

## 전자문서 관리 및 유출통제를 위한 엔드포인트 통합 보안솔루션



# Contents

---



## I. 회사 소개



## II. 통합시스템 개요



## III. 주요 기능

당사는 1999년 창립하여 Endpoint 보안 기술을 토대로 온라인 PC보안 및 DLP 보안시장을 이끌고 있으며 최근에는 Endpoint 통합 보안 플랫폼시장으로 그 영역을 확대하고 있습니다.



### 일반현황 및 주요연혁

- 회 사 명 : 킹스정보통신(주)
- 대 표 자 : 오충건
- 사업종류 : 정보보호 솔루션 및 정보보호 서비스 개발
- 주 소 : 경기도 하남시 조정대로 150, 953,954호  
(아이테크 지식산업센터)
- 연 락 처 : Tel. 1544-1014 Fax. 031-790-0708
- 회사설립 : 1999년 06월
- 사업기간 : 1999년 6월 ~ 현재 (24년)

현재 50명

기술 인력(정보보호연구소)	33명
관리 인력	2명
영업인력 및 기술지원	15명



### 킹스정보통신(주) 주요연혁

- 2024.01 : KESS Guard-Zone V4.1 GS 인증
- 2023.06 : KESS Guard-Zone V4.1 보안기능확인서 취득
- 2022.02 : 신협중앙회 데이터유출방지시스템 구축
- 2021.06 : “K-Crypto V3.4” 국가정보원 암호모듈 재검증
- 2020.12 : 기업은행 내부정보유출방지시스템 구축
- 2020.02 : 암호화통신 프로토콜 제어모듈 특허 등록
- 2017.06 : 가상/모바일 키패드 보안 제품 출시
- 2015.05 : 엔드포인트 통합보안솔루션 KESS@Enterprise 출시
- 2013.03 : “Palm Box” 출시(국내외 특허 10건 출원)
- 2012.06 : Guard-Zone CC인증(EAL2) 획득
- 2011.03 : 본사 사옥이전
- 2010.04 : KT 국내 최대규모 내부정보유출방지(DLP) 솔루션 구축
- 2009.04 : 암호화 모듈 국정원 검증완료 - “K-Crypto”
- 2007.08 : 기술혁신형중소기업(이노비즈기업) 인증(A등급)
- 2006.07 : 중소기업 기술혁신개발사업 사업자 선정(중기청)
- 2001.04 : 기업부설 정보보호연구소 설립
- 2000.12 : 병무청 병역특례지정업체 선정
- 1999.06 : 킹스정보통신(주) 법인설립

당사는 EndPoint 보안시장에서 다양한 솔루션을 개발하여 공급하고 있으며, 관련된 각종 특허 및 인증을 보유하고 있습니다.



### 주요 사업분야 및 특허/인증현황

#### 주요 사업 내용

분 야	제품 개요	제 품 명
엔드포인트 통합유출방지	내부 정보 유출 방지	Guard-Zone
	개인정보보안	Pi-Filter
	컨텐츠 보안	PalmBox Local
		PalmBox Centralized
		Secon-Doc
온라인 보안	키보드 보안	K-Defense
	개인 방화벽	I-Defense

#### 수상 및 인증



벤처기업 확인서



INNO-BIZ 확인서



기업부설연구소  
협정서



보안기능확인서  
(Kess Guard-Zone)



국정원 암호화  
모듈 증서



CC인증서  
(Guard-Zone)

고객사	프로젝트 명	프로젝트내용	공급수량	수행기간
경희의료원	내부정보 유출방지시스템 구축	통합 유출방지 시스템	2,300명	2023.12
아시아나항공	내부정보 유출방지시스템 구축	통합 유출방지 시스템	6,200명	2023.09
금호석유화학	내부정보 유출방지시스템 구축	통합 유출방지 시스템 고도화	3,000명	2023.04
IBK기업은행(외부망)	내부정보 유출방지시스템 구축	외부망 DLP시스템 고도화	3,000명	2023.01
DB생명	내부정보 유출방지시스템 구축	통합 유출방지 시스템	1,300명	2022.10
세라젠	내부정보 유출방지시스템 구축	통합 유출방지 시스템	1,000명	2022.07
KDB생명	내부정보 유출방지시스템 구축	통합 유출방지 시스템	5,000명	2022.06
KT클라우드	내부정보 유출방지시스템 구축	On/Off-Line 정보유출방지 시스템	1,500명	2022.03
LG디스플레이	내부정보 유출방지시스템 구축	클라우드 로컬파일 삭제시스템	20,000명	2021.10
군인공제회	내부정보 유출방지시스템 구축	통합 유출방지 시스템	200명	2021.09
KT서비스(북부,남부)	내부정보 유출방지시스템 구축	통합 유출방지 시스템	200명	2021.08
카카오	내부정보 유출방지시스템 구축	외부 유통문서 2차유출통제 시스템	500명	2021.07
NH선물	내부정보 유출방지시스템 구축	매체제어 시스템 고도화	200명	2021.04
조선내화	내부정보 유출방지시스템 구축	통합 유출방지 시스템	600명	2021.02
신협중앙회	내부정보 유출방지시스템 구축	통합 유출방지 시스템 구축	25,000명	2020.12
감사원	내부정보 유출방지시스템 구축	저장매체통제 및 보안USB 구축	1,400명	2020.12
KT텔레캅	내부정보 유출방지시스템 구축	통합 유출방지 시스템 고도화	1,200명	2020.10
KCC건설	내부정보 유출방지시스템 구축	통합 유출방지 시스템 고도화	1,000명	2020.09
롯데손해보험	내부정보 유출방지시스템 구축	매체제어 시스템 고도화	2,500명	2020.09
SM신용정보	내부정보 유출방지시스템 구축	통합 유출방지 시스템 고도화	1,200명	2020.09
롯데물산	내부정보 유출방지시스템 구축	통합 유출방지 시스템 고도화	200명	2020.07
한국코퍼레이션	내부정보 유출방지시스템 구축	통합 유출방지 시스템 고도화	1,500명	2020.04







