

원-플랫폼 전사 통합 문서보호 솔루션



시큐어존

목차

1

개요

2

제품 소개

3

특장점

4

주요기능

5

구축사례

6

도입효과

7

레퍼런스

8

회사 소개

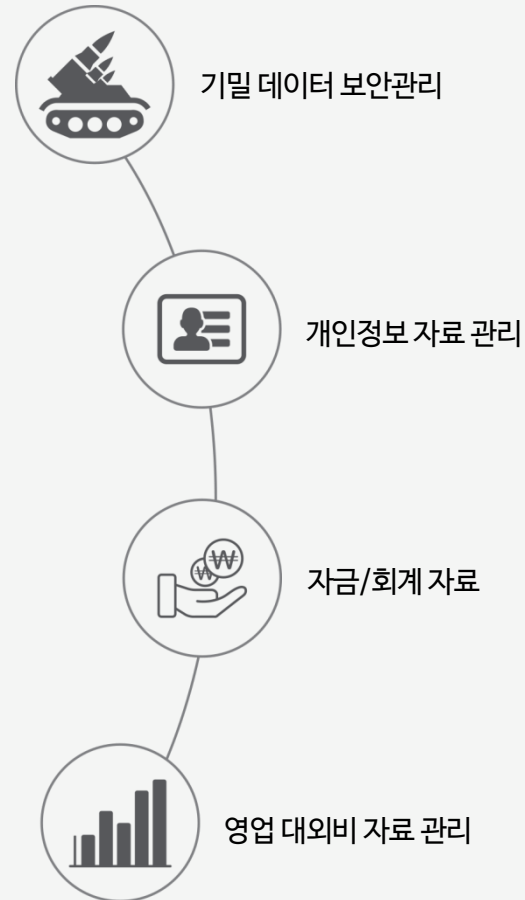
“문서 유출과 문서 유실 문제? 경영진과 IT부서의 2가지 고민”

[문서 유출(Leak) 문제]

- 중요자료 내부자 유출
- 외부 반출 문서 유출
- 협력사에 의한 유출

[문서 유실(Loss) 문제]

- HDD장애 등 IT재해
- 퇴직자 고의 삭제
- 랜섬웨어 암호화 등



개요 - 문서보안 현황 및 도입의 필요성

「개인정보 보호법」 31조 2항 4호

- 개인정보 보호책임자의 의무: 개인정보 유출 및 오용과 남용 방지를 위한 내부통제시스템 구축
- 내부직원 및 협력업체에 의한 개인정보 유출사고 발생
- 랜섬웨어 등 치명적 사이버공격 증가 및 IT재해 대비의 필요성 증가

외부
요인



[검토요인]

내부
요인

- 도면, 회계문서 등 회사 중요자료 내외부 유출경로에 대한 통제방안 마련
- 현행 문서보안 관리의 한계 존재

[고객 문서보안관리 현황]

- 개인정보 검색 및 개인정보 관리 부재
- 의도를 가진 내부 사용자의 외부 유출을 막지 못함
- 사용자 PC에 대한 백업시스템 미비로 인해 랜섬웨어 등 PC 장애시 데이터 유실 가능
- 개인정보 및 기업정보의 유출시 차단 및 방지 불가능
- 문서 외부 반출시 통제수단이 존재하지 않음 (기간 및 유통통제, 결재수단 미비)

[이노티움의 제안]

데이터 유출방지

내부 DRM + DLP

기업 내부종사자의 고의(故意) 또는 과실(過失)에 의해서 유출 · 개량 혹은 권리가 없는 자가 액세스하는 것을 원천 차단할 수 있어야 한다.

외부(반출협업) DRM

현직원의 출장, 지사, 협력업체 등 중요문서의 외부 열람, 공유, 협업을 자유롭게 지원하며 외부 유출 시에도 차단 및 추적이 가능하여야 한다.

데이터 유실방지

보안 백업(문서중앙화)

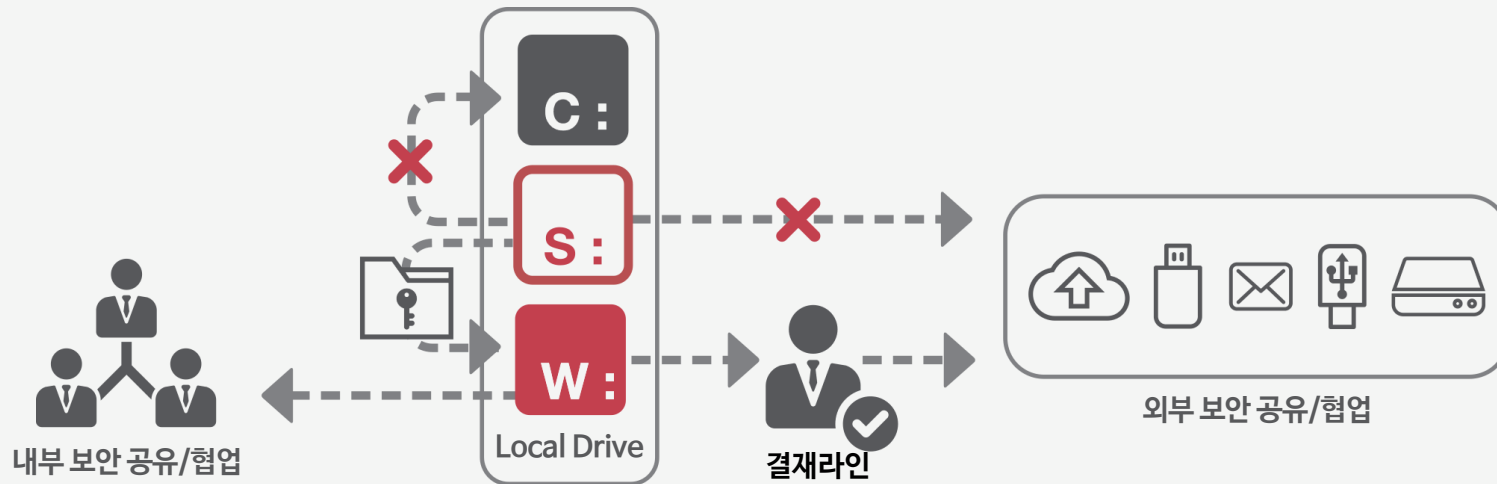
사이버 위협, 유실 및 유출 가능성, 보안기술의 한계, 천재지변 등으로부터 안전을 확신할 수 없어 파일기반의 물리적 또는 원격 소산백업 환경을 갖추어야 한다.

Anti-Ransomware(Malware)

‘네트워크단 방어, 엔드포인트단 차단 및 보안백업/복구’ 등의 3중 방어 기술을 융합하여 어떠한 신종 및 변종 랜섬웨어 공격에도 데이터를 안전하게 보호하여야 한다.

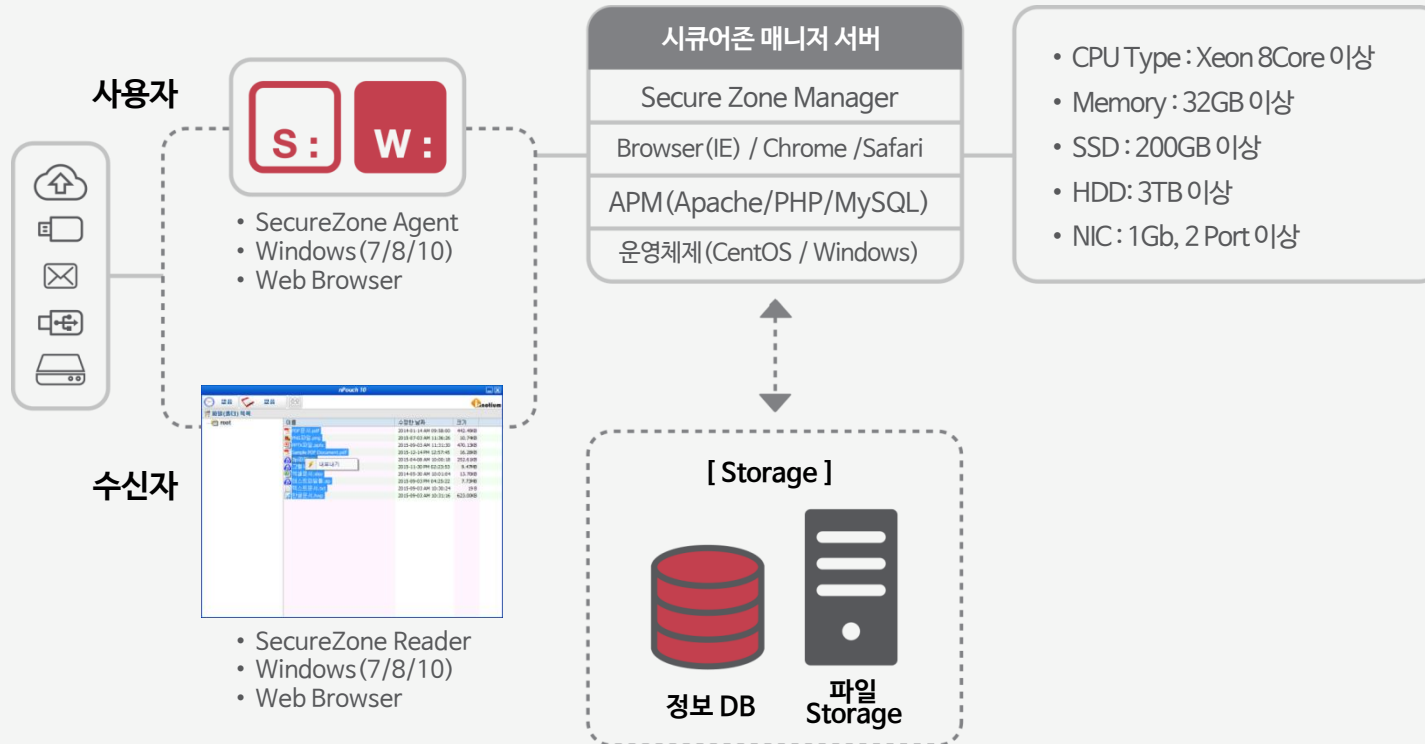
제품 소개 - 엔파우치 시큐어존

[DRM/DLP Convergence]



