IBM Security Guardium 데이터 암호화 솔루션

끊임없이 발생하는 보안 침해가 우려를 자아내고 각종 규제가 더욱더 엄격해짐에 따라, 각 조직은 데이터 보호 통제를 하이브리드 멀티클라우드 환경의 전 범위로 확장할 필요가 있습니다. IBM Security Guardium Data Encryption(데이터 암호화 솔루션)은 확장형 공통 인프라를 기반으로 하면서 중앙에서 키와 정책을 관리하는 통합 모듈식 암호화 솔루션입니다. 직관적인 웹 기반 인터페이스를 통해 관리 작업의 부담을 줄이도록 설계되어 있습니다.

IBM Security Guardium Data Encryption은 파일, 데이터베이스, 애플리케이션을 암호화하고 해당 액세스를 제어하면서 클라우드, 가상 환경, 빅데이터 환경, 물리적 환경에 있는 각종 자산을 보호하는 데 유용합니다. 또한 어떤 사용자나 그룹이 어떤 권한을 갖는지에 관한 정책을 정의하고, 암호화 키를 데이터와 별도로 관리할 수 있습니다.

IBM Security Guardium Data Encryption은 기업이 안전하게 클라우드 마이그레이션을 진행하도록 지원합니다. 혁신적인 멀티클라우드 BYOE(Bring Your Own Encryption) 솔루션과 독립된 중앙 집중식 암호화 키 관리 기능을 활용하여 특정 클라우드 벤더의 암호화 기술에 종속되는 문제를 방지합니다. 아울러 데이터 이동성을 보장하여 여러 클라우드 벤더 사이를 오가는 데이터를 효율적으로 보호합니다. 온프레미스에서 클라우드까지 확장된 범위에서 일관성 있게 정책을 적용할 수 있습니다. 그리고 보안을 한층 더 강화하기 위해 GDE를 고객의 기본 보안 인프라와 함께 사용할 수도 있습니다. 즉, 온프레미스 또는 클라우드 HSM(Hardware Security Module)과 연계하여 통합적으로 데이터를 보호합니다.

Guardium Data Encryption 의 포괄적인 기능으로 보안 및 개인정보 보호에 관한 각종 요건을 이행할 수 있습니다. PCI DSS(Payment Card Industry Data Security Standard),

주요 특징

- 세분화된 데이터 보호, 중앙에서 키와 정책 관리
- 하이브리드 멀티클라우드 환경의 전 범위에서 일관성 있게 보안 및 컴플라이언스 지원
- 지원되는 HSM, 타사의 암호화 키 소스 등 기존 보안 툴과의 호환성

GDPR(General Data Protection Regulation), HIPAA(Health Insurance Portability and Accountability Act), FISMA(Federal Information Security Management Act)는 물론 지역별로 제정된 데이터 보호법 및 개인정보 보호법이 모두 해당합니다. 저장된 데이터는 형식을 보존하는 토큰화 기능으로 난독화 (Obfuscation)하고, 사용 중인 데이터는 동적 데이터 마스킹으로 보호해야 합니다. GDE는 고강도 데이터 암호화, 엄격한 사용자 액세스 정책, 데이터 액세스 감사 로깅, 키 관리 기능으로 컴플라이언스 문제를 해결합니다.

기업의 데이터가 클라우드 또는 온프레미스에 저장된 어떤 경우에도, IBM Security Guardium Data Encryption 의 강력한 툴로 사내외로부터의 위협에 맞서고 상시 제어 기능을 구축할 수 있습니다.

Guardium Data Encryption 포트폴리오 구성요소

CipherTrust Manager(이전의 Data Security Manager, DSM)

Guardium Data Encryption은 는 여러 제품이 통합된 솔루션이며, CipherTrust Manager, 즉 CM이라는 이름의 단일 공동 관리 서버에서 모두 관리합니다. 가상 어플라이언스의 형태로 제공되는 이 중앙 관리 지점에서 하이브리드 멀티클라우드 엔터프라이즈 환경 전체의 키 및 데이터 액세스 정책 관리를 수행합니다.

CM은 키 생성, 백업 및 복원, 비활성화, 삭제 등 키 라이프사이클 관리의 제반 활동을 간소화합니다. 이 콘솔에서는 역할에 따라 키와 정책에 액세스하고, 멀티테넌시를 지원하며, 사용 및 운영에 관한 주요 변경사항을 면밀하게 감사하고 보고하는 등의 핵심 기능을 제공합니다.

그 밖에도 다음과 같은 주요 기능이 있습니다.

