

Secure Disk

차세대 문서 보안의 표준



INDEX

차세대 문서 보안의 표준 시큐어디스크



01 회사소개 ————— 03 p

02 제안의 개요 ————— 06 p

03 제품 소개 ————— 10 p

04 제품 특징 ————— 12 p

05 상세 기능 ————— 17 p

07 기대 효과 ————— 33 p

08 APPENDIX ————— 35 p

01 회사 소개

01 일반 현황

02 주요 사업 분야

일반 현황

세상을 더 안전하게 만드는 ESTsecurity

(주)이스트시큐리티는 (주)이스트소프트 보안 SW개발 및 서비스 자회사로서 지능형 보안 위협에 대응하는 통합 보안 선도기업 입니다.



회사명	(주)이스트시큐리티 (ESTsecurity Corp.)
대표 이사	정 상 원
법인설립일	2017년 1월 2일
본사소재지	서울특별시 서초구 반포대로 3 (서초동 1464-30) 이스트빌딩
사업분야	보안SW 개발 및 서비스
임직원 수	113명 (2017년1월 기준)
홈페이지	www.estsecurity.com

주요 사업분야

불법문서유출 방지,
편리하고 안전한 협업,
랜섬웨어 공격으로부터 안전한
차세대 문서보안 솔루션



국내외 글로벌
보안/관리 앱시장의 선두주자

1500만개 이상의 센서에서 수집된
악성코드 및 URL 정보를
딥러닝 분석을 통해 신뢰성 있는
보안 인텔리전스로 제공하는 플랫폼

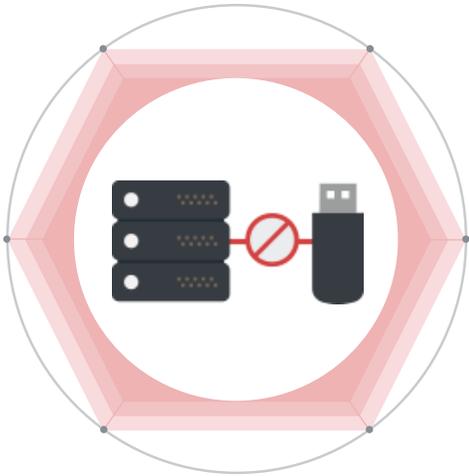
APT 공격에 대해 신속하고
정확한 탐지/대응이
가능토록하는
엔드포인트 보안 솔루션

02 제안 배경

- 01 다양한 문서 보안 이슈
- 02 기존 문서 보안 솔루션

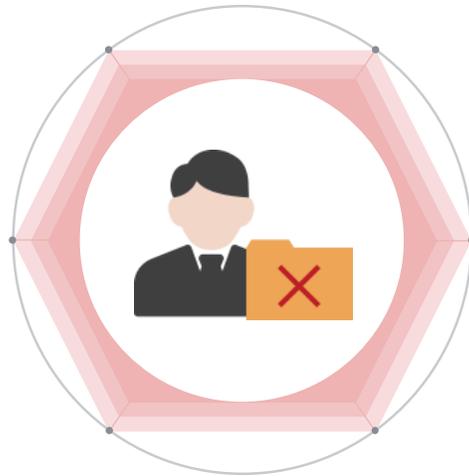
다양한 문서보안 이슈

기업과 기관의 중요 문서 보안 환경을 더욱 효과적으로 구축 할 수 있는 방법은 무엇일까?



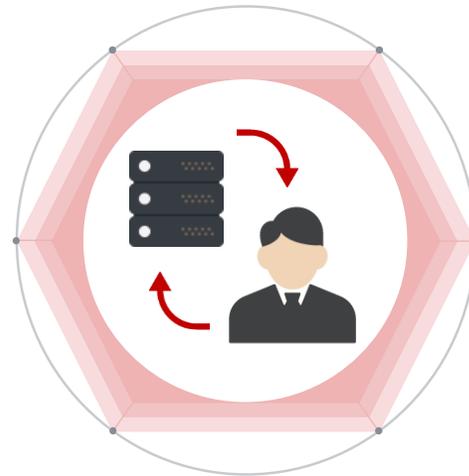
내부 자료 유출 사고 증가

내부 자료/회사 대외비 유출
영업 기밀 경쟁사 유출



문서 유실로 업무 손실 증가

직원 퇴사, 실수로 인한 업무 공백
랜섬웨어 피해 등 대량의 파일 유실



협업이 가능한 문서 보안 환경 필요 증가

협업과 공유가 가능한
문서 보안 환경 부재



내부 문서 자산 가치 증가

내부 문서의 개인화 환경
문서 통합관리 체계 부재

기존 문서 보안 솔루션

기존 문서 보안 솔루션의 한계



01. DRM



02. DLP

제안 배경

기존 문서 보안 솔루션 대비 강점

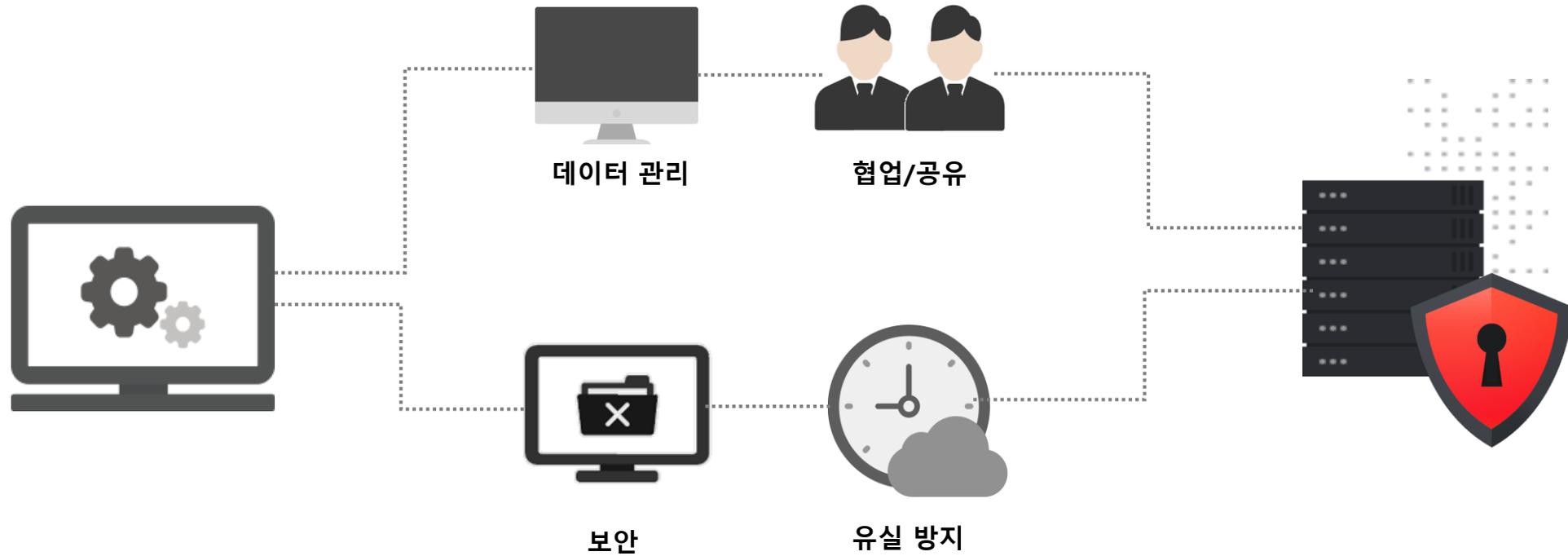
		Secure Disk	DRM	DLP
통합 관리	중앙 집중화를 통한 문서 통합관리	○		
보안	유출 사전 방지 유실 방지 랜섬웨어 피해 방지	○	△	△
공유/협업	개인, 부서 공유 디스크 협업 가능	○		
호환성	종속성 없음 다른 애플리케이션 충돌 가능성 낮음	○		

