KEY®KE
Automate security, secrets and vault

Zero Trust 와 Cloud

Cloud Secret Asset Management Platform

동훈아이텍 신승목 상무

DONGHOON 동훈아이텍

‘BMW 너 마저’ – 내부 민감 정보 고스란히 노출…

BMW 클라우드 스토리지 서버, 인터넷 노출 "얼마나 많은 데이터가 어느 정도 노출됐는지 정확히 알 수 없어”

[더구루=홍성일 기자] 독일의 완성차 업체 BMW의 민감한 내부 정보를 보관하는 클라우드 스토리지 서버가 인터넷에 그대로 노출된 것으로 확인됐다. BMW는 개인 정보가 유출되지는 않았다며 대응에 나섰다.

미국 IT전문매체 테크크런치는 2024년 02월 15일(현지시간) 마이크로소프트(MS) 애저에 구축된 BMW의 클라우드 스토리지 서버가 비공개가 아닌 공개상태로 인터넷에 노출됐다고 보도했다. 이는 사이버 보안기업 SOC레이더(SOCRadar)의 연구원 캔 욜레리(Can Yoleri)에 의해 확인됐다.

이번에 문제가된 스토리지 서버는 BMW 내부에서는 '버킷(bucket)'으로 불리는 것으로, 노출된 버킷 안에는 비공개 버킷에 접속하기 위한 비밀키, 기타 클라우드 서비스에 대한 세부 정보가 포함된 스크립트 파일 등이 보관돼 있었다. 구체적으로는 미국, 중국, 유럽에 있는 BMW 클라우드 서버에 접속할 수 있는 개인 키와 BMW 생산 및 개발 데이터베이스에 대한 로그인 자격 증명이 포함됐다.

캔 욜레리는 이번 문제에 대해서 "안타깝게도 얼마나 많은 데이터가 얼마나 오래 노출됐는지 정확히 알 수 없다"고 설명했다.

BMW도 사태를 파악하고 대응에 나섰다. BMW 측은 "고객이나 회사 직원 개인의 정보는 영향을 받지 않았다"고 설명하며 노출된 버킷을 비공개 처리했다.

캔 욜레리 연구원은 BMW 대응이 불충분하다고 경고했다. 그러면서 "버킷을 비공개로 설정했더라도 액세스 키를 변경해야 했다"며 "더 이상 버킷이 비공개로 설정돼 있는지는 중요하지 않다"고 말했다.

메르세데스-벤츠에 이어 BMW도 내부정보가 담긴 클라우드가 노출되는 사태가 벌어지면서 독일 완성차 업체들의 보안에 물음표가 생길 것으로 보인다.

지난달 사이버 보안 연구소 레드헌트 랩(redhunt labs)은 메르세데스-벤츠 직원의 개인키가 액세스가 가능한 상태로 깃허브에 공개됐다고 보고했다. 해당 개인 키를 사용하면 메르세데스-벤츠의 깃허브 엔터프라이즈 서버에 무제한 접속할 수 있는 권한이 부여, 회사 내부 정보가 무차별적으로 노출될 수 있는 상황이었다.

원문보기: https://www.theguru.co.kr/news/article.html?no=66624

암호키 유출 사례

- **핀테크 서비스 페이코 "서명키 유출사건(비대칭키)"**

  2022년 12월 5일 에버스핀은 페이코의 서명키가 유출됐고 이를 악용해 앱이 제작·유포됐다는 내용의 '긴급 공문'을 자사 금융 고객사들에게 발송한 것이 기점

  페이코의 서명키가 유출된 8월 부터 약 4개월 동안 인지 할 수 없었음

  서명키를 이용한 위변조된 앱이 배포되어 5000여건 이상의 탐지 발생

  - 원문 보기 : https://www.boannews.com/media/view.asp?idx=112602

- **매리어트 그룹 지불결제 " 암호키 유출사건(대칭키 유출)"**

  2018년 11월 5억명의 개인정보 유출 사건 발생

  2018년 9월 8일 웨스틴(Westin), 쉐라톤(Sheraton), 세인트 레지스(St. Regis) 및 W 호텔을 포함한 메리어트 스타우드(Marriott's Starwood)의 내부 손님 예약 데이터베이스에 액세스하려고 시도하는 수상한 내부 보안 도구를 포착했다. 신용카드 번호는 암호화된 형태로 저장됐지만, 암호화 키가 동일한 서버에 저장되어 있었다. 여권번호에 대해서는 일부는 암호화되어 있었던 반면, 대다수는 단순히 저장되어 있었다

  2014년 부터 지속되었고 개인정보를 AES 128로 암호화 하고 있었으나 암호키가 유출된 것으로 추축하고 있음

  - 원문 보기 : https://www.itworld.co.kr/news/144342#csidx3527bfd0f4e6c2995b0742dfbc0e464

인증서 악용 사례

- **인증서의 관리 소홀로 인한 악성코드 배포**

2019년 '광주버스'라는 앱이 플레이스토어에 업데이트됐는데, 해당 앱에 악성 기능이 포함돼 있어 문제가 발생

해당 앱은 2012년에 서비스를 시작했으며, 2018년 개발자가 개발 및 업데이트를 중단했지만, 인증서 정보는 폐기하지 않았다.

그 이후 공격자는 인증서와 코드, 그리고 플레이스토어에 업로드한 개발자의 아이디 및 패스워드를 취득했고, 이를 활용해 해당 앱에 악성코드를 추가해 플레이스토어에 재업로드했다. 또한, 해당 악성코드가 포함된 앱이 정상적으로 업데이트돼 개인 사용자의 구글 아이디와 비밀번호를 탈취했다.

원문 보기 : https://www.boannews.com/media/view.asp?idx=114833

파일 관리 (SBOM)

- **SBOM을 이용한 애플리케이션 관리 필요성**

솔라윈즈 플랫폼과 **Log4j의 취약점을 이용한 공격**으로 인해 이를 사용하는 수많은 애플리케이션이 영향을 받았다

아파치 소프트웨어 재단에서 오픈소스로 제공하는 Log4j는 수백만 자바 애플리케이션에 영향을 주기도 했다.

특히 자바로 개발된 금융권 등 기업의 주요 애플리케이션이 영향을 받아 그 파급효과가 더욱 컸었다.

종속성 트리에 있는 모든 모듈이 어떤 것인지 정확하게 파악하고 있고, 또 이들 상태를 실시간으로 모니터할 수 있다면
이 중 하나만 문제가 생겨도일단 애플리케이션 사용을 중단함으로써 **문제 확산을 최소화할 수** 있을 것이다.

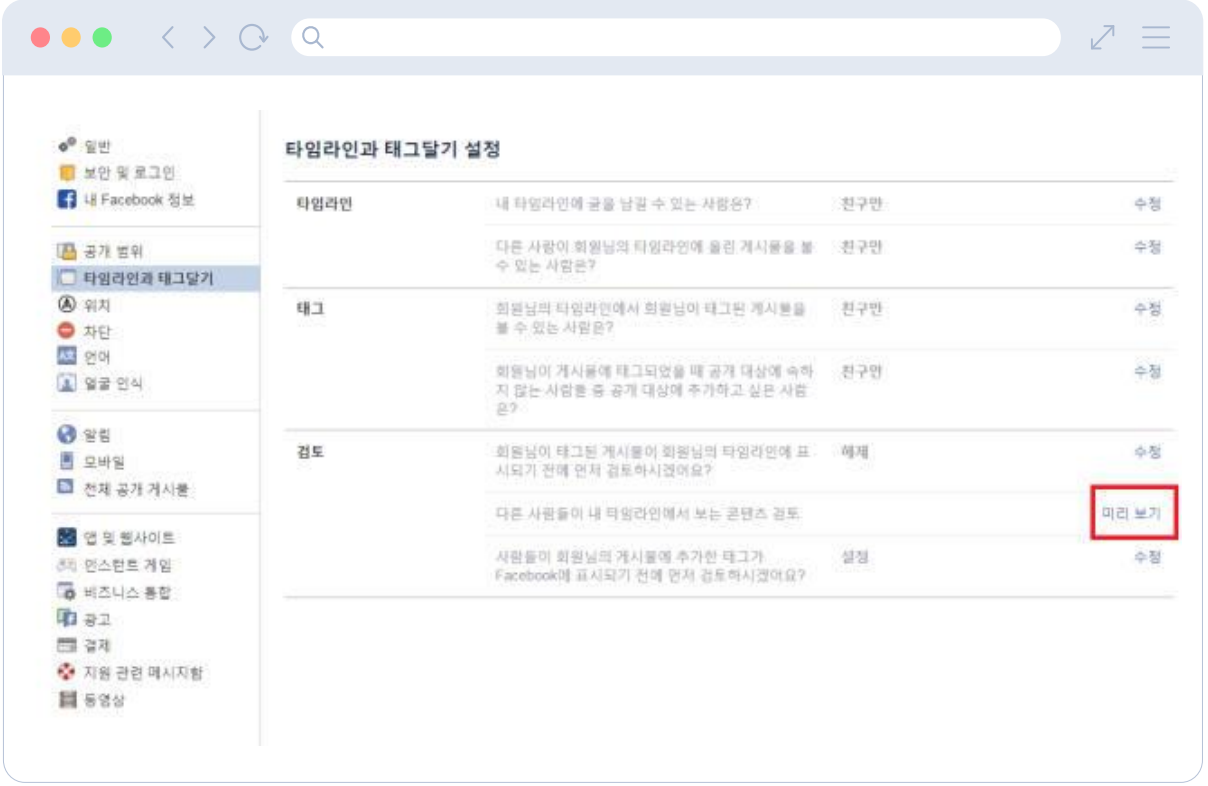
SBOM이 사이버 보안에 매우 중요한 요소인 이유다. SBOM은 소프트웨어 버전, 첵썸 정보, 그리고 종속성 트리 및 호환성 정보 등을 모두 갖추고 있어야 하며, 이 모든 정보는 기계가 판독할 수 있어야 한다. 따라서, SBOM을 구성하는 정보를 정형화해서 가능한 표준화하는 것이 필요하다.