- 사용자 PC의 로컬 디스크에 보안영역(S:)과 반출영역(W:)을 생성, 기업의 중요 정보자산을 **사용/협업/보호/반출추적**
- 보안영역(S:)의 데이터는 저장소 내에서만 사용되며 여타 매체로 저장, 사본저장, 이동, 화면캡처, 전송 불가
- 내부 협업 또는 외부 반출 필요 시, 반출영역(W:)에 전송하여 **DRM 패키징 (엔파우칭)** 수행
- PC환경과 동일한 UI/UX 제공과 기존 후킹방식의 DRM 솔루션의 단점을 개선하여 성능, 유지보수성, 업무효율성 향상

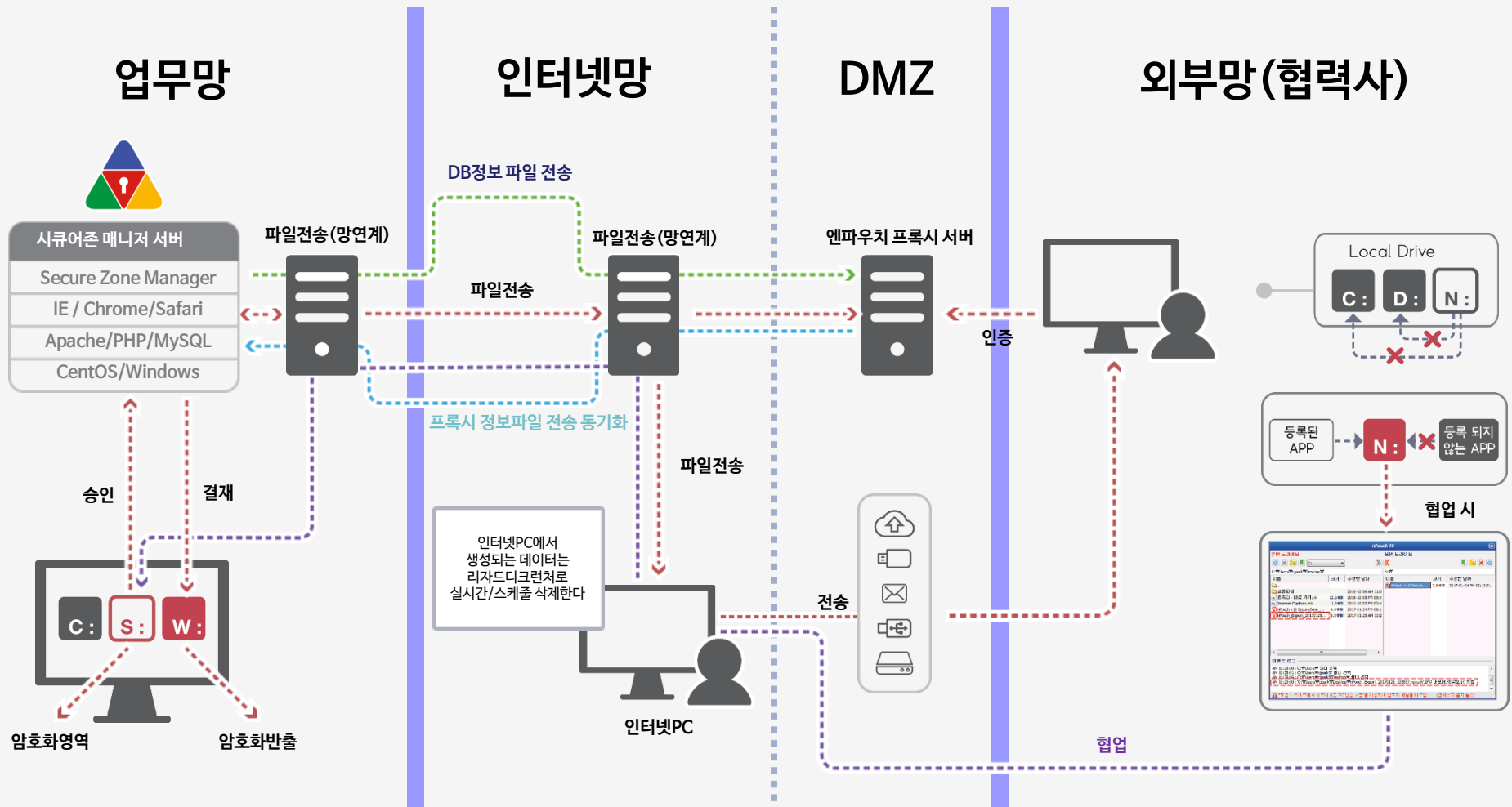
제품 소개 - 시스템 구성도



- S/W 구성도 : 제품 구성은 서버(Manager), 사용자(Agent), 외부 반출문서 수신자(Reader) 로 구성
- H/W 구성도 : 서버(Manager 운영), Storage 로 구성

제품 소개 - 망분리 시스템 구성도(제안구성)

망분리 시 반출문서 유출 보호 및 외부협업



특장점 - 주요 기능



저장통제

영역 암호화 제공

- 바탕화면 영역 암호화 제공
- 로컬디스크에 대한 영역암호화 제공 및 통제



가용성

장애시 대응

- 문서 유출방지 장애시 연속성 제공



편의성

기존환경변화 최소화

- OS에서 제공하는 폴더구조 변경 최소화

파일 공유시 편의성

- 편리한 부서별 문서공유 방법 제공



결재편의성

결재시 불편 최소화

- 문서반출 및 유통시 불편 최소화
- 자가 결제 및 개인 결제라인 등록 기능 제공



백업 관리

사용자PC의 백업 제공

- 영역 암호화 공간 백업 기능 제공



안정성

데이터 안정성 확보

- 문서 유실에 대비한 시스템 구성 제공



보안성

권한이 없는 드라이브 접근제한

- C,D 등 기존 드라이버 사용자 사용 제한

프로세스 제한

- 저장공간에 대한 White/Black List 프로세스 통제



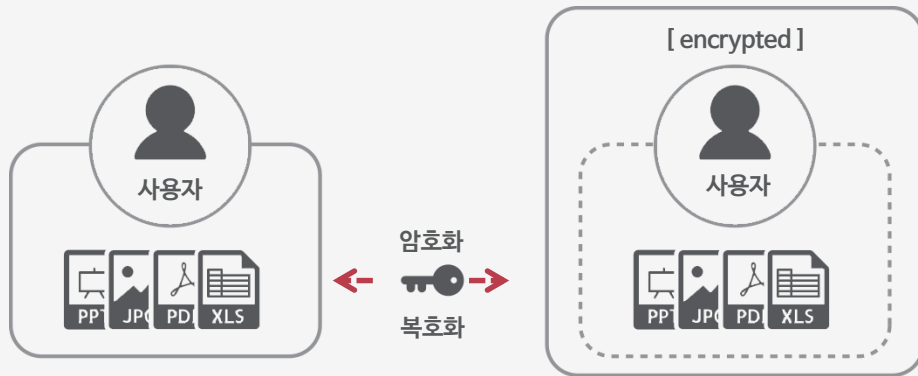
연동여부

기 도입 솔루션과의 연동 가능

- 저장통제가 된 상황에서 보안 USB사용여부 확인

특장점 - Envelope(영역암호화) 방식 탑재

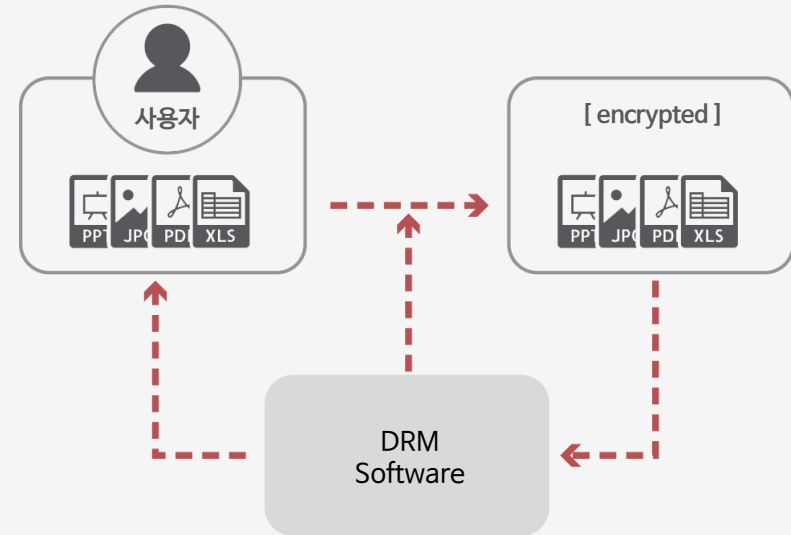
Envelope방식 (차세대)



- 문서의 종류에 상관없이 암호화 가능
- 형식에 상관없이 암호화 제공

- 암호화 키 관리가 매우 중요
- 키가 없으면 파일을 오픈 하지 못함

Hooking방식 (1세대)



[장점]

- 구현이 비교적 쉽다.

[단점]

- 프로그램 종속적이라 프로그램 변경 시 업데이트 필요
- 많은 리소스를 사용하여 성능 저하 발생

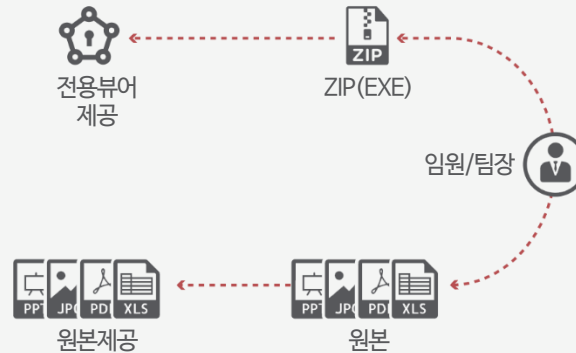
특장점 - 반출 프로세스

외부 반출 시



- 팀장 부재시 차석자가 결재할 수 있음
- 차석자 결재시 팀장 참조

자가/원본 반출 시 (임원/팀장 전용)



- 자가결재로 용도에 맞추어 사용가능
- 반출자료는 서버에 저장되며, 추후 감사 자료에 활용될 수 있음

긴급 반출 시 (업무연락필요)