03 제품 소개

01 제품 소개

제품 소개

문서중앙화를 통해 자료 유출, 유실 방지 및 통합관리가 가능한 차세대 문서보안 솔루션



04 제품 특징

- 01 유출 차단
- 02 유실 방지
- 03 협업 / 공유
- 04 데이터 통합 관리

유출 차단

온라인 경로, 오프라인 경로 및 기타 경로 유출 차단



유실 방지

고의 또는 실수로 문서가 삭제 되거나, 퇴사자에 의해 파일이 유실 되더라도 쉽게 복구 가능



고의, 실수 등으로 **유실된 문서**에 대해서
복원이 가능할까?



파일 삭제



파일 복원

고의 또는 실수 등으로 파일이 삭제되더라도
시큐어디스크 서버 내 삭제된 문서 복구 기능을 통해
복원이 가능합니다.



※Windows의 휴지통 개념과 일부 동일하지만 버전관리, 완전 삭제 기능 설정 등
파일 관리에 최적화된 기능을 제공합니다.

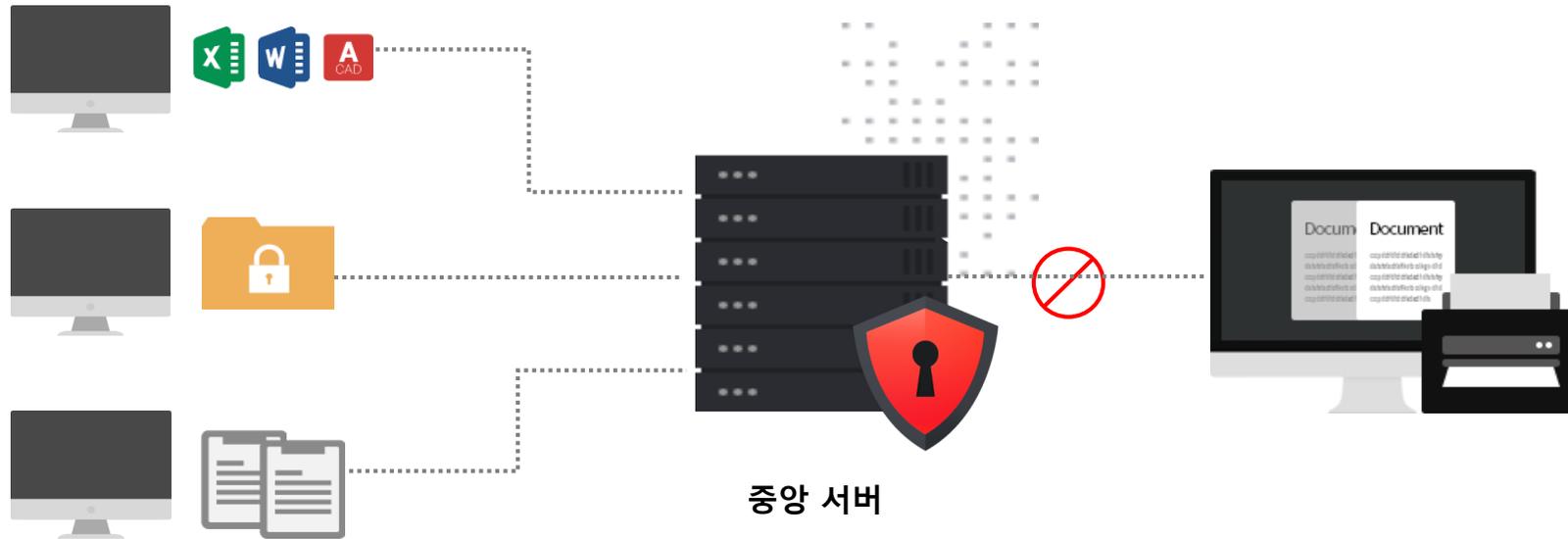
협업 / 공유

목적 별 디스크 생성이 가능하여, 기업 내부 프로젝트 또는 외주 업체간 협업 시 원활한 문서 작업 및 공유 환경 구축



데이터 통합관리

문서중앙화 환경을 통한 PC에 산재된 내부 문서/자료 통합관리



05 상세기능

- 01 사용자 기능
- 02 관리자 기능

보안

보안 정책 적용

보안 대상 프로그램 / 확장자에 대해 제품 설치 시점부터 보안 정책 적용 가능

프로그램/확장자 등록

**보안 대상 프로그램/ 확장자 적용을
등록하여 보안을 적용 할 수 있습니다.**

관리 확장자

▶ 사용자 PC에 존재하거나 저장하지 못하도록 설정할 확장자를 선택해 주세요.
alz:(X) CELL:(X) DOC:(X) DOC*(X) egg:(X) HPT:(X) HWP:(X) lzh:(X) NXL:(X) PDF:(X)
XLS:(X) XLS*(X)

선택



제품 설치 시점부터
정책 위반 파일 확인

정책 위반 파일 강제 이관

파일 이관

검색된 내 PC의 파일을 시큐어디스크로 이관합니다.
파일 개수에 따라 몇 십분이 소요될 수도 있습니다.

