백서

시크릿 관리 솔루션을 선택하는 방법

cpl.thalesgroup.com

THALES
Building a future we can all trust

목차

개요

오늘날의 IT 환경은 기하급수적으로 증가하는 시크릿으로 인해 점차 거대해지고 있습니다. 기업들이 클라우드 컴퓨팅, 컨테이너, 마이크로서비스 및 DevOps 실무를 도입함에 따라 인증과 암호화에 필요한 시크릿이 급속도로 증가하고 있습니다.

서비스, 애플리케이션, 시스템 등이 안전하게 통신할 수 있는 이유는 암호, API 키, SSH 키, 암호화 인증서 같은 시크릿이 있기 때문입니다. 하지만 이러한 시크릿이 무분별하게 확산하면서 동시에 보안 위험을 낳고 있는데, 널리 알려진 보안 사고들 대부분이 시크릿 탈취와 관련이 있습니다.

본 백서에서는 효과적인 시크릿 관리 솔루션이 시급히 필요한 이유에 대해 알아보고, 위험부터 요구사항에 이르기까지 시크릿 관리에 따른 문제를 자세히 살펴봅니다. 이와 더불어, 조직의 요건에 부합하는 시크릿 관리 시스템을 계획, 평가 및 선정하는 데 도움이 되는 지침을 제시합니다.

시크릿 관리가 필요한 이유

시크릿이란 시스템 간, 혹은 인간과 시스템의 상호작용 과정에서 인증하는 데 사용되는 자격 증명, 인증서, 키를 말합니다. 자동 프로세스, 가상 머신, 그 밖에 서비스를 실행하는 프로세스는 자격 증명, 인증서, 키 등을 사용해 인증에 필요한 리소스에 액세스해야 합니다.

지난 몇 년간 컨테이너화, 클라우드 트랜스포메이션, DevOps, 자동화 등의 트렌드가 확산하면서 하이브리드 클라우드, 온프레미스, 멀티 클라우드 등 모든 환경에서 사용되는 시크릿의 수가 엄청나게 증가했습니다(그림 1).

이러한 확산으로 인해 보다 확실한 시크릿 관리가 필요해졌습니다. 그렇지 않다면 Uber, Scotiabank, Nvidia 등이 겪은 탈취 사고가 무수히 발생할 것입니다. 지난 몇 년간 일어난 사건에서 볼 수 있듯이 공격자들은 탈취한 시크릿을 이용해 IT 환경에 액세스하고 있습니다. 시크릿이 공격 벡터에 노출되고 액세스 권한이 승격되어 데이터가 유출되면서 네트워크 전체가 공격에 노출될 수 있습니다.