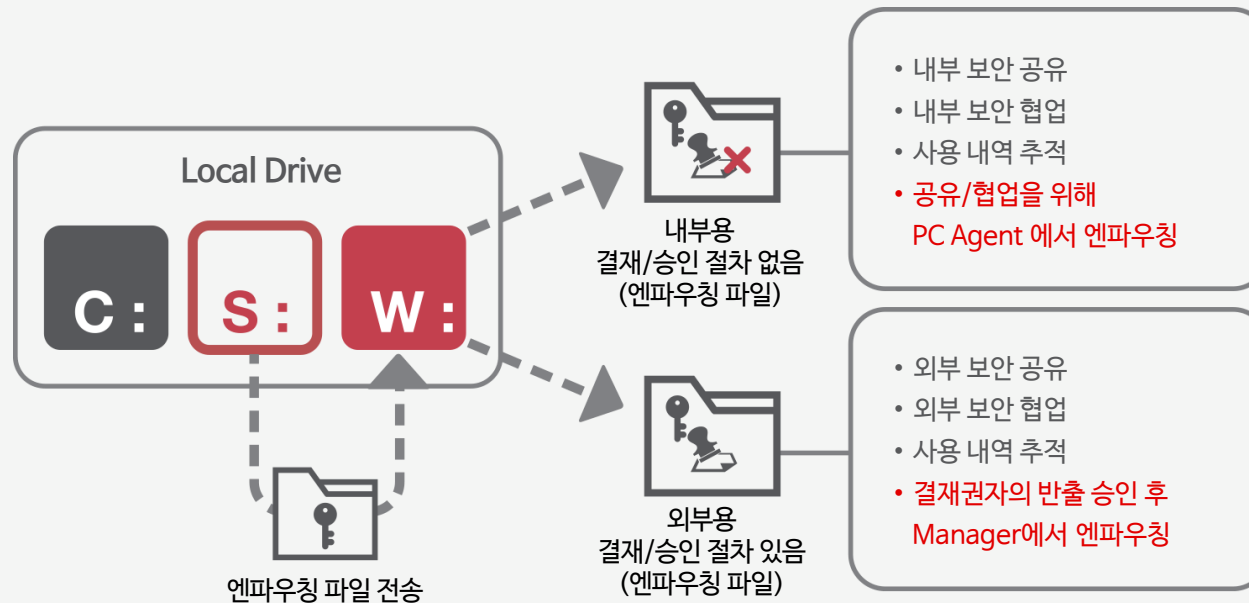
- 팀장/차석자 부재시 외부 반출시 사용
- 비정규업무로 반출 증적 필요(업무연락) 야간 및 휴일 미지원

주요 기능 - Manager 부문

[Manager - 기능 구성도]

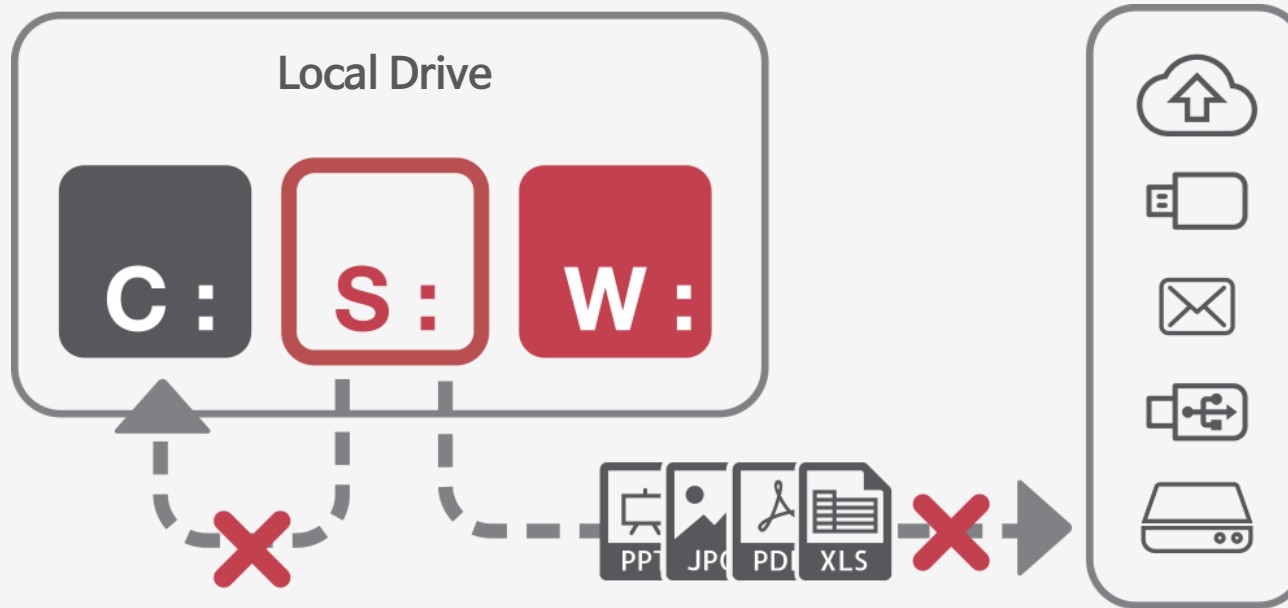


주요 기능 - 내/외부 반출문서 암호화



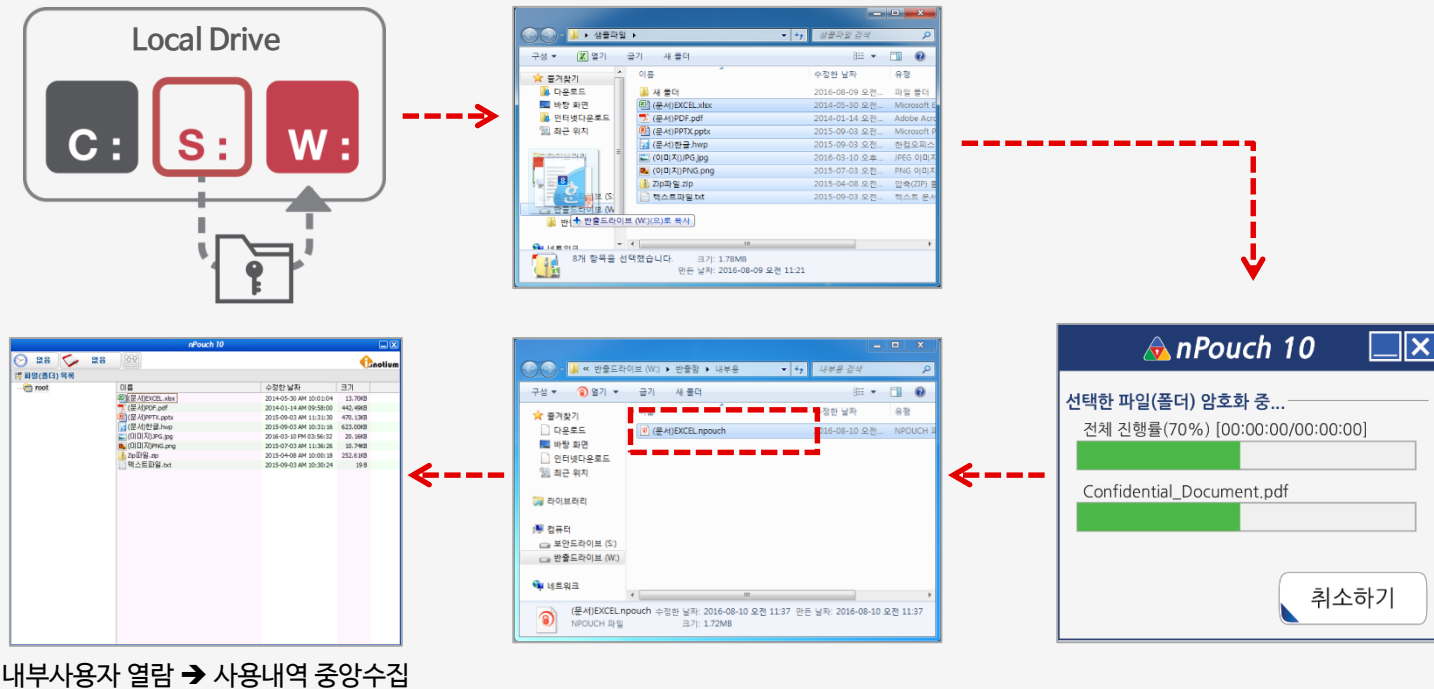
- 내부 협업 또는 외부 반출 필요시, 반출영역(W:)을 경유하여 엔파우칭(DRM 패키징) 및 반출결재 프로세스 수행
- 내부용은 업무효율성을 위하여 결재/승인 절차를 배제하고 외부반출 협업 시에만 반출결재 프로세스 적용
- 문서 반출을 위한 결재 프로세스 모듈을 기본 제공하여 반출/승인 간소화와 저비용, 고효율 제공

주요 기능 - 전자문서 유출 원천 차단



- SecureZone Agent 설치 후 보안영역(S:)에 보관하여 사용되는 모든 전자파일에 대해 유출 차단
- 보안영역(S:)은 암호화 및 어플리케이션 제어(화이트리스트) 기술 적용으로 파일 반출/입 보안 통제
- 보안영역의 데이터는 보안영역(S:) 내에서만 자유롭게 유통되며 여타 매체로 저장, 사본저장, 이동, 전송 불가

주요 기능 - 내부 공유 · 협업



- 파일/폴더 또는 드라이브 단위로 반출영역(“W:₩내부용” 폴더)에 복사 또는 이동시 자동 엔파우칭 TB급 대용량 외부 DRM 지원
- 국제표준 AES256 암호화 사용(국정원 인증 암호화 모듈 지원)

주요 기능 - 출력물 보안

☒ 출력물에 워터마크 출력하기

☐ 텍스트로 표시하기

워터마크 문구 :

각도 :

☒ 이미지로 표시하기

이미지 첨부 : [이미지 첨부](#)

