The Inspirations For Cyber Security

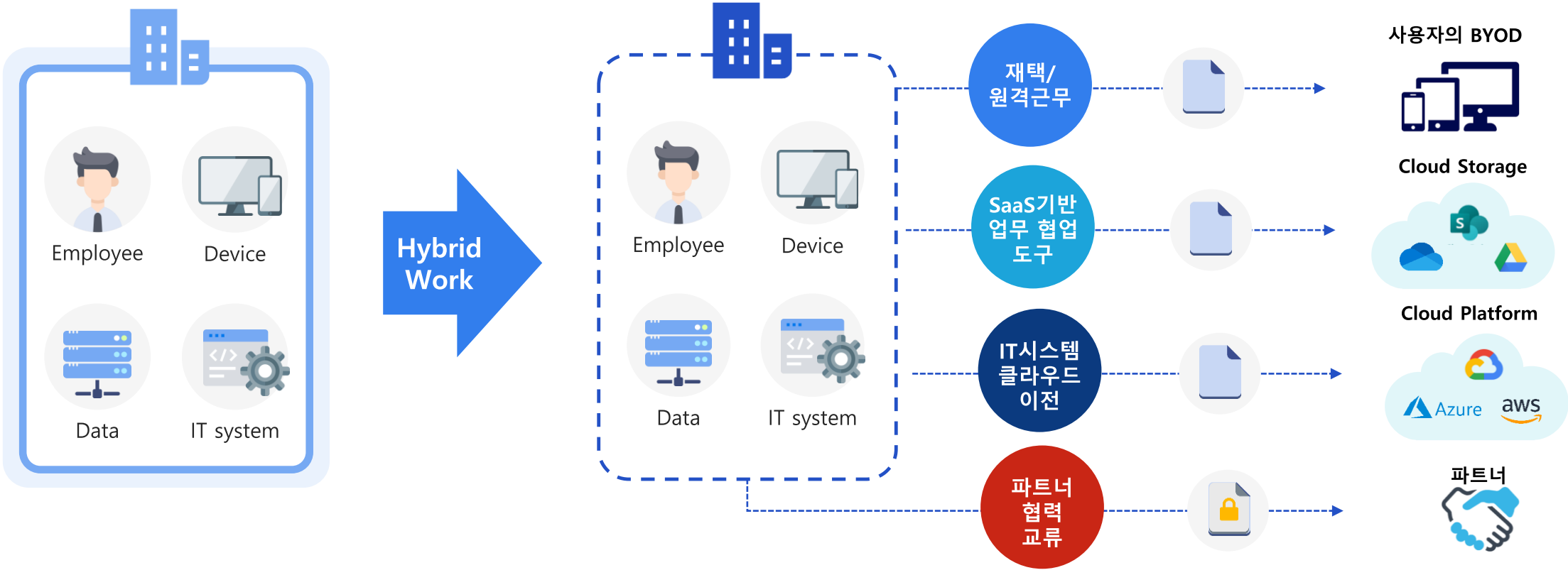
제로 트러스트 관점의 문서 보안 오케스트레이션 실현 방안

소프트캠프
컨설팅본부 이경화

SOFTCAMP

IT 환경의 변화

› 하이브리드 근무 환경 및 클라우드 협업 도구 도입으로 업무의 경계가 사라졌습니다.
데이터는 더 이상 사내에만 존재하지 않으며, 경계 보안만으로는 대응이 불가능합니다.

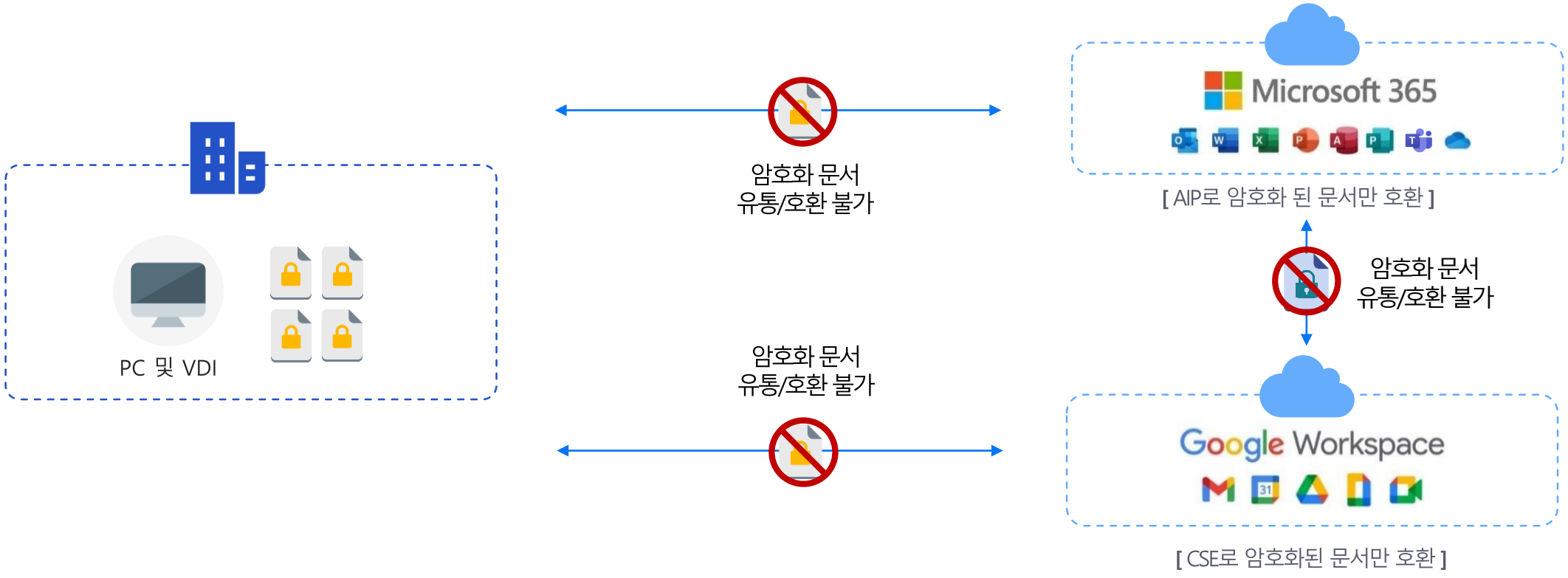


목표

- 경계 밖에서도 업무(파일의 열람/편집) 가능 및 보안 유지
- 파트너 보안이 강화된 상태로 문서, 도면 등의 협력

클라우드 협업 환경 도입

› 기존 암호화 문서는 Microsoft365, Google Workspace와 같은 업무 협업 SaaS 도구들 내에서는 협업 기능을 사용할 수 없기 때문에 문서 사용성에 이슈가 발생합니다.



문제점

- 클라우드 서비스(Microsoft, Google)마다 다른 DRM / 문서 암호화 방식 제공
- 기존 DRM 문서의 호환성 결여
- 클라우드 서비스의 내 문서 협업 기능(열람/편집/공동편집 등) 사용 불가

1. 협업 환경 변화에 따른 문서 오케스트레이션- 차세대 DRM의 요구 사항

› 다양한 클라우드 협업 환경의 도입으로 기존 DRM은 더욱 확장된 기능이 필요합니다.
경계가 사라지고 보다 다양해진 환경에 맞는 보안을 제공해야 합니다.

