CLOUDSEC 2023 ENVISION IT

Hosted by TREND MICRO

경계 없는 업무 환경에서 문서 보안 오케스트레이션

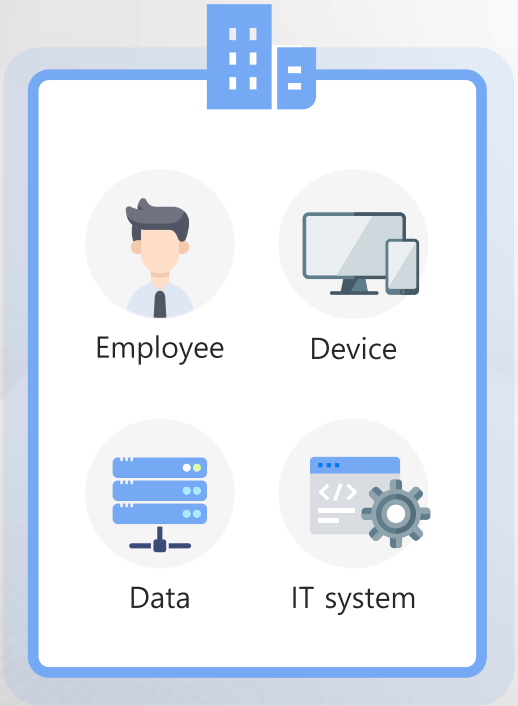
제로 트러스트 모델의 적용

SOFTCAMP

문서 보안 오케스트레이션

경계보안 기반의 DRM 한계

› 지금까지의 DRM은 경계 기반의 On-Premise DRM 이였습니다.
사내에서 유통되는 문서를 사외에서 무단으로 유출할 수 없도록 암호화를 하는 것이 솔루션의 목표였습니다.



Local PC 중심의 Agent 기반 솔루션

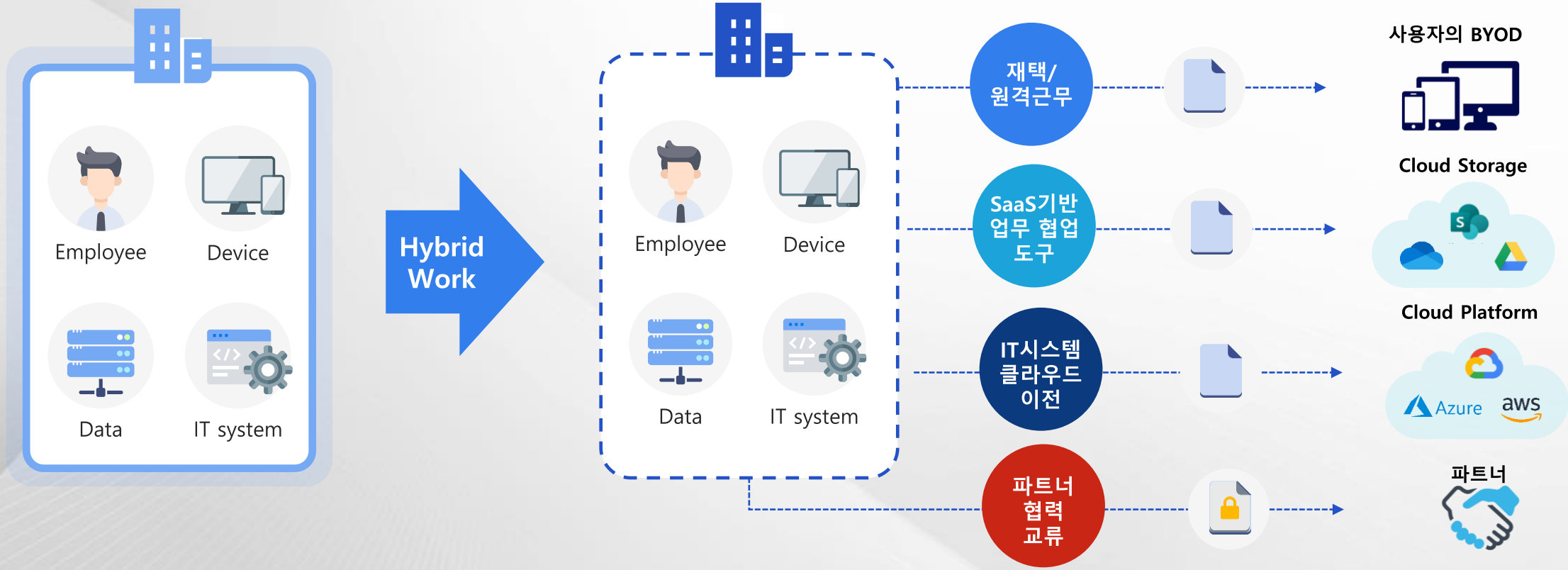
사내에서 유통되는 문서 암호화

사외에서는 암호화 문서 사용 불가

문제점	경계(사무실) 밖으로 이동된 문서는 열람(또는 사용)하지 못하게 한다.

기존의 유출방지 보안 방식의 한계

› 하이브리드 근무 환경으로 전환되면 업무의 경계가 사라졌습니다.
데이터는 더 이상 사내에만 존재하지 않으며, 경계 보안만으로는 대응이 불가능합니다.



목표

- 경계 밖에서도 업무(파일의 열람/편집)가 가능해야 하고, 보안은 유지되어야 한다.
- 파트너 보안이 강화된 상태로 문서, 도면 등의 협력이 필요하다.

컴플라이언스 이슈

“국가 핵심기술 “ 관련 법규 ← 클라우드에 저장할 수 없다.

산업기술의 유출방지 및 보호에 관한 법률

제14조(산업기술의 유출 및 침해행위 금지)

6. 국가핵심기술을 외국에서 사용하거나 외국에서 사용될 것임을 알면서도 제11조의2제1항에 따른 승인을 받지 아니하거나

“영업비밀 보호“ 관련 법규 ← 비밀의 관리성

부정경쟁방지 및 영업비밀보호에 관한 법률

제2조(정의)

2. “영업비밀”이란 공공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로서, 비밀로 관리된 생산방법, 판매방법, 그 밖에 영업~

제9조의2(영업비밀 원본 증명)

① 영업비밀 보유자는 영업비밀이 포함된 전자문서의 원본 여부를 증명 받기 위하여 원본증명기관에 그 전자문서로부터 추출된 고유의 식별값 [이하 “전자지문”(電子指紋)이라 한다]을 등록할 수 있다.

금융기관 망 분리

전자금융감독규정

제15조(해킹 등 방지대책)

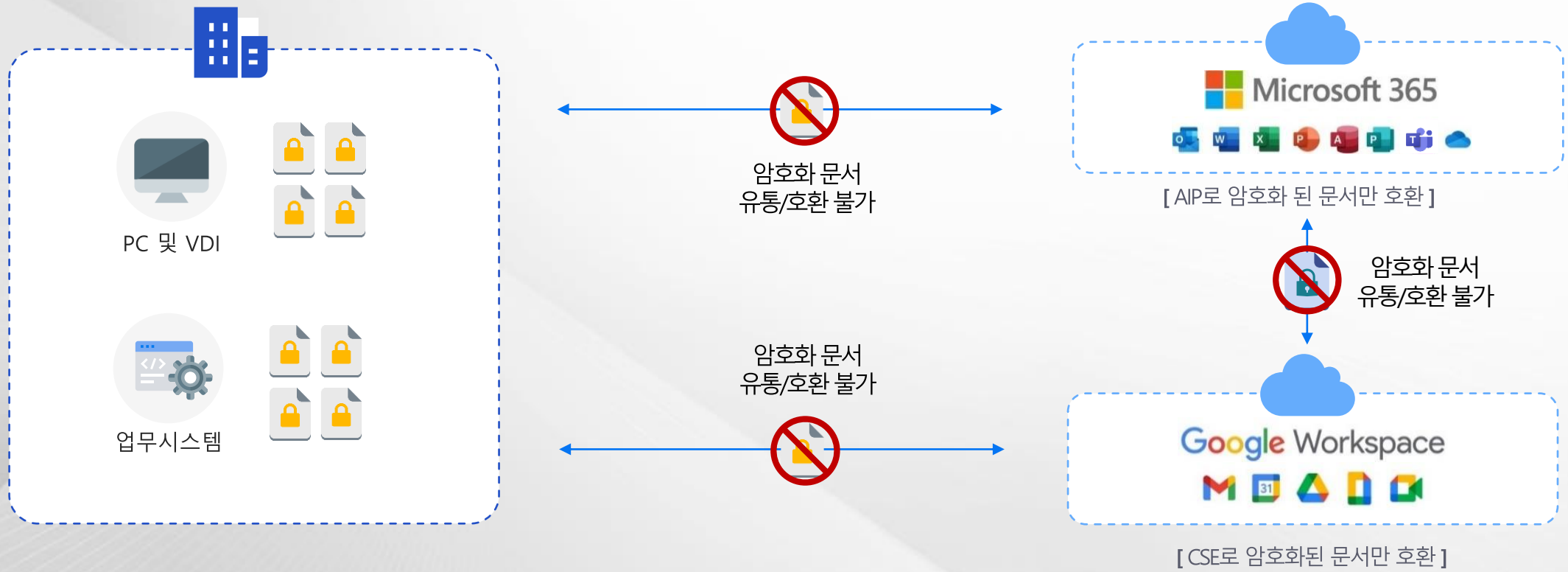
3. 내부통신망과 연결된 내부 업무용시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리 · 차단 및 접속 금지.

CSAP(Cloud Security Assurance Program) ←민간 사업자 제공 클라우드의 국가 공공기관 사용 인증 제도

상 등급 : 민감정보 포함 or 행정 내부업무 운영 시스템 (예정), 중 등급 : 비공개 업무 자료 포함(예정), 하 등급 : 그 외

기술적 환경 변화

› 기존 암호화 문서는 Microsoft365, Google Workspace와 같은 업무 협업 SaaS 도구들과 **호환되지 않아** 업무 생산성 및 문서 사용성에 이슈가 발생합니다.



문제점

- 클라우드 서비스(Microsoft, Google)마다 다른 DRM / 문서 암호화 방식 제공
- 기존 DRM 문서의 호환성 결여
- 클라우드 서비스의 혜택/기능(공동편집 등) 저해

1. Hybrid 환경에 따른 최적의 보안 방법 - 차세대 DRM의 요구 사항

› 하이브리드 환경에서는 기존 DRM의 기능에서 더욱 확장된 기능이 필요합니다.
경계가 사라지고 보다 다양해진 환경에 맞는 보안을 제공해야 합니다.

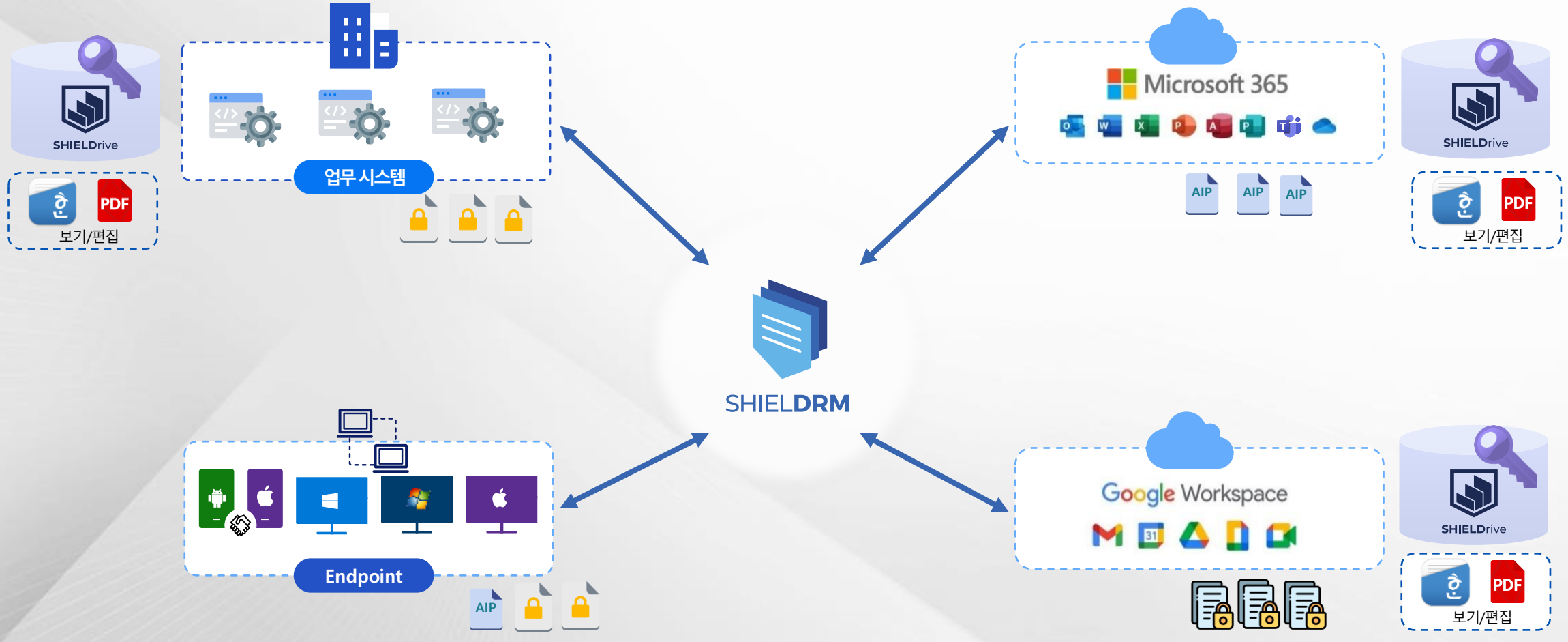
AS-IS

- 로컬 PC 내 문서 파일 암호화
- 사용권한 제어
- 평문 반출 승인
- 업무시스템 연동

TO-BE

- **다양한 환경 지원 (On-Premise, Cloud)**
- **다양한 업무 환경에 최적화된 보안 제공 (Zero-Trust Conditional Access)**
- **업무 환경의 확장으로 발생하는 Compliance 대응**
- **경계가 없는 환경에서 유통 가시성 확보**

1. Hybrid 환경에 따른 최적의 보안 방법



우수성

- 보안 관리자 : 다양한 환경, 문서 형태에 대해서 보안 유지 및 관리가 가능한 가시성 제공
- 사용자 : 보안 유지된 문서를 정책에 따라 편리하게 사용(별도로 변환, 작업, 승인 요청 필요 없음)

1. Hybrid 환경에 따른 최적의 보안 방법 – M365 지원

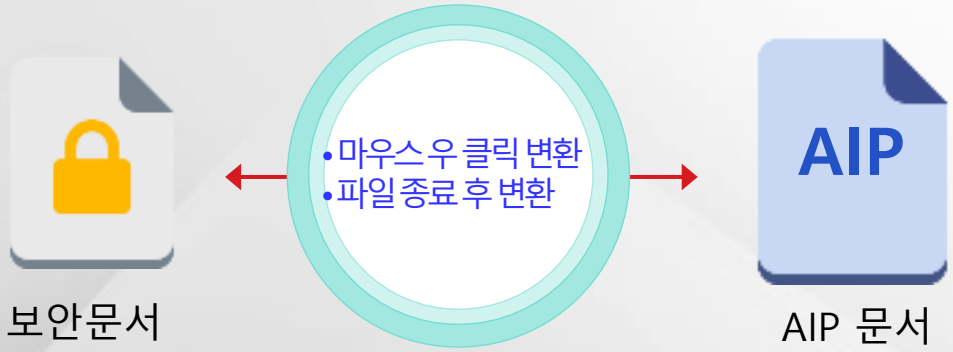
› Endpoint DRM (Document Security) 보안 문서를 OneDrive, Sharepoint, Teams 등 Cloud 저장소에 평문이나 암호화 문서 **업로드 시 AIP 문서로 자동 변환하여** 단절 없는 보안 및 사용성을 제공합니다.

서비스 특징

- 사용자 추가 조작 없이 문서를 Microsoft365 서비스로 업로드하여, 사용(열람/편집/공동편집) 가능
- 클라우드 스토리지 내에서도 AIP 적용을 통한 Cloud-Native 보안 적용
- Zero Trust Conditional 정책으로 사용자/문서 유형 등에 따른 문서 변환(DRM <-> AIP) 정책 집행
- 변환을 위한 **개별 서버 구축 필요 없음**

1. Hybrid 환경에 따른 최적의 보안 방법 – M365 전환

› 로컬 PC (Windows)에서도 정책에 따라 SHIELDRM Local App을 통해
DRM 문서를 AIP로 변환하거나, AIP 문서를 DRM 문서로 변환할 수 있도록 할 수 있습니다.



주요 기능

문서 -> '오른쪽 버튼'을 통한 **문서 변환 제공**
DRM <-> AIP 문서

DRM 문서 열람 후 종료 시 AIP 문서 변환
또는 AIP 문서 열람 후 종료 시 DRM 문서
변환 기능 제공(택일)

DRM 정책과 AIP정책을 매핑하여 각 연계된
암호화 정책으로 변환 제공
* 전사키 DRM 문서는 전사키 AIP 문서로, 특정 조직키 DRM 문서는 특정 조직키 AIP 문서로 변환

서비스 특징

- 로컬 PC에서도 DRM <-> AIP 문서 변환 가능
- 로컬 PC 및 클라우드 환경 모두 보안 적용 및 클라우드와 로컬 간 보안 연계

1. Hybrid 환경에 따른 최적의 보안 방법 – 아이콘 구별

› 기존 암호화 문서와 AIP 레이블 적용 문서를 직관적으로 인식할 수 있도록 아이콘이 식별됩니다.
AIP 레이블은 암호화/비 암호에 따라 추가 구분이 지원됩니다.