고객사	프로젝트 명	프로젝트내용	공급수량	수행기간
일진그룹	내부정보 유출방지시스템 구축	통합 유출방지 시스템 고도화	1,000명	2020.03
투썸플레이스	내부정보 유출방지시스템 구축	통합 유출방지 시스템 구축	500명	2020.03
한양대학교	내부정보 유출방지시스템 구축	Off-Line 매체제어시스템	200명	2020.01
고려신용정보	내부정보 유출방지시스템 구축	통합 유출방지 시스템 고도화	2,000명	2019.12
한국 맥도날드	내부정보 유출방지시스템 구축	통합 유출방지 시스템	1,000명	2019.12
롯데홈쇼핑	내부정보 유출방지시스템 구축	통합 유출방지 시스템 고도화	2,400명	2019.11
농심	내부정보 유출방지시스템 구축	통합 유출방지 시스템 고도화	3,000명	2019.08
창신INC	내부정보 유출방지시스템 구축	통합 유출방지 시스템	2,400명	2019.06
IBK기업은행(내부망)	내부정보 유출방지시스템 구축	통합 유출방지 시스템	20,000명	2019.06
경동나비엔	내부정보 유출방지시스템 구축	통합 유출방지 시스템 고도화	1,500명	2019.05
GC헬스케어	내부정보 유출방지시스템 구축	통합 유출방지 시스템 고도화	110명	2019.04
환인제약	내부정보 유출방지시스템 구축	통합 유출방지 시스템	460명	2019.02
행정공제회	내부정보 유출방지시스템 구축	Off-Line 매체제어시스템	350명	2019.01
대림대학교	내부정보 유출방지시스템 구축	통합 유출방지 시스템	500명	2019.01
재너시스BBQ	내부정보 유출방지시스템 구축	문서암호화 기능 추가	500명	2019.01
하나손해보험	내부정보 유출방지시스템 구축	통합 유출방지 시스템 고도화	1,000명	2019.01
흥국화재	내부정보 유출방지시스템 구축	통합 유출방지 시스템	3,000명	2018.11
세스코	내부정보 유출방지시스템 구축	통합 유출방지 시스템 고도화	1,500명	2018.10
미래에셋증권	내부정보 유출방지시스템 구축	통합 유출방지 시스템 고도화	10,000명	2018.10
미래에셋생명	내부정보 유출방지시스템 구축	통합 유출방지 시스템 고도화	3,000명	2018.07
아워홈	내부정보 유출방지시스템 구축	통합 유출방지 시스템 고도화	3,000명	2018.07
KT	On/Off-Line 중요정보유출방지 시스템 구축	통합정보유출방지 시스템 구축	75,000명	2011.06



KESS(Kings Endpoint Security System)는 업무용 단말기 내 전자문서 생성·저장·관리·유통 등 모든 보안적인 요소를 통합적으로 관리할 수 있는 차세대 보안솔루션으로 기업의 업무환경을 고려하여 다양한 시스템을 구축할 수 있습니다.

제 품 명	KESS Guard-Zone V4.1	출시년월	2015년03월	KESS
제 조 사	킹스정보통신(주)	인증현황	보안기능확인서	
제품개요	업무용 단말기를 통해 전자문서가 유출될 수 있는 경로를 통제 및 전자문서 암호화, 업무영역 가상화 통제, 문서중앙화 등 콘텐츠 중심의 보안정책을 병행함으로써 엔드포인트 보안을 제고할 수 있는 차세대 통합 보안기능을 제공함			

 통제기능 측면	<ul style="list-style-type: none"> <li>• 콘텐츠 기반 온·오프라인 통제를 통한 로그 무결성 구현</li> <li>• MTP, 스마트폰 테더링, 무선AP 통제, BAD USB, 등 최신의 저장매체 통제 기능 지원</li> <li>• 화면보호기, 계정 및 비밀번호 관리, 노트북 반출관리, 방화벽 설정 등 다양한 보안 기능 제공</li> <li>• 프린트 워터 마킹, 개인정보 및 기업정보보안 통제, 화면캡처방지, 모니터워터마크 등에 대한 추가 기능 구현 용이</li> </ul>
 시스템 확장 측면	<ul style="list-style-type: none"> <li>• 컴포넌트 기반의 선택적·단계적 보안 기능 구축 용이</li> <li>• 개인정보검색, 문서 암호화, PC내 영역 암호화, 문서중앙화 등 보안 업그레이드 용이</li> </ul>
 관리의 효율 측면	<ul style="list-style-type: none"> <li>• Dash Board, 통계 및 리포트 제공을 통한 다양한 보안 현황 조회 기능 제공</li> <li>• 자체 결재시스템 및 설치유도, 다국어 String 지원 환경 등 제공</li> </ul>
 안정성 및 비용 측면	<ul style="list-style-type: none"> <li>• Windows 10, 11 (32/64bit) 지원</li> <li>• 단위 솔루션 별 다양한 사이트에서 검증된 보안 기능을 통합하여 제공</li> <li>• 별도의 보안솔루션 구축 및 유지보수 비용 대비 절감효과 극대화</li> </ul>



### Off-Line 통제(DLP)

#### PC기반 유출경로 통제

- › 저장매체/네트워크/프린트
- › USB/외부저장장치 통제
- › 블루투스,하드교체 사용 통제

### On-Line 통제(DLP)

#### PC기반 네트워크 통제

- › 메일/메신저 첨부파일 통제
- › HTTPS 암호화 통신 감시 기능
- › 사이트 접속 차단

### 프린터 통제

#### 프린터 통제/사본 저장

- › 프린트 워터마크 생성  
(가시성 / 비가시성)
- › 프린터 본문 및 출력 로그 저장
- › 외부제출용 워터마크 예외 기능

### 개인정보 검색 통제

#### 개인정보/기업정보 보호

- › 외부 유출시 개인정보, 기업정보에  
관한 키워드 포함한 파일을  
검색하여 통제
- › 개인정보/키워드 검색 프린터 통제
- › 개인정보 마스킹처리 출력
- › 개인정보 격리 또는 암호화 처리

### 문서 암호화(DRM)

#### 외부 유출시 최종 보안

- › 모든 문서 파일 (오피스,한글,PDF)
- › 영역 암호화 (PC 보안 드라이브)
- › 문서 콘텐츠 사전 통제
- › 문서 반출 프로세스 제공

### 화면 캡처/복사 /촬영 통제

#### 화면 캡처/복사기능/촬영

- › 화면 캡처 방지
- › 클립보드 통제
- › 모니터 화면 워터마크 삽입  
촬영을 못하도록 유도 및 추후  
추적 감사 (가시성 / 비가시성)

