cpl.thalesgroup.com

AKEYLESS | THALES
Building a future we can all trust

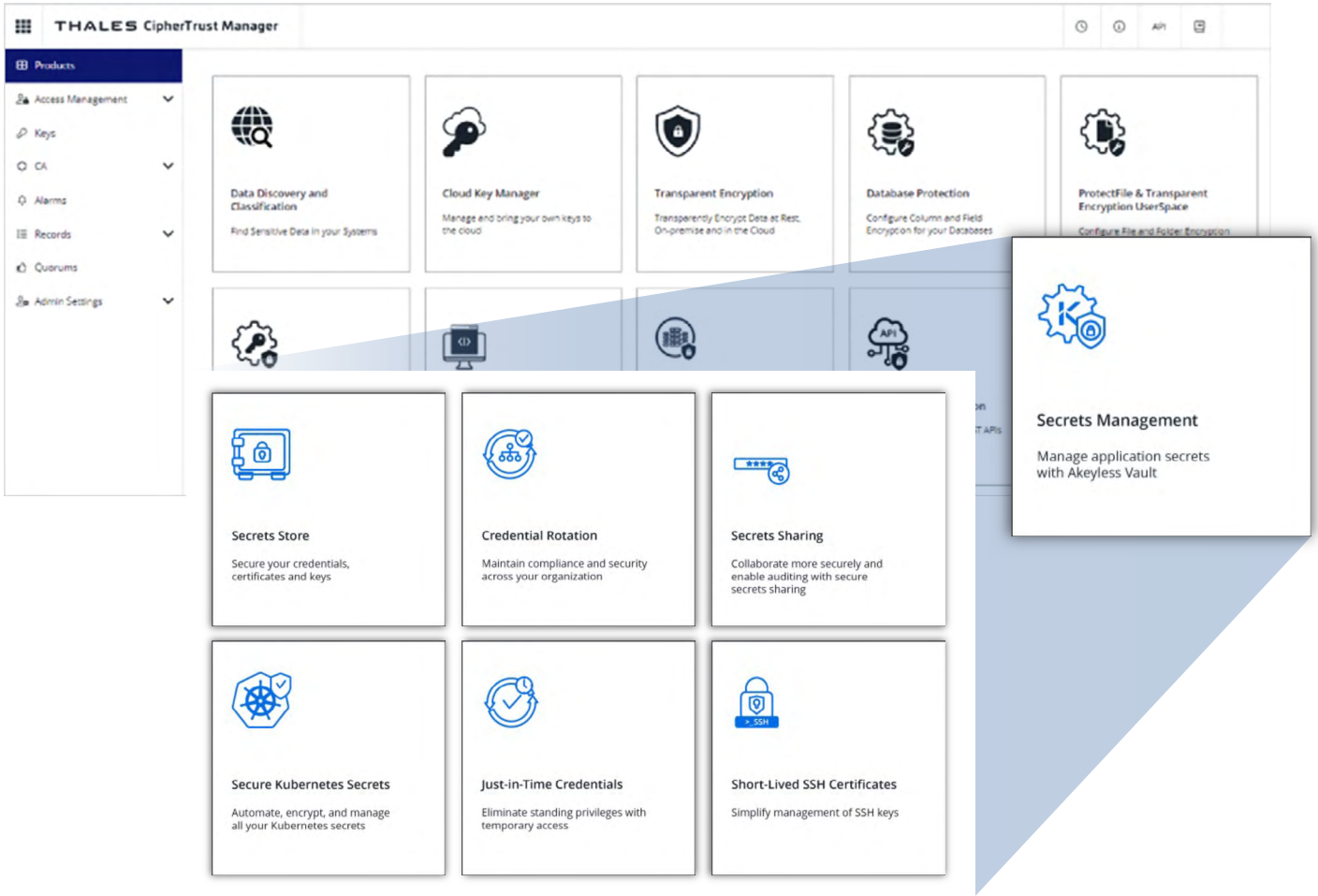
CipherTrust Secrets Management
Securing Secrets at Scale