SBOM 포맷 SPDX, CycloneDX, SWID와 같은 주요 포맷들이 정의되어 있다. (SPDX 지원/ RDFa, .xlsx, .spdx, .xml, .json, .yaml.)

원문 보기 : https://www.itworld.co.kr/tags/154167/SBOM/250420#csidx945673cae841b7d8a1b0178f9bcb052

토큰 탈취

- **페이스북 해킹 사례**



원문보기: https://www.etnews.com/20180930000032

외부 공격자는 특정 방법을 이용해 동영상 업로더에 접근했고,

페이스북 모바일 애플리케이션(앱) 로그인 가능한 '**액세스 토큰**'을 탈취했다.

여기서 생성된 **액세스 토큰을 공격자가 확인 후 계정에 접근 가능한 '키'를 가져갔다.**

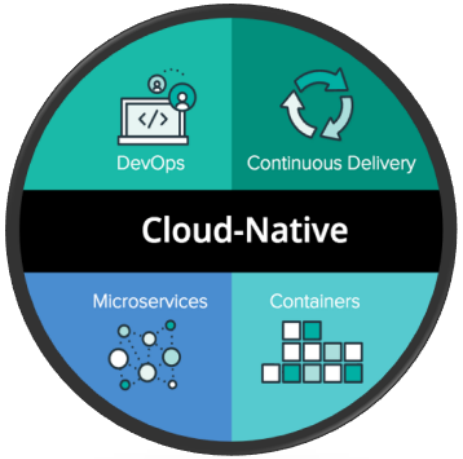
이번 해킹으로 페이스북 비밀번호가 노출된 것은 아니지만,

탈취한 액세스 토큰을 이용해 비밀번호나 2단계 인증을 사용하지 않고도

API를 이용해 계정 정보 탈취 가능하다.

Zero Trust Security 배경

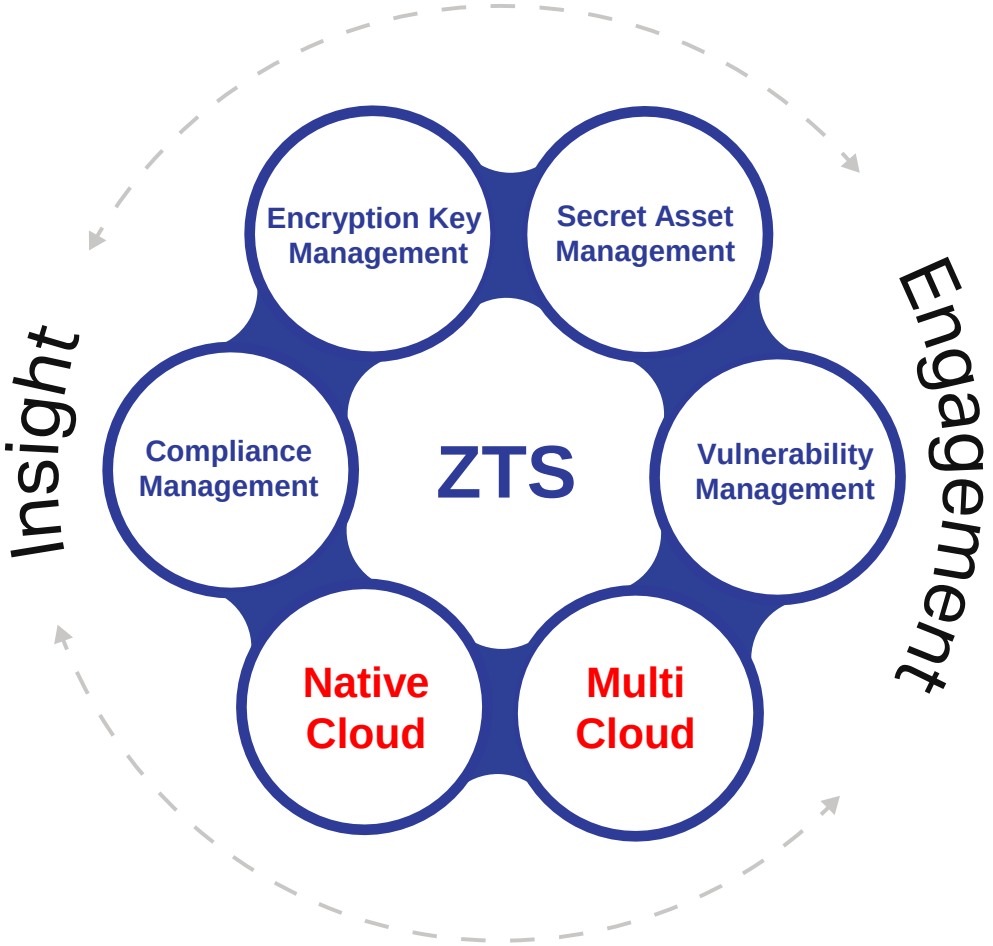
클라우드의 확산

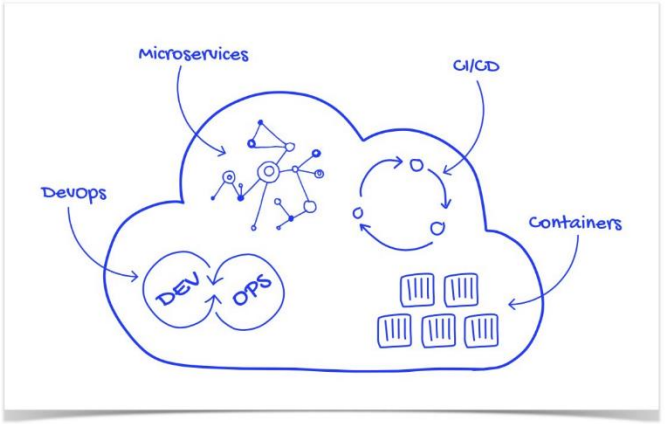


클라우드-네이티브
애플리케이션

랜섬웨어의 위협

Cloud Native에서의 보안이란?