### 외부유통문서 2차 통제

#### 승인 문서 외부 유통 통제

- › 패스워드 설정
- › 사용기한 및 횟수 제한
- › 다른이름저장 통제
- › 복사금지 및 출력통제

### 문서중앙화

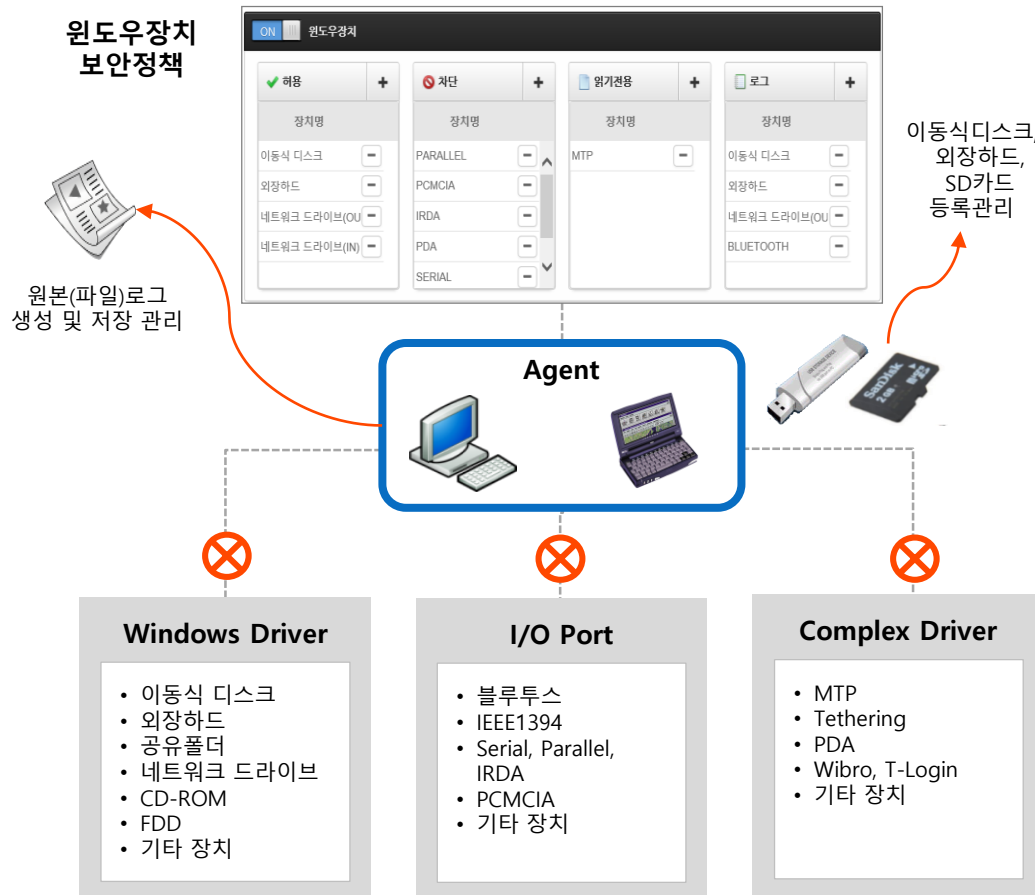
#### 네트워크 드라이브 협업

- › 조직도 기반 그룹 공유 드라이브
- › 사용자 지정 협업 공유 드라이브
- › 개인사용자를 위한 개인드라이브

기업의 환경을 고려한 다양한 엔드포인트 기반 전자문서에 대한 보안을 강화하고 추가적인 보안 요구사항에 대한 즉각적인 수용역량을 확보함은 물론 구축 기간과 비용 절감을 통해 투자 효과를 극대화 할 수 있을 것으로 기대합니다.



윈도우 기반 PC와 관련된 주변 저장장치를 통제할 수 있는 기능이며 윈도우 드라이버, PORT, 복합장치 드라이버 방식으로 제어를 합니다.



### 원본로그 생성 및 모니터링 관리

- 콘텐츠 기반 오프라인 이동 파일통제 기술
- 프로세스 기반 콘텐츠 접근 통제 기능
  - : Explorer.exe(이동식저장장치, CD-RW, 공유폴더, 네트워크 드라이브 등)
  - : Fsquirt.exe(블루투스), Itunes.exe(MTP) 기타
- 알려지지 않은 저장매체 및 프로세스 등록을 통한 확장적인 보안 통제 기술
- 장치사용 및 접근에 대한 로그(차단, 허용)
- 원본로그 생성관리

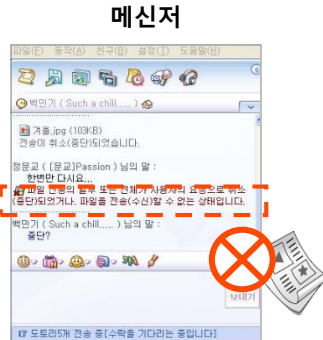
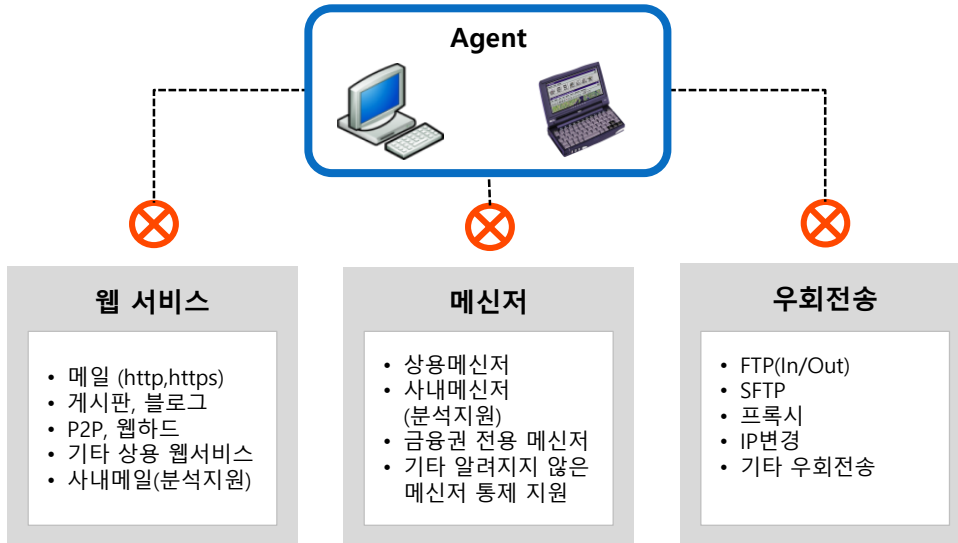
### 이동식 디스크 등록 관리

- 이동식디스크(USB Memory 및 USB 외장하드, SD카드, Bad USB ) 대상으로 사전 등록하여 사용하는 기능
- 관리자 승인/반려, 등록관리

### 일반 USB 데이터 영역 가상화 (옵션)

- 일반USB를 데이터 영역 가상화 할 수 있는 기능 제공
- 일반 영역, 가상화 영역 생성 분할

국내 최초 로컬 Proxy통제방식(특허보유)으로 다양한 네트워크 프로토콜 및 어플리케이션 경로에 대해 실시간으로 통제합니다.



인터넷 어플리케이션 파일 첨부통제 및 모니터링

#### 온라인서비스 통제 범위 및 기술

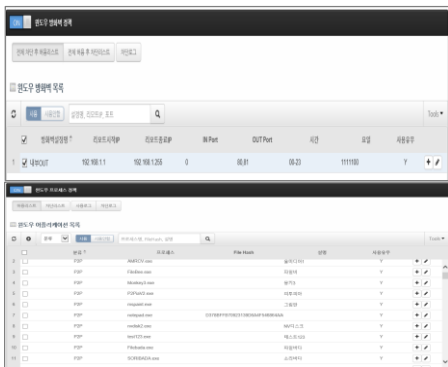
- 사내 업무용 메일, 메신저 분석 지원
- 온라인 서비스 예외 목록 관리
  - : 프로세스, HOST명, PORT, remote 시작IP 등 등록 처리

#### 원본로그 생성 및 모니터링 관리

- 콘텐츠 기반 온라인 이동 파일통제 기술
- **Edge, IE, Chrome, 웨일, Firefox**, 메신저, 클라우드 등 인터넷 Application 대상
- **HTTPS 암호화 통신 감시 기능(특허 등록)**
  - : Web Mail 의 파일 통제 및 로그(**메일 본문로그, 원본로그 포함**) 생성, 사이트 접속 차단
- **Office Outlook을 통한 SMTP+SSL / SMTP+TLS 감시 및 제어**
- 프로세스 기반 콘텐츠 접근 통제 기능 (어플리케이션 프로세스 등록을 통한 확장적 보안 통제)
- 알려지지 않은(분석되지 않은) 프로그램에 대한 원천 통제

윈도우 방화벽/프로세스 관리/화면보호기/계정잠금/무선AP 통제 관리기능을 제공합니다.