CSM(CipherTrust Secrets Management)은 Akeyless Vault 플랫폼을 기반으로 하는 최첨단 시크릿 관리 솔루션으로, DevOps 도구와 클라우드 워크로드에서 시크릿, 자격 증명, 인증서, API 키, 토큰 등 업무에 중요한 시크릿에 대한 액세스를 보호하고 자동화합니다. 이러한 새로운 기능은 CipherTrust Data Security 플랫폼의 기능을 향상시켜 보안 및 거버넌스 팀이 운영 전반에 걸쳐 보안 프로세스를 간소화하여 위험을 줄이는데에 도움을 줍니다.

엔터프라이즈급 시크릿 관리 기능은 시크릿의 생성, 저장, 순환 및 제거를 위한 자동 프로세스를 제공합니다. 다음과 같은 이점 덕분에 인적 오류 가능성을 줄이고, 조직 전체에 보안 정책을 일관되게 적용할 수 있습니다.

- 모든 유형의 시크릿을 중앙에서 관리
- DevSecOps에서 자동화된 기능을 손쉽게 사용
- 하이브리드 및 멀티 클라우드 환경에서 SaaS(Software as a Service) 확장성 지원

하나의 툴에서 시크릿 관리를 통해 포괄적인 데이터 보호



모든 유형의 시크릿을 위한 안전한 저장소

Akeyless Vault 기반의 CSM을 사용하면 자격 증명, 인증서, 키 등 시크릿을 포괄적으로 관리할 수 있습니다. 정적 시크릿, 동적 시크릿, SSH 키, API 키 및 토큰이 여기에 해당합니다.

중요 사용 사례는 다음과 같습니다.

- 시크릿 저장소
- 자격 증명 자동 순환
- 시크릿 공유
- 동적 JIT(Just-in-Time) 암호 생성 및 관리
- 감사 및 규정 준수에 사용되는 시크릿의 로그

하나의 툴로 키와 시크릿을 관리

시크릿 관리와 키 관리를 결합하면 모든 귀중한 자산을 한 곳에서 안전하게 보호할 견고한 저장소를 구축할 수 있습니다. 또한, 단일 공급자를 통해 모든 데이터 보호 요구사항을 해결함으로써 효율성을 높일 수 있습니다. CipherTrust Data Protection 플랫폼은 그 어떤 업체도 구현할 수 없는 심층적이고 광범위한 데이터 보호를 제공합니다. 단일 플랫폼에서 별도의 로그인 없이 보안 게이트웨이를 통해 Akeyless Vault 플랫폼으로 손쉽게 마이그레이션할 수 있습니다.

운영상의 복잡성 해소

오늘날 조직의 62%는 자사가 보유하고 있는 키나 인증서의 개수가 몇 개인지 모릅니다.[1] 이렇게 되면 무단 액세스와 데이터 유출에 취약해지게 됩니다. DevSecOps는 솔루션 개발을 위해 더 많은 서비스와 도구를 사용하면서 키와 시크릿을 이용해 상호 간에, 또는 클라우드에 이러한 도구와 서비스를 인증하고 있습니다. 결과적으로 시크릿이 무분별하게 확산되어 위험이 끝없이 증가하게 됩니다. 조직에서 사용되는 서비스 및 도구의 수와 함께 시크릿의 수가 기하급수적으로 증가함에 따라 시크릿이 확산되면서, 악의적인 공격자가 시크릿에 쉽게 액세스해서 이를 손상시켜 심각한 위험에 처하게 될 수 있습니다.

