Cloud Innovation 2023

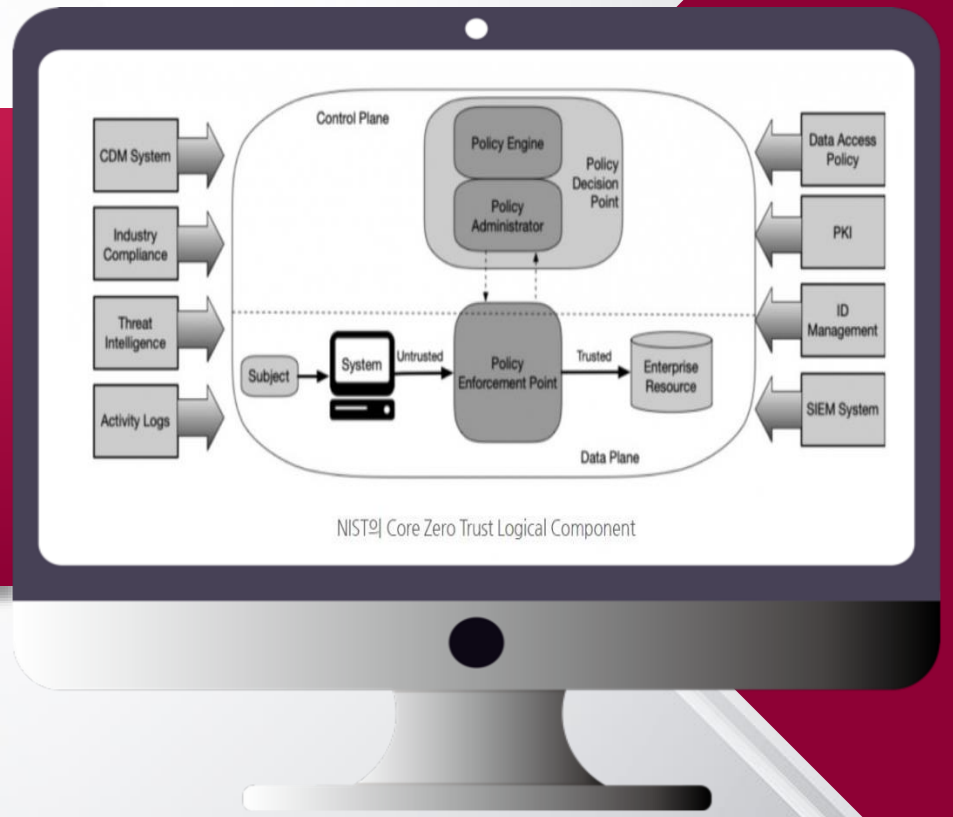
제로 트러스트 기반
차세대 지능형 데이터
보안플랫폼 아키텍처

Innotium

1

제로 트러스트 정의와 아키텍처

“Never Trust, Always Verify”



NIST의 Core Zero Trust Logical Component

미국 NIST(미국 국립표준기술연구소) 관점

01 제로 트러스트 정의: “Never Trust, Always Verify”

네트워크상 **침해로 간주되는 상황**에서 정보시스템 및 서비스에서 요구에 따라
정확하게 접근결정 시 불확실성을 줄이기 위해 설계된 개념과 아이디어의 집합

02 제로 트러스트 7대 원칙

① 모든 **데이터 소스와 컴퓨팅 서비스는 리소스**로 간주
② 네트워크 위치와 관계없이 **모든 통신을 안전하게 유지**
③ 개별 엔터프라이즈 리소스에 대한 **액세스는 세션 각각으로 승인**
④ 액세스는 클라이언트 ID와 애플리케이션, 서비스, 요청 자산의 상태확인 등 **동적 정책으로 결정**
⑤ 모든 소유 및 관련 자산의 무결성과 **보안 상태를 모니터링하고 측정**
⑥ 모든 리소스 인증 및 권한 승인은 가변적이며 **액세스 허용 전 엄격히 적용**
⑦ 자산, 네트워크, 인프라, 통신의 현재 상태정보를 수집하고, 이를 활용해 **보안 상태 개선**