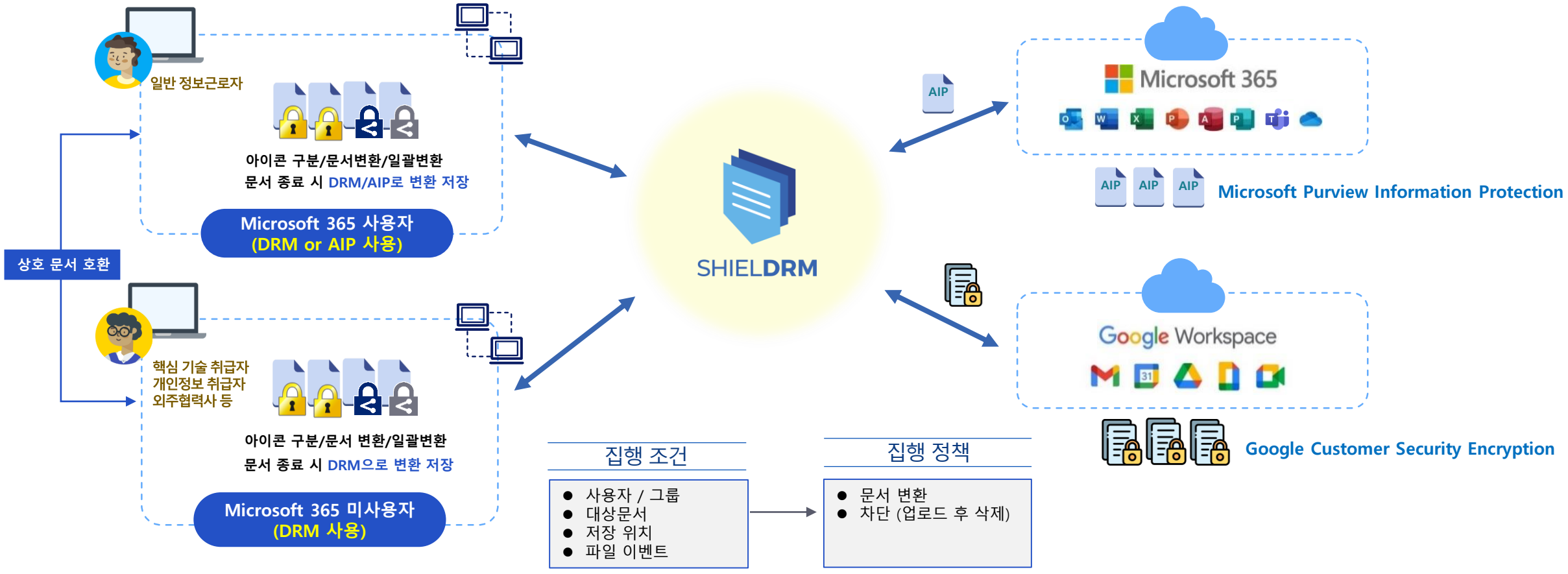
AS-IS

- 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. 협업 환경 변화에 따른 최적의 보안 협업 방안 - SHIELDRM

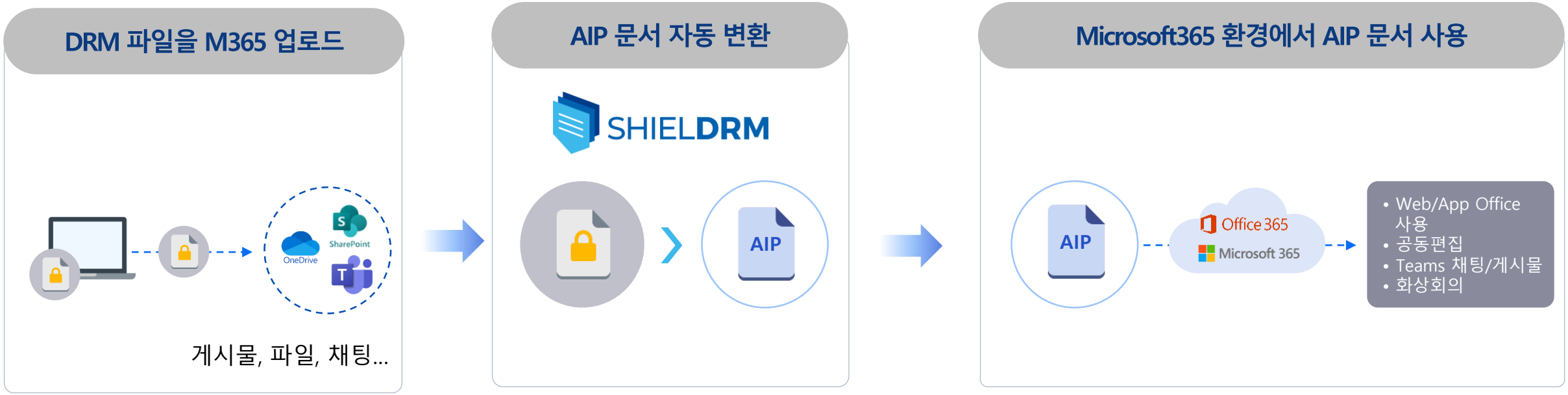


우수성

- 보안 관리자 : 다양한 협업환경, 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. 협업 환경 변화에 따른 최적의 보안 방법 – M365 지원

› Endpoint DRM(Document Security) 보안 문서를 M365(OneDrive, Sharepoint, Teams 등) Cloud 저장소에 **업로드 시 AIP 문서로 자동 변환하여** 단절 없는 보안 및 사용성을 제공합니다.



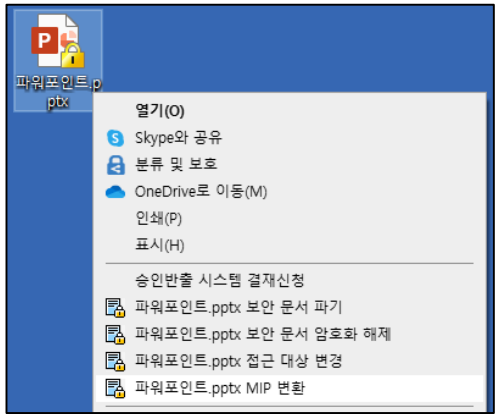
서비스 특징

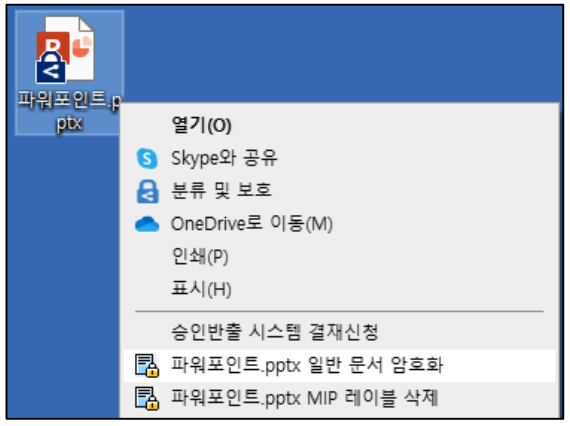
- 사용자 추가 조작 없이 문서를 Microsoft365 서비스로 업로드하여, 사용(열람/편집/공동편집) 가능
- 클라우드 스토리지 내에서도 AIP 적용을 통한 Cloud-Native 보안 적용
- Zero Trust Conditional Adaptive 정책으로 사용자/문서 유형 등에 따른 문서 변환(DRM <-> AIP) 정책 집행
- 변환을 위한 **개별 서버 구축 필요 없음**

1. 협업 환경 변화에 따른 최적의 보안 방법 – 아이콘 구별

› **DRM 문서를 AIP로 변환하거나, AIP 문서를 DRM 문서로 변환**할 수 있고

› 기존 암호화 문서와 AIP 레이블 적용 문서를 직관적으로 인식할 수 있도록 아이콘이 식별됩니다.