기존 암호화 문서

AIP 레이블 적용 아이콘

암호화 여부 | 레이블 차이

암호화 레이블 일반 레이블

서비스 특징

- AIP 레이블 문서 여부 사용자 가시적 확인 가능
  * 기존 M365는 아이콘 구분이 안됨(AIP 문서와 일반 문서 구별 불가)
- 암호화(민감도) 레이블 적용 문서에 대한 가시성 확보 및 업무 혼란 최소화

2. Hybrid 환경의 컴플라이언스 준수 – 국가핵심 기술 취급자

Pain-Point

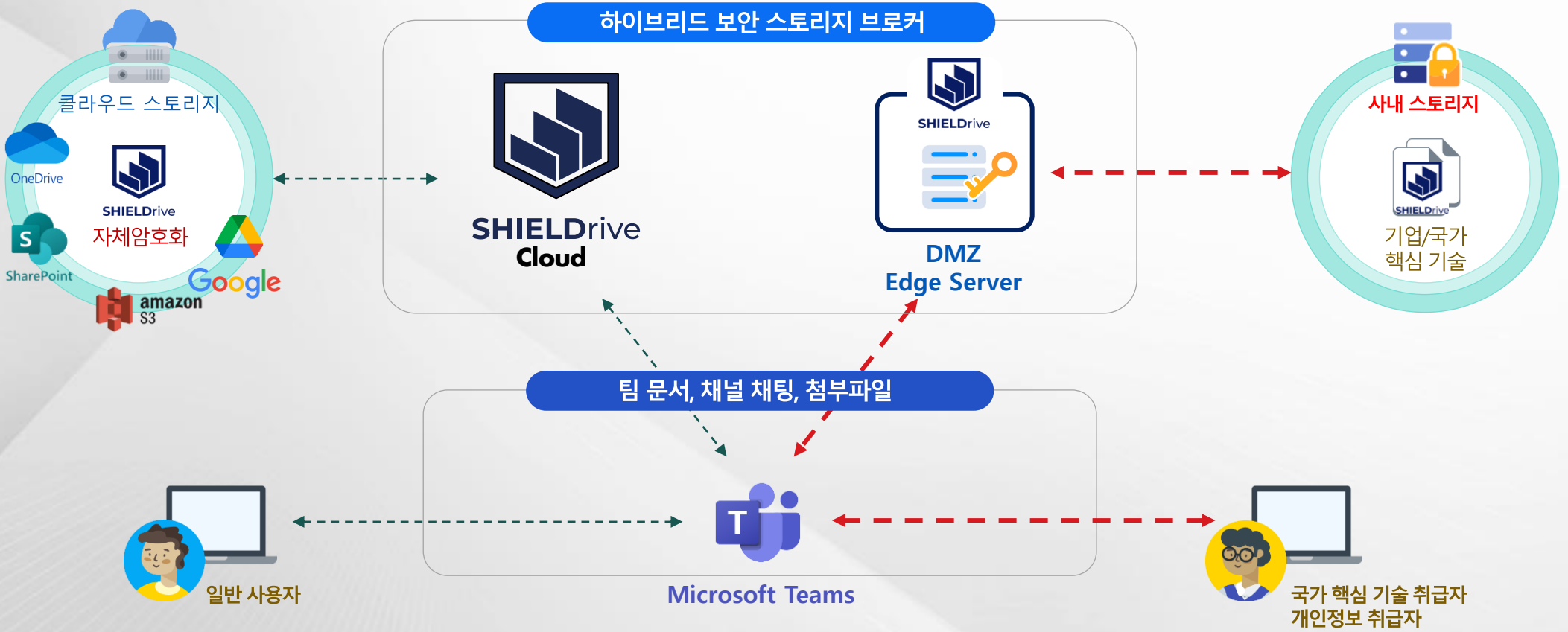
- 협업 도구로서 Teams를 사용하고자 하나
  국가핵심기술 취급자는 클라우드에 사용을 금지하고 있다
- 핵심기술 취급자는 사내 파일서버를 클라우드 처럼 사용하고 싶다
- SharePoint, OneDrive에 저장된 문서의 외부인에 의한 유출이 걱정된다

SHIELDrive

- 다중 스토리지 보안 브로커
  클라우드 저장소(M365, Google 등)와 사내 저장소(파일서버,NAS)의 동시 관리
- 클라우드에 저장된 문서의 암호화/난독화로 데이터 주권 확보
- 컴플라이언스를 준수하면서 협업 가능
  핵심기술 취급자 Teams 등 협업툴 사용가능(문서 공유)

2. Hybrid 환경의 컴플라이언스 준수 – 국가핵심 기술 취급자

› **문서의 주권 확보**(클라우드에 저장되는 문서를 우리회사 암호화키로 관리; BYOK)
Teams 협업 기능 사용 + 사내 시스템에 문서저장 (핵심 정보 사용자 등 클라우드 사용 불가 사용자)



서비스 특징

- 조건부 정책에 따라 클라우드 스토리지 사용자와 **사내 스토리지 사용자 구분 제어**
- 클라우드에 저장되는 문서의 암호화 및 파일명 난독화를 통하여 데이터 주권 확보
- 파일별 암호키 관리로 개인정보보호법 및 **GDPR 요건 충족**(암호키 삭제로 문서 삭제 보장)

2. Hybrid 환경의 컴플라이언스 준수 – 국가핵심 기술 취급자

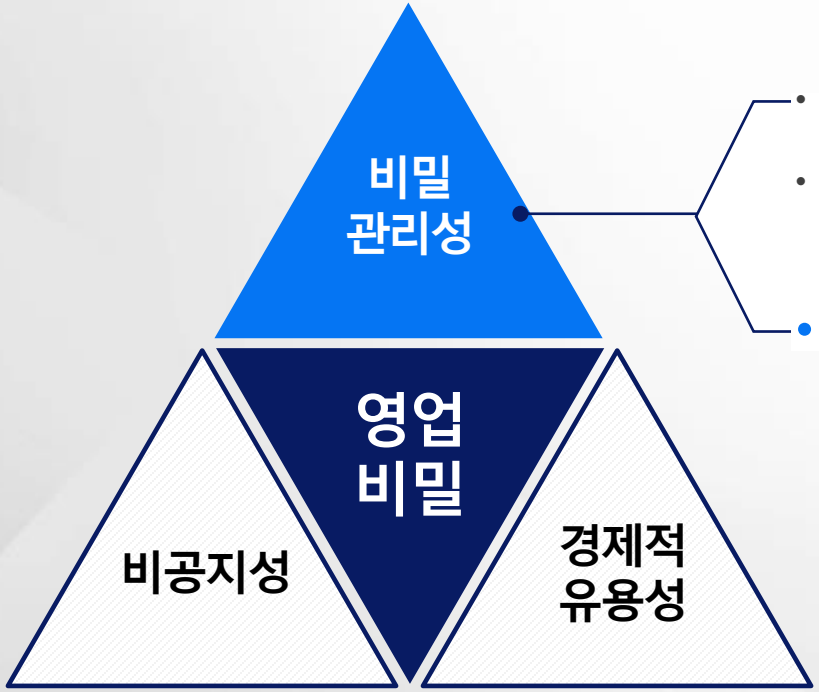
› 연결된 스토리지 유형에 따른 열람/편집/공동편집을 지원합니다.

저장 스토리지 유형	기본 문서 편집기	기타 확장자 문서 편집기
OneDrive SharePoint Microsoft 365 클라우드 스토리지	•Micrososft365 지원 확장자는Microsoft Office App/Web 으로 문서 열람„편집 및공동 편집	•hwp, hwpx 등의 확장자는 한컴오피스 웹로 공동편집 • 그 외 확장자는 SHIELDViewer로 읽기 전용으로 사용 *SHIELDViewer는 소프트캠프에서 제공하는 웹 뷰어입니다.
Google Drive	•Google docs 지원 확장자는Google docs를통해 웹으로문서 열람„편집 및공동 편집가능	•hwp, hwpx 등의 확장자는 한컴오피스 웹로 공동편집 • 그 외 확장자는 SHIELDViewer로 읽기 전용으로 사용 *SHIELDViewer는 소프트캠프에서 제공하는 웹 뷰어입니다.
S3, NAS 등 문서편집기 미 제공 스토리지	•S3, NAS 등자체웹문서편집기가없는스토리지는 한컴오피스웹을통해열람,편집 및공동 편집가능 *지원Web 문서편집기는 향후 변경 될 수 있습니다.	• 한컴오피스 웹에서 지원하지 않는 확장자는 SHIELDViewer(자체 웹 뷰어)로 읽기 전용으로 사용

*도면(CAD) 파일과 AIP암호화된 PDF는 현재 웹 뷰어를 제공하지 않습니다.

2. Hybrid 환경의 컴플라이언스 준수 – 영업 비밀의 관리

› 영업비밀 침해로 인한 **분쟁 시 중요한 쟁점 및 판단 기준은?**



- 실무상 비밀관리성 부정되는 경우 많음
- "경제적 유용성"이 다투어지는 경우는 드묾
  실제 사건에서는 주로 "**비공지성"과 "비밀관리성"이 쟁점**
- **최근 "비밀관리성"이 중요한 쟁점 및 판단 기준**

부정경쟁방지 및 영업비밀관리에 관한 법률

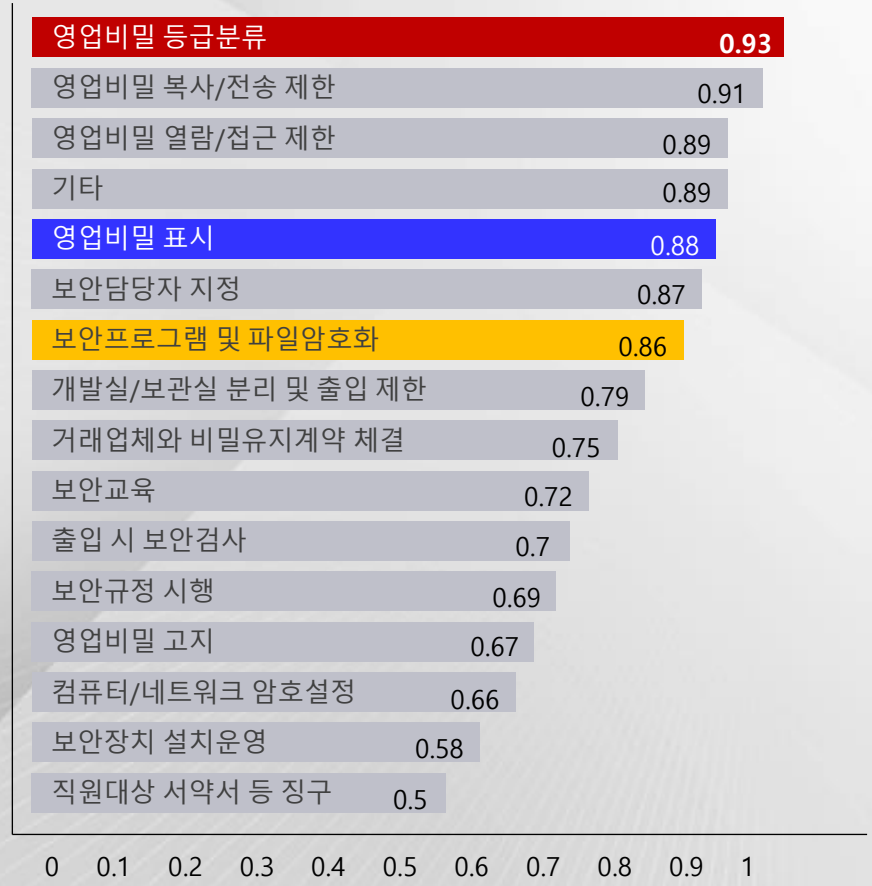
- 부정경쟁방지법은 절취, 기망, 협박 기타 부정한 수단으로 영업비밀을 취득하거나(부정취득) 근로계약 등에 의해 비밀유지 의무가 있는 자가 재직 중 또는 퇴직 후에 부정이익을 얻을 목적으로 영업비밀을 사용·공개하는 행위(비밀유지의무위반)를 침해행위로 규정 하고 있다.
  이 법은 영업비밀 침해행위에 대하여 손해배상청구, 금지·예방청구 및 강력한 형사처벌(5년 이하의 징역) 등을 규정하고 있다

관리조치 - 제3장 영업비밀의 관리

- 영업비밀 보유자는 영업비밀이 포함된 전자문서의 원본 여부를 증명 받기 위하여 제9조의3에 따른 영업비밀 원본증명기관에 그 전자문서로부터 추출된 고유의 식별값 [이하 "전자지문"(電子指紋)이라 한다]을 등록할 수 있다.
- 제9조의3에 따른 영업비밀 원본증명기관은 제1항에 따라 등록된 전자지문과 영업비밀 보유자가 보관하고 있는 전자문서로부터 추출된 전자지문이 같은 경우에는 그 전자문서가 전자지문으로 등록된 원본임을 증명하는 증명서("원본증명서")를 발급할 수 있다.

2. Hybrid 환경의 컴플라이언스 준수 – 영업 비밀의 관리

› 영업 비밀 침해로 인한 기업의 손실을 관리하는 방안은?



[영업비밀 관리 방법과 법원 판례 승소율 분석]

'비밀관리성' 유지 위한 다양한 방안 마련 필요

- 기업에서 수기로 대량의 영업비밀을 관리 하기엔 한계
- 모든 영업비밀관리 방안을 갖추기엔 막대한 비용 문제 발생
- 체계화 되고 편리한 자동화 솔루션 필요

소프트캠프 문서 분류 및 등급 관리 서비스

- **체계화** : 기존 고객사의 다양한 문서 패턴 파악
- **자동화** : 수기로 일일이 문서 등급 분류를 하지 않고 간단한 절차만으로 자동 분류 가능
- **간소화** : 다양한 영업분리 방안을 한번에 지원

2. Hybrid 환경의 컴플라이언스 준수 – 영업 비밀의 관리

› 소프트캠프의 문서분류 및 등급관리 서비스는 사용자의 **간단한 문서 등록 만으로** 영업비밀관리가 이루어집니다.

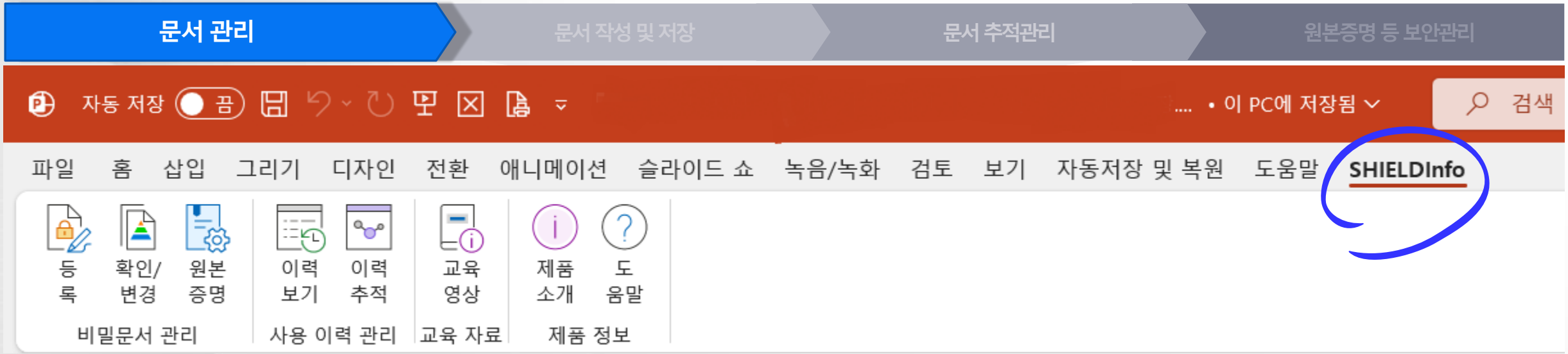
SHIELDInfo

- ✓ 문서 등급관리
- ✓ 비밀 문서 열람 고지 / 동의
- ✓ 원본 증명

사용자 시나리오

1. **신규문서 작성** — 영업비밀문서로 등록
2. **영업비밀등급 평가** — 단계별 문서 분류
3. **자동등급 설정** — 자동으로 문서등급 분류
1. **등록문서 열람** — 영업비밀문서로 등록된 문서
2. **영업비밀등급 고지** — 영업비밀문서 고지 안내
3. **자동등급 확인** — 리본메뉴에 보안등급 표시