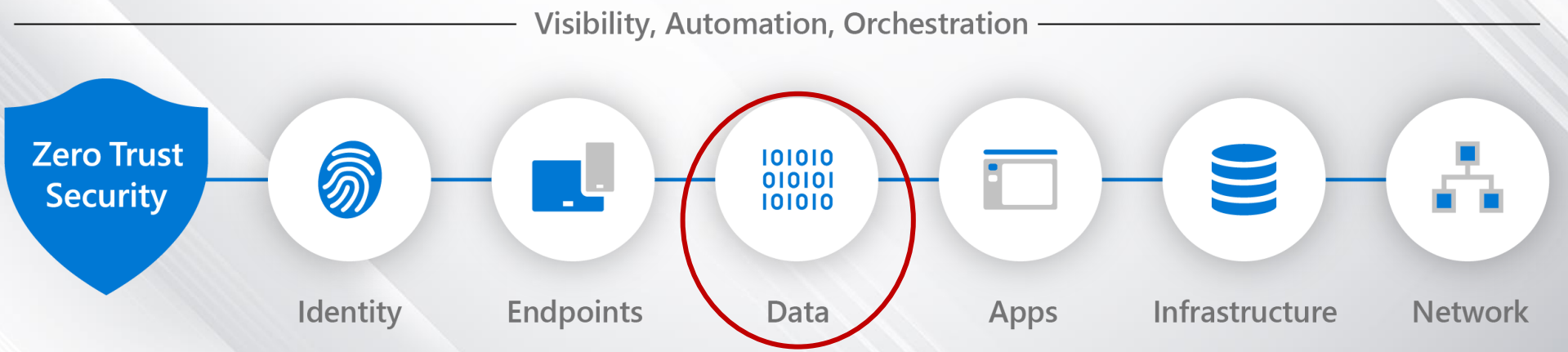
MICROSOFT 관점

01 제로 트러스트 정의: 제품/서비스 아닌 보안전략

3대 보안원칙 디자인 및 구현 접근방식

- ○ 명시적 확인
- ○ 최소 접근권한 허용
- ○ 위반 전제

02 주요 기술 핵심 요소에 대한 제로 트러스트 접근 방식



MICROSOFT 관점

03 3대 데이터 보호전략

전사 보유 데이터 이해 및 분류

- ○ 전사 데이터 내용 검색
- ○ 전체 데이터의 민감도/기밀도 수준별 분류

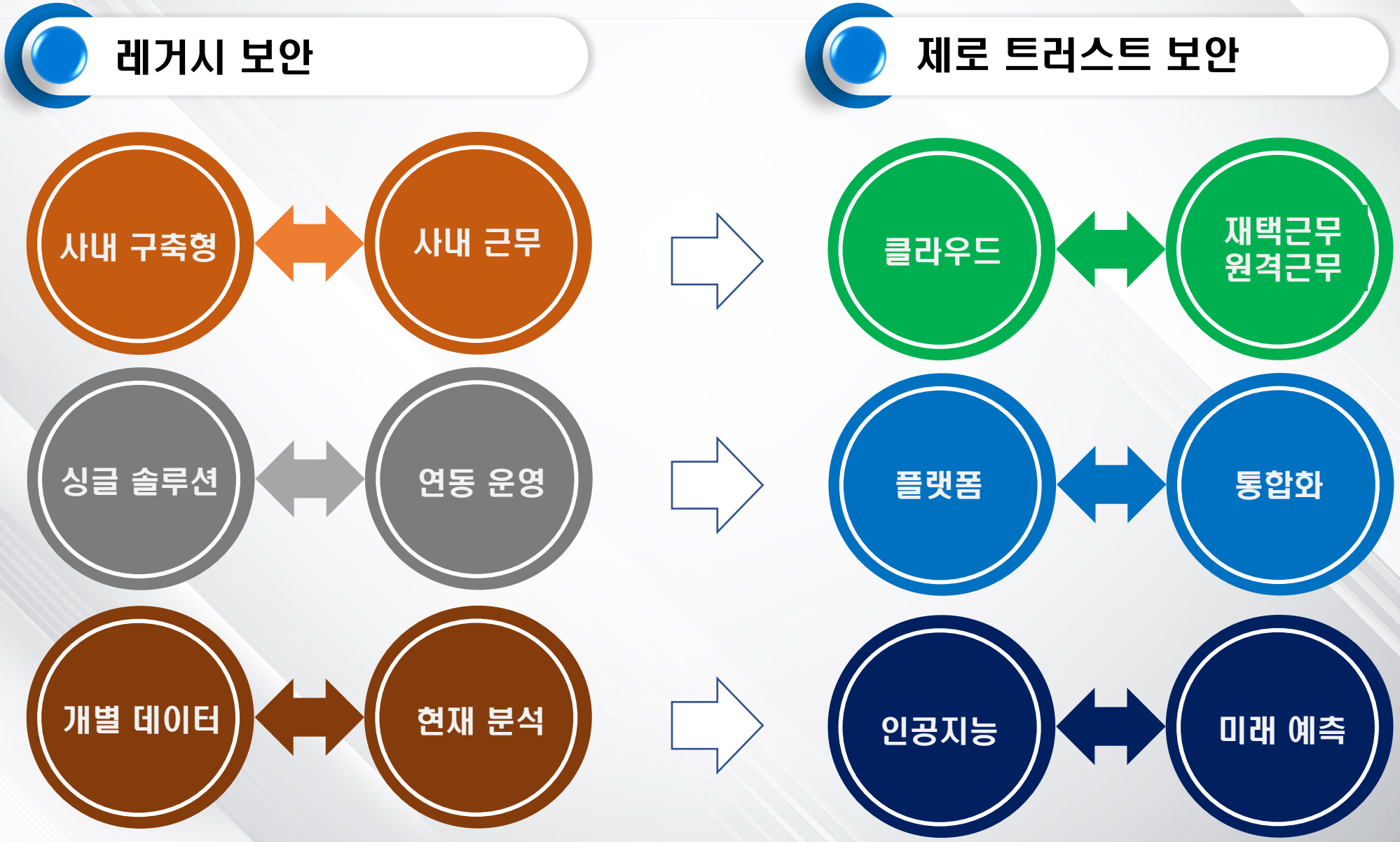
데이터 보호 및 손실/유출방지

- ○ 중요 데이터 레이블 지정 및 암호화, 과도한 공유 차단
- ○ 외부 이동시 권한 데이터만 접근 가능

모니터링 및 위반자 조치

- ○ 지속 모니터링으로 정책위반과 위험 사용자 동작 탐지
- ○ 액세스 취소, 사용자 차단 및 보호 정책 구체화

레거시 보안 VS 제로 트러스트 보안 관점 비교



2

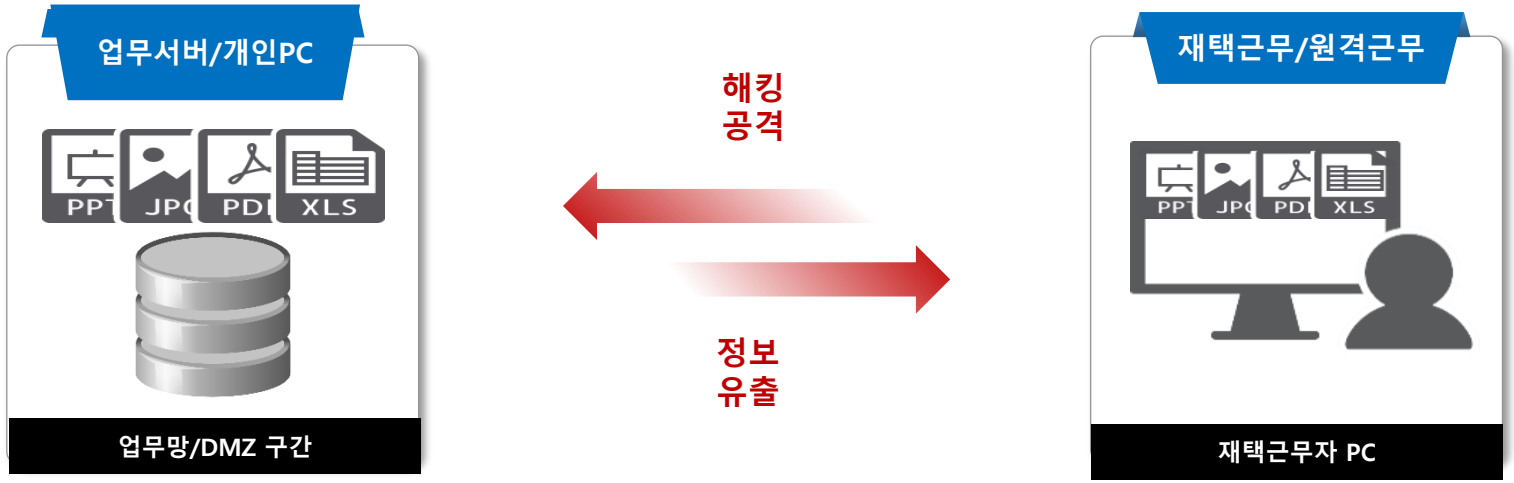
제로 트러스트 보안 필요성

-비대면 시대 도래

-신위협 VS 신보안

재택/원격근무시 8대 보안 취약점

코로나19 발생으로 인한 일하는 방식과 환경이 변화하여 보안 위협이 크게 증가



유출 위협

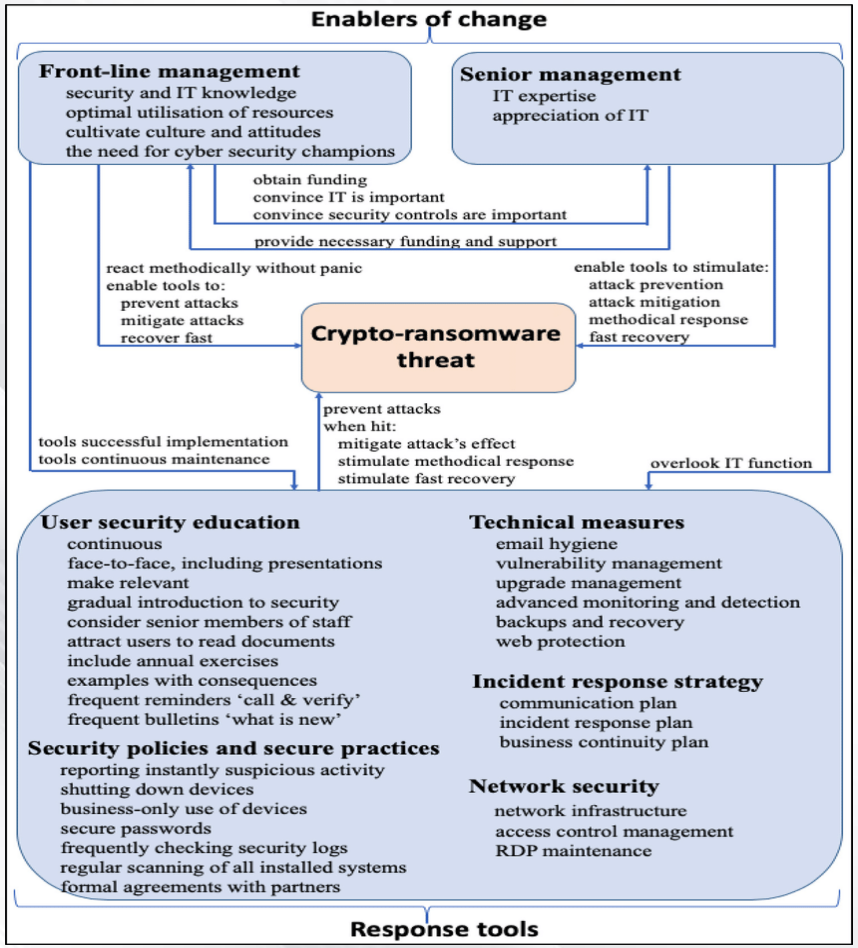
I. 개인정보/기밀자료 유출
II. 카메라 촬영 의한 유출
III. 화면 캡처 의한 유출
IV. 프린트/복사 의한 유출

해킹 위협

I. 랜섬웨어 암호화 침해
II. APT공격 해킹
III. ID/PW 유출
IV. RDP 이용 제3자 PC로 중계

랜섬웨어가 악성코드를 지배하다

- 랜섬웨어의 급증과 서비스형 랜섬웨어(RaaS) 등장에 따라 랜섬웨어 대응 시장이 급증하고 있어 보안백업, 디지털 포렌식 등 기술 확보 필요



랜섬웨어 대응

- 랜섬웨어가 급증하며, 랜섬웨어를 제작해제공하는 서비스형 랜섬웨어(Ransomware as a Service, RaaS) 등장 등으로 기업과 개인들의 랜섬웨어 대응 위한 시장수요가 급증할 것으로 보임
- 랜섬웨어 대응 시장은 2019년 48.5조원에서 2027년 163.6조원으로 매년 16.4%의 고성장을 보일 것으로 전망됨
- 랜섬웨어 대응을 위하여 전통적인 보안 솔루션 · 서비스 외에도 랜섬웨어에 특화된 보안백업, 디지털 포렌식 기술과 준비도 등 다양한 기술과 서비스 제공 필요

한국랜섬웨어침해대응센터

rancert 한국랜섬웨어침해대응센터

Ransomware Computer Emergency Response Team

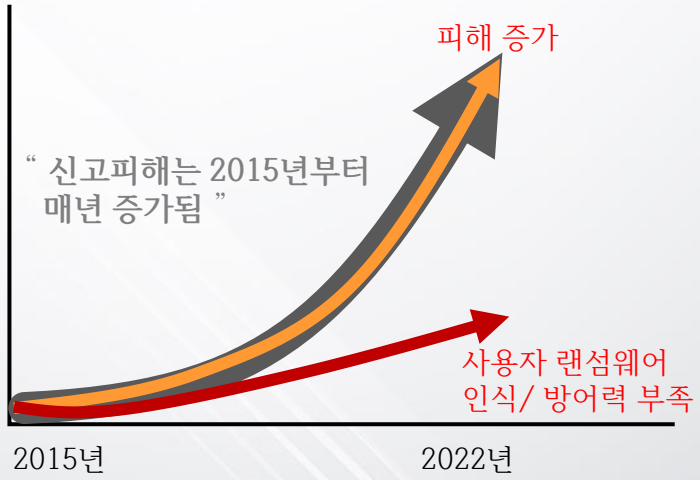
설립일자

2015년 2월 1일

✔ 센터장

이형택 ㈜이노티움 대표

- 랜섬웨어 침해사고 신고 접수 및 초기 대응 지원
- 침해 랜섬웨어 기술 분석
- 피해상황 인지 및 사후 예방을 위한 컨설팅 제공
- 침해사고 통계 및 분석
- 국내 유관 기관과 협력
- 그 외 침해 예방 안내



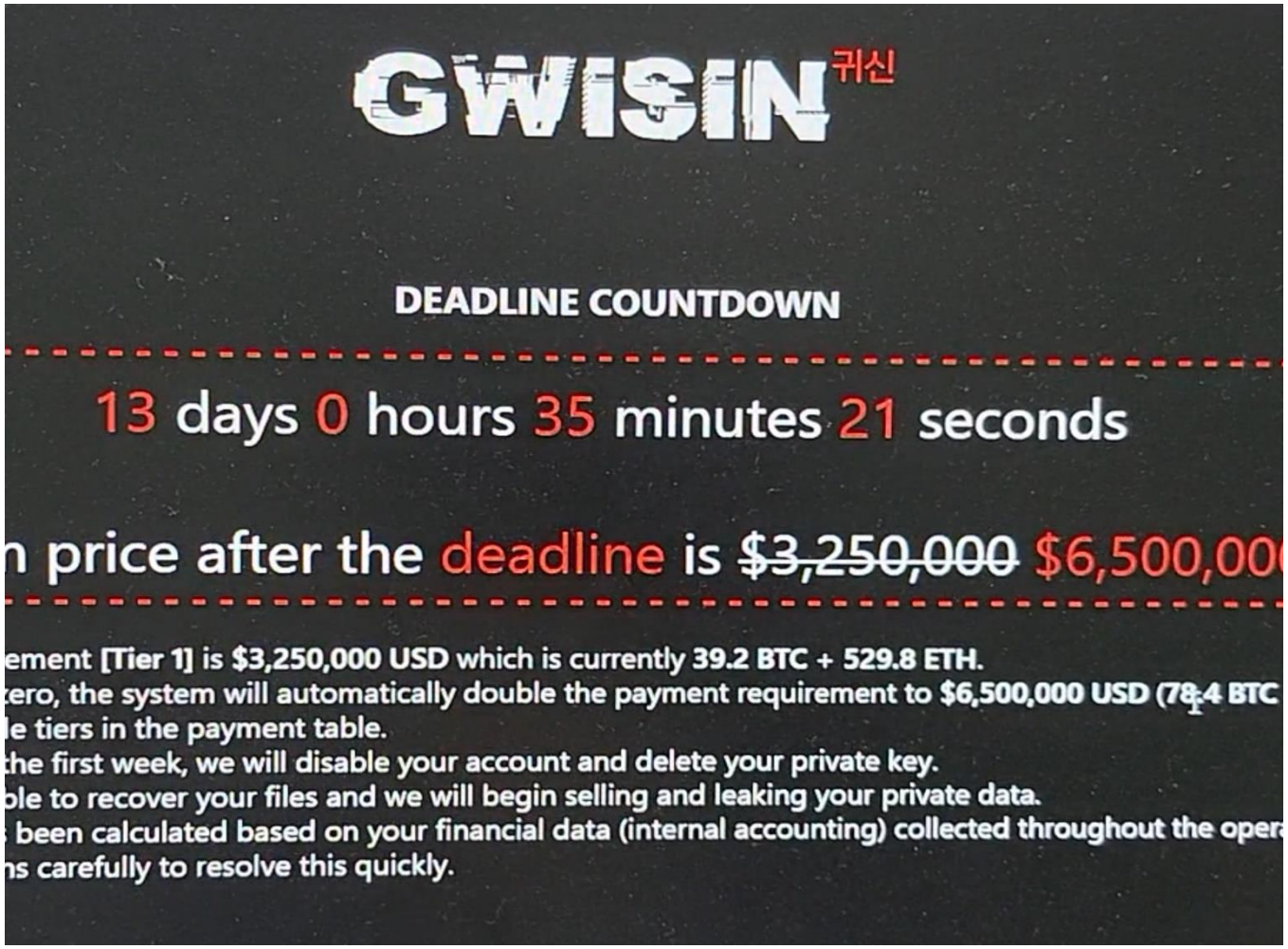
랜섬웨어 사례분석

2022년 대형기업 서버 랜섬웨어 침해 사례 (1/2)

- 기업규모: 제조서비스업, 매출-4조원, 직원수-5,000명
- 피해규모: 서버 200대 DB/File 암호화(VDI서버, 이메일 서버, 파일 서버)
- 피해일시: 2022년 1월
- 랜섬웨어 종류: REvil 변종
- 요구사항: 복호화 대가 암호화폐 (1,000만불-120억원)
- 특이사항:
  - -중요자료 탈취보관
  - -백업시스템 완전삭제
  - -취약점 분석보고서 제출
  - -경고: KISA/사이버수사대 연락금지, 복호화 금지

