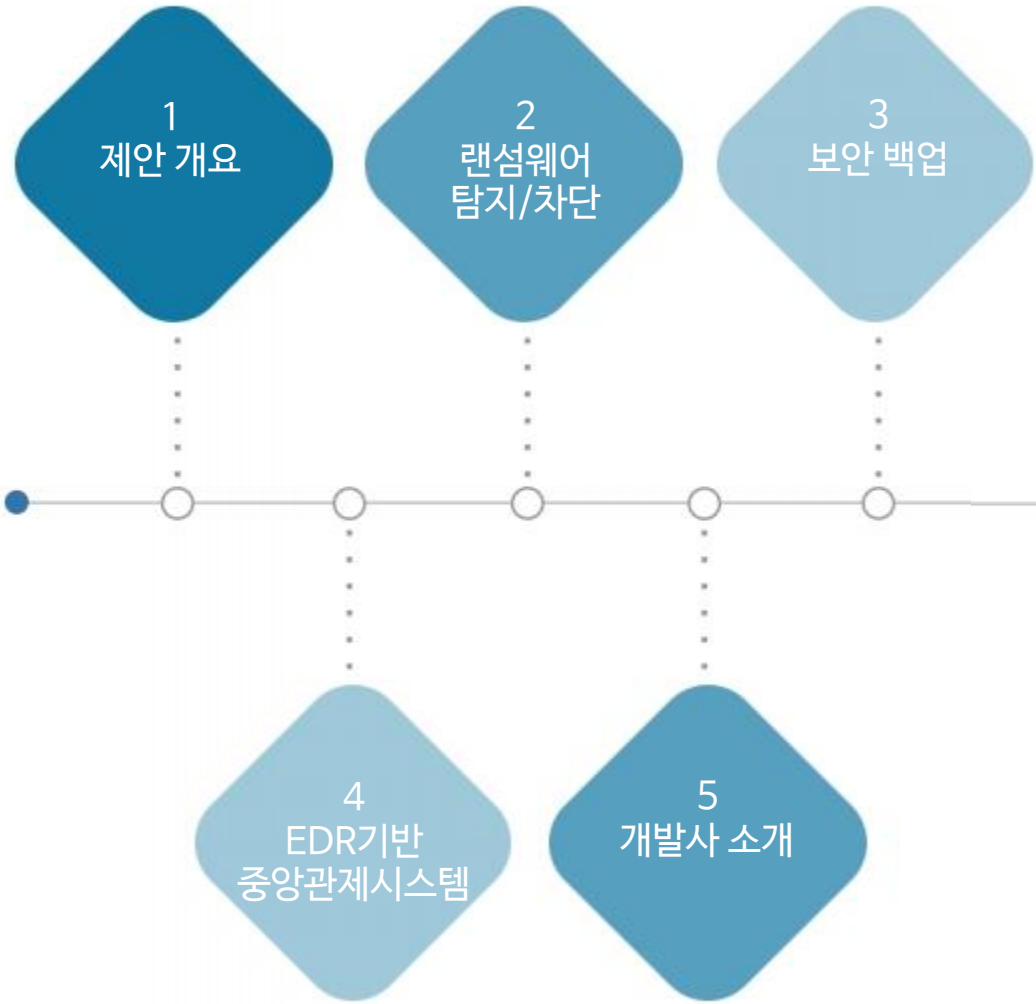
LIZARD
|C|L|O|U|D|

EDR기반 4단계 랜섬웨어 방어 솔루션

리자드 클라우드

|주|애플소프트

목차

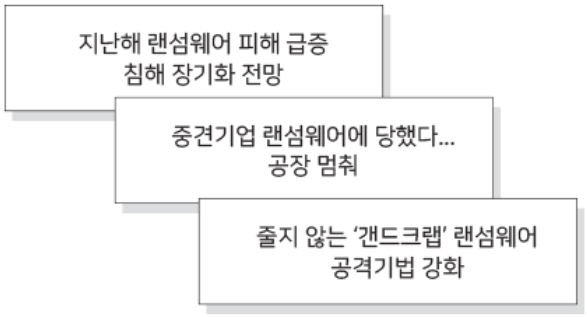


제안 개요

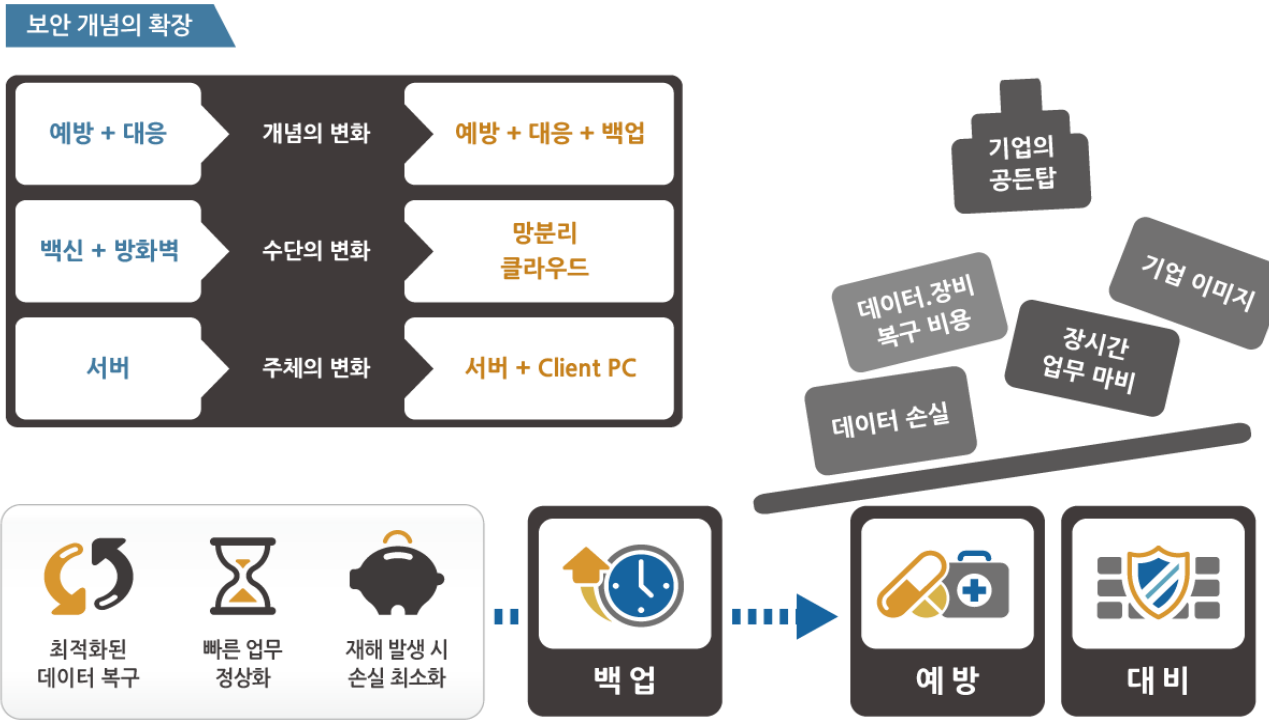
제안배경 및 목적

제안 배경 기본에 충실한 데이터 관리의 중요성 부각

최근 기업 내 데이터가 폭발적으로 증가되면서 기업환경에 최적화된 데이터 보호 및 관리방안의 마련은 기업의 최우선 과제로 자리잡고 있습니다.
앞으로의 사이버 공격은 튼튼한 방어벽을 쌓는 것 만으로 만일의 사태에 대비할 수 없기 때문에 재정적 손실이 예상되는 백업과 복구 영역도 충분히 대비해서 보안의 완성도를 제고해야 합니다.



〈 고도화된 랜섬웨어 공격 〉



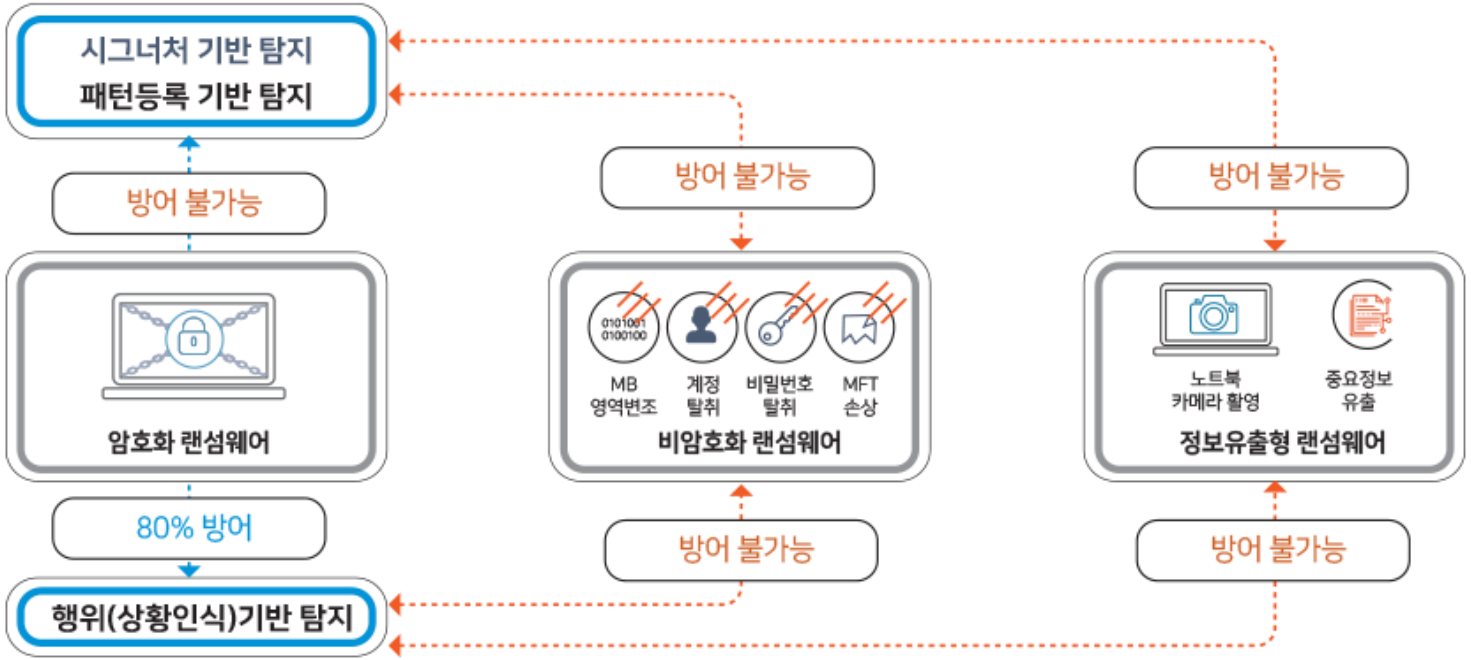
〈 보안과 백업의 융합〉

1. 제안 개요

제안배경 및 목적

제안 배경 지능화 ·표적화 랜섬웨어 공격에 기존 보안기술 취약

이메일 첨부파일 및 특정 사이트 접속으로 PC와 서버의 데이터를 암호화 한 후 복호화 키를 대가로 금전을 요구하는 랜섬웨어의 대규모 공격으로 개인, 기업, 정부기관 등의 피해가 현실화되고 점점 더 진화하는 추세입니다. 진화된 랜섬웨어 및 IT재해는 기존의 방식으로는 100%방어가 불가능 합니다.