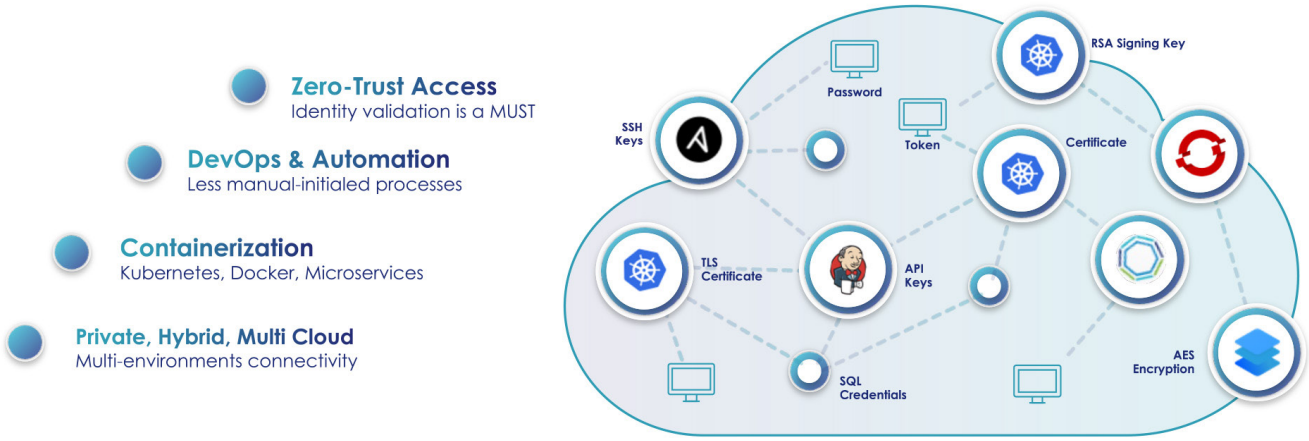

그림 1: 폭발적으로 증가하는 시크릿 수

시크릿 관리에 따른 과제

곳곳에서 확산하는 시크릿

시크릿은 소스 코드는 물론이고 구성 파일, 자동화 스크립트, Ansible/Chef/Puppet 같은 도구 등 IT 환경 곳곳에 흩어져 있습니다. 이렇게 되면 시크릿을 추적하고 보호하기가 어렵습니다.

모든 환경에 필요한 시크릿 관리

시크릿은 개발, 테스트, 스테이징, 프로덕션 등 다양한 환경에 필요합니다. 또한 리전 전역의 온프레미스 및 멀티 클라우드 인프라까지 포괄할 수 있어야 합니다. 하지만 시크릿을 복제하고 관리하는 것은 매우 복잡한 일입니다.

미션 크리티컬

애플리케이션을 실행하고, 다른 애플리케이션과 서로 연결하려면 시크릿이 필요합니다. 또한 다수의 애플리케이션을 동시에 실행하려면 고가용성 시스템도 운영해야 합니다.

컨테이너는 다량의 트래픽을 스핀업할 수 있습니다. 그래서 피크 타임에는 최대 3,000개의 컨테이너를 동시에 실행하는 경우도 있습니다. 하지만 이러한 컨테이너들을 모두 인증하여 실행하려면 시크릿이 필요합니다.

사일로화된 솔루션

많은 부서가 클라우드 공급업체 도구나 오픈 소스 저장소처럼 사일로화된 시크릿 관리 솔루션을 실행하고 있습니다. 이 경우 조직 내 가시성이 미흡하여 파편화와 비일관성을 초래하게 됩니다. 또한 시크릿 관리 솔루션을 마이그레이션하고 통합하기가 어려워집니다. 시크릿 관리는 시크릿을 단순히 저장하는 것에서 끝나지 않기 때문입니다.

시크릿마다, 그리고 각 부서마다 다양한 유형의 솔루션을 사용하여 사일로 문제를 겪는 상황이 자주 발생합니다. 기업 내에서 사용하는 기존 솔루션들은 시크릿 관리 성숙도가 서로 다른 경우가 많습니다. 심지어 시크릿 관리자를 전혀 사용하지 않는 부서도 있고, 클라우드 서비스 공급업체의 시크릿 관리자를 사용하는 부서도 있습니다. 혹은 오픈 소스 프로젝트를 활용하기도 합니다. 이렇게 통일된 표준이 없다 보니 조직적으로 해결해야 할 과제를 피할 수 없습니다.

시크릿 관리의 목적

시크릿 관리의 목적은 비즈니스의 운영을 지속하면서 시크릿의 확산을 통제하고 시크릿의 노출 위험을 줄이기 위한 것입니다. 시크릿 노출 위험을 제어하고, 통제하고, 완화하는 것이 중요합니다. 구성 파일, 소스 코드, 또는 서비스 런타임 시 시크릿을 제공하는 애플리케이션 실행 인프라에 존재하는 시크릿을 제거할 수 있다고 생각해 보세요. 시크릿 관리 서비스를 이용하면 중앙 집중식 거버넌스, JIT(Just-in-Time) 액세스, 역할 기반 액세스 관리 등이 가능해집니다.