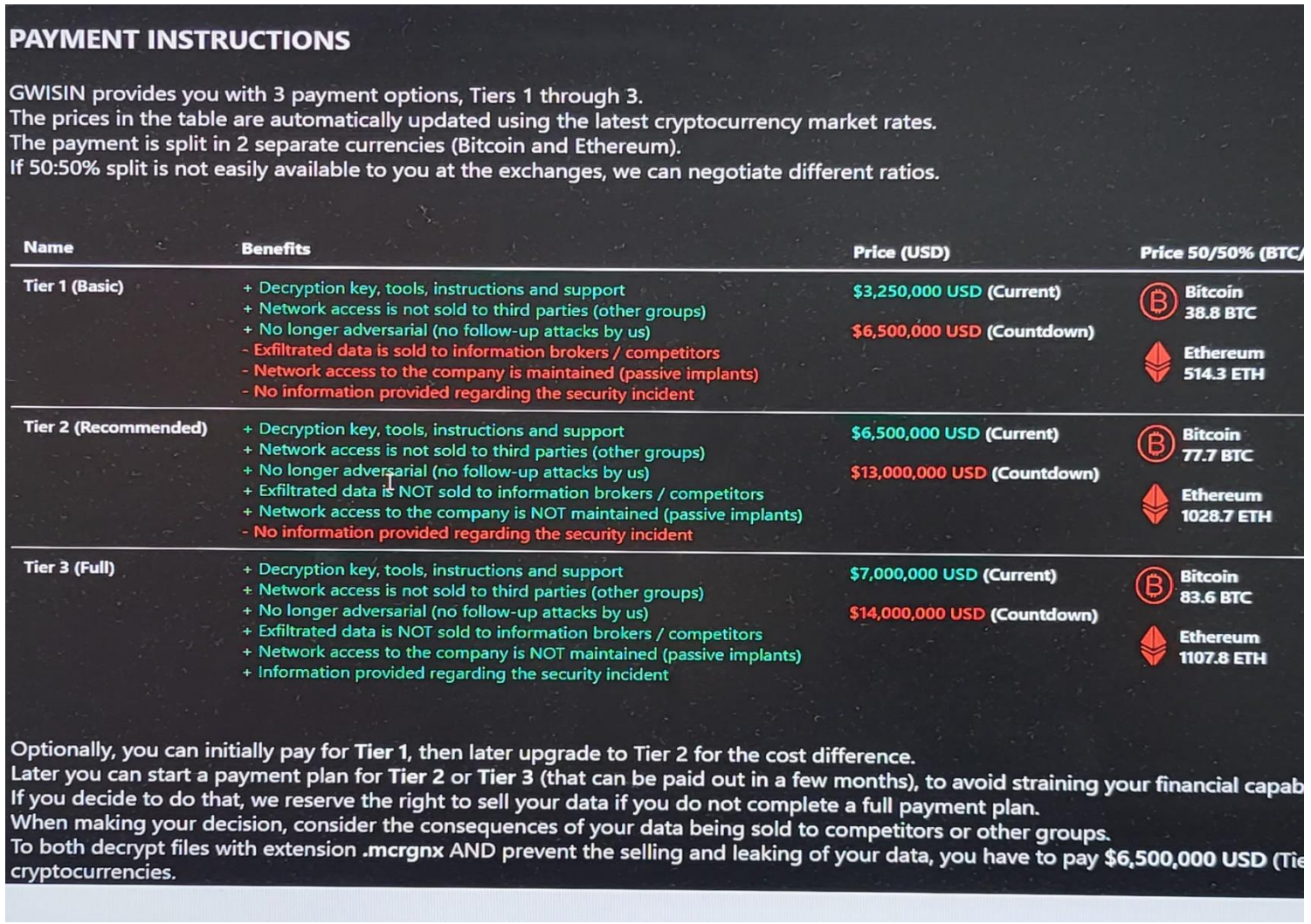
랜섬웨어 사례분석

랜섬 노트 실제 사진-GWISIN Ransomware 한국 기업 맞춤형 랜섬웨어



랜섬웨어 사례분석

조건별 해커의 요구금액 실제 사진



PAYMENT INSTRUCTIONS

GWISIN provides you with 3 payment options, Tiers 1 through 3.
The prices in the table are automatically updated using the latest cryptocurrency market rates.
The payment is split in 2 separate currencies (Bitcoin and Ethereum).
If 50:50% split is not easily available to you at the exchanges, we can negotiate different ratios.

Name	Benefits	Price (USD)	Price 50/50% (BTC/
Tier 1 (Basic)	+ Decryption key, tools, instructions and support + Network access is not sold to third parties (other groups) + No longer adversarial (no follow-up attacks by us) - Exfiltrated data is sold to information brokers / competitors - Network access to the company is maintained (passive implants) - No information provided regarding the security incident	$3,250,000 USD (Current) $6,500,000 USD (Countdown)	Bitcoin 38.8 BTC Ethereum 514.3 ETH
Tier 2 (Recommended)	+ Decryption key, tools, instructions and support + Network access is not sold to third parties (other groups) + No longer adversarial (no follow-up attacks by us) + Exfiltrated data is NOT sold to information brokers / competitors + Network access to the company is NOT maintained (passive implants) - No information provided regarding the security incident	$6,500,000 USD (Current) $13,000,000 USD (Countdown)	Bitcoin 77.7 BTC Ethereum 1028.7 ETH
Tier 3 (Full)	+ Decryption key, tools, instructions and support + Network access is not sold to third parties (other groups) + No longer adversarial (no follow-up attacks by us) + Exfiltrated data is NOT sold to information brokers / competitors + Network access to the company is NOT maintained (passive implants) + Information provided regarding the security incident	$7,000,000 USD (Current) $14,000,000 USD (Countdown)	Bitcoin 83.6 BTC Ethereum 1107.8 ETH

Optionally, you can initially pay for **Tier 1**, then later upgrade to Tier 2 for the cost difference.
Later you can start a payment plan for **Tier 2** or **Tier 3** (that can be paid out in a few months), to avoid straining your financial capab
If you decide to do that, we reserve the right to sell your data if you do not complete a full payment plan.
When making your decision, consider the consequences of your data being sold to competitors or other groups.
To both decrypt files with extension **.mcrgnx** AND prevent the selling and leaking of your data, you have to pay **$6,500,000 USD** (Tie
cryptocurrencies.

2022 랜섬웨어 공격기법 분석

1단계 : 침투 경로 확보

-관리자 ID/PW 해킹 (30~60일 소요)
-RDP 경유 해킹 /웹서버 취약점 해킹

2단계 : 백업 삭제-데이터 탈취-암호화

-백신 및 보안제품 삭제
-백업 데이터 삭제 및 백업 시스템 무력화
-민감 데이터 탈취 및 암호화

3단계 : 금전 요구-다크웹 유포/거래

-금전 요구
-불응시 민감 정보 다크웹 유포/거래

랜섬웨어 침해시 4대 조치사항

1 비상 업무 시스템 가동 (Resilience)

- -가동 가능한 모든 자원 동원 (개인보유 이메일 송수신자료 등)
- -클라우드 활용 임시 가동

2 해커와의 협상

- -해커의 메시지 분석 및 요구사항 확보
- -랜섬 요구액 협상/취약점 분석보고서 요청

3 해킹 경로 추적 및 침해 시스템 안전성 진단

- -전문가 의한 해킹경로 추적 분석
- -침해 시스템 안전성 진단 및 가동여부 결정

4 재발방지 보안조치 및 공조체제 가동

- -추후 재발방지 인적/정책적/관리적/기술적 보안 조치
- -민관 합동 공조체제 가동

랜섬웨어 방어의 최후 보루: 보안백업

01 전통적 백업 개념

IT재해 대비 백업

1. HW 손상 대비 백업
2. 화재 / 태풍 / 지진 대비 원격지 백업

백업 3대 원칙

1. 기기가 달라야 한다.
2. 네트워크가 달라야 한다.
3. 지역이 달라야 한다.

해킹 공격 방어 기능 부재

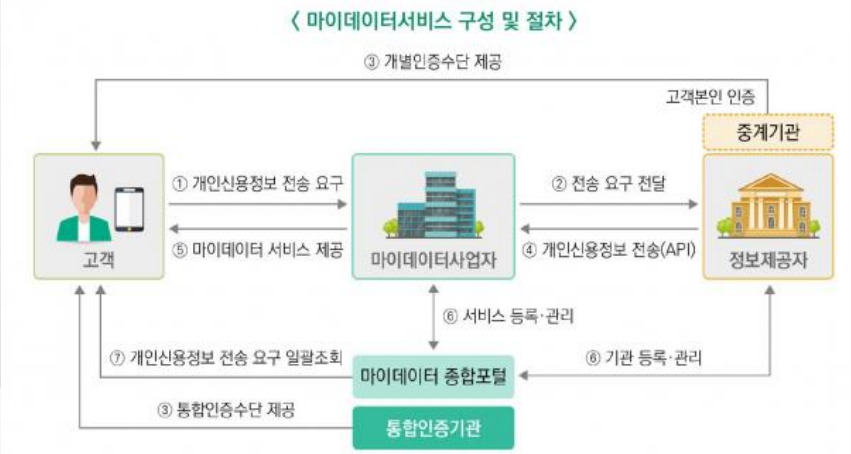
보안백업 정의

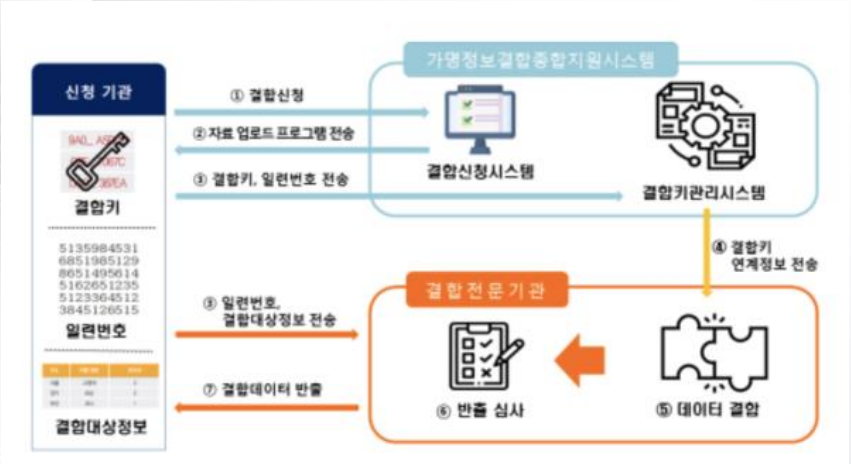
02 리자드백업-보안백업(Secure Backup) 개념

- 랜섬웨어 감염 파일 탐지 및 격리 조치
- 백업 저장소 보호 기능(백업 프로세스 단일 접근)
- 암호화 백업 (AES256/ARIA256)
- 안전한 통신 프로토콜 적용 (SFTP Protocol)
- White-List 기반 프로세스 제어 및 차단 기능
- 행위기반 탐지 차단 기능과 연동

개인정보보호 강화

- 데이터 3법 시행 이후 개인정보 가명정보 사용 확대와 마이데이터 산업 시행 등 개인정보 활용 환경 변화 따른 새로운 개인정보 보안 수요 형성





개인정보 활용 환경 변화

- 20년 8월, 데이터3법 시행 이후 개인정보 활용 환경이 변화하고 있으며 이에 대한 기업들의 보안 수요가 증가하고 있음
- 올 12월, 마이데이터 산업이 시행됨에 따라 40여 개의 금융기관이 참여할 것으로 예상 되며, 하나로 통합된 개인·금융·신용정보 등을 보호하기 마이데이터 산업의 보안 시장이 형성될 것으로 예상
- 가명정보 개념 도입에 따라 가명정보와 결합된 가명정보 활용이 진행되고 있으며, 가명정보 결합가명정보 관련 보관과 전송 가명화 등의 과정에서 개인정보 침해 리스크에 대응하기 위한 보안 수요 형성