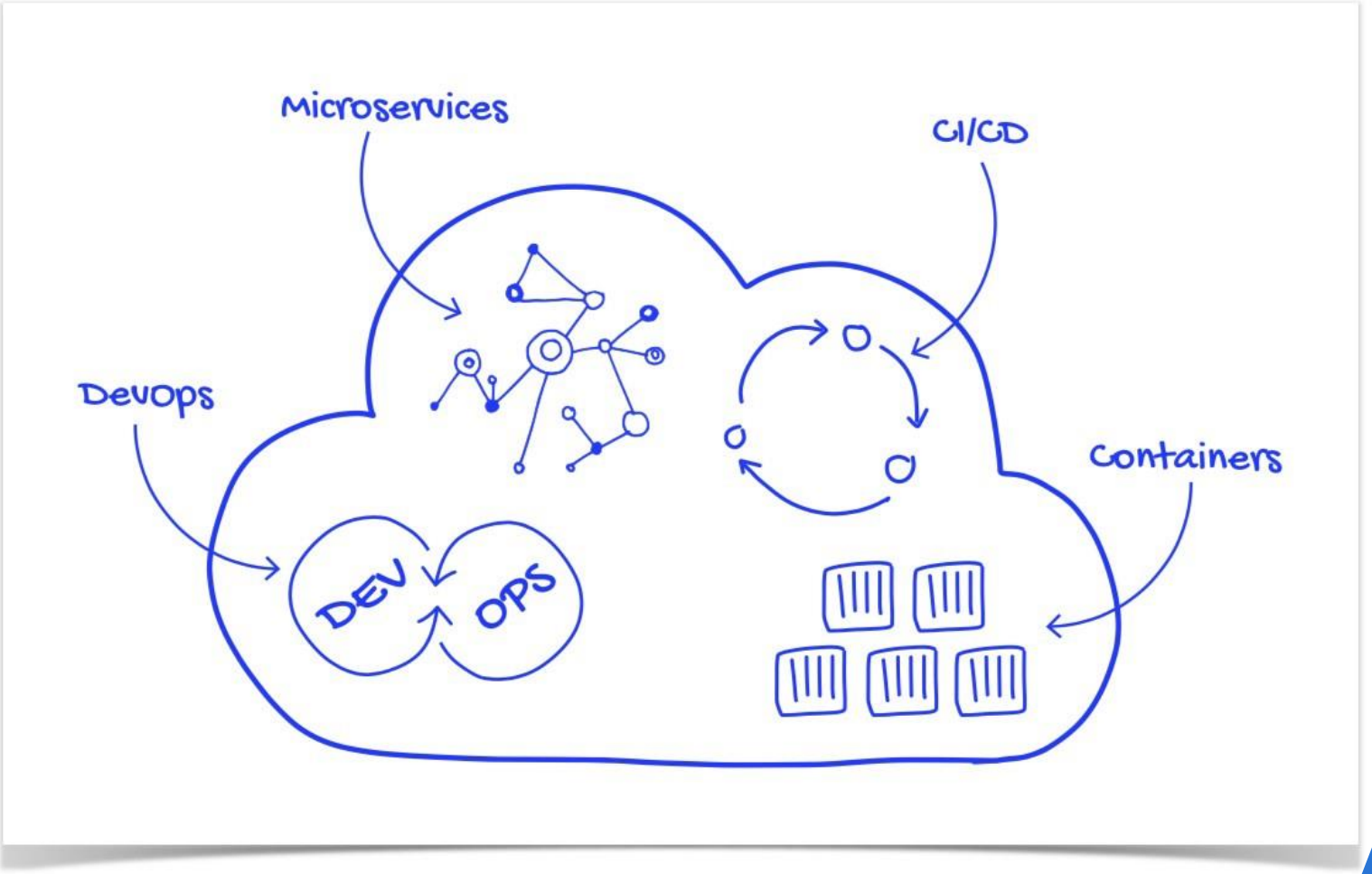
LIFT & SHIFT — REFACTORING — CLOUD NATIVE

Native Cloud 환경에서의 보호 대상

'Native Cloud' 환경으로의 전환은 기존의 전통적인 'Cloud'의 방식이 아닌 'Cloud'의 이점을 최대한 활용하여 비용 절감, 운영 효과성 증대 등의 목적을 위해 전통적인 'Cloud' 환경을 'Refactoring' 하는 것입니다.

Native Cloud의 특징

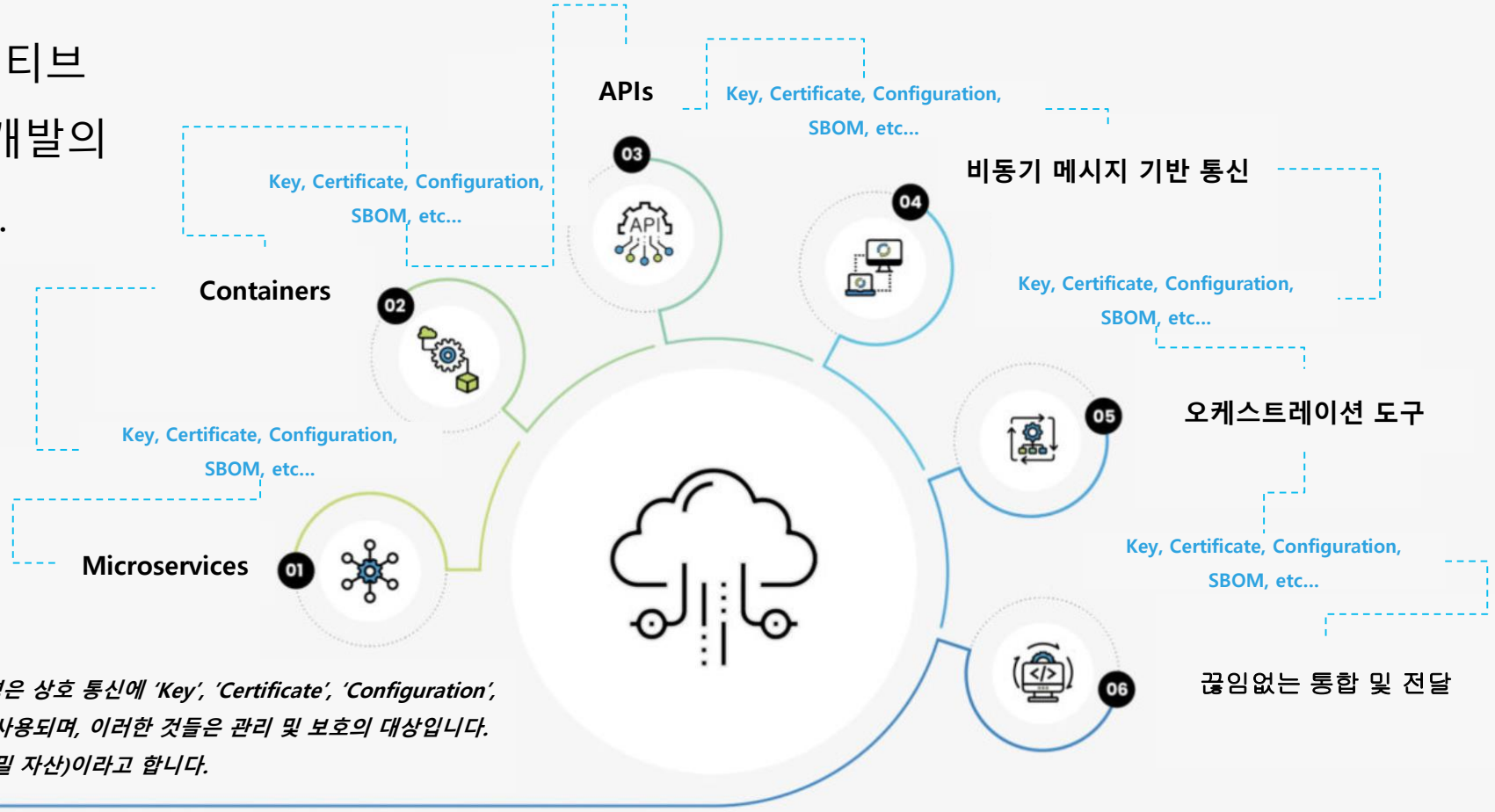
- **Serverless 환경** : 클라우드 제공업체가 기반 서버 인프라를 전적으로 관리하는 클라우드 네이티브 모델입니다. 개발자는 응용프로그램에 사용되는 리소스에 대해서만 비용을 지불합니다.
- **CI/CD 환경** : 지속적 통합 (CI)은 개발자가 오류 없이 자주 변경 사항을 공유 코드 베이스에 통합하는 소프트웨어 개발 방식. 지속적 전달 (CD)은 클라우드 네이티브 개발을 지원하는 소프트웨어 개발 방식.
- **DevOps 환경** : 개발 및 운영 팀의 협업을 개선하는 소프트웨어 문화입니다. 이는 클라우드 네이티브 모델에 부합하는 설계 철학입니다.
- **Micro Service 환경** : 전체적으로 하나의 완전한 클라우드 네이티브 소프트웨어로 작동하는 소규모의 독립적인 소프트웨어 요소입니다. 서로 통신하는 독립적인 소프트웨어 구성 요소입니다.
- **Container 환경** : 컨테이너는 클라우드 네이티브 응용프로그램에서 가장 작은 컴퓨팅 유닛입니다. 또한 클라우드 네이티브 시스템에서 마이크로 서비스 코드 및 기타 필수 파일을 패키징 하는 소프트웨어 구성 요소입니다.
- **API 환경** : 둘 이상의 소프트웨어 프로그램이 서로 정보를 교환하는 데 사용하는 방식입니다. 클라우드 네이티브 시스템은 느슨하게 결합된 여러 마이크로 서비스를 API를 사용하여 통합합니다. API는 결과를 달성하기 위한 단계를 지정하는 것이 아니라, 마이크로 서비스에 필요한 데이터와 마이크로 서비스가 제공하는 결과를 알려줍니다.