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

기존 암호화 문서

AIP 레이블 적용 아이콘

암호화 여부 | 레이블 차이

암호화 레이블 일반 레이블

* 아이콘 구분은 PC 내 저장된 문서에서 지원

서비스 특징

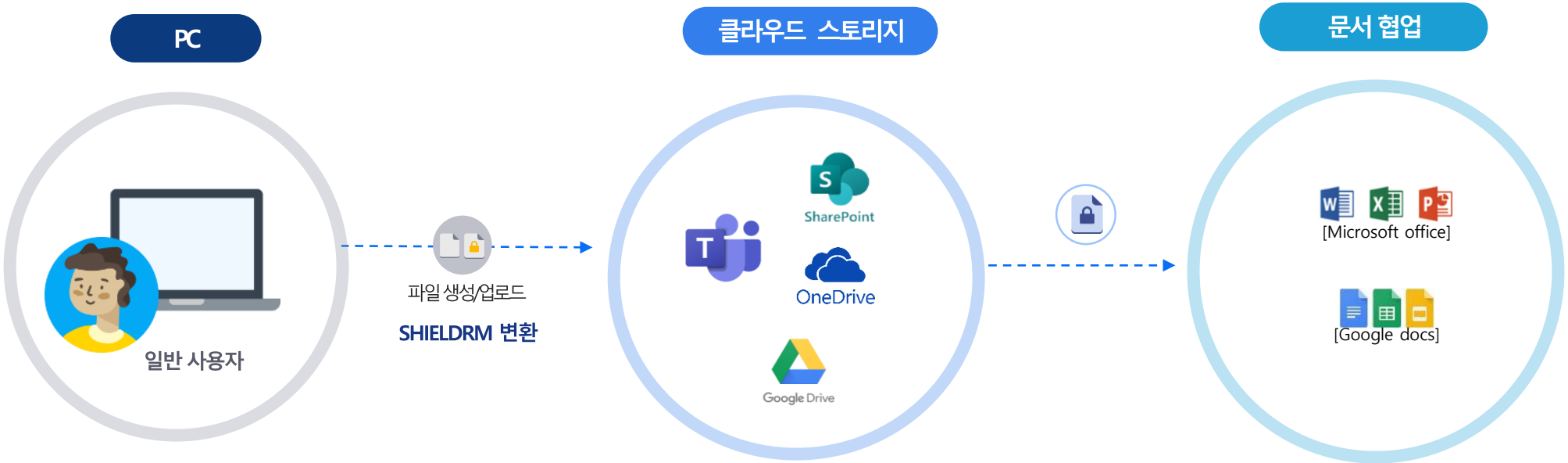
- 로컬 PC에서도 DRM <-> AIP 문서 변환 가능
- AIP 레이블 문서 여부 사용자 가시적 확인 가능
  * M365 서비스 자체적으로 아이콘 구분이 안됨(AIP 문서와 일반 문서 구별 불가)
- 암호화(민감도) 레이블 적용 문서에 대한 가시성 확보 및 업무 혼란 최소화

데모 동영상- SHIELDRM

2. Hybrid 환경의 컴플라이언스 준수 – 국가핵심 기술 취급자

SHIELDrive

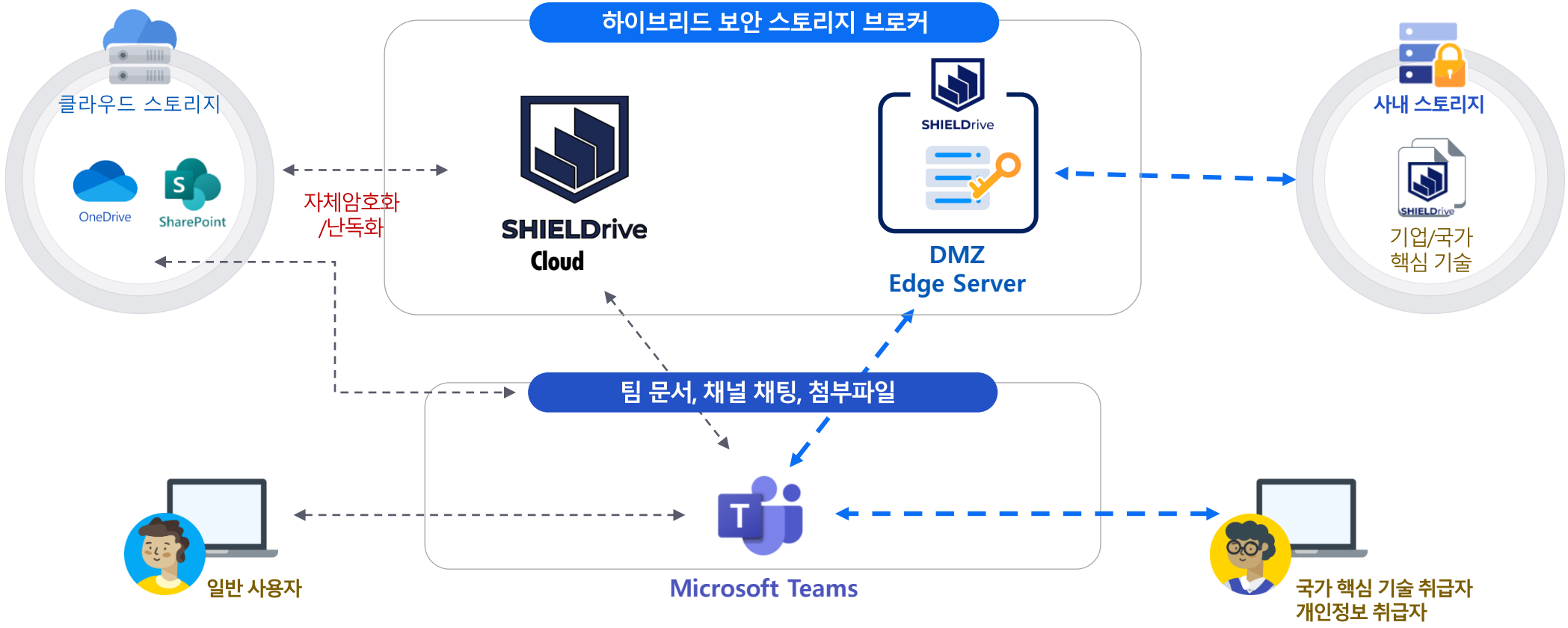
- 협업 도구로서 클라우드 협업도구를 사용하고 싶지만,
  "국가 핵심기술 " 관련, 산업기술의 유출방지 및 보호에 관한 법률
  해외 클라우드 저장소 사용을 금지하고 있다.
- 핵심기술 취급자도 문서 협업 서비스를 사용하고 싶다.
- SharePoint, OneDrive에 저장된 문서를 CSP 로부터 정보주권을 유지하고 싶다.



2. Hybrid 환경의 컴플라이언스 준수 – 국가핵심 기술 취급자

2. Hybrid 환경의 컴플라이언스 준수 – 국가핵심 기술 취급자

› 클라우드 사업자로 부터 **문서 주권을 확보**(클라우드에 저장되는 문서를 우리회사 암호화키로 관리; BYOK)하고
Teams 협업기능 + 사내 시스템에 문서저장(핵심 정보 사용자 등 해외 클라우드 사용 불가 사용자)이 가능합니다.



서비스 특징

- 조건부 정책에 따라 **클라우드 스토리지 사용자**와 **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)