레거시 “경계선 보안 " 한계 도달

01 중요 기밀자료 유출 발생

- 유출방법의 고도화로 기존 보안기술 취약점 대두
- 업무 효율성과 보안성과의 충돌
- 외부 협력사에 의한 기밀자료 유출 발생

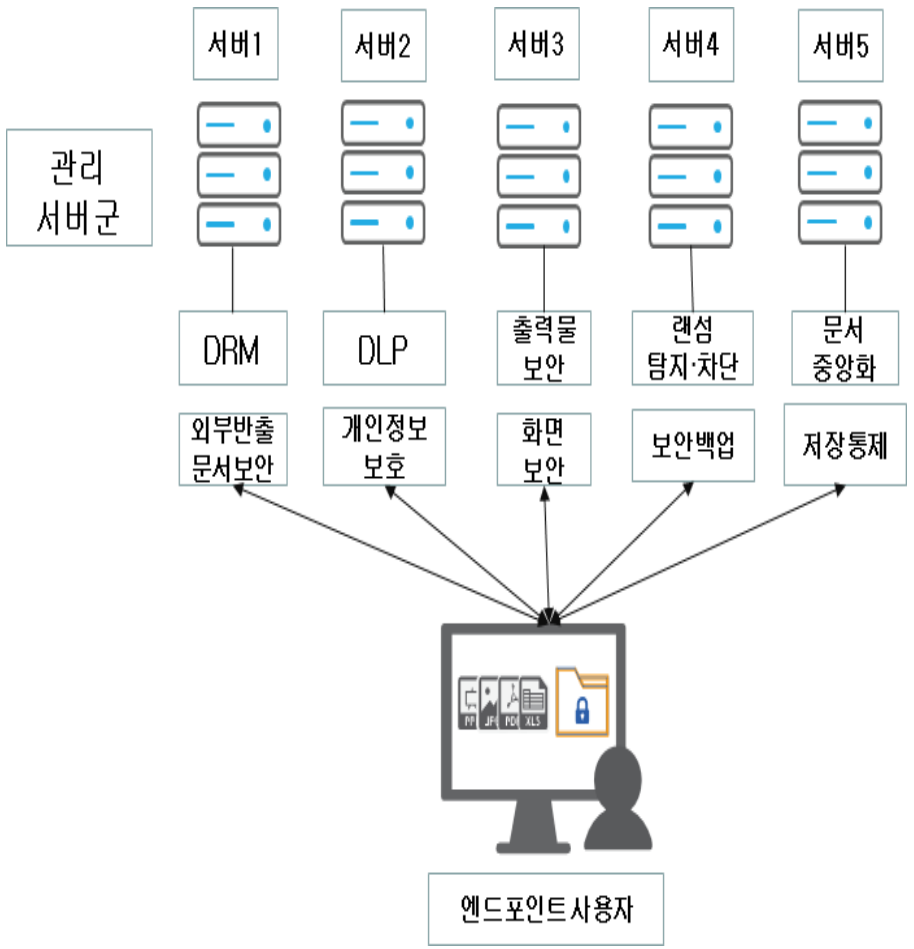
02 랜섬웨어 등 신변종 악성코드 침해

- 시그니처 / 패턴 기반 보안기술의 한계 봉착
- 해커의 기존 보안기술 분석 및 해킹 방법의 지능화
- 사용자 데이터에 대한 파악과 관리 부재
- 법/제도/인증으로 인한 신기술 도입의 시간적 격차 발생

3

제로 트러스트 기반
차세대 지능형 데이터보안 플랫폼
아키텍처

기존 엔드포인트 문서보안 시스템 구조도



[엔드포인트 문서보안 시스템 구성도]