파일 이관 중...(61 / 480) 남은 시간 00:00:00

0.00 bytes / 0.00 bytes

파일 이름	파일 크기	파일 상태
<input type="checkbox"/> 강제이관_test - ...	0 bytes	이동 완료
<input type="checkbox"/> 강제이관_test - ...	0 bytes	이동 완료
<input type="checkbox"/> 강제이관_test - ...	0 bytes	이동 완료
<input type="checkbox"/> 강제이관_test - ...	0 bytes	이동 완료
<input type="checkbox"/> 강제이관_test - ...	0 bytes	이동 완료
<input type="checkbox"/> 강제이관_test - ...	0 bytes	이동 완료
<input type="checkbox"/> 강제이관_test - ...	0 bytes	이동 완료
<input type="checkbox"/> 강제이관_test - ...	0 bytes	이동 완료
<input type="checkbox"/> 강제이관_test - ...	0 bytes	파일 비동중...

완료 >

접속방식

윈도우 탐색기 인터페이스

윈도우 탐색기에 문서를 바로 실행/편집하여 타사 자체 개발 인터페이스에 비해 업무 친화성 향상

안전한 파일시스템

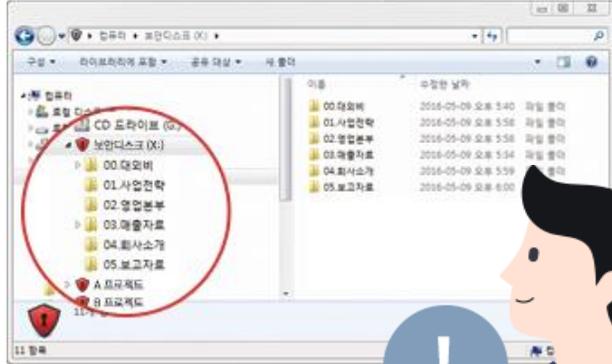


시큐어디스크 윈도우탐색기
 자체 개발 프로토콜(WID) 드라이브 연결
 - EST Windows Network 표시

타사 윈도우탐색기
 공개형 파일시스템 SAMBA 드라이브 연결
 - Microsoft Windows Network 표시

* 랜섬웨어 워너크라이(WannaCry) SMB 프로토콜 취약점 통해 전파
 * SMB 프로토콜 보안 지적 대상

윈도우탐색기 인터페이스



기존과 100%동일한 업무환경

타사 자체 개발 인터페이스



자체 인터페이스로 인한 친화성 부족

협업

목적 별 디스크 생성

목적 별 디스크 생성이 가능하여 기업 내부 프로젝트 또는 외주 업체 간 협업 시 원활한 문서 작업 및 공유 환경 구축



보안

유출 차단 _ 1. 온라인 및 오프라인

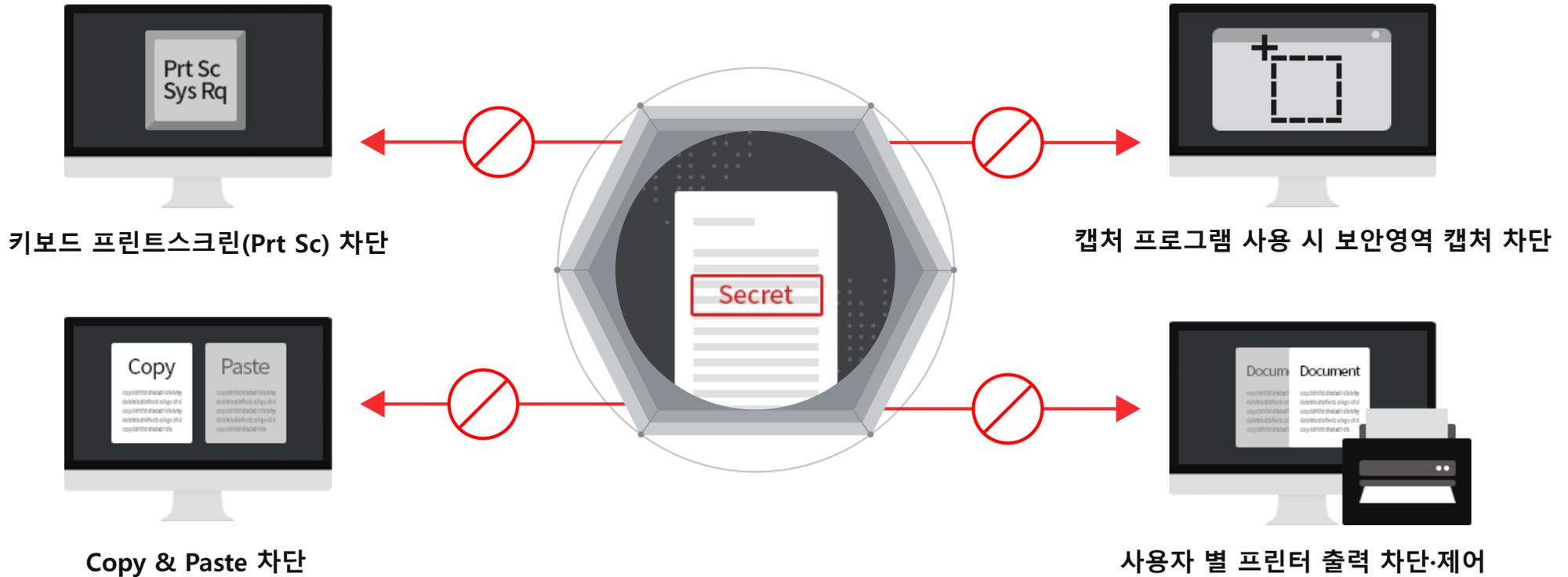
웹 메일, 메신저, 클라우드 저장소, OUTLOOK 등 온라인 매체를 통한 유출과, USB메모리, 외장하드, CD 등 오프라인 매체를 통한 유출 차단