완전한 직무 분리를 통한 DevSecOps 효율성 향상

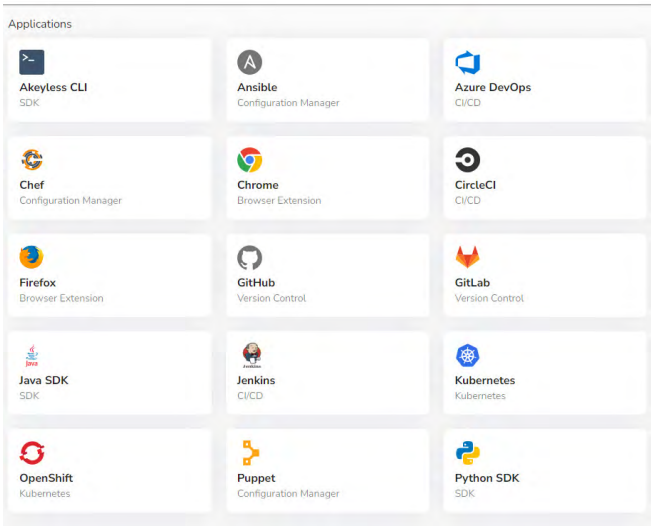
DevSecOps는 멀티 클라우드 애플리케이션에서 키 관리, 암호화 작업 및 시크릿 관리를 신속하게 통합하여 CI(Continuous Integration)/CD(Continuous Delivery) 프로세스를 보호하고 촉진할 수 있습니다. DevSecOps 환경에서 직무를 완전히 분리하기 위해서는 키 관리, 암호화 작업 및 시크릿 관리와 관련된 책임을 다양한 팀이나 개인에게 분배해야 합니다. 이렇듯 직무를 완전히 분리하면 보안 위반을 방지하고, 책임 소재를 명확히 하며, 개발, 보안 및 운영 프로세스의 전반적인 효율성을 높일 수 있습니다.

하이브리드/멀티 클라우드 솔루션

클라우드로의 마이그레이션으로 인해 일부 리소스는 온프레미스 환경에 상주하고 나머지 리소스는 다수의 퍼블릭/프라이빗 클라우드에 분산되는 하이브리드 멀티 클라우드 환경이 형성되는 경우가 많습니다. CSM은 이러한 환경과 구성에서 실행되도록 설계되었습니다.

손쉬운 통합

Akeyless Vault 기반의 CSM은 GitHub, Kubernetes, OpenShift 같은 타사 애플리케이션과 쉽게 통합됩니다.



신속한 배포 및 확장

CSM은 CipherTrust Manager 대시보드에서 손쉽게 액세스할 수 있습니다. CipherTrust Manager에 액세스하는 데 사용되는 자격 증명을 그대로 사용하여 CipherTrust Manager 의 대시보드에서 타일을 통해 액세스할 수 있습니다. 이런 액세스 방식으로 CSM을 쉽고 빠르게 시작할 수 있습니다. Secrets Management 타일을 클릭하고 작업할 구성을 선택하면 시크릿를 제어할 준비가 완료됩니다!

Akeyless 소개

Akeyless에는 혁신적인 기술과 클라우드 네이티브 아키텍처가 고유한 방식으로 결합되어 있기 때문에 DevOps, 클라우드 워크로드 및 레거시 환경을 신속하게 보호하는 동시에, 규정 준수 요건을 충족할 수 있습니다.

탈레스 소개

개인정보를 중요시하는 사람들은 데이터 보안을 위하여 탈레스의 솔루션을 사용합니다. 기업은 데이터 보안과 관련하여 갈수록 결정적인 순간을 맞이하고 있습니다. 탈레스를 사용하면 이러한 순간(암호화 전략 구축, 클라우드 이전, 규정 준수 요건 충족)에도 디지털 트랜스포메이션을 지속할 수 있습니다.

결단이 필요한 순간을 위한 결정적인 솔루션

1 2023 머신 ID 관리 현황 보고서

> cpl.thalesgroup.com <

연락처 – 모든 사무실 위치 및 연락처 정보는 cpl.thalesgroup.com/contact-us를 참조하시기 바랍니다.