2. Hybrid 환경의 컴플라이언스 준수 – 영업 비밀의 관리



문서 등급 지정

- 문서 분류 및 등급을 지정
- 등록된 문서 분류 및 등급 수정

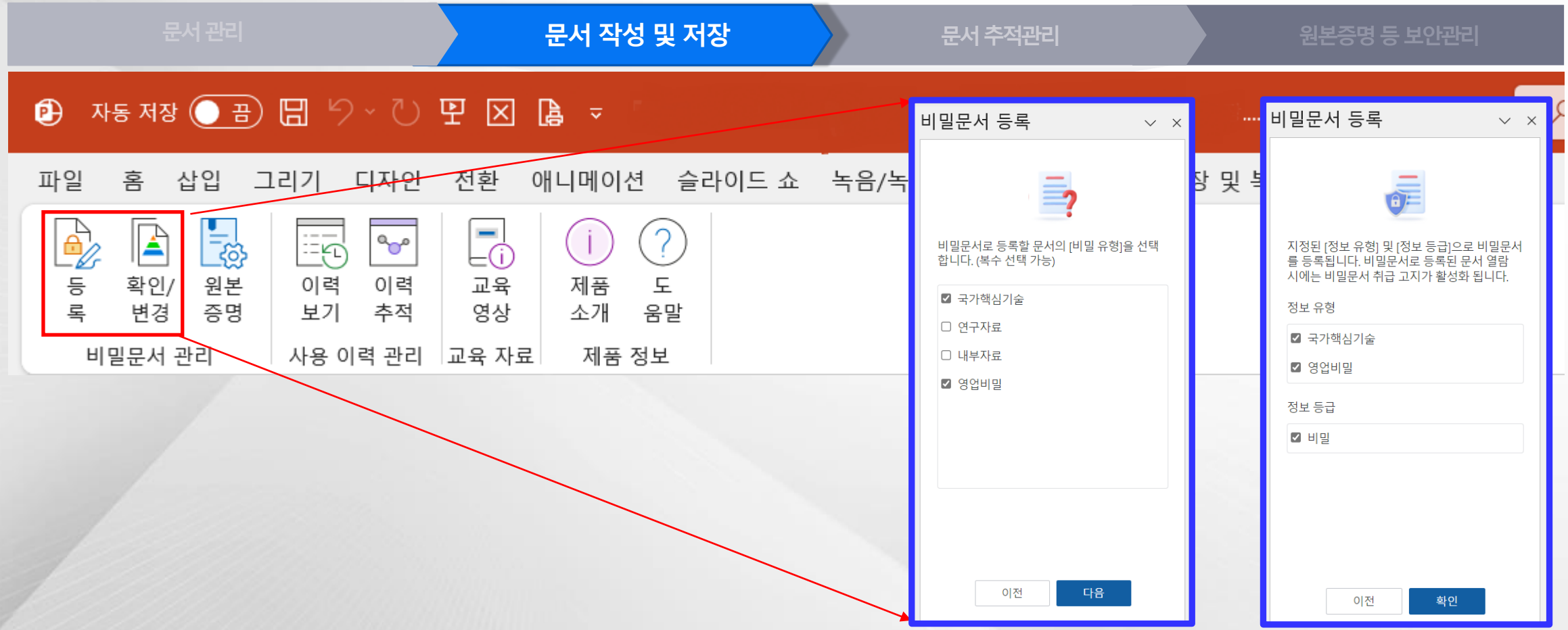
문서 등급 확인

- 등록된 문서의 분류 및 등급 확인
- 문서의 취급주의 안내 표시 및 동의

도움말

- 온라인 사용자 도움말 표시

2. Hybrid 환경의 컴플라이언스 준수 – 영업 비밀의 관리

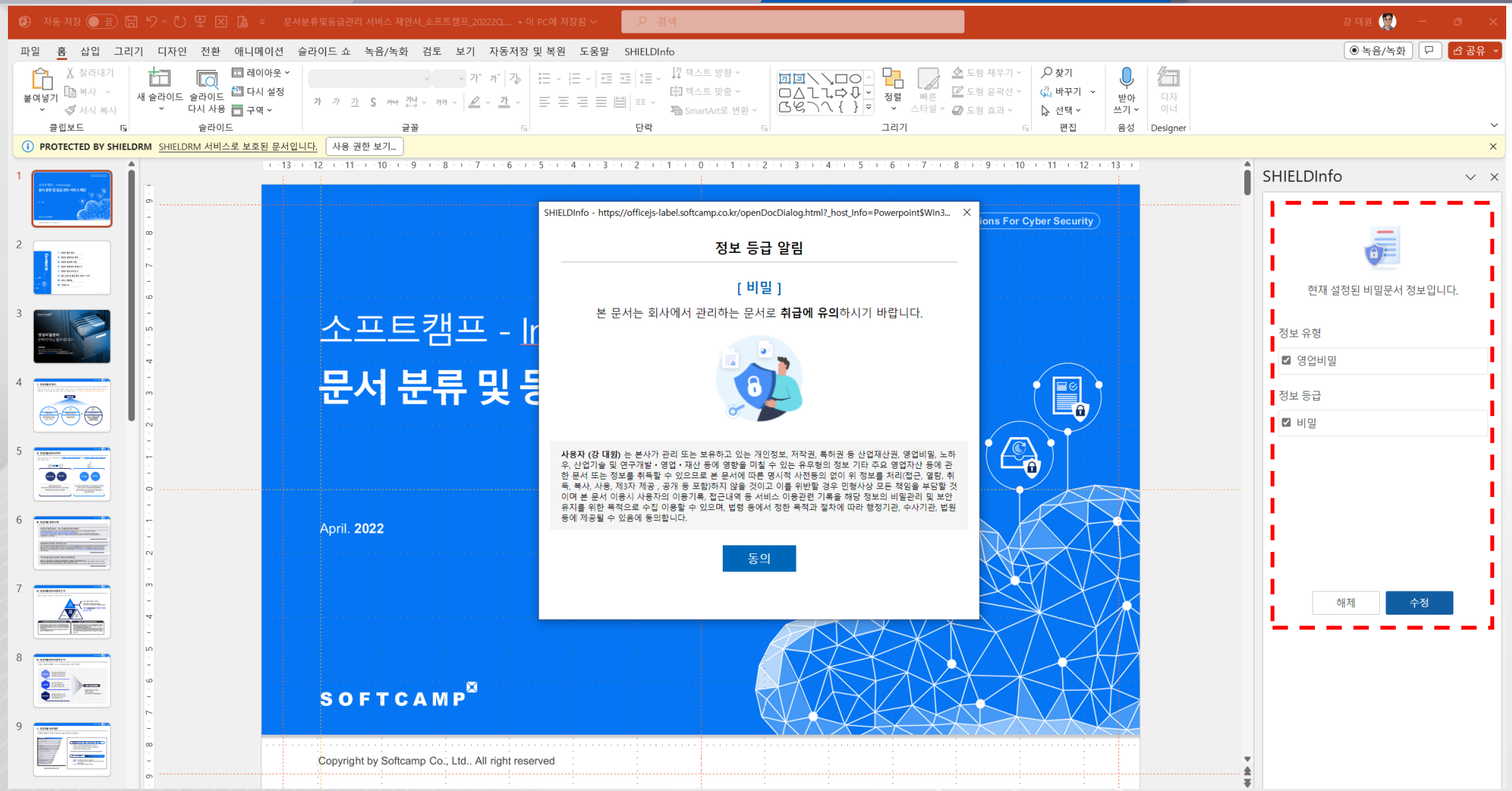


특징

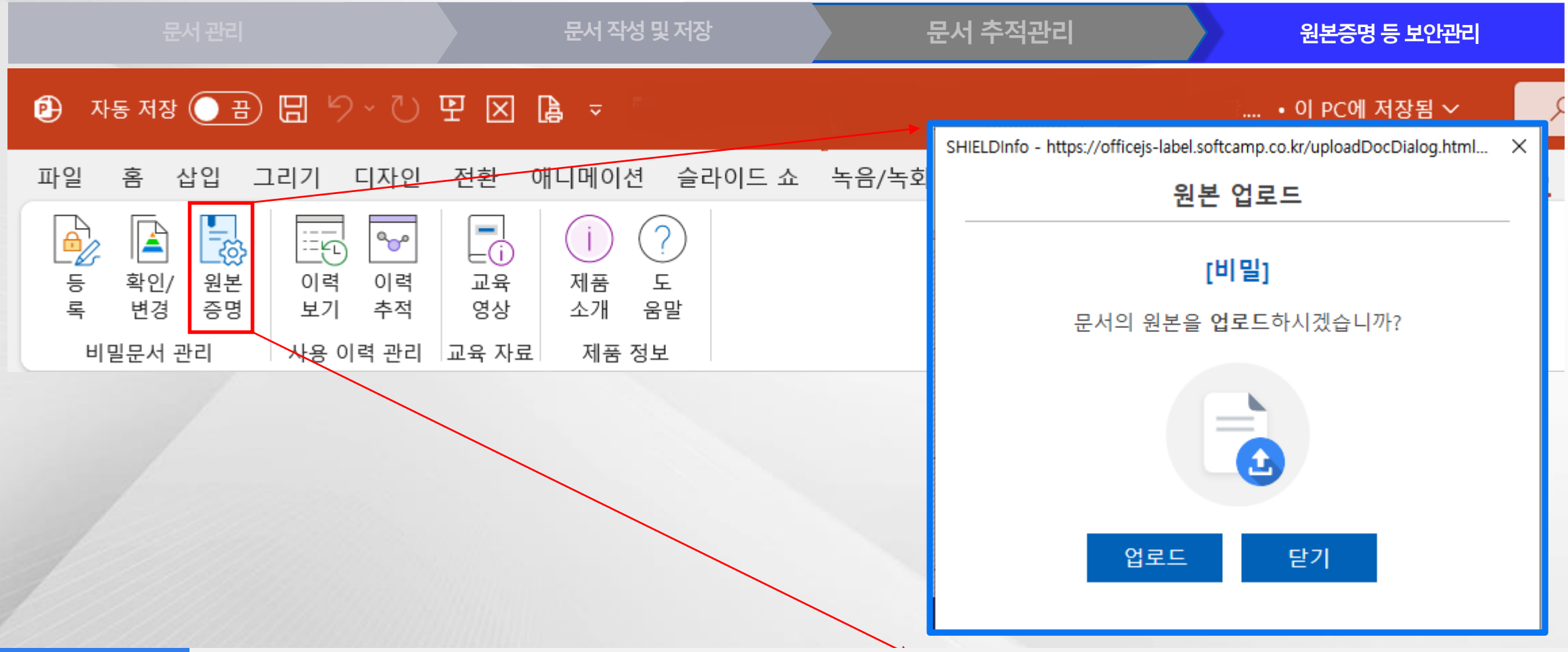
- 문서 작성 완료 후, 문서 작성자가 직접 정보 유형 및 정보 등급 지정

2. Hybrid 환경의 컴플라이언스 준수 – 영업 비밀의 관리

문서 관리 | 문서 작성 및 저장 | **문서 추적관리** | 원본증명 등 보안관리



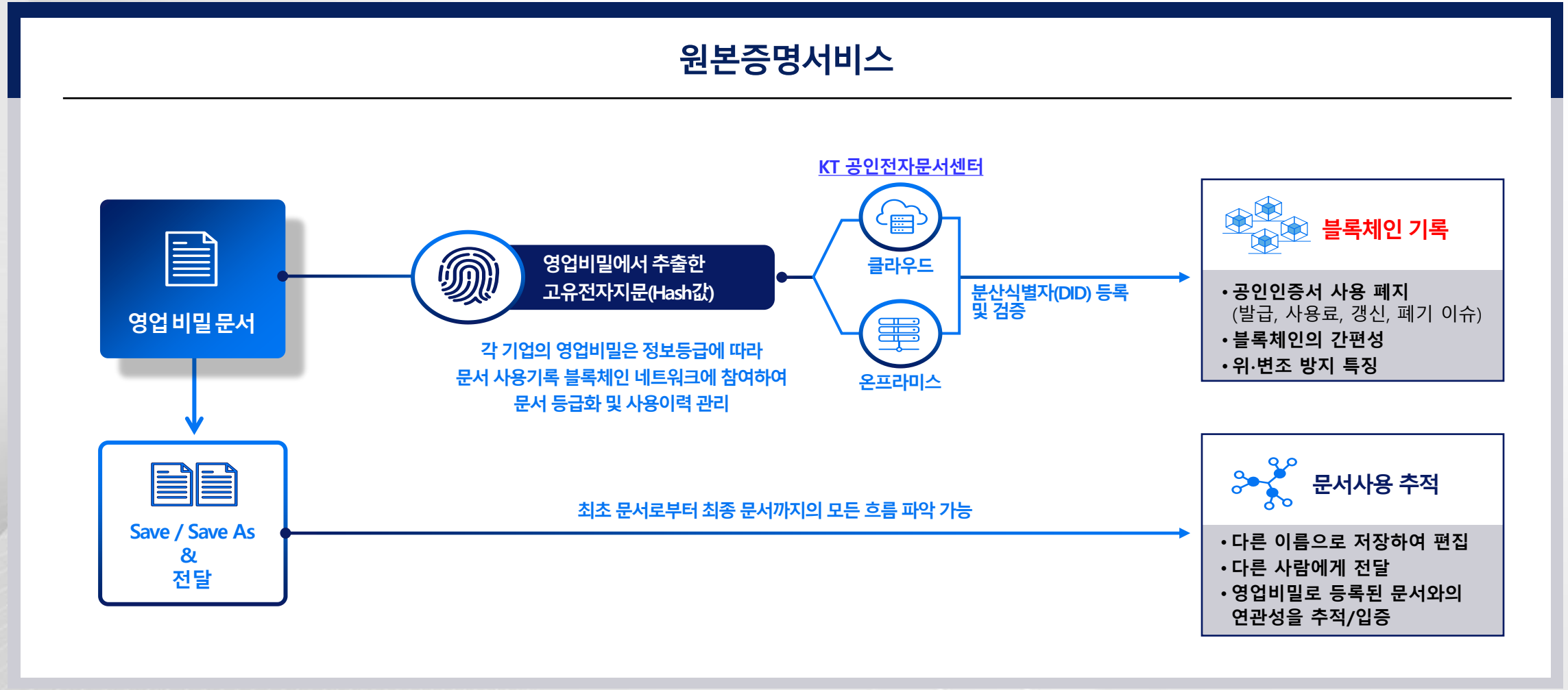
2. Hybrid 환경의 컴플라이언스 준수 – 영업 비밀의 관리



특징	• 문서를 업로드하여 원본임을 증명하는 기능 (Hash 값 등록, 증명서 발급)

2. Hybrid 환경의 컴플라이언스 준수 – 영업 비밀의 관리

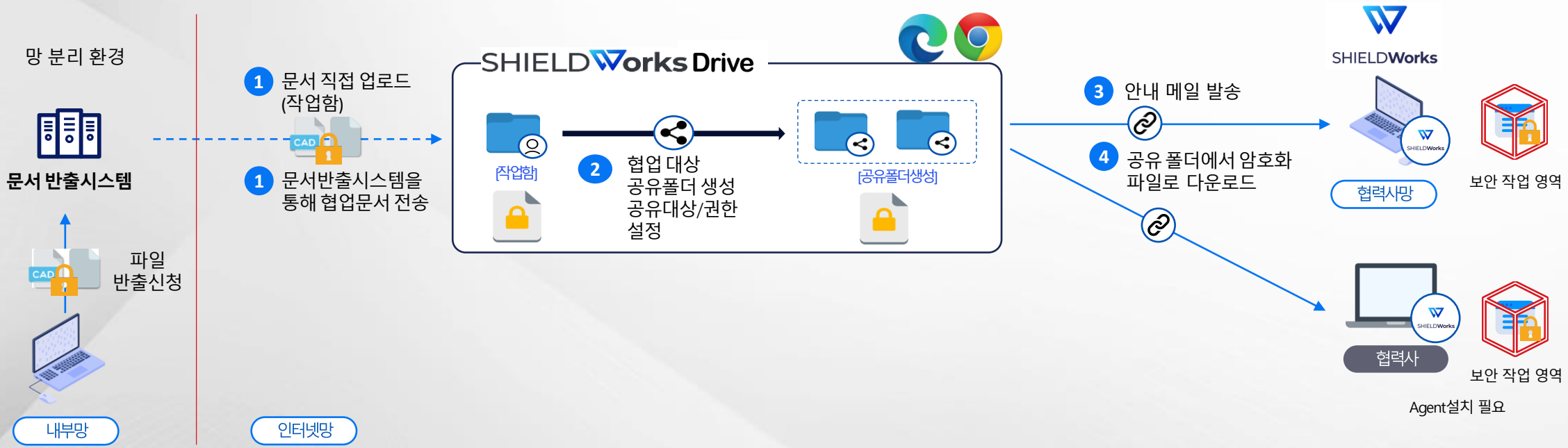
› 블록체인을 활용한 원본증명으로 공인인증서 사용으로 인해 발생하는 다양한 이슈 방지



3. 사외 사용자 협업에 대한 오케스트레이션

› **협력업체와 암호화된 문서로 공유** 되어야 하고 협력업체 **외부로 반출이 불가능**(격리된 보안 영역에서 문서 사용)

› 망 분리 환경에서도 협력업체와 문서 공유가 가능



특징

- **안전한 전달**(web 다운로드 + 암호화 유지), **유출방지**(보안 영역 작업), **회수** 또는 삭제(일정 기간 경과 시)
- 망 분리 환경의 경우 내부망 문서 반출 시스템을 통하여 협력업체까지 공유 가능
- 협력업체는 Agent 설치 후 다운로드 파일 실행하여 보안영역에서 문서 열람 및 편집
- Windows 탐색기에서도 문서 관리 가능(단 보안 영역 외부로는 이동 불가)