보안

유출 차단 _ 2. 기타경로

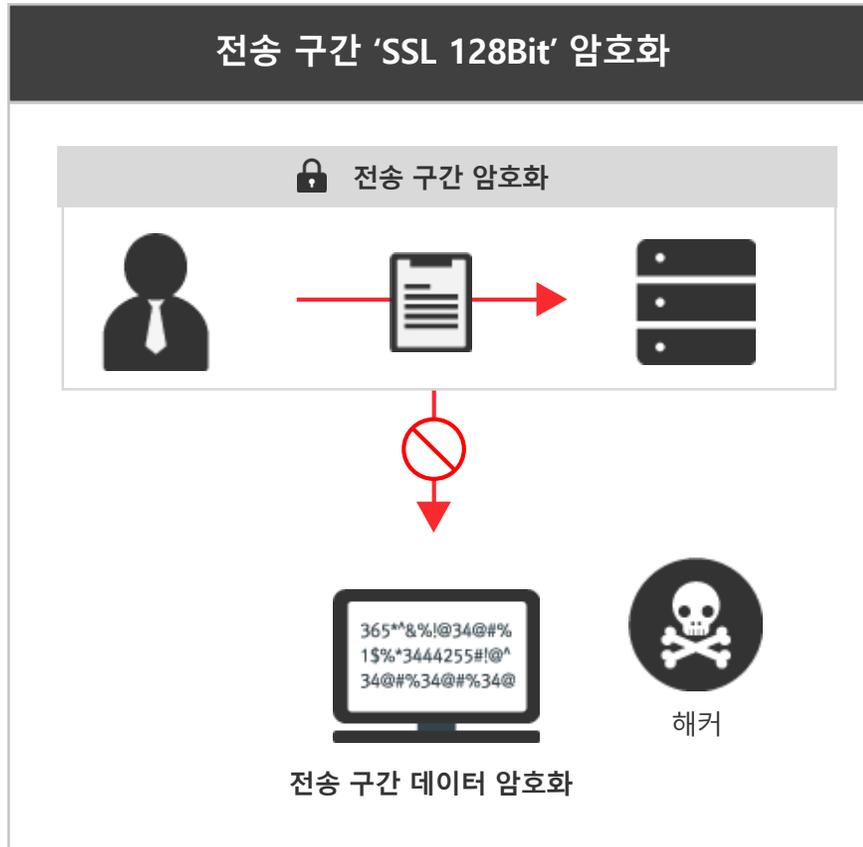
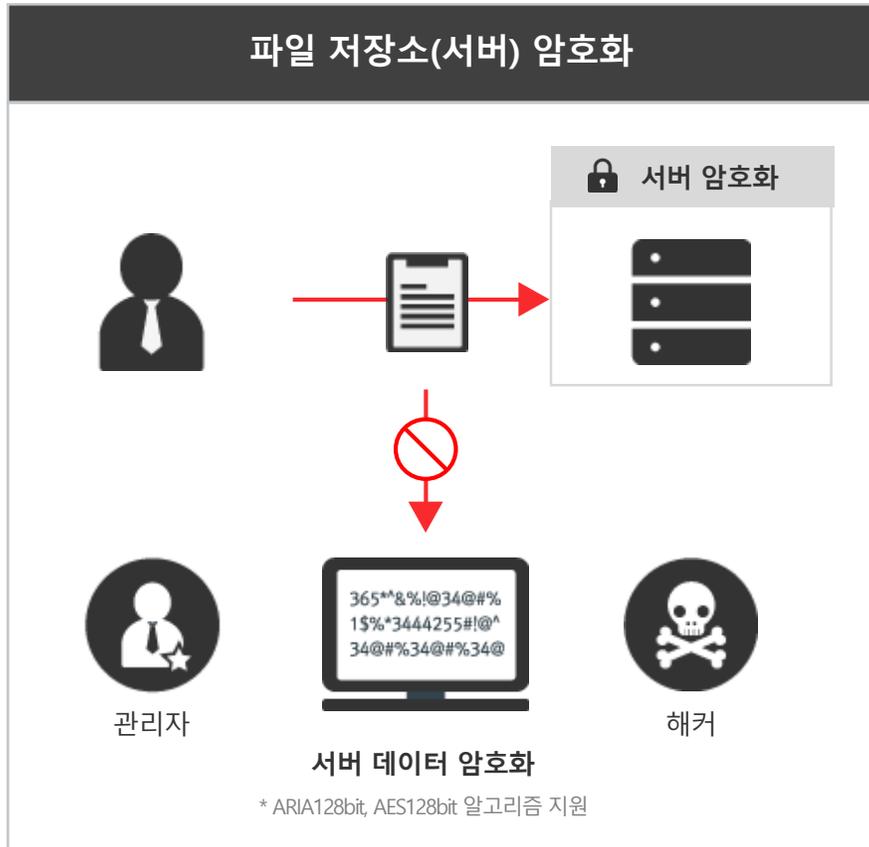
키보드 프린트 스크린, 캡처 프로그램, COPY&PASTE, 프린터 출력 등과 같은 사용자 문서의 다양한 유출 경로 차단



보안

암호화

파일 전송 구간과 서버에 저장된 파일을 암호화 하여, 해킹에 의한 데이터 유출 또는 물리적인 디스크 유출에도 대응



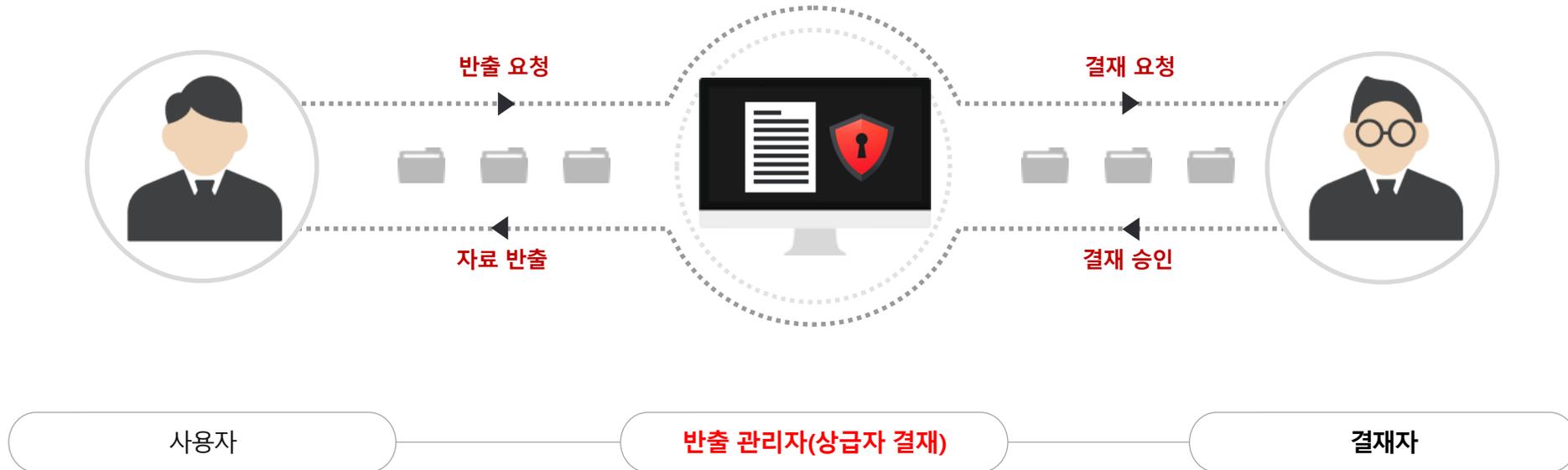
국정원 인증 암호화 모듈

The block features the KCMVP logo, which consists of the text 'KCMVP' in a large blue font above '암호모듈인증' in a smaller black font. Below the logo, the text '국정원 검증필 암호화 모듈 KCMVP 탑재' (Government verification required encryption module KCMVP installed) is displayed.

