The Inspirations For Cyber Security

클라우드 기반 문서 보안 오케스트레이션

2023-11-28

SOFTCAMP

ⓒ SOFTCAMP Co., LTD. All rights reserved.

클라우드 저장소, 사내 NAS / 파일서버의 문제점 ?

관리의 어려움

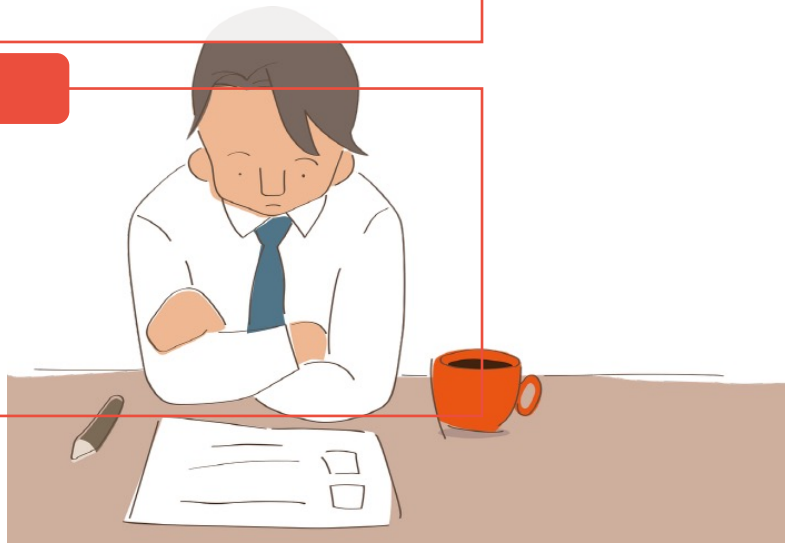
- 부서별, 개인별, 사외 공유 폴더 관리
- 폴더별 권한 관리, 접근 제어
- 파일 버전 관리(과거 버전 열람, 회귀)
- 용량 관리(개인별, 부서별, 폴더별)

사용 불편함

- 공동편집
- 문서 변환 이슈(DRM 문서)
- 웹 환경에서 문서 사용
- 파일명 검색, 본문 검색

보안성

- 이력 조회 불가
- 장비 분실 우려
- 백업 파일에 대한 유출 우려
- 완전 삭제(복제, 백업 파일까지 제거)
- 클라우드 문서 주권 확보



ⓒ SOFTCAMP Co., LTD. All rights reserved

Hybrid Security Storage Broker !!

Storage Broker란 - **다양한 스토리지 시스템을 단일 인터페이스로 제공**하는 소프트웨어.
- 보안, 관리 등 다양한 기능을 부여하여 데이터를 저장하고 처리하는 기능 제공

›다양한 스토리지 적용

파일서버, NAS 등 On-Pre 장비, Private Cloud 저장소, Public Cloud 저장소(M365, Google, ..) 등 다양한 저장소 지원

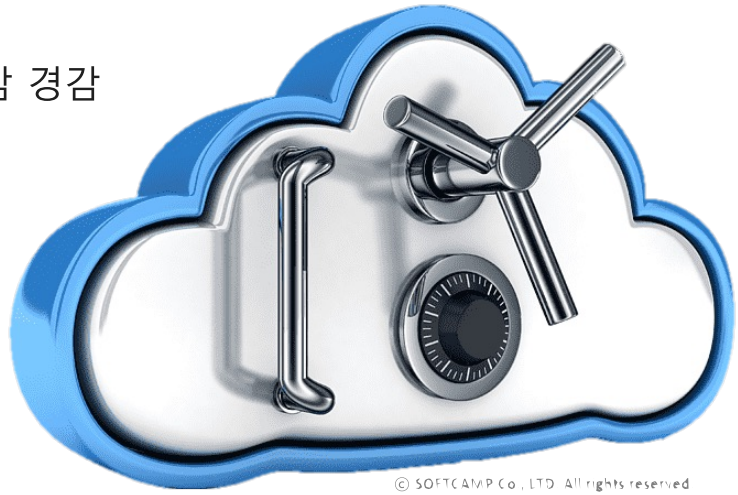
›강력한 보안 기능

강력한 보안 기능제공으로 데이터의 유출, 삭제, 변조 등 보안 사고 방지

- 데이터 보안 강화 : 데이터 암호화, 접근 제어, 감사 로그 기록 등으로 데이터를 안전하게 보호
- 규정 준수 확보 : 데이터 보안을 강화하여 관련 규정을 준수할 수 있도록 지원(분류에 따라 Public 클라우드 업로드 금지)
- 데이터 손실 방지 : 데이터의 유출, 삭제 등의 사고를 방지하여 데이터 손실을 방지

›관리 및 운영 효율성

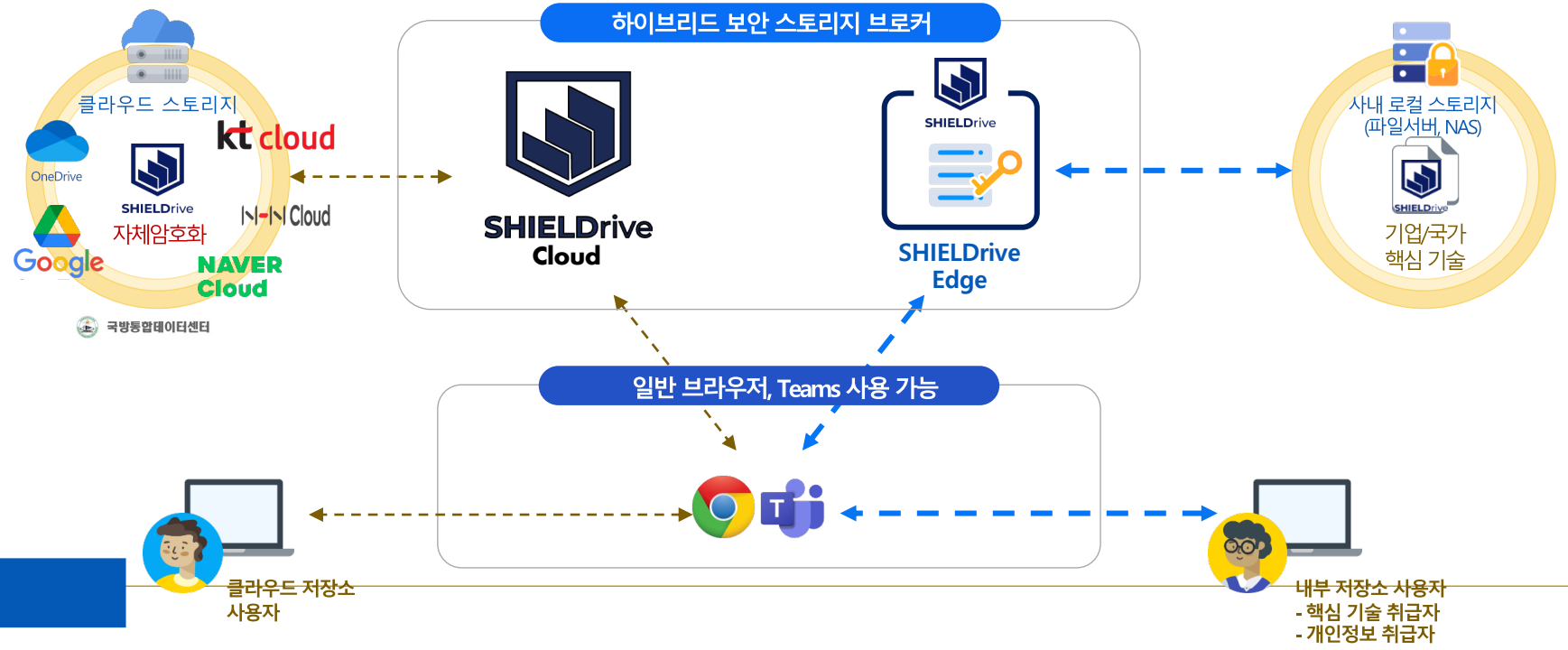
관리 콘솔을 통해 쉽게 설치, 구성, 관리할 수 있어 IT 관리자의 업무 부담 경감



© SOFTCAMP Co., LTD. All rights reserved

다양한 스토리지 통합 구성

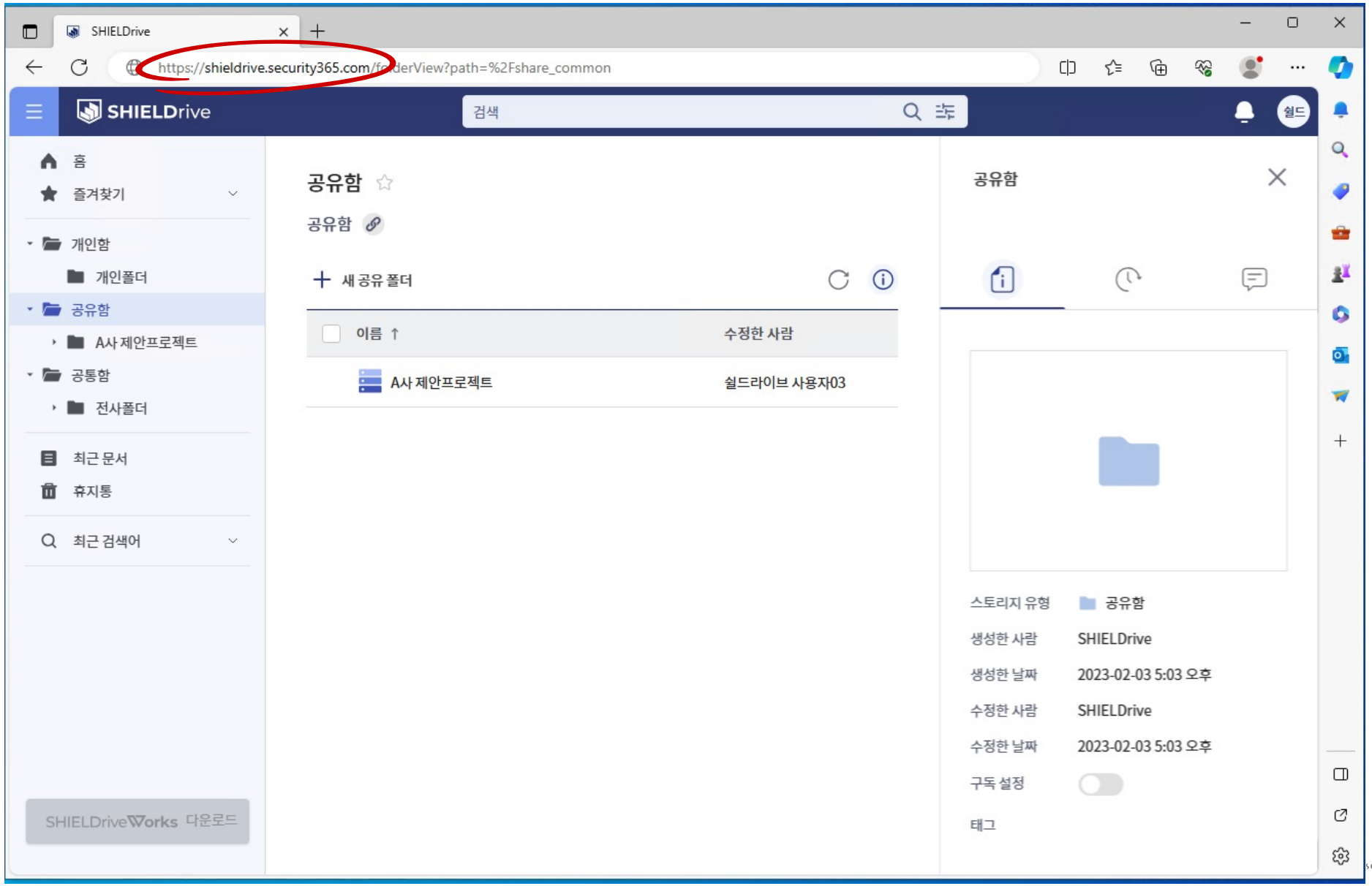
- 클라우드 스토리지 또는 사내 스토리지(NAS 등) 등 여러 종류의 스토리지 관리 가능
- 스토리지 자체 기능 을 사용하지 않는 별도 폴더 및 권한 관리 기능 부여



- 조건부 정책에 따라 클라우드 스토리지 사용자와 사내 스토리지 사용자 구분 제어 가능
- 스토리지에 대한 폴더 관리(개인별, 팀별/부서별, 외부 공유 폴더 등)
- 여러 개의 스토리지를 하나로 통합하여 관리 및 운용 가능
- 사용자 등 조건에 따라 저장 스토리지 지정 또는 폴더 구분(지역에 따라 저장소 지정 가능)

ⓒ SOFTCAMP Co., LTD. All rights reserved

Web Browser를 통한 접속 – 모든 표준 Browser



다양한 역할의 폴더와 기능

문서를 드래그&드롭으로 업로드 가능

Web Browser를 사용할 때 드래그 & 드롭으로 스토리지에 문서 업로드 가능(폴더 전체 업로드 / 다운로드 가능)