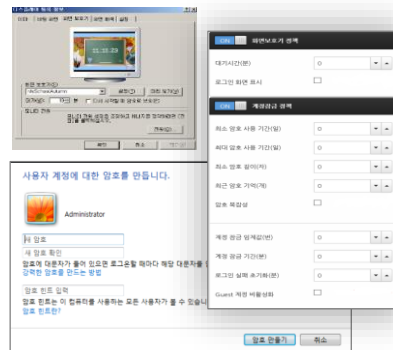
### 윈도우 방화벽/프로세스 관리



#### 윈도우 방화벽 / 웹사이트 차단 / 프로세스 실행 통제

- 리모트IP, Port를 지정시간, 요일, 사용유무 방화벽 중앙 설정 (Black&White방식)
- 웹사이트 접속 차단, 차단, 사용로그 생성
- 프로세스명, 파일해쉬정보를 Black&White 방식으로 실행 통제
- 사용/차단 로그 생성

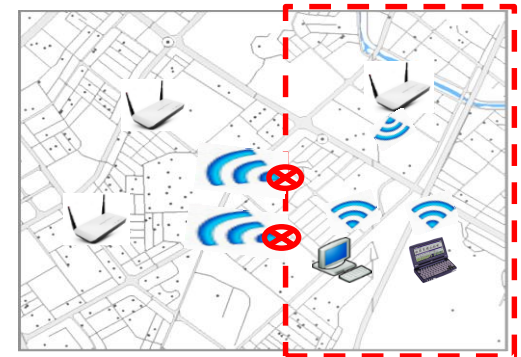
### 화면보호기/계정잠금 관리



#### 화면보호기 / 계정잠금 정책

- 화면보호기 대기시간 설정
- 로그인 화면 표시 여부 설정
- 계정잠금 시 암호사용에 대한 보안 정책 준수
- 계정잠금에 대한 보안 정책 준수

### 사내 무선 AP 통제



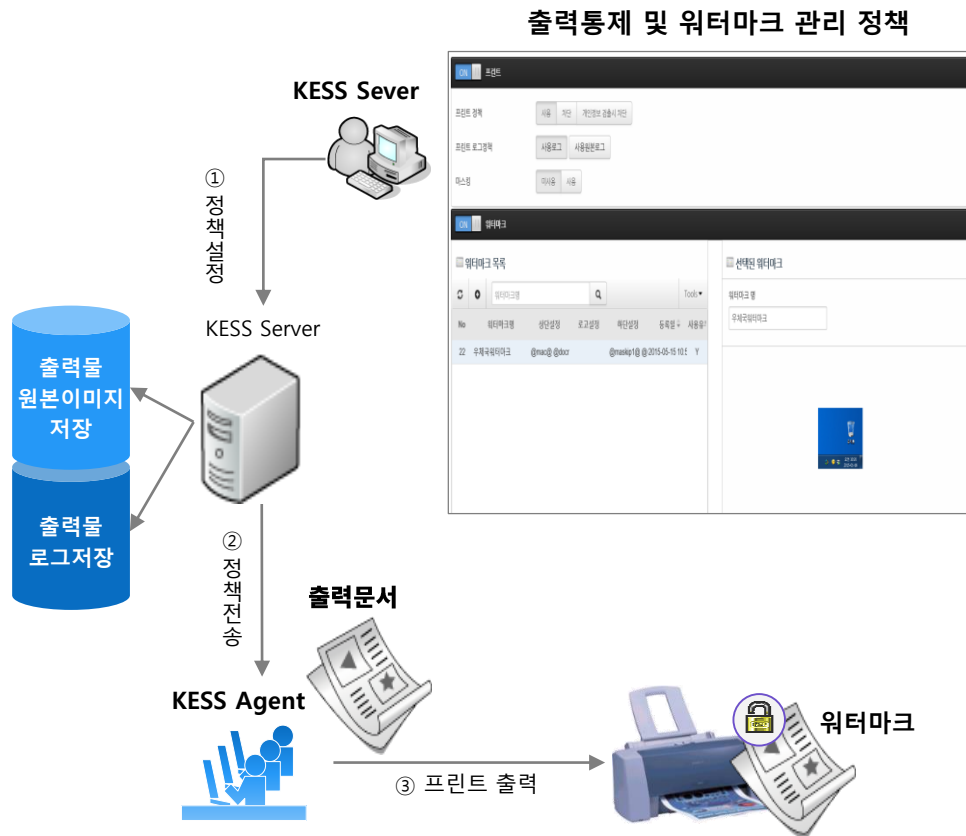
#### 사내 무선 AP 통제

- SSID, MAC, AP명 기반 통제
- 인증/허용/차단
- 로그 제공



## 4.1 Visible 프린터 통제 및 출력물 워터마크

프린터 장치에 대한 허용/차단 설정은 물론 원본로그 생성하며 출력물에 대해서는 워터마크 생성을 통해 보안을 설정을 할 수 있습니다.



## 프린트 통제 및 원본로그 생성 기술

- 개인별/부서별 프린트 통제 정책 관리
- 프린트 사용로그 및 원본로그 관리

## 워터마크 정책

- 용지여백, 폰트, 폰트농도, 워터마킹 위치 등 설정
- 위치별 설정 값(부서명, 사용자명, 사용자ID, 컴퓨터명, IP, MAC, 문서명, 프린트 날짜 등) 설정 지정
- 로고설정
- 미리보기
- PCL 6 표준 환경 권장
- 외부 제출용 워터마크 예외 기능 제공

## 4.2 Invisible(비인자) 출력물 워터마크 관리

프린터 출력으로 인한 문서 유출을 랩코드가 작용하여 문서 검증을 통해 작성자 시간을 알 수 있으며 문서 외부 유출에 대한 추적을 할 수 있습니다.

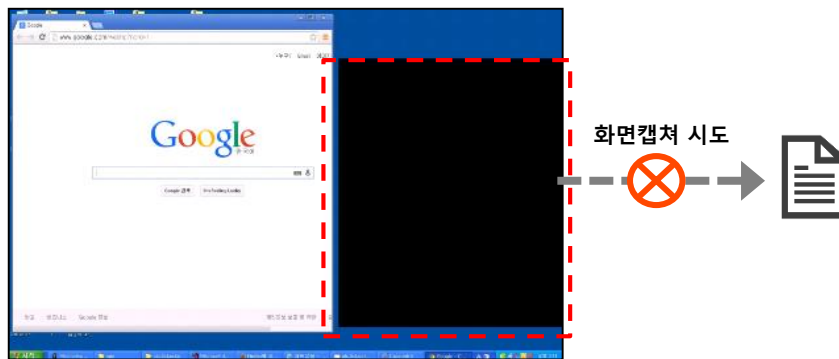


### 출력물 보안 솔루션

- 솔루션 실행 시 출력물에 보이지 않는 랩코드가 자동 적용
- APP으로 해당 문서 스캔 시 해당 출력물에 대한 정보 확인
- 낙서, 찢어짐 등 훼손된 문서 인식 가능 / 문서 일부분으로도 유출자 식별 가능

화면캡처를 방지하고자 하는 프로그램 및 웹 페이지를 대상으로 손쉽게 적용이 가능하며 다양한 형태의 캡처 프로그램에 대해 안전하게 보호하는 기능을 제공합니다.