보안

반출

외부 반출이 필요한 경우 자체 탑재 된 결재 프로세스를 통해 상급자 결재 후 메일 전달 또는 USB, 반출함에 저장 형태로 반출

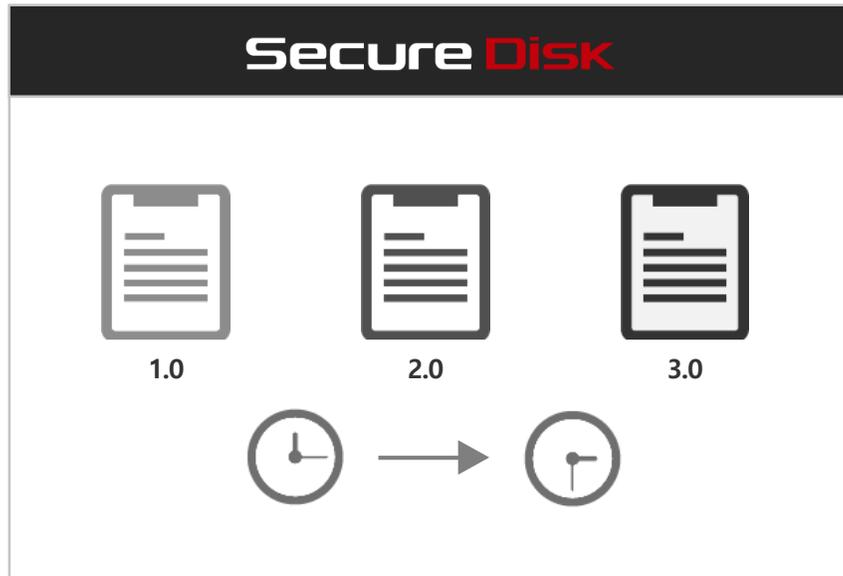


반출함은 파일 이동이 자유로운 디스크 영역이며, 반출함에 반출된 파일은 추가적인 결재 프로세스 없이 사용 가능합니다.

버전 관리

삭제 및 복원

문서 버전 관리 기능을 통해 고의 또는 실수로 문서가 삭제 되거나, 공동작업자에 의해 파일이 유실 되더라도 쉽게 복구 가능



- 사용자PC의 시큐어디스크(D:)는 서버 저장 공간
- 문서 버전 관리

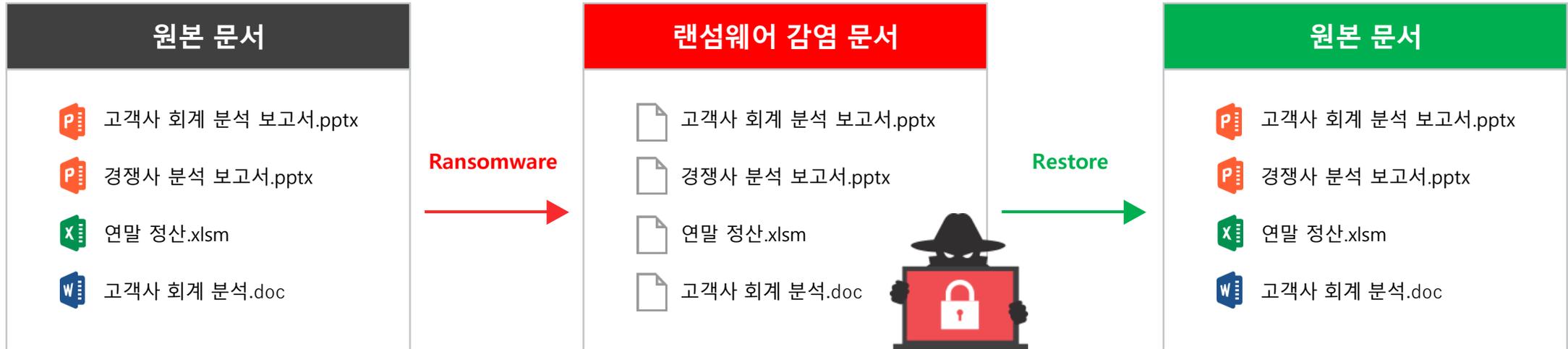


- 변경된 내역이 없어도 내려받기(복원)가능

유실 방지

랜섬웨어 대응

랜섬웨어로 인한 시큐어디스크 내 암호화 된 문서 복원 가능



랜섬웨어로 인한 파일 암호화시 시큐어디스크 내 파일 변경 버전(히스토리) 관리를 통해 일괄 복원 가능합니다.

보안

오프라인 디스크

네트워크가 끊겨 오프라인 상태가 될 경우, 사용자 PC영역에 임시 디스크를 생성하여 암호화 저장을 하고 다시 온라인으로 상태 변경 시 자동 이관 됩니다.



로그

모든 작업 내역 관리

서버 내 모든 파일의 작업 이력 조회, 에이전트 현황 조회, 정책 위반 시도 내역 조회 가능



모든 파일
작업 이력 조회



에이전트
현황 관리



정책 위반
내역 조회

보안

권한 관리

사용자 별 폴더에 관한 접근권한을 설정하여 부서별 특성에 맞는 정책 수립 가능, 제한된 접근과 파일 유통으로 인해 권한 없는 사용자에게 의한 자료 정보 유출 방지