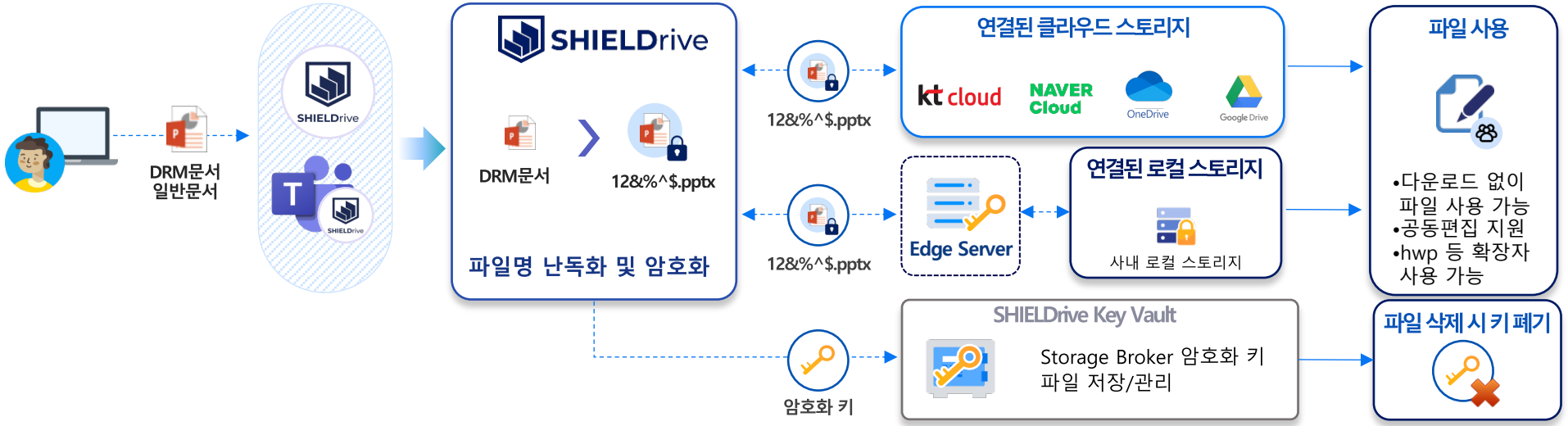
파일명, 문서 본문 검색 기능

LTD. All rights reserved

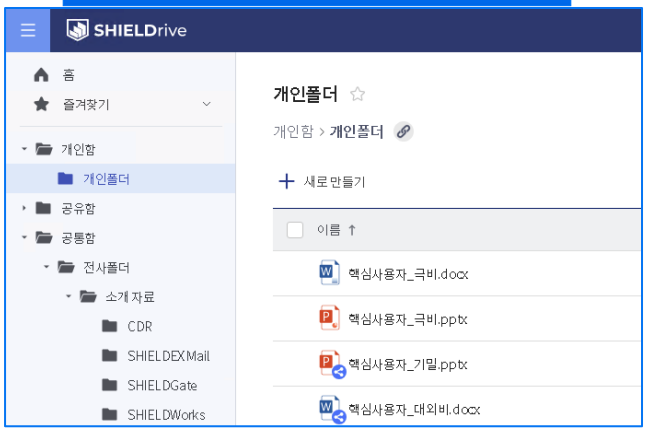
암호화 , 난독화

› 스토리지 파일 저장 시 **문서의 주권 확보** ← 백업 파일에서 직접 열람 불가

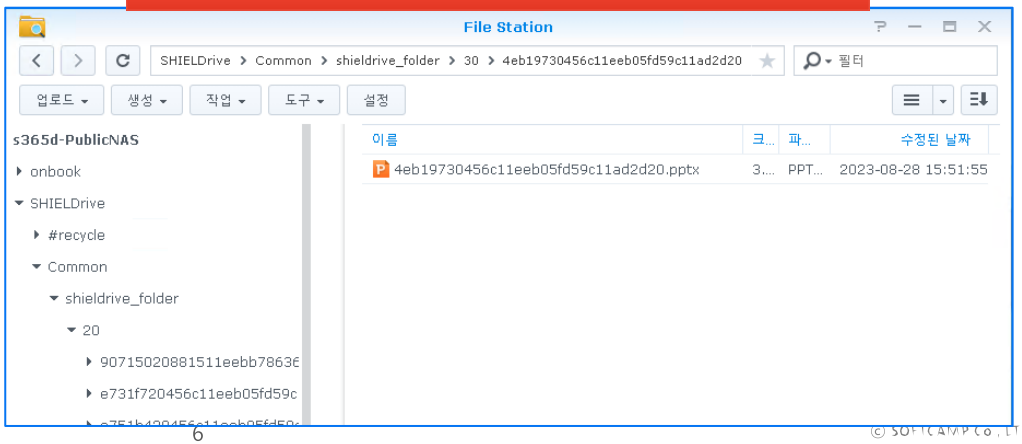
› 자체 파일 내용 **암호화**, 파일명/폴더명 **난독화** ← 파일별 암호화 키 관리, 삭제 시 암호키 삭제



SHIELDrive 내 폴더 구조 및 파일 표시



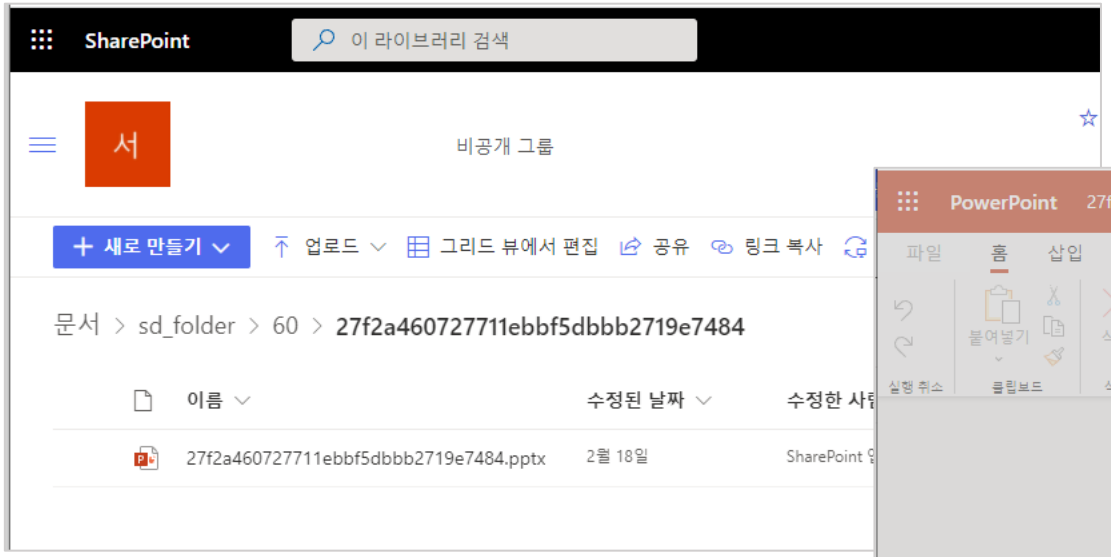
실제 스토리지 내 저장된 문서의 폴더 구조 및 파일 표시



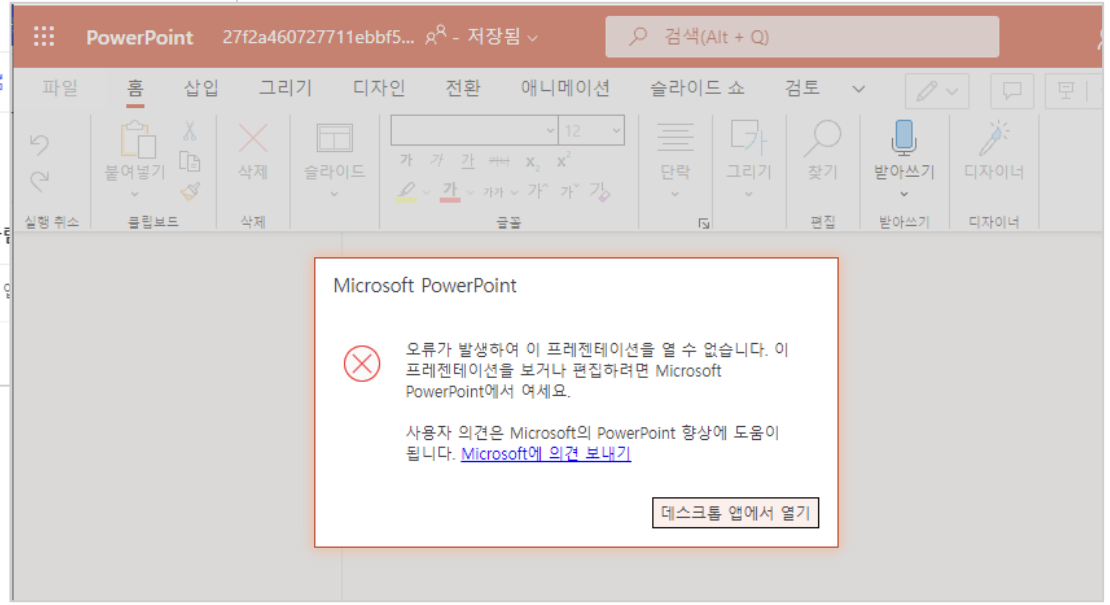
© SOFTCAMP Co., LTD. All rights reserved

스토리지에서 직접 문서 열람 불가 – 유출 방지

- Storage Broker와 연결된 스토리지에 직접 접속하여 문서 열람 시 열람 불가 → 암호화
- 스토리지 백업본에서도 직접 열람 불가 / 장비 분실 또는 유출 시에도 내부 컨텐츠 확인 불가



파일명 난독화



파일 암호화

© SOFTCAMP Co., LTD. All rights reserved

문서 라이프사이클 관리

› Storage Broker를 통해 파일 업로드/생성 시 **암호화 키가 생성**되고, 파일이 암호화 됩니다.
생성된 암호 키는 파일 삭제 시 함께 파게 됩니다.

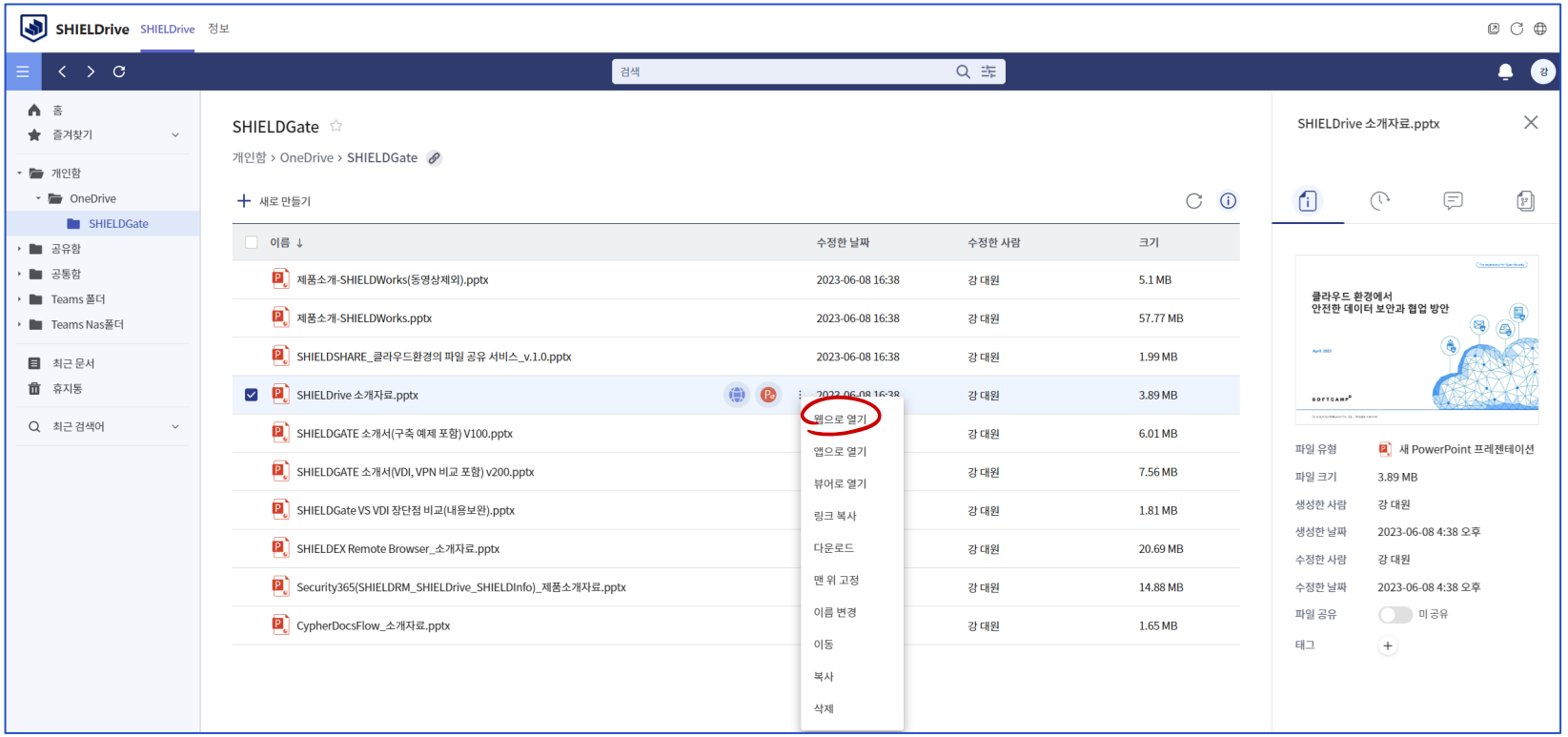
Storage Broker를 통해 파일이 업로드 되거나, 파일 생성 시 **파일 암호화 키 생성 및 파일 암호화 진행**
Storage Broker를 통해 파일 삭제 시 해당 스토리지 내 **파일 삭제 및 파일 암호화 키도 함께 폐기**
이를 통해 파일의 위치를 식별 할 수 없는 **Cloud 환경에서도 파일 Life-Cycle 관리** 가능

* GDPR(General Data Protection Regulation; EU 개인정보보호 관련 규정)에서도
Cloud 환경에서는 암호화 된 파일의 암호화 키가 폐기되었을 경우 파일이 완전히 삭제된 것으로 인정하고 있음.