- 셀프서비스 라이센싱: 효율적으로 커넥터 라이센스를 프로비저닝하고 계속 관리
- 시크릿 관리: 시크릿 및 난독 개체를 생성하고 관리하는 기능 제공
- 멀티테넌시: 여러 도메인을 생성하고 각각의 의무를 구분하는 데 필요한 기능 제공

- REST API: 반복되는 작업 자동화
- 강력한 감사 및 보고: 키 상태 변경, 관리자 액세스 및 정책 변경 추적 기능 포함
- 기존 보안 인증과 손쉽게 통합

Guardium for File and Database Encryption

Guardium for File and Database Encryption에서는 저장된 데이터(data-at-rest)를 암호화합니다. 또한 중앙에서 키를 관리하고, 특별 사용자 액세스 권한을 제어하며, 면밀하게 데이터 액세스를 감사 로깅(audit logging)하면서 컴플라이언스 보고 기능도 수행합니다. 이 솔루션은 정형화되지 않은 데이터베이스와 파일, 그리고 Amazon S3와 같은 클라우드 스토리지 서비스를 보호하도록 지원합니다. 사용자와 그룹이 각종 시스템, LDAP/Active Directory, Hadoop에서 정책에 액세스할 수 있습니다. 프로세스, 파일 형식 등과 같은 매개변수를 기준으로 한 제어도 가능합니다. “신뢰할 수 있는” 애플리케이션으로 허용 목록을 만들어, 신뢰하지 않는 바이너리(예: 랜섬웨어)가 데이터 저장소에 액세스하지 못하도록 액세스 정책을 정의할 수 있습니다.

Guardium for File and Database Encryption은 기본 스토리지 기술과 상관없이 물리적 환경, 가상 환경, 클라우드 환경, 빅데이터 환경 등 어디서나 사용할 수 있습니다. 구축 시 애플리케이션, 사용자 워크플로우, 비즈니스 프랙티스, 운영 절차 등을 변경할 필요가 없습니다. 에이전트는 서버의 파일 시스템 레벨 또는 볼륨 레벨에서 실행할 수 있으며, Microsoft Windows Server, 다양한 Linux 버전, IBM AIX 운영 체제에서 사용 가능합니다. SAP HANA와 Teradata의 파일 시스템도 지원합니다. 관리자는 CipherTrust Manager를 통해 정책 및 키 관리를 모두 해결합니다.

Live Data Transformation: Live Data Transformation은 Guardium for File and Database Encryption의 부가 기능입니다. 암호화 및 키 재입력(rekeying) 기능으로 초기 암호화나 이후의 유지보수 단계에서 전례 없는 수준의 가동 시간 및 관리 효율성을 실현합니다. 관리자는 이 솔루션을 통해 사용자, 애플리케이션, 워크플로우에 미칠 혼란을 줄이면서 데이터를 암호화할 수 있습니다.

암호화가 진행되는 동안, 사용자와 프로세스는 데이터베이스 또는 파일 시스템과의 상호 작용을 평소와 다를 바 없이 이어갑니다. 보안 베스트 프랙티스와 규제 요건에 따르면, 정기적으로 키를 로테이션해야 합니다. 이는 Live Data Transformation의 온라인 키 로테이션 및 데이터 키 재입력 기능으로 해결할 수 있습니다. 더 신속한 백업 및 아카이브 복구도 지원합니다.

Guardium for Container Data Encryption: 이 Guardium for File and Database Encryption의 확장 기능은 컨테이너를 인식하는 데이터 보호 및 암호화 기능을 제공합니다. 따라서 Docker 및 OpenShift 호스트/이미지와 같은 컨테이너 기반 환경에서 더 세부적인 데이터 액세스 제어 및 데이터 액세스 로깅이 가능합니다. 보안 팀은 이 솔루션을 활용하여 컨테이너별로 암호화, 액세스 제어, 데이터 액세스 감사 로깅을 수정할 수 있습니다. 컨테이너 내부의 데이터뿐만 아니라 컨테이너에서 액세스 가능한 외부 스토리지의 데이터도 대상으로 합니다. 컨테이너 볼륨을 보호하고, 컨테이너 내에서 루트 사용자 액세스, 특별 권한 사용자 액세스 또는 허가받지 않은 사용자 액세스를 방지합니다. 다른 컨테이너에서 시도하는 권한 에스컬레이션 공격(privilege escalation attacks)도 차단합니다. 사용자는 컨테이너별로 데이터 액세스를 격리할 수 있습니다. 특정 사용자, 프로세스, 리소스 세트를 기준으로 세분화된 액세스 정책을 마련할 수도 있습니다.