4. Zero Trust Architecture Model 적용

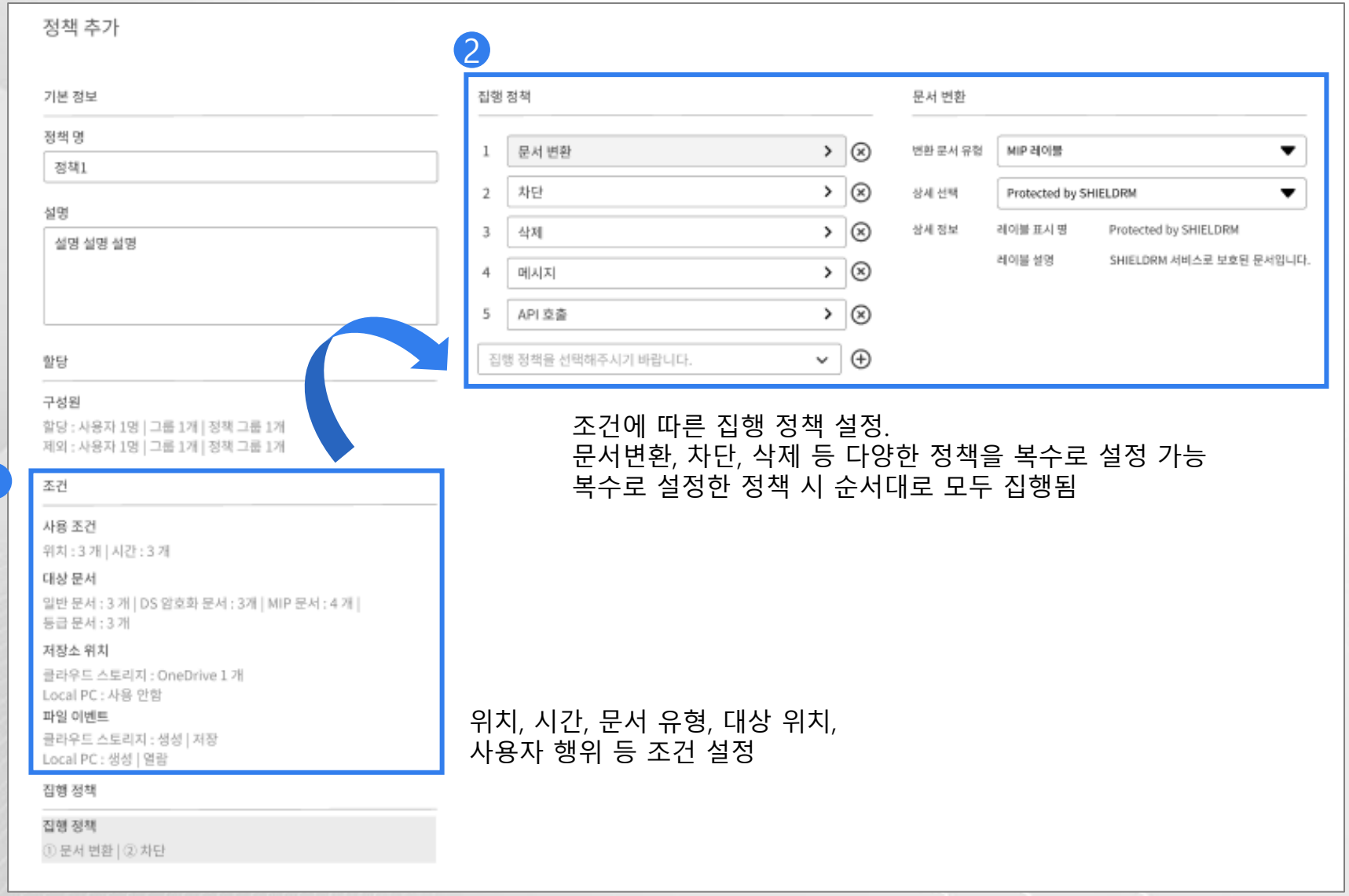
› 제품과 서비스는 Zero-Trust Conditional Adaptive Policy(ZTCAP)로 관리 됩니다.
기업 및 조직의 모든 시스템 보안을 강화할 수 있는 최신 보안 모델 입니다.

특징

- **Zero-Trust**(제로 트러스트) : 모든 사용자, 장치, 애플리케이션, 데이터에 대한 미 신뢰 원칙을 기반
- **Conditional**(조건부) : 접근 권한은 다양한 조건(사용자, 기기, 위치, 시간 등)에 의해 설정
- **Adaptive**(적응형) : Zero-Trust 정책은 실시간으로 조정되며, 사용자 또는 기기의 상태에 따라 **권한을 동적으로 변경**
- ZTCAP의 주요 목표 : **위험 감지 및 완화**, **적응성**, **인증 및 권한관리**, **보안 이벤트 모니터링**

4. Zero Trust Architecture Model 적용 – 화면 예제

› 관리자 페이지를 통해 ZTCAP 정책을 문서 종류, 사용자, 사용자의 행위, 대상 스토리지, 암호화 방식 등에 따라 유연하고 확장성 높은 보안 정책을 설정 할 수 있습니다.

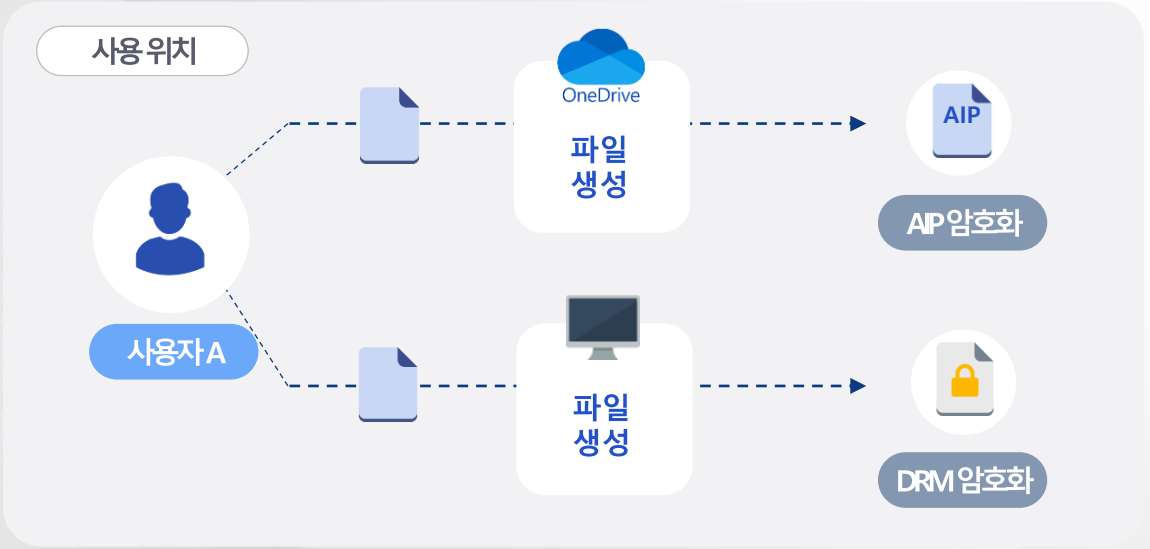


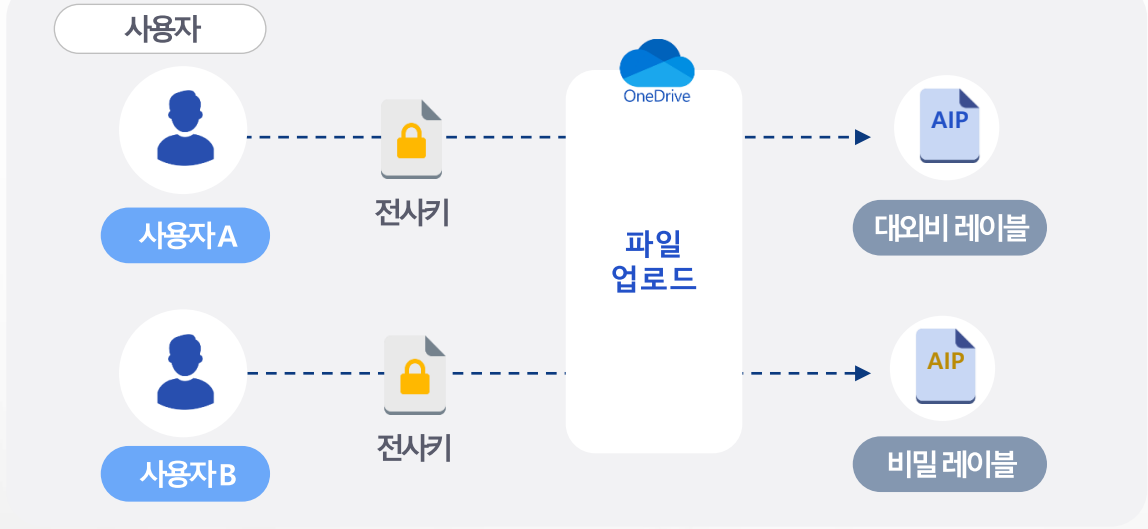
조건에 따른 집행 정책 설정.
문서변환, 차단, 삭제 등 다양한 정책을 복수로 설정 가능
복수로 설정한 정책 시 순서대로 모두 집행됨

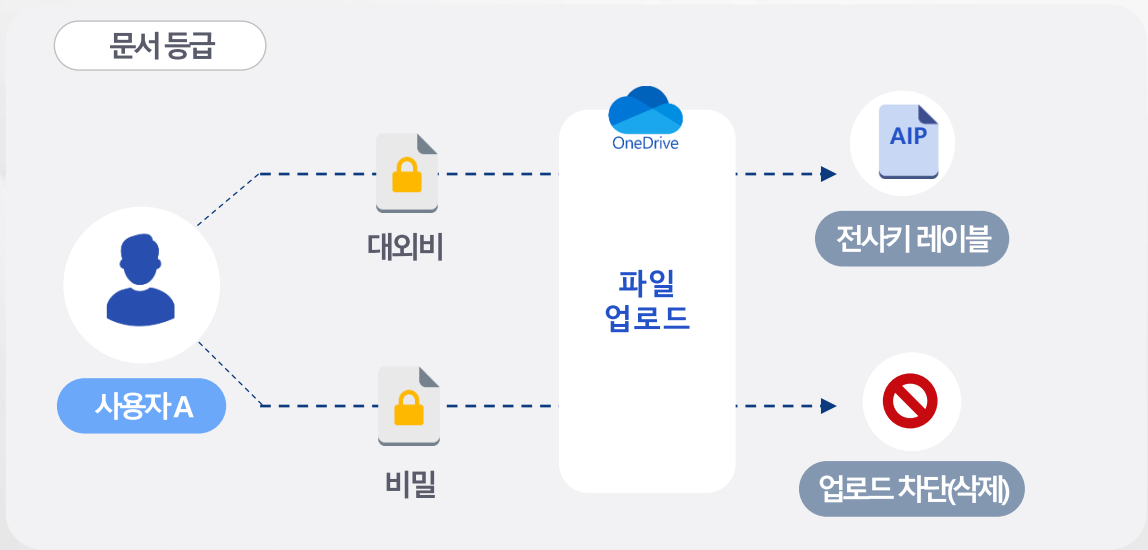
위치, 시간, 문서 유형, 대상 위치,
사용자 행위 등 조건 설정

4. Zero Trust Architecture Model 적용 – 적용 예시

› 정책을 통해 사용 위치, 사용자/그룹, 문서유형, 문서 등급에 대해서 사용자의 행위, 대상 스토리지, 암호화 방식에 따라 유연하고 확장성 높은 보안 정책을 설정 할 수 있습니다.







5. 외부에서 유입되는 문서에 대한 안전한 컨텐츠 반입 - CDR기술

문서 파일내의 **잠재적 위협요소를 제거**(Disarm)후,
비주얼 컨텐츠만 추출하여 **문서를 재조합**(Reconstruction)하는 기술

CDR(Contents Disarm & Reconstruction)

Format Verification

1

포맷확인

- 본문구조확인
- 헤더구조검사

Structure Analysis

2

구조분석

- 문단,도형,그림,표 등 모든 문서구성요소들의 구조 검증

Component Extraction

3

추출 및 검증

- 비주얼 구성요소 추출
- 올바른 구성요소인지 검증

Reconstruction Verification

4

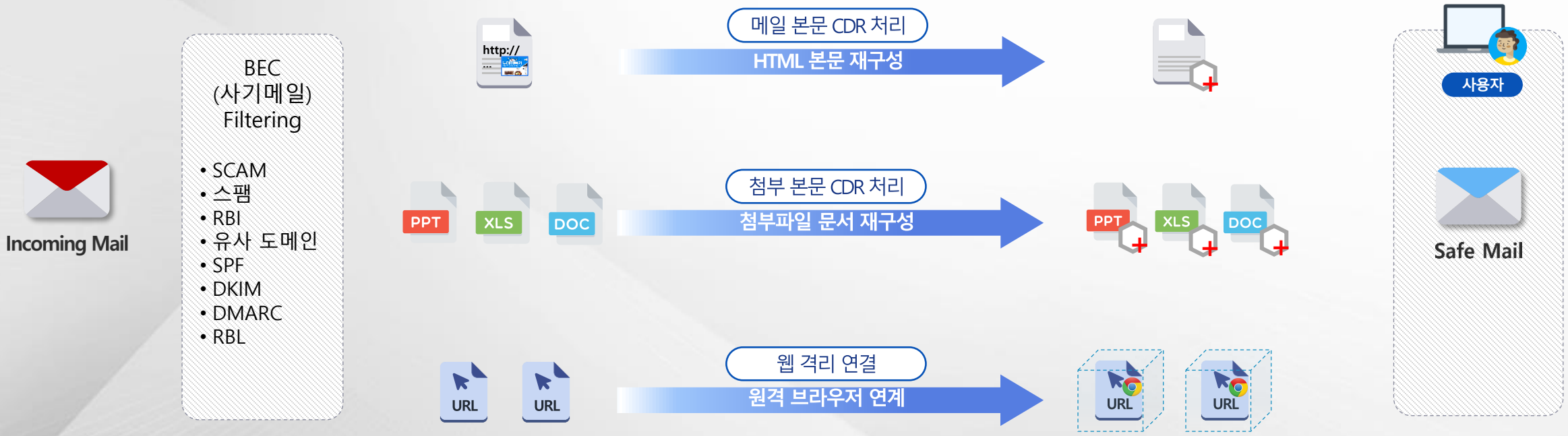
문서 재구성

- 추출된 구성요소로 문서를 재구성 함

5. 외부에서 유입되는 문서에 대한 안전한 컨텐츠 반입 - 이메일 격리

수신 이메일 격리 시스템

수신 이메일의 본문, 첨부파일, URL링크의 위협요소를 필터링하여 재구성 및 격리



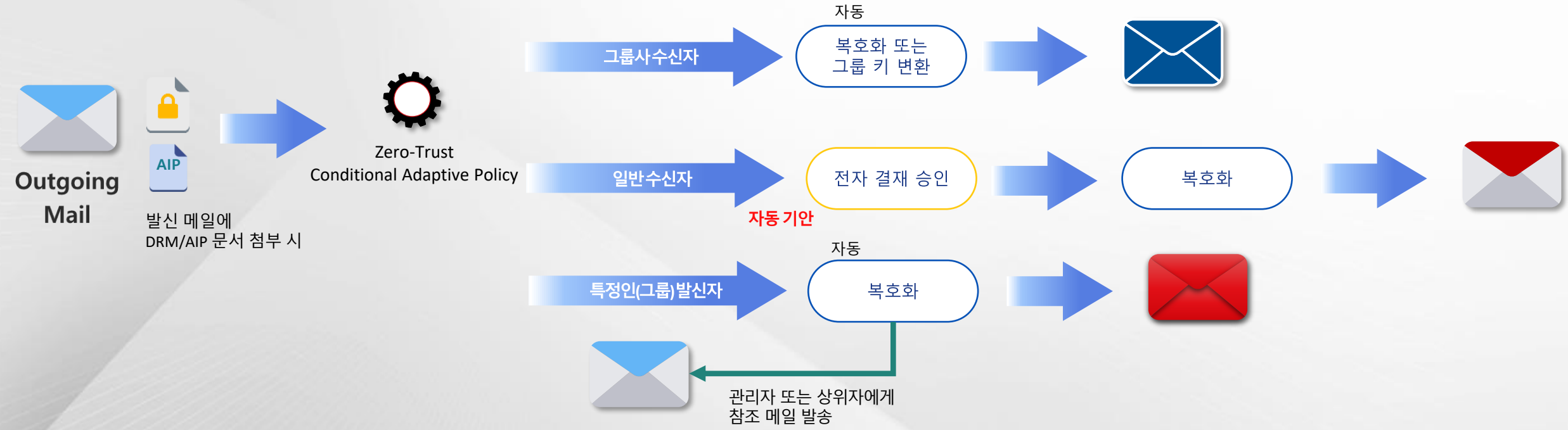
서비스 특징

- 이메일 **본문**에 포함된 Content의 **무해화** 처리(HTML 방식의 Body에서 스크립트 등 제거)
- 첨부 파일 무해화, **URL Link는 Remote Brower를 통하여 접속**(PC로 부터 격리하여 클라우드에서 접속)
- 본문에 포함된 이미지 표출용 URL 또는 미디어 파일에 대한 무해화 처리(스테가노그래피 방어)
- On-premise 메일서버 및 Gmail, Microsoft Exchange 클라우드 메일 서비스 연동 지원

