



LIZARD
| C | L | O | U | D |
dCruncherRC

리자드디크런처RC

인터넷망PC 문서보안 및
랜섬웨어 탐지/차단 솔루션

Contents

- **01. 제품 개요**
- 02. 제품 소개
- 03. 중앙관리
- 04. 개발사 소개

제안배경

국정원 망분리 구축 가이드에 따르면 인터넷망 PC에서는 문서를 편집하거나 저장할 수 없다. 그러나 상당수가 망분리 후에도 업무상 편의를 위해 인터넷망 PC에서 문서를 작성하고 저장하고 있다. 이는 심각한 보안 위반 사항이지만 현실적으로 모든 문서를 업무용 PC로 망간 전송하여 처리할 경우 업무의 효율성과 신속성이 떨어진다. 이러한 이유로 금융위원회의 금융전산 망분리 가이드라인에서는 관리자의 승인 하에 인터넷망 PC에서 문서 편집을 제한적으로 허용하고 있다.

순간 복구 솔루션

방식 : 부팅시 저장 문서 삭제

문제점 : PC 재부팅 전까지 외부 해킹시
보안 취약



리자드 클라우드 디크런처

방식 : 문서 편집 및 저장시 영역암호화 기반의
보안드라이브로 저장

장점 : 업무 효율성과 보안성 확보



Contents

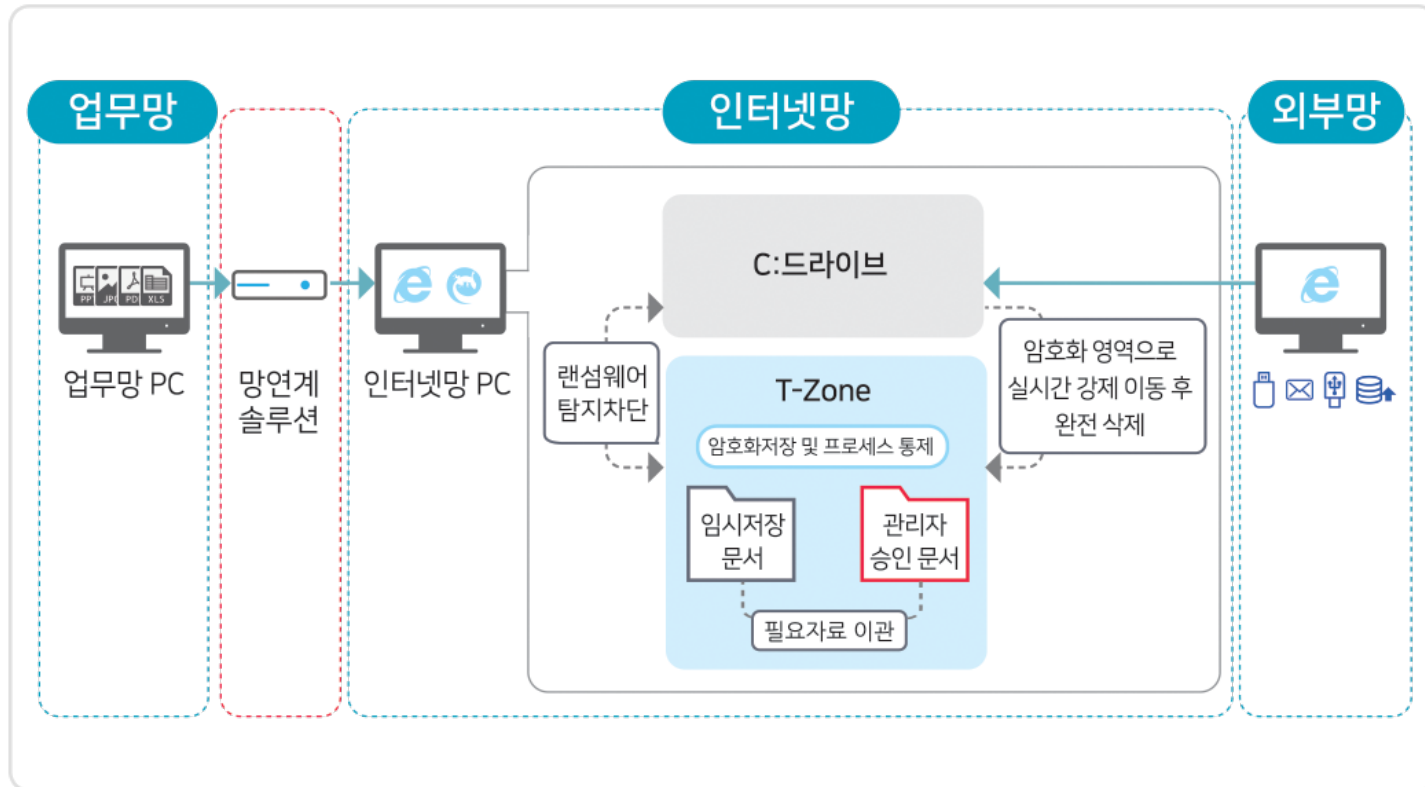
- 01. 제품 개요
- **02. 제품 소개**
- 03. 중앙관리
- 04. 개발사 소개