01 과도한 도입 비용 및 유지 비용 발생

02 솔루션별 다수의 전문인력 투입

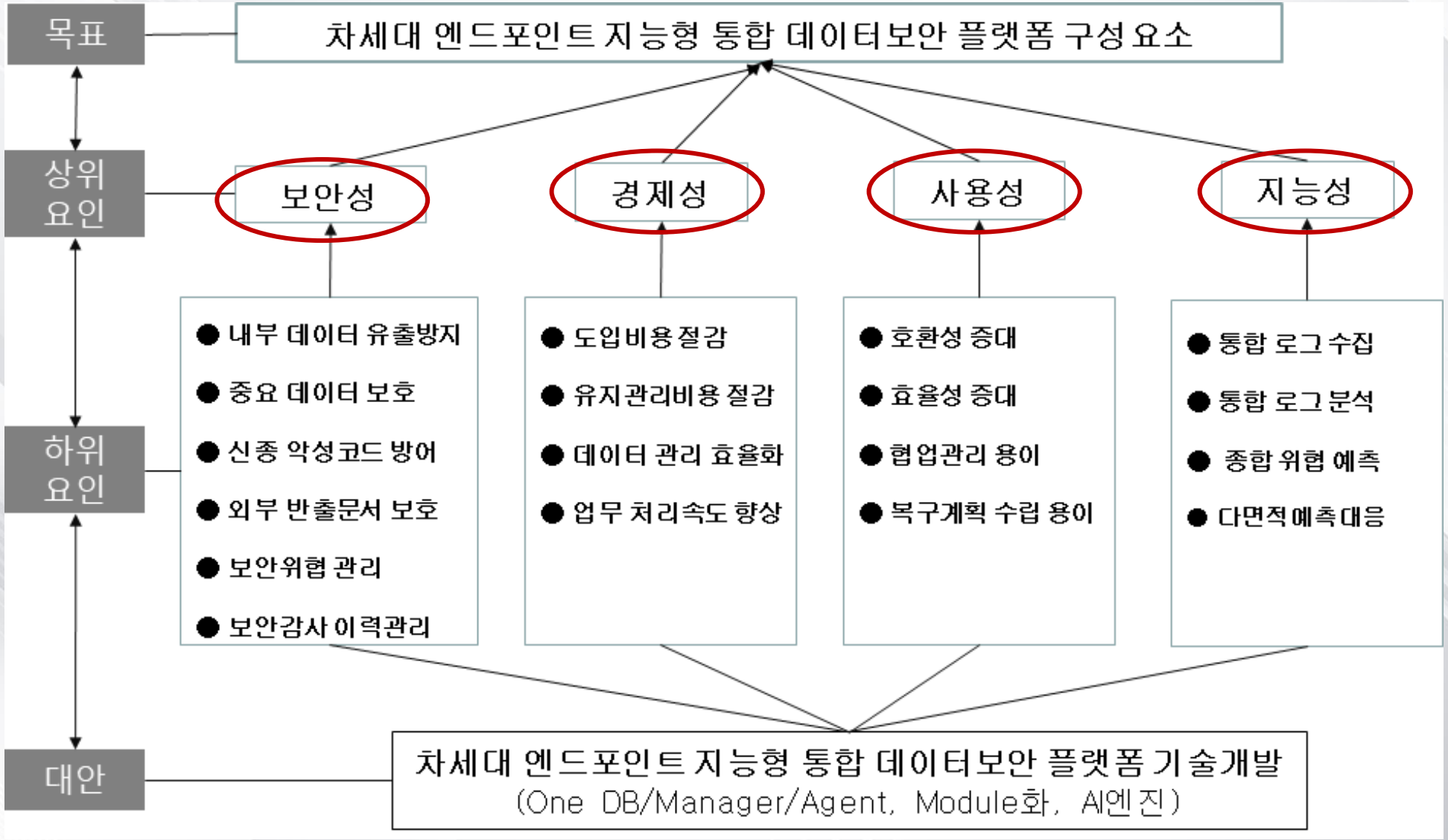
03 신규 도입 및 업데이트 시 충돌 문제 발생

04 연동 등 사용상 다양한 불편함 내재

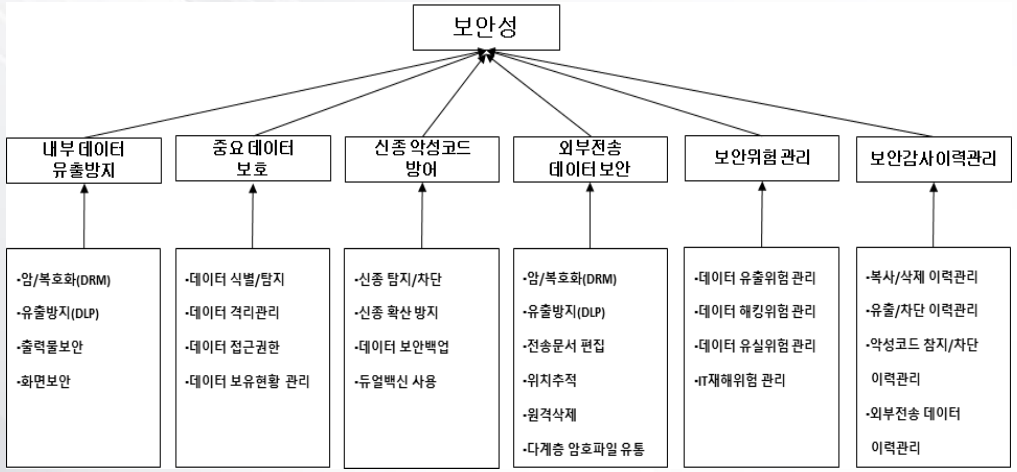
05 데이터 보안 고도화의 어려운 구조

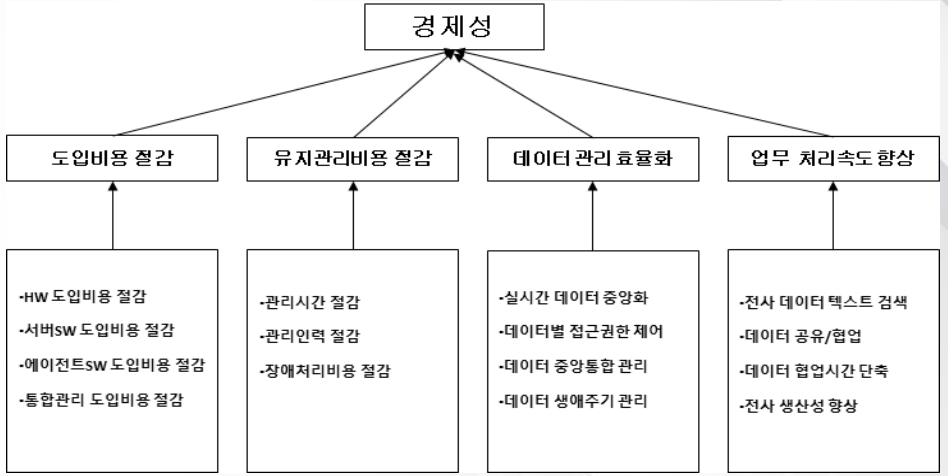
06 데이터 정규화 불가로 AI 접목 불가

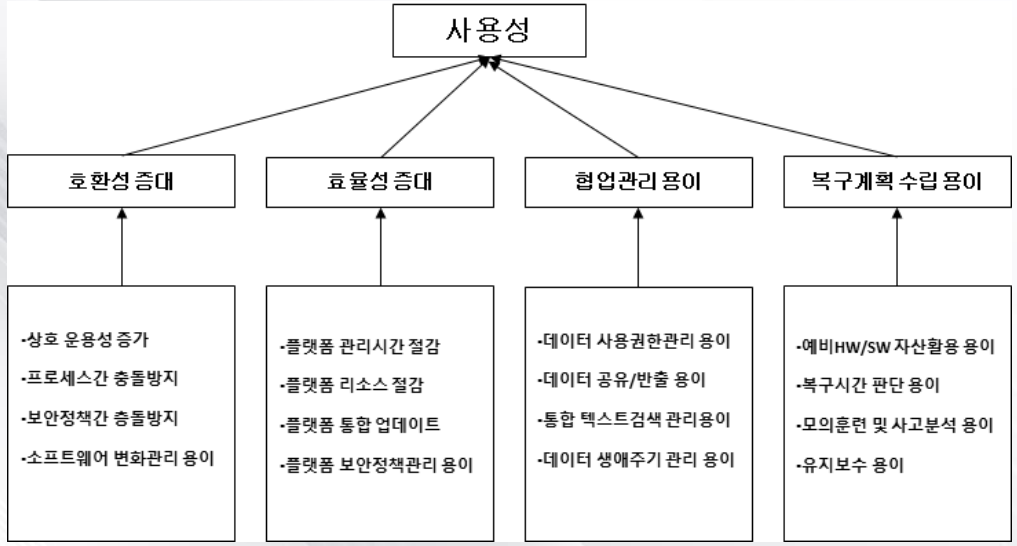
차세대 엔드포인트 데이터 보안기술 연구

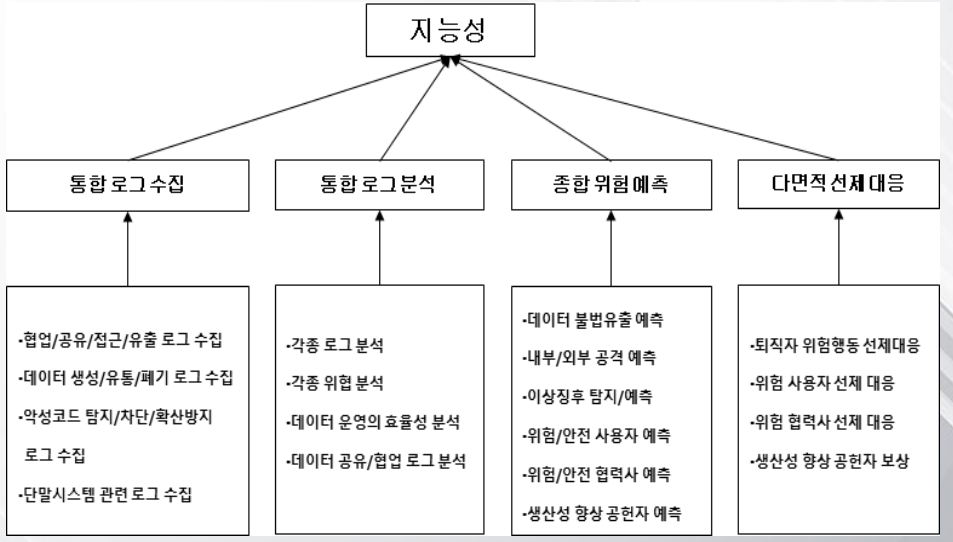


차세대 엔드포인트 데이터 보안기술 연구



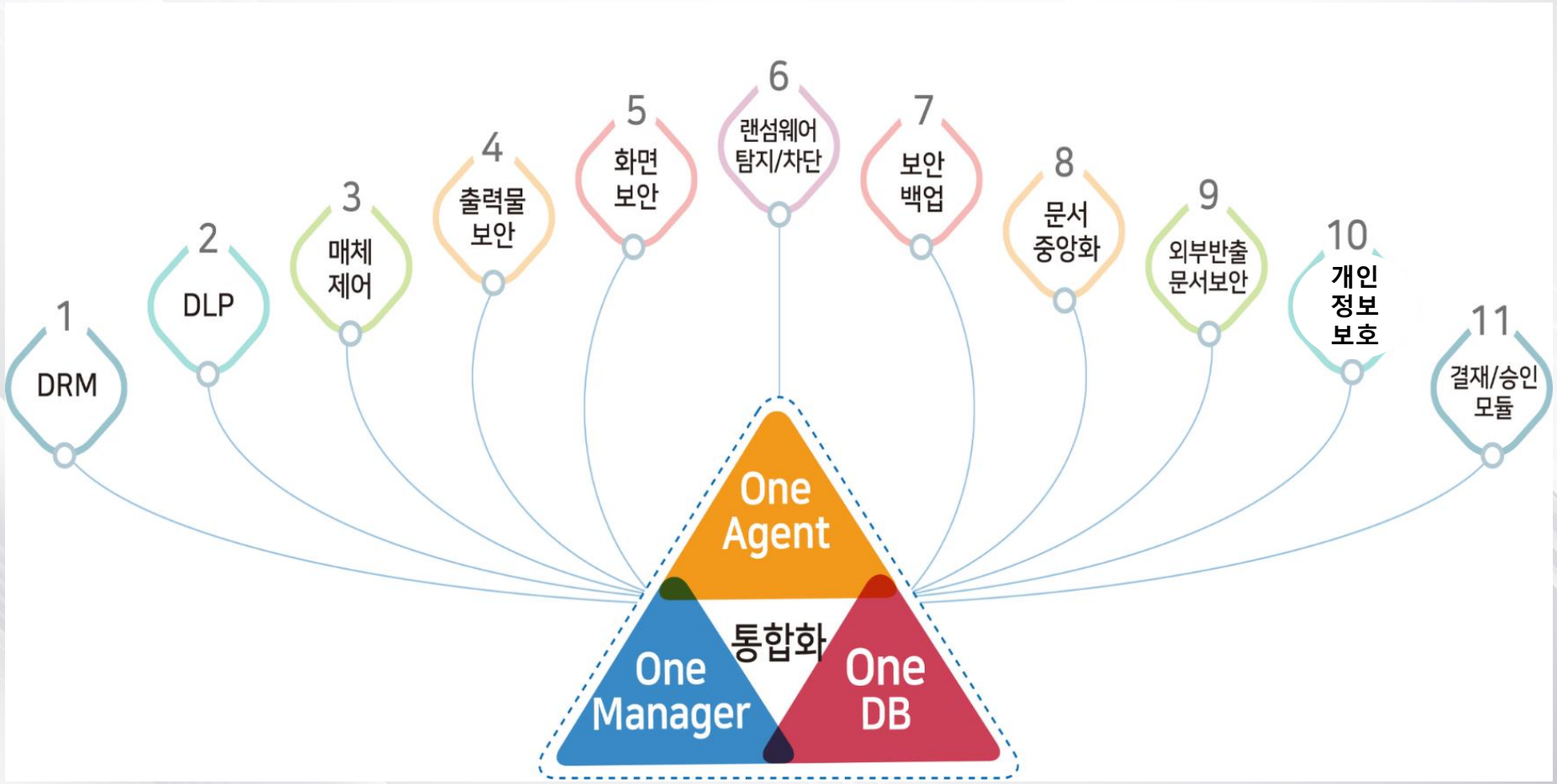




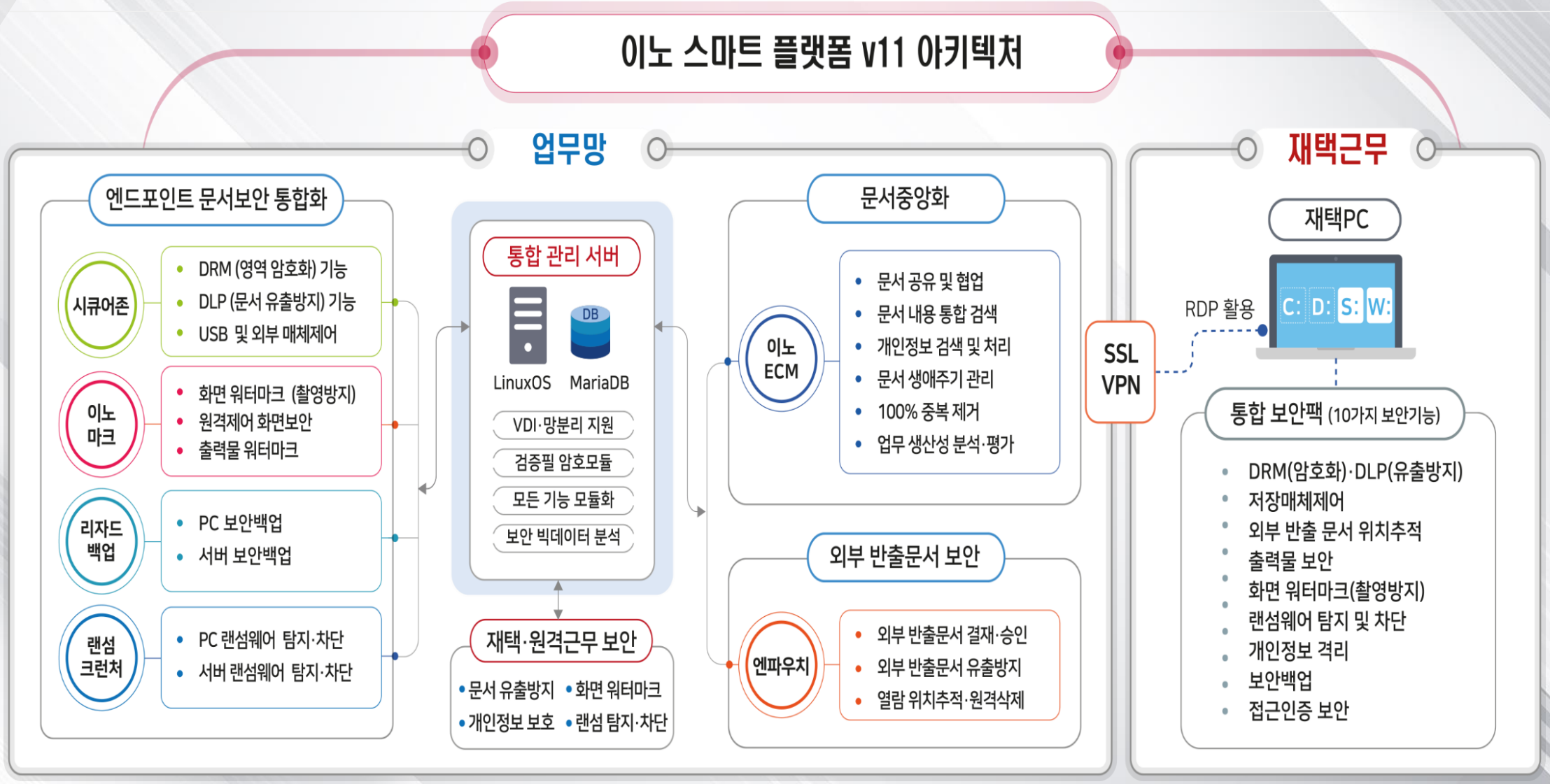


사용자 요구사항

엔드포인트 데이터 보안 사용자들의 오랜 염원 "하나로 안돼?"

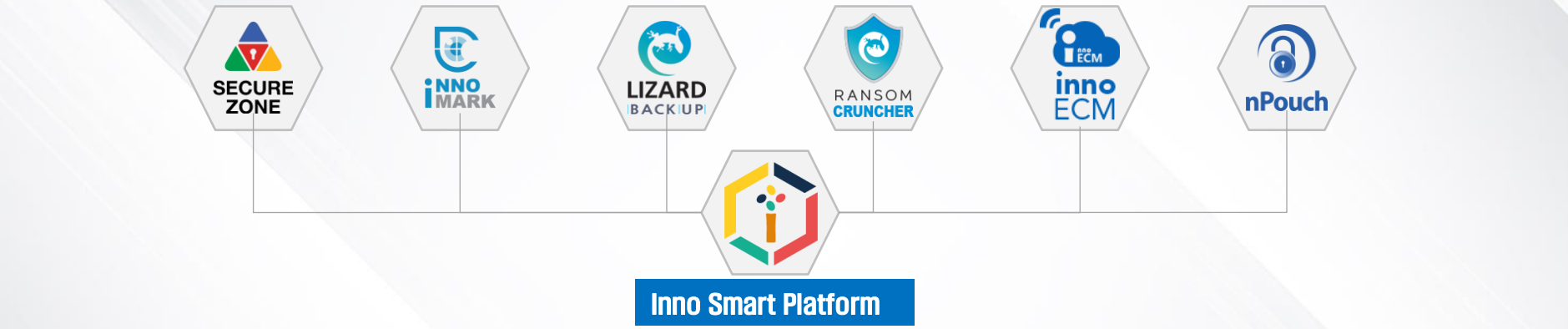


이노 스마트 플랫폼 탄생


이노 스마트 플랫폼 v11 아키텍처
업무망
재택근무
엔드포인트 문서보안 통합화
시큐어존
DRM (영역 암호화) 기능
DLP (문서 유출방지) 기능
USB 및 외부 매체제어
이노 마크
화면 워터마크 (촬영방지)
원격제어 화면보안
출력물 워터마크
리자드 백업
PC 보안백업
서버 보안백업
랜섬 크런처
PC 랜섬웨어 탐지·차단
서버 랜섬웨어 탐지·차단
통합 관리 서버
DB
LinuxOS
MariaDB
VDI·망분리 지원
검증필 암호모듈
모든 기능 모듈화
보안 빅데이터 분석
재택·원격근무 보안
문서 유출방지
화면 워터마크
개인정보 보호
랜섬 탐지·차단
문서중앙화
이노 ECM
문서 공유 및 협업
문서 내용 통합 검색
개인정보 검색 및 처리
문서 생애주기 관리
100% 중복 제거
업무 생산성 분석·평가
외부 반출문서 보안
엔파우치
외부 반출문서 결재·승인
외부 반출문서 유출방지
열람 위치추적·원격삭제
SSL VPN
재택PC
RDP 활용
C: D: S: W:
통합 보안팩 (10가지 보안기능)
DRM(암호화)·DLP(유출방지)
저장매체제어
외부 반출 문서 위치추적
출력물 보안
화면 워터마크(촬영방지)
랜섬웨어 탐지 및 차단
개인정보 격리
보안백업
접근인증 보안

이노 스마트 플랫폼 소개 동영상

사용 목적별 모듈별 구성 매트릭스 (1/2)

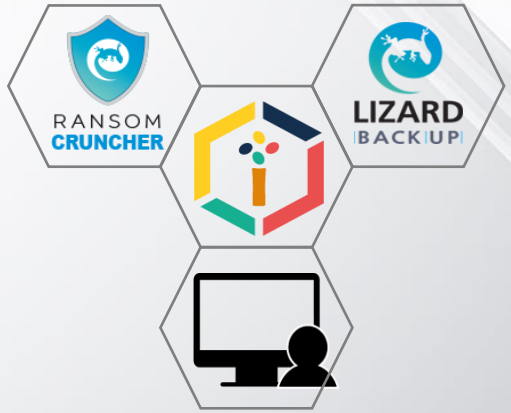


" 고객의 다양한 데이터 보안 요건에 따른 시나리오 별 Object 단위 제품 구성 "