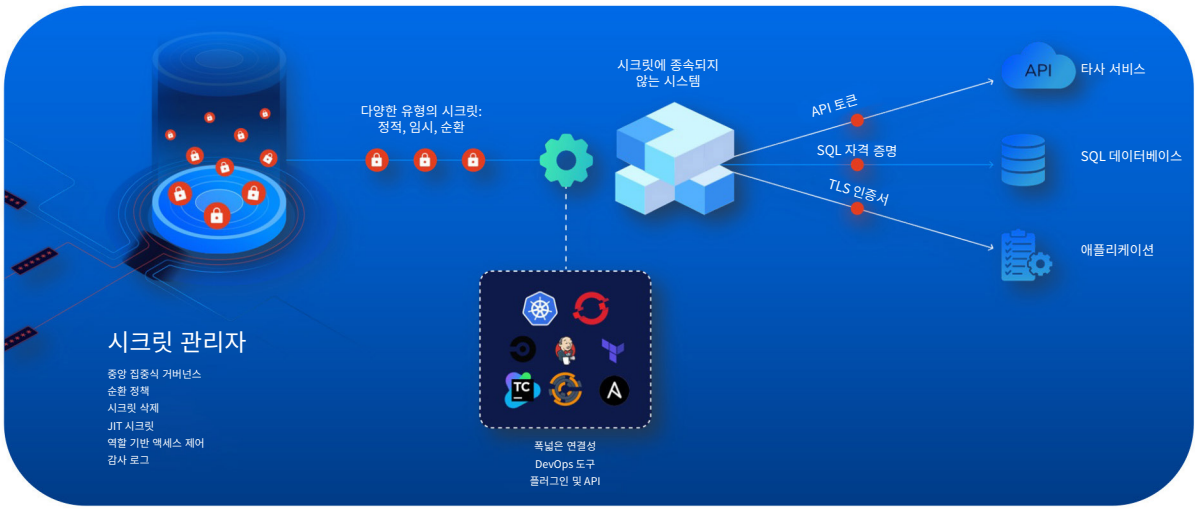

그림 2: 목적에 적합한 시크릿 관리 설계

이를 위해서는 애플리케이션이 연결 계층을 이용해야 합니다. 여기서 연결 계층이란, 애플리케이션을 시크릿 관리 시스템에 연결하는 데 필요한 플러그인, API, 명령줄 인터페이스(CLI), SDK 등을 말합니다. 시크릿 관리 시스템은 애플리케이션에서 인증을 통해 타사 서비스, 데이터베이스 또는 기타 애플리케이션에 액세스해야 할 때마다 해당하는 시크릿을 가져와서 사용합니다. 이후 메모리에 저장되어 있던 시크릿들은 최종적으로 파기되어 제거됩니다. 따라서 시크릿을 사용하지 않을 때는 시크릿이 애플리케이션에 저장되지 않습니다(그림 2).

“ 2021년 기준 10% 미만에 머물던 기업의 데이터 보안 플랫폼 도입률이 2025년에는 30%까지 증가할 것으로 보입니다. 이는 더욱 높은 수준의 데이터 보안을 요구하는 시장 수요와 빠른 제품 기능 향상에 기인합니다.”

– Gartner, 2023년 데이터 보안 플랫폼 도입을 위한 전략적 로드맵, 2022년 9월 22일, Joerg Fritsch, Brian Lowans

시크릿 관리 시스템의 8대 요건

1. 다양한 유형의 시크릿 지원

시크릿 관리 시스템은 다양한 유형의 시크릿을 지원해야 합니다. 예를 들면 다음과 같습니다.

- 데이터베이스에 액세스해야 하는 워크로드의 경우 데이터베이스 자격 증명이 필요합니다.
- 자동 프로세스에서 Linux 서버에 액세스하려면 해당 서버에 대한 인증을 위해 SSH 키가 필요합니다.
- 애플리케이션에서 SaaS 환경 또는 그 밖의 환경에 액세스하려면 API 키가 필요합니다.

그 밖에도 인증서 서명이나 데이터 암호화에 필요한 AES와 RSA를 포함해 SSH 키, API 키, SSH/PKI 암호화 키 인증서 등이 있습니다. 시크릿 관리 시스템은 이러한 온갖 유형의 시크릿을 지원해야 합니다.

2. 다중 플랫폼 순환 기능

순환 기능을 갖추면 누군가가 자격 증명을 유출할 위험이 줄어듭니다. 만약 자격 증명을 입수하더라도 암호가 주기적으로, 또 자동으로 바뀌기 때문에 암호가 유출되더라도 쓸모가 없습니다. 암호는 시크릿 관리 시스템의 자동 프로세스에 따라 순환됩니다. 이것으로 순환 메커니즘에 대해 이해했다면, 무엇보다 시크릿 관리 시스템에서 플랫폼에 따라 다양한 유형의 암호를 순환시킬 수 있다는 점을 알고 있어야 합니다. 현재 사용되고 있는 기술들은 폭넓은 지원이 필요합니다. 예를 들어 다양한 유형의 데이터베이스들이 SSH/API 키 순환을 지원하거나, 그 밖에 사용자 지정 순환 기능을 이용해 환경에 존재하는 키를 순환시킬 수 있는 기능을 지원해야 합니다.