6. 외부로 발송되는 메일에 대한 문서 오케스트레이션

발신 이메일 첨부 파일 처리 시스템

사외로 발송되는 첨부파일이 포함된 메일에 대하여 Zero-trust Conditional Adaptive Policy 적용



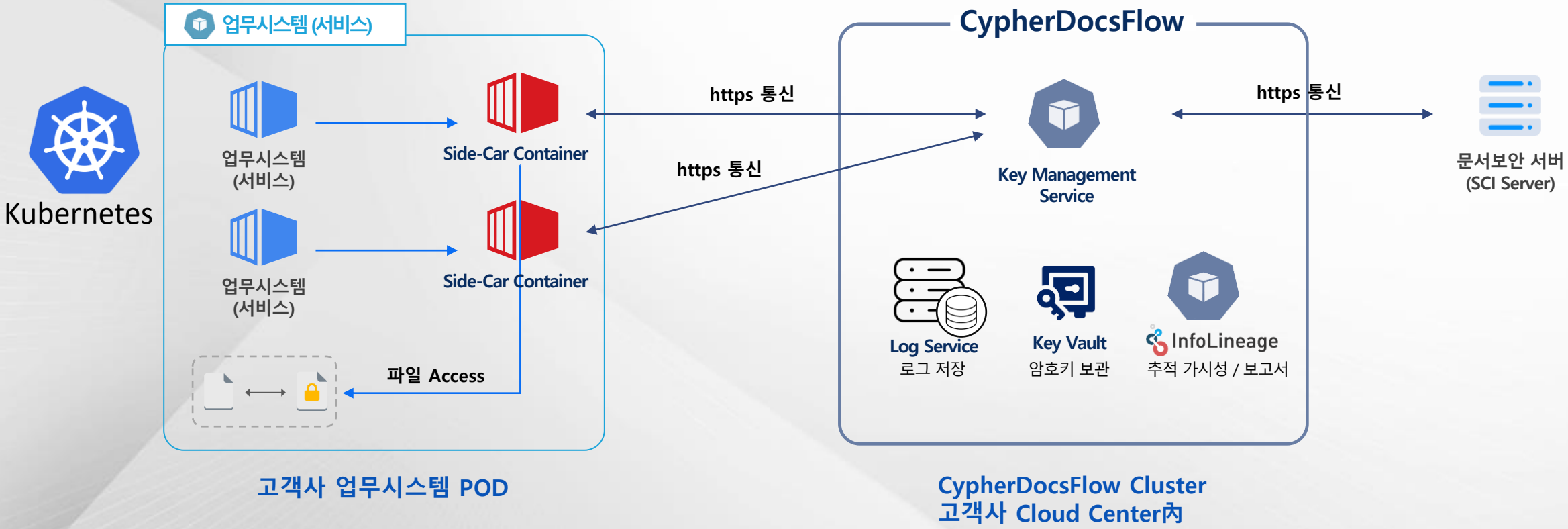
서비스 특징

- 사전에 **DRM 해제 결재 신청이 필요하지 않음**
- 발신자 PC에 암호 해제된 문서가 존재하지 않음
- **'보낸 편지함'에 암호해제 문서가 존재하지 않음**
- Exchange Connector를 통하여 라우팅함으로 기존 메일 환경에 영향 없음(ex2016이상, On-premise/Exchange Online 모두 지원)

7. 클라우드 네이티브 어플리케이션 통합 문서 보안 관리

› 업무 시스템이 클라우드(Kubernetes)로 이전 되었을 때 **클라우드 환경의 문서 파일을 보호하는 서비스** 입니다.
클라우드에서 유통되는 문서 파일에 암호화 적용하고, Local PC DRM과 호환성을 제공합니다.

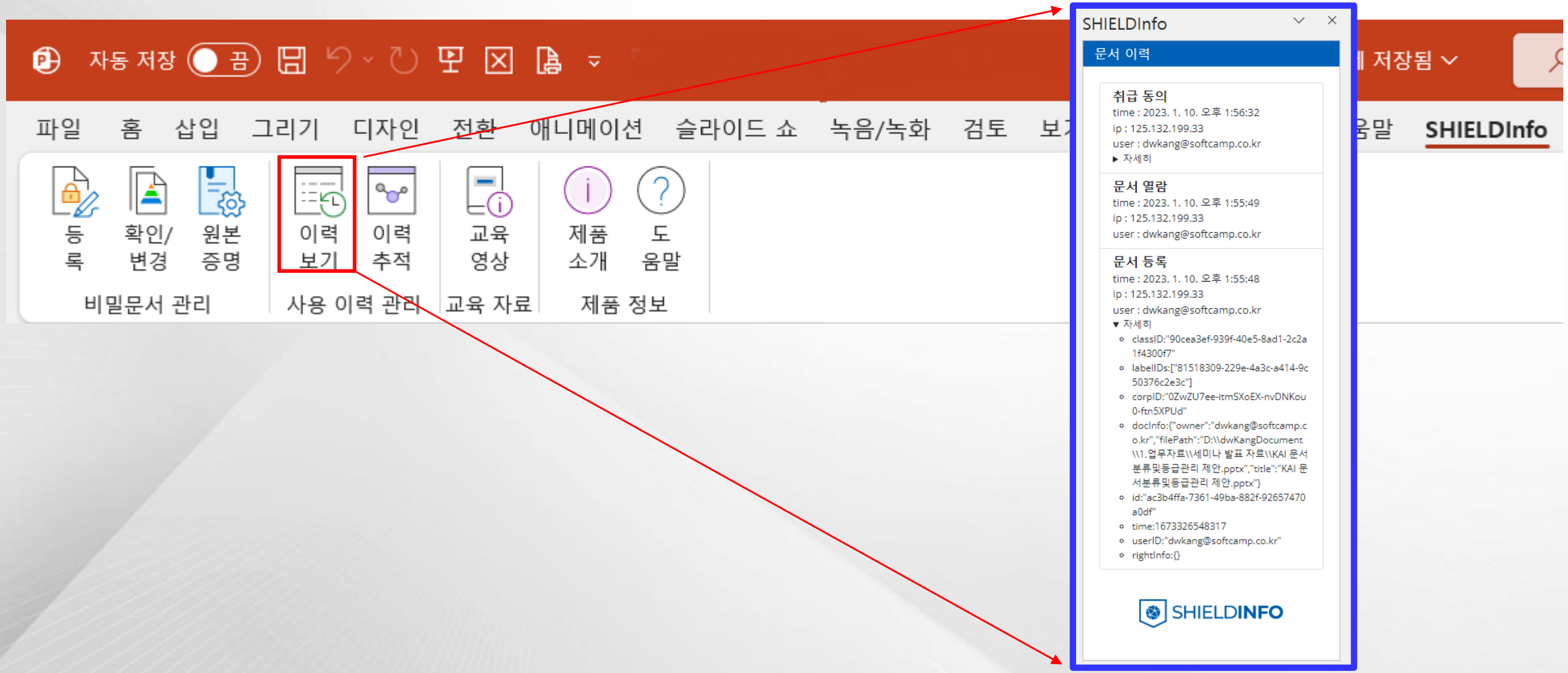
7. 클라우드 네이티브 어플리케이션 통합 문서 보안 관리



서비스 특징

- 고객사 업무시스템 POD 내 Container 구성(Side-Car Container)
  * Side-Car Container는 업무시스템의 파일에 대한 접근이 가능해야 함
- CypherDocsFlow는 별도 Kubernetes Cluster 구성
  * CypherDocsFlow에 연동된 업무시스템 정보 신규(또는 추가) 등록/관리
- 업무시스템 POD과 CypherDocsFlow 간, CypherDocsFlow와 문서보안 간 https 통신

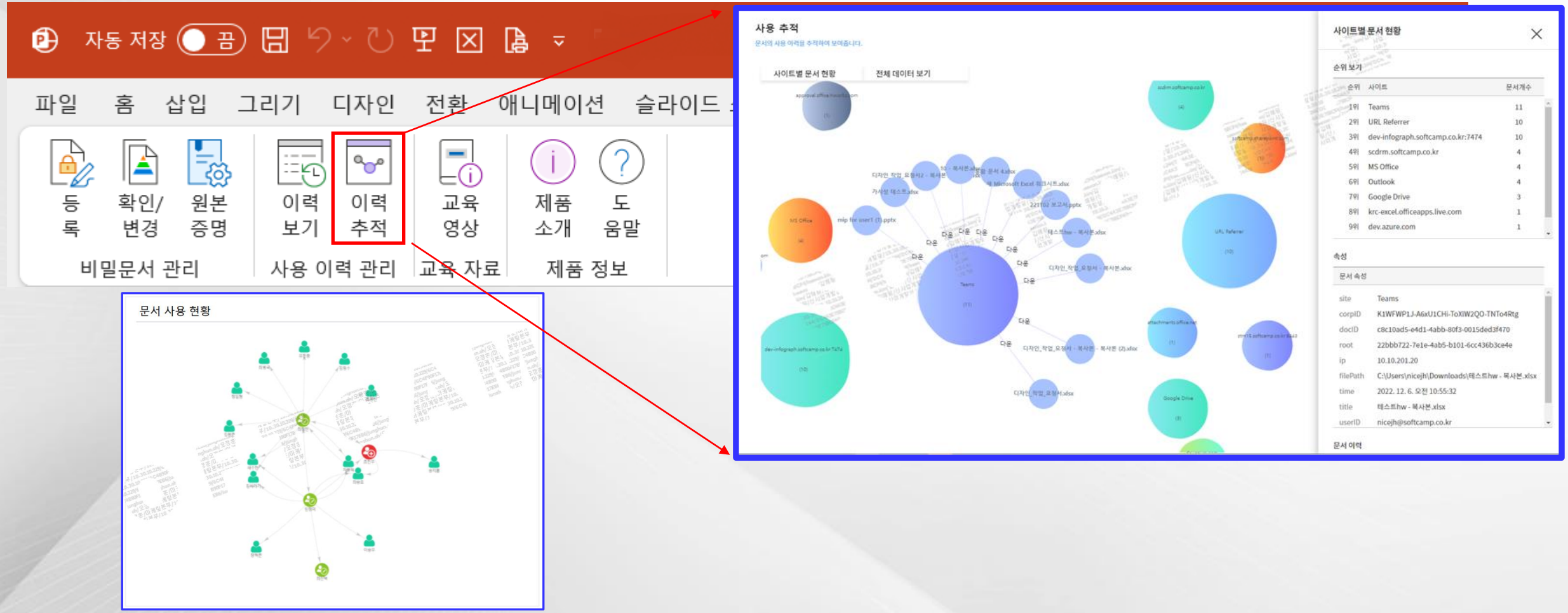
8. 문서의 유통 가시성 확보



특징

- 등록 / 열람 / 동의 / 인쇄 / 편집 등 문서 이력 조회 기능
- 작성자 및 중간 편집자, 동의자 등 표시

8. 문서의 유통 가시성 확보



특징

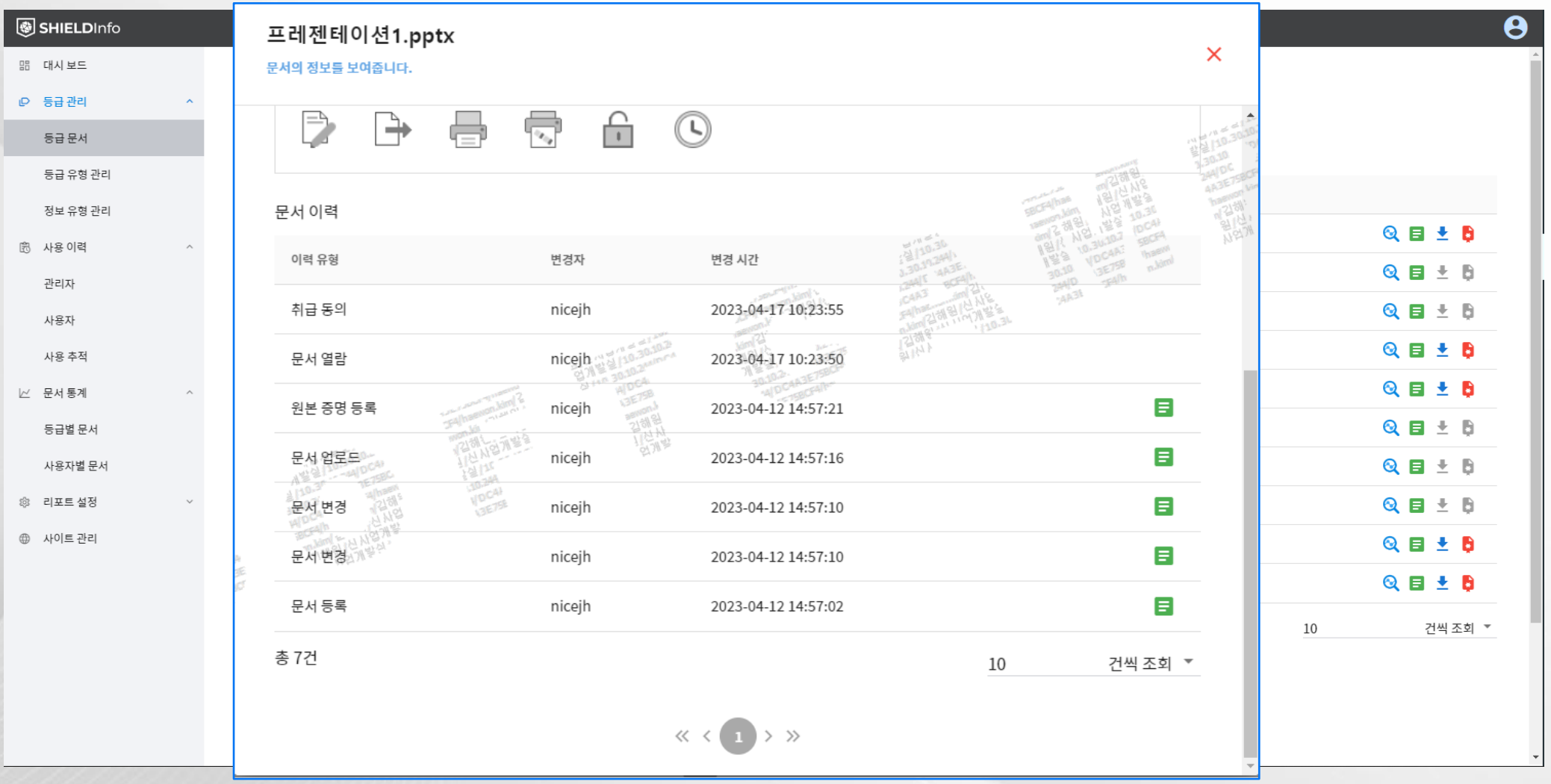
- 문서 유통 경로 , 이력 조회 기능
- 문서의 속성, 흐름 표시, 문서 추적

8. 문서의 유통 가시성 확보

특징

- 문서 접속 이력 보고 기능
- 각 개개인에게 문서 접속 이력 메일로 리포팅

8. 문서의 유통 가시성 확보



특징

- 관리자의 이력 조회, 통계 리포터
- 문서에 대한 상세 이력 조회, 원본보기 등

Zero Trust Security
업무환경 구현

기존 인터넷 사용 / 사외 근무 환경의 보안 한계

내부에서 인터넷 사용시 보안의 한계

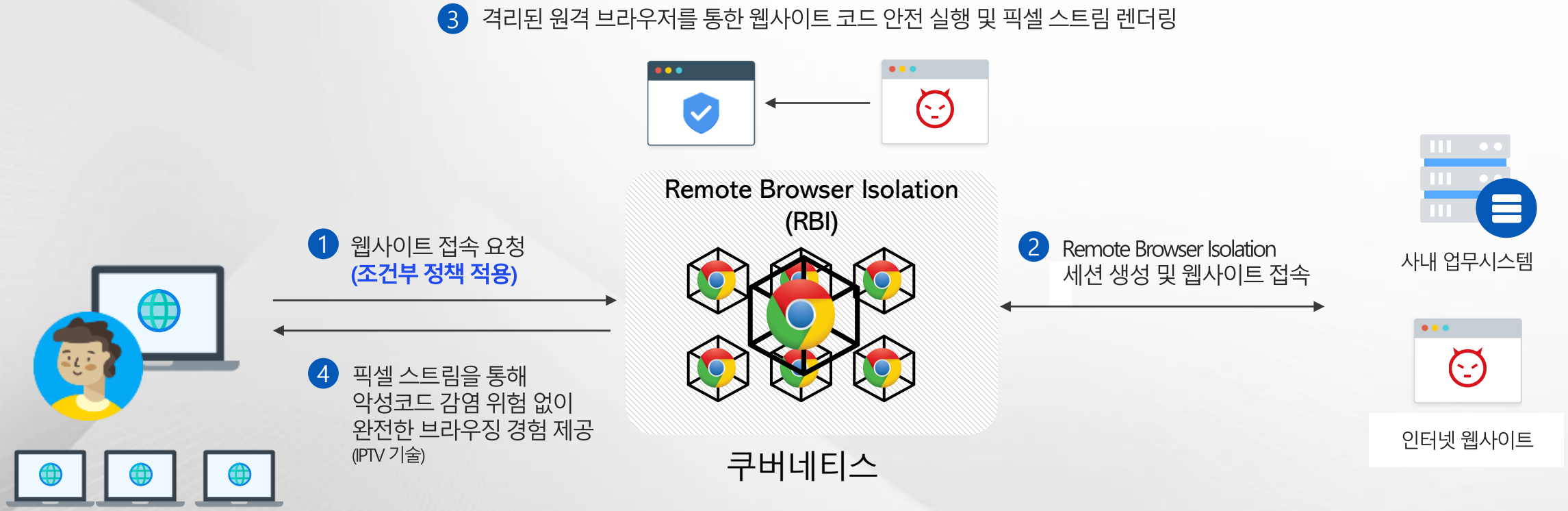
- 유해 사이트 차단용 웹 필터의 한계(신규 URL 에 대한 구분 어려움)
- Client PC에 백신, EDR, XDR 등을 설치해도 랜섬웨어 방어가 어렵다.
- 외부 수신 메일에 대한 BEC 방어가 어렵다.(바로가기, 첨부파일)
- 인터넷을 통한 문서 또는 중요 정보 유출 차단이 어렵다.
- 인터넷 사용 내역을 모니터링 하기 어렵다.