ⓒ SOFTCAMP Co., LTD. All rights reserved

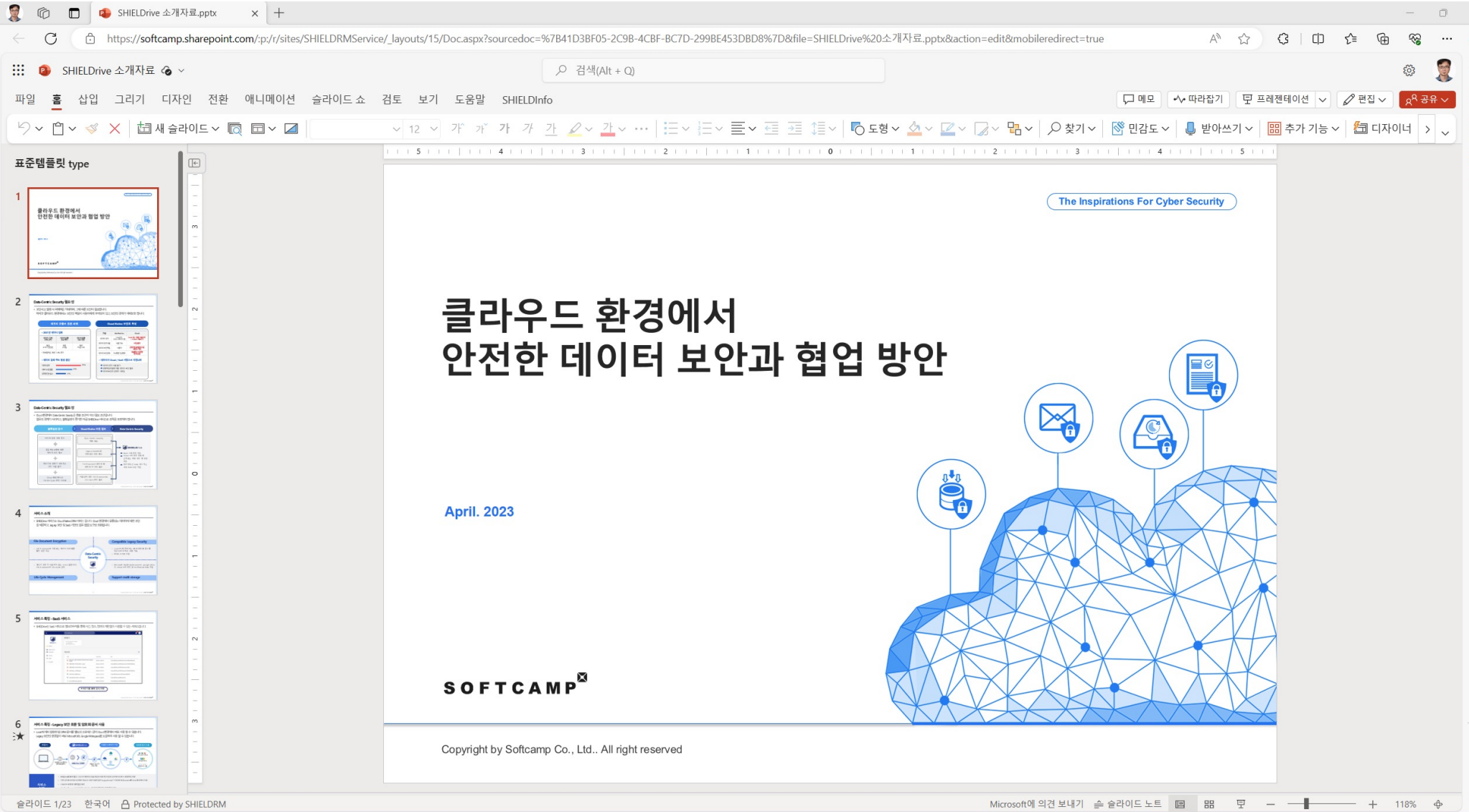
웹 편집기, 공동 편집

- 설치된 문서 편집기 없이 **웹에서 문서 열람/편집/인쇄** ← 워드, 엑셀, 파워포인트, **한글**
  → 설치된 문서 편집기 없이 사용 가능
  → PDF 등 편집이 불가능한 문서는 Viewer로 열람 가능 SHIELDViewer
- 웹에서 **공동 편집 가능**→ 2명 이상이 동시에 문서를 열람 및 편집 가능



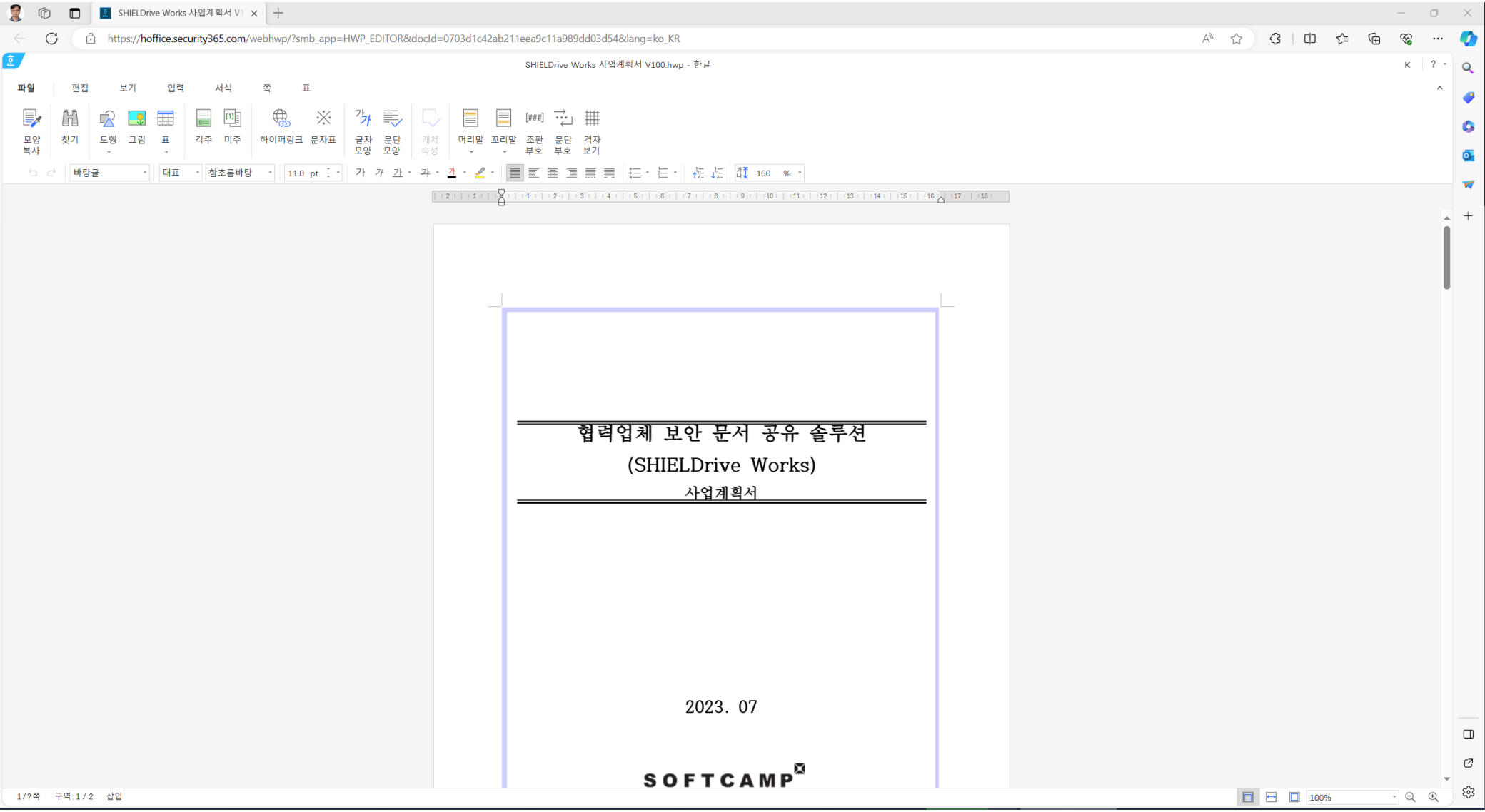
ⓒ SOFTCAMP Co., LTD. All rights reserved