망분리 인터넷망 PC 문서의 실시간 암호화 저장 유출 방지 자동폐기 보안 솔루션

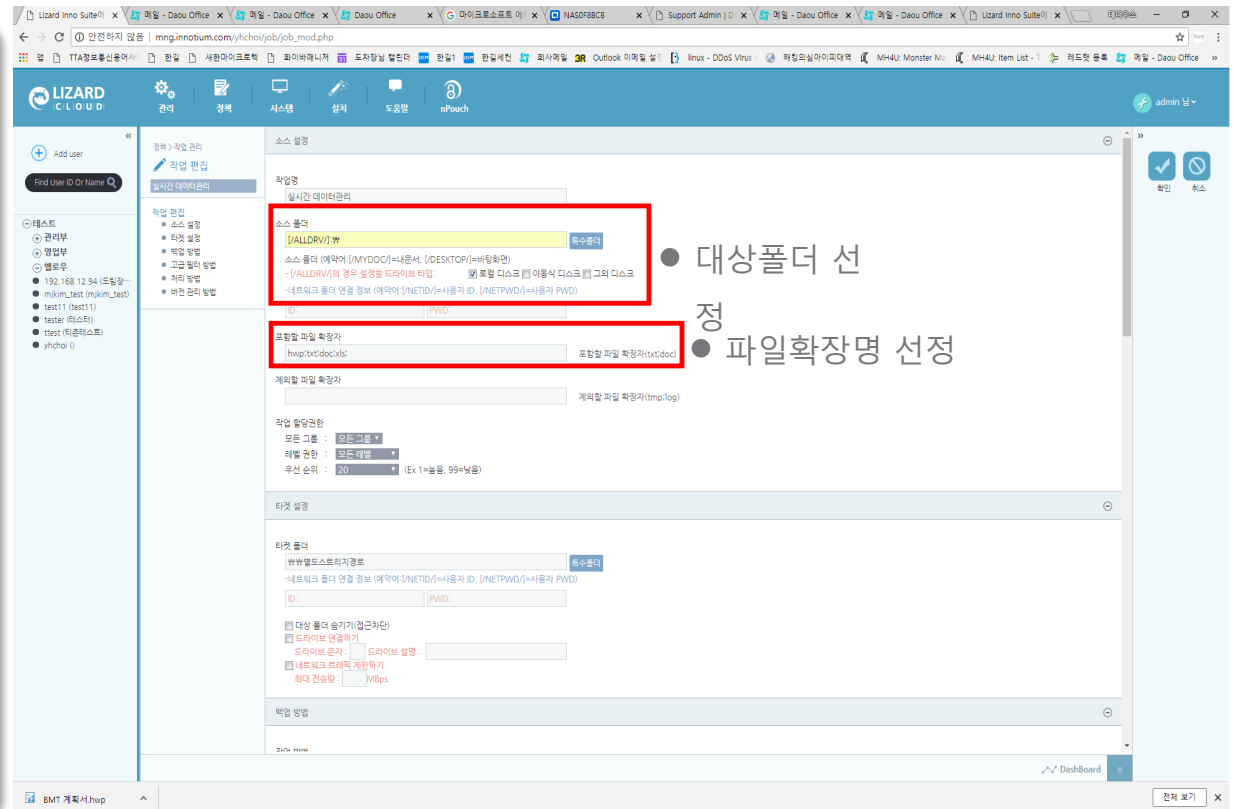
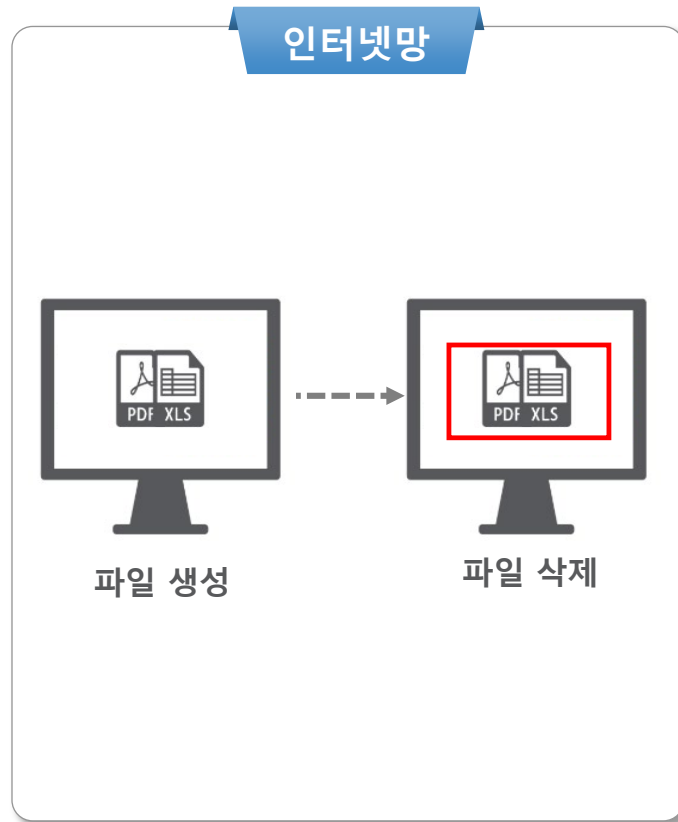
리자드 클라우드 디크런처 Lizard Cloud v10 dCruncher