사외에서 사내 업무 시스템 접속 보안 한계

- **VPN을 이용한 네트워크에 한계**
  - VPN은 선 연결 후 인증 방식으로 보안이 취약하다
  - VPN으로 내부에 접속되면 내부 네트워크에 보안 홀이 발생할 수 있다
  - VPN을 접속하는 장비(PC)의 보안솔루션을 별도 관리해야 한다
- Zero-Trust Conditional Adaptive Policy 정책 적용이 불가능 하다.
- 업무 시스템을 내부 네트워크에서 접속용과 외부 네트워크에서 접속용을 각각 관리해야 한다.
- 모바일 Version을 따로 구축해야 한다.
  - 모바일 종류에 따라 별도의 Version관리를 해야 한다
  - 신규 모바일 OS가 출시 될 때 마다 Upgrade해야 한다
- 고가의 VDI를 도입해야 한다.

Remote Browser 소개

› 원격 브라우저 격리(RBI)는 서버에 가상 브라우저로 인터넷을 접속하고,
사용자 브라우저에서는 **접속한 화면을 픽셀 스트림으로 전송 받는 기술**입니다.



서비스 강점

- 접속하는 사용자의 PC에서 접속한 인터넷 컨텐츠의 (악성코드가 포함된) 어떤 스크립트도 End Point(접속한 PC)에서 실행되지 않음
- 알려지지 않은 인터넷 사이트를 통해 다운로드 받은 파일도 사내 PC에서 안전하게 사용 가능

Zero Trust Security 업무 환경 구현 방안- 내부에서 인터넷 사용

› SHIELDGate / SHIELDEX Remote Browser는 Zero-Trust 보안 기술이 적용된 인터넷 접속 보안 서비스입니다.
인터넷 접속 시 ZTCAP에 따라 정책을 집행하고, RBI를 통해 접속하여 위협을 원천적으로 차단합니다.

SHIELDGate

SHIELDEX Remote Browser

서비스 설명

Zero-Trust 보안 모델을 적용하여
사용자가 접속한 사이트의 컨텐츠를 어떠한 위협도 없이
안전하게 사용 할 수 있는 인터넷 접속 보안 서비스

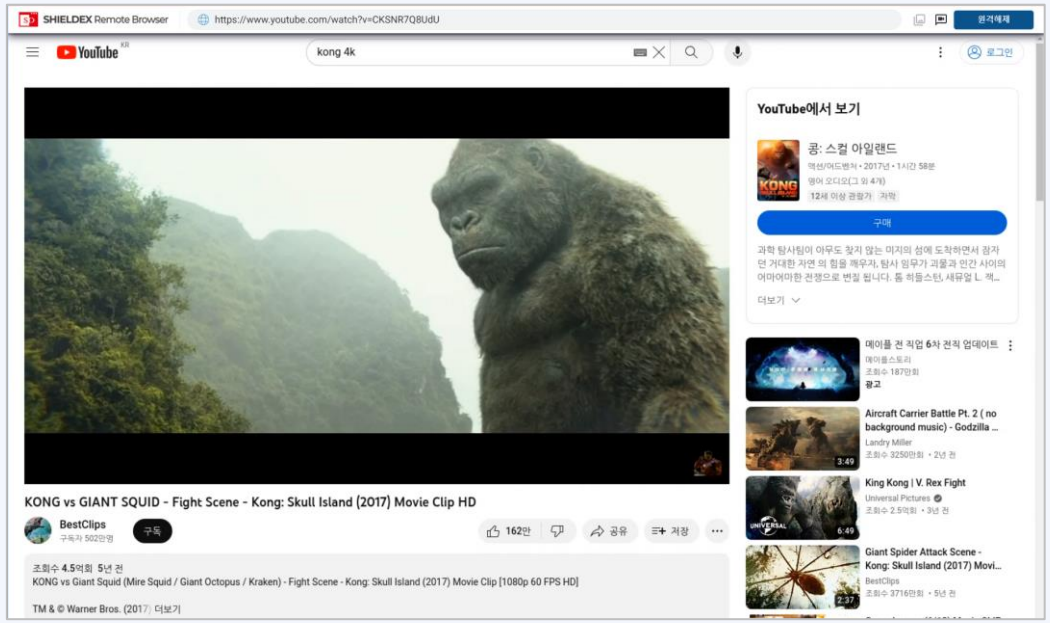
서비스 특장점

- 서비스의 접속(사용) 환경에 따른 정책 집행
  - **ZTCAP, Zero-Trust Conditional Adaptive Policy**
- 사이트의 어떤 스크립트도 엔드 포인트에서 실행하지 않음
  - **Remote Browser Isolation**
- 접속한 사이트에서 다운로드 받은 파일은 무해화 처리
  - **CDR, Contents Disarm & Reconstruction**
- 가시성 높은 통계 Reporting 제공

Zero Trust Security 업무 환경 구현 방안- 내부에서 인터넷 사용

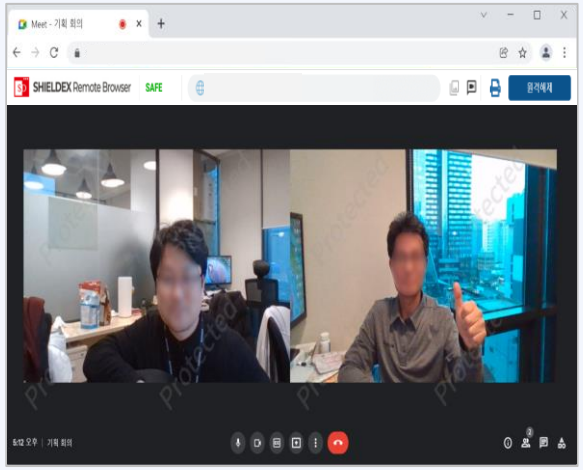
› 지금까지 인터넷을 사용했던 사용자 경험을 그대로 제공합니다.
사용자는 이전과 같이 인터넷을 이용하지만 100% 격리된 안전한 화면만을 보게 됩니다.

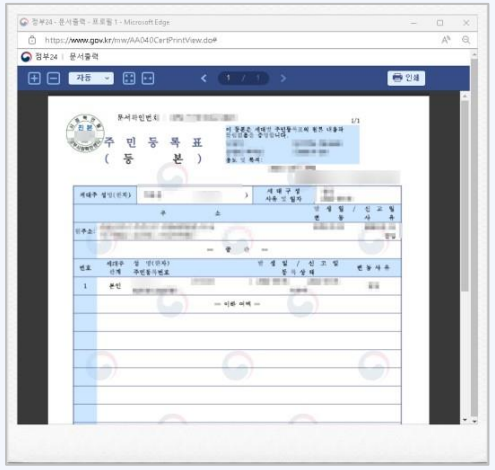
4K 영상도 재생 가능한 최상의 사용자 경험 제공



- DRM 영상 재생 가능
- 인터넷 온라인 교육 완벽 지원

화상 회의 / 전자민원발급 지원

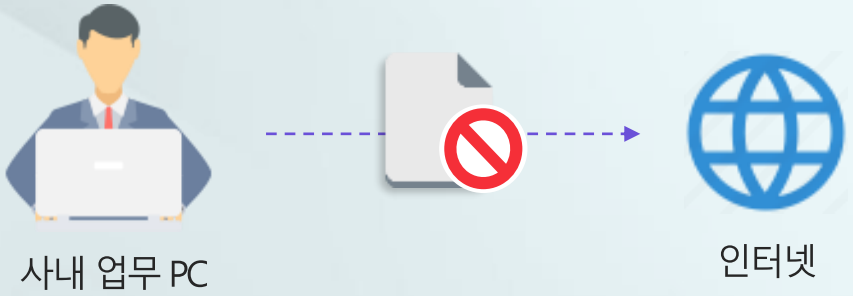




- SaaS 화상 회의 지원 (카메라/마이크 터널링 연결)
- 전자민원서류 발급 지원 (간편 인증)

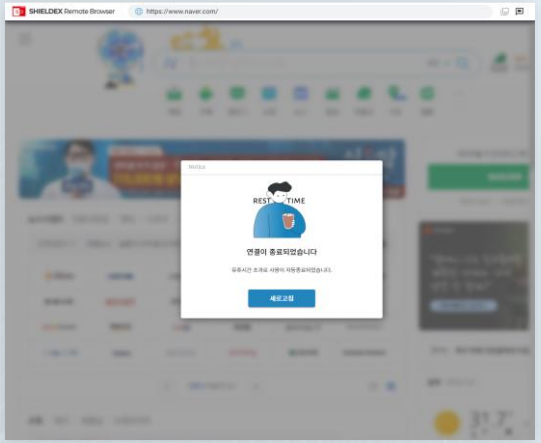
Zero Trust Security 업무 환경 구현 방안- 내부에서 인터넷 사용

› 가상 브라우저를 직접적으로 제어할 수 있으므로, **기존에 구현하지 못했던 각종 보안 기능을 실현**합니다

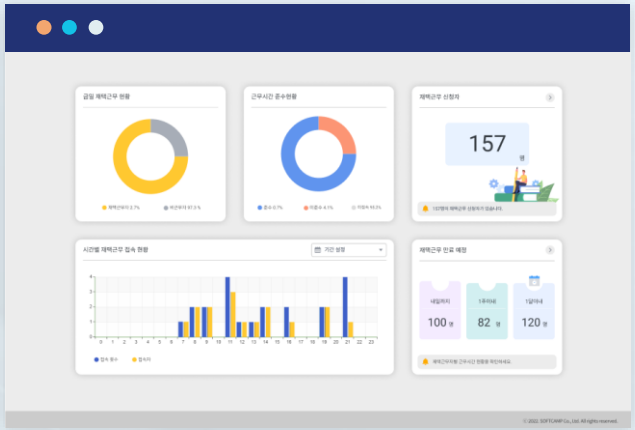


자료 무단 반출 통제

민감 정보 입력 통제



유휴시간 경과시 화면 잠금



인터넷 사용 이력

Zero Trust Security 업무 환경 구현 방안- 내부에서 인터넷 사용

› 조건에 따른 다양한 사용 정책 부여(Zero-Trust Conditional Adaptive Policy)

› ZTCAP 정책에 따라, 사용자의 환경 및 접속 대상 인터넷 컨텐츠를 모두 검사하고 정책을 집행합니다.

조건 판단

- 접속 사용자
- 접속 시간
- 접속 URL, 사이트 분류
- 파일 첨부
- 파일 다운로드
- 양식에 정보 전송

Policy Decision Point

Policy Engine

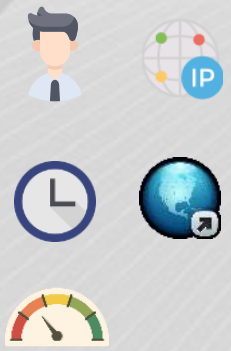
Policy Administrator

정책 판단 및 부여

집행 정책 목록

- 접속 허용/차단
- 키보드 입력 허용/차단
- 파일 첨부 차단
- 다운로드 파일 CDR 처리
- 다운로드 파일 웹디스크 저장
- 양식 입력정보 감사/통제

Subject



System

Policy Enforcement Point

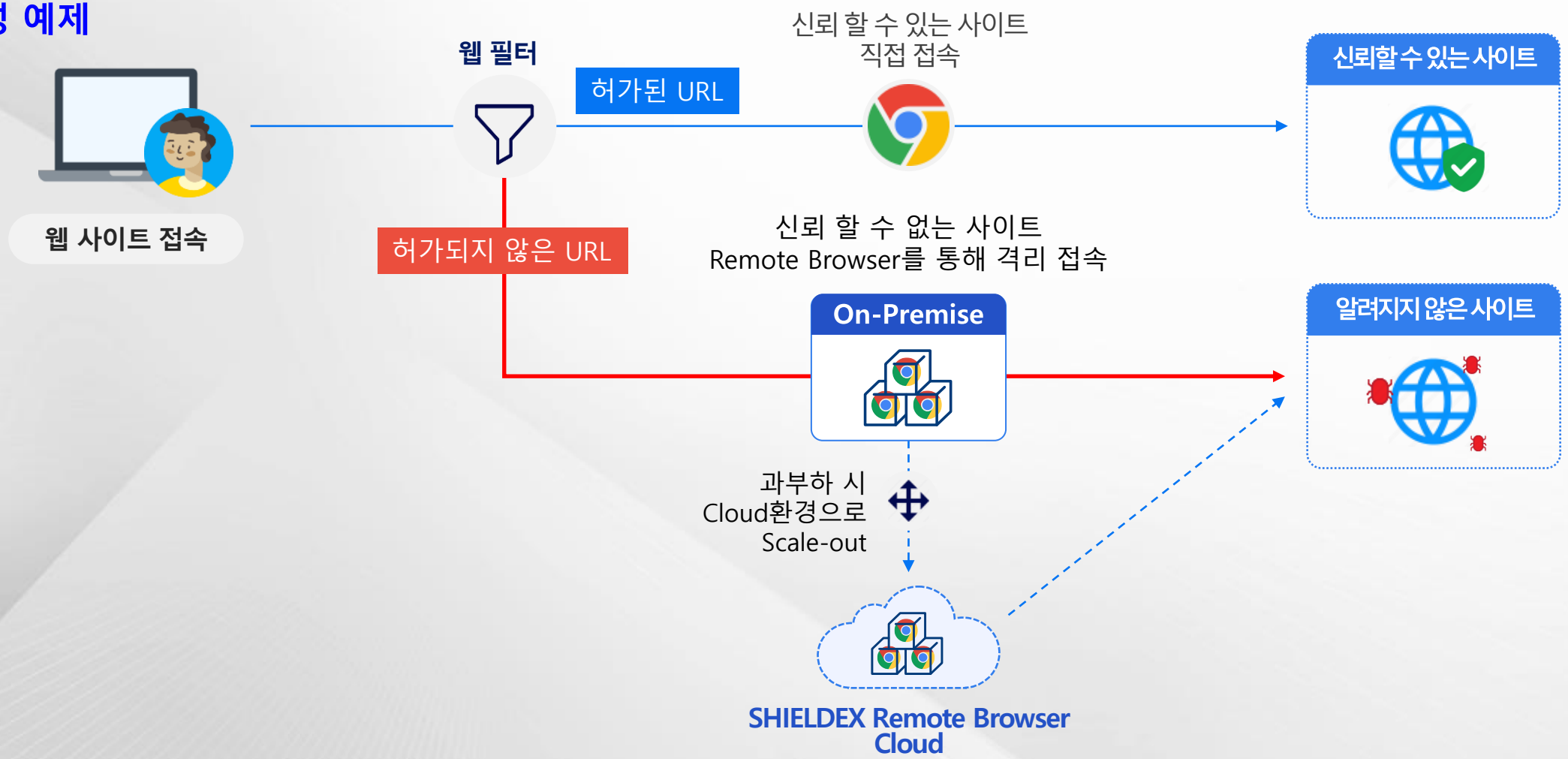
SHIELDEX Remote Browser

접속 허용/차단
및 정책 집행

Internet

Zero Trust Security 업무 환경 구현 방안- 내부에서 인터넷 사용

구성 예제

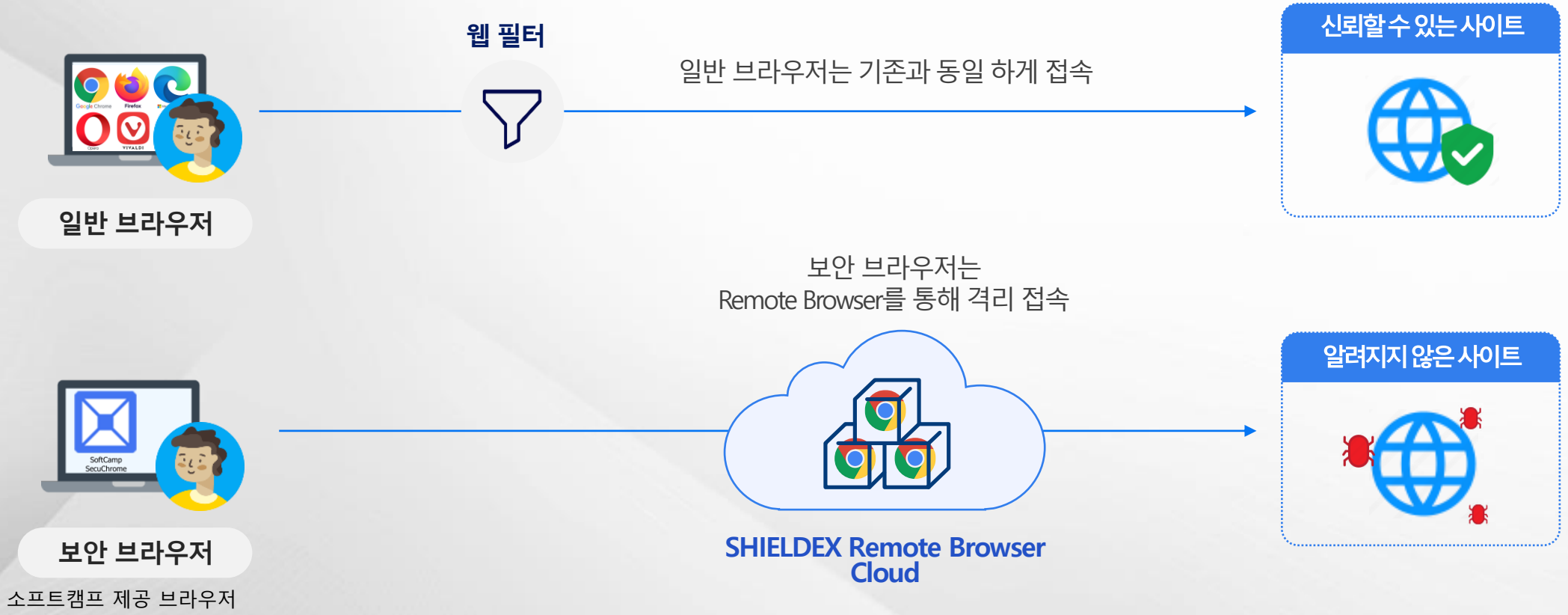


서비스 강점

- 웹 필터를 통해 사용자가 접속하는 사이트의 신뢰 여부 판단
- 신뢰 할 수 없는 사이트(ex. 그레이 사이트)는 온프레미스 환경에 구성된 SHIELDEX Remote Browser를 통해 접속
- 온프레미스 구성 환경 과부하 시 클라우드 환경으로 Scale-out하여 격리 브라우저를 통해 신뢰할 수 없는 사이트 접속