웹 페이지 화면캡처 방지



#### 연동대상

- 프로세스, 도메인, 폴더

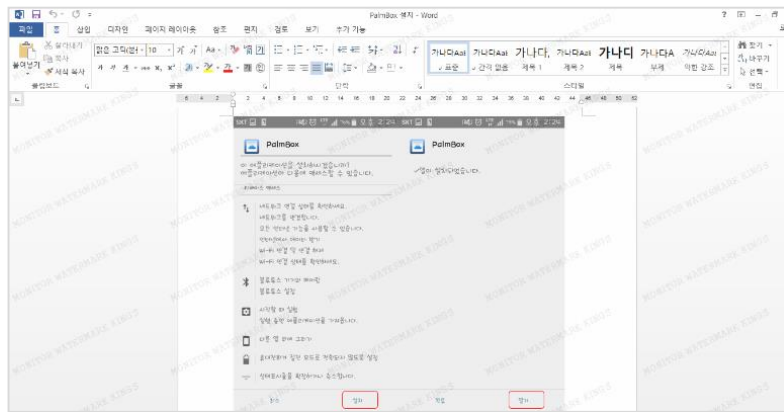
#### 지원범위

- 일반 캡처, 윈도우에서 제공하는 캡처, 인코딩, 원격 캡처 등 다양한 방식의 캡처 방식 차단
- 차단이 된 로그 생성관리
- Edge, IE, Chrome, Firefox 웹 브라우저 지원

스크린 캡처 형태		지원여부
Windows 제공 화면캡처 방식(PrintScreen Key, Alt+PrintScreen Key)		지원
Capture 전용 프로그램 방식	전체화면/지정화면	지원
	윈도우화면	지원
	선택캡처	지원
	동영상녹화	지원
Toolbar Capture		지원
다중모니터 사용 화면 Capture 방지		지원

## 6.1 Visible 모니터 워터마크

PC 모니터상에 중요 정보를 오픈하고 이를 악의적으로 카메라 촬영을 통해 유통하는 것을 방지해 주는 기능으로 특정 어플리케이션 및 웹브라우저 등에 적용이 가능합니다.

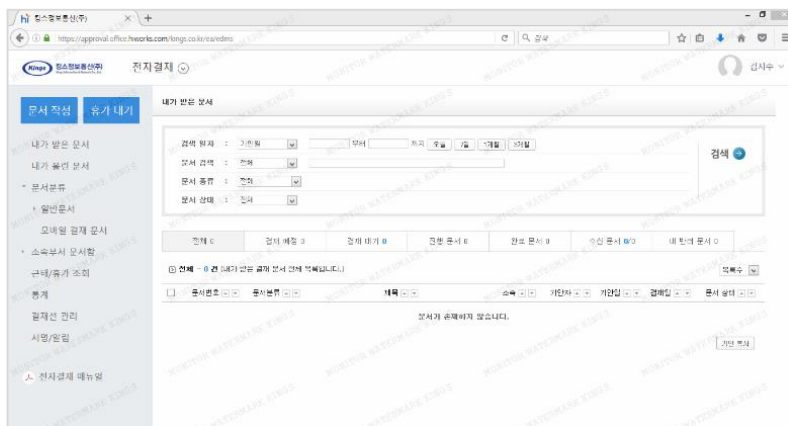


### 기대효과

- 모니터 화면으로 유출될 수 있는 기밀정보 중요자산 보호
- 악의적 모니터 카메라 촬영에 대한 심리적 경각심 고취

### 주요기능

- 텍스트(사용자정보 및 PC정보 삽입) 또는 이미지 설정을 통한 모니터 워터마킹
- 프로세스별 모니터 워터마킹 적용
- 사용자 ID 기반 정책 구성 및 예외처리 기능
- 자체 프로세스 보호 기능



## 6.2 Invisible(비인자) 모니터 워터마크 관리

PC 화면에 랩코드를 레이어드하여 화면 캡처 및 촬영 후 불법 유출을 방지합니다.



### 사용 플로우

- 실행 시 콘텐츠 내 회원정보를 담은 랩코드 레이어드 적용
- 캡처/촬영 등에 대한 유출 발생 시, 파일 검증 통해 유출자 확인

### 주요기능

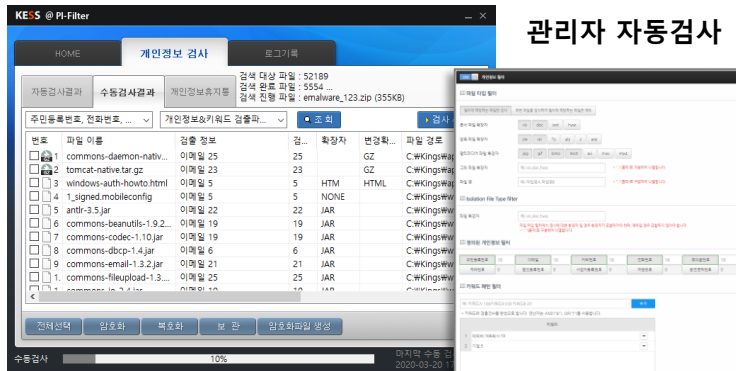
- 모니터 화면 전체에 **보이지 않는** 유저 데이터가 담긴 레코드 오버레이
- 워터마크를 피해 촬영 시 부분 유출 가능성 배제  
(일부 화면 유출 시에도 유출자 파악 가능)
- 화면 캡처/ 촬영 등으로 인한 유출 시 해당 화면의 작업자, 작업시간 등의 정보 확인



## 7.1 개인정보 필터

‘개인정보보호법’에 근거 PC내 개인정보 및 기업정보(키워드)를 추출하고 통제(암호화,격리,삭제)할 수 있는 기능이며 관리자 설정에 의한 자동검사 및 사용자가 직접 설정하여 검색할 수 있는 수동검사 기능을 동시에 제공합니다.