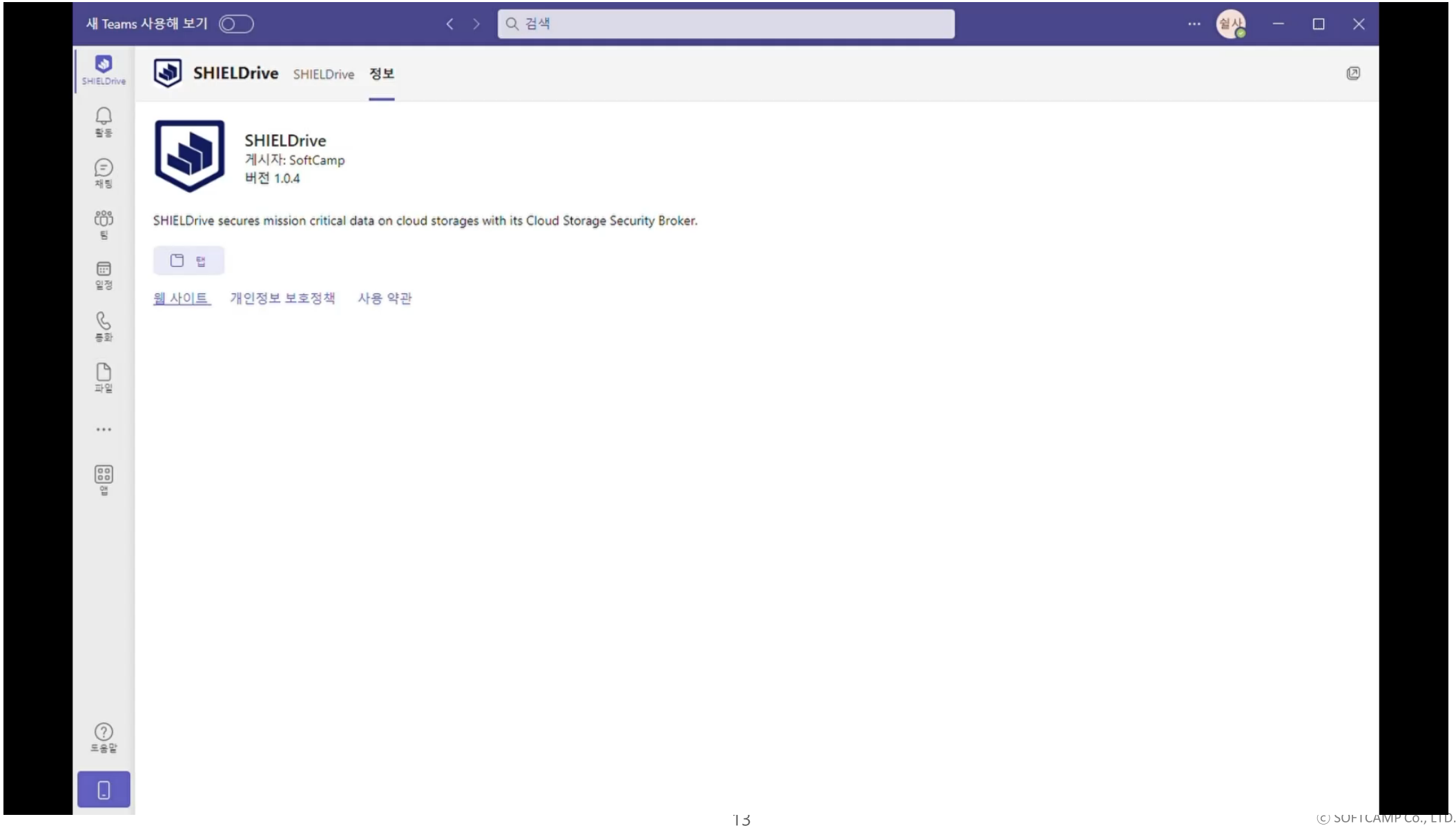
2. Hybrid 환경의 컴플라이언스 준수 – 국가핵심 기술 취급자

› 연결된 스토리지 유형에 따른 열람/편집/공동편집을 지원합니다.

저장 스토리지 유형	기본 문서 편집기	기타 확장자
OneDrive SharePoint **Microsoft 365 클라우드 스토리지**	• Microsoft 지원 확장자는 Microsoft Office App/Web 으로 문서 열람, 편집 및 공동 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 확장자는 Google docs를 통해 웹으로 문서 열람,, 편집 및 공동 편집 가능	• hwp, hwpx 등의 확장자는 한컴오피스 웹로 공동편집 • 그 외 확장자는 SHIELDViewer로 읽기 전용으로 사용 * SHIELDViewer는 소프트캠프에서 제공하는 웹 뷰어입니다.
S3, NAS/ 파일서버 등 문서편집기 미 제공 스토리지	• 자체 웹 문서편집기가 없는 스토리지는 한컴 오피스 웹 을 통해 열람, 편집 및 공동 편집 가능 *지원Web 문서편집기는 향후 변경될 수 있습니다.	• 한컴오피스 웹에서 지원하지 않는 확장자는 SHIELDViewer(자체 웹 뷰어)로 읽기 전용으로 사용

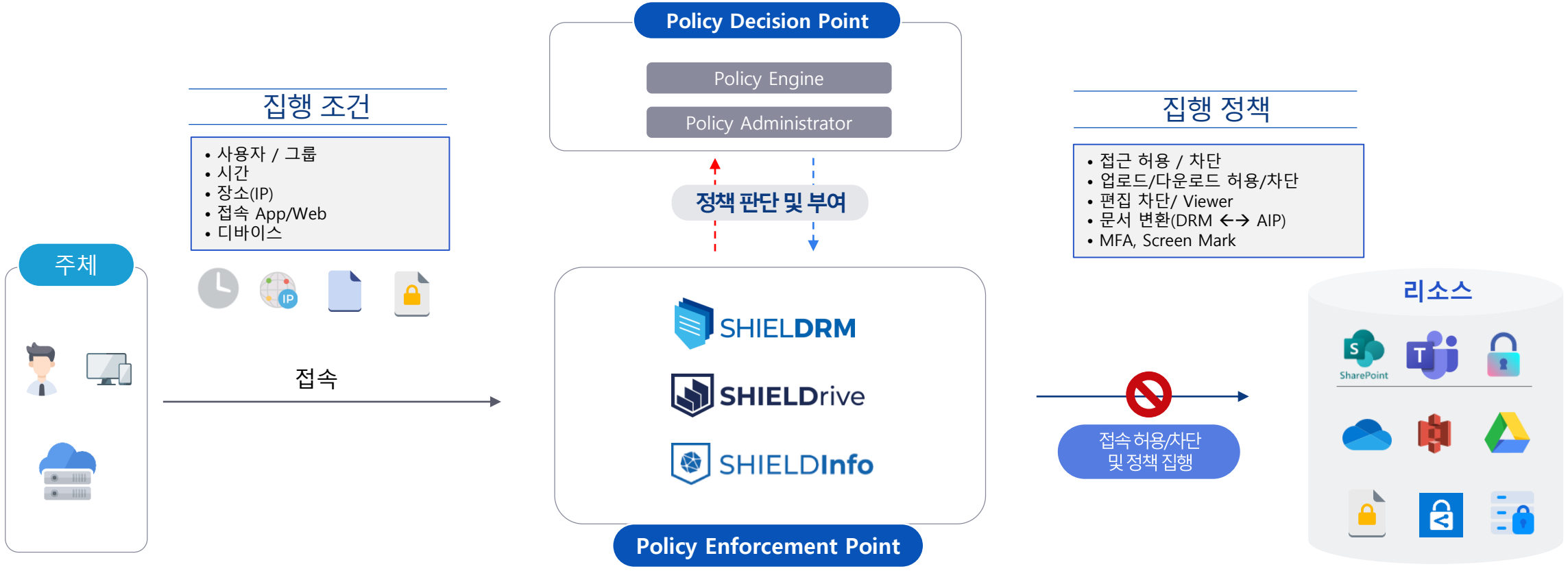
*도면(CAD) 파일과 AIP암호화된 PDF는 현재 웹 뷰어를 제공하지 않습니다.

데모 동영상- SHIELDRIVE



3. 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.

