를 선택할 수 있습니다. 본 하드웨어는 RESTful, SOAP 및 커맨드라인 API는 물론 웹 기반관리 인터페이스 기능을 제공합니다.

모든 데이터보호 요건 충족

Vormetric Data Security Platform은 포괄적인 데이터 보안 솔루션으로, 저장 데이터를 보다 쉽게 보호할 수 있도록 지원합니다. Vormetric Tokenization with Dynamic Data Masking, Vormetric Application Encryption, CipherTrust Cloud Key Manager 가 포함되어 있습니다.

탈레스에 대하여

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 기술.

> thalescpl.com <

대한민국 - 서울특별시 용산구 독서당로 98 여선교회관 5층 503호 우)04420 • 전화:82.2.2088.4678 • 팩스:82.2.3278.8290 • 이메일: korea.sales@thalesesecurity.com