1. 제안 개요

제안배경 및 목적

제안 목적 랜섬웨어 및 IT재해에 대비 및 보안 백업

기업의 시스템 환경을 보호하고 보안 백업과 재해복구를 간소화 하며, 개별 파일부터 전체 서버까지 원하는 규모의 데이터나 서비스의 시스템을 보안 백업 및 복구하여 기업 업무 환경의 연속성을 보장하며 원활한 데이터 관리를 하는 것이 목적입니다.

업무 연속성 보장 및 운영 비용 절감

업계 최고의 탐지/차단 및 보안 백업 관리 시스템 구축

업무 연속성 보장

- 랜섬웨어 및 IT재해에 대비 가능
- 기업의 시스템 환경을 보호하고 백업과 재해복구를 간소화하며 개별 파일부터 전체 서버까지 원하는 규모의 데이터나 서비스의 시스템을 복구하여 기업업무 환경의 연속성을 보장

랜섬웨어 탐지 / 차단

- EDR기반 랜섬웨어 방어플랫폼으로 신/변종 랜섬웨어 탐지 / 차단
- 기존 랜섬웨어 사전탐지 및 차단 기술의 불안정성을 획기적으로 발전시킨 기술로서 랜섬웨어 및 기타 IT재해 위협 차단

기업 정보 보호를 위한 최선의 데이터 관리

원활한 데이터 관리

- 직무 데이터를 보안백업 함으로써 퇴사자 및 사고에 의한 데이터 유실에 예방 가능
- 중복 제거 백업을 구성하여 백업 저장소의 용량을 효율적으로 관리 할 수 있어 업무 생산성 향상

중앙관리매니저

- 중앙 관리자를 통해 설정된 정책을 사용자 PC에 할당할 수 있으며, 전체 탐지로그 및 프로세스 수집 및 분석 할 수 있어 사후 감사로그에 사용할 수 있습니다.

대내외 환경 분석

대내외 환경

2015년을 기점으로 랜섬웨어 피해 건수가 기하학적으로 급증하기 시작했으며 기존 불특정 대상이 아닌 국내외 기관 및 금융, 기업들에게 지능형 위협, 표적형 사이버공격을 가하고 있으며, 이에 각종 안티 바이러스 및 다양한 보안 솔루션으로 사전 방어체계를 구축하고 있으나 연일 다양한 신 · 변종 랜섬웨어가 발생하고 피해 받아 해마다 막대한 금액 손실이 증가하고 있다

AS-IS

현재 기업시스템의 현황

- 기업의 핵심 자산과 산출물인 데이터가 축적/관리 되지 않고 개별적으로 관리 /위임 되고 있음
- 이동식 디스크에 백업데이터를 보관하여 데이터 손실 및 유실의 문제가 있음
- 동일데이터의 이중백업으로 인한 용량부족 문제 발생
- 랜섬웨어 및 악성코드에 의한 데이터 손실 발생

TO-BE

앞으로의 개선 방향

- 중앙관리매니저를 통하여 사용자 및 그룹을 효율적으로 관리하여 데이터의 회사 자산화
- 중앙스토리지에 데이터를 보관함으로써, 데이터 손실 및 유실 감소
- 버전관리 및 데이터 중복제거를 통해 효율적인 스토리지 관리 가능
- 탐지 / 차단 및 백업으로 랜섬웨어 및 악성코드에 의한 데이터 손실 최소화

1. 제안 개요

리자드 클라우드 v10

리자드 클라우드는 랜섬웨어 공격을 EDR기반으로 사전에 차단하고, 데이터를 실시간으로 안전한 저장소에 보안백업 하여,
랜섬웨어 및 IT재해에 대비해 업무 연속성 보장 및 데이터 관리에 최적화된 통합데이터 보안관리 솔루션 입니다.

용도	제조사	모델명	구성
보안백업	(주)이노티움	리자드 클라우드	SW(매니저+에이전트)

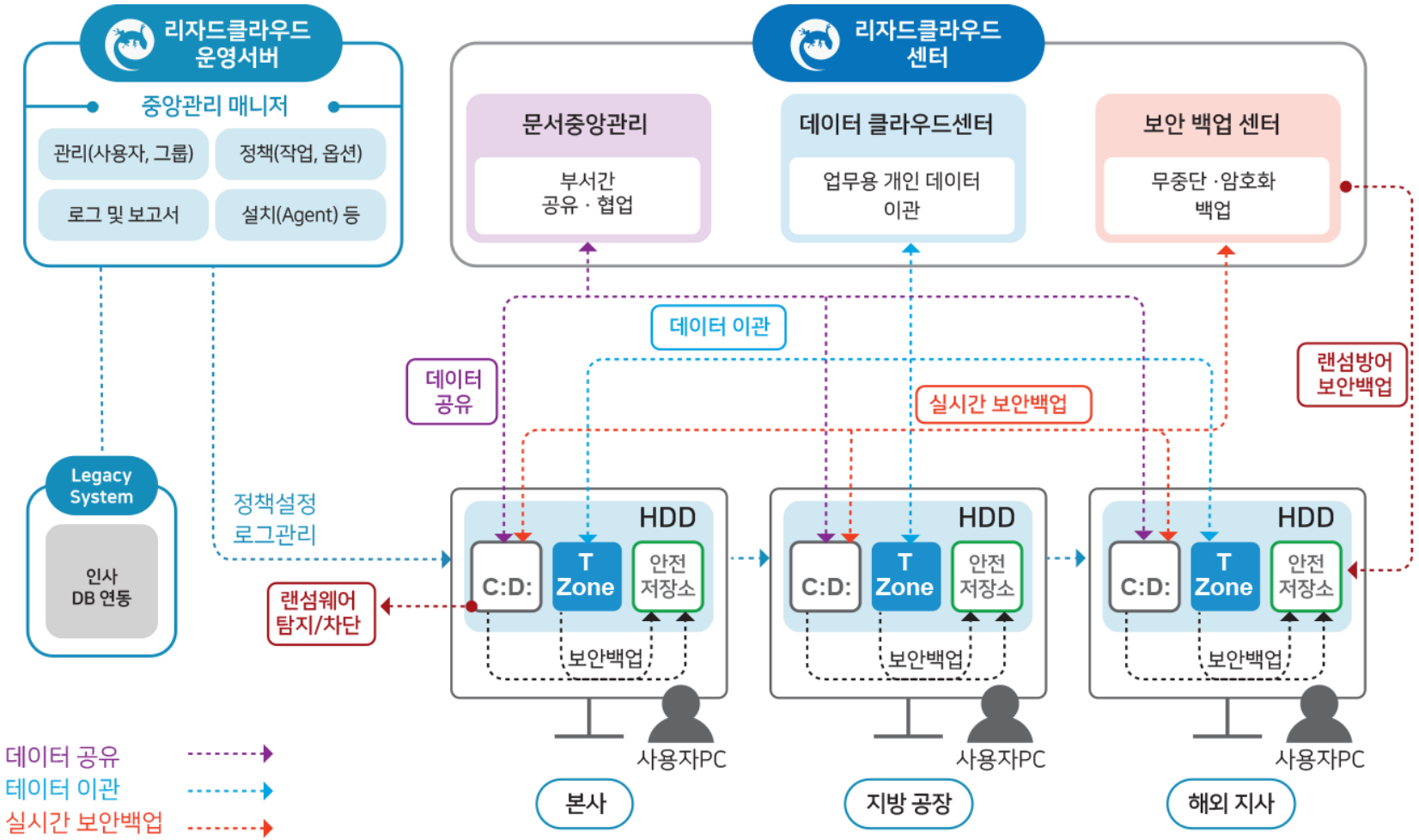
리자드 클라우드 v10
Lizard Cloud v10

제품 주요 기능

- 사용자별 IT재해(HDD장애,개인정보손실등)대비 보안 백업
- 랜섬웨어 차단 · 탐지 기능
- 백업 저장소 보호 및 랜섬웨어 방어(ARIT 기술 탑재)
- 보안 디스크 생성(로컬 디스크 내에 암호화된 공간 생성 관리)
- 개인정보 및 중요문서의 내용 검출 및 백업 후 완전 삭제
- 실시간/스케줄 백업/암호화백업/이력관리
- PC 사용자/그룹, PC Agent 중앙관리
- 각종 백업 로그 및 통계 관리
- DB/파일 백업, 중분/차등 백업, MS Outlook 백업, 대량 파일 백업
- USB,외장HDD,제어판,CMD명령어,Regedit 차단,로컬 PC 매체제어
- 중앙관리매니저에 의한 정책 설정 및 로그 관리

구 분	하드웨어 권장 사양(500 User기준)	
중앙관리매니저 SW 탑재	- CPU 8Core이상 - Memory 32GB 이상	- HDD : SSD 200GB X2ea(RAID1 구성) - Dual Power - 운영체제 Cent OS - DBMS Maria DB

리자드 클라우드 v10 아키텍쳐



리자드 클라우드 핵심기능

적은 비용과 편리함으로 보안사고 예방과

법적인 요건을 충족하는 솔루션 “리자드 클라우드 V10”

랜섬웨어 탐지 차단

랜섬웨어 피해 예방
업무 중단 방지

보안 백업

랜섬웨어 피해시
백업된 데이터 보호

백업 데이터 암호화

해킹 대응
개인정보 보호

리자드 클라우드 V10

문서 공유와 보안 협업

부서별, 프로젝트별 구성원간
안전하고 편리한 자료공유와 협업

매체 제어

원본삭제를 통한
USB 및 이동기기 제어

디지털 암호화 보안 영역

로컬 디스크내 생성 되어,
기밀문서 보관 가능

원상복구보증서

리자드 클라우드는 국내 유일의 원상복구 보증서를 발행하여, 랜섬웨어 및 기타 IT재해에 데이터가 감염되었을 경우 100% 데이터 복원을 보장합니다.