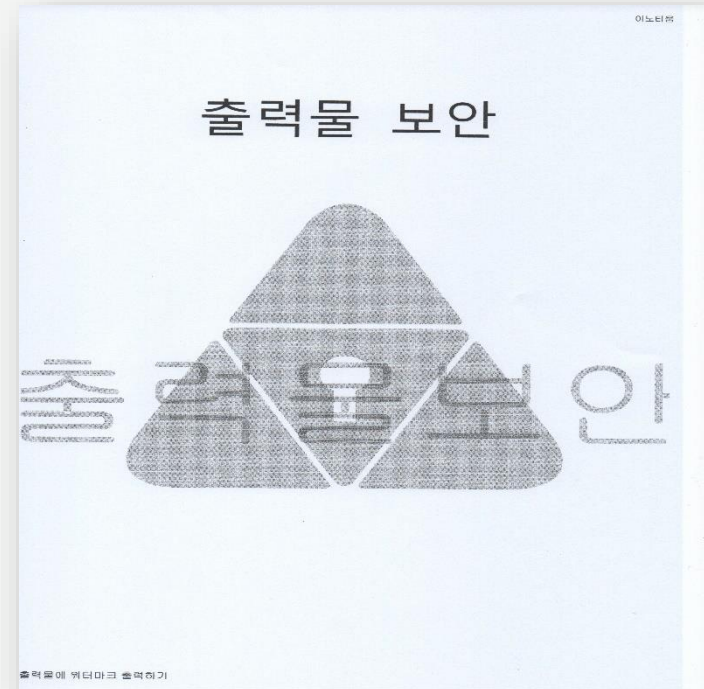
이미지 폭 : cm

미리보기 : 

상단문구 : 이노티움
예약어 사용가능 [/GRPNAME/], [/USERID/], [/USERNAME/]

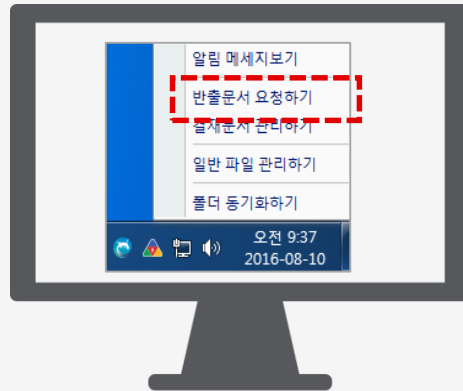
중간문구 : 출력물보안
예약어 사용가능 [/GRPNAME/], [/USERID/], [/USERNAME/]

하단문구 : 출력물에 워터마크 출력하기
예약어 사용가능 [/GRPNAME/], [/USERID/], [/USERNAME/]

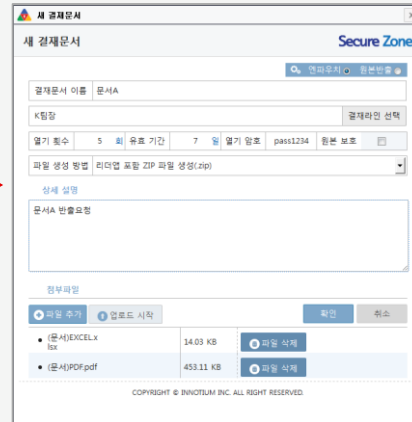


- 내부 문서 출력 시 워터마크 기능 제공
- 워터마크 각도 조절 기능
- 출력 로그 관리(시간, 파일명, 페이지 수 등)

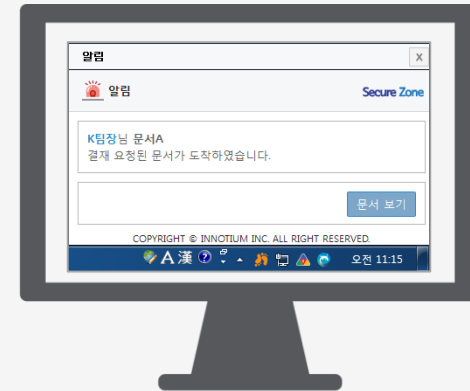
주요 기능 - 외부 반출문서 승인



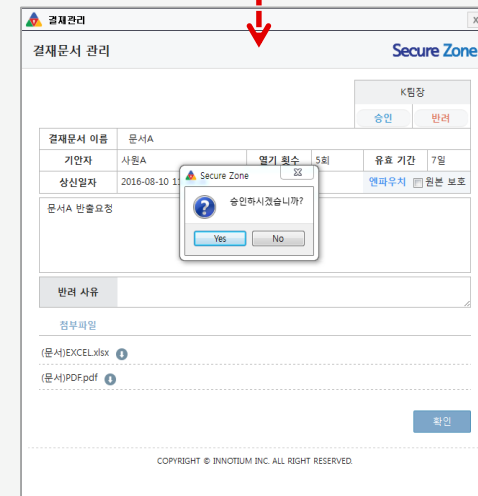
기안자 : 외부 반출요청



반출내용 작성과 파일 첨부 후 승인 요청



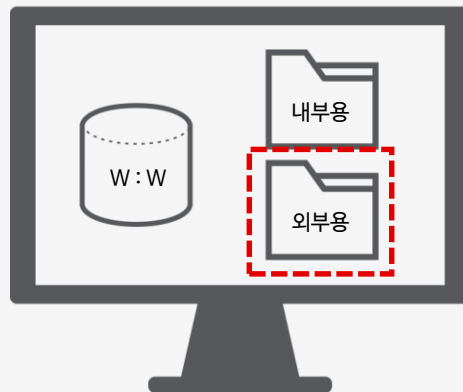
결재권자 : 결재승인 알림



결재권자 : 반출 승인 또는 반려

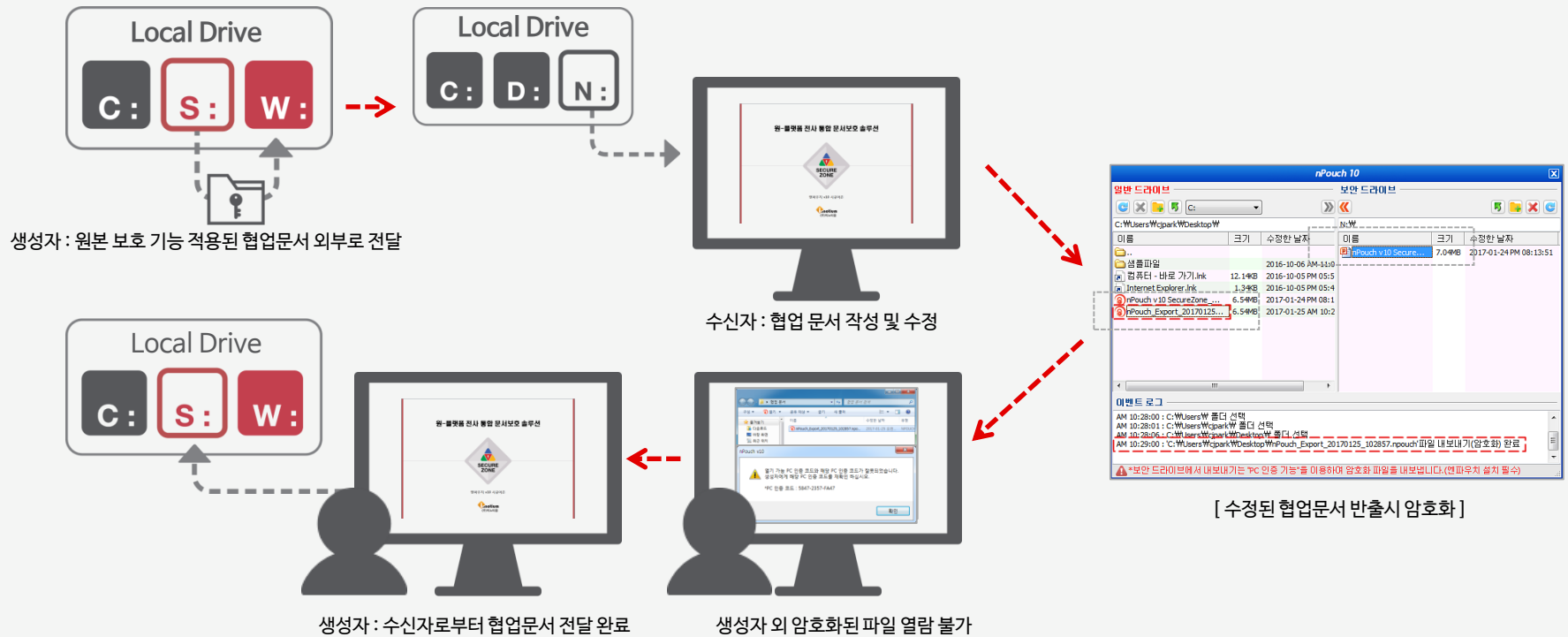


nPouch SecureZone Manager
엔파우칭 후 전송



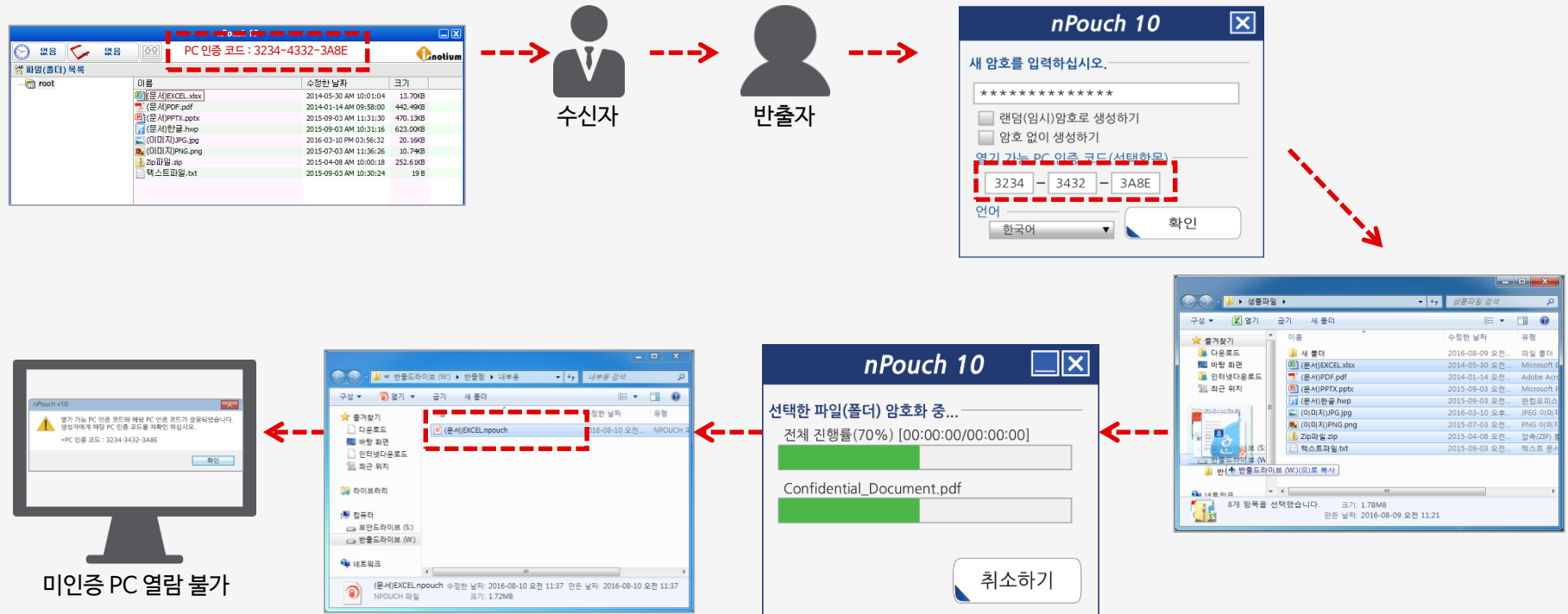
기안자 : 승인된 엔파우치 파일 수신

주요 기능 - 반출문서 2차 유출 보호/원본문서 외부 협업



- 원본 보호 기능 적용시 엔파우칭된 파일은 보안드라이브(N:₩)가 마운트되어 열람 가능
- 수신자는 파일을 보안드라이브(N:₩)로만 저장 및 수정 가능, 생성자에게 전달시 암호화를 해야 하며, 생성자외 다른 수신자 열람 불가
- 협업문서 반출 암호화된 파일은 생성자 PC에서만 열람 가능, 문서 유출을 방지하며 외부 협업이 가능한 프로세스