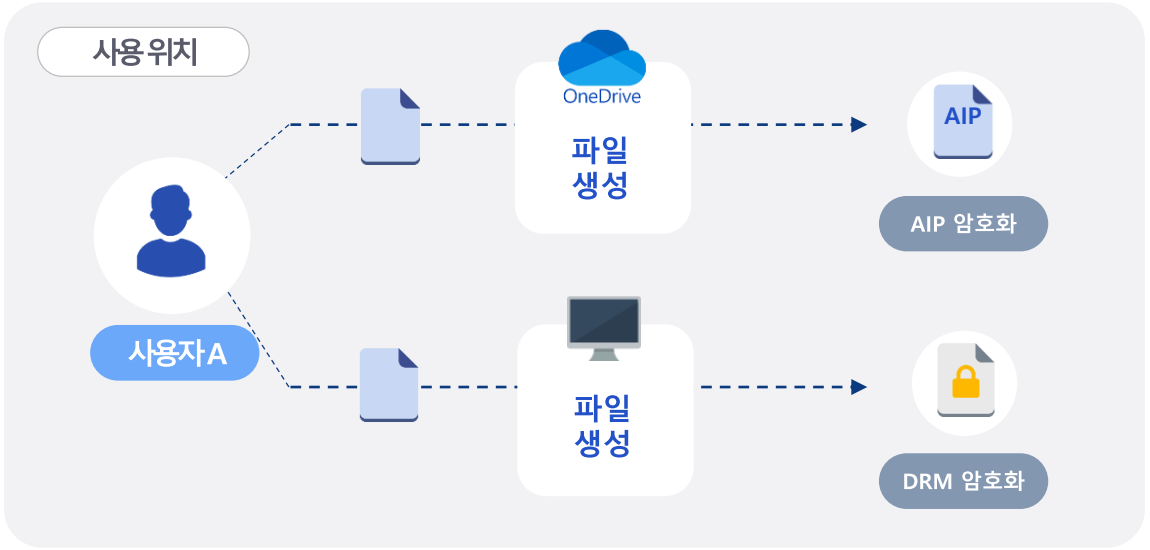


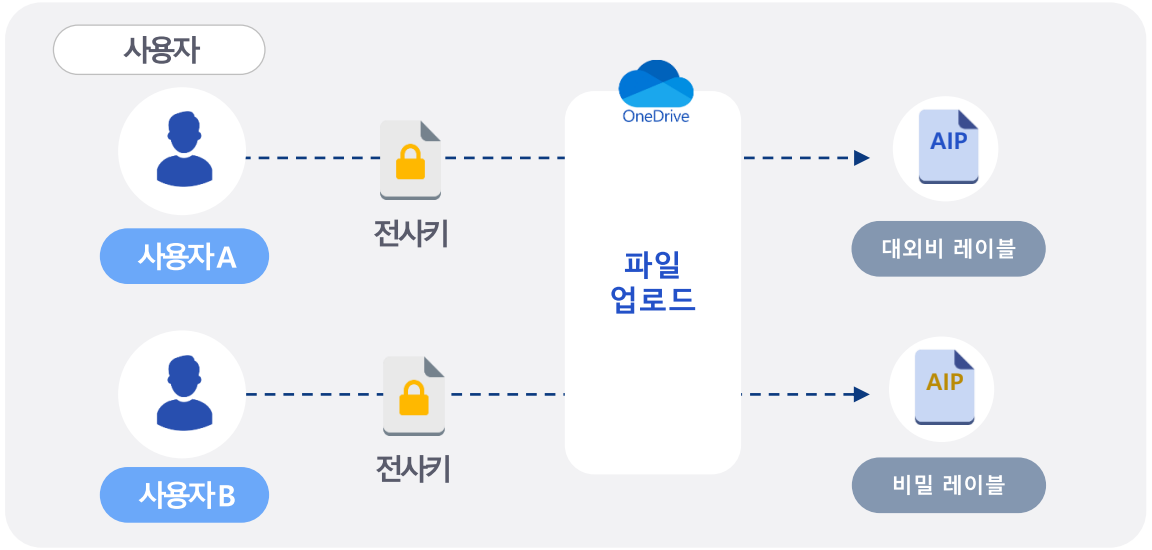
특징

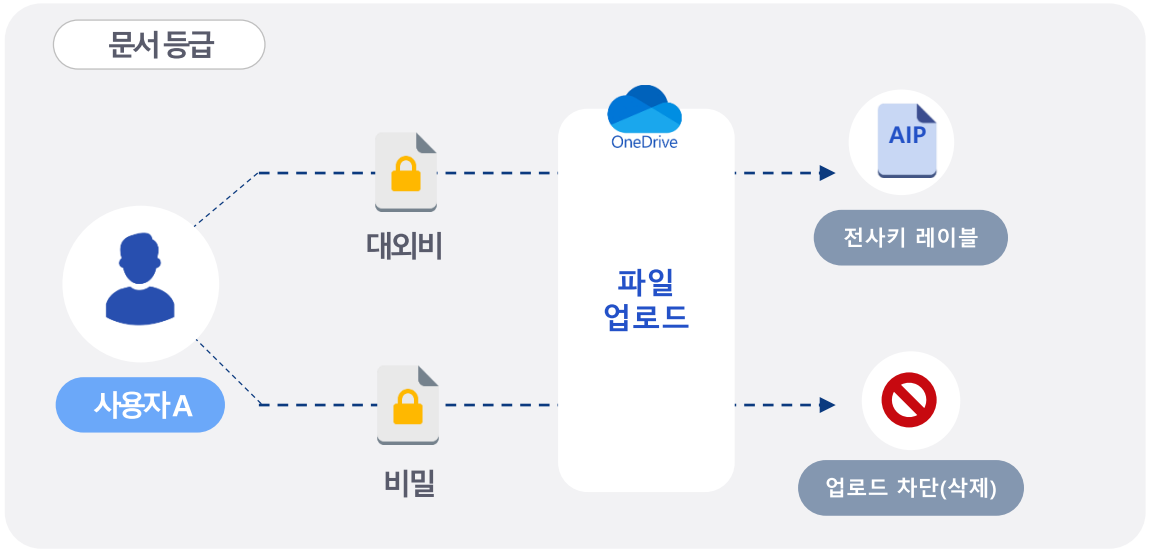
- **Zero-Trust**(제로 트러스트) : 모든 사용자, 장치, 애플리케이션, 데이터에 대한 미 신뢰 원칙을 기반
- **Conditional**(조건부) : 접근 권한은 다양한 조건(사용자, 기기, 위치, 시간 등)에 의해 설정
- **Adaptive**(적응형) : Zero-Trust 정책은 실시간으로 조정되며, 사용자 또는 기기의 상태에 따라 **권한을 동적으로 변경**
- ZTCAP의 주요 목표 : **위험 감지 및 완화**, **적응성**, **인증 및 권한관리**, **보안 이벤트 모니터링**

3. 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.