웹 편집기 문서 작업 화면 – Cloud별 웹 편집기 제공



ⓒ SOFTCAMP Co., LTD. All rights reserved

웹 편집기 문서 작업 화면 – 한컴 웹오피스 제공

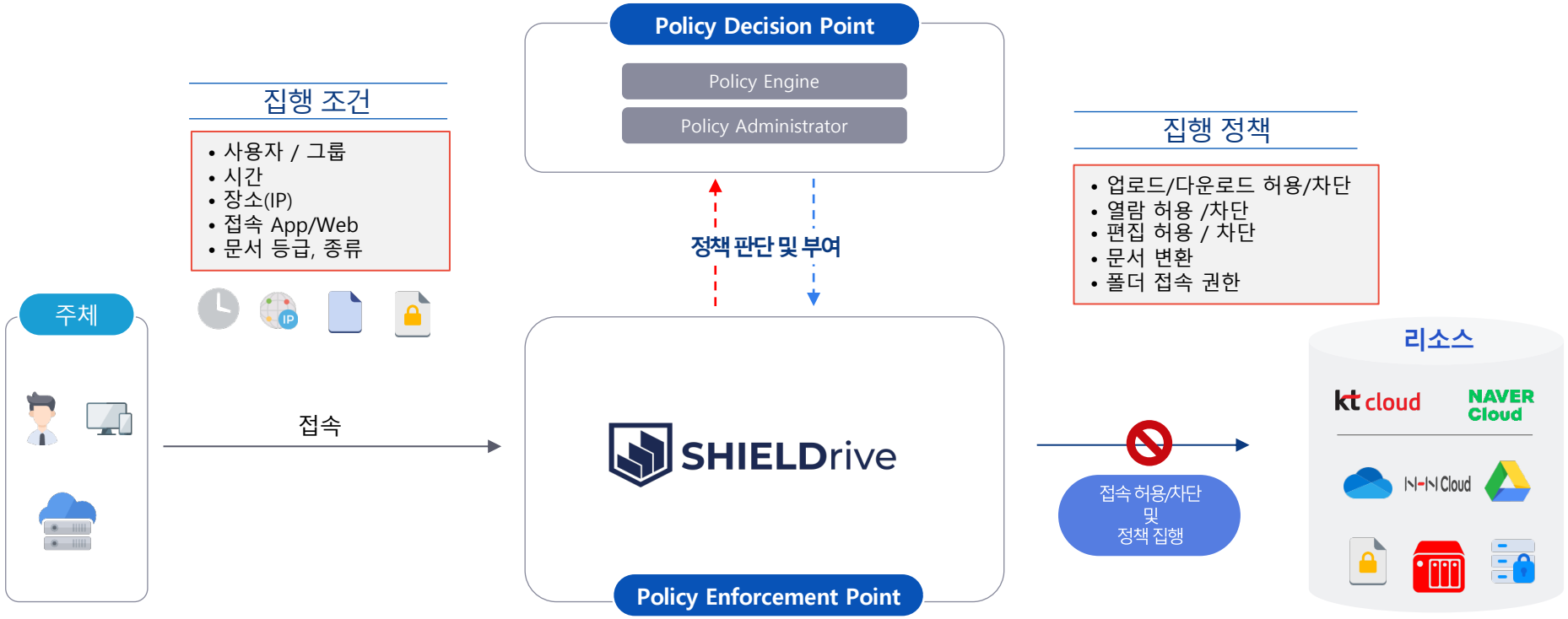


ⓒ SOFTCAMP Co., LTD. All rights reserved

Zero Trust Architecture Model 적용

› Zero-Trust Conditional Adaptive Policy에 따른 적응형 보안 정책 적용

› 상황에 따른 권한 및 정책 동적 적용 가능

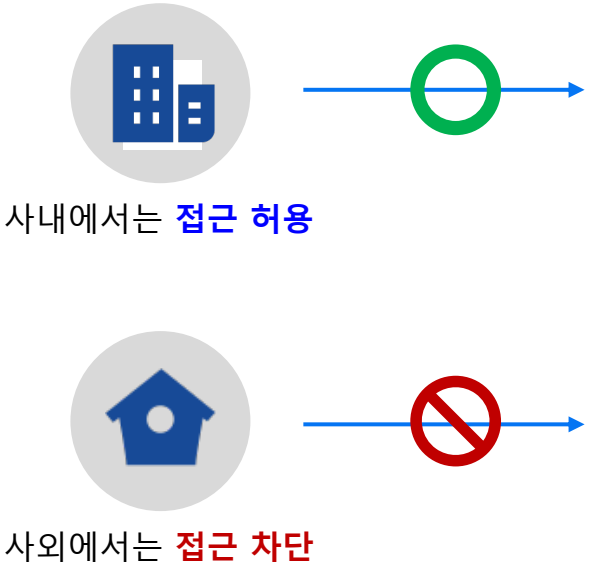


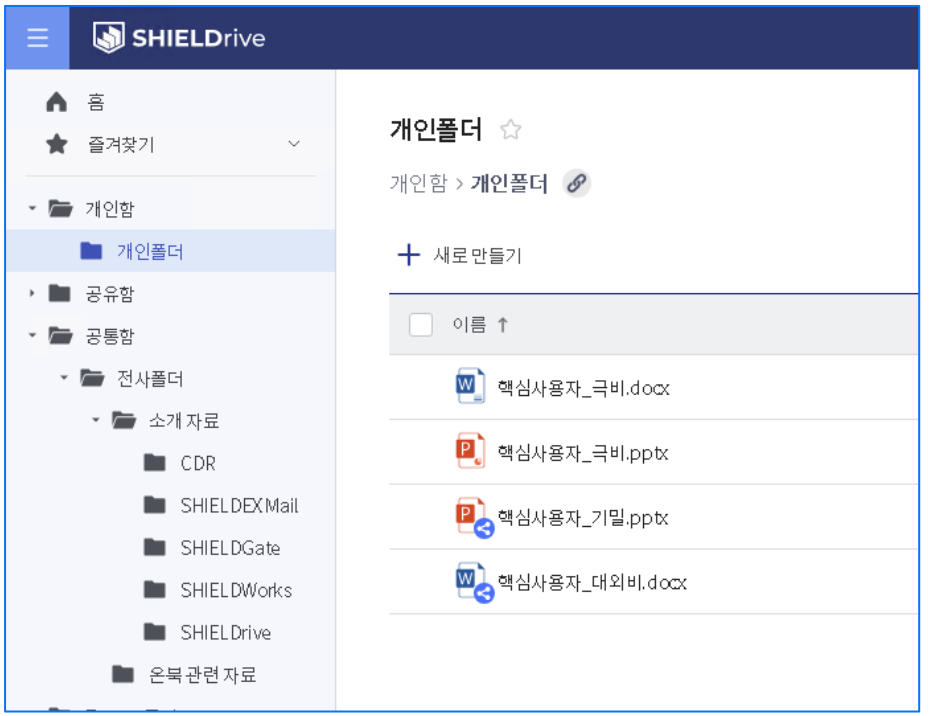
※ Zero Trust Architecture Model – NIST(미국 국립표준기술연구소)

© SOFTCAMP Co., LTD. All rights reserved

ZT-CAP 설정의 예제

› 스토리지에 저장된 파일은 사내에서만 사용되며, 사외에서는 접근을 차단할 수 있습니다.





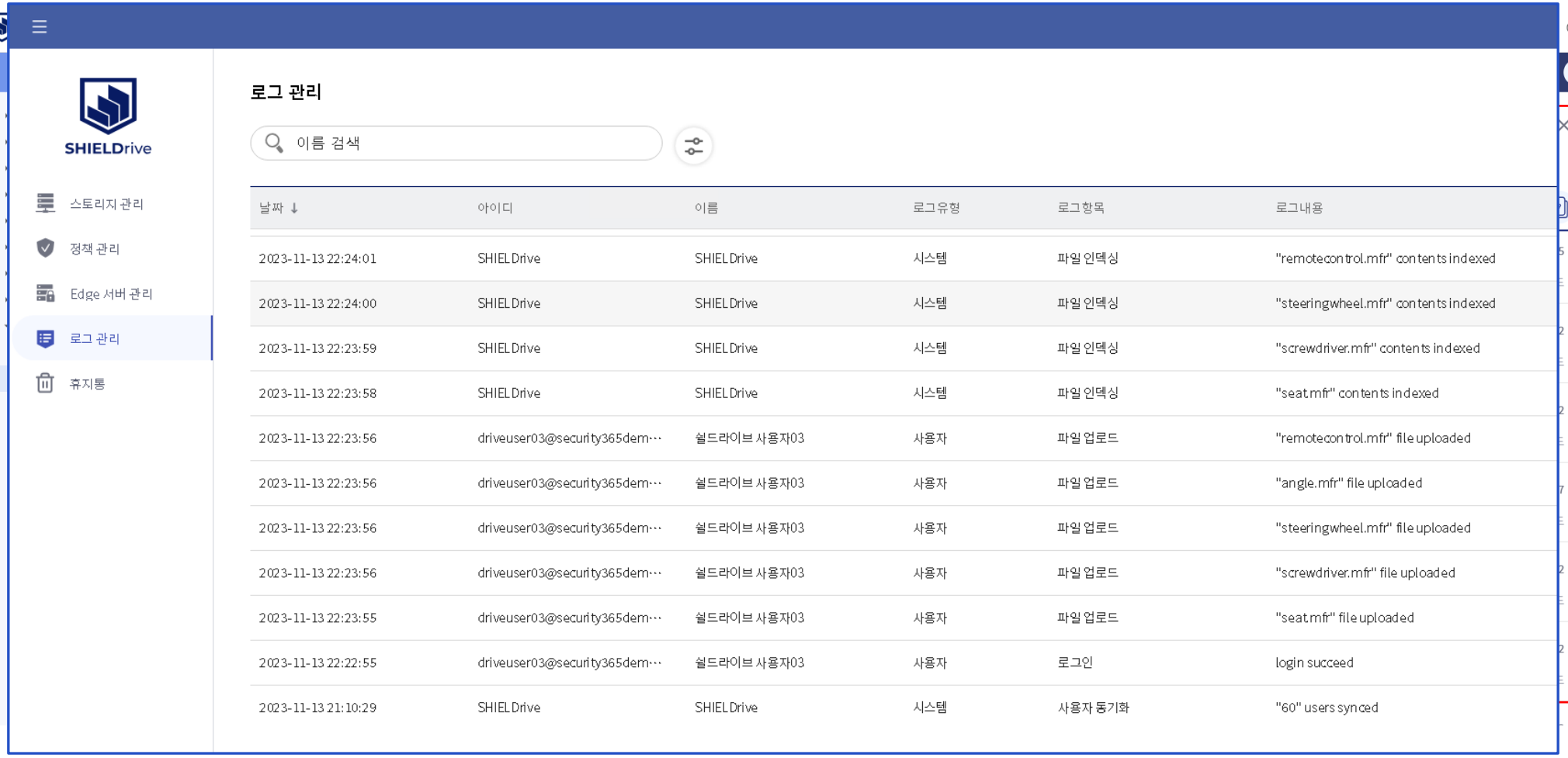
ZT-CAP 정책 적용으로 핵심기술 데이터의 사외 접근 차단 및 보안 유지

ⓒ SOFTCAMP Co., LTD. All rights reserved

Version 관리, 이력 조회

› 파일별 Version 관리 → 과거 파일 열람 / 편집 가능

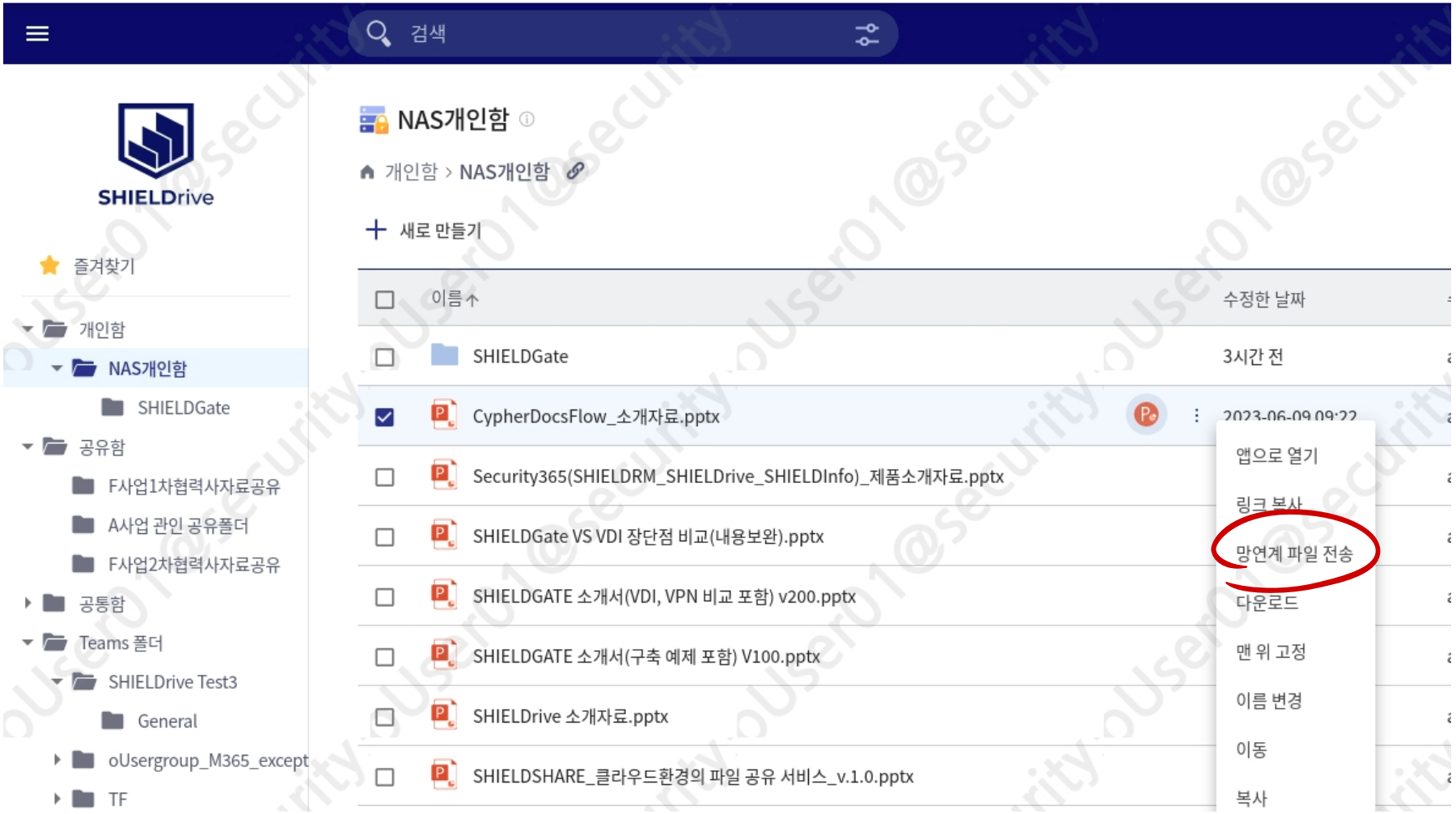
›파일 접속자 편집자 이력 조회



날짜 ↓	아이디	이름	로그유형	로그항목	로그내용
2023-11-13 22:24:01	SHIELDrive	SHIELDrive	시스템	파일 인덱싱	"remotecontrol.mfr" contents indexed
2023-11-13 22:24:00	SHIELDrive	SHIELDrive	시스템	파일 인덱싱	"steeringwheel.mfr" contents indexed
2023-11-13 22:23:59	SHIELDrive	SHIELDrive	시스템	파일 인덱싱	"screwdriver.mfr" contents indexed
2023-11-13 22:23:58	SHIELDrive	SHIELDrive	시스템	파일 인덱싱	"seat.mfr" contents indexed
2023-11-13 22:23:56	driveuser03@security365dem…	쉴드라이브 사용자03	사용자	파일 업로드	"remotecontrol.mfr" file uploaded
2023-11-13 22:23:56	driveuser03@security365dem…	쉴드라이브 사용자03	사용자	파일 업로드	"angle.mfr" file uploaded
2023-11-13 22:23:56	driveuser03@security365dem…	쉴드라이브 사용자03	사용자	파일 업로드	"steeringwheel.mfr" file uploaded
2023-11-13 22:23:56	driveuser03@security365dem…	쉴드라이브 사용자03	사용자	파일 업로드	"screwdriver.mfr" file uploaded
2023-11-13 22:23:55	driveuser03@security365dem…	쉴드라이브 사용자03	사용자	파일 업로드	"seat.mfr" file uploaded
2023-11-13 22:22:55	driveuser03@security365dem…	쉴드라이브 사용자03	사용자	로그인	login succeed
2023-11-13 21:10:29	SHIELDrive	SHIELDrive	시스템	사용자 동기화	"60" users synced

망 間 자료 전송

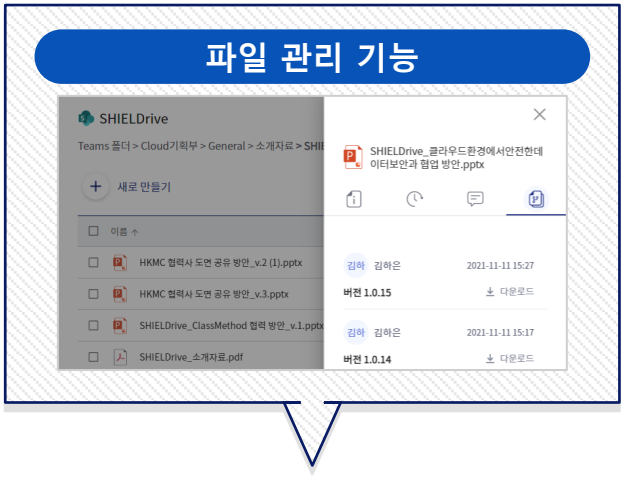
- 폐쇄망으로 자료 전송을 위한 망 연계 솔루션 연동가능
- Remote Browser Isolation 제품과 연동 가능