리자드 클라우드 디크런처는 인터넷망 PC문서의 실시간 암호화로 기존 평문 저장 방식의 보안 취약점을 고도화 하고 T-Zone 암호화 보안 영역 탑재로 해킹과 유출을 방지하며 중앙관제에 의한 문서 자동 생성 · 폐기 관리 솔루션입니다.



실시간 데이터 보안 관리

인터넷PC HDD내 신규 데이터 생성 시 실시간 / 스케줄 설정대로 삭제 관리 및 암호화 저장이 가능



개인정보 / 특정 문서 검색 기능

개인정보 / 특정 문서가 생성되거나 수정 작업된 파일의 내용 검색 기능이 가능

인터넷망



검색

검출할 문자 설정

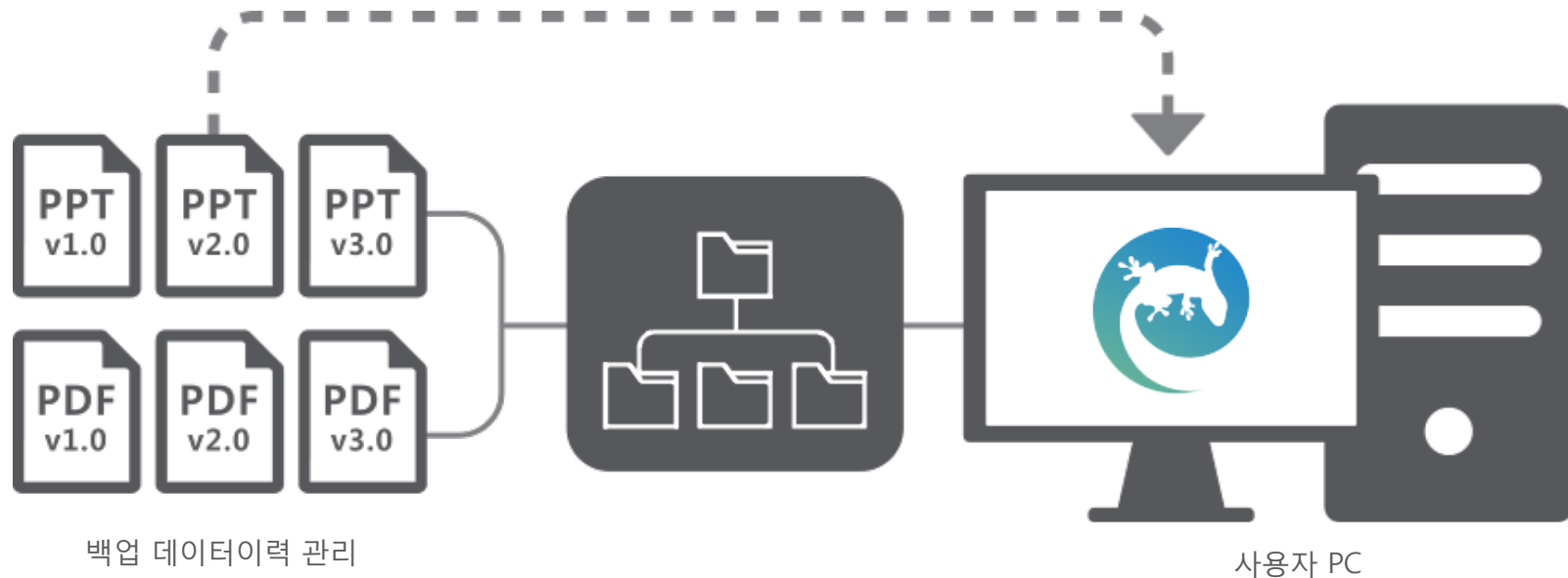
☐ 주민등록번호 ☐ 이메일 ☐ 운전면허번호 ☐ 여권번호 ☐ 전화번호 ☐ 사업자등록번호 개 이상