그림 3: 순환 기능을 통한 위험 완화

그 밖에 복잡한 정책 지원도 필요합니다. 예를 들어 오전 2시에, 30일마다 한 번씩, 혹은 1시간마다 순환이 필요한 경우도 있습니다. 이렇게 시크릿 관리 솔루션에서 순환 시간과 주기를 입력하여 설정할 수 있는 정책이 필요합니다.

3. 임시 JIT 시크릿

정적 시크릿을 비롯해 이러한 시크릿의 순환 기능을 지원하는 것도 중요하지만 이러한 유형의 자격 증명은 정적이다 보니 언제든지 유출될 수 있습니다. 아이덴티티는 오래 전부터 이렇게 정적인 방식으로 생성되어 왔습니다. 하지만 시크릿 관리를 도입할 때 보안 실무를 더욱 강화할 수 있는 메커니즘이 있습니다. JIT(Just-in-Time) 액세스라고도 하는 임시 시크릿도 고려 요건 중 하나입니다.

임시 시크릿은 무엇일까요? 말 그대로 아이덴티티를 만들면 반드시 삭제해야 한다는 것을 의미합니다. 한 번 사용된 아이덴티티는 바로 파기되는 것입니다. 데이터베이스에 액세스해야 하는 워크로드의 경우 상시 권한을 부여하지 않고 시크릿 관리 시스템에게 해당 데이터베이스에 한해 이용할 수 있는 임시 아이덴티티를 가져오도록 요청합니다. 그러면 시크릿 관리 시스템이 임시 자격 증명을 생성하여 나중에 사용할 수 있도록 애플리케이션에게 제공합니다. 그런 다음 사용을 마치고 컨테이너가 스핀 오프된 이후, 혹은 애플리케이션에서 필요한 작업을 마친 후에는 자격 증명이 삭제됩니다. 이와 같이 시크릿 관리 시스템에서 임시 시크릿을 관리할 수 있어야 합니다.

그림 4: JIT 액세스

JIT 시크릿에는 제로 트러스트도 포함됩니다. IT 환경에서 규정 준수 및 감사 프로세스를 실행한다고 가정해 봅시다. 이때 임시 시크릿을 이용하면 감사 프로세스를 진행하여 감사관에게 어떠한 권한도 남지 않았음을 데이터베이스를 통해 보여줄 수 있습니다. 실제 사용 목적에 따라 임시로 생성된 아이덴티티가 이용 후 삭제되었기 때문에 기본 아이덴티티 외에는 아이덴티티가 남지 않습니다. IAM(Identity and Access Management) 관점에서는 이를 제로 스탠딩 권한이라고도 합니다.

4. 보안 액세스

시크릿에 액세스할 수 있는 사용자와 시크릿 관리 시스템에 액세스하여 할 수 있는 역할도 또 한 가지 고려해야 할 요건입니다. 여기에는 몇 가지 계층이 존재합니다.

인증

첫 번째 계층은 시크릿 관리 시스템에 인증하여 액세스해야 하는 사용자입니다. 아이덴티티는 소규모 부서부터 팀 구성원, 워크로드에 이르기까지 매우 다양합니다. 하지만 아이덴티티 유형에 상관없이 인증이 가능한 아이덴티티를 설정해야 합니다.

역할 기반 액세스 제어(RBAC)

특정 시크릿을 편집하거나 생성할 수 있는 아이덴티티 권한을 부여하려면 먼저 아이덴티티 권한을 정확하게 설정해야 합니다. 혹은 다른 아이덴티티에게 특정 시크릿을 삭제할 권한을 부여해야 할 수도 있습니다. 이러한 유연성이 필요합니다.