주요 기능 - 반출문서 수신자 지정 전송



- 반출된 파일이 지정한 PC에서만 동작하도록 PC 인증코드를 입력 후 보안 파일을 생성
- PC의 MAC, CPU ID, HDD ID 값을 혼합하여 PC의 고유 인증코드를 생성하고 지정 PC 이외의 다른 PC에서 파일 열람 불가

주요 기능 - 반출문서 제어

nPouch v10

열기 횟수를 초과하였습니다.

확인

상세보기

(기밀) VIP 일정표-150815.zip

설정 정보

열기횟수 제한	1/5	목록 허용	ON
기간제한	2015-08-21	열기 허용	OFF
암호 제한	1111	접속자 추적	
원본 보호기능 사용하기	ON	SMS 전송	OFF
PDF문서 보호	ON	사용자 중지	OFF
열기 시간 제한 문서			

첨부파일 목록

파일명	파일 크기	수정일
(기밀) 그룹 투자계획서.hwp	8.50KB	2015-08-16 19:50:03
(기밀) 인사기록 및 연봉 현황.hwp	8.50KB	2015-08-16 19:45:12

추적 정보

Type	Os	Browser	Acc	IP	접속 날짜
PC	Windows 7,.....	nPouch	1	192.168.11.1	2015-08-16 19:58:35

nPouch v10

생성자가 사용을 중단하였습니다.

확인

옵션 관리

Total : 9

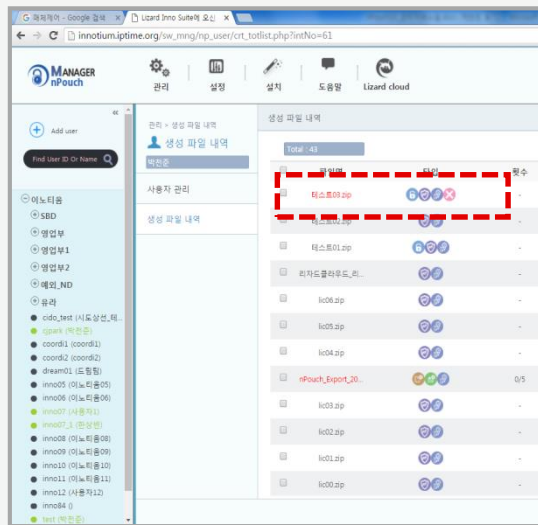
	열기 횟수	유효 기간	열기 암호	압축 파일	온라인 체크
<input type="checkbox"/> CODI_OPT	5	7	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> NP_OPT	-	-	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> NP_OPT_03	-	-	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> NP_OPT_APP	-	-	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> NP_OPT_RZ	5	7	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> NP_OPT_박전준	-	-	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> NP_OPT_한상빈	10	14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> SV_OPT	5	7	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> SV_OPT_한상빈	5	7	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Manager - 사용권한 옵션

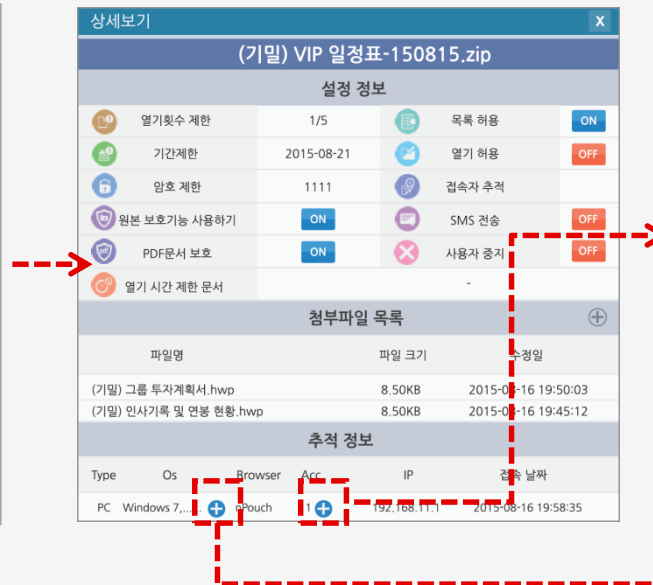
- 열람횟수, 열람기한, 인쇄제어, 화면 캡처방지, 사용 이력 관리 및 추적 등
- 반출된 파일은 관리자가 엔파우칭 파일 리스트를 이용하여 관제
- 반출된 파일을 관리자가 즉시 폐기할 수 있는 강제 사용중지 기능(실수 반출 또는 유실 위험 감지)

주요 기능 - 반출문서 수신자 시스템정보 추적 · 수집

[수신자 Trace - 접속정보(IP,접속날짜), 시스템정보(OS, Name, 계정, Mac)]



nPouch v10 SecureZone Manager



로컬 IP	접속 날짜
192.168.10.5	2016-07-25 18:25:58
192.168.10.5	2016-07-25 18:29:57
192.168.10.5	2016-07-25 18:30:22
192.168.10.5	2016-07-25 18:33:43
192.168.10.5	2016-07-25 18:40:05

OS 정보	
운영체제	Win 7, 64-bit
컴퓨터 이름	KVJOO-PC:kyjoo
계정 이름	soft1
MAC Address	1C6F65C17B5C

주요 기능 - 수신자 오프라인 시 반출문서 보호



- On-Line : 파일 열람시 시스템정보를 중앙 관제 서버로 전송하여 사용 제어
- Off-Line : 파일 오픈시 시스템 정보(Mac, User, OS, IP 등)를 포함한 QR-Code 를 실시간 생성 시스템정보 전송
- 생성된 QR-Code는 휴대폰 QR-Code 인식 범용앱을 이용하여 인증코드 획득 후 열람

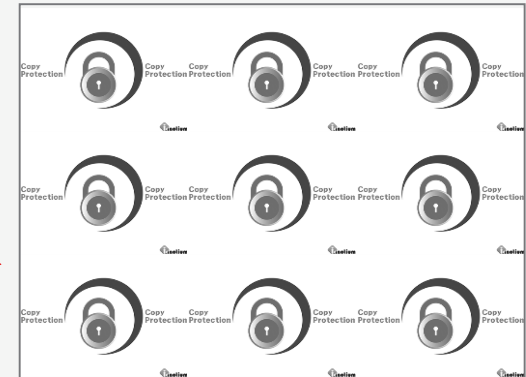
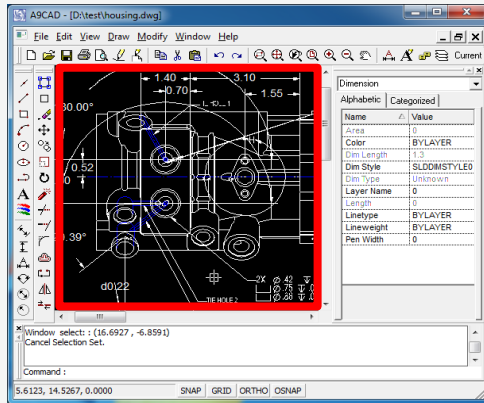
주요 기능 - PDF 문서 보안 및 추적관리



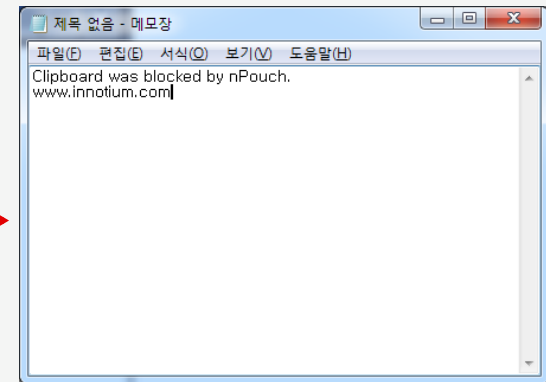
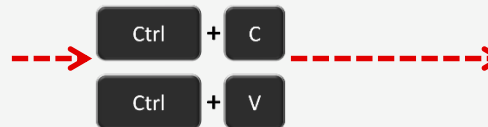
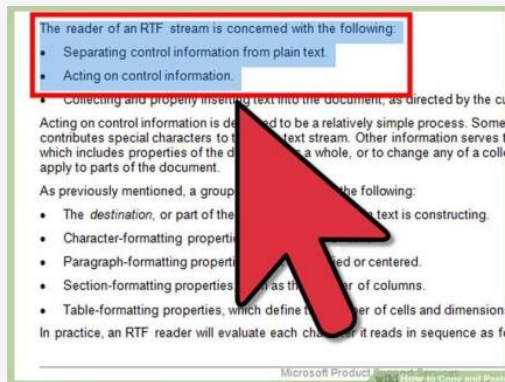
- ① PDF 문서에 대한 보호 기능 설정
- ② PDF 문서에 프린트 허용 여부 및 화면/출력용 워터마킹 (MAC, IP, 사용자 ID) 설정
- ③ 사용내역 추적 여부 설정
- ④ 화면용 워터마킹 예시 (카메라 촬영 방지 심리제어 기능)
- ⑤ 원본파일 오픈시 워터마킹

주요 기능 - 화면캡처 방지

[프로그램에 의한 화면캡처방지, 클립보드 통제, Ctrl+C / V 차단]