☐ 검출되면 포함하기

☒ 검출되면 제외하기

암호화 파일 이력관리

파일이 저장되는 시점에 이력생성, 원하는 시점으로 복구가능



- 같은 문서를 여러번 수정/저장시 설정에 따라 백업된 파일의 리비전(revision) 관리
- 버전관리는 예기치 않은 사용자의 실수나 과거 버전의 내용 복구를 위한 문서복원 기능
- 하나의 파일을 여러 번 백업하여도 인덱스(색인) 정보를 활용하여 필요한 시점으로 복원 가능

리자드 클라우드 디크런처 특징점

망분리 인터넷망 PC 문서의 실시간 암호화 저장 유출 방지 자동폐기 보안 솔루션



리자드 클라우드 디크런처 Lizard Cloud v10 dCruncher



실시간 데이터 보안관리

인터넷PC HDD내 신규 데이터 생성시
즉시 암호화 저장 및 상세 관리



문서 생성 및 삭제 로그관리

인터넷망 PC내의 문서생성 및
삭제에 대한 로그 관리



개인정보 / 특정 문서 검색기능

개인정보 / 특정 문서가 생성되거나 수정
작업된 파일의 내용 검색 기능



문서 등급별 자동 삭제 관리

임시저장 문서와 관리자 승인문서
구분 및 자동 삭제 관리



암호화 파일 이력관리

파일이 저장되는 시점에 이력 생성,
원하는 시점의 버전으로 복구



영역암호화 기반 T-Zone

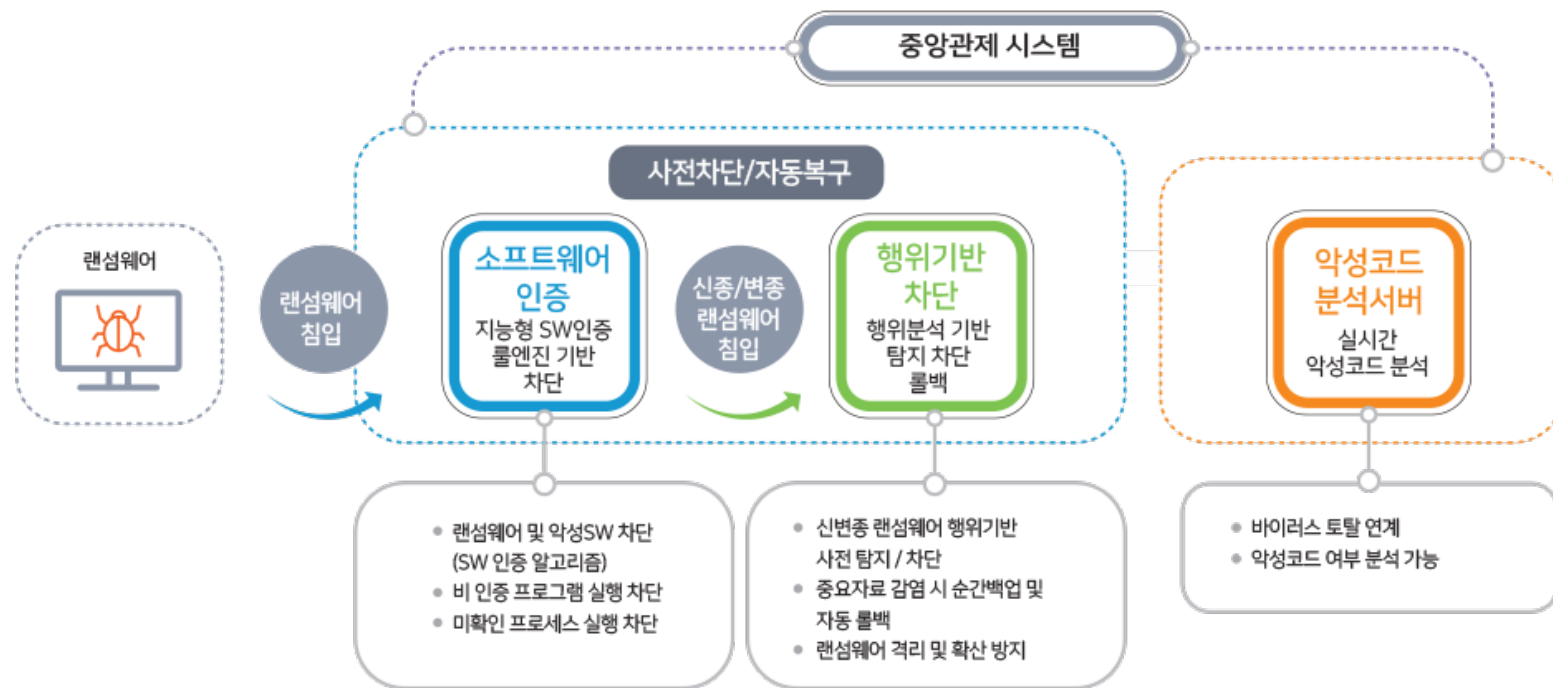
영역 암호화 기반의 히든(Hidden) 보안
드라이브로 문서의 실시간 암호화 저장 및 관리