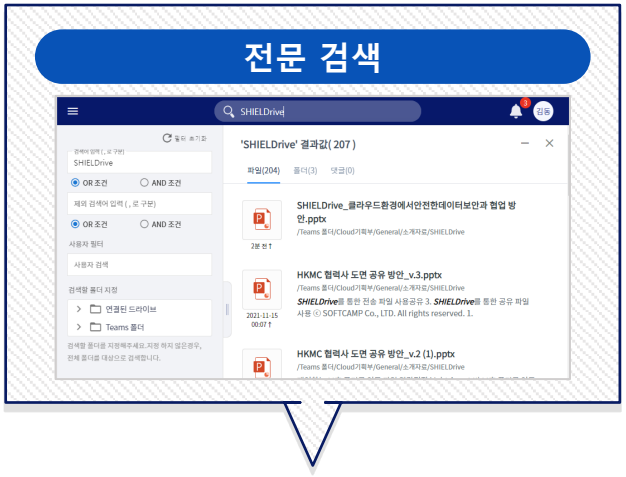


© SOFTCAMP Co., LTD. All rights reserved

부가 특징 – 검색 및 소셜 기능

- Storage Broker는 파일 관리 및 협업 기능을 제공
- 전문 검색 기능을 제공 합니다 ← 파일명, 본문 내용 검색 기능
- 파일 버전와 소셜 기능을 통해 조직 내 다른 구성원들과 협업
- 구독 기능을 통하여 폴더에 문서가 업로드 될 때, 문서가 편집될 때 알림 수신





파일 관리 기능

- **버전 이력관리**
  이전 버전 파일 내용 확인 가능
- **파일/폴더 활동 내역 확인**
  열람, 편집, 다운로드 등 확인 가능

전문 검색

- **전문 검색**
  모든 스토리지의 파일명, 본문 내용 검색 가능

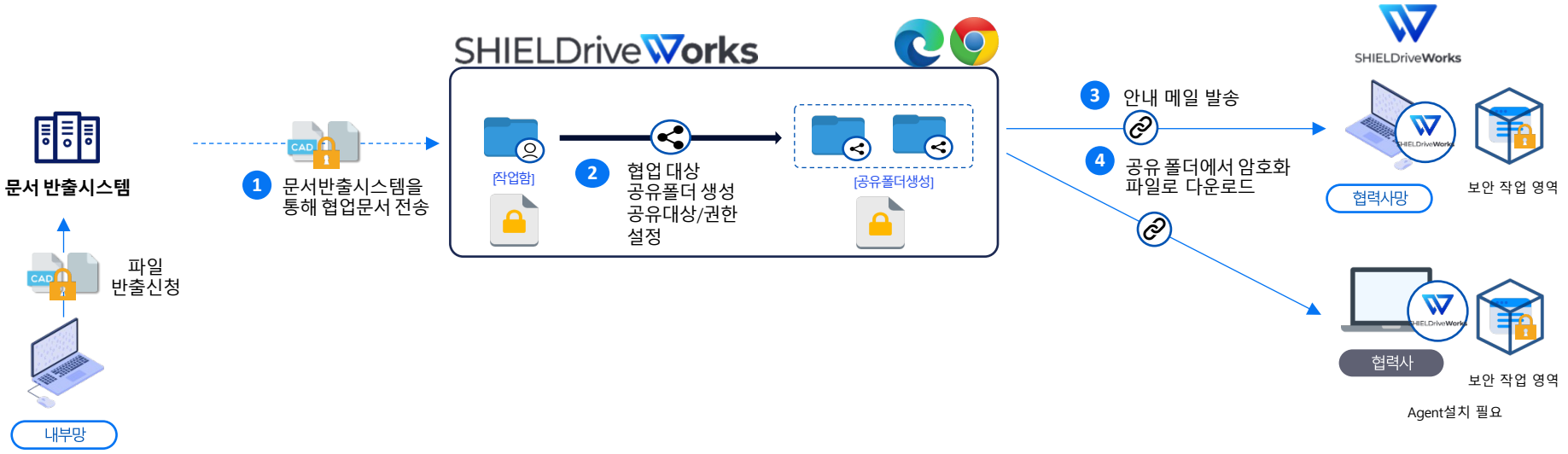
소셜 기능

- **댓글 기능**
  문서에 대한 댓글을 통한 의사소통
- **구독 기능**
  파일/폴더를 구독하여 파일/폴더 업데이트 시 알림을 주는 기능

ⓒ SOFTCAMP Co., LTD. All rights reserved

사외 협력사 문서 보안 공유 지원

- Storage Broker에서 협력사와 **파일/도면 등을 보안 강화 상태에서 안전하게 공유** 할 수 있습니다.
- 폐쇄망의 경우 반출시스템을 통하여 반출 할 수 있습니다



- 협력사 공유함 내 공유 폴더 및 공유대상/사용권한 설정. 공유할 개인함 내 파일은 생성한 공유 폴더로 이동/복사
- 추가된 사용자에게는 공유 폴더 링크가 메일로 발송
  * 폴더의 권한에 기 등록된 사용자가 아니면 초대 및 사용방법 안내 메일 발송하여 접속 요청
- 공유 폴더에서 다운로드 받은 파일(폴더명.SHW)은 **Aira로 암호화** – Agent 로그인 없이 오픈 불가

ⓒ SOFTCAMP Co., LTD. All rights reserved

협력사 문서 협업 Agent 주요 기능

로컬 파일 보안

- 로컬 PC 내 보안 작업 폴더 생성
- 보안 작업 폴더 외부로 파일 반출 차단
- 파일 ARIA 암호화 적용(도면, 문서 등 모든 파일)

Storage Broker 연계 기능

- 보안 다운로드(*.SHW) 파일 실행 시 보안 작업 폴더 자동 생성
- 보안 작업 폴더 내 파일 사용 시 공유 폴더 사용 권한 동기화

Slim Agent

- **윈도우 기본 탐색기 사용 가능** (반입 허용, 반출 차단)
- 기본 보안 기능 제공(Screen Watermark, Print Watermark)

파일 반출 차단

- 인가된 웹 사이트(Storage Broker) 이외 업로드 차단
- 일반 폴더로의 반출/복사/드래그 등 차단
- 기간 경과 시 접속 차단, 회수[삭제] 기능

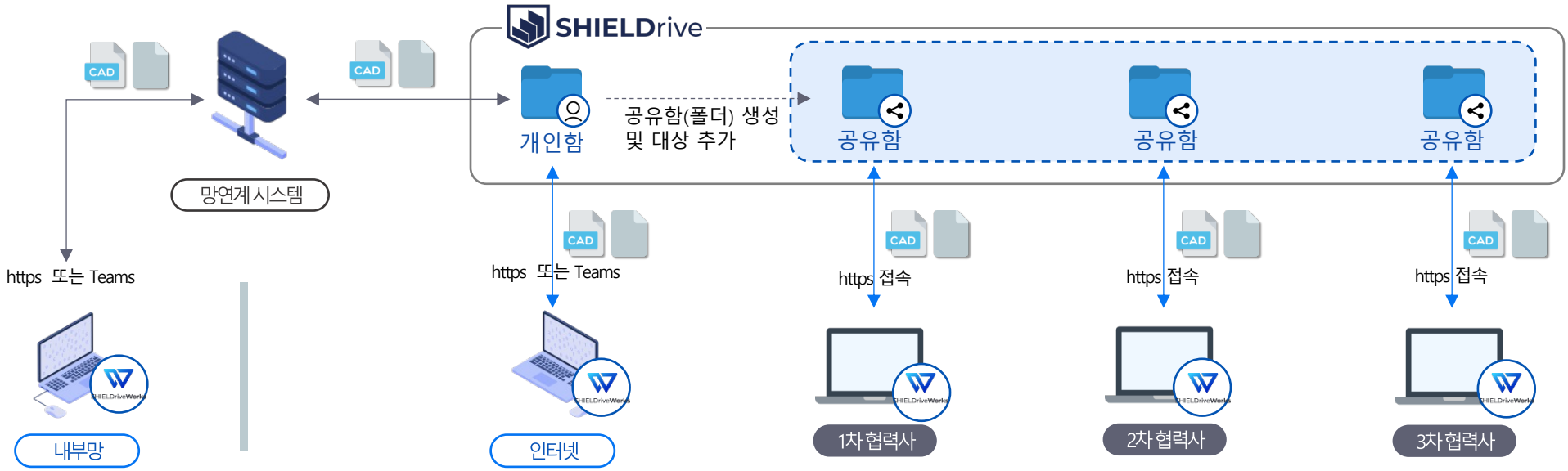
조건부 액세스

- 사용자 접속 시 접속 환경에 따른 사용권한 제어
  * 접속 IP대역, 시간에 따른 로그인 차단 및 권한(다운로드 등) 제어

ⓒ SOFTCAMP Co., LTD. All rights reserved

협력사 문서 흐름도

› 새로운 파일 협업시스템에서는 모든 사용자가 Storage Broker를 통해 문서/도면을 유통합니다.
Local PC에는 Agent를 설치하여 문서/도면에 대한 보안을 제공합니다.



문서 흐름

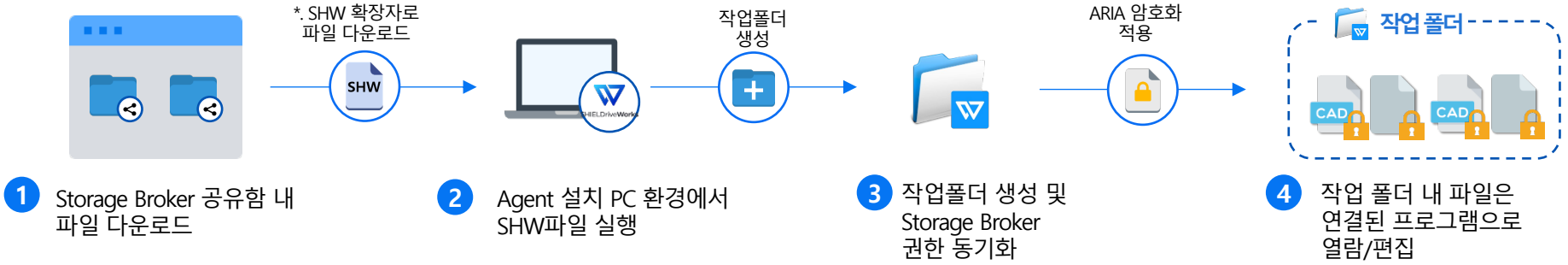
- 폐쇄망의 경우 내부망 내 문서/도면은 망 연계 시스템을 통해 Storage Broker 개인함으로 전달
- 인터넷망 사용자는 Storage Broker 공유함(폴더) 생성 후 1~N차 협력사 사용자에게 공유
- 문서/도면 다운로드 후 사용 시에는 Agent을 통해 파일 보안

➔ **인터넷망 데이터 유통 시 보안 적용 및 유통 경로 추적**

ⓒ SOFTCAMP Co., LTD. All rights reserved

WorkFlow – 다운로드 및 파일 사용

› Storage Broker 공유함에서 파일 다운로드 시 *.SHW 확장자로 보안다운로드(암호화된 상태)가 진행됩니다.
Agent가 설치된 PC에서 더블클릭 시 보안 작업 폴더가 생성되며, **파일이 ARIA로 암호화** 됩니다.



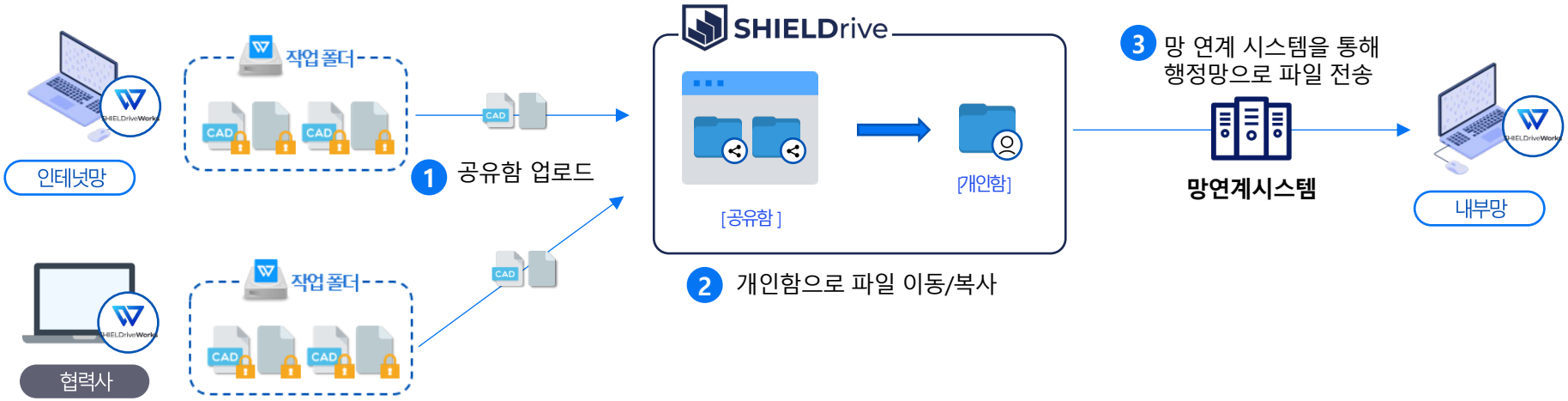
① 협력업체 사용자는 Storage Broker 공유 파일 다운로드. 다운로드 시 *.SHW 확장자로 파일 다운로드
② SHW 파일은 Agent 설치 환경에서만 오픈(실행) 가능. 미 설치 환경에서는 오픈 불가.
③ *.SHW파일 더블 클릭 시 공유 폴더 명으로 작업 폴더 생성 및 Storage Broker 폴더 권한과 권한 동기화
④ 작업 폴더 내에 공유 폴더의 문서가 저장되며, 파일 저장 시 ARIA 암호화 적용.
ARIA 암호화 적용 상태에서 연결된 프로그램으로 열람/편집

* 작업폴더 내 파일은 비 작업 폴더 이동/복사 및 Storage Broker 외 사이트로 업로드 자동 차단

ⓒ SOFTCAMP Co., LTD. All rights reserved

WorkFlow – 파일 재 전송(upload)

› 보안 작업 폴더에서 편집/수정된 파일을 원청사에 재 전송하고자 할 경우 Storage Broker에 업로드 가능하다.
› 탐색기에서 작업 폴더 마우스 우 클릭 또는 Agent 메뉴에서 업로드 할 수 있다.