원상복구 보증서

Certificate of Assurance

(주)이노티움은 아래 대상 제품을 구입한 고객의
데이터가 랜섬웨어 공격으로부터 암호화될 경우
원상복구할 것을 보증합니다.

대상제품 1. 리자드백업 v10 DB서버 랜섬크런처
2. 리자드클라우드 v10 랜섬크런처

(FTP/SFTP 프로토콜 백업 한정)

2019년 2월27일
주식회사 이노티움 대표이사

inotium

- 국내 보안 개발사는 도입 이후 사이버 테러 및 해킹을 당할 경우 대부분 책임 회피를 하고 있으나, 글로벌 보안 회사는 **'Cyber Security Insurance'** 를 통해 리스크를 최소화 시킴
- 특히 랜섬웨어는 데이터를 암호화하여 업무가 중단되어 막심한 2차 피해를 입게 되는 특성이 있어 빠른 데이터 복구가 필요함
- 보안백업 기술과 연동하여 랜섬웨어 침해로 데이터가 암호화될 경우 개발사에서 무상으로 데이터를 원상복구하는 보증제를 도입하고자 함

기대효과

리자드 클라우드는 랜섬웨어 공격을 EDR기반으로 사전에 차단하고 데이터를 실시간으로 안전한 저장소에 보안 백업하여,
랜섬웨어 및 IT재해에 대비해 업무 연속성 보장 및 데이터 관리에 최적화된 통합데이터 보안관리 솔루션 입니다.

구축 후 기대효과

랜섬웨어 침해/IT재난 발생시 신속한 대응으로 업무 연속성 확보

- 랜섬웨어 침해/사이버 테러/해킹에 의한 개인정보 삭제시 즉시 복원 대응 조치
- HDD고장으로 인한 개인정보 유실시 즉시 복원 대응 조치

업무 활용 편의성 제공

- 부서내 개인정보 공유를 통한 업무 효율성 증가
- 인사 이동시 업무파일의 인수인계
- 사용자 문서 덮어쓰기 및 삭제시 즉시 복원으로 사무 효율성 제고

직무 개인정보의 실시간 회사 자산화

- 실시간 보안백업으로 전자문서 및 개인정보의 회사 자산화 조치
- 백업된 개인정보의 사용자에 의한 삭제 방지로 자산 보호 조치

운영비 절감 및 클라우드 플랫폼 대비 확장성 제공

- 개인정보 관리 비용 절감 및 협업 기능 제공으로 업무 생산성 향상
- 향후 클라우드 플랫폼(VDI) 도입시 호환성과 확장성 제공

직무 개인정보 관리의 효율성 제고

- 파일 중복제거 기능으로 30% 이상 저장소 원가 절감 가능
- 직원 인사이동시 자료이동, PC이동 등에 따른 불편 해소
- PC 및 HDD 등 HW 교체시 손쉬운 직무 개인정보 마이그레이션

직원, 경영자, IT관리자 모두 만족

- 경영자 : 개인정보 리스크 매니지먼트 체계 구축
- 직원 : 완벽한 랜섬웨어 방어 및 IT재해 대비
- IT관리자 : 전사 개인정보 관리 효율화 및 IT환경 고도화

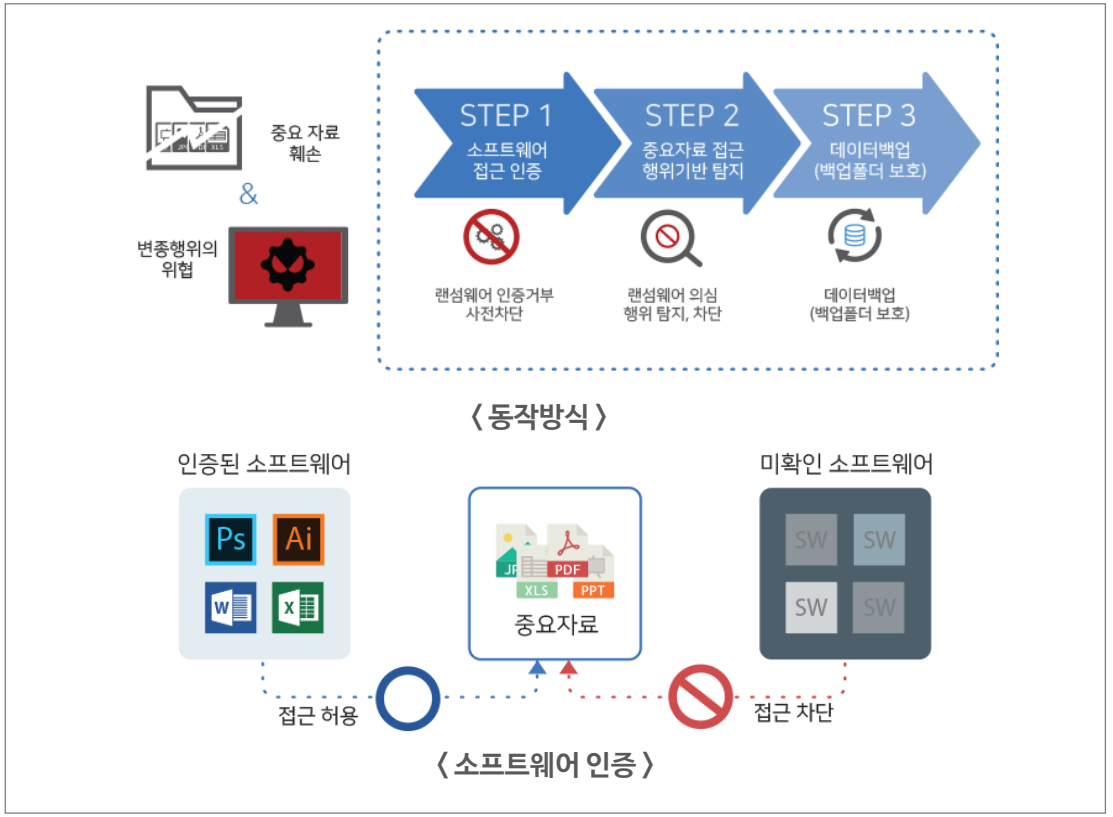
지능화 · 표적화 랜섬웨어 공격
사전 탐지/차단

2. 지능화 · 표적화 랜섬웨어 공격 사전 탐지/차단

한국형 EDR기반 다계층 랜섬웨어 방어 알고리즘

랜섬웨어 방어 알고리즘은 기존 랜섬웨어 사전탐지 및 차단 기술의 불안전성을 획기적으로 발전시킨 기술로써 랜섬웨어 혹은 정보탈취를 목적으로 하는 신종 악성코드가 포함된 악성 소프트웨어를 실시간으로 검증하고 차단합니다. PC데이터를 공격하는 랜섬웨어 뿐만 아니라 관리자 PC를 경유하여 서버의 DB를 공격하는 랜섬웨어를 강력하게 방어합니다.

랜섬웨어 탐지 차단 알고리즘



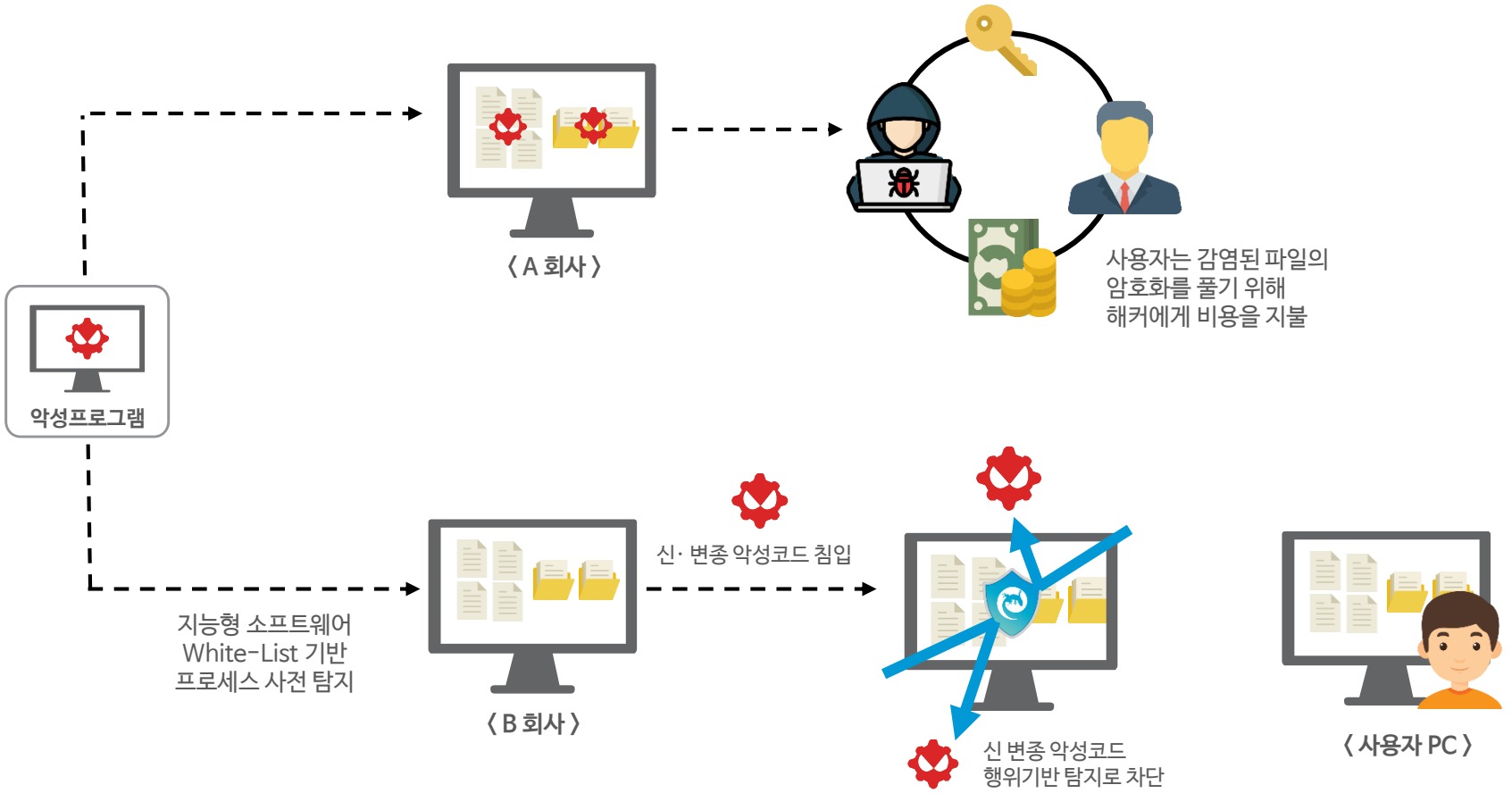
내용 설명

- 랜섬웨어 및 악성 SW 차단
- 비 인증 프로그램 실행 차단
- 미확인 프로세스 실행 차단
- 신 변종 랜섬웨어 행위 기반 사전 탐지/차단
- 중요 자료 감염 시 순간 백업 및 자동 롤백
- 랜섬웨어 격리 및 확산 방지
- 최종 랜섬웨어 침입 대비 무중단 보안 백업
- PC데이터 실시간 자동 백업 및 복구
- 데이터 이력관리 및 중복 제거