랜섬웨어 방어플랫폼

랜섬크런처 Ransom Cruncher

랜섬크런처 알고리즘은 기존 랜섬웨어 사전 탐지 및 차단 기술의 불안전성을 획기적으로 발전시킨 기술로써 랜섬웨어 혹은 정보탈취를 목적으로 하는 신종 악성코드가 포함된 악성 소프트웨어를 실시간으로 검증하고 차단할 수 있습니다.



랜섬웨어 탐지 · 차단(1/3)

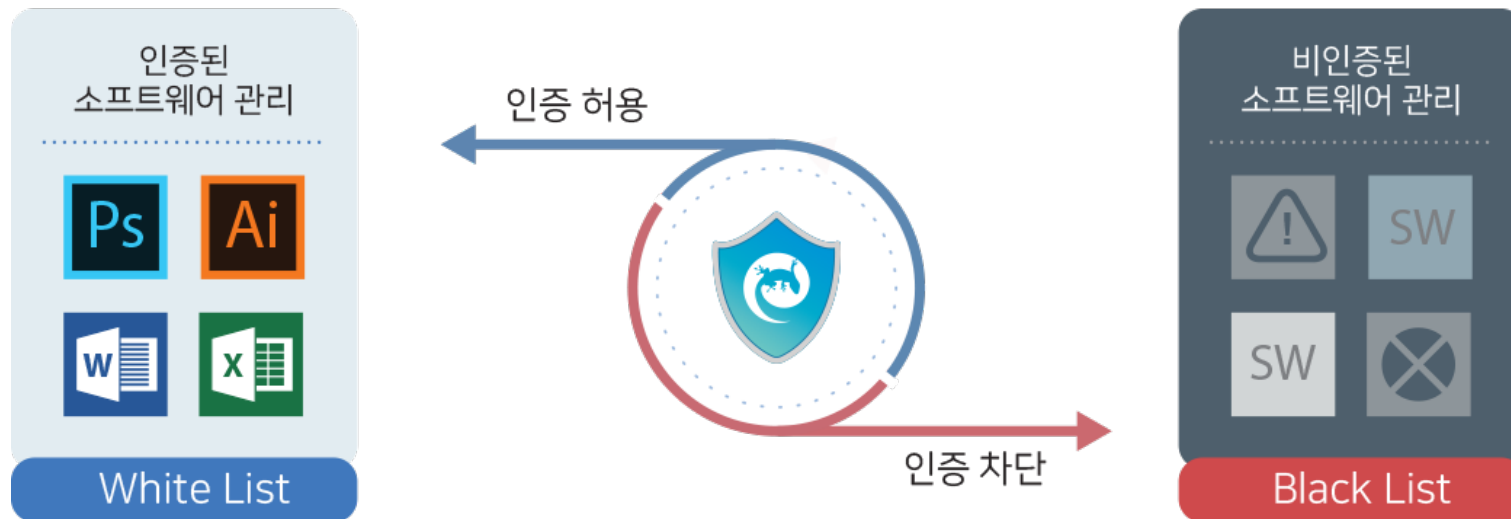
소프트웨어 인증



- 사용자가 중요자료를 위해 사용하는 소프트웨어를 인증 -> 접근 허용
- 인증된 소프트웨어만을 중요자료에 접근 허용하므로 사용자가 의도치않게 설치된 알 수 없는 소프트웨어나 이미 백그라운드에서 활동하는 악성 소프트웨어 접근자체 차단 가능

랜섬웨어 탐지 · 차단(2/3)

지능형 소프트웨어 인증 롤엔진 기반 랜섬웨어 차단



- 불필요한 중요 파일접근 차단으로 암호화/비암호화/정보유출형 랜섬웨어 대응
- 보안위협에 노출된 불법 소프트웨어를 추가하여 사용자에게 인증된 소프트웨어 설치 유도

랜섬웨어 탐지 · 차단(3/3)