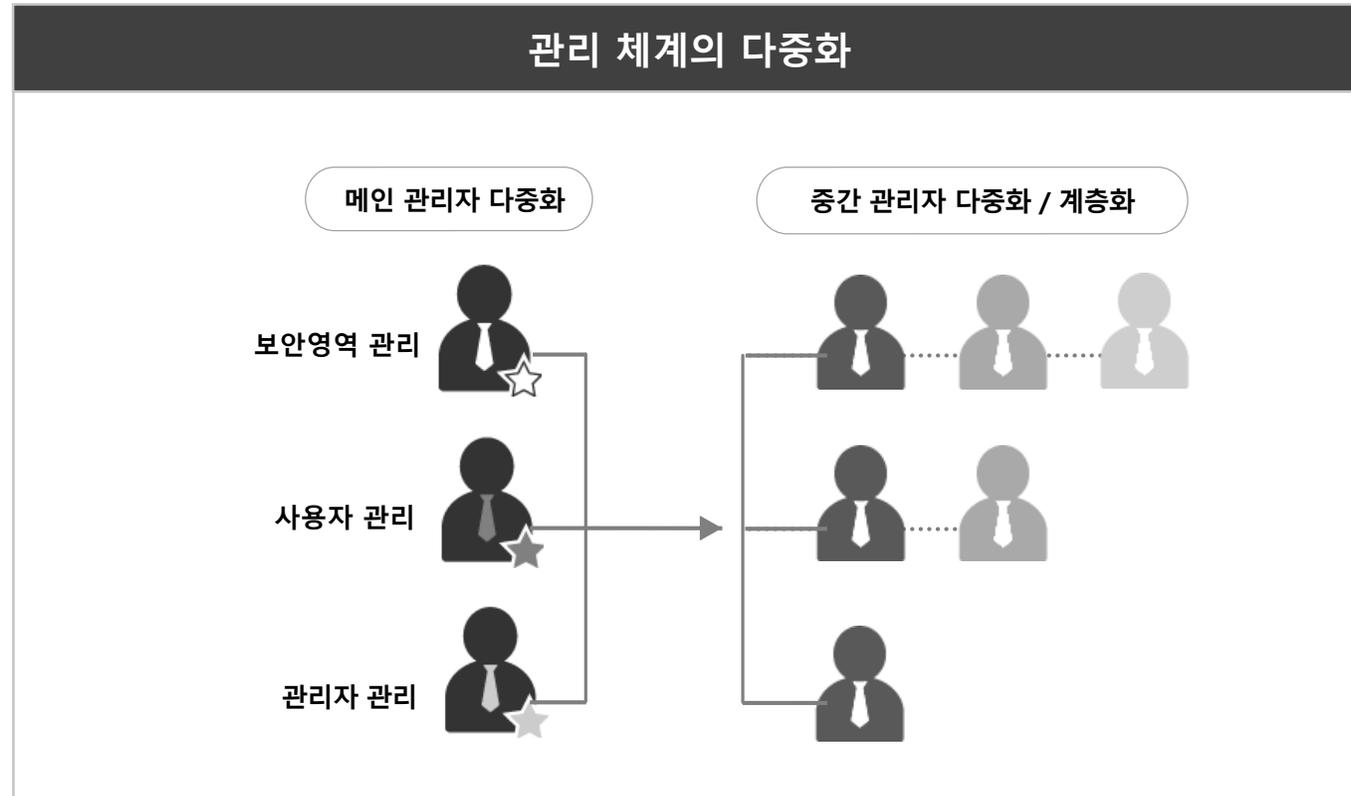


외부 인력이 사용하는 모든 PC에 시큐어디스크를 설치하여
외주 업무 (프로젝트) 수행 과정에서 발생하는 모든 문서와 프로젝트 산출물에 대한
유출을 차단하여 보안을 강화 할 수 있습니다.

보안

관리자 다중화

부문 별 관리자 분화를 통한 효율적이고 책임감 있는 관리 가능, 관리자 다중화로 최상위 관리자 보안 문제 해결



06 기대효과

01 도입 기대효과

도입 기대효과



내부 중요한 데이터 보호

- 사용자 PC 자료 저장 차단, 저장 매체 제어
- 온/오프라인 유출 경로 차단으로 내부자료 유출 방지
- 서버 저장 및 전송구간 암호화로 데이터 유출에 대응



문서 유실 방지

- 문서버전 관리로 시점 별 복구, 랜섬웨어 같은 비인가 프로그램으로 인한 문서 유실 방지



내부 중요한 데이터 보호

- 윈도우탐색기 인터페이스 제공으로 사용자 친화성 보장
- 목적에 맞는 디스크 생성으로 원활한 문서 협업 환경 제공

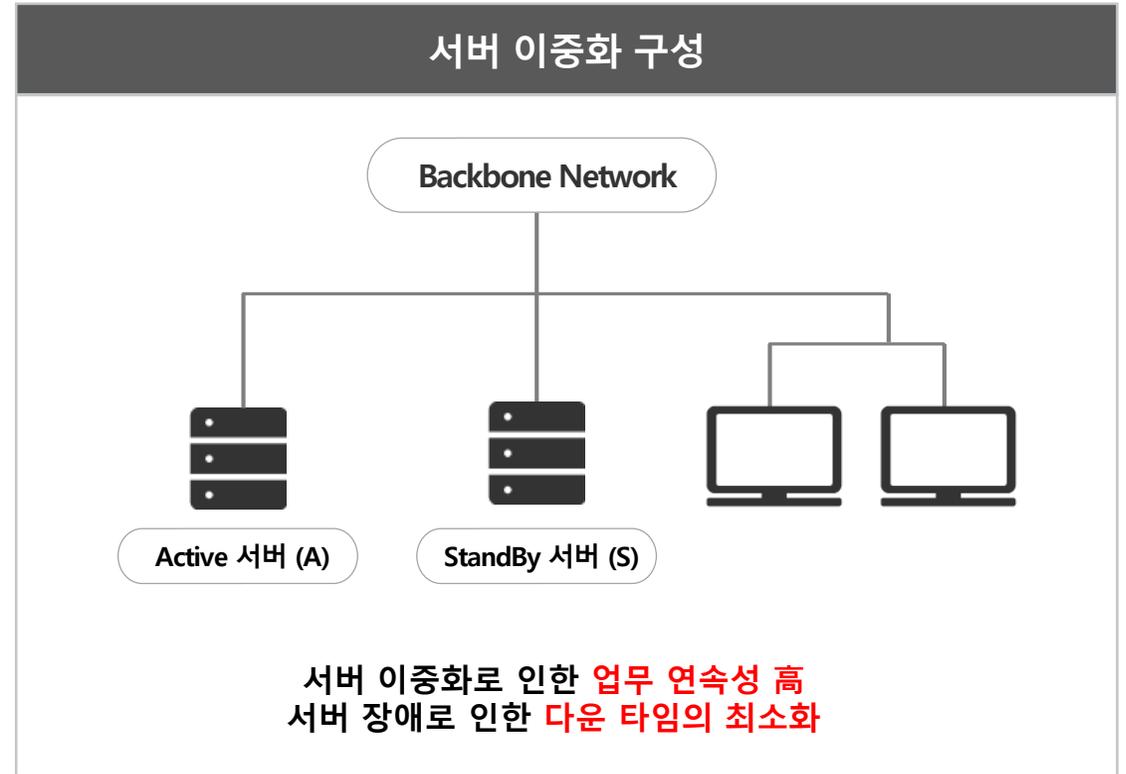
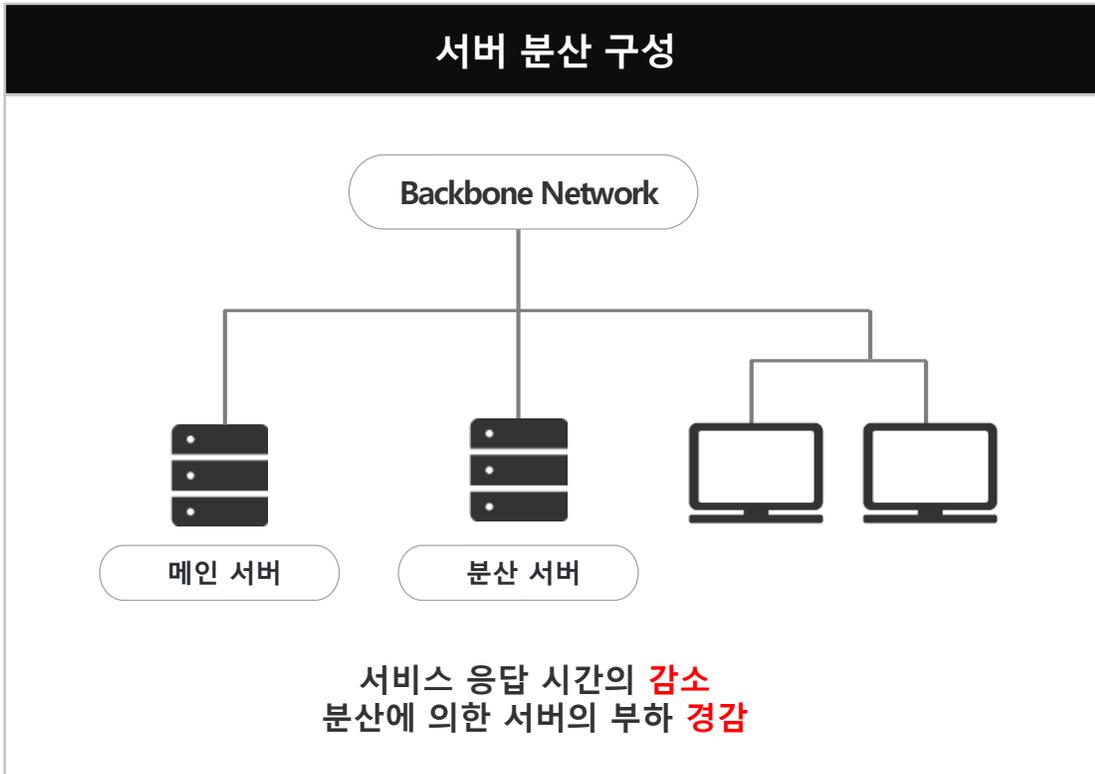
07 APPENDIX