재택/원격근무 데이터 보안	협력업체 협업 보안	랜섬웨어 보안 환경

재택/원격 근무자

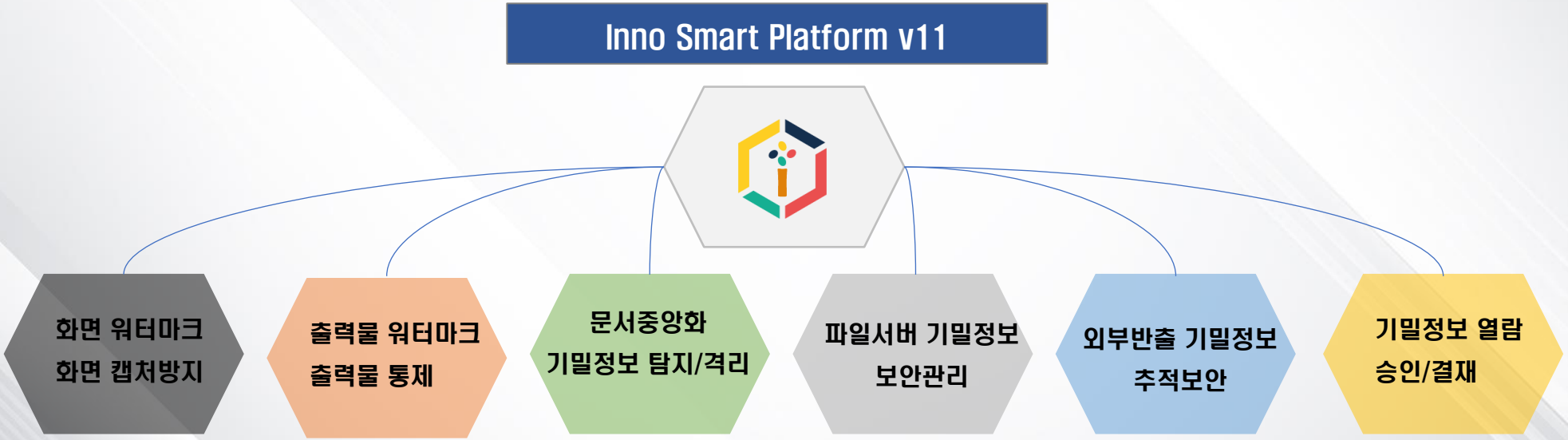
협력사 직원



내부 직원

사용 목적별 모듈별 구성 매트릭스 (2/2)

기관/기업의 기밀정보/데이터 보안플랫폼 아키텍처



" 다양한 기밀정보 보호 상황에 따른 시나리오별 모듈 구성 "

4

이노 스마트 플랫폼 v11

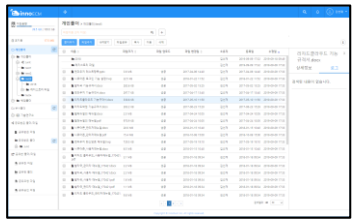
핵심 기능

문서중앙화: 이노ECM (1/3)

문서중앙화: 이노ECM (2/3)

윈도우탐색기

+



WEB 브라우저

중앙화 시스템

개인 폴더

[개인 폴더]
- Junit
- test1
- test2
- test3
- test4

백업 폴더

[백업 폴더]
- sjkim
  - C
  - D
  - dst

부서 폴더

[부서 폴더]
- 기술연구소
- test

협업 폴더

- 공유 받은 파일
- 공유 받은 폴더

문서자산화

개인문서	부서문서	협업문서	백업문서
• 파일 추가 • 파일내려받기 • 파일버전관리 • 파일공유 • 파일분류	• 문서분류 • 파일공유 • 파일권한관리 • 파일버전관리 • 소유자 변경	• 공유승인/거절 • 공유삭제 • 공유받은 폴더/파일 • 공유한 폴더/파일 • 공유승인 폴더	• 파일보안관리 • 파일버전관리 • 파일 암호화 • 기간 검색 • 결과 공유요청

문서활용	권한/보안	통합검색	시스템관리
• 분류 조회 • 부서/개인별 검색 • 삭제/이동/편집/복사 • 다운로드 • 소유권 이전	• 백업문서 보안 • 파일 소유 권한 • 사용자 별 문서 보안	• 부서/개인별 검색 • 제목 검색 • 내용 검색 • 기간 검색 • 결과 공유요청	• 사용자/부서/역할/저장소관리 • 폴더/파일 권한 관리 • 휴지통관리 • 로그관리

보안/암호화 | 접근권한 통제 | 모니터링(통계) | Repository 관리

생성 → 유통 → 보관 → 활용 → 이관 → 폐기

보안파일서버 Framework

컨텐츠 통합저장소

개인 문서 | 부서문서 | 백업문서 | 협업/공유 자료 | …… | 수신문서

Index DB | Content DB

문서저장 | 백업 대상파일 | 사용자 /조직정보 | 통합검색

연계

PC파일 저장 | 보안백업 | 인사조직 | 통합검색

통합검색

조회/검색/활용

일반사용자

전사함 분류/ 문서 관리

관리/운용

시스템 관리자

시스템 운영관리

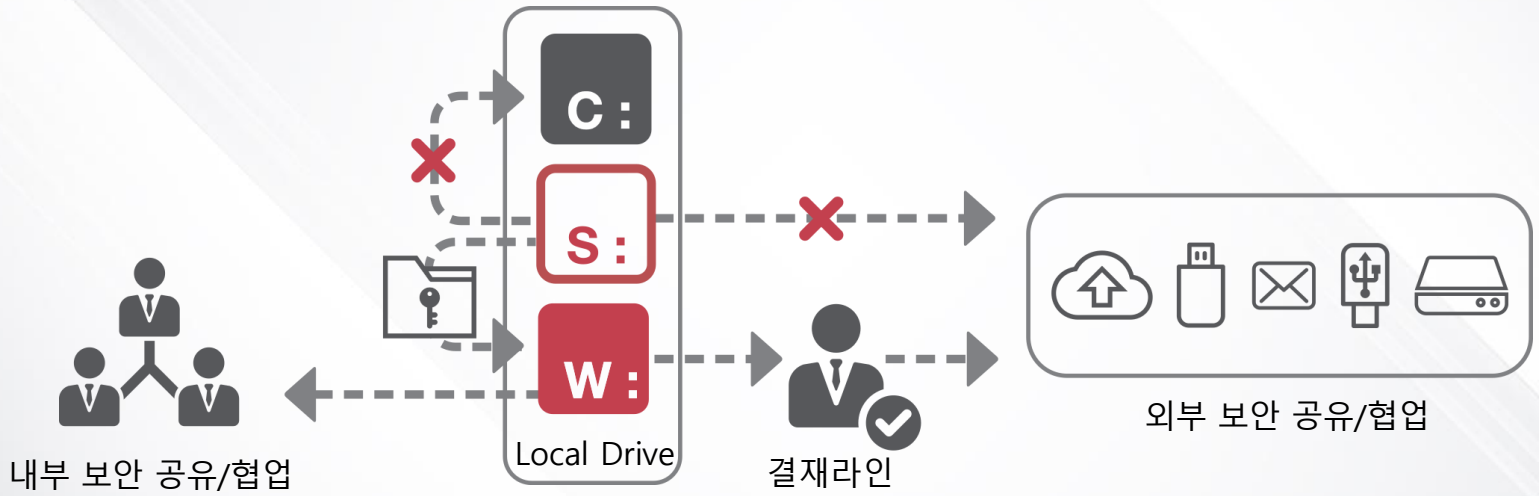
문서중앙화: 이노ECM (3/3)

이노ECM 문서중앙화의 우수성

항목	파일구조 방식	DB구조 방식 (이노ECM)	이노ECM 우수성
글로벌 중복제거 기술	-	탑재	스토리지 확장 비용/시간 절감
5,000명 10GB씩 동일문서 보유시 용량	50 TB (5,000 x 10GB)	10 GB (1 x 10GB)	5,000분의 1 용량
내용 검색 시간	매우 느림	매우 빠름	업무 효율성 극대화
개인정보/기밀정보 자동 분류 및 열람시 결재 기능	-	탑재	개인정보보호 컴플라이언스 강화 및 기밀정보 보안 강화
DRM 대체 기능	-	탑재	국내 2개업체 보유기술
확장비용	고	저	느린 확장주기와 저비용 구조

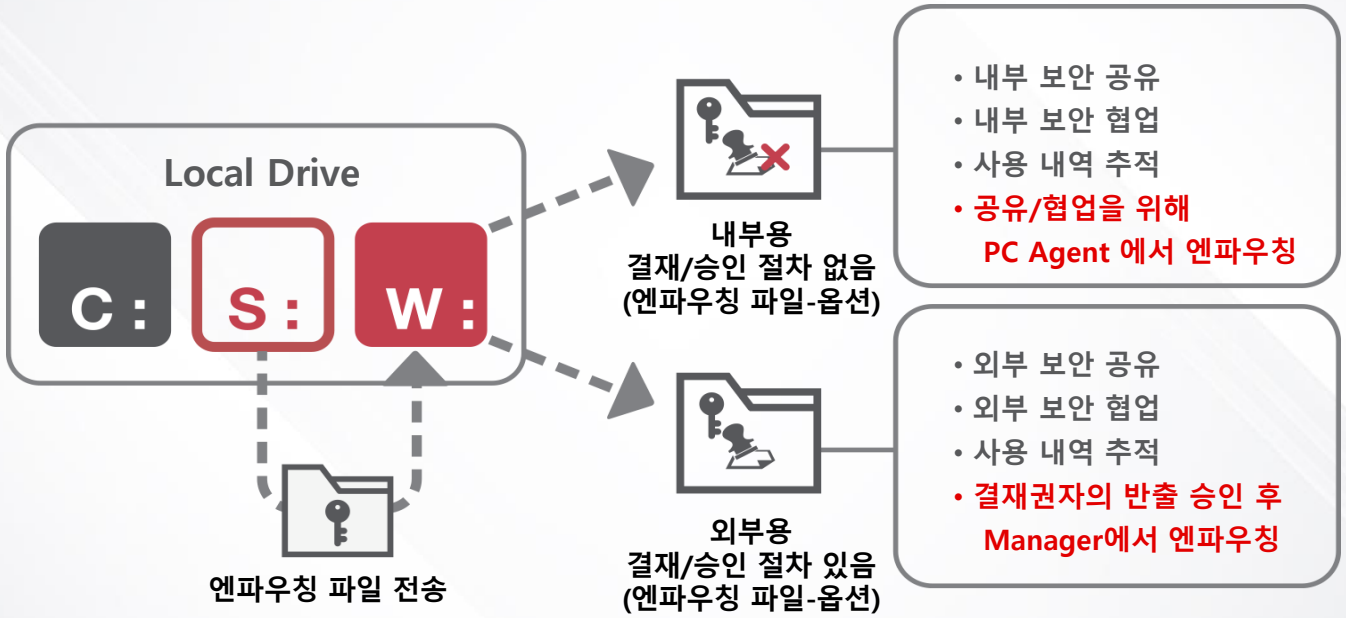
단말기 저장통제/유출방지: 시큐어존 (1/2)

[DRM/DLP Convergence]



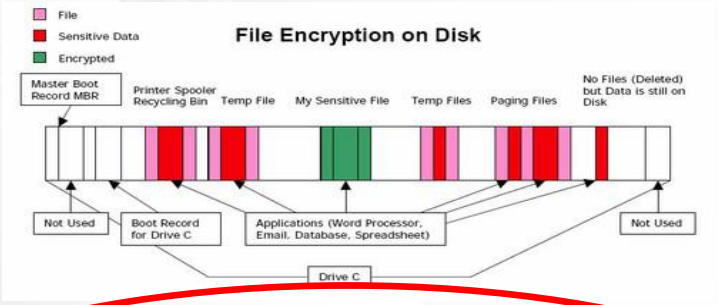
- 사용자 PC의 로컬 디스크에 보안영역(S:)과 반출영역(W:)을 생성, 기업의 중요 정보자산을 사용/협업/보호/반출 추적
- 보안영역(S:)의 데이터는 저장소 내에서만 사용되며 여타 매체로 저장, 사본저장, 이동, 화면캡쳐, 전송 불가
- 내부 협업 또는 외부 반출 필요 시, 반출영역(W:)에 전송하여 DRM 패키징(엔파우칭) 수행
- PC환경과 동일한 UI/UX 제공과 기존 후킹방식의 DRM 솔루션의 단점을 개선하여 성능, 유지보수성, 업무효율성 향상