2. 지능화 · 표적화 랜섬웨어 공격 사전 탐지/차단

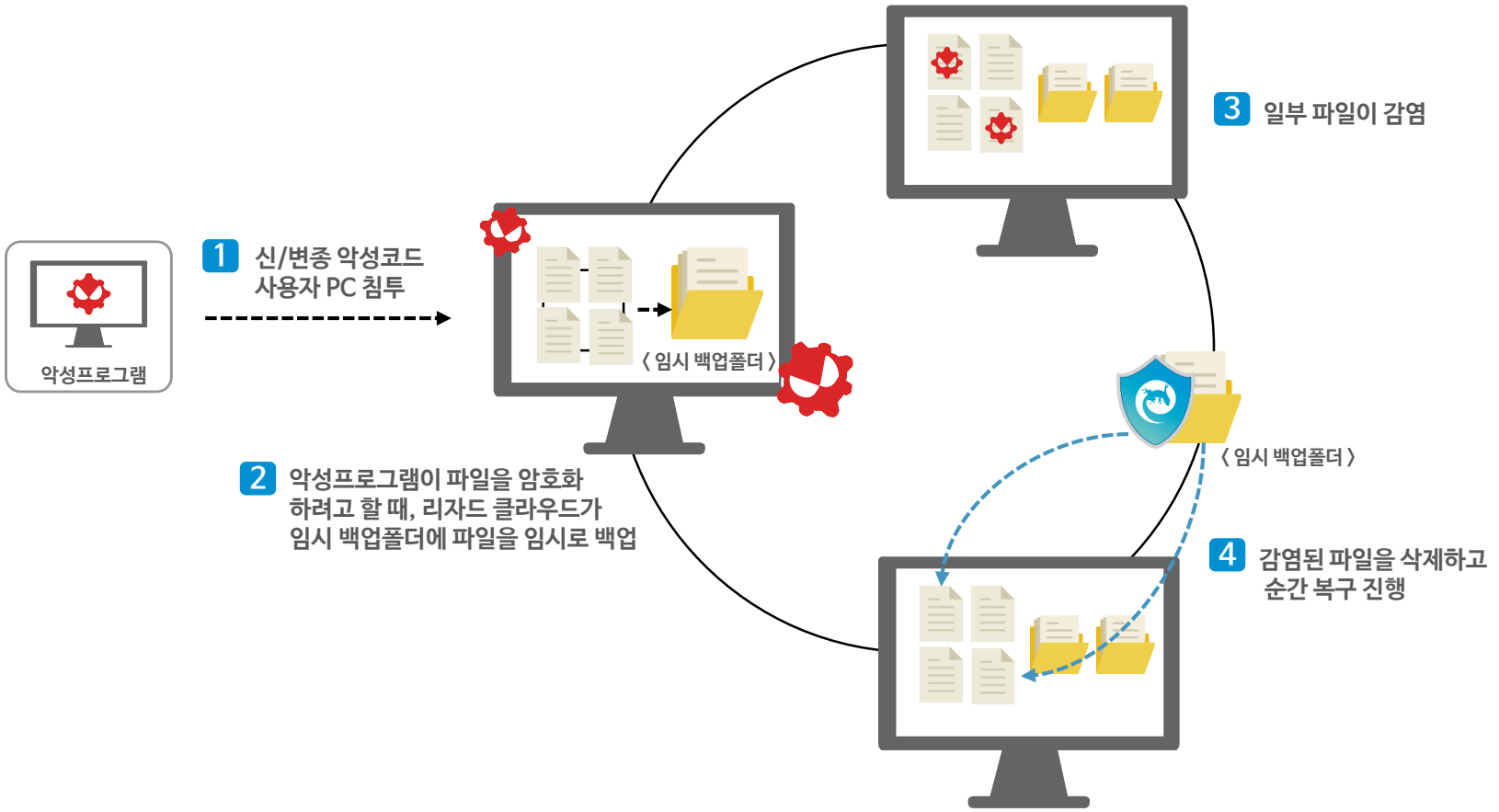
사전 탐지 차단 기능소개(1/2)

리자드 클라우드는 보안문제를 해결하기 위해 지능형 White List 기반으로 프로세스를 탐지하고, 신 변종 악성코드 탐지를 위해 행위기반 탐지하여 사용자 PC데이터를 보호합니다.



사전 탐지 차단 기능소개(2/2)

사용자 파일이 예기치 않은 악성프로그램의 위협에 감염 되었을 시, 감염된 파일을 삭제하고 실시간으로 복원해주는 기능입니다.
사용자는 감염이 되어도 순간 복구를 통해 복원의 과정을 거치지 않고 파일을 사용할 수 있습니다.



업무 연속성 보장 및 데이터 관리에
최적화 된 보안 백업 솔루션

3. 업무 연속성 보장 및 데이터 관리에 최적화 된 보안 백업 솔루션

보안백업 이란?

보안백업은 신/변종 랜섬웨어에 대비하여 백업된 저장소를 보호 하고, 랜섬웨어를 탐지 및 차단 합니다. 보안 백업된 데이터는 암호화 백업이 되어 데이터가 유실되어도, 해당 데이터는 암호화 되어 사용할 수 없습니다. 또한 중앙관리를 통해 사용자의 정책설정, 로그 관리 등이 가능하기 때문에 사후 감사관리가 가능합니다.

보안백업의 기준

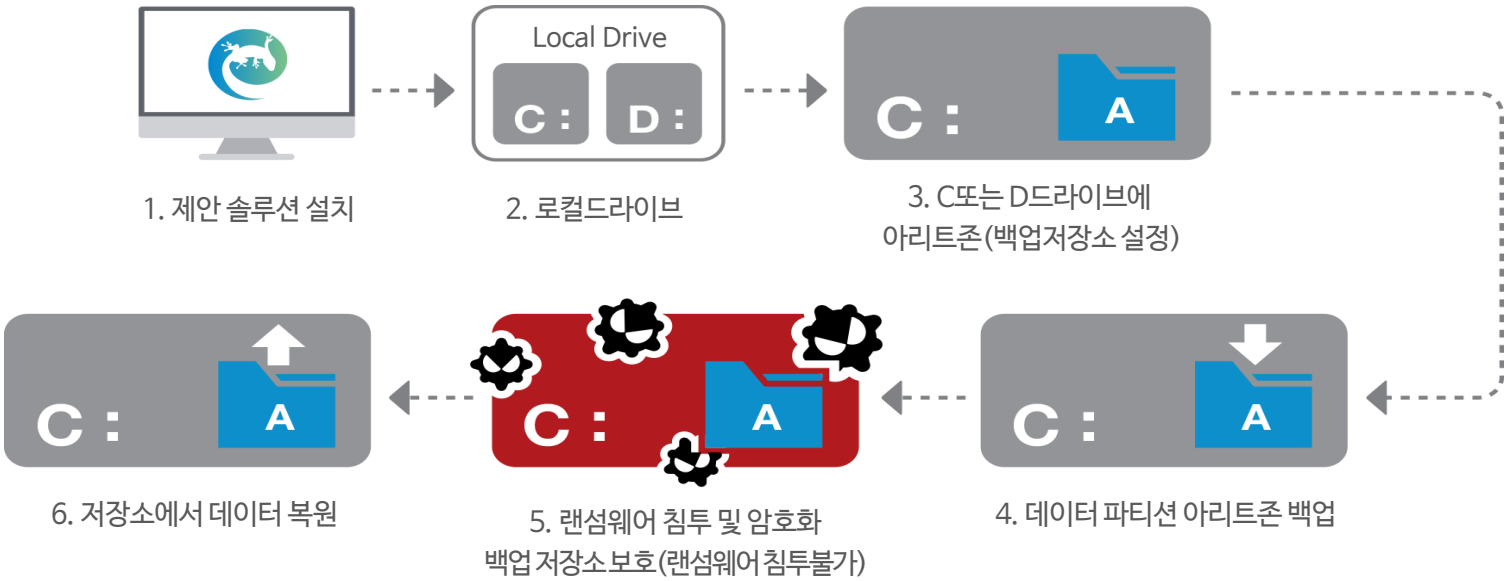
Step1	Step2	Step3	Step4
백업 주기	백업 정보	설정 백업	백업 데이터
사용자가 얼마나 자주 별도로 백업을 해야 하는가?	백업된 정보는 최신 정보 인가?	원하는 파일 혹은 드라이브만 백업할 수 있는가?	백업한 데이터는 랜섬웨어 로부터 안전한가?
보안백업			
파일 저장과 동시에 실시간 자동 백업	백업개인정보는 항상 최신의 데이터 상태 유지	파일 필터링 및 소스 폴더 설정을 통하여 사용자 설정 백업 가능	ARIT 기술을 통하여, 랜섬웨어로 부터 백업 데이터 보호

3. 업무 연속성 보장 및 데이터 관리에 최적화 된 보안 백업 솔루션

백업 데이터 보호 ARIT Zone

ARIT Zone이란 랜섬웨어 및 IT침해 로부터 백업된 파일을 보호하는 영역을 만들어주는 기술입니다. 리자드 클라우드의 프로세스만이 저장소 폴더에 접근할 수 있으며, 이외에 프로세스는 저장소 영역에 접근할 수 없습니다.