Zero Trust Security 업무 환경 구현 방안- 내부에서 인터넷 사용

구성 예제

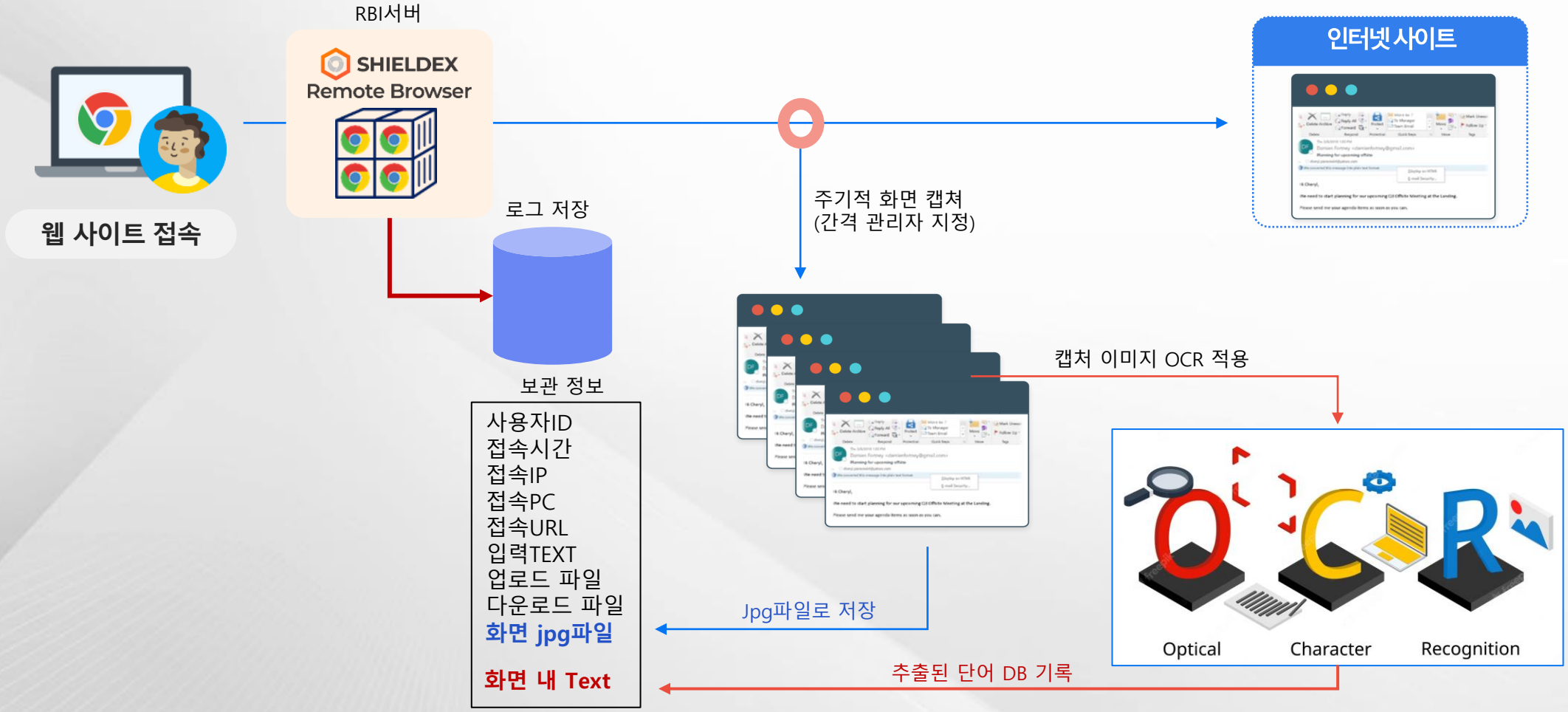


서비스 강점

- 일반 브라우저로 접속할 경우 기존과 동일 하게 접속(웹 필터로 유해사이트 차단)
- 보안 브라우저(Softcamp 제공)로 접속 할 경우 Remote Browser를 통하여 안전하게 접속
- Remote Browser 서버에서도 Blacklist, Whitelist 기반의 URL 통제가 가능 합니다.

Zero Trust Security 업무 환경 구현 방안- 내부에서 인터넷 사용

› 구성 예제 – 사용 이력 모니터링



서비스 강점

- SHIELDEX Remote Browser 서버는 인터넷 사용 기록을 모두 저장 보관(저장 기간 조정 가능)
- 접속PC IP, 대상 URL 등 정보를 저장 및 조회, 보고서 발행이 가능
- 접속 화면을 주기적으로 캡쳐 하여 이미지로 저장, 저장 이미지에서 OCR로 단어 추출하여 저장

Zero Trust Security 업무 환경 구현 방안- Remote Browser

타 제품과의 기능 비교

분리 방식	화면을 전송하는 방식 (가상 브라우저)	화면은 전송하는 방식 (가상 데스크톱)	실행 환경을 분리하는 방식	화면을 전송하는 방식 (원격 브라우저)
적용 기술	App 가상화	VDI	HTML 재구성	Remote Browser Isolation
표시 방법	분리 환경에서 브라우저에 내용을 화면 전송으로 표시	분리 환경에서 데스크탑에 표시 한 내용을 화면 전송으로 표시	스크립트를 원격에서 실행하고 렌 더링은 로컬 브라우저	컨테이너내의 브라우저 엔진이 렌 더링한 픽셀 스트리밍
브라우저	별도 프로그램	별도 프로그램	**기존 브라우저**	**기존 브라우저**
파일 다운로드	파일 교환 서버를 통해 다운로드	파일 교환 서버를 통해 다운로드 (※ 기본 서비스로 포함되지 않음)	직접 단말기에 다운로드 (미리 보기로 내용 확인 가능)	직접 단말기에 다운로드 (CDR 처리 가능) (미리보기로 내용 확인 가능)
분리도	**완전 분리 (화면 전송)**	**완전 분리 (화면 전송)**	부분 분리 (컨텐츠 렌더링은 로컬 브라우저)	**완전 분리 (화면 전송)**
클라이언트 소프트웨어	필요	필요	**불필요**	**불필요**
부팅(준비)속도/ 페이지이동 속 도	부팅 : 수분 소요 페이지 이동 : 즉시	부팅 : 수분 소요 페이지 이동 : 즉시	부팅 : 없음 페이지 이동 : 3-5초	부팅 : 없음 페이지 이동 : 즉시
Script차단	**완벽 차단**	**완벽 차단**	일부 차단	**완벽 차단**

Zero Trust Security 업무 환경 구현 방안- 내부에서 인터넷 사용

적용 사례 ; 웹 디스크 / 웹 편집기를 통한 기능 확장

- 웹디스크를 통하여 인터넷 가상 브라우저로 파일 업로드/ 다운로드 / 열람 / 편집
- 인터넷 파일을 자료 교환 체계를 통한 반입 최소화하며 업무 수행

- 인터넷 다운로드 파일의 웹디스크 자동 저장
- 웹편집기를 통한 열람/편집
- 링크를 통한 내부 유통(또는 망 간 전송)

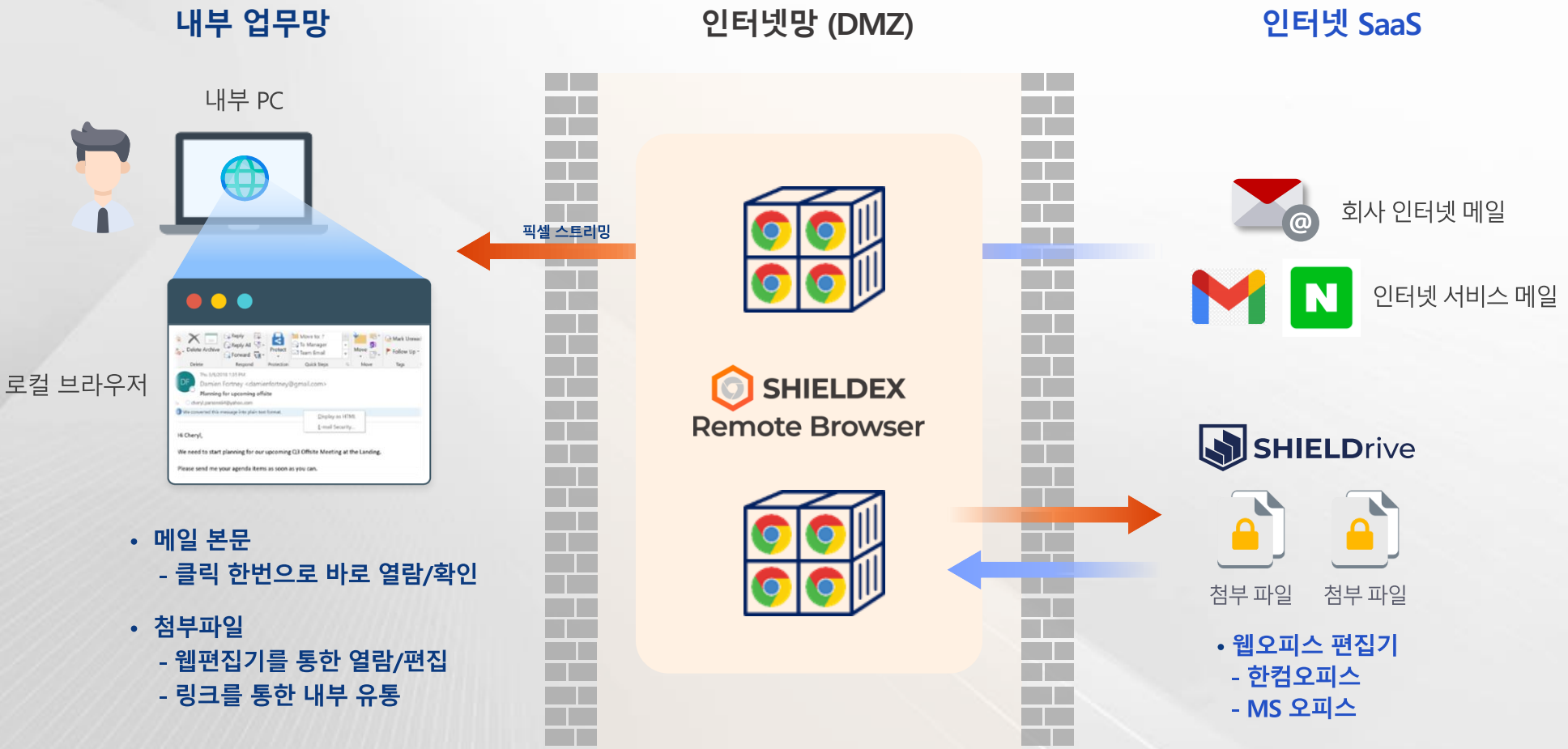
➔ **자료교환체계 반입 최소화**

- 파일 업로드 시 위치 지정 가능 (접속 PC 또는 지정 웹 디스크)
- 파일 다운로드 시 위치 기정 가능 (접속 PC 또는 지정 웹 디스크)
- 파일 다운로드 시 CDR 적용 가능 (무해화 처리 후 반입)

Zero Trust Security 업무 환경 구현 방안- 내부에서 인터넷 사용

적용 사례 ; 내부망에서 인터넷 메일 열람

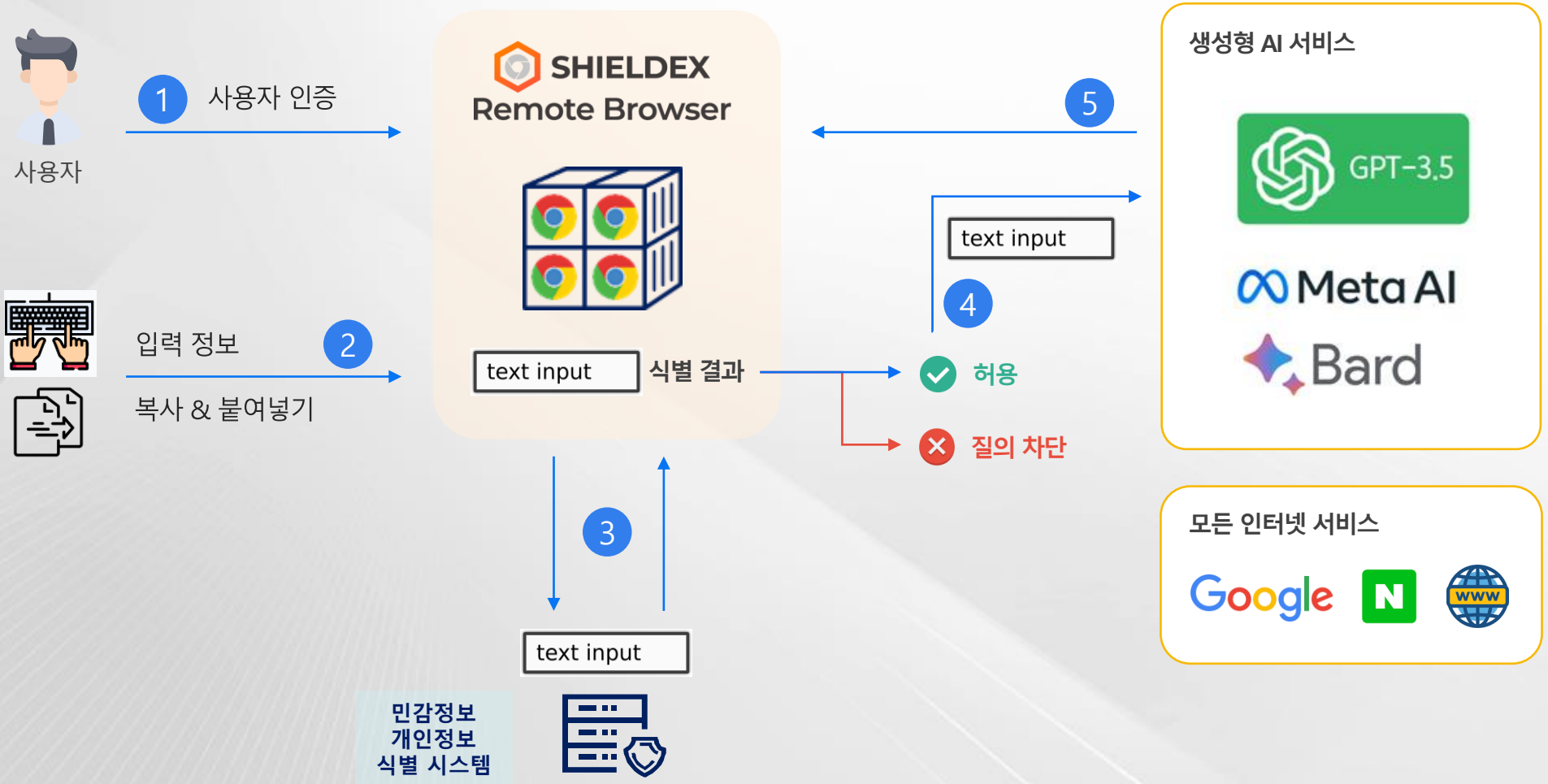
› 웹 격리 솔루션을 통해서 **웹 메일 및 업무를 위한 인터넷사이트를 허용**하여 편의성과 보안성 제공
(내부 업무망에서 인터넷 메일 열람 가능, 망연계 솔루션과 연계한 파일 반출입 승인처리)



Zero Trust Security 업무 환경 구현 방안- 내부에서 인터넷 사용

적용 사례 ; 내부망에서 생성형 AI 사용 시

› 생성형 AI 사용 시 질의어에 대하여 사전 검증 실시, 민감 정보, 개인정보 등 사전 검토 후 차단

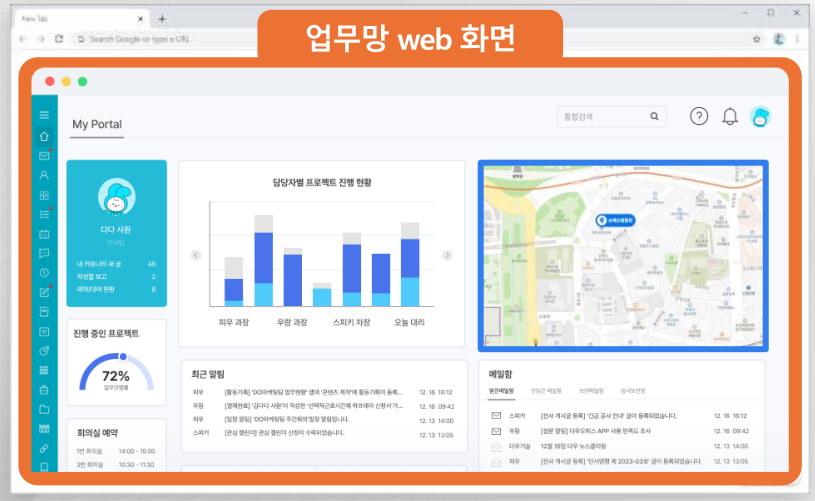


Zero Trust Security 업무 환경 구현 방안- 내부에서 인터넷 사용

적용 사례 ; 내부망 업무시스템에 인터넷 일부 컨텐츠 반영

› 내부 업무망의 업무시스템의 화면 일부분에 인터넷 컨텐츠를 결합하여 업무 효율성 향상 도모

내부 업무망

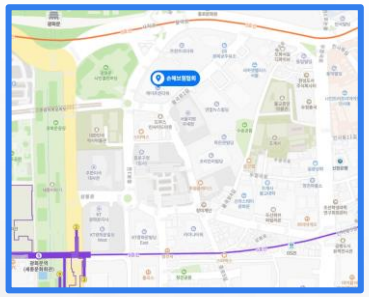


업무망 web시스템에 인터넷망 Content 연결
업무 시스템 주소 입력 시 지도 Focus 이동 및 확대
지도 클릭 시 업무시스템에 좌표 및 주소 등록

