Vault

클라우드 보안 자동화

퍼블릭, 프라이빗 클라우드 전반에서
보안 관리 및 민감한 데이터 보호

인프라의 보안 과제

클라우드 환경의 도입은 기존 정적 인프라에서 탈피해 동적 인프라를 프로비저닝하고 관리하는 방식으로 전환이 필요합니다. 무한한 서비스와 리소스, 스토리지같은 인프라가 불변성(Immutability)과 일시성(Ephemerality)을 수용하고 여러 환경에 걸쳐 배포가 가능해야 한다는 것을 의미 합니다.

STATIC

기본적으로 신뢰도가 높고 경계가 분명한 네트워크를 보유한 데이터센터

DYNAMIC

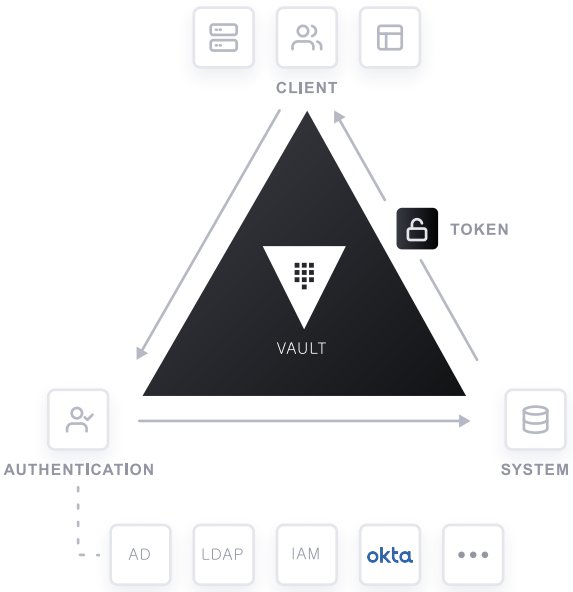
명확한 네트워크 경계가 없는 다수의 클라우드 및 프라이빗 데이터센터

HashiCorp Vault

Vault는 UI, CLI, 또는 HTTP API를 이용해 토큰, 비밀번호, 인증서, 암호 key 및 기타 민감한 데이터에 대한 액세스를 보호 및 저장하고 엄격하게 제어할 수 있도록 합니다.

모든 보안 운영을 중앙에서 관리함으로써 시스템, 라이센스 및 오버헤드를 줄여 생산성을 높이고 비용을 절감할 수 있습니다. 또한, Vault는 보안을 중앙 집중화함으로써 정적이며 하드 코딩된 인증 정보를 제거함으로써 침해 위험을 줄일 수 있도록 지원합니다.

- **ID 브로커링(Identity Brokering)**을 통한 여러 다른 클라우드에 대한 인증 및 액세스, 정책 적용, 용이한 자동화 수행
- **단일 워크플로우**로 기존 인프라 통합, 비용 절감 및 통합 감사 추적 제공
- **개방적이고 확장 가능**한 강력한 오픈소스 커뮤니티, 대규모 파트너 에코시스템 및 완벽한 기능의 멀티 클라우드 보안 엔진



솔루션 및 이점

데이터 유출 위험 감소

민감한 데이터를 단일 워크플로우 및 API를 통해 API의 중앙에서 관리하고, 암호화 키를 이용하여 전송 중 저장된 민감한 데이터를 보호합니다.

침해 위험 감소

Vault로 보안을 중앙 집중화함으로써 하드코딩된 정적 인증 정보를 제거합니다. 또한 신뢰할 수 있는 ID를 기반으로 철저하게 액세스를 제어 합니다.

생산성 증가

개발 팀이 자체 애플리케이션 빌드와 배포 프로세스 상에 자동으로 보안을 적용하고, 단일 API를 통해 프로그래밍 방식으로 민감한 데이터를 보호할 수 있도록 합니다.

통합

- 신뢰할 수 있는 ID를 이용해 여러 다양한 클라우드, 시스템 및 엔드포인트에 대한 인증 및 액세스 실행
- 데이터 암/복호화를 위한 중앙 집중식 key 관리 및 단순한 API로 애플리케이션 데이터의 보안 유지
- 토큰, 비밀번호, 인증서 및 암호화 key 등과 같은 동적 보안 요소를 중앙에서 저장, 액세스 및 배포
- 이기종 환경 전반에 일관된 환경 지원과 이미 사용하고 있는 워크플로우 및 기술 통합

주요 고객

Adobe

BARCLAYS

SAP Ariba

SPACEFLIGHT

cruise

credit karma

주요 기능

	오픈소스 실무자	엔터프라이즈 기업 조직
동적 보안	✓	
보안 요소 저장소	✓	
보안 플러그인	✓	
세부적인 감사 로그	✓	
시크릿의 임대와 해지	✓	
ACL 템플릿	✓	
Vault 에이전트	✓	
Init & Unseal 워크플로우	✓	
키 롤링(Rolling)	✓	
클러스터 관리를 지원하는 UI	✓	
엔티티 및 아이덴티티 그룹	✓	
액세스 제어 정책	✓	
아이덴티티 플러그인	✓	
서비스형 암호화	✓	
Transit Backend	✓	
암호화 키 롤링(Rolling)	✓	
AWS KMS Auto-unseal	✓	
Azure Key Vault Auto-unseal	✓	
GCP Cloud KMS Auto-unseal	✓	
모든 오픈소스 기능		✓
재해 복구(DR)		✓
네임스페이스		✓
복제		✓
복제 필터		✓
Read Replicas		✓
Control Groups		✓
HSM Auto-unseal		✓
다중 요소 인증		✓
Sentinel 통합		✓
FIPS 140-2 & Seal Wrap		✓
KMIP 지원		✓

HashiCorp

www.hashicorp.com