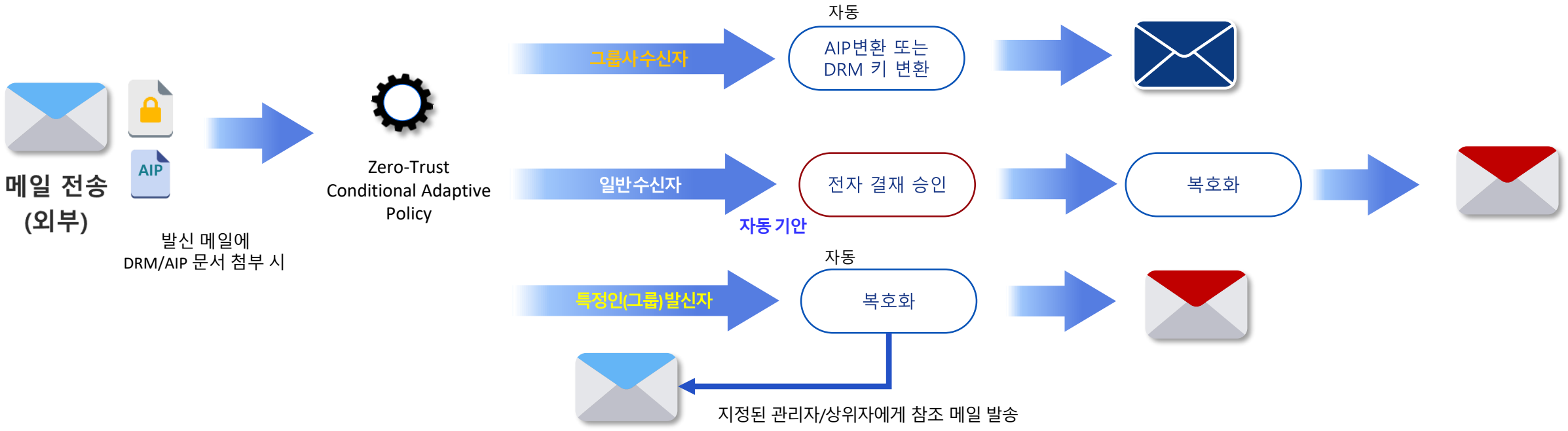




4. 외부 발송 메일에 대한 문서 오케스트레이션

발신 이메일 첨부 파일 처리 시스템

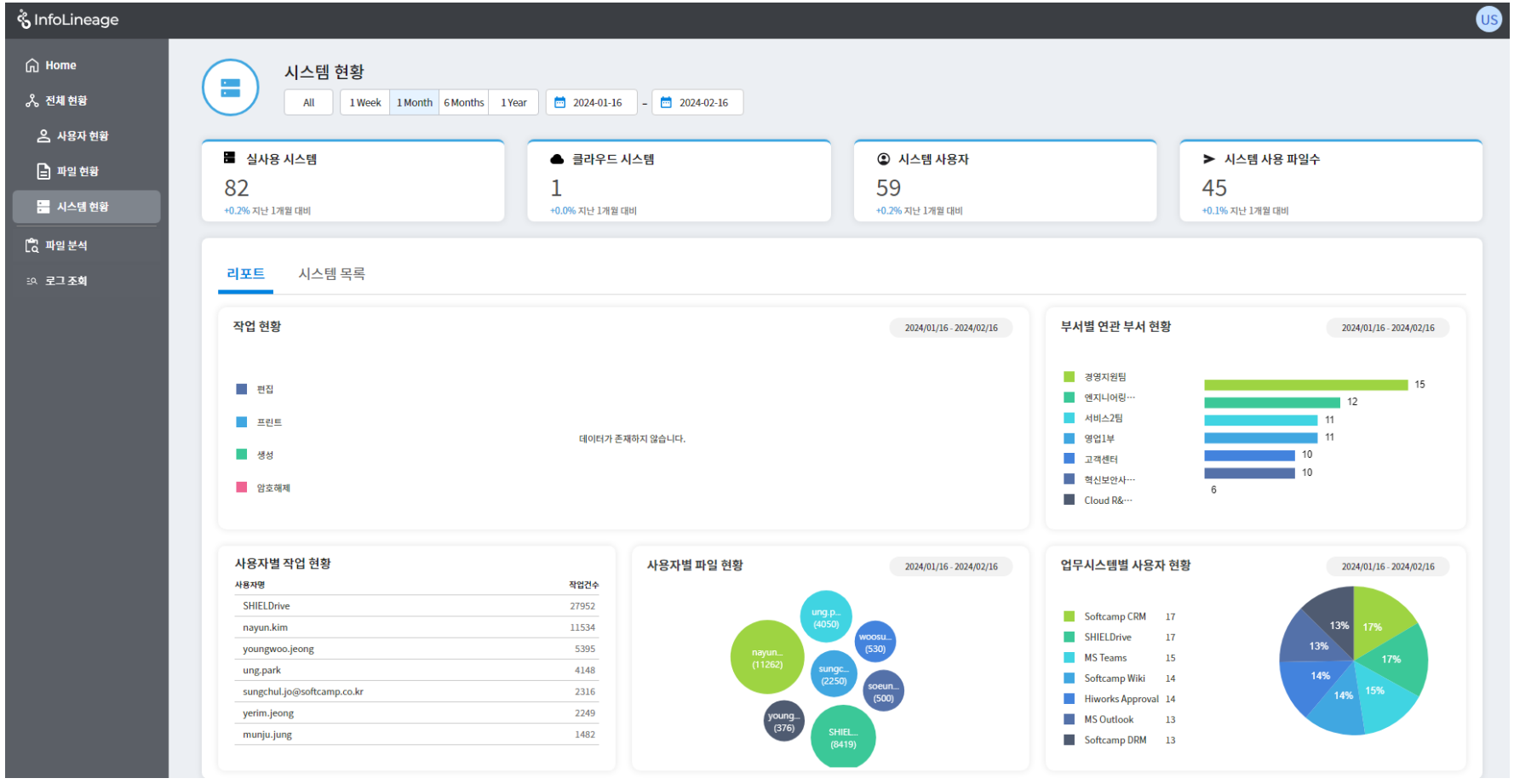
사외로 발송되는 메일의 경우, 문서 수신자에 따라서 첨부파일 암호화 형태의 변환이 필요한 경우,
정책에 의해 사용자 개입없이 문서암호화 방식 변환 및 복호화를 자동화 할 수 있습니다.



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**(Exchange Server 2016이상, On-premise/Exchange Online 모두 지원)