침해예방 자체 개발 아리트(ARIT) 기술



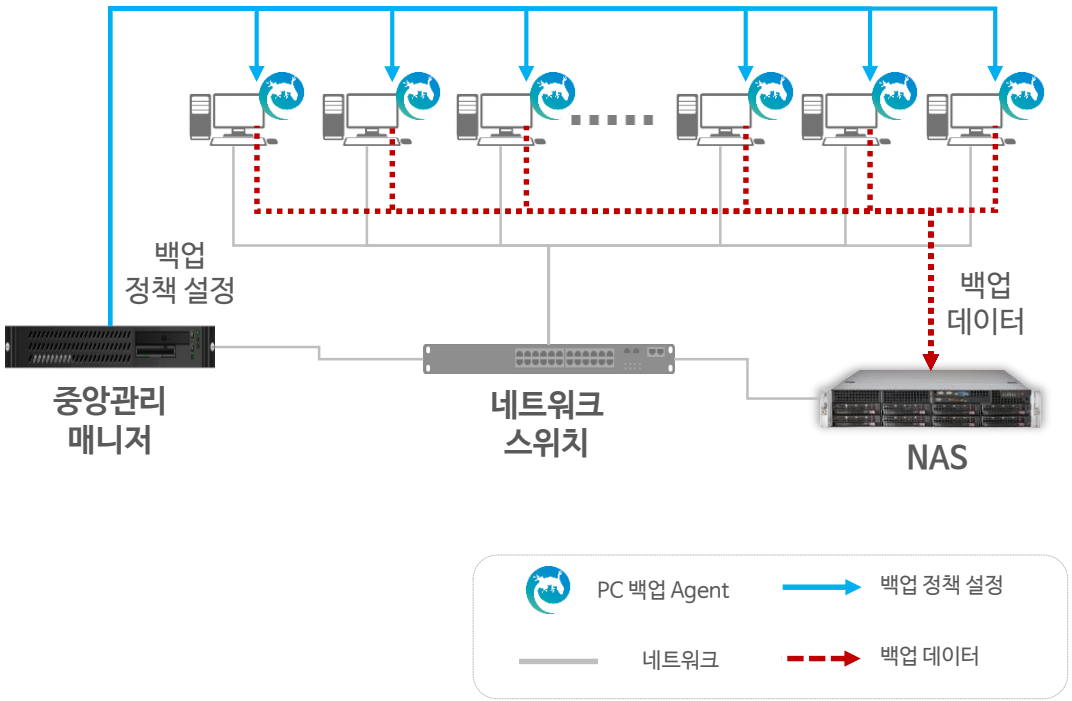
※ 최초 랜섬웨어 침해예방 자체 아리트(ARIT)기술 개발 및 탑재

제안 솔루션 보안 백업은 PC · 서버 · VDI클라우드 엔드포인트 데이터를 실시간으로 백업하여 랜섬웨어 침해 및 사이버 테러와 돌발적인 IT재해에 대비하는 리스크 매니지먼트 솔루션입니다. 특히 국내 최초로 '한국랜섬웨어침해대응센터' 운영을 바탕으로 실제 랜섬웨어인 크립토월, CTB-Locker, TeslaCrypt, 최초 한글 버전인 크립토락커 악성코드에 테스트를 진행하며 아리트 기술을 개발 탑재하여 예방수준이 타제품과 비교되지 않습니다.

리자드 클라우드의 보안 백업

리자드 클라우드의 보안백업은 백업주기를 설정할 수 있으며, 백업된 데이터는 항상 최신버전을 유지하며 버전관리가 가능합니다.
백업할 데이터를 설정하여 백업 할 수 있으며, 백업된 데이터는 자체 개발한 ARIT기술을 통해 안전하게 보호됩니다.

보안 백업 구성도



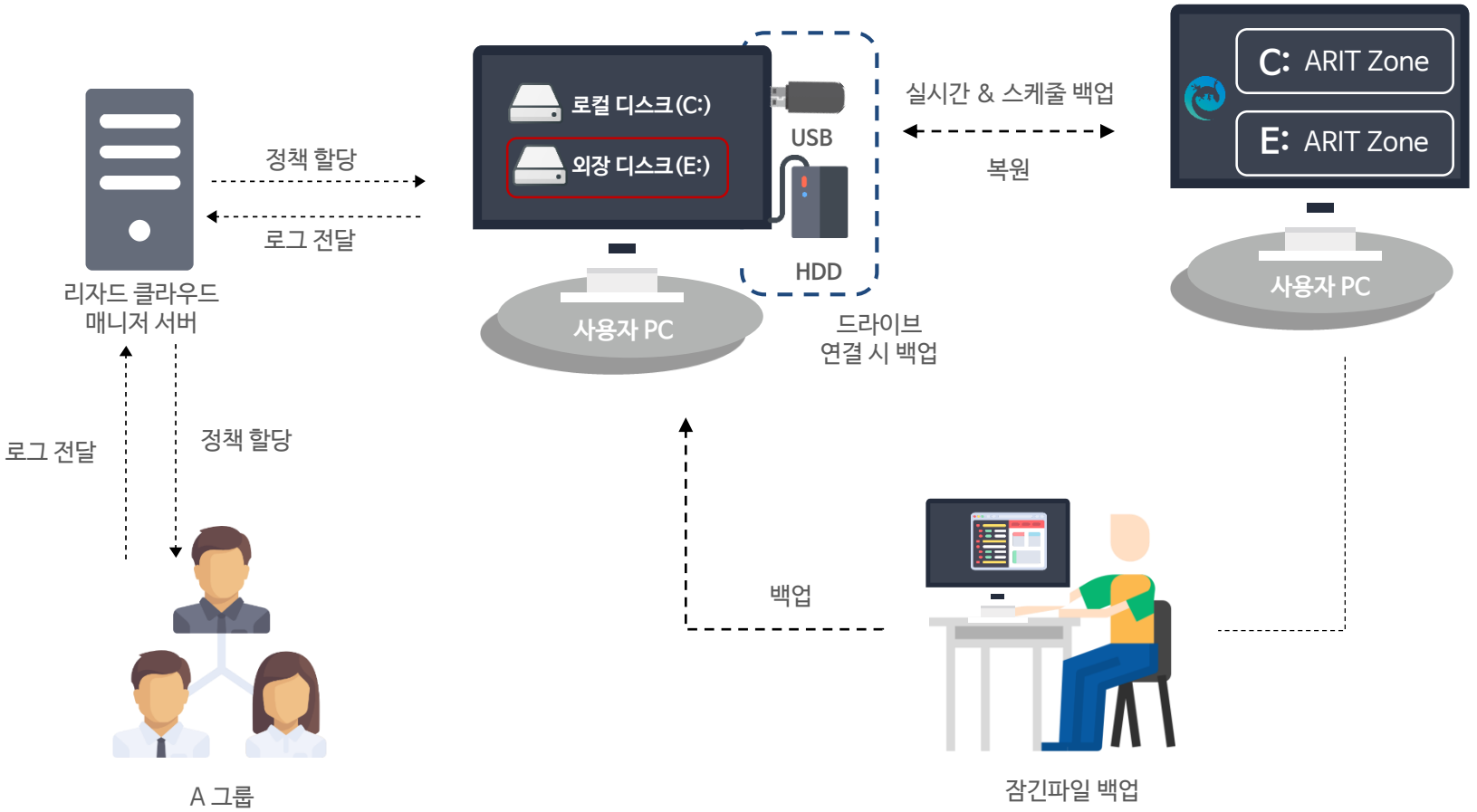
내용 설명

- 실시간 / 스케줄 암호화 보안 백업
- 폴더 백업 / 파일 확장자별 백업
- 백업 후 원본 삭제 기능 (문서 저장 방지 기능)
- SFTP 사용 백업 시 패킷 보호
- 데이터 중복제거
- 디스크 증설 비용 절감 및 네트워크 부하 감소
- 변경된 내용만 별도 저장 관리
- 중앙관리자에 의한 정책 설정
- 전체 탐지 로그 및 프로세스 수집 / 분석
- 사용자, 부서 , 그룹별 폴더 접근 및 작업 권한 세부 설정
- 부서별, 프로젝트별 디스크를 생성하여 구성원간 안전하고 편리한 자료 공유와 협업

보안 백업 기능소개(1/3)

리자드 클라우드의 보안백업은 중앙관리매니저에서 사용자 PC에 작업을 할당하고 사용자는 해당 정책으로 실시간&스케줄 백업을 진행합니다.

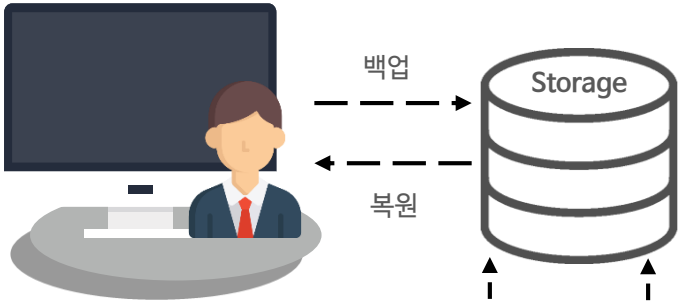
- 드라이브 연결 시 백업 : 드라이브가 연결되면 자동으로 백업이 진행되어 이동식 디스크의 데이터 손실을 줄일 수 있습니다.
- 잠긴파일 백업 : 열려 있는 DB파일은 복사나 백업이 어렵지만, 해당 기능을 이용하면 열려있는 파일도 백업진행이 가능하여, 업무를 중단하지 않고 백업할 수 있습니다.