사업 단위 분리

다수의 사업 단위로 구성된 기업에서는 각 사업 단위마다 자체적으로 시크릿을 제어할 수 있는 독립성이 보장되어야 합니다. 이렇게 사업 단위가 분리되어 있으면 특정 시크릿 관리 시스템에 따라 논리적이거나 물리적인 분리도 가능합니다.

영지식(Zero knowledge)

시크릿을 관리할 때는 사용망에서 시크릿이 필요한 엔드포인트 외에는 그 어떤 것도 시크릿에 액세스하지 못하도록 보장해야 합니다. 이를 위해서는 시크릿을 안전하게 저장하고 가져오는 메커니즘이 필요합니다.

정부 액세스

정부 액세스 여부도 고려해야 합니다. 만약 정부에서 액세스하는 경우에는 정부에서 시크릿에 액세스하지 못하도록 차단할 수 있는 시크릿 관리 솔루션을 선택해야 합니다.

5. 연결성

또 한 가지 기본적으로 고려해야 할 요건으로 연결성이 있습니다. 몇 가지 유형의 시크릿으로 보호되는 리포지토리도 있습니다. 그렇다면, 특정 워크로드를 시크릿 관리 시스템과 서로 연결하려면 어떻게 해야 할까요? 여기에는 몇 가지 방법이 있습니다. 예를 들어 특정 시크릿을 요구하는 소스 코드라면 SDK를, 스크립트에 삽입해야 하는 경우라면 명령줄 인터페이스를, 에칭이 필요한 경우에는 API를 사용하면 됩니다.

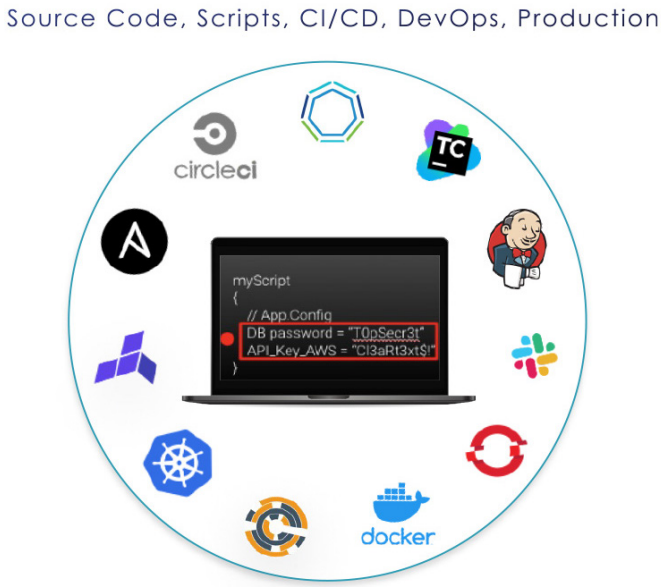

그림 5: 플러그인이 필요한 플랫폼들

무엇보다 중요한 것은 Jenkins, CircleCI, Ansible, Chef, Puppet 같은 자동화 플랫폼을 이용할 경우 플러그인을 통해 연결해야 한다는 점입니다. 이러한 플랫폼들은 모두 플러그인을 통해 시크릿을 가져와야 사용할 수 있기 때문입니다. 따라서 이러한 도구들은 시크릿 관리 시스템에서 시크릿을 요청할 수 있어야 합니다(그림 5).

연결성에서 또 한 가지 고려해야 할 사항은 바로 풍부한 사용자 인터페이스 지원입니다. 이러한 사용자 인터페이스는 상황을 판단하는 데 도움이 될 뿐만 아니라 우수한 사용자 경험까지 제공하기 때문입니다.

6. 다중 환경

시크릿은 어디에서 사용해야 할까요? 보통은 모든 곳에서 사용해야 합니다. 또 한 가지 필요한 시크릿 관리 시스템의 요건은 온프레미스, 하이브리드, 멀티 클라우드 등 다양한 리전과 환경을 지원해야 한다는 점입니다. 시스템이 모든 리전 및 클라우드 환경에서 개발부터 테스트, 스테이징, 프로덕션 단계에 이르기까지 시크릿을 전역적으로 복제하고 동기화해야 합니다. 하지만 여기서 조직의 동적인 특성이 난관으로 작용합니다. 따라서 시크릿 관리 솔루션은 스핀업과 스핀다운을 반복하는 환경의 동적 특성을 원활하게 지원해야 합니다.