'Native Cloud' 환경에서는 'Secret Asset(비밀 자산)'이 가장 중요합니다.

Native Cloud 환경에서의 보호 대상

클라우드 네이티브
응용프로그램 개발의
필수 요소.



느슨한 구조의 'Cloud Native' 환경은 상호 통신에 'Key', 'Certificate', 'Configuration', 'SBOM' 등 다양한 중요 파일들이 사용되며, 이러한 것들은 관리 및 보호의 대상입니다. 이러한 파일들을 Secret Asset (비밀 자산)이라고 합니다.

Native Cloud, Multi Cloud 환경에서 필요한 보안 요소

보안 대상 자동화 관리
- Life Cycle Management, Visibility

보안 대상의 격리 및 보호
- 높은 보안과 활용성을 고려한 보관

장애 / 재해 안정성
- 복구 또는 복원 시, 빠르고 안전성 확보

클라우드 취약점 관리
- CVE, CCE, CWE

컴플라이언스 준수
- ISMS-P, IOS27001, etc…

DevSecOps
- 안전한 개발 및 운영 환경 제공

On-Premises

Hybrid

Cloud

클라우드 네이티브 환경에서의 비밀자산 관리
보호해야 할 **비밀자산(Secret Asset)**에 대한 식별을 통해 비밀 자산들에 대한 체계적인 라이프 사이클 관리를 제공합니다.

암호화 및 접근 제어
Secure Zone 저장 방식의 안전한 키 보관 및 최소 권한 부여를 통한 접근 제어 기능을 제공합니다.

시스템 분리 및 보관
비밀 자산을 기존 시스템에서 분리하여 보관함으로써 장애 또는 재해 발생 시 **주기적 백업**을 통한 복구 및 정상화 기능을 제공합니다.

CVE / CCE / CWE
클라우드 시스템 환경 및 소프트웨어 취약점 점검 및 관리 기능을 제공합니다.

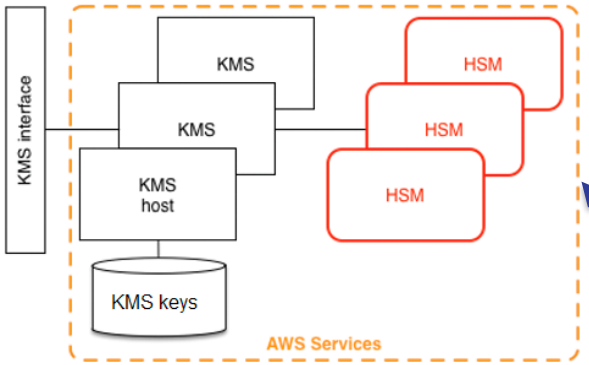
시스템 기반 관리
ISMS-P, CSAP, ISO27001 등 주요 컴플라이언스 충족을 시스템적으로 보장하는 기능을 제공합니다.

개발 보안 환경
주요 암호 키 및 환경 파일을 분리하고 운영 시 동적으로 할당함으로써 개발 / 운영에 대한 보안성을 높일 수 있는 기능을 제공합니다.

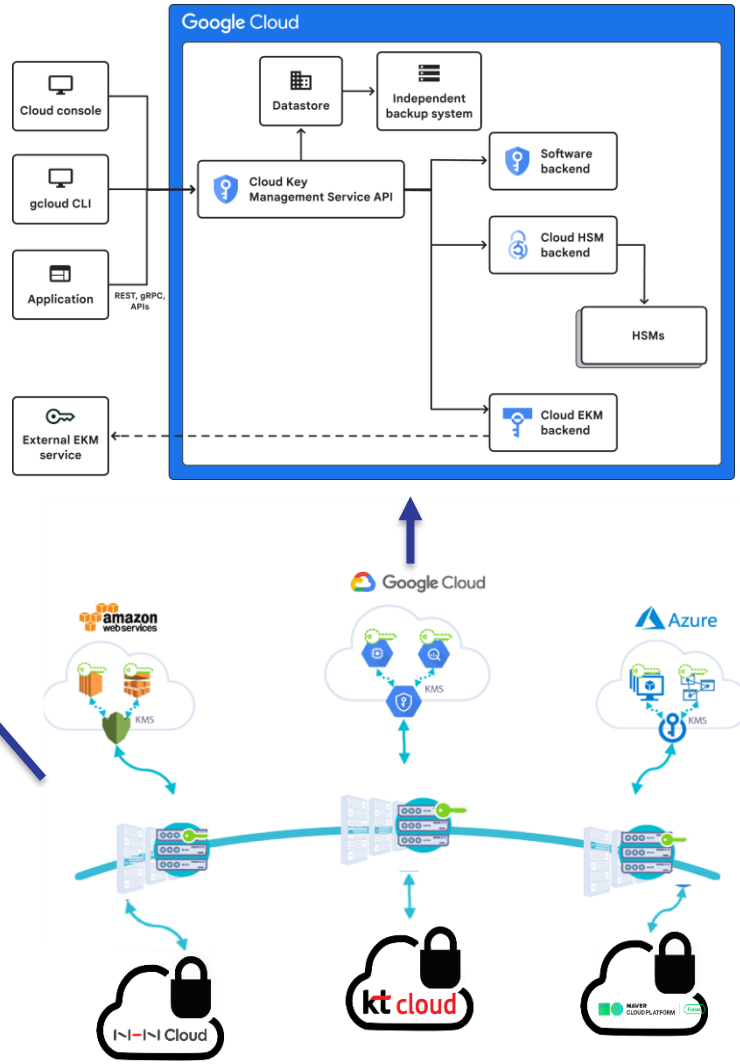
현재 우리가 직면한 클라우드 환경

멀티 클라우드 (Multi-Cloud) 환경으로 전환을 위해서는 'Native Cloud' 로의 'refactoring'도 중요하지만, 각각의 Public Cloud, Private Cloud 에서 개별적으로 관리하는 Key 및 Certificate에 대해서 중앙 집중식 관리를 고려해야 합니다.

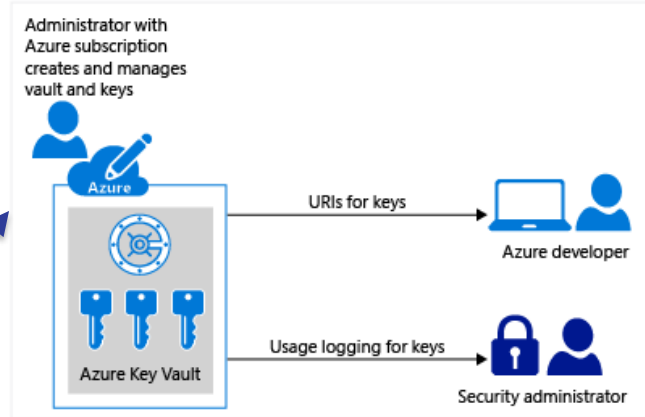
- **비용 절감 및 복잡성 제거**
- **가시성(Visibility) 확보를 통한 시스템간 연관성 분석**
- **IT 조직의 관리의 편의성 및 보안성 확보**



AWS KMS: AWS Key Management Service (KMS)는 데이터 암호화에 사용되는 암호화 키를 쉽게 생성하고 제어할 수 있는 완전 관리형 서비스입니다. AWS KMS는 다른 AWS 서비스와 통합되며 AWS KMS API를 지원하는 자체 응용프로그램과 함께 사용할 수 도 있습니다.

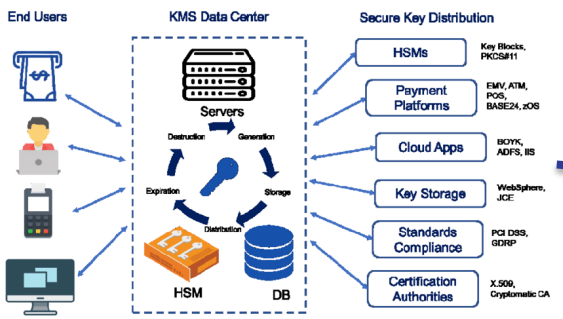


Google Cloud KMS: Google Cloud Key Management Service (KMS)는 클라우드 서비스의 암호화 키를 관리할 수 있는 클라우드 기반 서비스 입니다. Google Cloud KMS는 키에 대한 강력한 보호 기능을 제공하고 여러 암호화 알고리즘을 지원합니다.