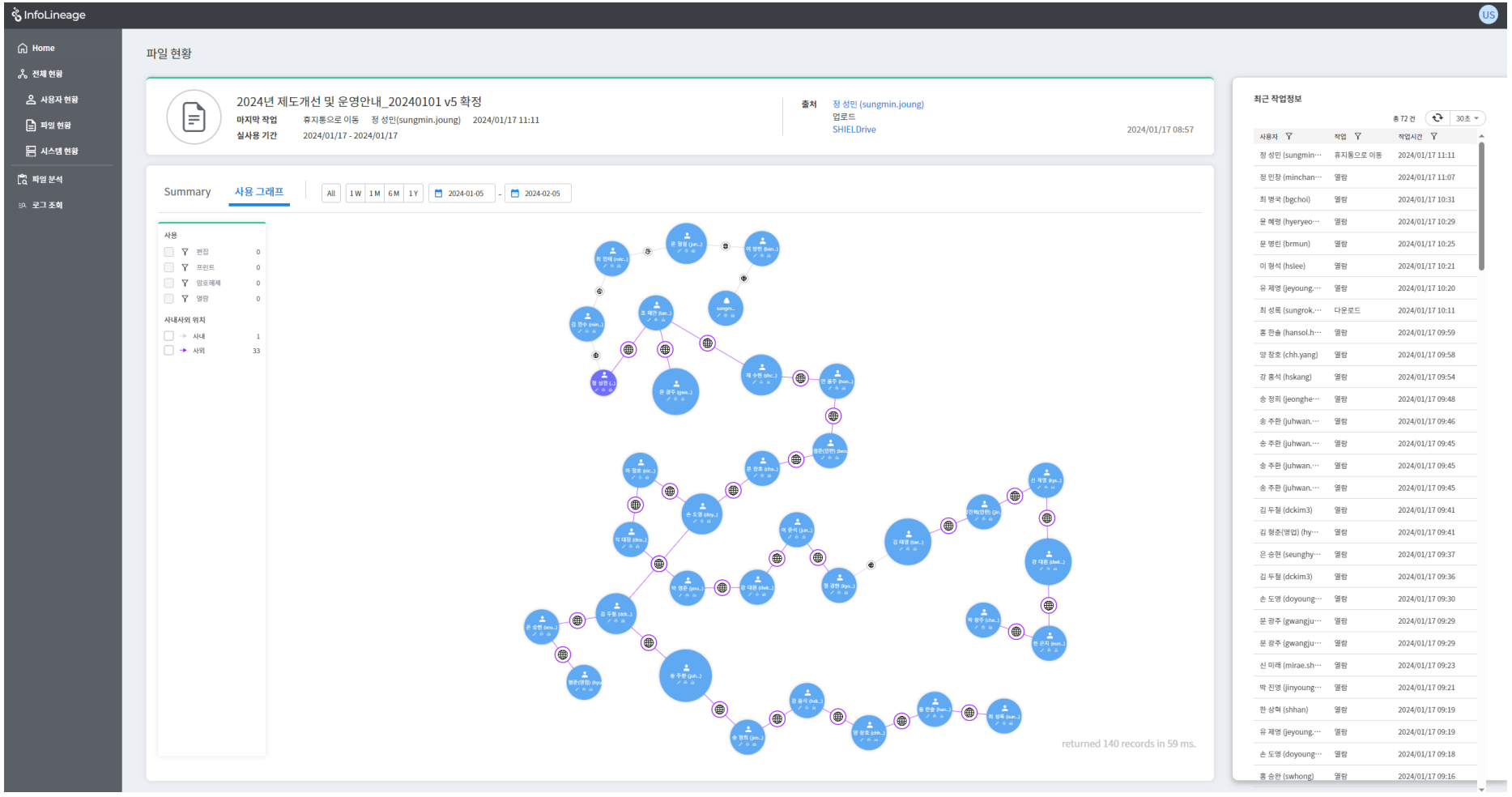
5. 문서의 유통 가시성 확보 - InfoLineage



특징

- 부서별/파일별/사용자별 문서작업 확인 및 협업/유통 이력 조회
- 사내 시스템 문서 현황 및 로그 조회

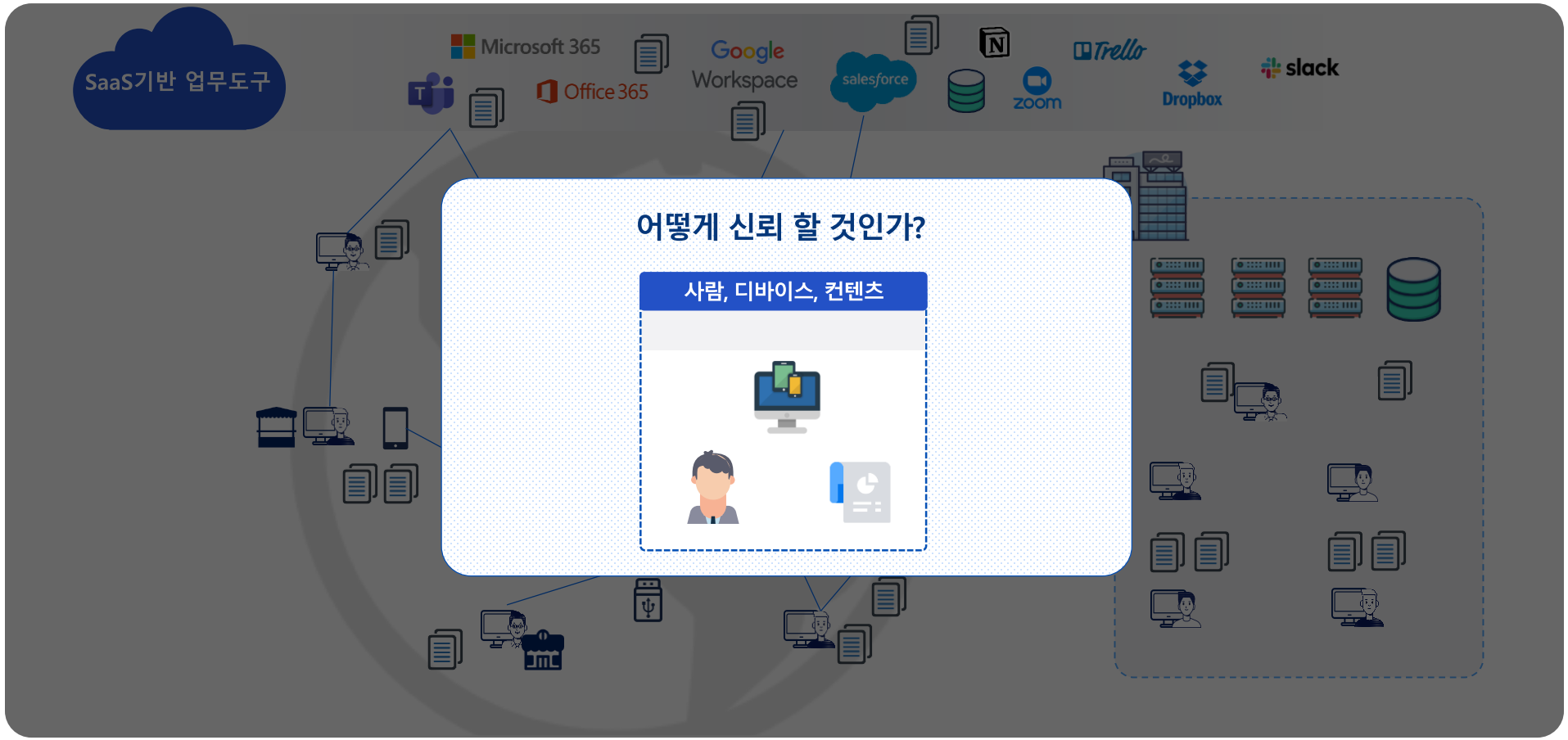
5. 문서의 유통 가시성 확보 - InfoLineage



특징

- On-Premise, Cloud(M365 등) 통합 문서 가시성 제공
- 최초 생성자 부터 중간 편집자, 전달자, 인쇄 등 **모든 유통 경로에 대한 가시성 현황** 제공
- (SHIELD Mail 사용시) 문서 사외 반출 모니터링 가능

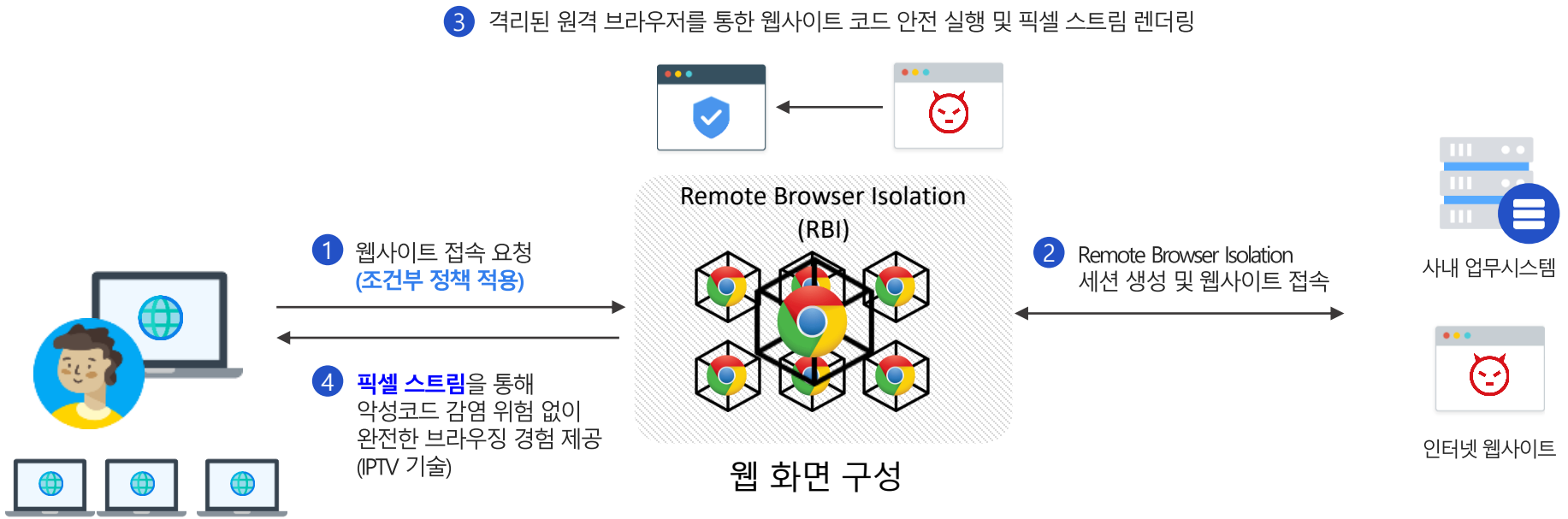
6. 신뢰할 수 있는 접속 보안



6. 신뢰할 수 있는 접속 보안 – Remote Browser Isolation

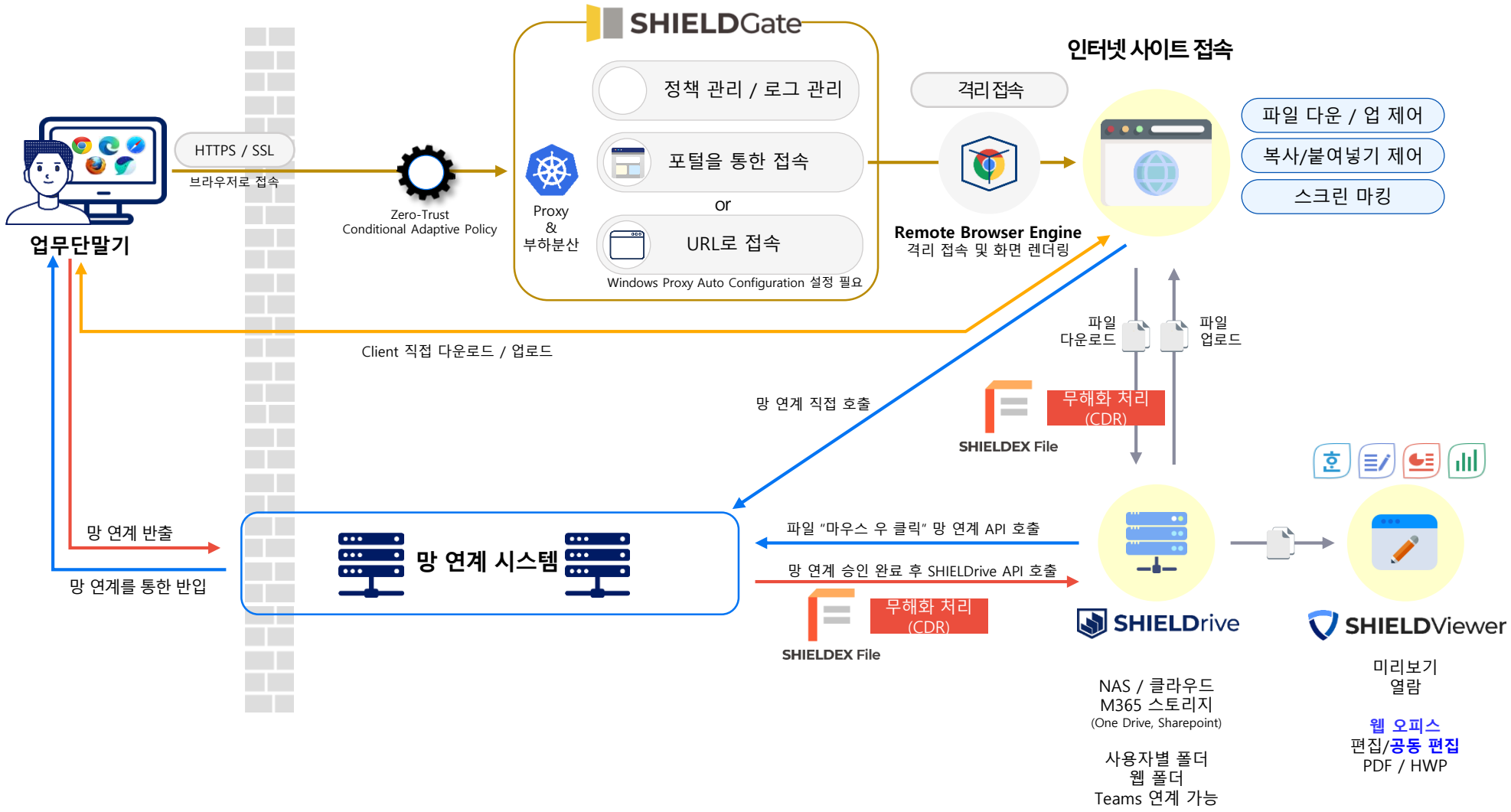
› 원격 브라우저 격리(RBI)는 서버에 가상 브라우저로 인터넷을 접속하고,
사용자 브라우저에서는 **접속한 화면을 픽셀 스트림으로 실시간 전송 받는 기술**입니다.