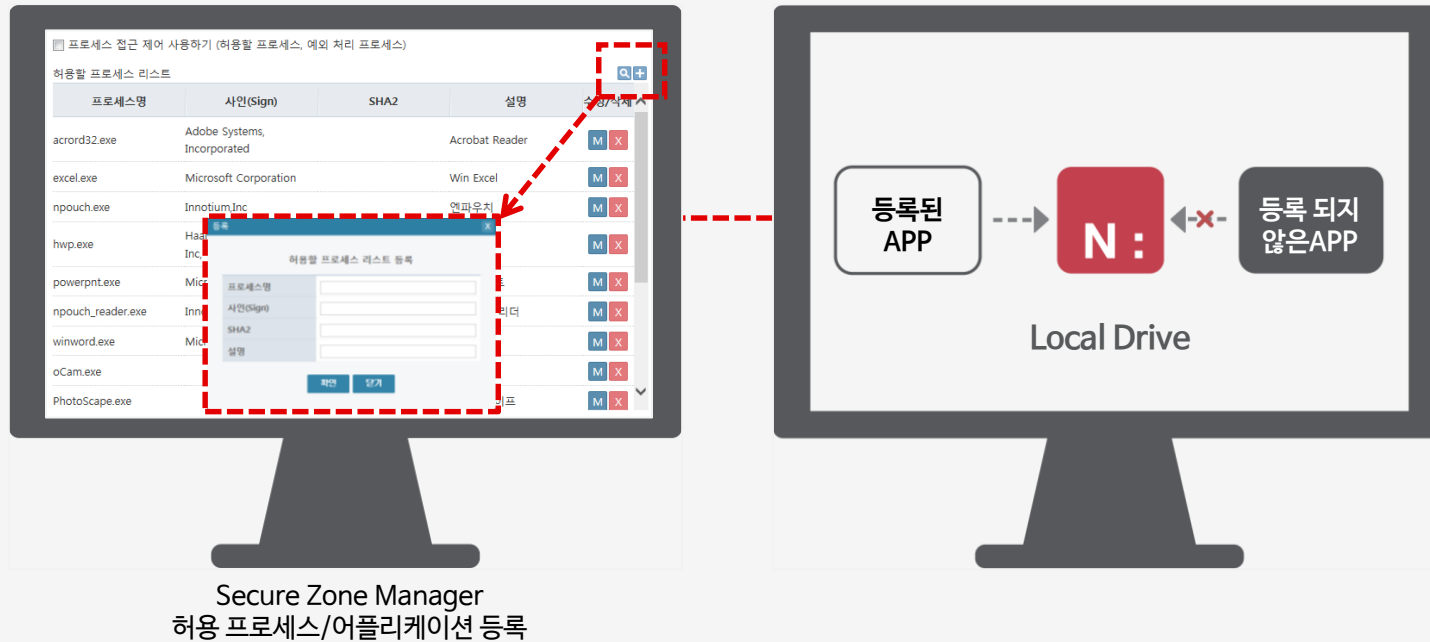


캡처프로그램에 의한 복사 방지



Ctrl+C / V 복사 방지

주요 기능 - 프로세스, 어플리케이션, 업무시스템 제어



- 보안영역(S:, W:) 저장소는 영역 암호화 및 어플리케이션 제어(화이트리스트) 기술 적용으로 파일 반출/입 보안 통제
- 등록된 프로세스와 허용된 어플리케이션들은 보안영역(S:) 내의 파일들을 자유롭게 접근 사용
- 미 등록된 프로세스, 어플리케이션, 업무는 보안영역에 접근 불가

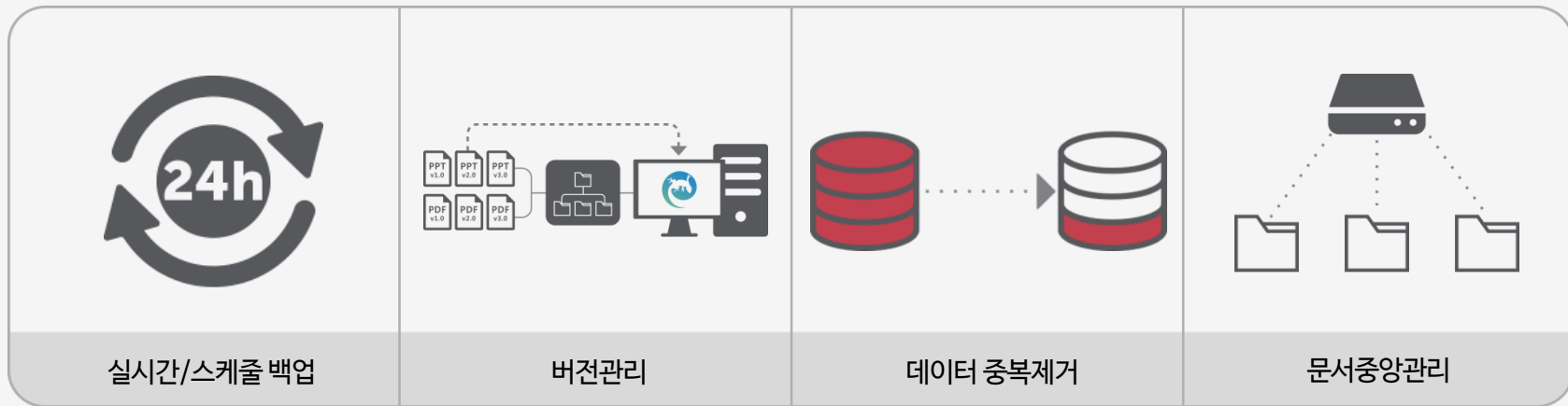
주요 기능 - 시스템 접근제어



- 사용자별 / 그룹별, 사용자PC에 접근 제어 설정으로 정보자산의 유출 가능성 최소화
- PC 자원의 감사 대상인 로컬디스크드라이브, USB, 제어판, REGEDIT, MMC, GPEDIT 등 정보유출에 대한 모든 위험요소 차단 제어

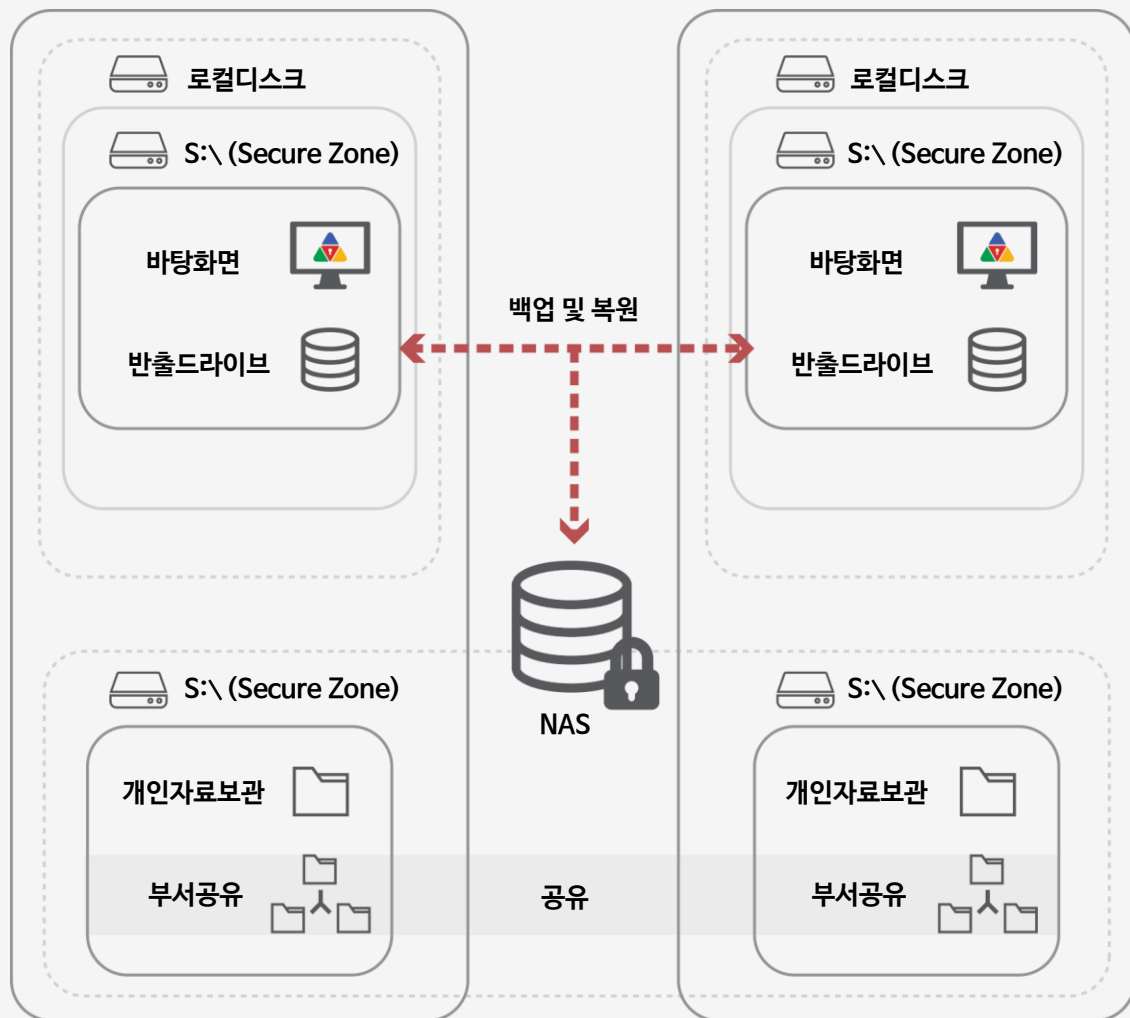
주요 기능 - 데이터 유실방지

[PC 보안백업 기능]