Azure Key Vault: Azure Key Vault는 중요한 데이터에 대한 안전한 키 관리 및 저장 기능을 제공하는 클라우드 기반 서비스입니다. 키 순환, 백업 및 복원, 감사와 같은 기능을 제공합니다.

가장 효과적인 비밀 자산(Secret Asset) 관리는?



KMS: 기업 내 자체 구축 및 관리

On-Premises

KMS: NHN Cloud 자체 Private Cloud 서비스 이용

KMS: KT Cloud 자체 Public Cloud 서비스 이용

KMS: Naver Cloud 자체 Private Cloud 서비스 이용

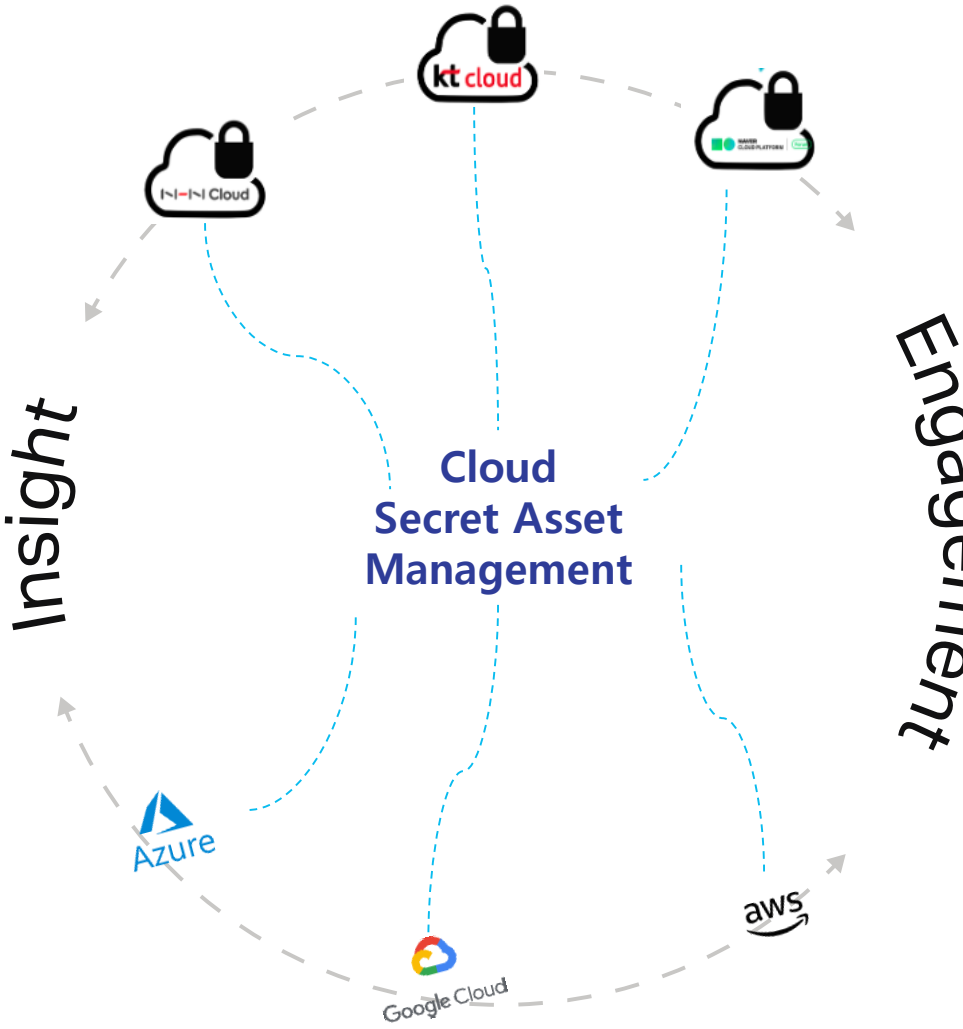
Hybrid

KMS: AWS 자체 Public Cloud 서비스 이용

KMS: Azure 자체 Public Cloud 서비스 이용

KMS: Google Cloud 자체 Public Cloud 서비스 이용

Cloud



On-Prem, Public Cloud, Private Cloud (Multi-Cloud) 환경을 단일 CSAM으로 관리할 수 있습니다.

효과적인 비밀 자산(Secret Asset)관리의 이점 I

비밀 자산에 대한 높은 가시성(Visibility)을 통한 상관관계 분석을 수행할 수 있다.

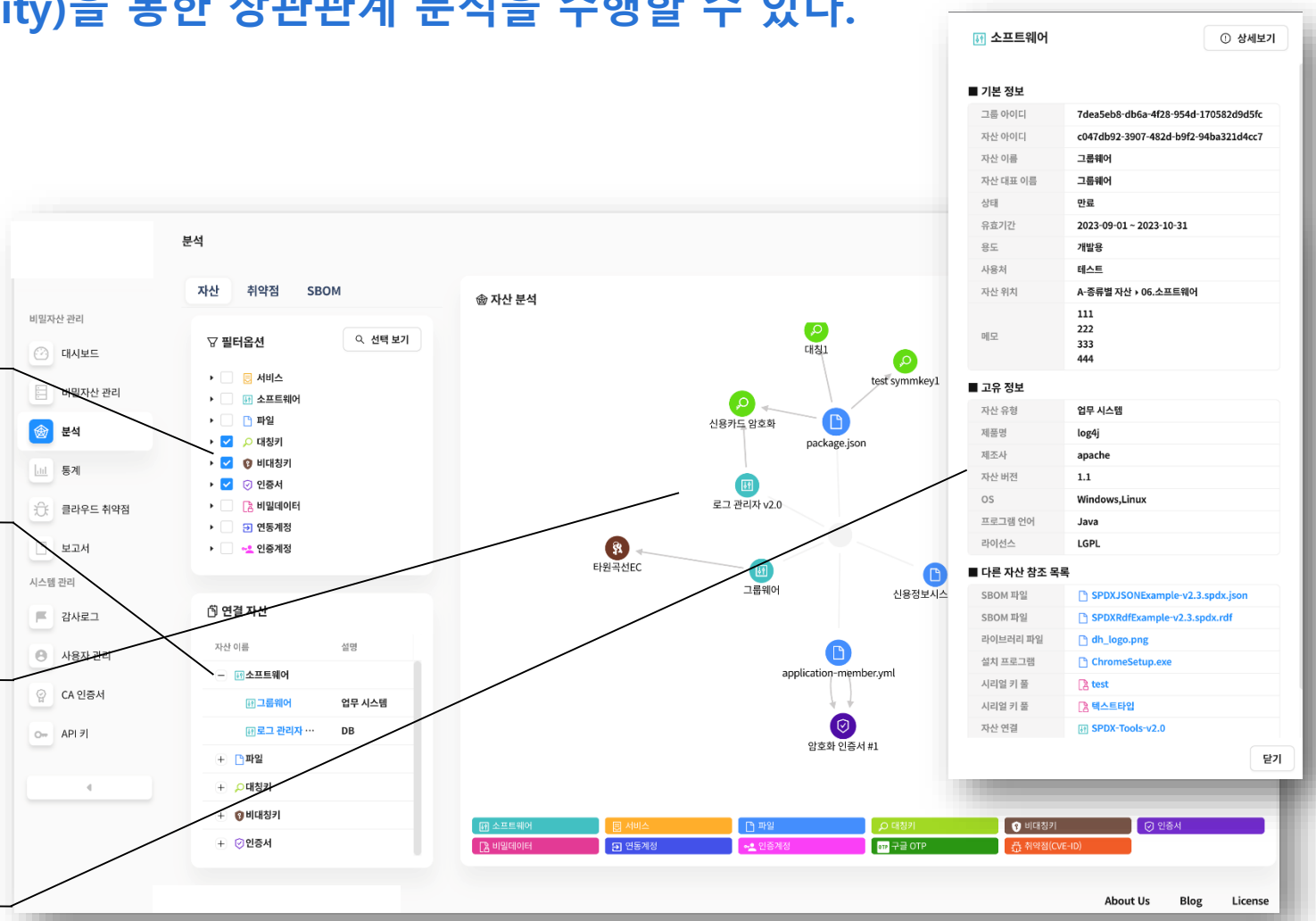
Management Console의 '분석' 기능은 Key 및 Certificate과 같은 Secret Asset(비밀 자산)들의 상관관계를 한눈에 파악할 수 있는 기능을 제공합니다.