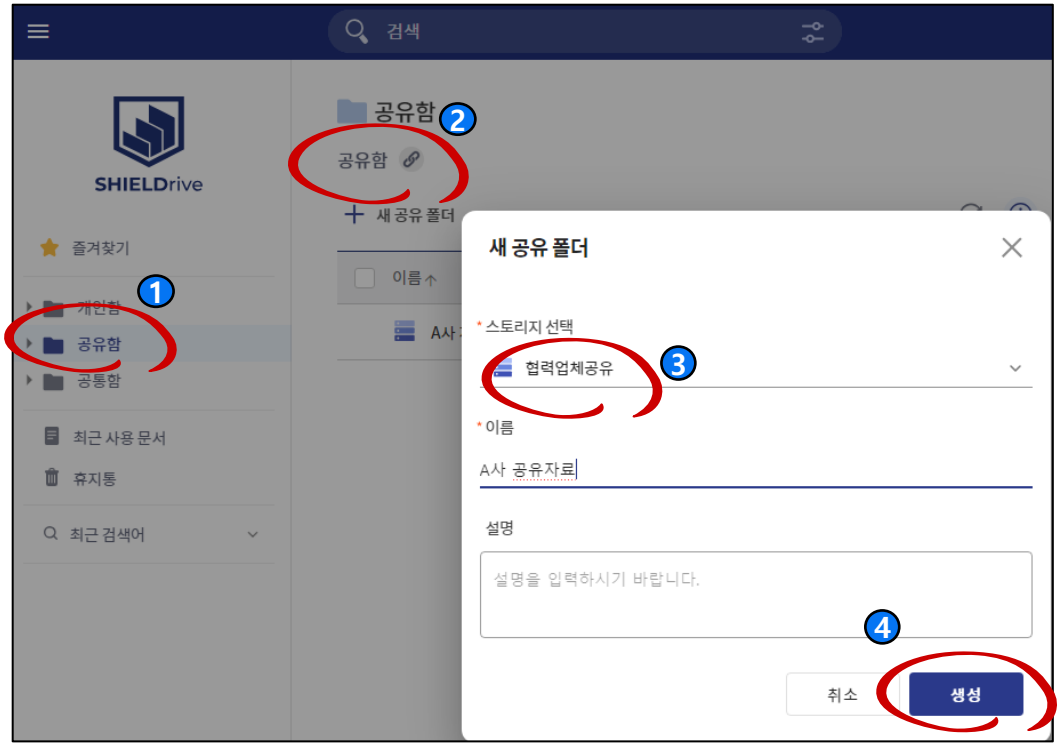
① 작업이 완료된 작업 폴더 내 파일은 Agent에서 제공하는 업로드 기능을 통해 Storage Broker 공유함에서 취합(Upload)
② 공유함에서 취합된 파일은 내부망 등 사내 파일서버 등으로 이동할 수 있다
③ 개인함으로 이동하여 망연계시스템을 통해 내부망으로 파일 전송 가능하다

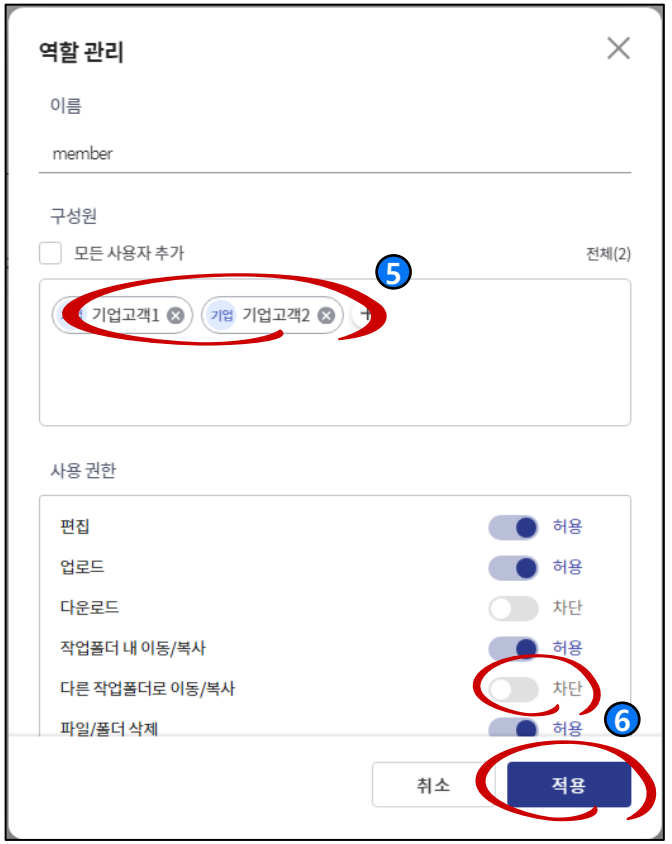
- 폐쇄망에서 공유함 내 파일을 자동으로 내부망 전송해야 할 경우 API 지원.

ⓒ SOFTCAMP Co., LTD. All rights reserved

사용방법 예제-외부 자료공유 (1)

- '공유함'에서 '공유 폴더'를 생성하고 공유대상/권한을 설정합니다.
- 역할관리에서 외부 협력사 '구성원'을 추가하고, 사용권한 및 사용기간을 설정하고 '적용'을 누릅니다.
- 기 등록된 협력사를 추가 하거나 신규 협력사일 경우 메일주소를 등록 합니다.
- 공유대상으로 지정된 협력사에는 안내 메일이 자동으로 발송 됩니다.(최초 협력사는 가입 안내 포함 메일 발송)





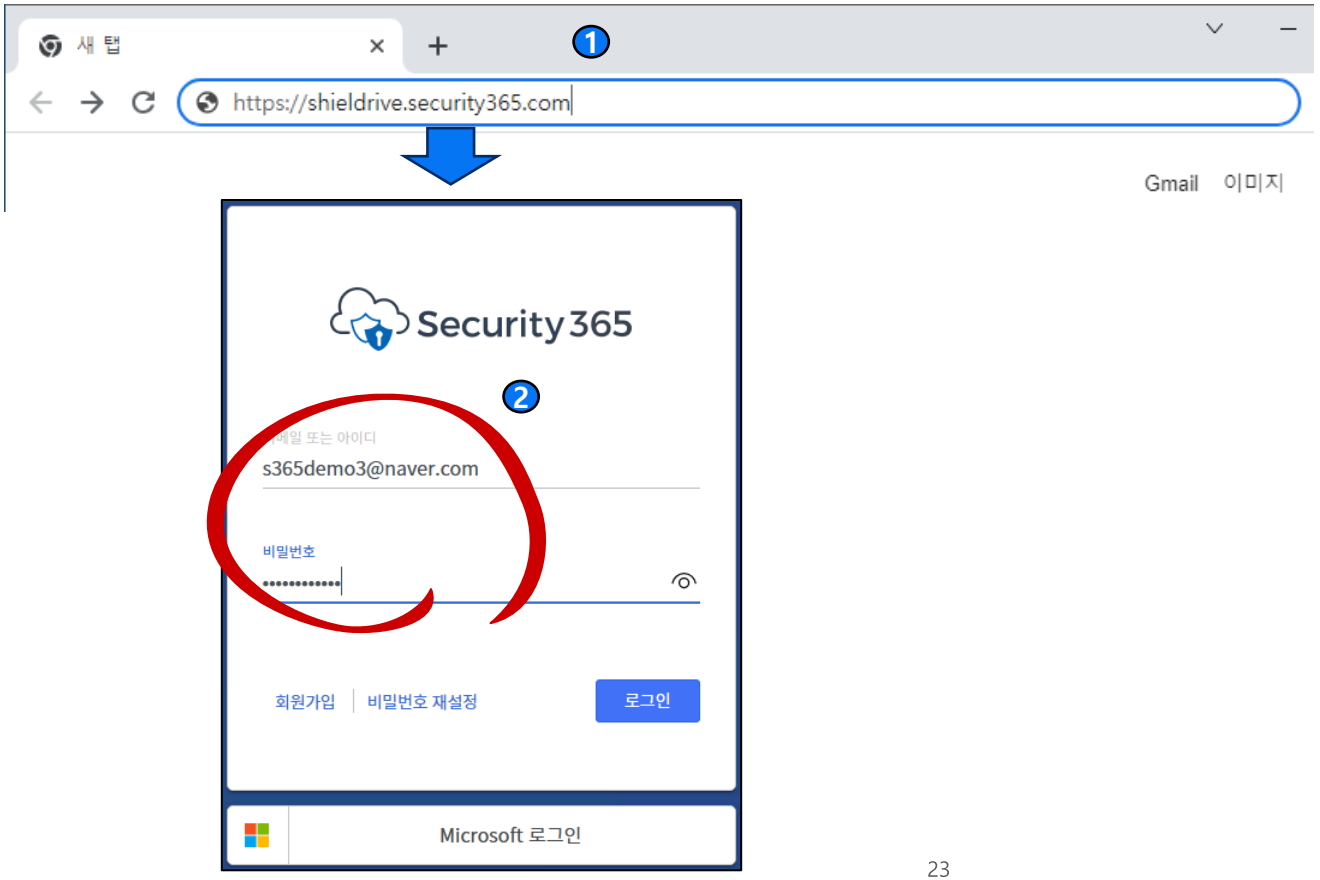
ⓒ SOFTCAMP Co., LTD. All rights reserved

사용방법 예제- 협력사 사용자 | 로그온

› 인터넷 브라우저(Edge 또는 Chrome)에서 https://shieldrive.security365.com 에 접속 한다

› 협력사 사용자 계정 (이메일 주소)으로 로그인 합니다.

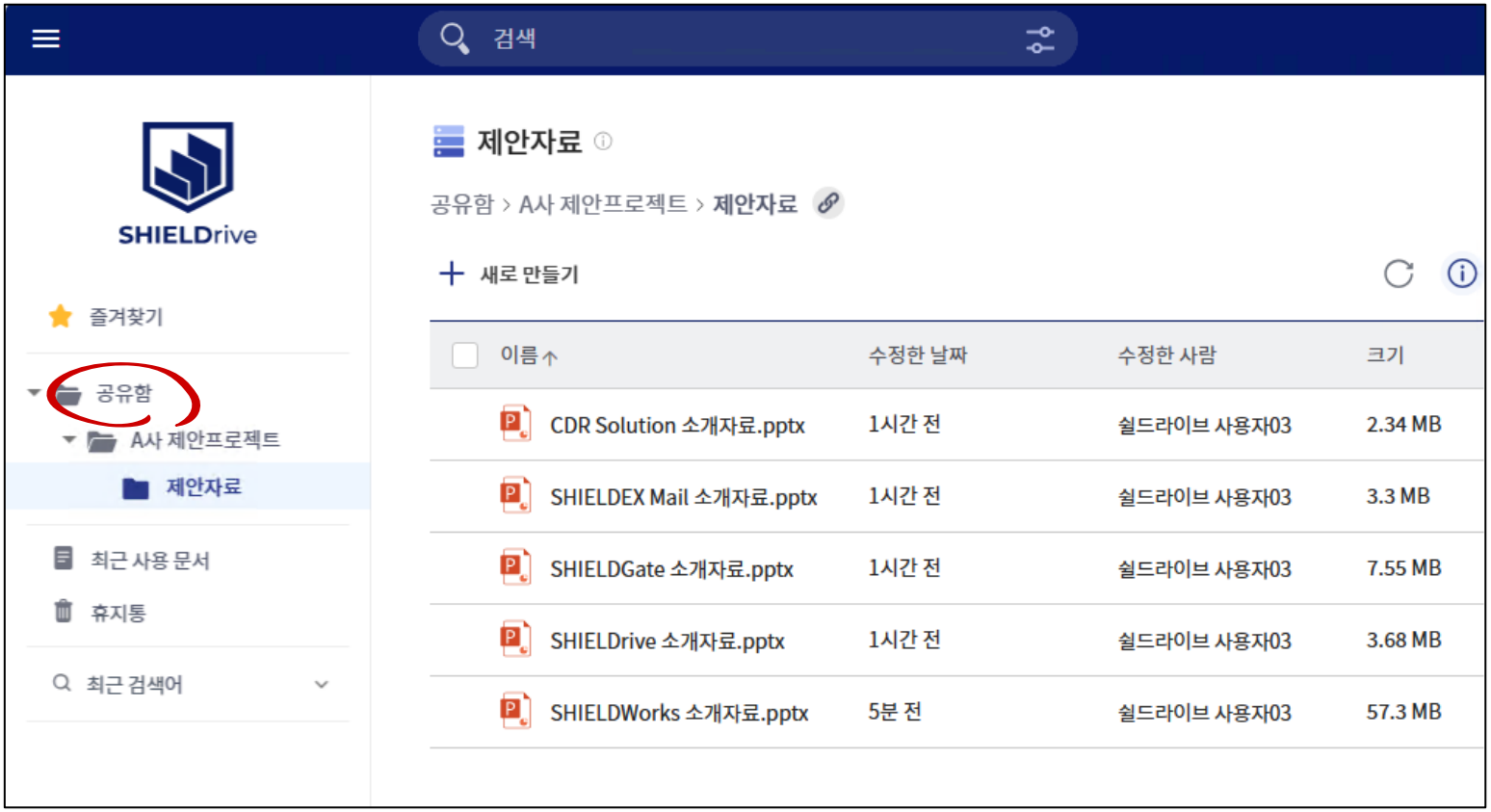
* 최초 사용 협력사는 이메일로 수신한 비밀번호로 로그인하고 비밀번호 재설정을 통하여 비밀번호 변경이 가능 합니다.