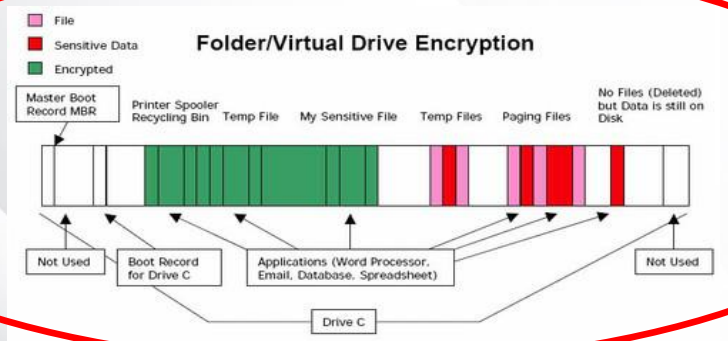
단말기 저장통제/유출방지: 시큐어존 (2/2)

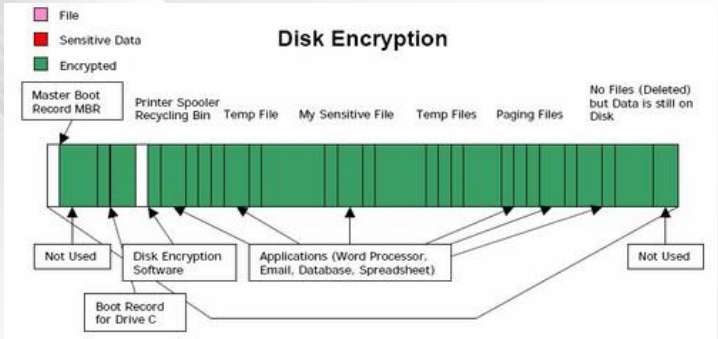


- 내부 협업 또는 외부 반출 필요 시, 반출영역(W:)을 경유하여 엔파우칭(DRM 패키징) 및 반출결재 프로세스 수행
- **내부용은 업무효율성을 위하여 결재/승인 절차를 배제하고 외부반출 협업 시에만 반출결재 프로세스 적용**
- 문서 반출을 위한 결재 프로세스 모듈을 기본 제공하여 반출/승인 간소화와 저비용, 고효율 제공

외부 반출문서 유출방지 및 추적: 엔파우치







nPouch
엔파우치

GPS기반 위치추적

유출방지

ARIA256 · AES256
도면 · 문서 · 영상
1MB~1TB 용량 암호화
DRM · DLP · 매체제어
화면보안 · 출력물보안
프로세스접근제어
캡처 · 클립보드 차단

원격삭제

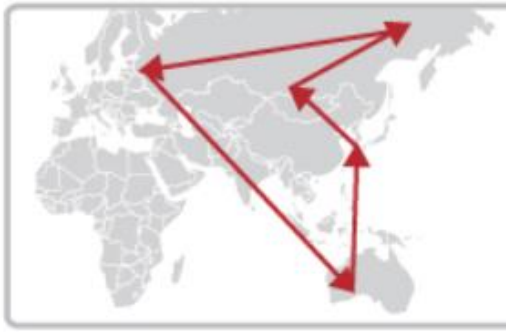
다계층 암호화

외부 반출문서 유출방지 및 추적: 엔파우치

국내 및 해외 국가별 정상/비정상 열람 분석

1	대한민국	100
2	중국	48
3	오스트레일리아	38
4	프랑스	38
5	러시아	28

기밀자료 데이터 이동경로 추적 분석

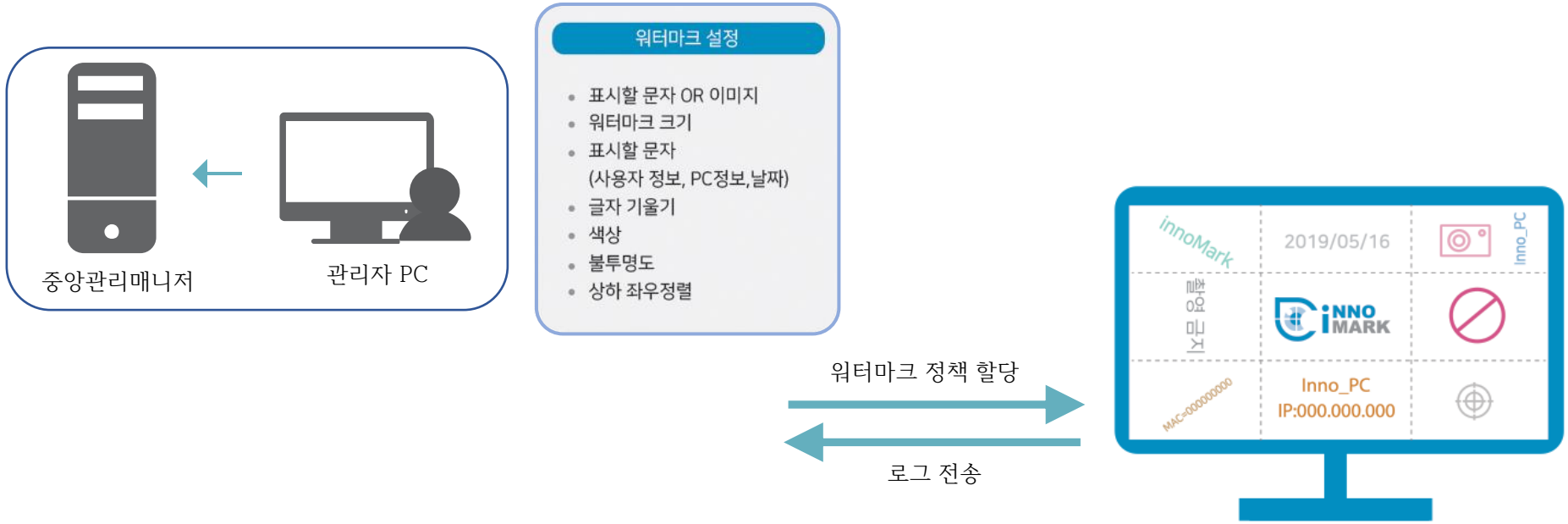


1	대한민국	100
2	중국	48
3	오스트레일리아	38
4	프랑스	38
5	러시아	28

엔파우치 핵심기능

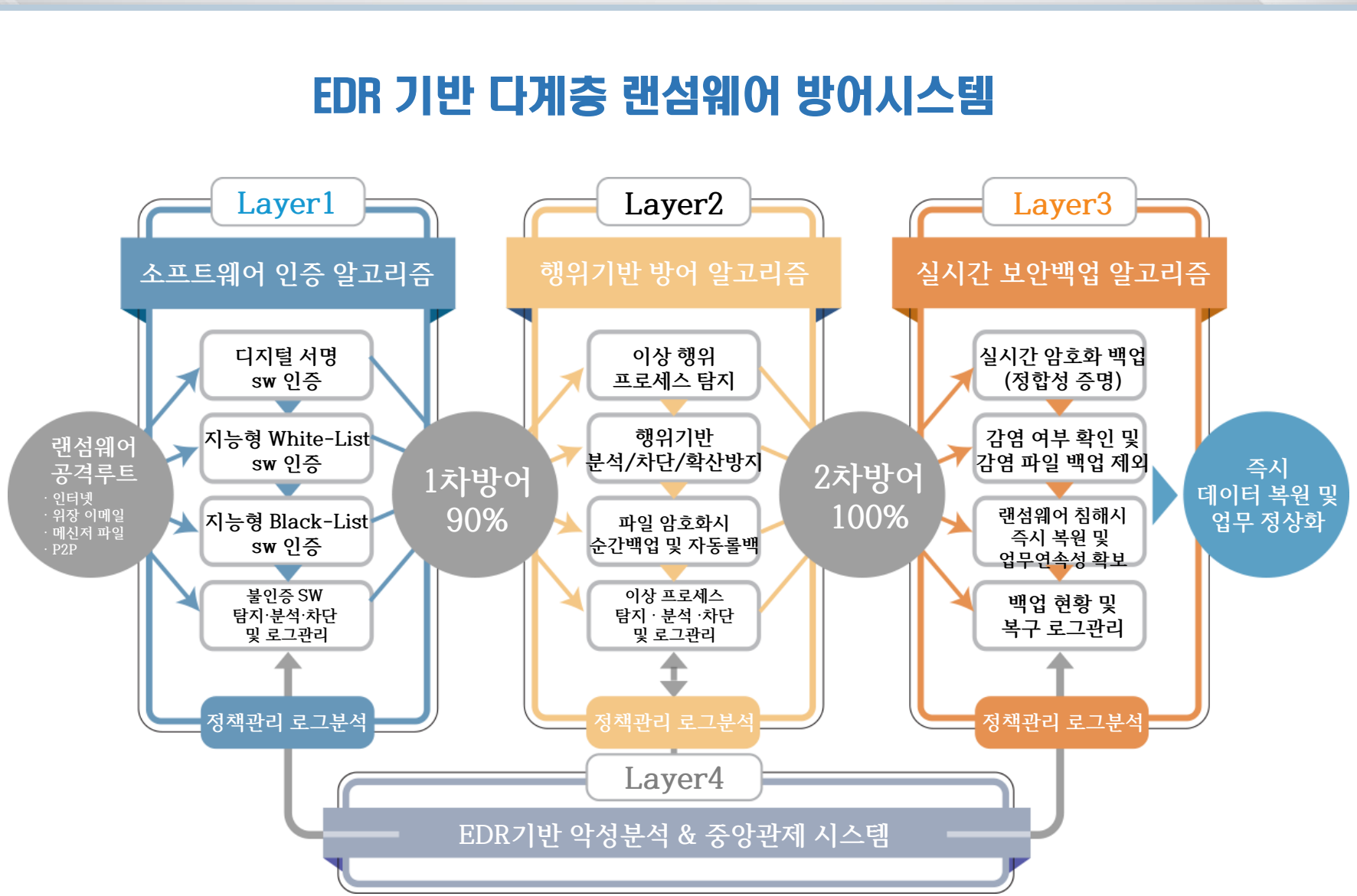
- 문서·도면·영상 영역 암호화 알고리즘
- 열람 추적 관리 및 원격 폐기
- 1~n차 협력사 간 보안협업
- 화면 및 출력물 워터마크
- 오프라인 시 유출방지 및 추적 기능
- 중앙관리
- 위험도 예측 분석

이노마크: 화면 워터마크/화면캡처방지



- 사용자 정보 및 PC 정보 화면 워터마크 설정(사번, 사용자 이름, IP, MAC등)
- 회사 로고 및 촬영 방지 이미지 삽입 가능
- 워터마크 크기 증감, 각도, 위치, 색상, 농도, 미리보기 기능 제공
- 내/외부 인지기반 워터마크 기술로 카메라 촬영방지
- Filter-Layer 화면 워터마킹 기술 기반
- 사용자 정보 화면워터마크(사번,사용자명)
- 사용자 PC 화면 워터마크 (IP, Mac)
- 사용일시 화면 워터마크(연도,월,일,시,분)
- 특정 문구 삽입(기밀, 대외비)

랜섬웨어 방어: 랜섬크런처 / 리자드백업



랜섬웨어 탐지 서비스 특장점

00 랜섬크런처- 랜섬웨어 탐지 차단

- 시그니처 기반 방식대비, 실행 파일의 일치 혹은 유사도를 판별하는 기법
- 패킹 기술과 같은 실행파일 난수화를 통한 감염에 무력화
- 랜섬크런처는 랜섬웨어의 행위 분석을 통해 탐지/차단
- 변화하는 공격방식을 보완하고 안전성을 담보한 서비스 제공
- 랜섬웨어 의심 시 종료(kill)이 아닌, 일시정지(suspend)하며 관리자 및 사용자의 판단을 통해 예외 처리되면 재실행(resume)되는 형태 관제팀과 협업