행위 분석 기반 탐지 · 차단



- 사용자가 확인되지 않은 소프트웨어 접근을 인증하여 중요자료를 침해 한다고 하더라도 행위 감시 차단 기능으로 중요자료 훼손행위 차단

Contents

- 01. 제품 개요
- 02. 제품 소개
- **03. 중앙관리**
- 04. 개발사 소개

문서 생성 및 삭제 로그관리

인터넷망 PC내의 문서생성 및 삭제에 대한 로그관리가 가능

Total : 7,274

선택 검색

시간 ▼	종류	사용자 (아이디)	그룹 정보	연락처	전제	변경	작업	에러	소요시간	백업 용량	설명
2018-06-21 12:10:30	스케줄 백업	보안팀 사원9 (seczone_13)	이노티움 > 시큐어존데스트	010-7565-1050	10,212 개	4 개	4 개	3 개	[00:00:26]	107.70 MB	백업 완료(이경호_백업)
2018-06-20 17:00:04	스케줄 백업	이인우 (applesoft-office)	이노티움 > 애플소프트 > 이인우		6,659 개	0 개	0 개	0 개	[00:00:02]	0 B	백업 완료(이인우_로컬백업_2)
2018-06-20 16:30:06	스케줄 백업	이인우 (applesoft-office)	이노티움 > 애플소프트 > 이인우		686 개	0 개	5 개	0 개	[00:00:04]	148.68 KB	백업 완료(이인우_로컬백업)
2018-06-20 12:11:29	스케줄 백업	보안팀 사원9 (seczone_13)	이노티움 > 시큐어존데스트	010-7565-1050	10,212 개	2 개	2 개	3 개	[00:00:23]	107.64 MB	백업 완료(이경호_백업)
2018-06-20 09:45:23	드라이브 연결 백업	보안팀 사원9 (seczone_13)	이노티움 > 시큐어존데스트	010-7565-1050	10,212 개	31 개	31 개	3 개	[00:15:53]	214.48 MB	백업 완료(이경호_백업)
2018-06-19 17:00:03	스케줄 백업	이인우 (applesoft-office)	이노티움 > 애플소프트 > 이인우		6,659 개	0 개	0 개	0 개	[00:00:02]	0 B	백업 완료(이인우_로컬백업_2)
2018-06-19 16:30:08	스케줄 백업	이인우 (applesoft-office)	이노티움 > 애플소프트 > 이인우		686 개	0 개	0 개	0 개	[00:00:02]	0 B	백업 완료(이인우_로컬백업)
2018-06-18 12:10:01	스케줄 백업	보안팀 사원9 (seczone_13)	이노티움 > 시큐어존데스트	010-7565-1050	0 개	0 개	0 개	0 개		0 B	플더 오류 백업 종료(이경호_백업) //19 2.168.11.33/secz_rz/기술연구소/seczone_13/backup/ 플더에 연결 오류
2018-06-18 10:13:46	드라이브 연결 백업	보안팀 사원8 (seczone_12)	이노티움 > 시큐어존데스트		47,627 개	3 개	8 개	0 개	[00:00:09]	2.26 MB	백업 완료(JH_TEST)
2018-06-15 18:00:12	스케줄 백업	보안팀 대리1 (seczone_2)	이노티움 > 시큐어존데스트		1 개	0 개	0 개	0 개	[00:00:01]	0 B	백업 완료(테스트)
2018-06-15 17:01:00	스케줄 백업	보안팀 대리3 (seczone_4)	이노티움 > 시큐어존데스트		87,065 개	47 개	81 개	0 개	[00:00:54]	2.27 MB	백업 완료(김선재 백업)
2018-06-15 13:47:05	드라이브 연결 백업	보안팀 사원8 (seczone_12)	이노티움 > 시큐어존데스트		47,627 개	3 개	8 개	0 개	[00:00:14]	2.26 MB	백업 완료(JH_TEST)
2018-06-15 12:10:49	스케줄 백업	보안팀 사원9 (seczone_13)	이노티움 > 시큐어존데스트	010-7565-1050	10,212 개	43 개	43 개	3 개	[00:00:47]	214.71 MB	백업 완료(이경호_백업)
2018-06-15 11:48:56	드라이브 연결 백업	보안팀 사원8 (seczone_12)	이노티움 > 시큐어존데스트		47,627 개	3 개	8 개	0 개	[00:00:10]	2.26 MB	백업 완료(JH_TEST)
2018-06-14 17:00:09	스케줄 백업	이인우 (applesoft-office)	이노티움 > 애플소프트 > 이인우		6,652 개	1 개	6 개	0 개	[00:00:07]	8.31 MB	백업 완료(이인우_로컬백업_2)
2018-06-14 16:30:03	스케줄 백업	이인우 (applesoft-office)	이노티움 > 애플소프트 > 이인우		677 개	0 개	0 개	0 개	[00:00:02]	0 B	백업 완료(이인우_로컬백업)
2018-06-14 12:11:31	스케줄 백업	보안팀 사원9 (seczone_13)	이노티움 > 시큐어존데스트	010-7565-1050	10,212 개	49 개	49 개	3 개	[00:01:28]	394.91 MB	백업 완료(이경호_백업)
2018-06-14 10:38:07	드라이브 연결 백업	보안팀 사원8 (seczone_12)	이노티움 > 시큐어존데스트		47,627 개	3 개	8 개	0 개	[00:00:20]	2.26 MB	백업 완료(JH_TEST)
2018-06-14 00:42:25	스케줄 백업	보안팀 사원9 (seczone_13)	이노티움 > 시큐어존데스트	010-7565-1050	0 개	0 개	0 개	0 개		0 B	플더 오류 백업 종료(이경호_백업) //19 2.168.11.33/secz_rz/기술연구소/seczone_13/backup/ 플더에 연결 오류