ⓒ SOFTCAMP Co., LTD. All rights reserved

사용방법 예제- 협력사 사용자 | 문서 확인

- 협력사 사용자가 Storage Broker에 로그인을 하면 권한이 부여된 '공유 폴더'가 확인 됩니다.
- 공유된 자료가 오피스 문서일 경우 다운로드 없이 직접 웹이나 앱으로 문서를 열람/편집 이 가능합니다.

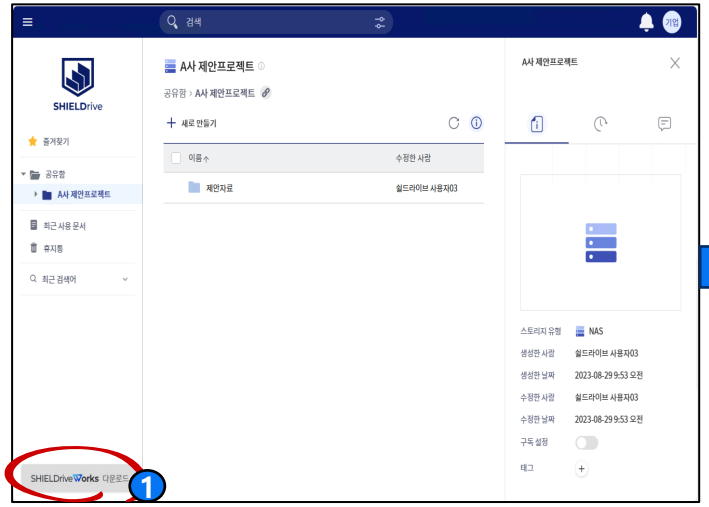


© SOFTCAMP Co., LTD. All rights reserved

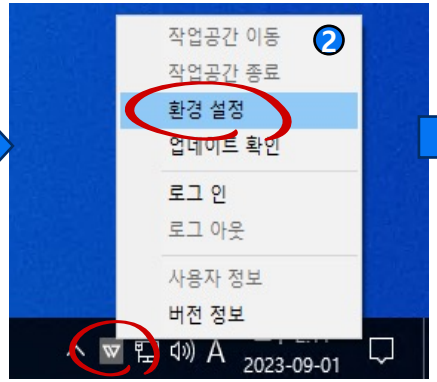
사용방법 예제- 협력사 사용자 | Agent 설치

› 공유된 문서를 PC 에 다운로드 받아 작업을 하기 위해서는 Agent 설치가 필요합니다.

› Agent는 1회만 설치하면 되며 로그온/오프로 제어 가능 합니다.



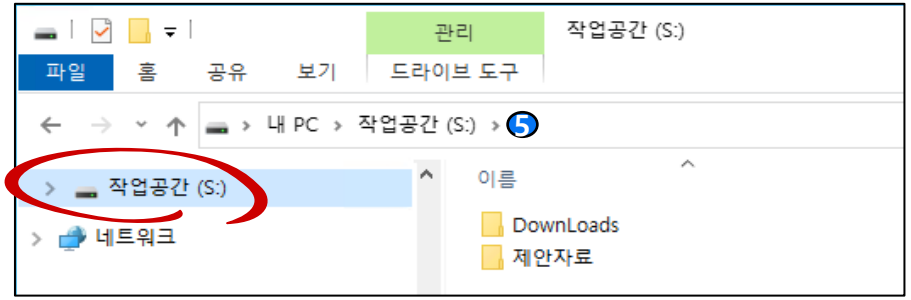
1. Storage Broker 웹화면에서 Agent 를 다운받아 설치



2. Agent 아이콘>우클릭>환경설정

3. 환경 설정(협력사가 설정할 필요는 없음)
(Tenant ID 와 Application Token는 고객사별로 확인 필요)

4. 로그인 확인
(파란색 아이콘 변경)



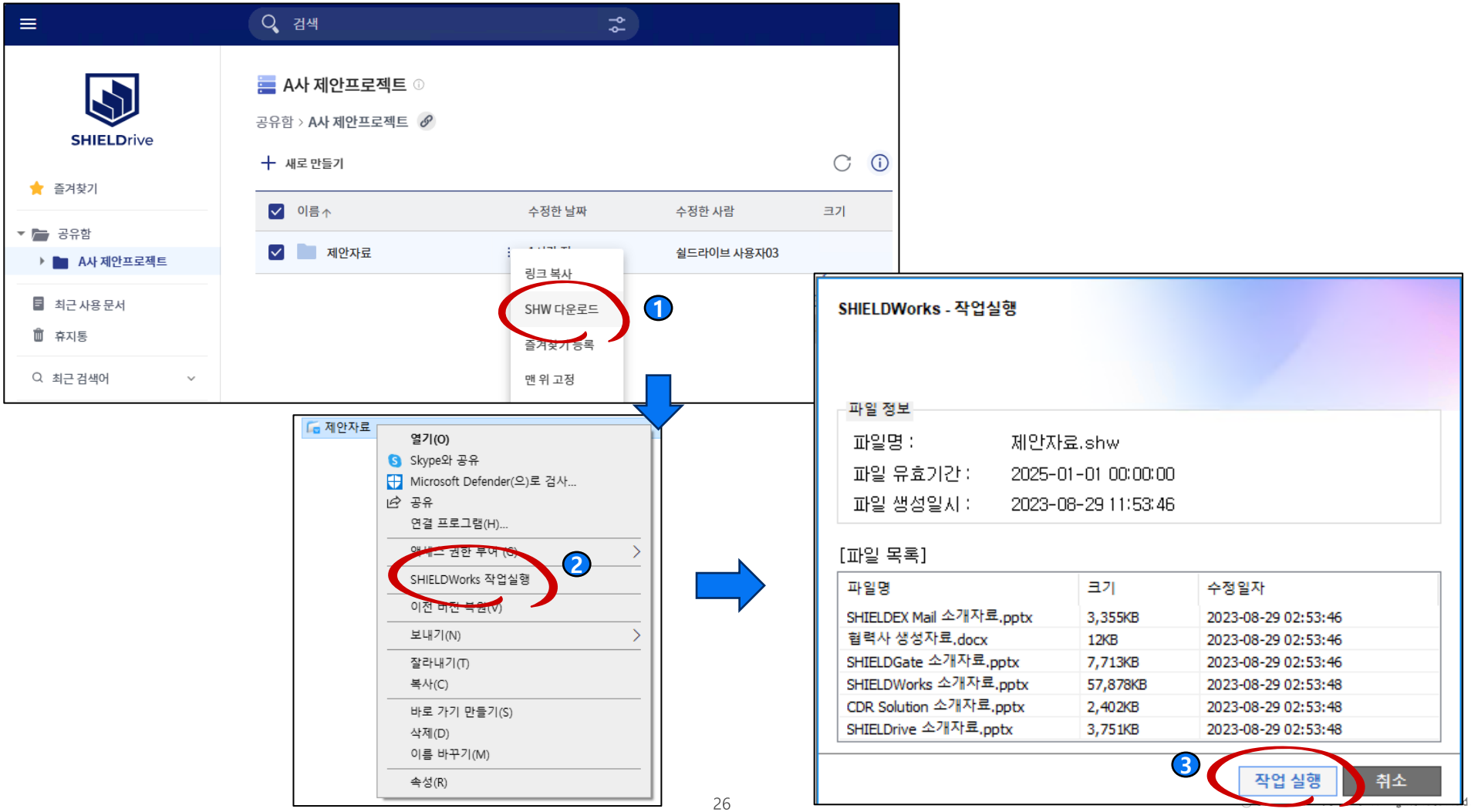
5. 탐색기에서 작업공간(S) 확인

ⓒ SOFTCAMP Co., LTD. All rights reserved

사용방법 예제- 협력사 사용자 | 자료 다운로드

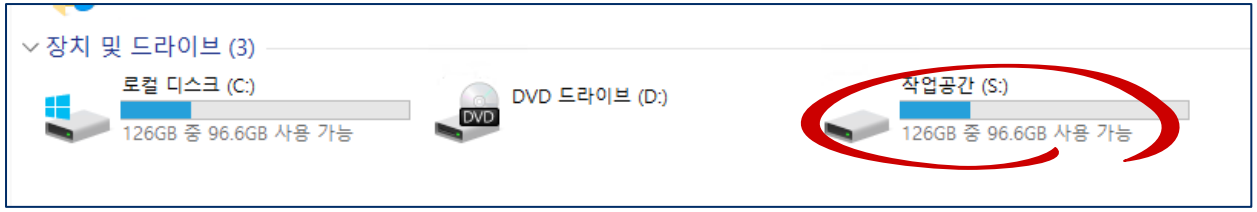
› 공유된 문서를 PC 에 다운로드 받으려면 '공유함' 내에 프로젝트명을 선택하고 'SHW 다운로드' 메뉴를 선택합니다.

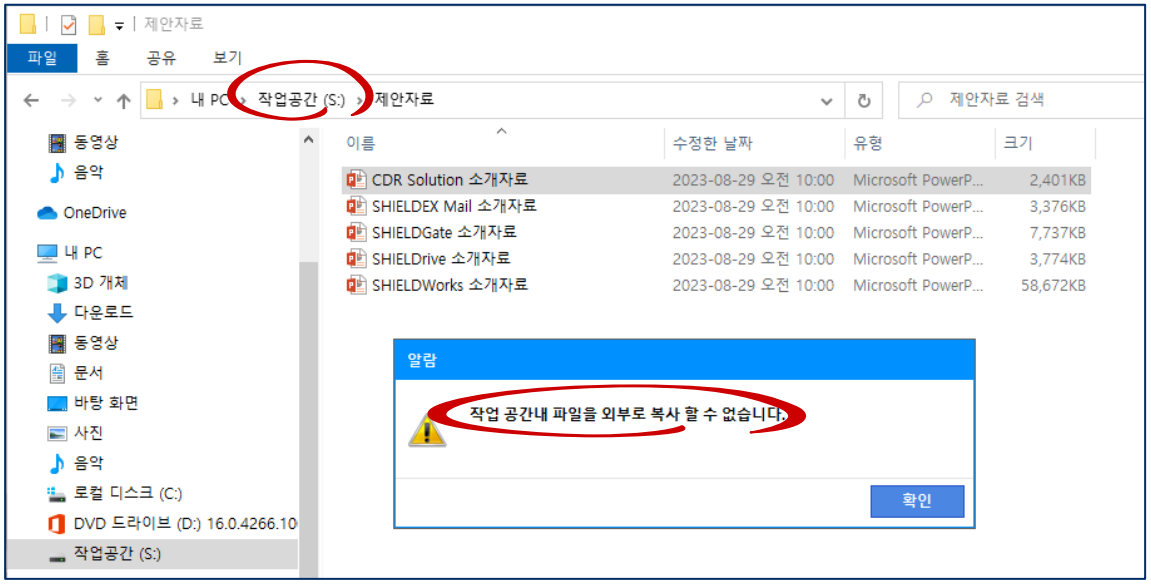
› 다운받은 SHW 파일은 '작업실행'[또는 더블클릭]을 통해서 보호된 보안영역에 문서가 자동으로 저장되고 작업할 수 있습니다.