- 01 시스템 구성
- 02 기술 지원
- 03 레퍼런스
- 04 구축 사례

구성

분산 & 이중화

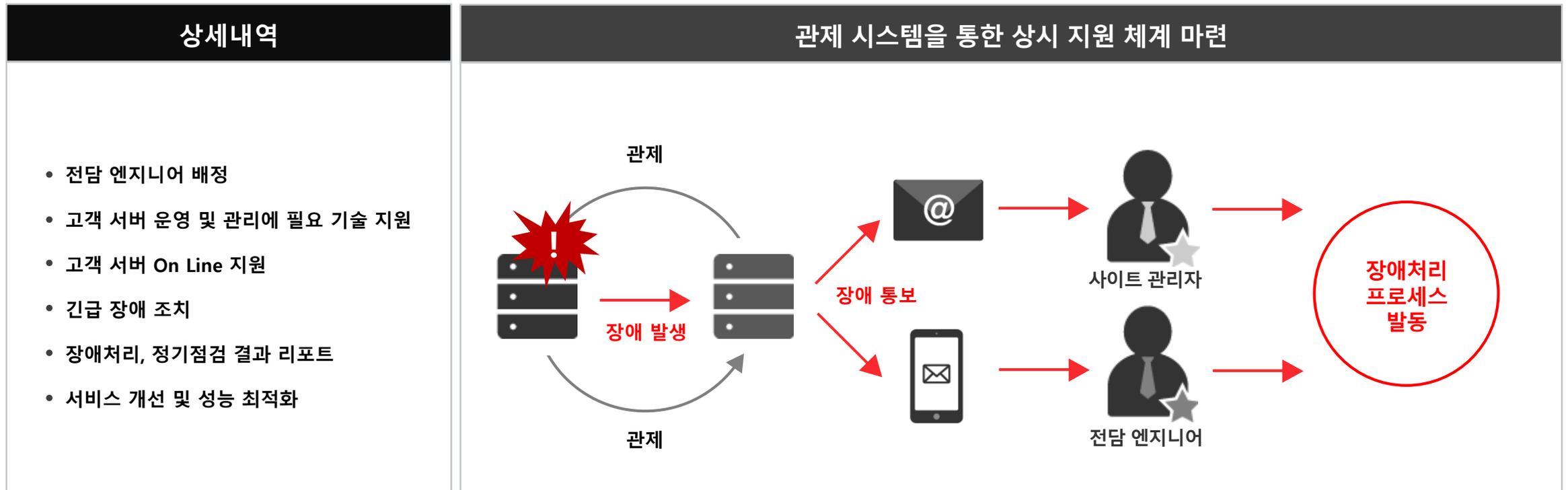
보안 대상 프로그램 / 확장자에 대해 제품 설치 시점부터 보안 정책 적용 가능



기술지원

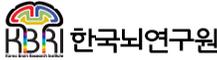
유지보수 & 관제센터 장애처리 시스템

전담 전문 파트너를 통해 철저한 장애 복구 대응 프로세스를 갖추고 완벽한 유지보수 지원을 약속합니다.