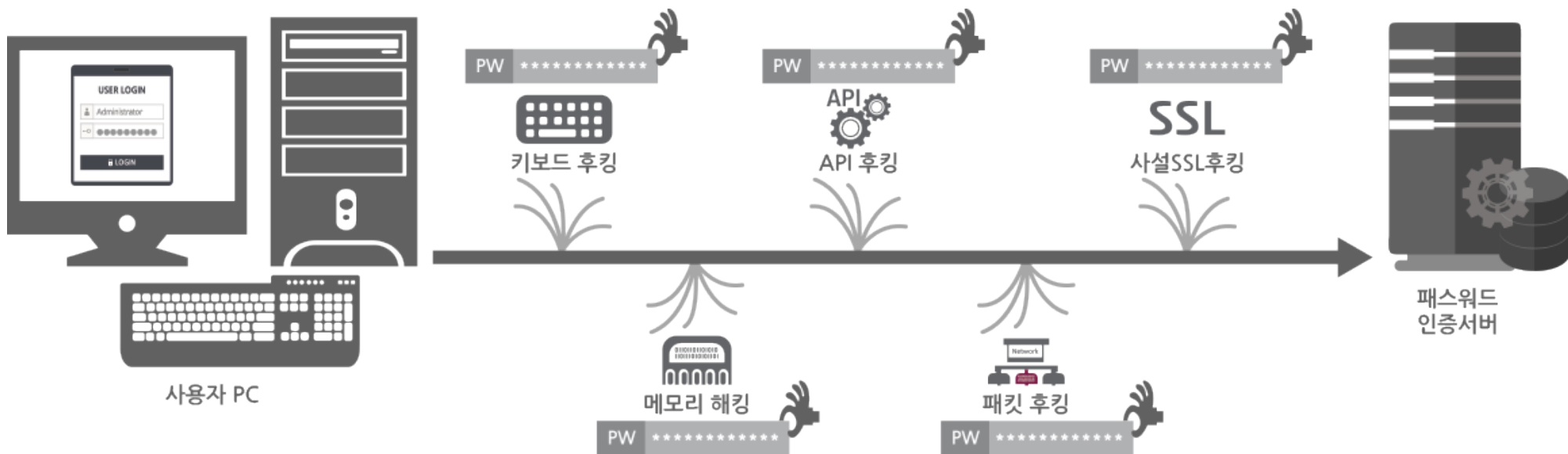
시스템 접근 제어

중앙관리매니저에서는 사용자 및 그룹에 접근제어 설정으로 정보자산의 유출을 최소화 할 수 있으며, PC자원의 감사 대상인 로컬 디스크 드라이브, USB, 제어판, REGEDIT, MMC, GPEDIT 등 정보 유출에 대한 모든 위험 요소를 차단할 수 있습니다.