그림 6: 온프레미스, 하이브리드 또는 멀티 클라우드 지원

7. 미션 크리티컬 워크로드 지원

시크릿 관리 시스템의 중요 요건은 워크로드에 필요한 시크릿을 필요할 때 모두 제공할 수 있도록 하는 것입니다. 그렇지 않으면 워크로드를 실행하지 못하고, 나아가 프로덕션까지 중단될 수 있습니다. 고가용성, 이중화, 확장성이 필요합니다.

고가용성

시스템은 이러한 트랜잭션은 물론이고 워크로드에서 요청을 가져오는 작업도 지원해야 합니다. 애플리케이션에서 요구할 때마다 24시간 상시 고가용성을 유지해야 합니다.

이중화

두 번째로 고려해야 할 요소는 이중화입니다. 이중화를 지원하지 못하면 어떻게 될까요? 예를 들어 캐싱 메커니즘을 이용할 수 있습니다. 많은 솔루션에서 필요할 때마다 시크릿 관리 솔루션의 완벽한 이중화 지원을 보장하도록 요구하고 있습니다.

확장성

세 번째로 고려해야 할 요소는 확장성입니다. 이러한 워크로드를 모두 동시에 실행할 경우 각 워크로드에서 시크릿까지 함께 요청하게 됩니다. 이때는 시크릿 관리 시스템이 모든 요청을 동시에 처리할 수 있어야 합니다.

8. 거버넌스

마지막 기본 요건은 거버넌스입니다.

추적

워크로드에서 시크릿을 요청하면 시크릿 액세스 및 관리 작업에 대한 감사 추적과 로그를 빠짐없이 수집해야 합니다.

가시성

다음은 가시성입니다. 모든 시크릿 작업에 대한 추적을 마치면, 해당하는 작업들을 유효한 대시보드에 표시하여 어떤 시크릿을 사용해 무엇을 했는지, 그리고 누가 시크릿에 액세스했는지 등에 대한 가시성을 제공하는 동시에 각 시크릿에 영향을 미치는 아이덴티티를 격리해야 합니다.

이벤트 로그 및 전송

기업들은 대부분의 경우 로그를 수집하여 내부 로그 관리 시스템인 SIEM 시스템으로, 혹은 추후 분석을 위해 내부 보안 시스템으로 전송해야 합니다.

사일로화된 저장소에 대한 해결 창구

클라우드 서비스 공급업체든, 오픈 소스 솔루션이든 상관없이 조직에 배포된 시크릿 관리 솔루션이 사일로 문제를 겪고 있다면 시크릿 관리 시스템을 기존 솔루션과 함께 사용하여 완전한 거버넌스를 구현하는 동시에 조직 내 시크릿의 위치를 정확하게 파악해야 합니다.

> 실제로 강력한 시크릿 관리 솔루션을 구현한다면 사일로화된 프로세스를 손쉽게 마이그레이션할 수 있는 해결책을 얻는 셈입니다.

새로운 엔터프라이즈급 시크릿 관리 솔루션으로 손쉽게 마이그레이션할 수 있는 프로세스가 필요합니다. 사일로화되어 솔루션을 마이그레이션하지 못하는 경우에는 가시성을 확보하고 시크릿이 저장된 위치를 파악하는 것이 매우 중요합니다.

솔루션 계획 시 필수 고려 사항

기업은 빈틈없는 계획을 통해 최신 시크릿 관리 솔루션을 구현하여 위험을 완화하고, 운영을 개선하고, 관리를 간소화하고, 혁신을 앞당길 수 있습니다. 솔루션 계획 시 반드시 고려해야 할 사항은 다음과 같습니다.