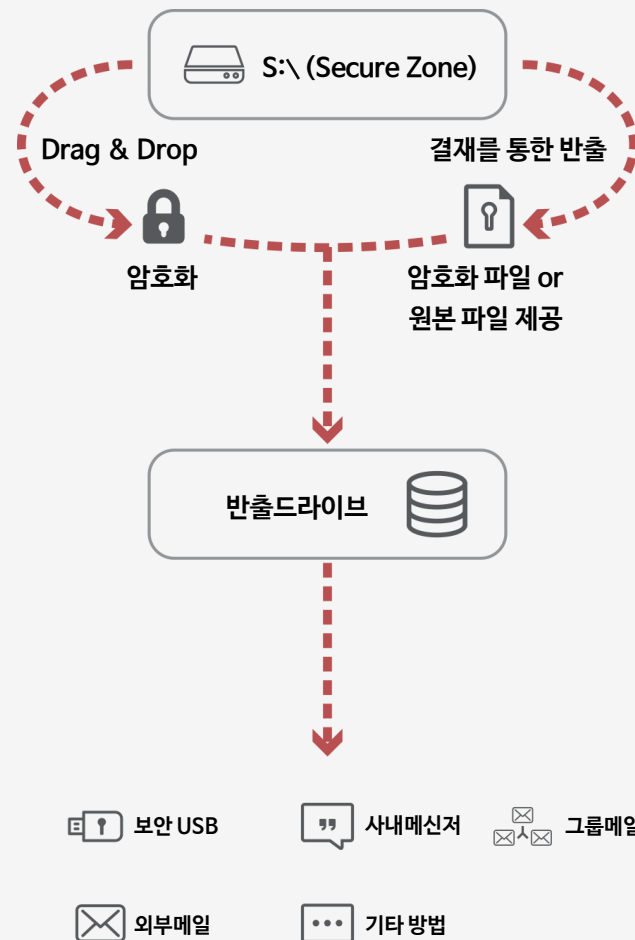


- 실시간 /스케줄 백업은 시스템 부하를 최소화하여 복사본, 단방향, 양방향 등의 다양한 옵션 지원
- 버전(이력)관리는 하나의 파일을 여러 번 백업하여도 인덱스(색인) 정보를 활용하여 필요한 시점으로 복원 가능
- 데이터 중복제거 기술은 디스크 증설비용을 최소화하고 시스템 가용성을 최적화 유지
- 문서중앙관리 : 모든 문서는 중앙관리 되므로 담당자 변경, 이직, 퇴사시에 자료 유실 위험 최소화

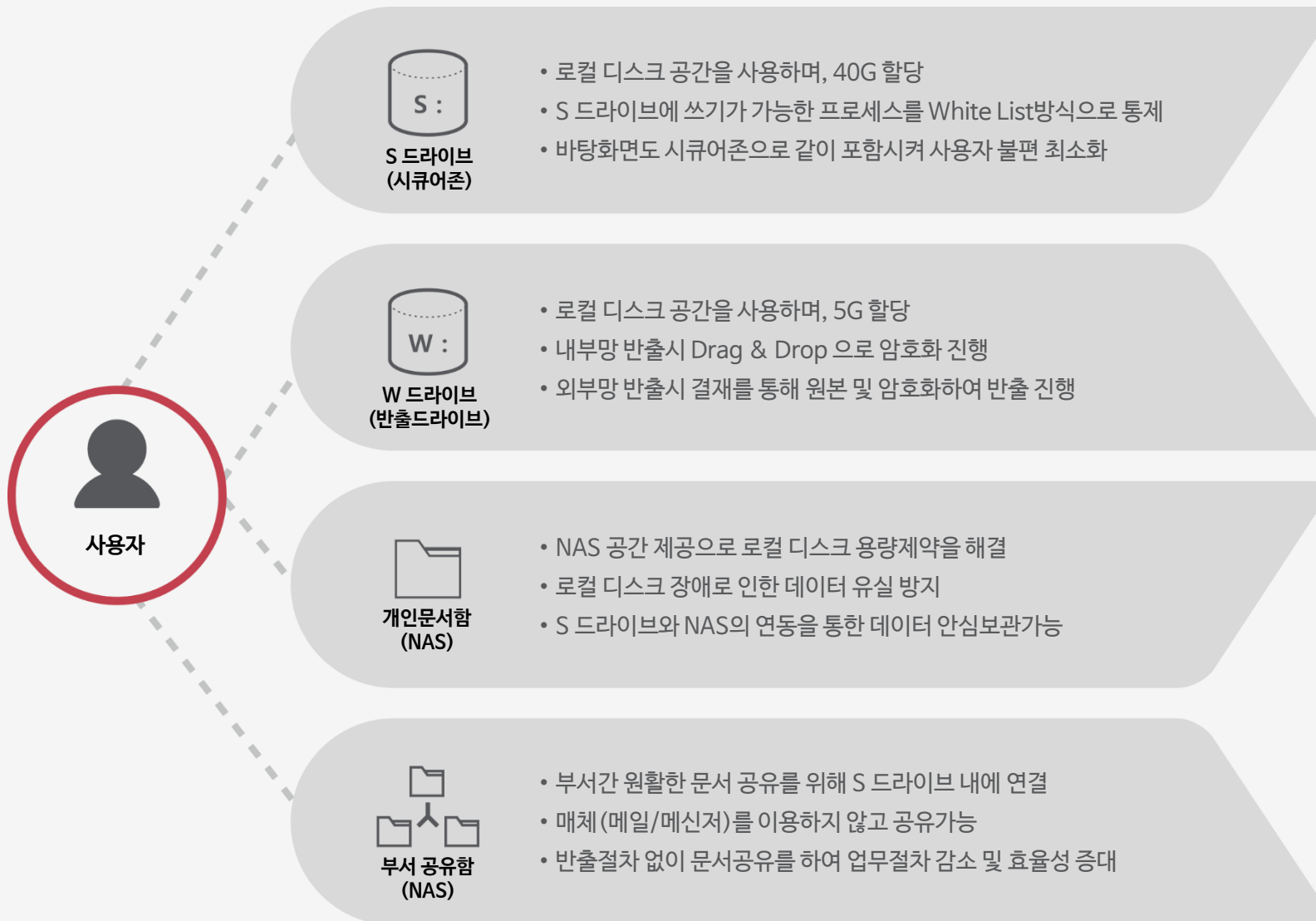
[저장 아키텍처]



[반출 흐름도]



구축 사례



[도입 효과]



정보자산 유출 원천 차단



업무

- 기업/기관 업무정보자산 유출 원천 차단
- 협업문서의 안전한 유통 및 관리 가능
- 업무외 정보 사용 근절로 인한 업무 효율성 상승



조직 내/외 반출문서 보안 협업



사용자

- 기존의 업무 환경을 그대로 유지 사용
- 업무 문서 자료에 대한 권한과 책임의식 高
- 보안 시스템에 대한 신뢰도 향상



기술

- 3 in 1, DRM/DLP/PC백업 융합 보안
- 사용자 편의의 신개념 문서보안 기술



관리

- 중앙통제 감시체계의 구축으로 손쉬운 보안 관리
- OS, S/W 업그레이드 시 추가비용 및 유지보수성 低

레퍼런스

경상남도청, 문화체육관광부, 특허청, KISA, 삼성전자, 현대자동차를 비롯하여 다양한 산업의 고객들에게 PC(엔드포인트) 랜섬웨어 탐지 및 개인정보 백업 사업을 수행하였으며 제품의 안정성과 신뢰성을 인정받고 있습니다.



공공

경상남도청 | 양산시청 | 통영시청 | 광명시청 | 강동구청 | 은평구청 | 강화군청 | 울주군청 | 문화체육관광부 | 한국전력거래소 | 우정사업본부 | 여성가족부 | 특허청 | 한국인터넷진흥원 | 한국전자통신연구원 | 한국수자원공사 | 대한석탄공사 | 한국전력기술

외 100여 기관

금융

KB카드 | 동부증권 | 신영증권 | KDB인프라자산운용 | 한화저축은행 | 스마트저축은행 | 골든브릿지저축은행

외 50여 업체

기업

삼성전자 | 현대자동차 | 두산중공업 | LS전선 | 대명 | 효성 | 유한화학 | 동국제약 | 이연제약 | 서울제약 | 미림화학 | 유한화학 | 국방일보 | 전남일보 | 국제신문 | 동아일렉콤 | 두산중공업 | 한화시스템 | 한진중공업 | 한화에어로스페이스

외 300여 업체

의료

국립암센터 | 충북대학교병원 | 국립정신건강센터 | 부산대학교병원 | 효성병원 | 효성세종병원

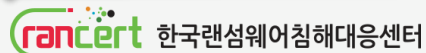
외 20여 업체

교육 및 협회

계명문화대학교 | 창원대학교 | 울산대학교 | 전북대학교 | 한국건설자원공제조합 | 벤처기업협회 | 한국전기기술인협회 | 한국전기공사협회

외 10여 기관

한국랜섬웨어침해대응센터



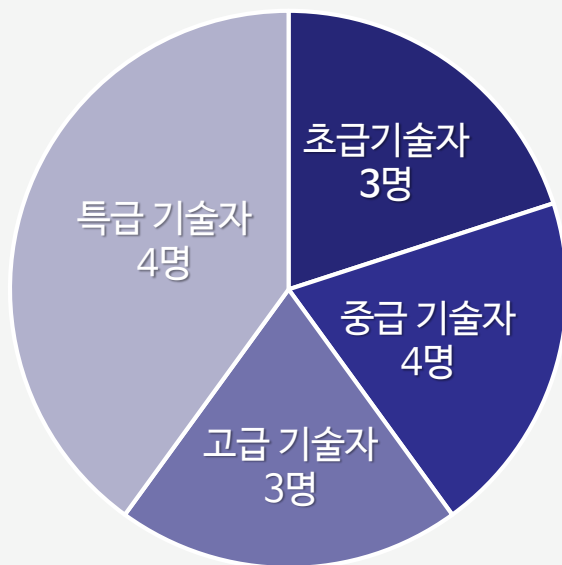
랜섬웨어 예방을 위한 개인사용자 무료 다운로드 200,000여명
www.rancert.com

개발사 - 현황

회사명	(주)이노티움 / Innotium Inc.
대표자	이형택 (010-6239-2764, htlee@innotium.com)
회사주소	T: 02-3283-2021 F: 02-3283-2015 A:서울시 구로구 디지털31길 20, 301호
설립일	2010년 1월 7일
영위사업	- 랜섬웨어 방어 사전차단/보안백업SW, 문서보안관리 SW, 반출문서 유출방지/추적관리 SW, 블록체인 플랫폼SW - 한국랜섬웨어침해대응센터 운영 - 리자드방산보안지원센터 운영

개발자 보유 현황

(2020년 2월 기준, 단위: 21명)