보안백업: 리자드백업

백업자동정리
암호화 · 압축 · 로그인
유휴타임 백업

대용량 파일 백업
이력관리
잠긴 파일 백업
클라우드 시스템 지원

서버DB 백업
MS-SQL Hot 백업
증분/차등 백업
백업이력 통보기능
중앙정책설정 · 로그관리

실시간 · 스케줄 백업
단방향 · 양방향 백업
랜섬웨어 대응 백업 저장소 보호

재택근무/원격근무용 단말기 보안

파일 저장통제 보안 기능

- 파일 보안 관리
- SW 및 URL 실행 통제
- 시스템 보호
- 사용자 관리
- 단말기 무결성 검증 보고
- 단말기 반출 결재/승인 관리

화면 및 원격접속 보안 기능

- 화면 워터마크
- 화면 캡쳐 방지
- 원격접속 관리
- 데이터 유출 방지
- 윈도우OS 안전모드 보안관리

악성코드 방어 기능

- 재택에서 사내로 랜섬웨어 및 악성코드 유입 방지
- MBR 영역의 위변조 차단

5

레퍼런스 소개

금융 레퍼런스

1) D은행 이노ECM(문서중앙화) 구축 사업 개요 & 기대효과

주요 이슈

1 주요 업무 문서 자산화

- 중요문서 체계적 관리 미흡
- 인수인계 절차 부재로 중요 업무 유실
- 자료 출력/유통에 따른 보안 취약
- 팀별 공유 문서는 접근제어 불가로 자료 유출 위험 증가

2 업무 문서 가시성 향상

- 체계적인 자료 분류체계 없음
- 자료 보존등급 및 주기 규정 준수 제약

3 조직 협업역량 극대화

- 개인 PC 문서가 공유되지 않음
- 부서별로 문서공유의 한계가 있음
- 협업 시, 공유 폴더를 이용하여 진행하여 자료의 정합성을 판단하기 어려움

목적 및 기대효과

사업목적

- 근무환경의 디지털전환을 통한 디지털마인드 확산
- 언제 어디서나 근무 가능 한 스마트오피스 환경 구축
- 자료의 중앙 보관 및 관리로 보안강화
- 조직개편 및 인사이동 시 유연한 대응 강화
- 전자문서의 통합 및 체계화를 통한 공유 및 협업지원

사업내용

- 전사 문서 중앙화(ECM) 솔루션 도입
- 내부정보 유출방지를 위한 통합 보안관리체계 구축
  (데이터 보호를 위한 DRM대체 기능 제공)
- 협업 지원, 인수인계 관리 등 스마트워크 환경 구축

기대효과

- 문서 이력관리 및 협업으로 인한 업무의 효율성 극대화
- 사용자PC 통제 강화를 통한 문서유출의 위험 제거
- 악성코드 및 랜섬웨어의 공격에 대응체계 마련으로 업무의 연속성 확보

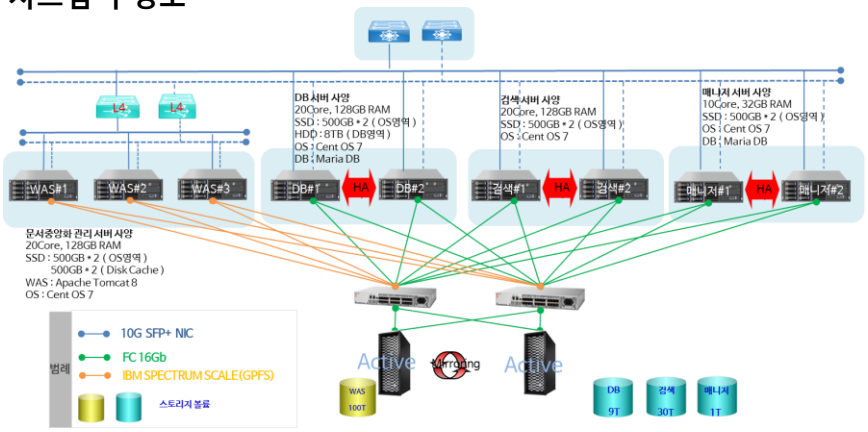
금융 레퍼런스

2) D은행 이노ECM(문서중앙화) 시스템 구성도

공급목록

구 분		제품명	제조사	수 량
SW 및 HW	문서중앙화 솔루션	innoECM v11	㈜이노티움	4,000 User
	DRM 암복호화모듈	마크애니 DRM 암복호화 서버 모듈	마크애니	3식
	Control-M	Control-M	가연정보통신	1식
	바이러스 검출	하우리 백신	하우리	3식
	검색엔진	-	㈜이노티움	1식
구축	사업관리	사업관리(PM)		4MM
	개발	문서중앙화 개발		8MM
	구축	문서중앙화 구축		2MM

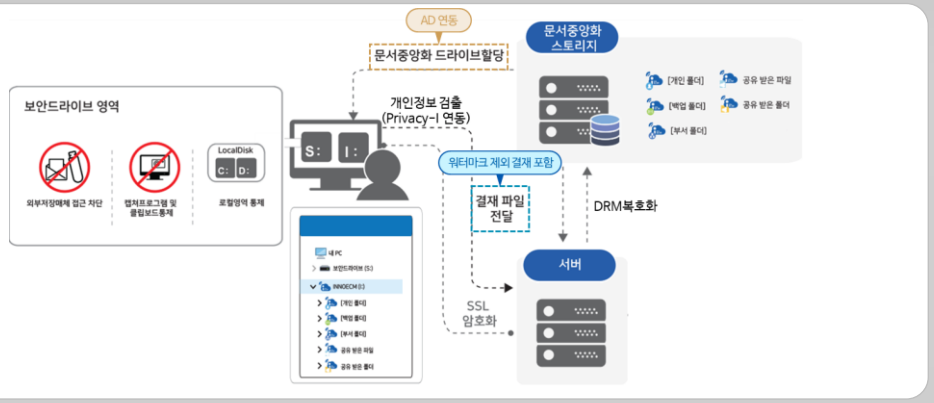
시스템 구성도



제안 특장점

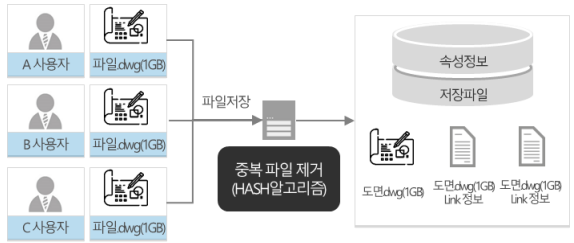
가) DRM 대체 기능 적용

이노ECM은 로컬Agent와 ECM 서버와의 통신 프로토콜은 SSL 암호화 통신 지원하며
문서중앙화 서버에 저장되는 파일은 암호화하여 보관.
파일DRM 대체 기능으로 보안 드라이브 기능과 화면 워터마크 기능 및 매체제어 기능을 제공



나) 글로벌 중복제거 기능

글로벌 파일 중복제거 기능을 통해 전 사 데이터 중 중복 문서를 제거하여 스토리지의 용량 절감



※실시간 중복제거

- 동일 문서 편집 후 저장 시 중복 체크를 통해 서버에서 자체 복제 기능 수행
- 문서중앙화에 저장된 모든 파일 대상으로 중복 파일 모니터링 현황 제공

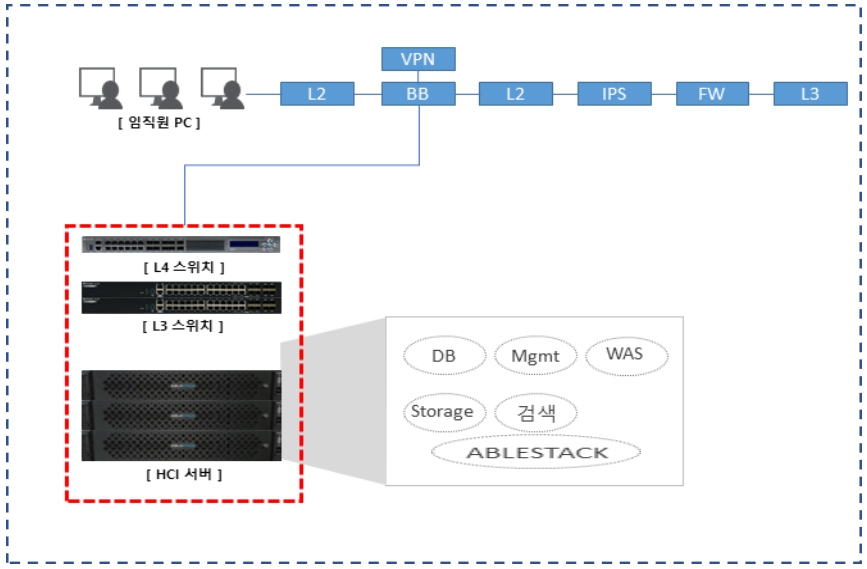
공공 레퍼런스

3) K원(공공) 이노ECM(문서중앙화) 시스템 구성도

공급목록

구 분		제품명	제조사	수 량
SW 및 HW	문서중앙화 솔루션	innoECM v11	㈜이노티움	1,000 User
	백업 솔루션	LizardBackup v11	㈜이노티움	1,000 User
	HCI 솔루션	AbleStack	㈜에이블스토어	1식 (3Node)
	HCI 서버	UX220P-EH	㈜유니와이드	3조

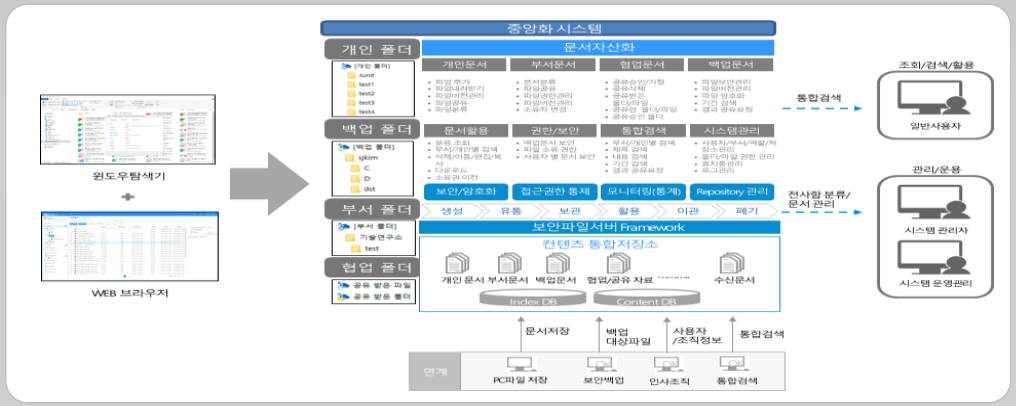
시스템 구성도



제안 특장점

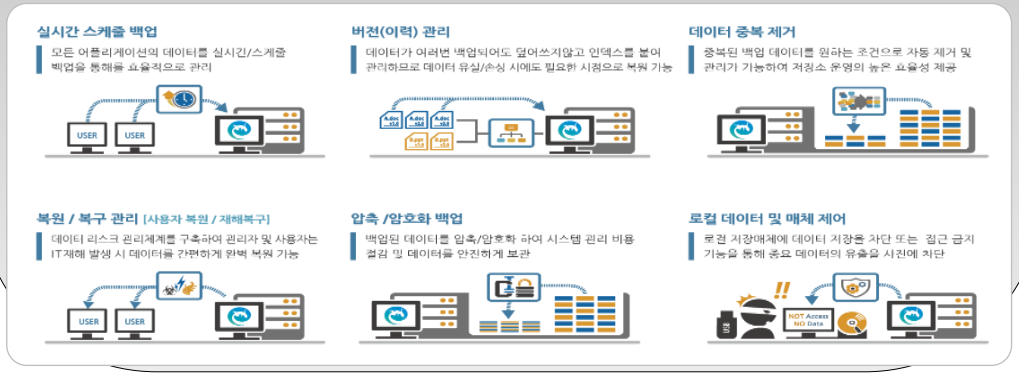
가) 본사 및 지사 문서중앙화 시스템 구축

진주 본원 및 각 지역 지사를 통합하는 문서중앙화 시스템을 구축하였으며,
HCI 기술을 활용하여 단일 HW 환경에서 운영 및 확장이 가능



나) 장애대응을 위한 백업 시스템 구축

HCI 기술을 활용하여 HW내 이중화 및 별도의 백업 시스템을 구축하여 장애시 완벽 대응



2022년
유비무환 보안태세
행복한 대한민국