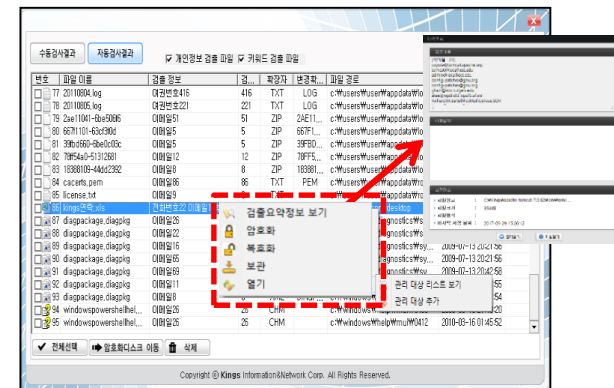
사용자 수동검사



## 개인정보 필터

- 검출파일 요약보기
- 개인정보 검출 암호화
  - 자동/수동 검사를 통해 검사된 파일에 대한 암호화 기능 제공
- 가상 보안영역 이동 격리
  - 암호화 드라이브 영역으로 검출된 파일 격리 이동
- 파일 완전 삭제
- 개인정보 파일 관리 대장 제공

검출파일 보안 기능

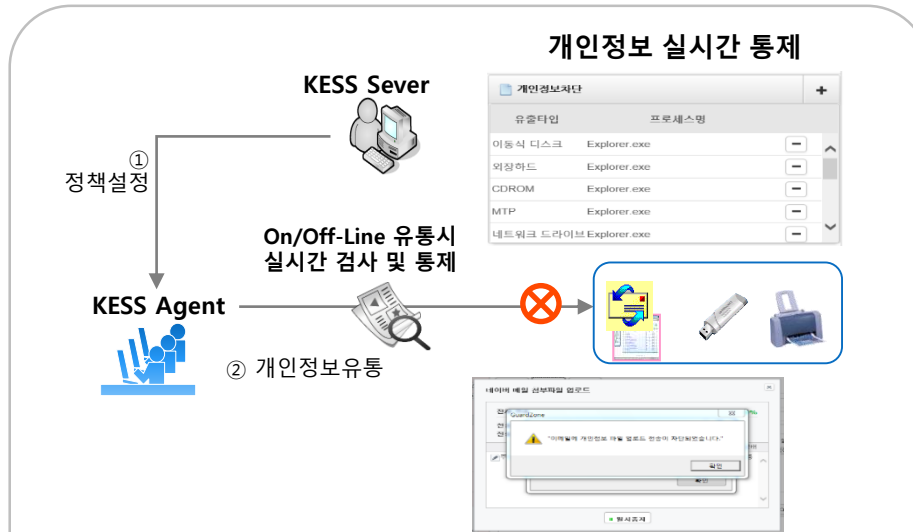


## 개인정보 검출 통제

- 스케줄링에 따른 관리자 지정 자동검사 및 사용자 임의 수동검사 기능
- 다중 스레드 방식에 의한 속도 가속화
- 개인정보 검색 패턴 및 체크섬
- 주요패턴 인접어/필수 키워드 검색 기능
- 키워드 설정 제공

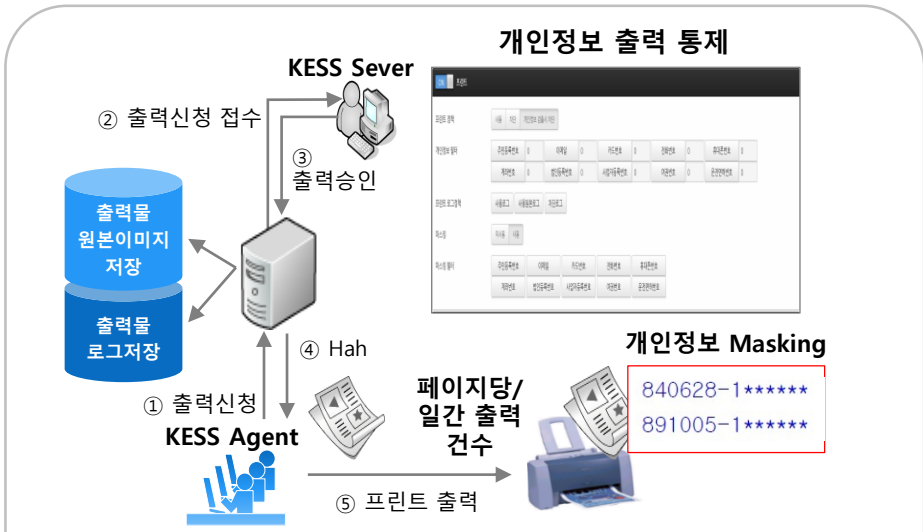
## 7.2 개인정보 실시간 통제 및 개인정보 프린트 통제

외부로 유통되는 파일에 대해 개인정보 및 기업정보(키워드) 포함여부 실시간으로 검사 및 통제 기능을 제공합니다.



## 온/오프라인 실시간 검사 및 통제

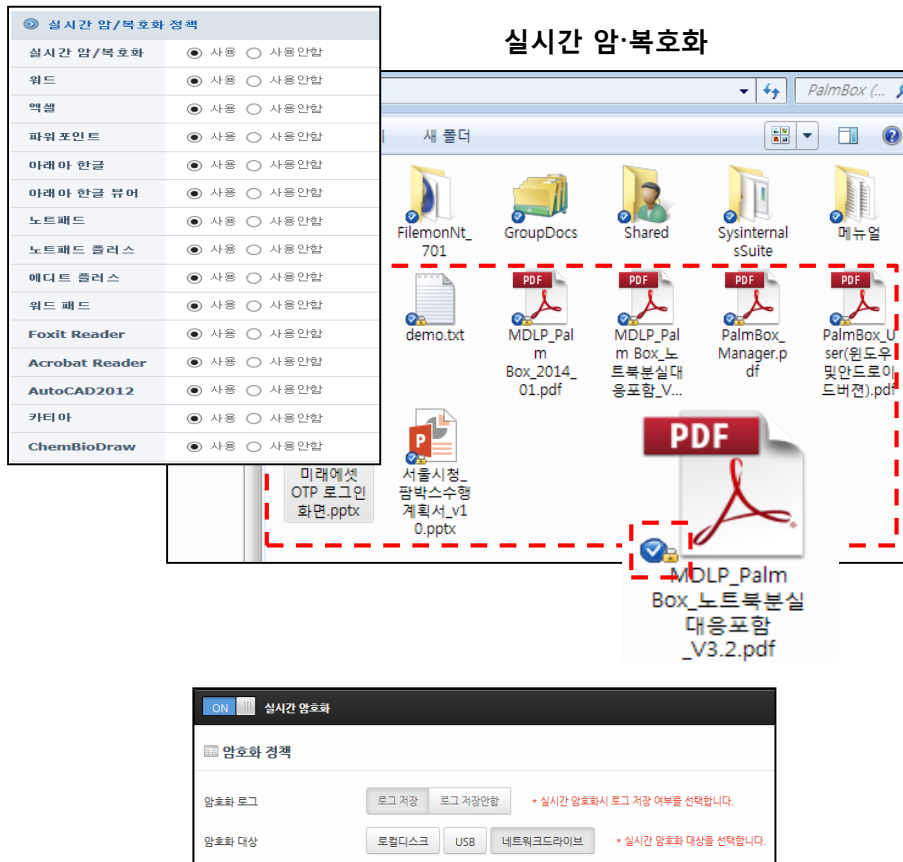
- 온/오프라인으로 유통되는 파일에 대한 실시간 개인정보 및 키워드 검사
  - OS 공통 기반 API 활용 및 제조사 API 지원
- 실시간 검출 과정 중 파일 검사 실패 시 자동 차단
- 확장자 별 선택 검사
- 메일 본문 내 개인정보 및 키워드 차단



## 개인정보 출력 통제

- 개인정보 출력 통제
  - 사용자 개인정보 출력 시도 시 실시간 검사를 통해 통제
  - 통제된 개인정보 패턴 조건과 보유현황에 따라 출력 신청 진행
  - 출력된 개인정보 패턴 로그 수집으로 저장 관리
- 개인정보 포함 출력물에 대한 Masking
  - 출력물 내용 중 개인정보 마스킹 출력

파일 암호화 모듈은 기존 문서보안 업체와 달리 어플리케이션에 종속되지 않는 방식으로 영향도를 최소화 하였으며 또한 신규 포맷에 대해 신속하게 대응할 수 있는 것이 특징이며 도면파일과 같은 특수 어플리케이션에도 적용이 용이 합니다.