보안 백업 기능소개(2/3)

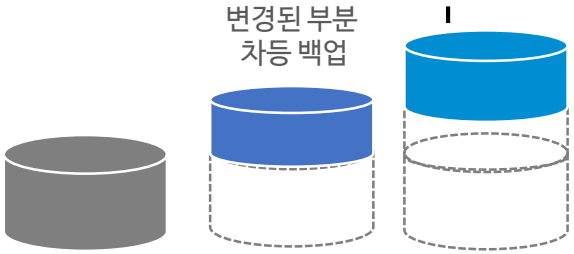
1 실시간 복원

백업된 데이터
실시간 복원 가능



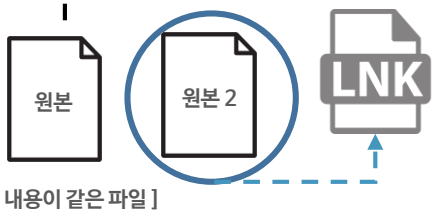
2 버전관리

백업된 데이터는 버전별로 저장되어,
원하는 날짜의 파일로 복원 가능



3 바이트 중복방지 백업

변경된 부분만을 차등백업 하기 때문에 DB파일과 같은
용량이 큰 파일을 백업할 때 유용



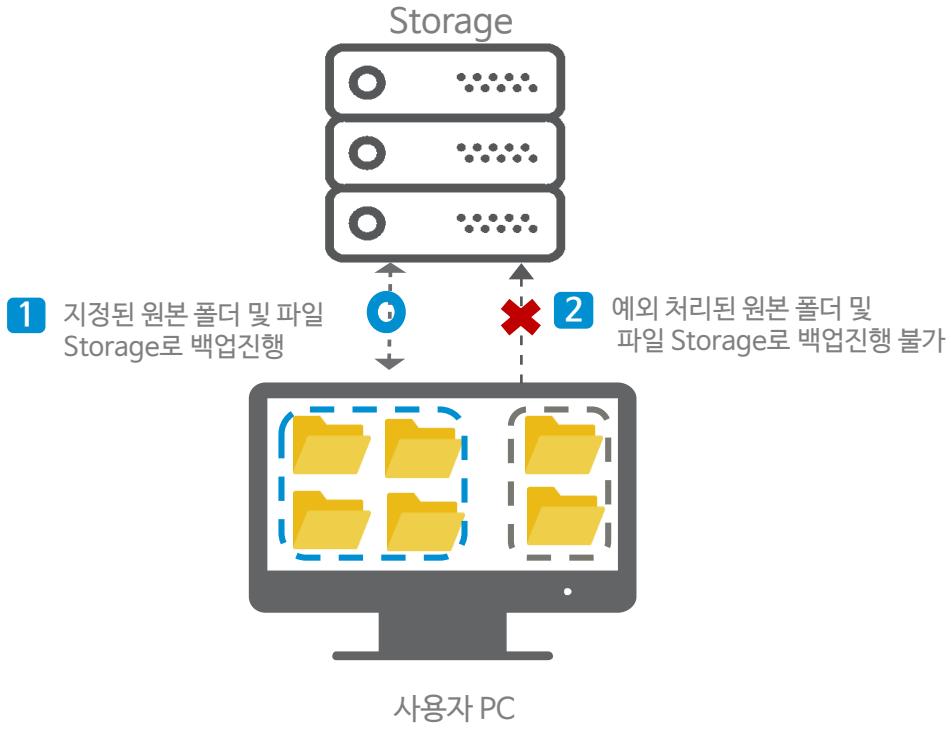
4 파일중복백업방지

파일명이 동일하더라도, 내용이 동일한 파일은 LNK파일로
백업되기 때문에 스토리지를 효율적으로 사용할 수 있음

보안 백업 기능소개(3/3)

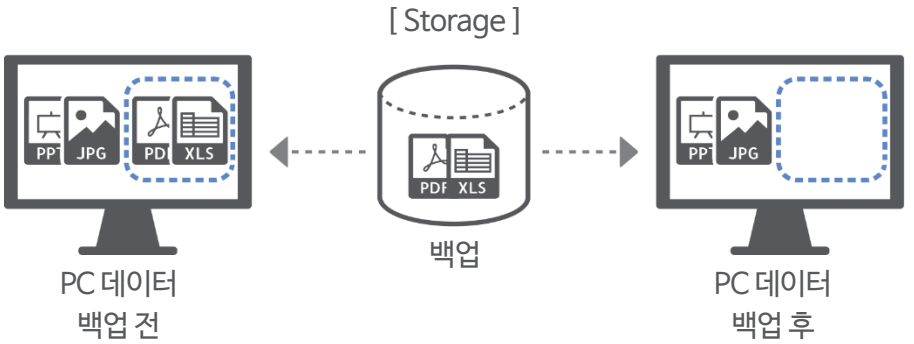
〈 확장자 및 폴더 지정 백업 〉

리자드 클라우드 보안 백업의 경우 폴더/ 확장자를 설정하여 백업하여
스토리지의 용량을 감소 시킬 수 있습니다.



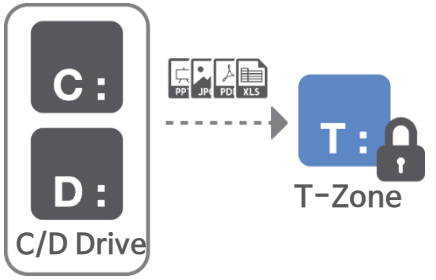
〈 백업 후 원본 삭제 〉

사용자 PC에서 백업이 완료된 데이터는 로컬영역에서 자동 삭제되므로
문서 중앙화처럼 사용 할 수 있으며, 이동 장비를 도난 분실 및 악의적 고의 유출에
대비 할 수 있습니다.



T-Zone(Trust Zone) 기능 : 디지털 보안 영역

1 관리자 T-Zone 정책 할당 2 사용자 Login 3 T-Zone 생성

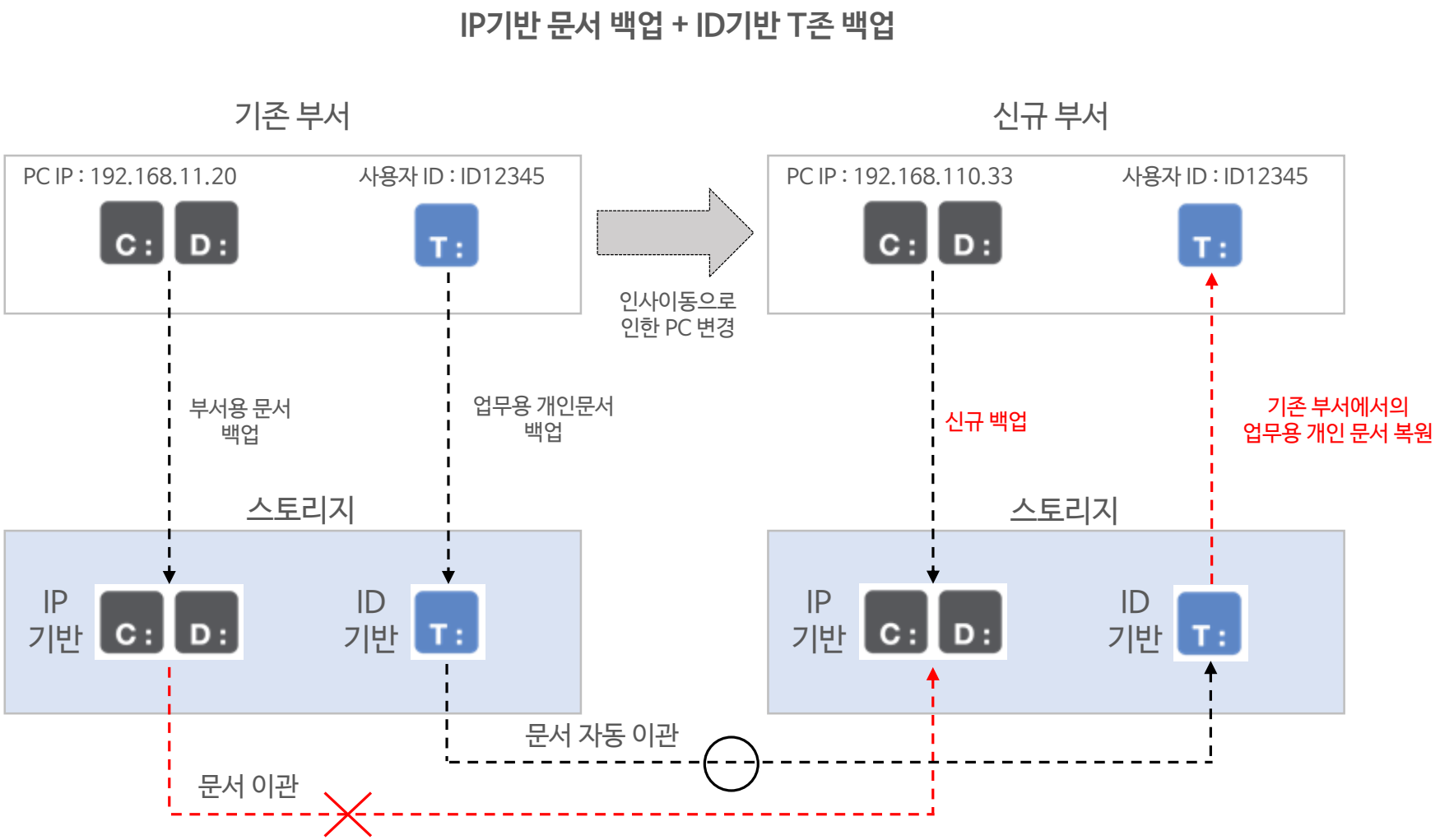


Local Drive 파일 탐지/이관 후 완전 삭제
자동 로그아웃 및 드라이브 감춤

『 특장점』

- 중앙관리 정책서버에 의해 로컬HDD에 가상보안드라이브 생성(예: T: ₩)
  : 보안 드라이브 기밀 문서 보관
- AES256 암호화 저장 보호
- 서버인증 기반의 로그인 후 사용 가능 PC 유휴시간 적용시 일정시간 후 자동 로그아웃 기능 프로세스 기반의 접근 통제
- 외부 침입자 해킹 또는 PC 분실/도난시 T-Zone 접근 차단
- 인사이동 시 기존 부서에서 사용했던 업무용 개인 문서를 신규 부서에서 그대로 사용 가능

T-Zone(Trust Zone) 기능 : 디지털 보안 영역



중앙에서 사용자를 통제하여
정책설정 및 로그관리

4. 중앙에서 사용자를 통제하여 정책설정 및 로그 관리

시스템 접근제어

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.