중앙관리 매니저 ID/PW 해킹방지 인증보안의 필요성

● Password Extortion

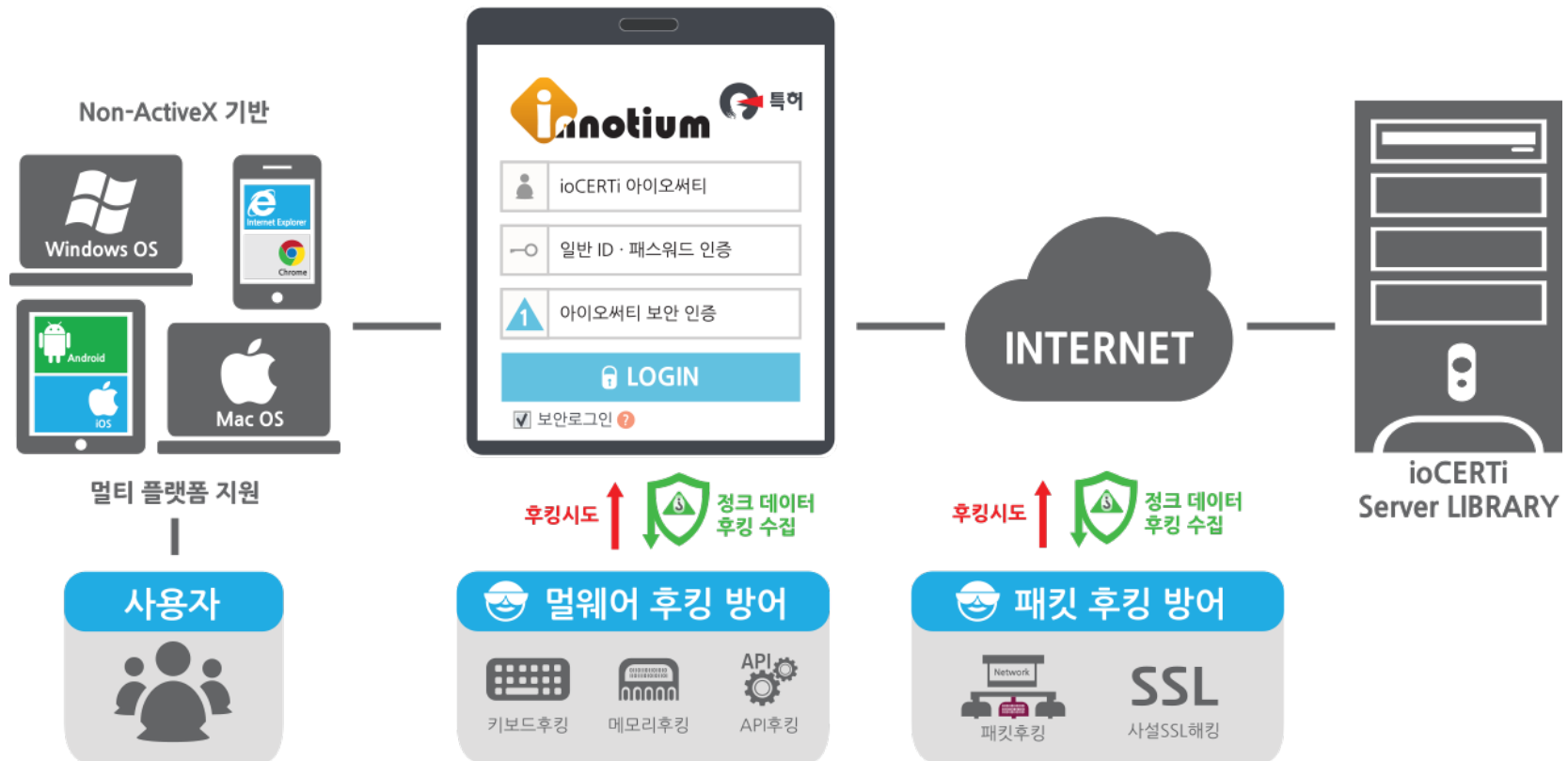


◆ 패스워드 전송 간 유출 위험

- ▶ 사용자 디바이스에서 인증서버로 패스워드를 전송하기 위한 모든 상황에서 유출의 위험성이 있습니다.
- ▶ 패턴 및 이미지 등의 방법으로 전달할 경우에도 전송 직전 메모리상에 입력된 패스워드가 유출될 수 있습니다.
- ▶ 유출 자체를 100% 막을 수 있는 방법은 현실적으로 존재하지 않습니다.

중앙관리 매니저 ID/PW 해킹방지 인증보안 아키텍처

● 시스템 아키텍처



리자드 클라우드 디크런처 RC 도입효과



망분리 인터넷망PC 중요 문서 보안과 업무생산성 동시 해결



인터넷망 PC
문서 유출 차단



망분리
구축 지침
이행



인터넷망 PC
보안 취약성
개선



직원
보안 의식 강화



랜섬웨어
방어

Contents

- 01. 제품 개요
- 02. 제품 소개
- 03. 중앙관리
- **04. 개발사 소개**

주요사업내용

개발사인 (주)이노티움은 다수의 특허와 인증서를 기반으로 실시간 PC(엔드포인트) 데이터 백업 및 랜섬웨어 예방 보안 백업, 문서보안, 외부반출문서보안 등 정형/비정형 전자문서의 관리와 정보보호 관련 솔루션 사업에 주력하고 있습니다.



레퍼런스

대기업 계열사인 두산 중공업을 비롯하여 다양한 산업의 고객사에 인터넷망 PC 데이터 보안 관리 사업을 수행하였으며 제품의 안정성과 신뢰성을 인정받고 있습니다.

두산 중공업



효성 중공업

HYOSUNG

대명



삼강엠앤티



공정거래위원회



공정거래위원회

HSD엔진



유비무환 有備無患

미리 준비하면 걱정이 없습니다.

(주)이노티움 www.innotium.com

P. 02)3283-2021 | E.info@innotium.com