인터넷망 (DMZ)

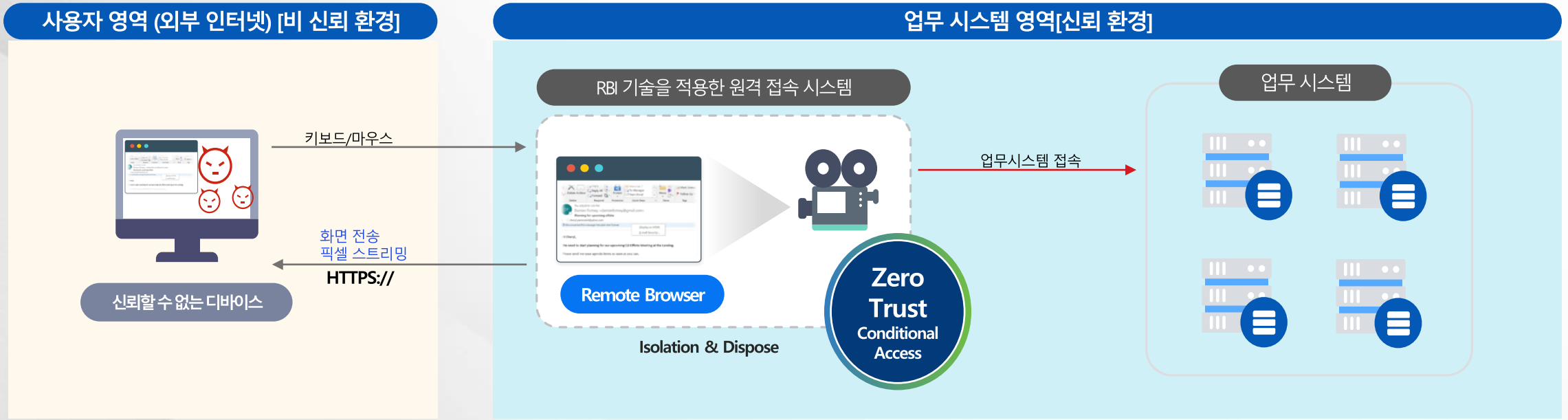
SHIELDEX
Remote Browser

인터넷 SaaS



지도 제공 웹사이트
(OOO 지도)

Zero Trust Security 업무 환경 구현 방안- 사외에서 내부 시스템 사용



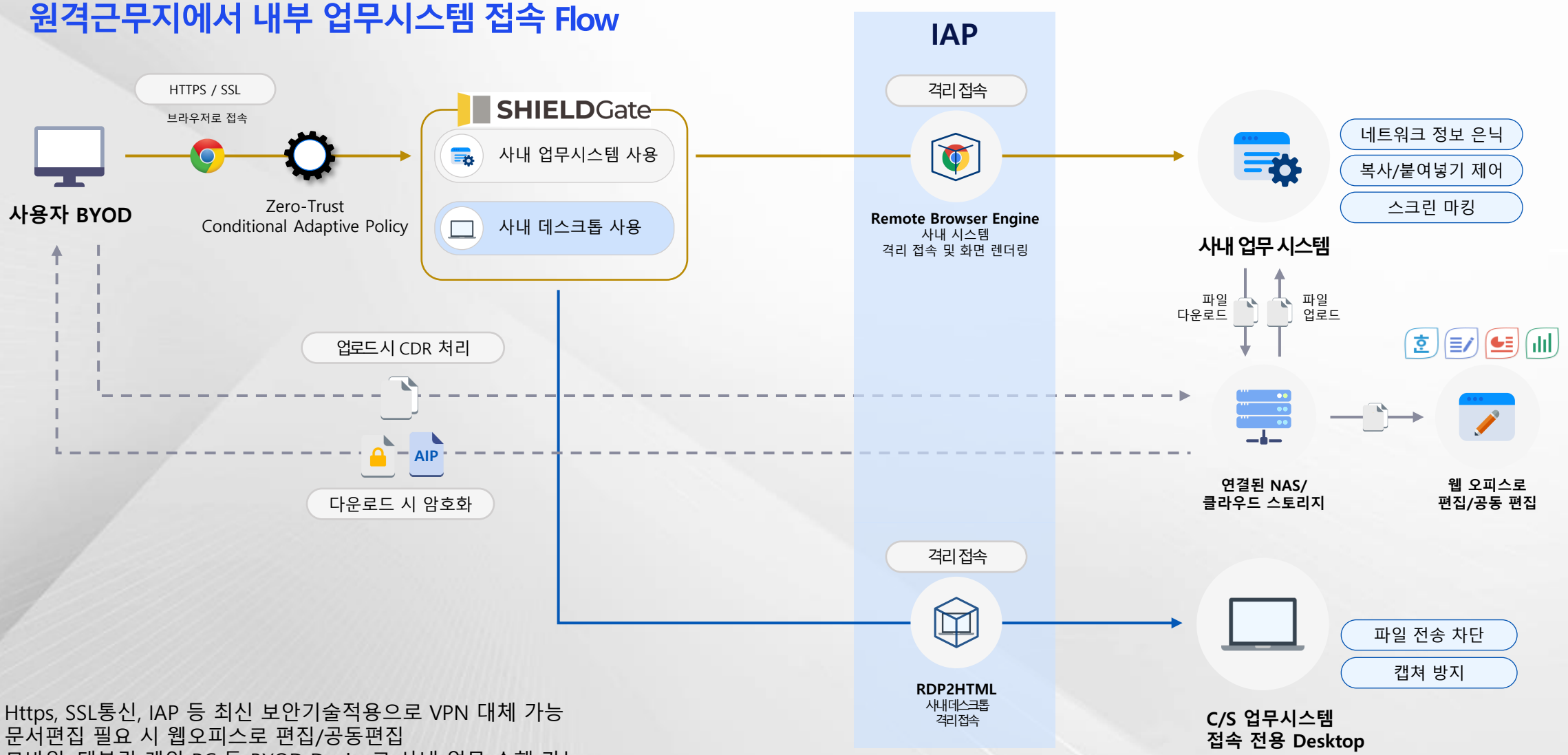
- 외부 접근 시 별도 프로그램 설치 불필요
  - 보안 프로그램 설치 불필요
  - 일반 브라우저로 사용(any device, mobile)
- 조건부 접근/사용 정책 적용
  - 추가인증 요구 (OTP, 생체 인식)
  - 패스워드 리셋 요구
  - 업로드/다운로드 차단
  - 스크린 마킹
- IP / Network 접속 정보 은닉
- 업로드/다운로드 파일 컨트롤
  - 업로드시 CDR
  - 다운로드시 암호화
  - 백신 검사
  - 개인정보 검사
- 기존 업무시스템의 수정 없음
- 웹 보안
  - 스크린 마킹
  - 캡처 방지
  - 임시 파일 삭제
  - 소스 보기 차단

최신 보안모델 적용

Remote Browser Isolation [RBI]	Zero-Trust Conditional Access [ZTCA]	Security Service Edge [SSE]
사용자 디바이스 대신 원격 서버에서 사용자의 웹 브라우징 세션을 호스팅하여 온라인 위협 무력화	사용자의 접속 환경에 따른 추가 인증 제공 & 사용권한 제어	업무 시스템의 액세스 제어, 위협 보호, 모니터링 등 통합 관리 기능

Zero Trust Security 업무 환경 구현 방안- 사외에서 내부 시스템 사용

원격근무지에서 내부 업무시스템 접속 Flow



- Https, SSL통신, IAP 등 최신 보안기술적용으로 VPN 대체 가능
- 문서편집 필요 시 웹오피스로 편집/공동편집
- 모바일, 태블릿 개인 PC 등 BYOD Device로 사내 업무 수행 가능

Zero Trust Security 업무 환경 구현 방안- 사외에서 내부 시스템 사용

프로그램 설치나 접속 흔적 없이 내부 시스템 액세스

접속 프로그램 설치 없이

브라우저로만 접속
(Any Device)

접속 정보 흔적 없이

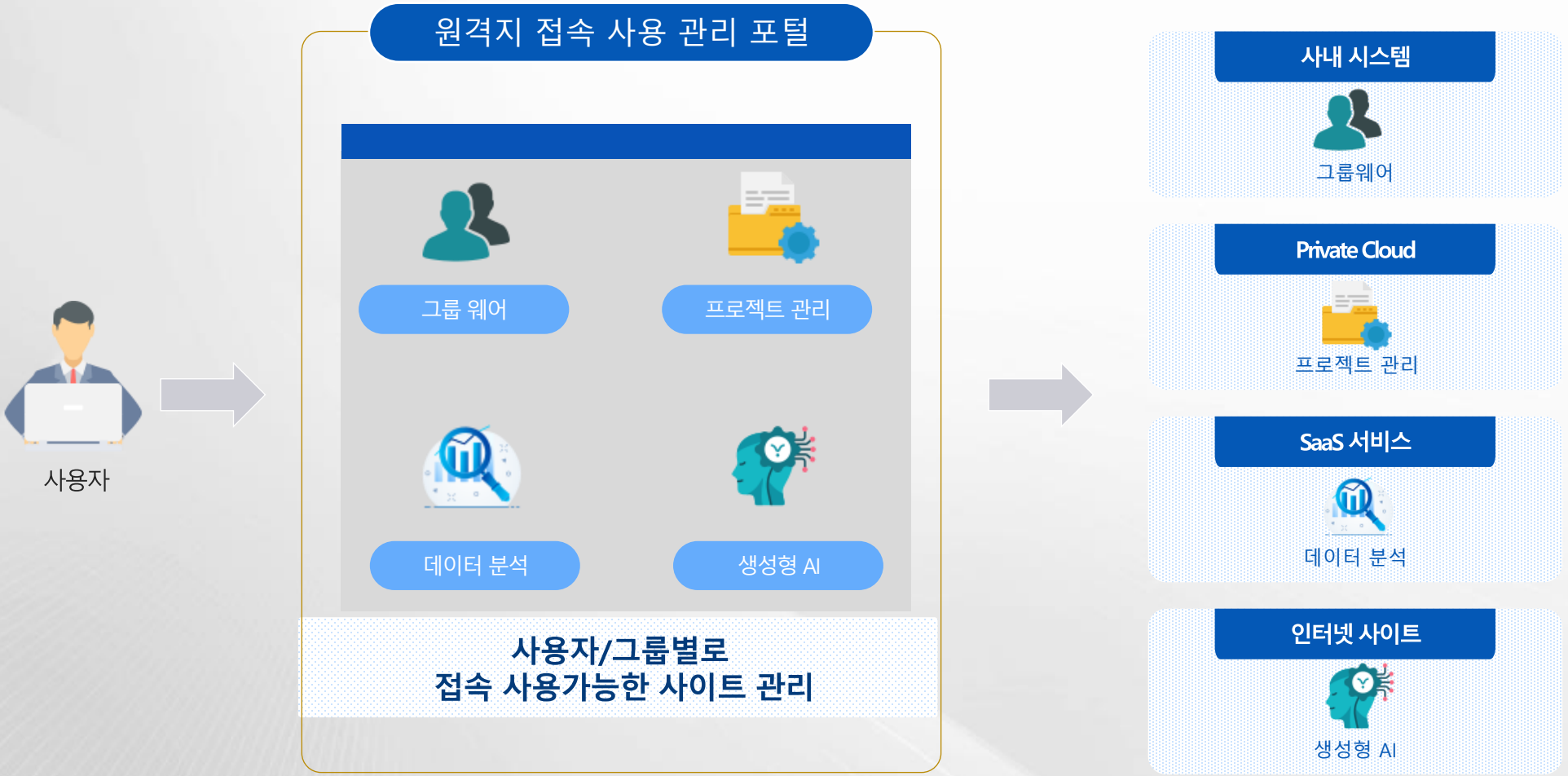
HTML 임시 파일 없음
쿠키 없음

파일 다운로드 없이

웹 편집기로 편집/저장/업로드

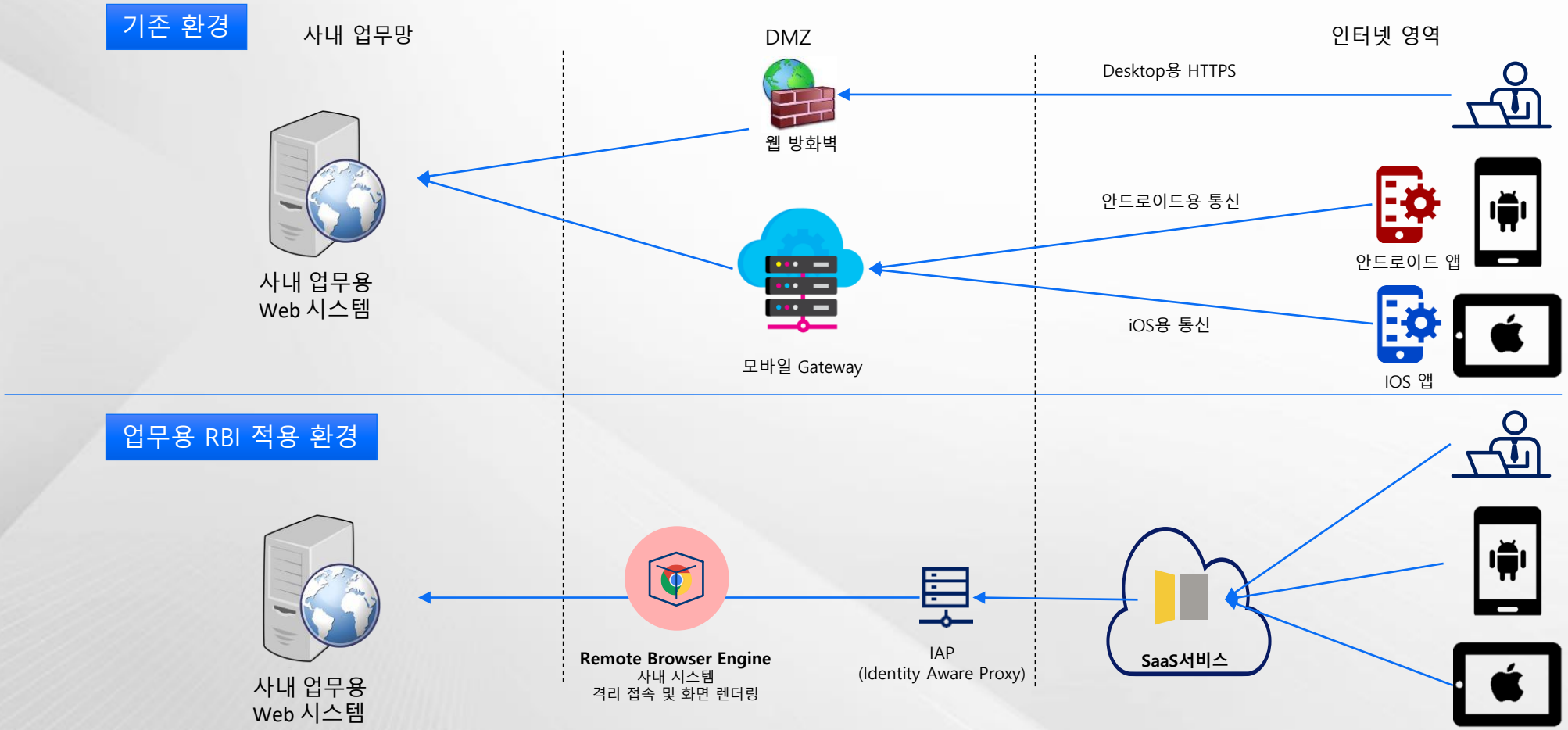
Zero Trust Security 업무 환경 구현 방안- 사외에서 내부 시스템 사용

원격근무지 업무용 Portal 화면 제공



Zero Trust Security 업무 환경 구현 방안- 사외에서 내부 시스템 사용

원기존 시스템 대비 구성 환경 예제



맺음말

› 소프트캠프 Security365 서비스는 다양한 환경으로 유통되는 데이터의 가시성 확보 및 거버넌스 제공을 목표로 합니다.

클라우드 협업 데이터 호환

Microsoft 365

Google Workspace

데이터 유통 호환성 확장

salesforce

Amazon S3

box

Dropbox

NAVER Cloud

kt cloud

Data Governance

On-Premise/Cloud 등
다양한 환경으로 유통되는
데이터 가시성 확보 및
거버넌스 제공

CLOUDSEC 2023 ENVISION IT

Hosted by TREND MICRO

SOFTCAMP

소프트캠프㈜ 경기도 성남시 분당구 성남대로 779번길 6, KT분당빌딩 3, 4층