- 기존 인프라 및 애플리케이션에 필요한 시크릿 요건을 빠짐없이 확인
- 현재 시크릿 관리와 위험 간 격차 평가
- 가용성 및 확장성 요건 확인
- 사일로화된 관리 솔루션의 통합 옵션 평가
- 액세스 제어 정책 및 RBAC 아키텍처 개발
- 시크릿 관리를 점진적으로 전환할 수 있는 마이그레이션 계획 수립
- 기존 아이덴티티 관리 시스템과 통합
- 규정 준수에서 요구하는 제어 정책 적용

요약

오늘날 클라우드 네이티브 DevOps 환경은 무분별하게 확산하는 시크릿을 제어하고, 최소 권한 액세스 정책을 적용하고, 가용성을 유지하고, 공격 대상을 줄일 수 있는 솔루션이 필요합니다. 시크릿을 관리하지 못하면 치명적인 사이버 위험에 노출되어 비즈니스 운영이 중단될 수 있습니다.

본 백서에서는 위험부터 요건에 이르기까지 시크릿 관리에 따른 과제를 총체적으로 살펴보았습니다. 기업들이 시크릿 관리 플랫폼을 선택할 때는 당면한 현실에 맞춰 전략을 조정하고 이러한 기준에 따라 요건을 평가해야 합니다.

강력하고 선제적인 시크릿 관리 솔루션을 갖춘 기업은 중앙 집중식 시크릿 오케스트레이션을 통해 클라우드 트랜스포메이션, 자동화, 혁신을 안전하게 구현할 수 있습니다. 또한 시크릿의 확산을 제어하면 침해 위험을 줄이고 IT 아키텍처를 간소화하는 등 다양한 측면에서 이점을 얻을 수 있습니다.

리소스

탈레스는 액세스 관리, 데이터 탐색, 데이터 보호, 중요한 데이터 및 정보 제어 등을 모두 간소화할 수 있는 통합 데이터 보안 플랫폼을 제공합니다. Thales CipherTrust Secrets Management가 Akeyless 기반의 최신 시크릿 관리 솔루션인 이유를 알아보십시오. Thales CipherTrust Secrets Management는 시크릿, 자격 증명, 인증서, API 키, 토큰 등 DevOps 도구와 클라우드 워크로드에 걸쳐 시크릿에 대한 액세스를 보호하고 자동화함으로써 이러한 요건을 충족하고 과제를 해결합니다.

자세한 정보:

- **CEO이자 공동 설립자인 Oded Hareven(Akeyless)과 비즈니스 개발 사업부 이사인 John Wohlfarth(Thales)가 진행하는 탈레스 파트너 솔루션 시리즈: CipherTrust Secrets Management for DevSecOps 웨비나로 이동하기**
- **데모 보기**
- **무료 데모/POC 예약하기**
- **90일 무료 평가판 시작하기**
- **Thales CipherTrust Secrets Management 웹페이지로 이동하기**

- **단일 플랫폼을 통한 시크릿 및 데이터 관리**
- **빠른 배포와 엔터프라이즈급 성능**
- **총소유비용**

Akeyless 소개

Akeyless는 독자적인 방식으로 혁신 기술과 클라우드 네이티브 아키텍처를 결합하여 기업이 DevOps, 클라우드 워크로드, 레거시 환경을 신속하게 보호하는 동시에 규정을 준수할 수 있도록 지원합니다.

탈레스 소개

오늘날 기업과 정부는 신뢰할 수 있는 디지털 서비스를 제공하기 위해 클라우드와 데이터 및 소프트웨어를 사용하고 있습니다. 이에 전 세계 유명 브랜드와 기업들이 클라우드와 데이터 센터에서부터 개별 장치와 네트워크에 이르기까지 전역에 걸쳐 데이터를 생성, 저장, 액세스하는 곳이라면 어디에서나 탈레스 솔루션을 이용해 중요한 정보와 소프트웨어를 보호하고 있습니다. 데이터 보안, IAM 및 소프트웨어 라이선싱에서 글로벌 리더로 자리잡은 탈레스 솔루션은 기업이 안전하게 클라우드로 전환하고, 자신있게 규정 준수를 실현하고, 소프트웨어에서 더 높은 가치를 창출하고, 수백만 명에 이르는 고객에게 하루도 빠짐없이 원활한 디지털 경험을 제공할 수 있도록 지원하고 있습니다.

THALES

Building a future we can all trust

문의

지사 위치와 연락처 정보는
cpl.thalesgroup.com/contact-us에서 확인할 수 있습니다.

cpl.thalesgroup.com