Guardium for Tokenization

Guardium for Tokenization은 애플리케이션 레벨의 토큰화(tokenization) 및 동적 디스플레이 보안 기능을 제공합니다. 중요 자산이 데이터센터, 빅데이터 환경, 클라우드 등 어디에 있더라도 상관없이 보호하고 익명화합니다. 저장된 데이터는 토큰화로 사용 중인 데이터는 정책 기반 동적 데이터 마스킹 기능으로 보호합니다. RESTful API를 중앙 집중식 관리/서비스와 함께 사용하면 필드당 코드 한 줄로 토큰화할 수 있습니다.

토큰화는 전용 분산형 클러스터 지원 토큰화 서버를 통해 제공되며 책임의 완전한 분리를 구현합니다. 운영 대시보드에서 편리한 워크플로우를 사용하여 토큰화를 관리하고 구성할 수 있습니다.

동적 데이터 마스킹 정책에서는 토큰화되는 필드를 완전히 마스킹된 상태로, 아니면 부분적으로 마스킹된 상태로 반환할지 여부를 정의합니다. 이때 AD 서버나 LDAP 서버에서 제어하는 사용자 ID를 기준으로 합니다. 이를테면 고객 서비스 담당자는 신용카드 번호의 마지막 4자리만 볼 수 있고, 매출채권 담당자는 신용카드 번호 전체에 액세스할 수 있도록 정책을 설정합니다.

형식 보존 토큰화로 데이터베이스 스키마 변경 없이 중요 데이터를 보호합니다. Guardium for Tokenization에서는 표준 프로토콜 및 환경 바인딩을 활용하므로, 필요한 소프트웨어 엔지니어링이 최소화됩니다. 고객이 선택한 가상 형태의 어플라이언스로 구축할 수도 있습니다.

Guardium for Application Encryption

Guardium for Application Encryption에서는 중요 데이터를 애플리케이션 레벨에서 암호화하는, DevSecOps 팀에 필요한 소프트웨어 툴을 제공합니다. 이 솔루션은 애플리케이션에서 다루는 어떤 데이터 유형도 암호화할 만큼 뛰어난 유연성을 발휘합니다. 애플리케이션 계층에서 데이터를 보호하면 최고 수준의 보안을 제공할 수 있습니다. 데이터가 생성되거나 처음 처리되는 시점에 즉각적으로 보호 조치를 실행하고, 데이터의 상태에 상관없이, 즉 전송, 사용, 백업, 복사 중일 때도 암호화 상태를 유지할 수 있기 때문입니다.

REST, C, .Net Core, Net, Java 암호화 라이브러리 지원을 통해 개발의 유연성을 보장함으로써 가장 다양한 프로그래밍 기술을 적용하여 암호화 애플리케이션을 개발할 수 있습니다.

아울러, 두 가지 측면에서 운영의 유연성을 누릴 수 있습니다. 첫째, 네이티브 C, PKCS#11, CSP(Cryptographic Service Provider), Windows용 CNG(Crypto Next Generation) 제공자, JCE(Java Crypto Engine)를 비롯한 다양한 암호화 서비스 제공자를 이용할 수 있습니다. 둘째, 코드 변경 없이 로컬 암호화 옵션과 CipherTrust Manager 옵션을 선택할 수 있다는 점도 암호화 운영 유연성과 연결됩니다.

이러한 옵션은 간단하게 구성을 변경하는 방법으로 구현합니다. 지원되는 환경에는 Windows, Linux, AIX, Teradata 등 모든 주요 클라우드 플랫폼이 포함되어 있습니다.

Guardium for Batch Data Transformation

Guardium for Batch Data Transformation은 정적 데이터 마스킹을 수행합니다. 즉, 선택된 데이터를 판독 불가한 형식으로 변환함으로써 데이터 세트 사용 시 중요 데이터 오용을 방지할 수 있습니다. Guardium for Tokenization 및 Guardium for Application Encryption의 부가 기능인 Batch Data Transformation은 방대한 데이터를 신속하게 보호합니다. 타사와의 공유, 개발, QA, R&D를 위해 데이터 준비 단계에서 마스킹하는 경우, 빅데이터 환경에 데이터 세트를 추가하기 전에 안전한 클라우드 마이그레이션을 위해 데이터를 준비하는 경우 등 다양한 활용 사례가 있습니다.