필터옵션:
다양한 키(대칭키, 비대칭키, 인증서 등)들 중에서 분석하기 원하는 값들만 선택합니다.

연결 자산:
선택한 키(대칭키, 비대칭키, 인증서 등)들과 연관된 다양한 비밀 자산(Secret Asset)들에 대한 목록을 보여줍니다.

자산 분석:
선택한 키(대칭키, 비대칭키, 인증서 등)들과 연관된 다양한 비밀 자산(Secret Asset)들 사이에 연관성을 한눈에 보면서 해당 키 값의 상태 변경이 시스템에 어떠한 영향을 미칠지 예상할 수 있습니다.

상세 정보:
[자산 분석] 화면에서 특정 키 값을 선택하면 상세정보를 나타내는 화면이 오른쪽에 출력됩니다.



효과적인 비밀 자산(Secret Asset)관리의 이점 II

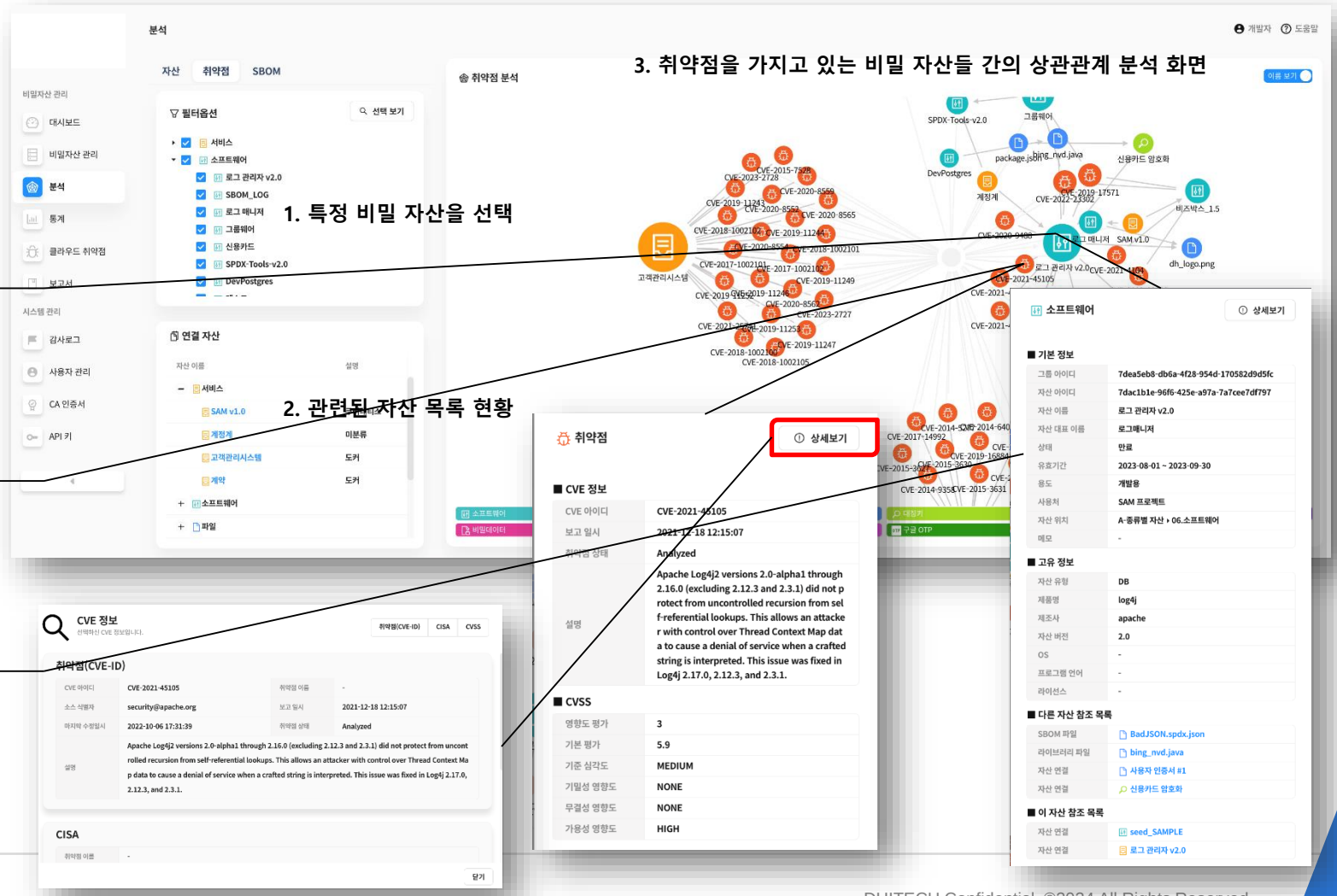
비밀 자산에 대한 높은 가시성(Visibility)을 통한 상관관계 분석을 통해 취약점, 컴플라이언스 대응에 높은 효율성을 제공한다.

Management Console의 '분석' 기능 중 [취약점] 탭은 특정 취약점을 가지고 있는 'Secret Asset(비밀 자산)'들 간의 연관 관계를 보여줌으로써, 해당 취약점이 영향을 미칠 수 있는 자산들의 현황을 쉽게 파악할 수 있습니다.

자산 링크:
특정 취약점을 가지고 있는 자산이 무엇인지 보여 주며, 해당 자산을 클릭하면 자산에 대한 상세 정보를 제공합니다.

취약점 링크:
특정 취약점을 클릭하면 해당 취약점에 대한 상세 정보를 화면에 출력해 줍니다.

상세보기:
[상세 보기] 버튼을 클릭하면 더 상세한 관련 정보를 화면에 출력해 줍니다.



효과적인 비밀 자산(Secret Asset)관리의 이점 II

비밀 자산에 대한 높은 가시성(Visibility)을 통한 상관관계 분석을 통해 취약점, 컴플라이언스 대응에 높은 효율성을 제공한다.

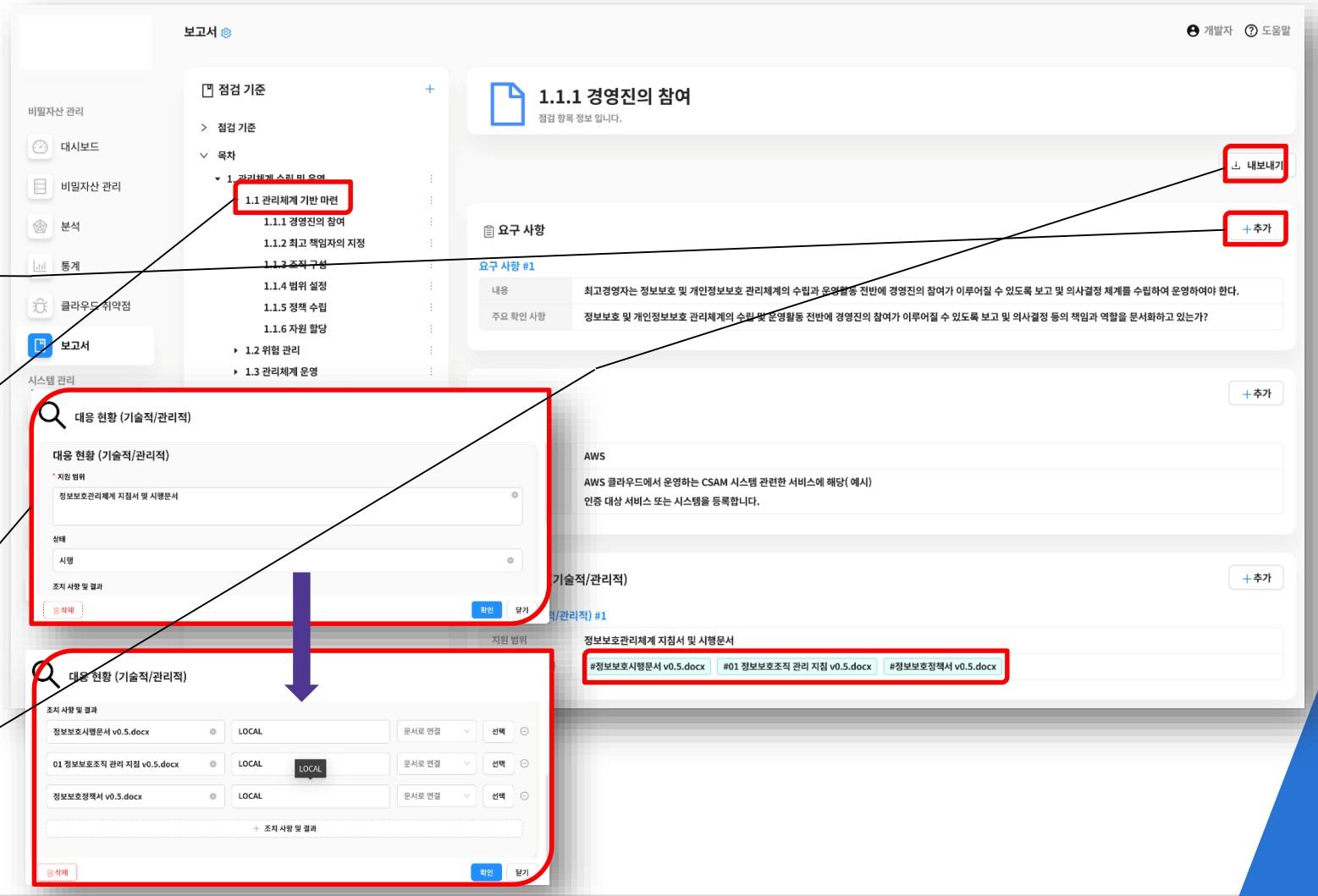
각각의 규제 점검 사항들에 상세 내용을 기업 및 기관에 적합한 형태로 입력하여 관리할 수 있는 기능을 제공합니다.