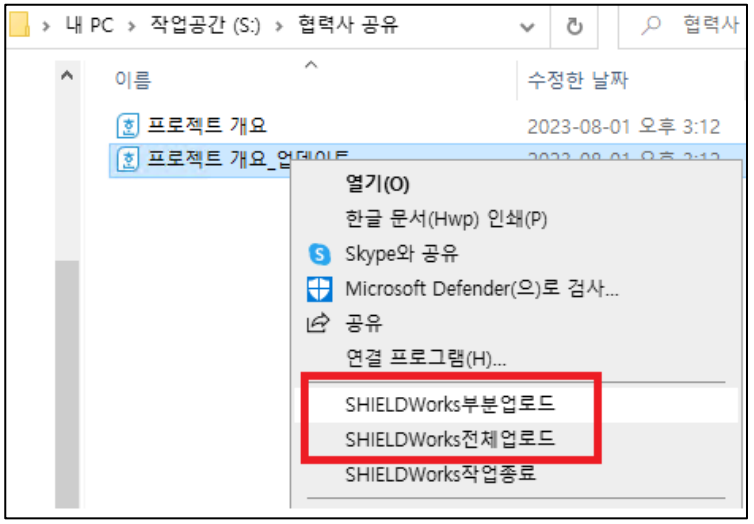


사용방법 예제- 협력사 사용자 | 자료 보호

- '작업공간' 영역은 Windows 탐색기 등을 통하여 접근이 가능 합니다
- 다운로드 받은 자료는 '작업공간' 이외의 공간으로 이동/복사가 불가능 합니다.
- CAD/CAM/CAE 등 대부분의 **도면 작업용 Application을 사용**할 수 있습니다.(유출 차단)
- 작업영역에서 편집된 자료는 '부분업로드', '전체업로드'를 통해서 원청사 공유자에게 회신할 수 있습니다.



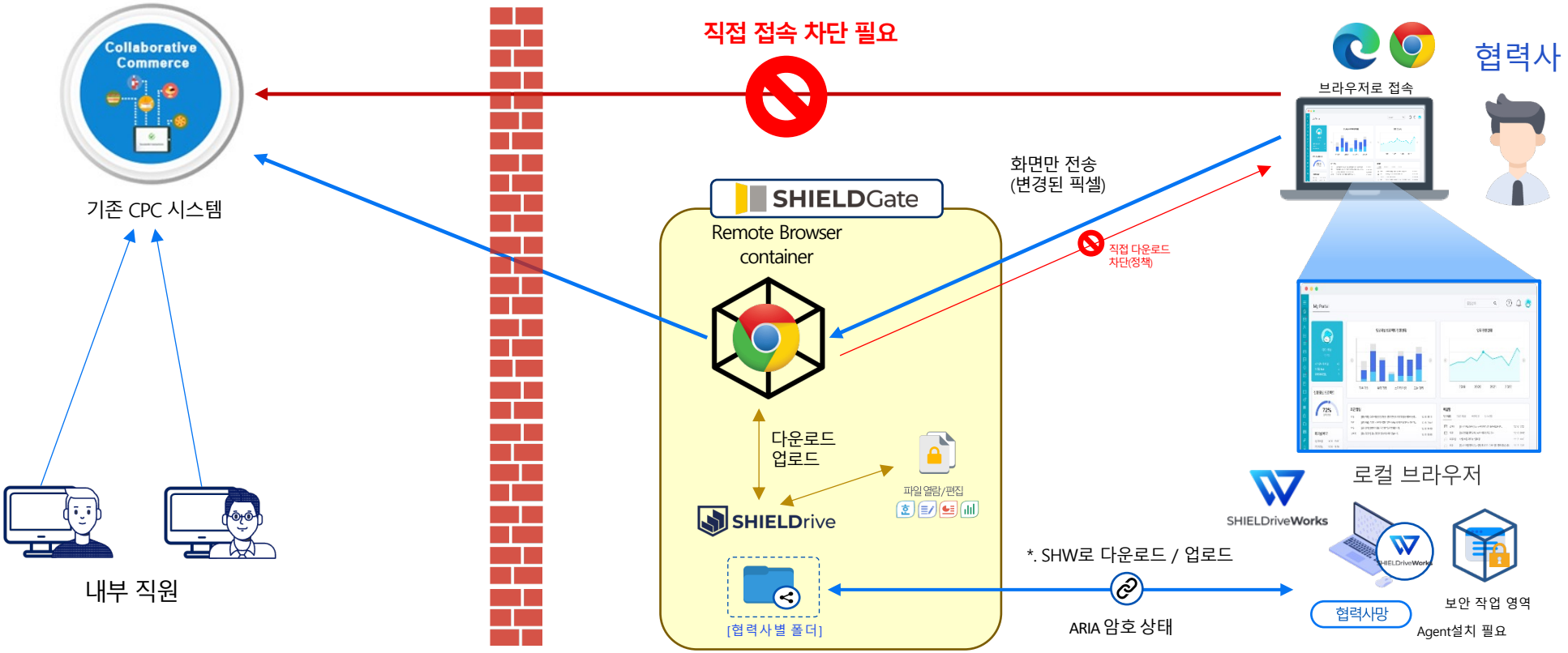




© SOFTCAMP Co., LTD. All rights reserved

기존 협력사 협업 시스템과 연계 사용

- CPC 등 기존 사용중인 협력사 협업 시스템을 수정 없이 보안 강화하여 적용이 가능 합니다
- 내부 직원은 기존과 동일하게 사용하고, 협력사는 RBI를 통하여 접속 후 보안 적용



- 기존 CPC 시스템 수정없이 협력사에 보안이 강화된 문서 협업이 가능
- RBI 기술이 적용되어 보다 보안이 강화된 환경으로 운영이 가능
- RBI 제품은 SaaS형으로 사용 가능하다

※ CPC : collaborative product commerce 협업적 제품 상거래, RBI : Remote Browser Isolation

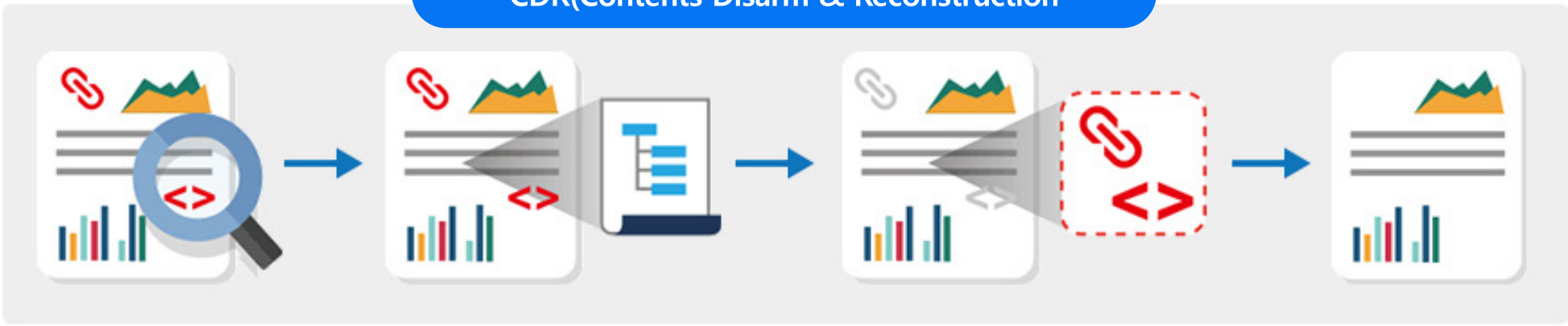
ⓒ SOFTCAMP Co., LTD. All rights reserved

외부 유입 문서 무해화 처리 - CDR기술

SHIELDEX File

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

© SOFTCAMP Co., LTD. All rights reserved

이메일 문서 보안 오케스트레이션(수신)

SHIELDEX Mail

이메일 격리 시스템

이메일의 본문, 첨부파일, URL링크의 위협요소를 필터링하여 재구성 및 격리

서비스 특징

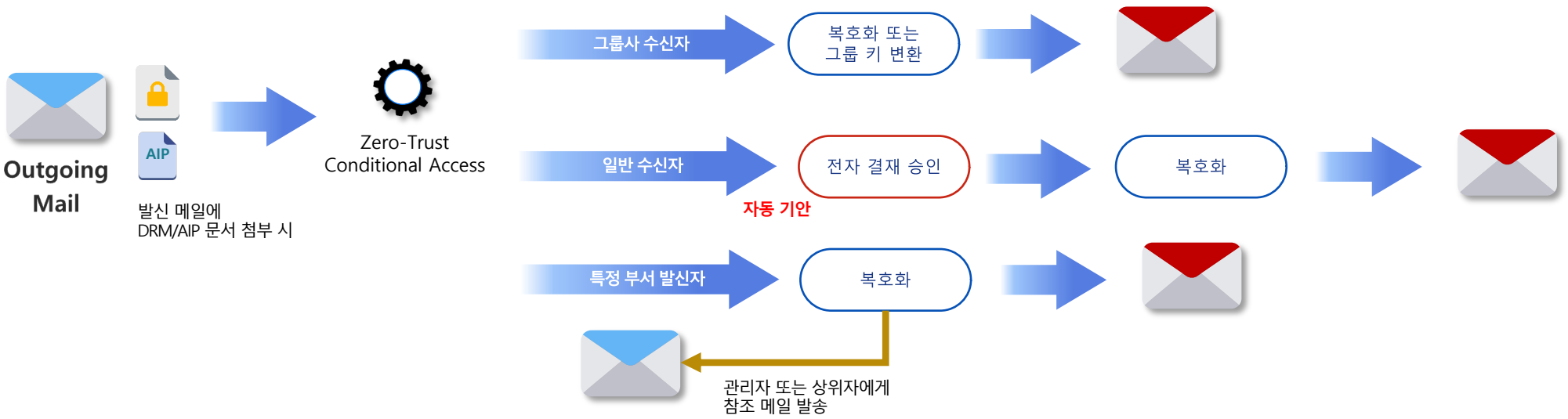
- 이메일 **본문**에 포함된 Content의 무해화 처리(HTML 방식의 Body에서 스크립트 등 제거)
- 첨부 파일 무해화, **URL Link는 Remote Brower를 통하여 접속**(PC로 부터 격리하여 클라우드에서 접속)
- 본문에 포함된 이미지 표출용 URL 또는 미디어 파일에 대한 무해화 처리(스테가노그래피 방어)

© SOFTCAMP Co., LTD. All rights reserved

이메일 문서 보안 오케스트레이션(발신)

SHIELDMail

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



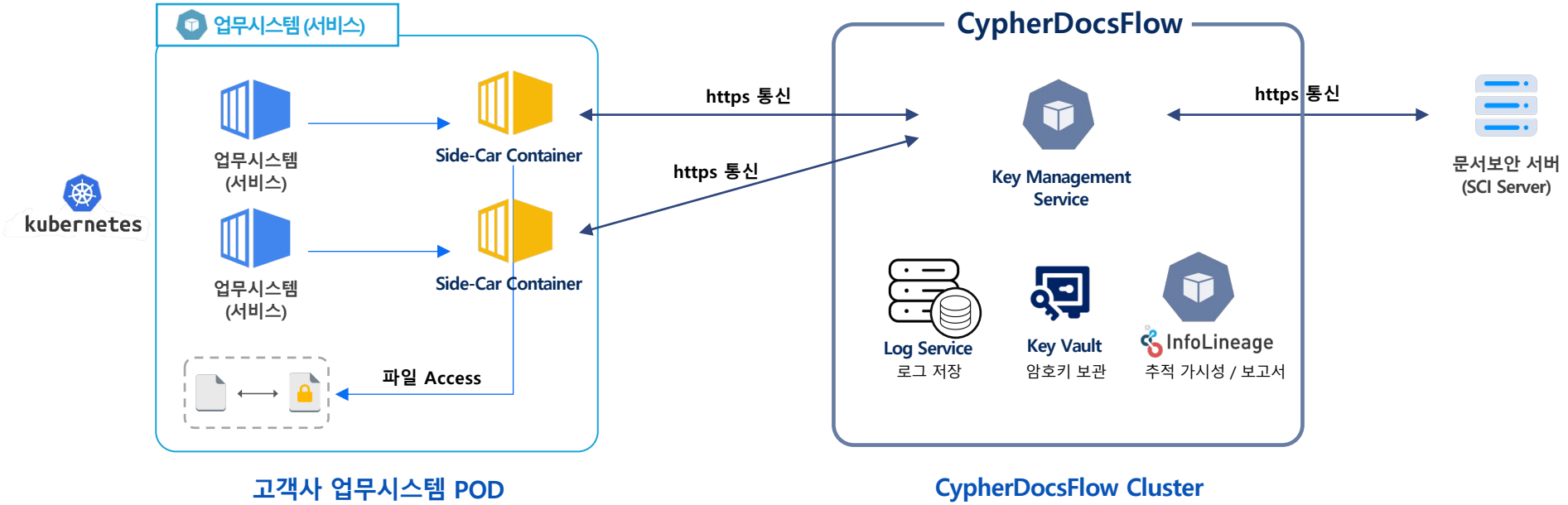
서비스 특징

- 사전에 DRM **해제 결재 신청이 필요하지 않음**
- PC에 암호 해제된 문서가 존재하지 않음
- **보낸 편지함 메일에 암호해제 문서가 존재하지 않음**
- 수신/참조가 여러 명 이라도 각각 수신자에 대한 정책 적용

ⓒ SOFTCAMP Co., LTD. All rights reserved

클라우드 네이티브 어플리케이션 문서 보안 지원

CypherDocsFlow



서비스 특징

- **고객사가 업무시스템을 Kubernetes 환경으로 전환 시 문서 암호화 API 지원**
- 고객사 업무시스템 Kubernetes POD 내 Container 구성(Side-Car Container)
- 별도 Kubernetes Cluster 구성하여 암 복호화 기능 지원

© SOFTCAMP Co., LTD. All rights reserved

www.softcamp.co.kr

THANK YOU

ⓒ SOFTCAMP Co., LTD. All rights reserved.

SOFTCAMP

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