Guardium for Cloud Key Management

클라우드에 중요 데이터를 안전하게 저장하려는 기업이라면, Guardium for Cloud Key Management의 첨단 멀티클라우드 중앙 집중식/독립형 암호화 키 관리 기능을 활용할 수 있습니다. 이 솔루션은 저장된 데이터를 암호화하는 기능을 제공하는 각종 IaaS(Infrastructure-as-a-Service), PaaS(Platform-as-a-Service), SaaS(Software-as-a-Service) 클라우드를 위해 BYOK(Bring Your Own Key) 라이프사이클 관리를 지원합니다. 데이터 보호에 관한 여러 베스트 프랙티스에 따르면, 클라우드 서비스 제공자와 떨어진 원격지에서 암호화 키를 관리하는 것이 좋습니다. BYOK 기반 고객 키 제어 방식에서는 암호화 키 또는 이 키를 생성하는 데 쓰이는 테넌트 시크릿을 분리, 생성, 소유, 제어하고 취소할 수도 있습니다. 키 로테이션 및 만료를 자동으로 관리하면서 IT 효율성을 높입니다. Guardium은 BYOK API를 통해 암호화 키의 라이프사이클 전반을 제어하고 관리 및 모니터링을 중앙화함으로써 키 관리의 복잡성을 줄이고 운영 비용을 절감할 수 있습니다.

중앙에서 단일 브라우저 창을 통해 각 클라우드 제공자에 액세스하고, 네이티브 클라우드 키를 관리하며, 자동 동기화로 클라우드 콘솔 작업을 중앙에서 확실히 모니터링하는 덕분에 IT 효율성이 한층 더 향상됩니다. 키 활동 로그 및 사전 패키지형 보고서로 더욱 신속한 컴플라이언스 보고가 가능합니다. 여러 syslog 서버나 SIEM 시스템에 로그를 보낼 수도 있습니다.

Guardium Cloud Key Management는 독립형 가상 어플라이언스의 형태로 사용합니다. CipherTrust Manager에서 안전하게 키를 생성하는 한편, 추가 보안 계층에서 IBM Cloud Hyper Protect Crypto Services와 같이 지원되는 HSM을 통해 키 생성 보안 및 저장 기능을 제공할 수 있습니다.

Guardium for Data Encryption Key Management

Guardium for Data Encryption Key Management는 Guardium Data Encryption 솔루션은 물론 타사 디바이스, 데이터베이스, 클라우드 서비스, 애플리케이션을 위해 중앙에서 키를 관리합니다. 클라이언트(어플라이언스, 애플리케이션)와 서버(키 저장소) 간 암호화 키 교환에 관한 업계 표준 프로토콜인 KMIP를 지원합니다. 표준화 덕분에 각종 스토리지 솔루션, 즉 SAN 및 NAS 스토리지 어레이, SED(Self-Encrypting Drive), HCI(Hyper-Converged Infrastructure) 솔루션 등을 위해 효과적으로 외부 키를 관리할 수 있습니다. KMIP를 따르면, 키와 암호화 대상 데이터를 분리해야 하는 요구사항을 간단히 해결하고, 더 나아가 하나의 공통 정책 세트로 키를 관리할 수 있습니다. Guardium이 KMIP 서버의 역할을 맡고, Microsoft SQL TDE, Oracle TDE 등을 비롯한 다양한 타사 애플리케이션 및 디바이스가 KMIP 클라이언트의 역할을 합니다.

왜 IBM인가?

IBM Security는 가장 발전되고 통합된 엔터프라이즈 보안 제품 및 서비스 포트폴리오를 제공합니다. 세계적 명성의 IBM X-Force® 연구소가 뒷받침하는 이 포트폴리오는 기업이 비즈니스의 기본 구성요소로 보안을 적용하여 불확실성을 극복하고 성공을 누리는 데 필요한 보안 솔루션을 제공합니다.

IBM은 가장 광범위하면서 수준 높은 보안 연구, 개발, 서비스 조직을 운영하면서 130여 개국에서 월 1조 건 이상의 이벤트를 모니터링하고 있으며, 3,000개 이상의 보안 특허를 보유하고 있습니다. 자세한 내용은 ibm.com/security를 참고하시기 바랍니다.

자세한 정보

IBM Security Guardium Data Encryption에 대한 자세한 정보는 IBM 영업대표 또는 IBM 비즈니스 파트너에게 문의하거나, 다음 웹 사이트에서 확인하세요. https://www.ibm.com/products/guardium-data-encryption

---

IBM이 제시하는 방향 또는 의도에 관한 모든 언급은 특별한 통지 없이 변경될 수 있습니다.