### 파일 자동 암호/복호화 기술

- 문서 파일 단위로 자동 암호/복호화 기능을 제공함
- 보안 Agent가 설치되어 있어야만 자동 복호화 가능
- **국정원 인증 암호모듈 탑재(K-Crypto, 자사 기술)**

### 실시간 암호화 대상 및 로그

- 실시간 암호화 대상 선택 : 로컬디스크, USB, 네트워크 드라이브
- 실시간 암호화 시 로그저장 여부 선택

### 암호화 식별

- 아이콘 오버레이를 이용 암호화가 되어 있는 경우  
자물쇠 모양의 오버레이 표출

### 프로그램 단위 별 암호/복호화 지정 가능

- MS오피스(워드, 엑셀, 파워포인트), 한컴오피스(한글, 한쇼, 한셀), PDF, 포토샵, 일러스트, 노트패드, 노트패드 플러스, 에디트 플러스, 오토캐드, 이미지뷰어 등
- 새로운 버전에 대한 신속한 대응

PC내 일반영역을 분할하여 가상드라이브 영역을 생성하고 이를 섹터단위로 암호화하여 외부로부터의 악의적 접근을 통제함은 물론 전자문서 외부 유통을 원천적으로 통제할 수 있습니다.



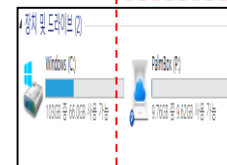
### PC기반 보안영역 생성 및 암호화 기술

- 영역 암호화 : 암호화 정도 조절 가능
- 악의적인 해킹 및 접근 불가
- 사용자 악의적 유출행위 통제
- 노트북 분실 등에 따른 내부정보 보호
- 국정원 인증 암호모듈 탑재(K-Crypto, 자사기술)

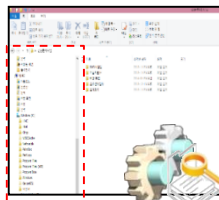
#### ① 사용자 인증(장치인증)



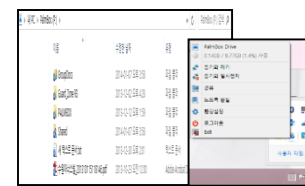
#### ② 가상암호화 영역 (P:) 생성



#### ③ 파일검색 엔진 자동실행



#### ④ (P:) 드라이브로 이동



### 보안영역 생성 프로세스

- KESS Agent 초기 설치 및 인증
  - 어플리케이션 연동 설치
  - 사용자 정보 및 단말기 장치 정보로 인증
- 보안영역 암호화 드라이브 생성
- 파일 검색 엔진 구동 (대상파일에 대한 격리 작업 : 파일확장자, 개인정보, 키워드)
- 보안 드라이브로 파일 자동 저장

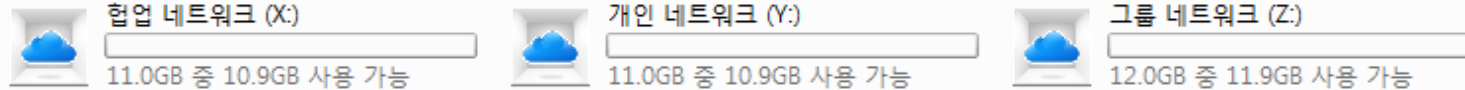
로컬드라이브에 데이터 저장금지와 네트워크 드라이브 문서공유 기능을 통해 업무 협업 기능을 효율적으로 제공합니다.  
조직도 구성에 따른 **그룹공유 드라이브**와 사용자 지정에 따른 **공유 드라이브** 기능을 제공합니다.



#### 로컬드라이브 저장 금지

- › 역할 : 저장되는 파일의 PC의 로컬드라이브 저장 금지
- › 기능 : 로컬 저장 금지 목록 및 예외 대상 지정 기능

#### 네트워크 위치 (3)



#### 협업 네트워크

- › 역할 : 프로젝트 및 협업 드라이브
- › 기능 : 타 부서원과 공동 작업 가능

#### 개인 네트워크

- › 역할 : 사용자 개인의 접근권한만 부여한 드라이브
- › 기능 : 개인사용자만 접근이 가능한 프라이버시한 공간

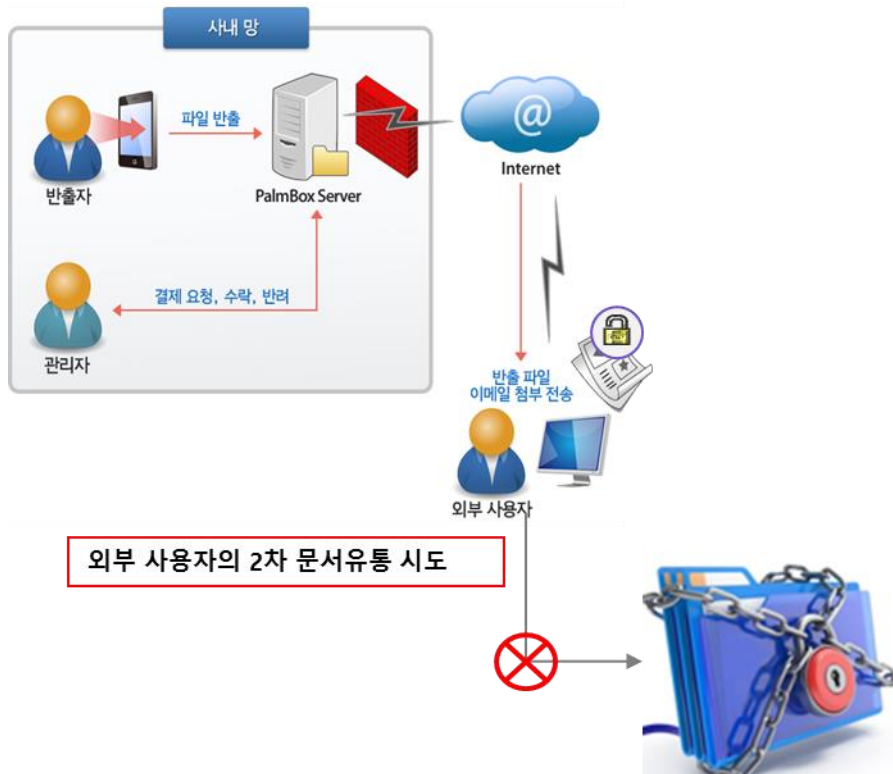
#### 그룹 네트워크

- › 역할 : 그룹폴더 내 개인폴더, 공동폴더 존재하는 그룹드라이브  
: 그룹개인폴더는 개인과 그룹장에게만 권한부여
- › 기능 : 그룹원과 문서공유, 그룹내 개인폴더 사용 가능



문서를 외부로 유통 시 보안정책을 설정하여 악의적인 2차 유통을 통제할 수 있는 기능을 제공합니다.