4. 중앙에서 사용자를 통제하여 정책설정 및 로그 관리

중앙관리매니저 정책 설정

정책 / 작업 관리 / 옵션 관리 / T-Zone 설정 / FTP 관리 / 랜섬웨어 차단

LIZARD CLOUD | 관리 | 정책 | 시스템 | 설치 | 도움말 | nPouch

작업 관리

소스 설정

- •작업명(예약어)
- •소스폴더
- •포함할 파일 확장자
- •제외할 파일 확장자

타깃 설정

- •타깃 폴더(예약어)
- •대상폴더 숨기기
- •드라이브 연결하기
- •네트워크 트래픽 제한

백업 방법

- •작업방법
- •작업주기
- •스케쥴 백업
- •백업 후 원본 삭제
- •최근 문서내역 삭제
- •드라이버 연결시 백업
- •잠긴 파일 백업
- •바이트 중복 백업 방지
- •대상파일 체크 백업
- •백업 후 시스템 종료
- •시스템 종료 시 백업
- •사용자 정의 백업
- •사용자/그룹 스케쥴 허용
- •명령문 백업

버전 관리

- •버전관리
- •사용자 버전관리 허용

고급 필터 방법

- •실시간 제외패턴
- •실시간 대기 패턴
- •반드시 포함할 패턴
- •작업명
- •소스폴더
- •포함할 파일 확장자
- •제외할 파일 확장자
- •실시간 제외패턴
- •실시간 대기 패턴
- •반드시 포함할 패턴
- •백업없이 원본완전삭제
- •제외할 폴더 패턴
- •제외할 하위 폴더
- •포함할 하위 폴더
- •파일크기 제한
- •파일 날짜제한
- •숨김,시스템파일 제외
- •확장자 없는 파일 제외
- •서명 변경파일 제외

처리 방법

- •파일 압축
- •파일 암호화(AES)
- •중복 백업방지
- •최근 날짜 덮어쓰기
- •파일명 대문자 처리
- •백업 없이 원본삭제
- •에러파일 체크
- •공유 작업

옵션 관리

Agent 기능 설정

- • 옵션명
- • 개인정보 가져오기 허용
- • 더블클릭 가져오기 활성
- • 복원허용 및 작업 통합

메뉴 설정

- •트레이 아이콘 표시
- •백업 결과 표시
- •비밀번호 변경 표시
- •백업하기 표시
- •백업 후 시스템종료 표시
- • 매니저 열기 표시
- • 최근 공지 보기 표시
- • 백업 중지 버튼 표시

시스템 접근 제어

- •지정 드라이브 숨기기
- •드라이브 접근 제어
- •USB 쓰기 금지
- •USB 접근 금지
- • 명령프롬프트 접근금지
- • 제어판 접근금지
- • REGEDIT 접근금지
- • MMC/GPEDIT 접근금지

보안 설정

- •편집/복원 암호설정
- •암호 묻지 않기
- •프로그램 제거 허용
- •관리자키 허용

부가 설정

- •로그전송날짜 제한
- •스케줄 동접수 제한
- •컴퓨터 표준시간 동기화
- •강제 Update

T-Zone 설정

트러스트존 설정

- •드라이브 지정
- •드라이브 라벨
- •드라이브 용량
- •드라이브 생성위치

보안 설정

- •폴더 바로가기
- •허용할 프로세스 사용
- •거부할 프로세스 사용

랜섬웨어 차단

랜섬웨어 차단 설정

- •감시할 파일 확장자
- •예외처리 프로세스
- •탐지 레벨
- •탐지시 묻지않고 차단

사용자 제어(중앙통제)

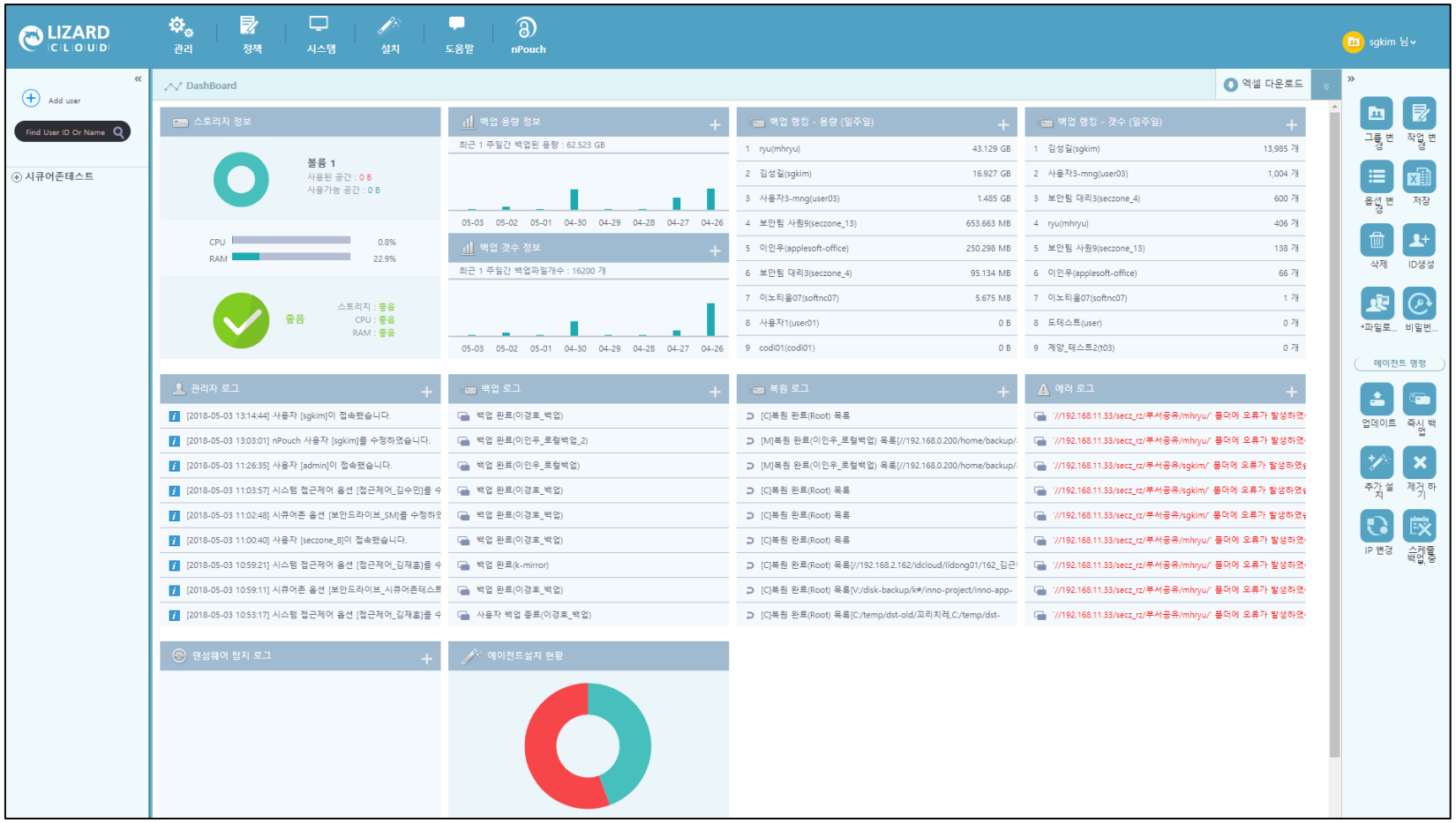
Agent 별로 사용자의 백그라운드 및 업무 영향의 최소화 한 쉐도우 백업 설정이 가능하며, 각 PC의 Agent 메뉴 활성화 여부 설정으로 각 사용자의 임의적 복원 및 악의적 사용을 제한할 수 있습니다.

『 활용 방안 』

- Agent 별로 사용자의 백그라운드 및 업무 영향의 최소화한 쉐도우(Shadow) 백업 설정
- 각 PC의 Agent 메뉴 활성화 여부 설정 : 각 사용자의 임의적 복원 및 악의적 사용 제한
- Agent 숨김 : 사용자의 업무 효율성 증대 및 거부감 최소화

4. 중앙에서 사용자를 통제하여 정책설정 및 로그 관리

중앙관리매니저(사용자 관리)



4. 중앙에서 사용자를 통제하여 정책설정 및 로그 관리

중앙관리매니저(로그 관리 - 상세 랜섬웨어 탐지 및 차단로그)