› Remote Browser Isolation(RBI) 기술은 현대 보안 환경에서의 중요한 트렌드 중 하나로 자리매김하고 있습니다.

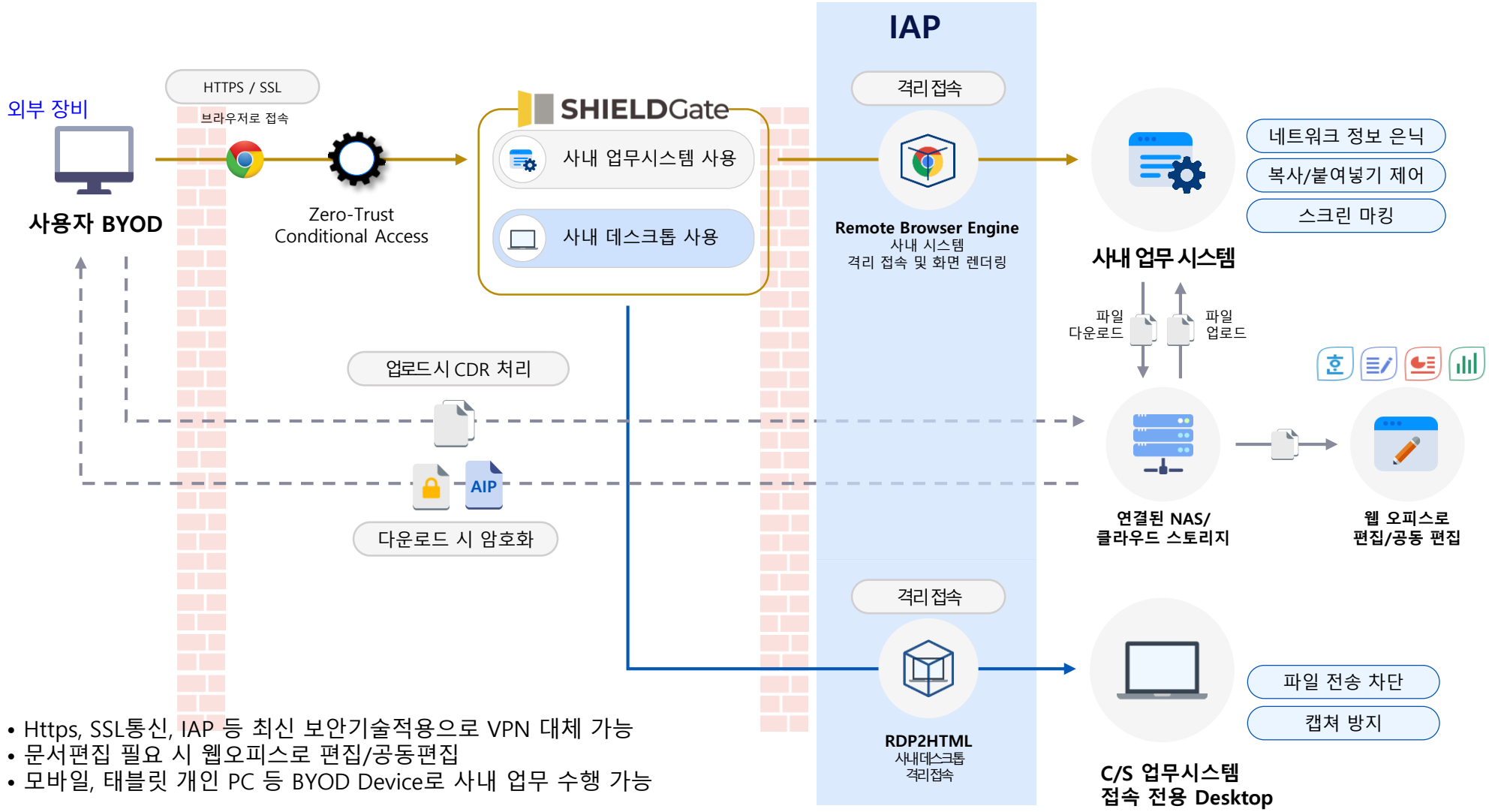


> 브라우저 격리 기술은 기업에서 웹 기반 공격을 대응할 수 있는 가장 효과적인 방법이다.
> 웹 브라우징으로 부터 엔드포인트(PC)를 지키는 측면에서는 웹 격리 기술이 보안에 가장 우수하다.
>
> SASE, SSE의 핵심 기술 요소 중 하나 Gartner

6. 신뢰할 수 있는 접속 보안 - 인터넷 격리 접속 흐름도



6. 신뢰할 수 있는 접속 보안 - 업무 시스템 원격 접속 흐름도

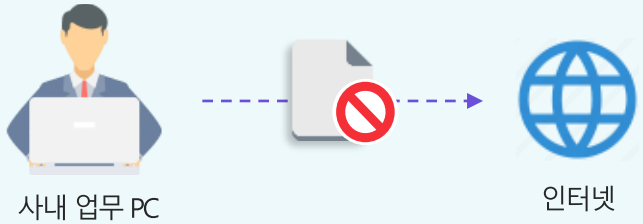


- Https, SSL통신, IAP 등 최신 보안기술적용으로 VPN 대체 가능
- 문서편집 필요 시 웹오피스로 편집/공동편집
- 모바일, 태블릿 개인 PC 등 BYOD Device로 사내 업무 수행 가능

※ IAP : Identity Aware Proxy – 신원 인식 프록시

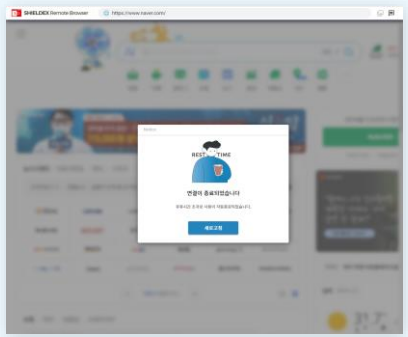
6. 신뢰할 수 있는 접속 보안 – 추가 웹 보안 기능 제공 가능

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

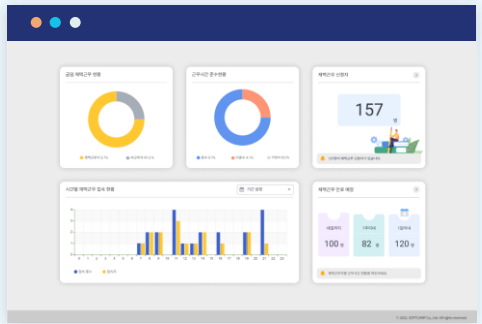


자료(파일) 무단 반출 통제

민감 정보 입력 통제



웹 화면 잠금 / 스크린 마크



Web 사용 이력 추적 / 저장

www.softcamp.co.kr

THANK YOU

SOFTCAMP

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