문서 2차 유출통제 기능



#### 외부로 유통된 문서의 2차 유출통제

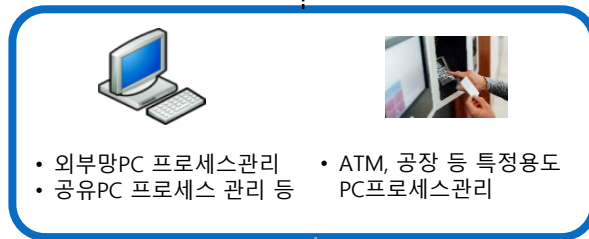
- 사용자에게 의해 기간, 횟수, 비밀번호를 생성
- 암호화된 EXE 형태로 수신인에 전송
- 전송된 파일은 정책에 의해 제한적으로 사용
  - : 열람기간 및 횟수 제한, 화면캡처/클립보드 방지
  - : 다른이름 저장금지, 폴더보호
  - : 프린트 출력통제 등
- 설치 방식이 아닌 포터블 방식으로 문서열람 시에만 보안기능 구동

White List 기반의 프로세스 제어 기능은 정책 및 인증으로 등록된 프로세스 외의 프로세스를 차단제어 하는 기능입니다.

WhiteList 프로세스 보안정책



Agent



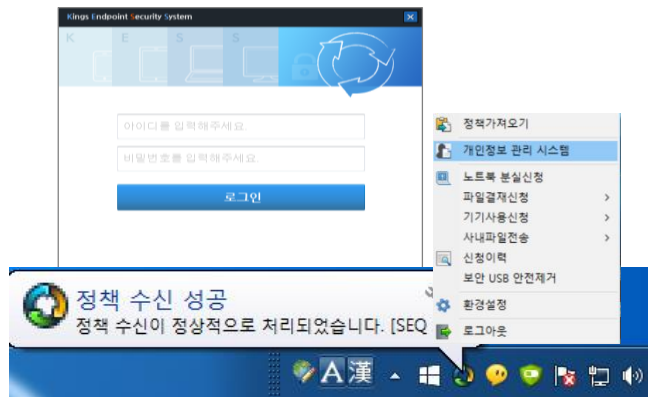
Process App

### 화이트 프로세스 통제 기능

- 정책 및 인증으로 등록된 프로세스 외의 모든 프로세스 차단
- 화이트 프로세스 정책 연동
- 화이트 프로세스 차단메시지 연동
- 화이트 프로세스 정책기반 프로세스 통제
- 화이트 프로세스 프로세스 실행 로그/차단 로그

사용자 및 기기를 확인할 수 있는 로그인 기능을 제공하며 프로세스 보호 및 안전모드 환경을 지원합니다.

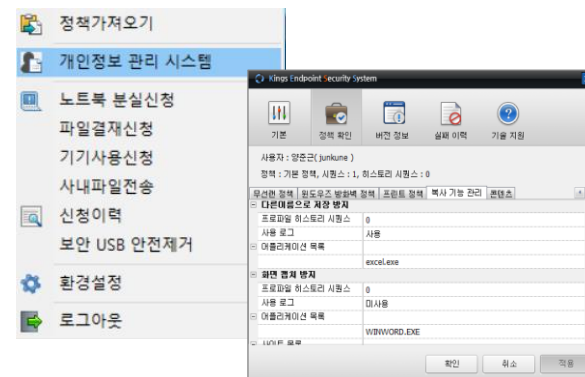
### 사용자 인증 및 AGENT 보호



### 사용자 인증 및 메뉴

- 사용자 인증(인사DB 기반 사용자 인증, 최초 인증 시 사용기기 인증, SSO, AD, LDAP 등 연동)
- Agent보호 기능(프로세스 및 레지스트리 보호, 안전모드 지원, 파일, 폴더 보호)
- Tray ICON 지원
  - 사용자 메뉴 확인 및 환경설정 기능 등 각종 편의성 제공

### 사용자 관리메뉴



### 사용자 관리 메뉴

- 환경설정 기능
  - 기본설정, 사용자 정책확인, 버전정보, 결재 실패이력, 기술지원
- 결재 시스템 기능
  - 노트북 반출, 기간예외정책, 출력물 등의 결재 요청
- 보안 드라이브 확인
  - 보안영역 드라이브내 파일 확인 등 지원
- 개인정보 수동 관리, 노트북 분실신청 등

### 12.1 정책생성 및 관리

엔드포인트 통합 보안시스템인 KESS는 다양한 보안기능을 통합적으로 제공하는 만큼 부서별/개인별 상황에 맞게 유연하게 보안정책을 수립할 수 있도록 구성되어 있습니다.

#### 정책생성 및 관리

#### 보안정책 생성 (Profile A+B+C)



#### 정책생성

- 각 보안기능별 Profile을 다양하게 구성
- 각 Profile을 조합하여 유연하게 정책을 생성함

#### 정책적용

- 기본/부서별/개인별/장치별 정책
- 사내/사외정책
- 오프라인 정책

#### 단위 Profile

- 윈도우장치, 윈도우프로세스, 온라인서비스, 윈도우방화벽, 무선AP, 콘텐츠, 프린트, 개인정보, 화면워터마크, 보안영역, 실시간파일암복호화, 2차유통관리 등

## 12.2 보안결재 시스템 관리

KESS는 자체적으로 보안 관련 결재시스템을 구성하고 있으며 필요에 따라서는 고객사 결재시스템과의 연동을 지원합니다.

### 결재라인 관리 기능

The screenshot displays the '결재라인 관리' (Approval Line Management) interface. It features a sidebar with a tree view of organizational units, a main table for managing approval lines, and a search panel at the bottom.

**결재라인 관리 기능**

결재분류: 사내사용신청

부서 조직도: 김준현

부서명: 인사부서

부서명: 인사부서

직원: 김준현(kjh)

직위: 사원

결재선: 1. 조은희(kingema) 사원 관리부 결재 2. 오종건(egoh) 사원 인사정보통신 결재

결재 관련 내용

사내임시사용정책

노트북 반출정책

문서공유 정책

개인정보 정책

출력물 통제 정책

분실기기 정책 : 노트북

이동식저장장치 인증 : USB저장장치, SD카드



# THANKS!

## Q&A

▶ [k-sales@kings.co.kr](mailto:k-sales@kings.co.kr)