추가 버튼:
각 규제에 따른 목차 또는 조직 내에서 정한 순서대로 입력하여 관리할 수 있는 항목들을 추가하는 역할을 지원합니다.

각 항목 별 링크 기능:
각 규제의 세부 사항들에 대한 관리를 위해 해당 항목에 관련된 규제 내용 및 조직 내에서 관리하는 증빙자료 들에 정보를 볼 수 있는 페이지를 출력합니다.

각 항목 별 상세 관리 내역 확인:
각 규제에 대한 상세 내용을 관리하는 대화창 입니다. 증빙 자료 등을 첨부하거나 제거하는 역할을 수행할 수 있습니다.

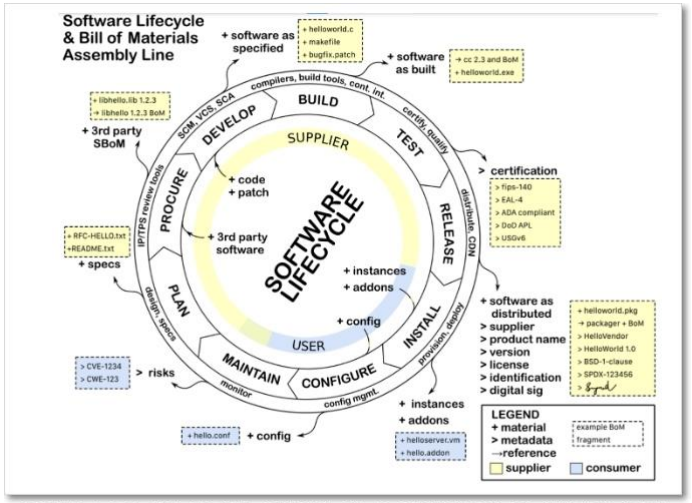
내보내기:
각 규제 별 관리하고 있는 내역들에 대한 현황 및 증빙 자료들을 보고서 형태로 출력하는 기능을 제공합니다. 외부 감사 시 효과적 입니다.



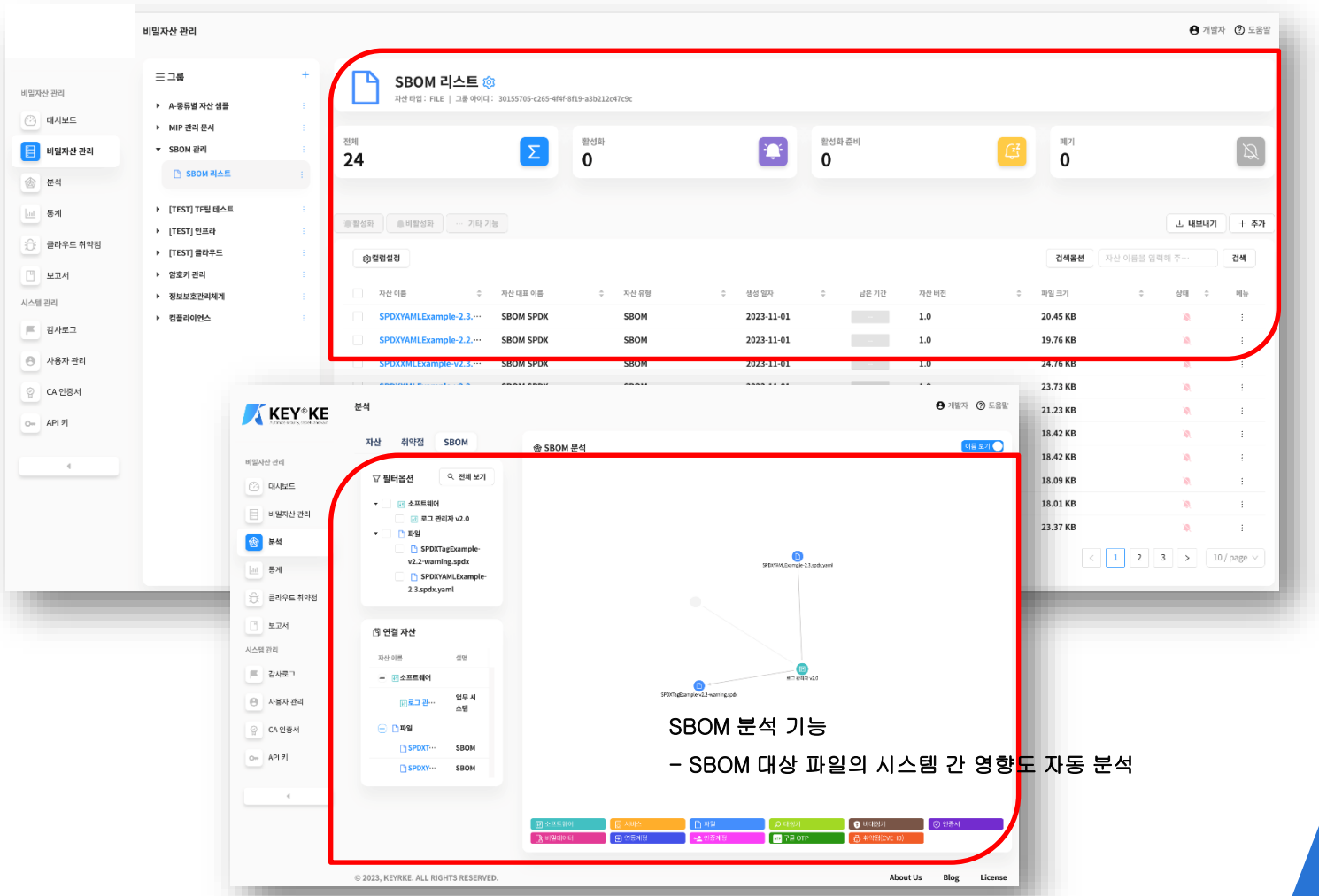
효과적인 비밀 자산(Secret Asset)관리의 이점 II

비밀 자산에 대한 높은 가시성(Visibility)을 통한 상관관계 분석을 통해 취약점, 컴플라이언스 대응에 높은 효율성을 제공한다.

개발자가 최종 제품을 위해 활용하는 제3자가 제공하는 라이브러리나 프레임워크 등도 '소프트웨어' 범주에 포함된다. 이러한 각 소프트웨어를 구성하는 또 다른 모든 소프트웨어의 목록 및 이력을 기록한 것이 SBOM 입니다. Management Console의 'SBOM' 기능은 이러한 "Software Bill of Material"을 관리해 주는 것입니다.