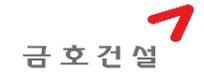
통합 레퍼런스

공공 기관

 행정자치부 정부통합전산센터	 방위사업청	 기획재정부	 기상청	 법무부
 국세청 National Tax Service	 문화체육관광부	 산업통상자원부	 특허청	 중소기업청
 KISA Korea Internet & Security Agency	 국군기무사령부 Defense Security Command	 대법원	 한국법제연구원 KOREA LEGISLATION RESEARCH INSTITUTE	 국토교통부 Ministry of Land, Infrastructure and Transport
 근로복지공단	 KoROAD 도로교통공단	 KR 한국철도시설공단	 생명보험협회 Korea Life Insurance Association	 KAERI 한국원자력연구원 Korea Atomic Energy Research Institute
 Kdn 한전KDN	 K water	 KBRi 한국뇌연구원	 한국행정연구원 Korea Institute of Public Administration	 kpc 한국생산성본부
 금융투자협회 Korea Financial Investment Association	 KICPA	 KINU 통일연구원 Korea Institute for National Unification	 한국가스공사 KOREA GAS CORPORATION	 TTA

통합 레퍼런스

기업

통합 레퍼런스



기업	<p>삼성생명, 삼성전자, 삼성엔지니어링, 현대자동차, 현대종합설계, 현대산업개발, 현대카드캐피탈, SC제일은행, KT, LG, SK, 아모레퍼시픽 CJ제일제당, 포스코, LS산전, 두산, 코카콜라음료(주), 한국후지필름, GS플라텍, 경남기업, LIG건설, STX조선, 금호건설, 금호타이어, 동부CNI 기아자동차, KBS, MBC, 보령제약, 대교, 도레이첨단소재, 루멘스, 삼일제약, 삼성올렛카드, 한솔도시락, KPX, 한세실업, 아이디병원 우림기계, KCC정보통신, 신세계조선호텔, 서울아산병원, 광주보훈병원, 한국제지, 세스코, SL Corporation, 우진INC, NVH코리아, 신영 신호제지, 한라산업주식개발, 세화기계, 삼미, 바텍, 동양ENP, 윤선생영어교실, 환인제약, 케피코, LOT배급, 조선대학교병원 등</p>
국공기관	<p>대전정부통합전산센터, 광주정부통합전산센터, 법무부, 방위사업청, 대법원, 한국인터넷진흥원, 한국철도시설공단, 도로교통공단 근로복지공단, 한국체육산업개발, 한국수자원공사, 문화체육관광부, 국세청, 산업통상자원부, 특허청, 중소기업청, 기획재정부 국군기무사령부, 한국법제연구원, 국토교통부, 근로복지공단, 도로교통공단, 한국철도시설공단, 생명보험협회, 한국원자력연구원 금융투자협회, 통일연구원, 한국가스공사, TTA, IT벤처기업연합회, 핵융합연구센터, 경기지방공사, 한국교총, 대한의사협회, 국립중앙박물관 한국석유공사, KERIS, 교육과학기술부, 농수산식품부, 한국과학재단, 증권예탁결제원, 국제금융센터, ETRI 등</p>
대학	<p>포항공과대학교, KAIST, 서울대학교, 연세대학교, 고려대학교, 한양대학교, 서울교육대학교, 경희대학교, 동국대학교, 중앙대학교 단국대학교, 부산대학교, 숙명여자대학교, 홍익대학교, 국민대학교, 성신여자대학교, 동덕여자대학교, 방송통신대학교, 한성대학교 전북대학교, 고등과학원, 가천대학교, 부산외국어대학교, 전남대학교, 인하대학교, 대구가톨릭대학교, 목포가톨릭대학교, 목포대학교 경상대학교, 영남대학교, 부산교육대학교, 순천대학교, 금오공과대학교, 원광대학교, 경남대학교, 진주산업대학교, 광운대학교, 경남대학교 홍익대학교 조치원캠퍼스, 대전신학대학교, 호서대학교, 군산대학교, 경동대학교, 전주대학교, 위덕대학교, 공주대학교 등</p>

구축 사례

<p>행정자치부 정부통합전산센터</p>	<p>내역목적</p>	<p>기관 내 기밀 자료에 대한 유출 방지 및 문서 중앙화 시스템 구축</p> <ul style="list-style-type: none"> · 내부 자료를 한 곳으로 통합하여 인력 별로 접근 통제 하고자 함 · 외부 협력업체의 업무 수행 과정에서 비 인가 매체로의 유출을 차단 하고자 함 · 자료의 유통 경로를 추적하고 작업 내역을 실시간으로 모니터링 하고자 함
	<p>내역역과</p>	<p>제한된 접근과 파일 유통으로 인해 권한 없는 사용자에게 의한 자료 유출 방지</p> <ul style="list-style-type: none"> · 로컬 PC 저장을 금지하고 모든 자료를 중앙 서버에만 저장 · 사용자 접근 권한 관리 및 매체 제어로 유출 차단 환경 구축 · 디스크 인계를 통한 퇴사자 자료 유실 방지
<p>KISA Korea Internet & Security Agency</p>	<p>내역목적</p>	<p>기관 내 중요 문서들의 내부 승인 과정을 거치지 않는 무분별한 반출로 파일 유통 경로 확인이 어려움</p> <ul style="list-style-type: none"> · 임직원 공유 및 협업 공간의 부재 · 기관 내 문서 자산가치 증가 · 산재된 문서의 통합관리 부재
	<p>내역역과</p>	<p>로컬 PC의 자료를 중앙 서버로 통합, 무분별한 반출이 가능한 유통 경로 차단</p> <ul style="list-style-type: none"> · 산재된 문서들의 통합관리 · 내부 기밀자료 보호 · 프로젝트 완료 후 산출물에 대한 중앙 관리 및 업무 연속성 마련

구축 사례

	<p>내역목적</p>	<p>프로젝트 산출물 보안 - 프로젝트 과정에서 생산되는 다양한 형식의 개발 자료들 효과적으로 보안하기 위한 방안을 마련하고자 함 외주 협력업체 임직원을 위한 공유 시스템 마련 - 협업 관계인 상주 인력을 위한 파일 공유 시스템 마련이 필요 - 프로젝트 종료 후 결과물을 중앙으로 통합 이관 시키기 위한 방안 마련이 필요함</p>
	<p>내역역과</p>	<p>내부자료 유출 차단 - 로컬 PC의 온/오프라인 매체를 통하여 중요한 내부 자료가 외부로 유출되는 것을 차단하고자 하는 목적에 적합함 문서중앙화 구축 - 모든 업무 관련 문서를 중앙 서버로 통합 저장하여 사용자의 접근 및 작업 권한을 통제하고 실시간 모니터링하여 체계적으로 관리함</p>
	<p>내역목적</p>	<p>기존에 사용중인 보안 제품의 호환성 문제로 지속적인 문제 발생, 프로젝트 산출물 보안 방안을 마련하고자함</p> <ul style="list-style-type: none"> · 업무의 중심 = 사용자 PC, 문서 보관소 = 사용자 PC · 원본의 복사, 유통이 자유롭고 통제가 불가능함 · 내부 공유와 외부 전달 매체가 다양함
	<p>내역역과</p>	<p>로컬 PC의 자료를 중앙 서버로 통합하고 실시간으로 모니터링 하여 체계적으로 관리하게 됨</p> <ul style="list-style-type: none"> · 로컬 PC저장을 금지하고 중앙 서버에만 저장 · UBS, 저장 매체 유출 차단 및 화면 캡처, 복사, 출력 차단 · 온라인 유출 경로 차단