■ 초급기술자 ■ 중급기술자 ■ 고급기술자 ■ 특급기술자

CEO 이형택 대표이사

CMO 이인행 부사장

사업부 : 6 명

기술컨설팅팀

정보보안사업팀

방산보안사업팀

CTO 김성완 부사장

기술연구소: 14 명

지능화/UI/UX팀

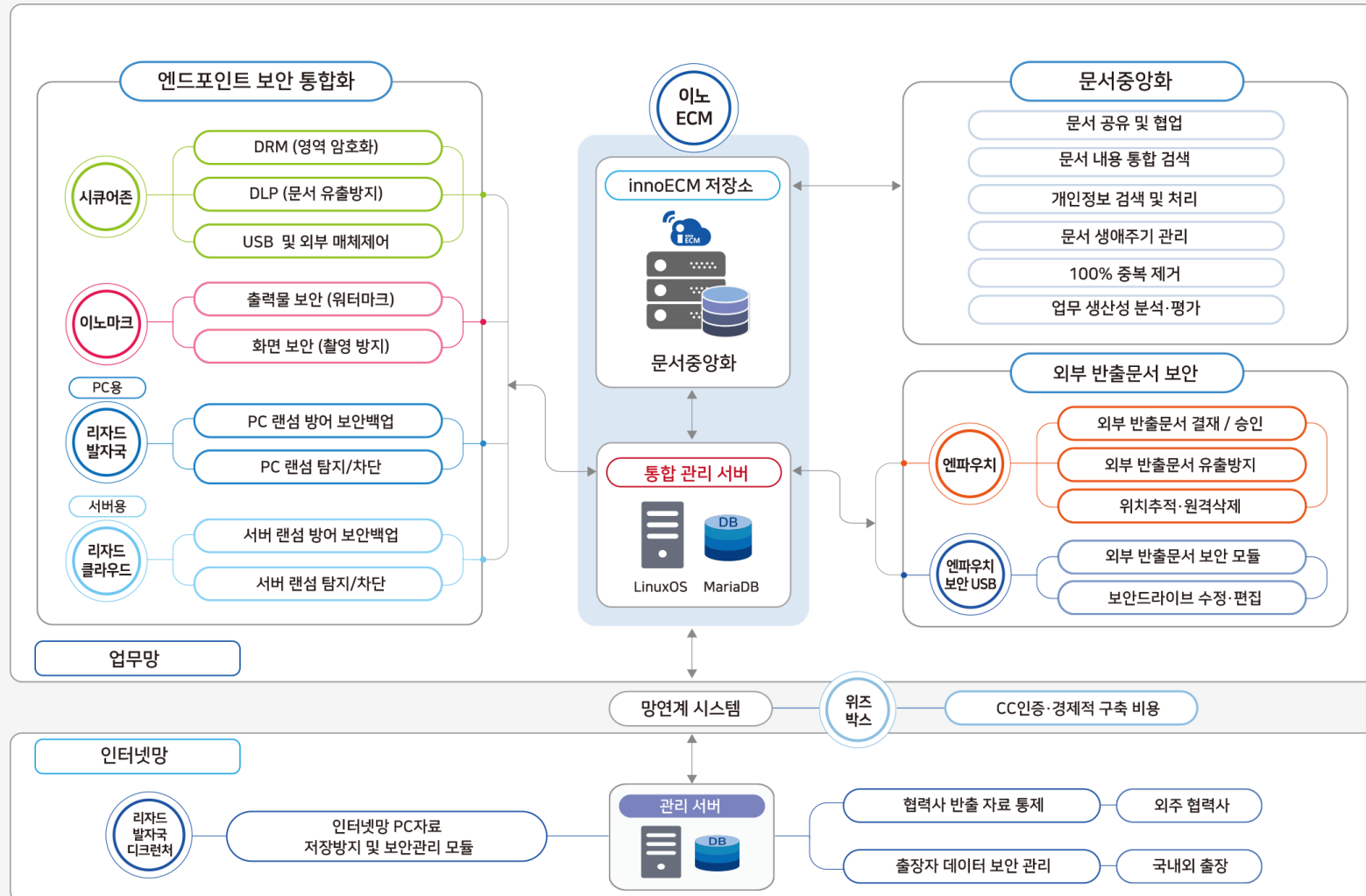
정보보안 개발팀

블록체인 개발팀

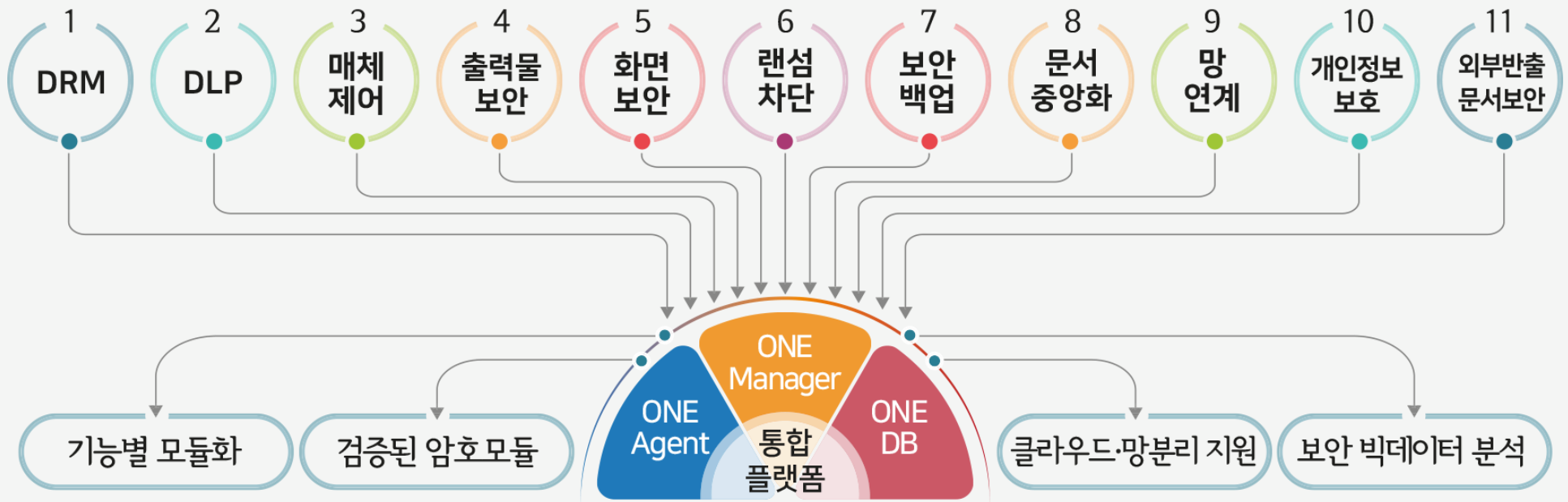
경영지원팀: 1 명

인사/총무/회계

이노티움 지능형 문서중앙화 기반 통합 문서보안 플랫폼



엔드포인트 보안 사용자들의 오랜 염원 “하나로 안돼?”



개발사 - 연혁

HISTORY



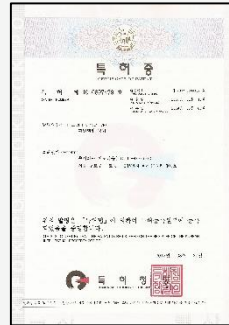
연도	내용
2019	<ul style="list-style-type: none"> -잇허질 권리 구현 블록체인 플랫폼 개발 InnoBlock Chain Platform -국가핵심기술 데이터 위치추적 서비스 개발 -사내 데이터 공유 및 협업을 위한 innoECM 개발 -엔드포인트 보안기술 통합화-지능화-시각화 프로젝트 개시
2018	<ul style="list-style-type: none"> -100대 방산업체 망분리 사업 15개 사이트(한화 에어로스페이스, 두산중공업 등) 수주 및 공급 -시험지 유출방지용 스마트 시험관리 통합 보안관제 플랫폼 개발 -2018 랜섬웨어 디펜더 컨퍼런스 개최: 2.6
2017	<ul style="list-style-type: none"> -한화그룹 외 방산부문 데이터 보안 사업 수주 및 공급 -에스원과 방산업체 망분리사업 협약 체결 -미래부 주관 랜섬웨어 민관 대응 핫라인 구성
2016	<ul style="list-style-type: none"> -2016 차세대 데이터 보호 컨퍼런스 개최 -에스원과 '대국민 랜섬웨어 대응서비스' 협약
2015	<ul style="list-style-type: none"> -한국랜섬웨어침해대응센터 오픈 -ID 패스워드 보안인증 핀테크 솔루션 “아이오써티” 출시 -리자드클라우드 엔파우치 v10 GS인증 획득
2014	<ul style="list-style-type: none"> -발자국 조달등록 -일본 서버백업용 클라우드백업 서버 수출 -중소기업청 “수출역량강화사업자” 선정 -삼성디스플레이 DB백업사업 수주 (100 Unit)
2013	<ul style="list-style-type: none"> -DB백업용 클라우드백업 일본 수출 -SW산업원천기술개발사업 “클라우드 환경의 DRaaS”개발 컨소시엄 참여 -엔파우치 특허등록 및 프로그램 등록
2012	<ul style="list-style-type: none"> -세무사협회 한길 TIS와 세무회계 데이터 온라인 백업서비스 개시 -특허청 VDI 클라우드 데이터 백업 솔루션 2,000유저 납품
2011	<ul style="list-style-type: none"> -일본KCS사와 클라우드백업v7 공급계약 체결 -사내 구축형 프라이빗 클라우드 “리자드 클라우드”출시
2010	<ul style="list-style-type: none"> -(주)이노티움 설립

개발사 - 특허증 및 인증서

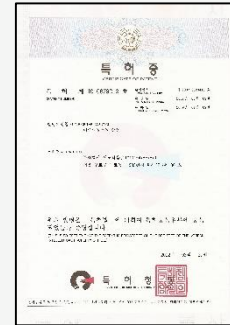
특허 / 인증



엔파우치 특허증



백업방법 특허증



이중파일백업 방법 특허증



원상복구 보증서



악성코드 탐지 방법 특허증



웹접속 정보 실행 특허증



리자드클라우드 엔파우치 v10 GS인증



발자국 v3.0 GS인증



리자드클라우드 상표등록증



엔파우치 상표등록증



발자국 행정업무용 소프트웨어 선정확인서

유비무환 有備無患

미리 준비하면 걱정이 없습니다.

(주)애플소프트 www.applesoft.co.kr

T. 02)836-4024 | E.yjyeung@applesoft.co.kr