소프트웨어 라이프사이클 각 단계에서의 코드 변경 및 이에 따른 SBOM 업데이트 [출처: NTIA 서베이 보고서]



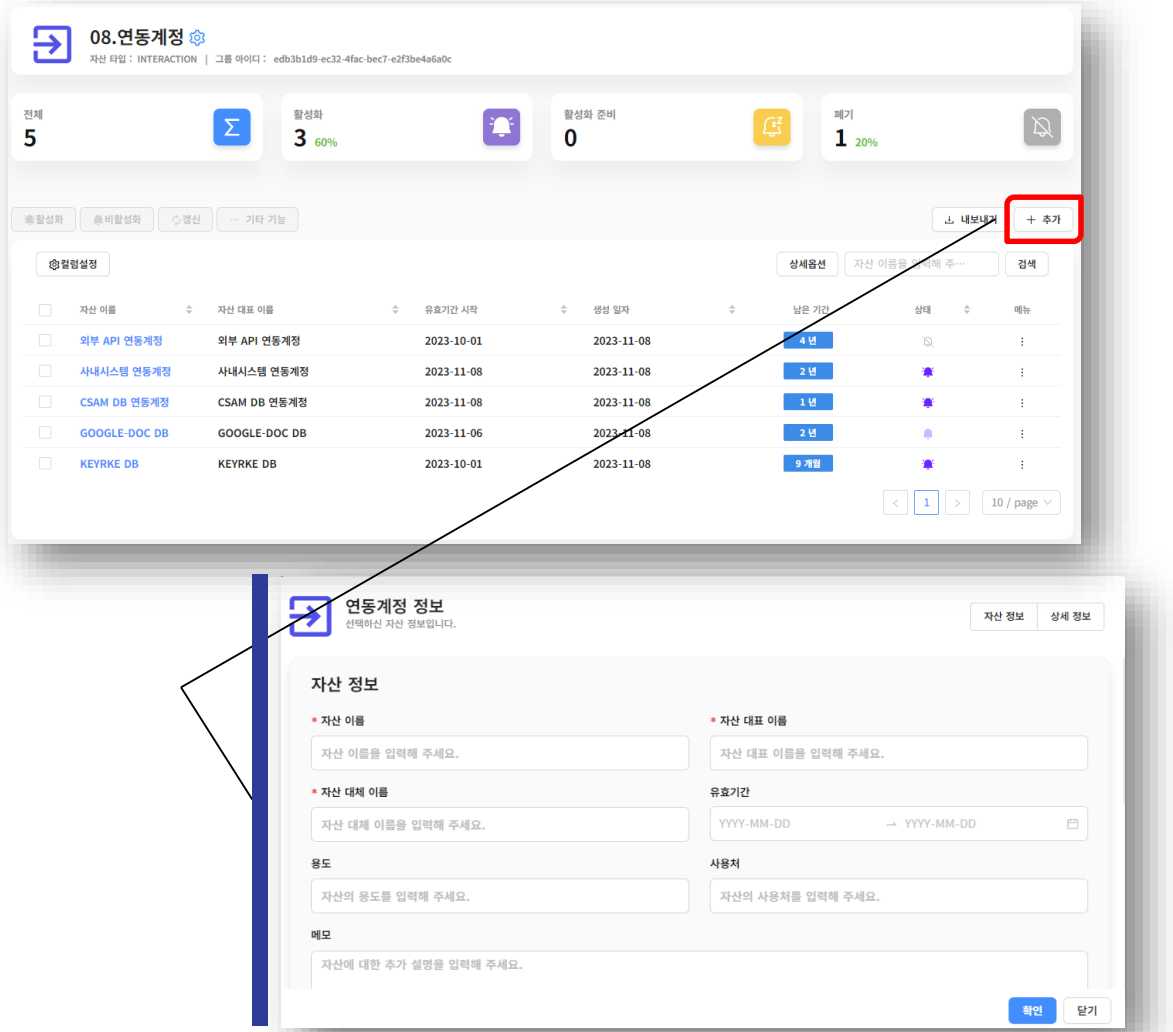
효과적인 비밀 자산(Secret Asset)관리의 이점 III

데이터베이스 패스워드에 대한 주기적인 자동 변경 등의 컴플라이언스 대응을 자동화 할 수 있다.

Management Console의 '연동 계정' 기능을 통해
'자동화된 DB 패스워드 변경' 기능을 구현할 수 있습니다.

컴플라이언스 준수: 정보통신망 이용촉진 및 정보보호 등에 관한 법률과 개인정보 보호법 준수를 위한 데이터베이스의 패스워드 자동화 관리

- 관리해야 하는 수많은 인프라 환경에서 관리자가 수동으로 변경 관리해야 하는 것을 자동화하여 편리함과 보안성 향상을 제공합니다.
- 다양한 환경에서 구현이 가능합니다.
  - ➢ On-prem
  - ➢ Public Cloud (AWS, Azure, Google Cloud, etc...)
  - ➢ Private Cloud (Naver Cloud, NHN Cloud, KT Cloud, etc...)
  - ➢ Hybrid Cloud



On-Premises

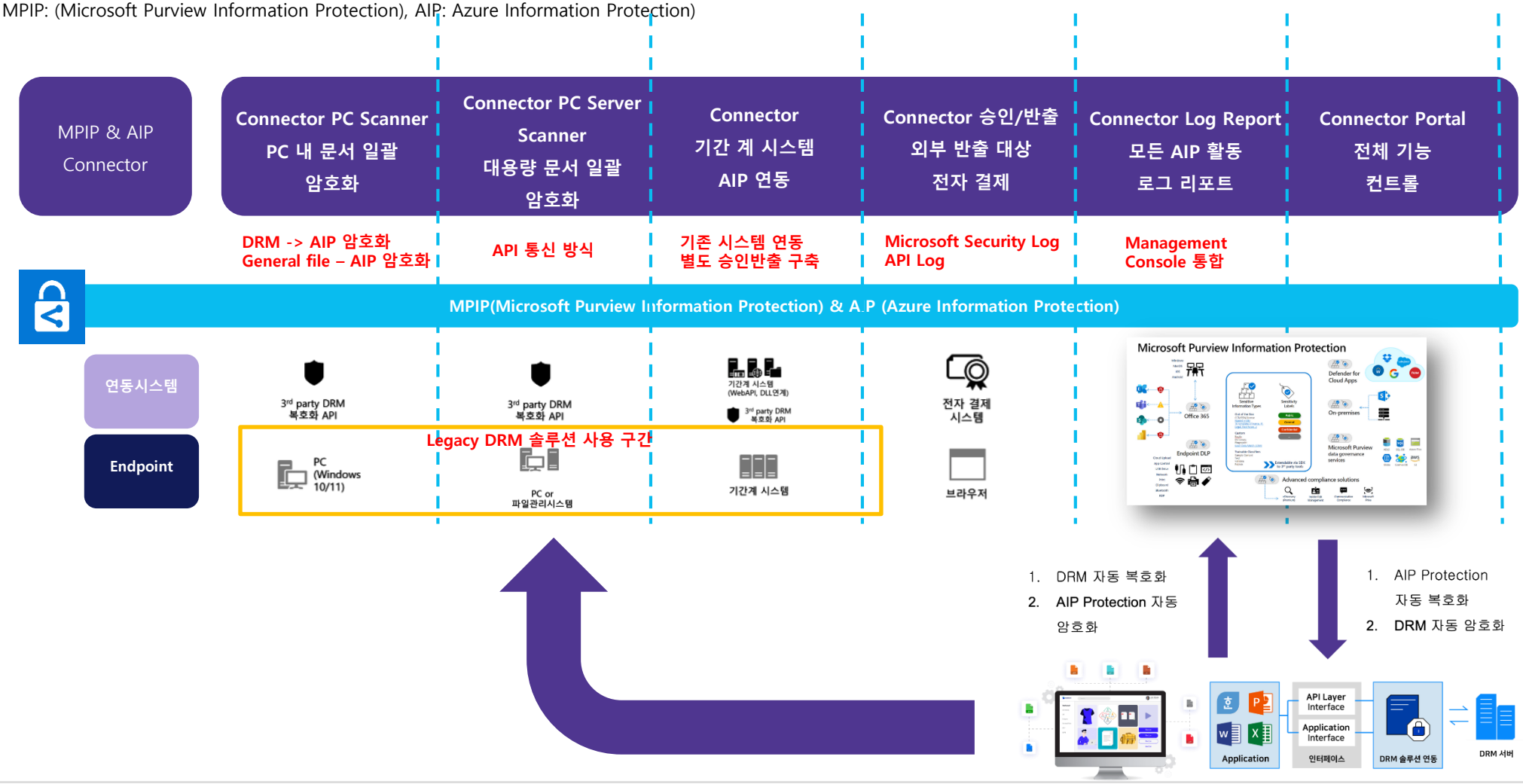
Hybrid

Cloud

효과적인 비밀 자산(Secret Asset)관리의 이점 IV

MPIP & AIP에 대한 시스템 운영 복잡성으로 인한 업무 과부하를 줄일 수 있다.

MPIP: (Microsoft Purview Information Protection), AIP: Azure Information Protection)



Thank You!

발표자 : 신승목 상무

M. 010-2032-8014

E. smshin@dhitech.co.kr