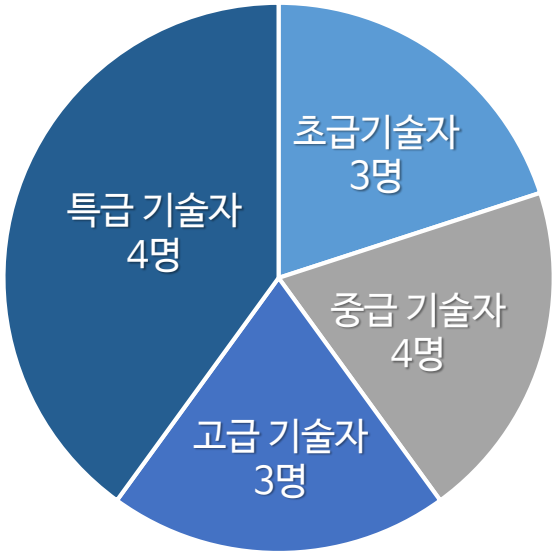
개발사 소개

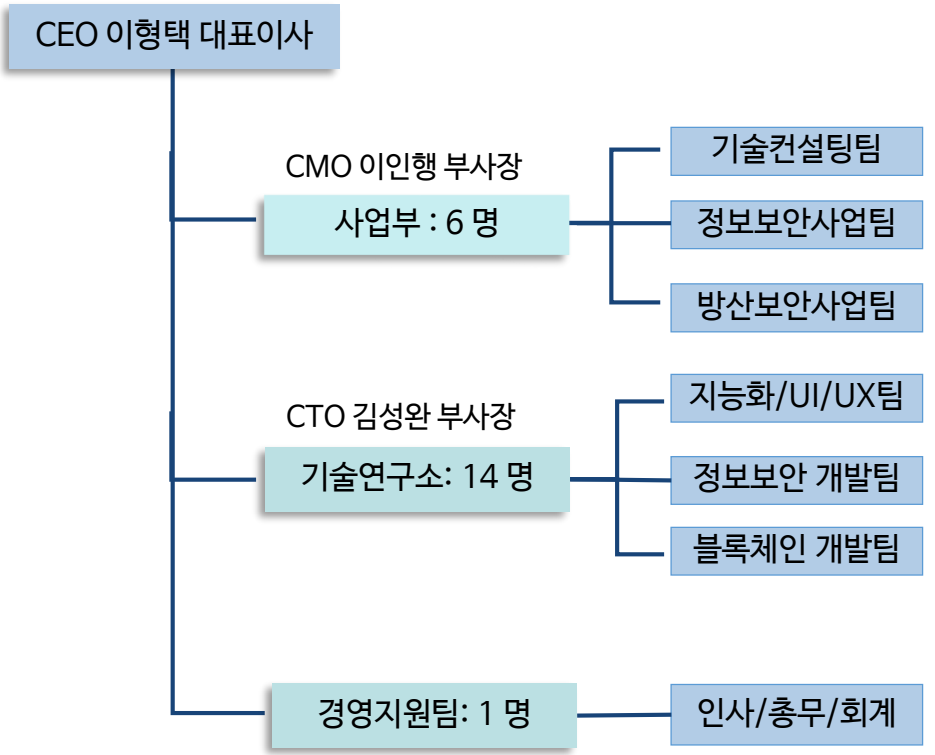
개발사 현황

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

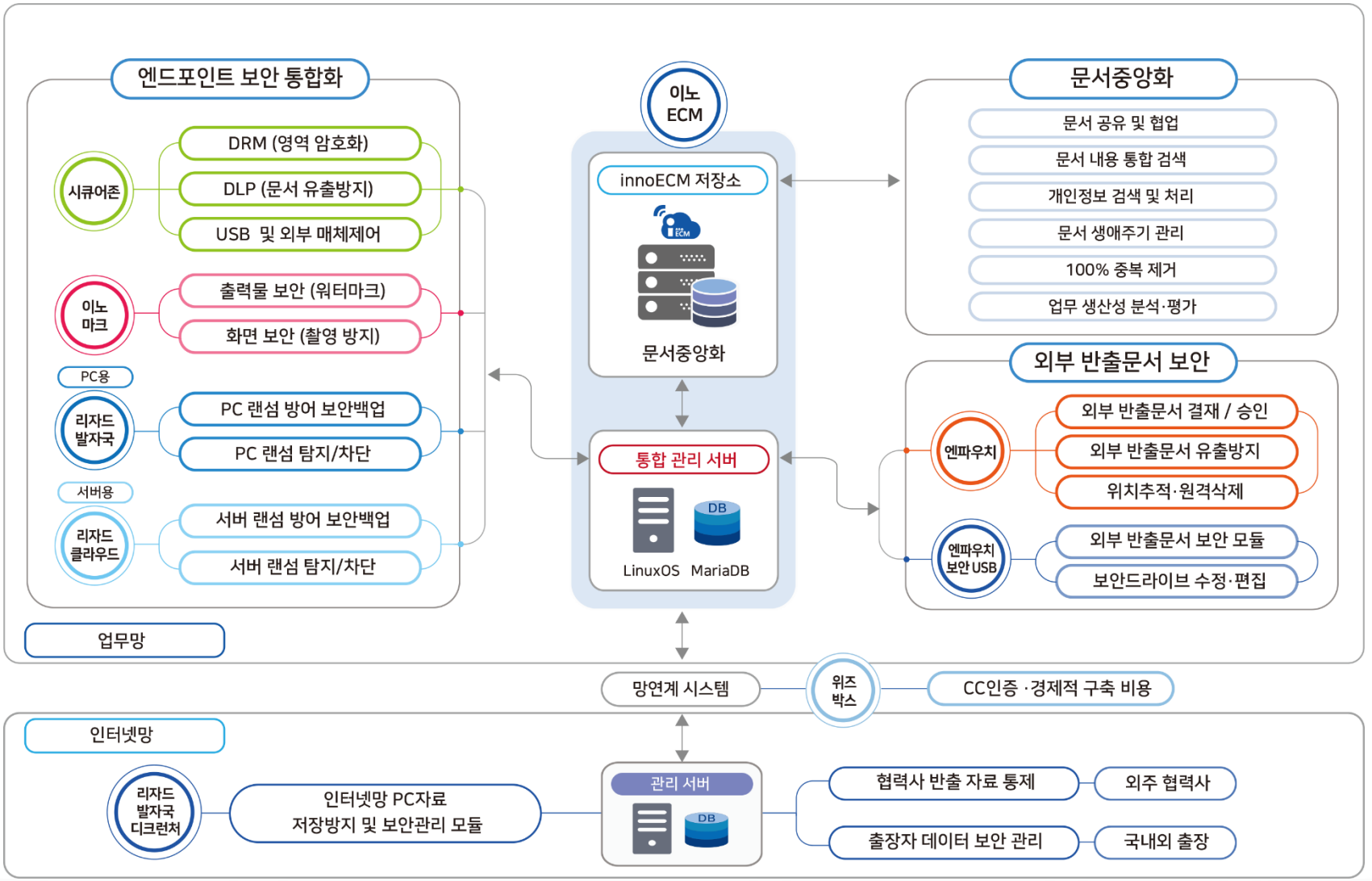
(2020년 2월 기준, 단위: 21명)





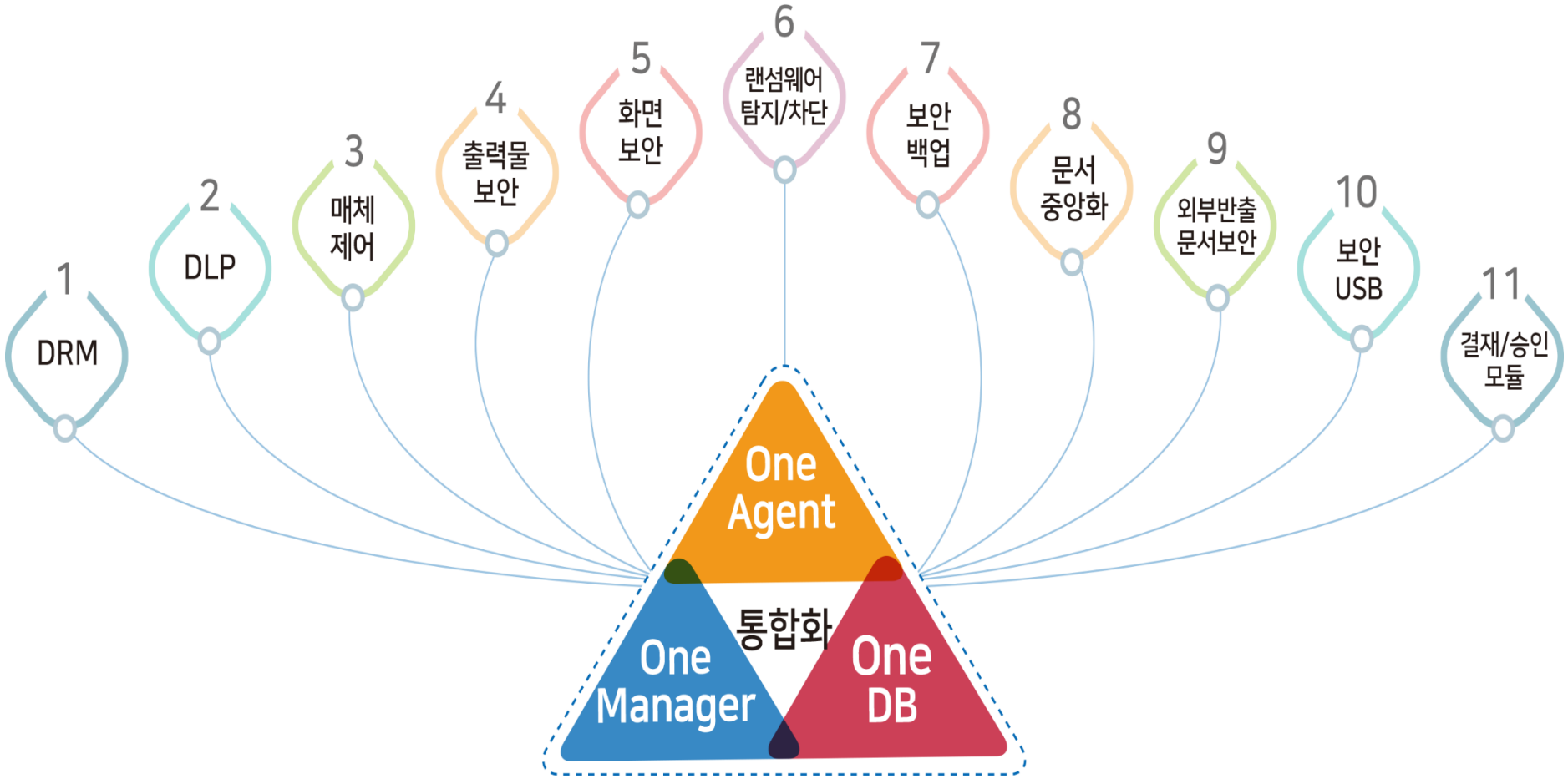
개발사 기술개발 도메인

이노티움 지능형 문서중앙화 기반 통합 문서보안 플랫폼



주요 사업 솔루션 내용

엔드포인트 보안 사용자들의 오랜 염원 "하나로 안돼?"



개발사 연혁

HISTORY

연도	내용
2019	-잊혀질 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	-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	-한화그룹 외 방산부문 데이터 보안 사업 수주 및 공급 -에스원과 방산업체 망분리사업 협약 체결 -미래부 주관 랜섬웨어 민관 대응 핫라인 구성
2016	-2016 차세대 데이터 보호 컨퍼런스 개최 -에스원과 '대국민 랜섬웨어 대응서비스 ' 협약
2015	-한국랜섬웨어침해대응센터 오픈 -ID 패스워드 보안인증 핀테크 솔루션 "아이오써티" 출시 -리자드클라우드 엔파우치 v10 GS인증 획득
2014	-발자국 조달등록 -일본 서버백업용 클라우드백업 서버 수출 -중소기업청 "수출역량강화사업자" 선정 -삼성디스플레이 DB백업사업 수주 (100 Unit)
2013	-DB백업용 클라우드백업 일본 수출 -SW산업원천기술개발사업 "클라우드 환경의 DRaaS"개발 컨소시움 참여 -엔파우치 특허등록 및 프로그램 등록
2012	-세무사협회 한길 TIS와 세무회계 데이터 온라인 백업서비스 개시 -특허청 VDI 클라우드 데이터 백업 솔루션 2,000유저 납품
2011	-일본KCS사와 클라우드백업v7 공급계약 체결 -사내 구축형 프라이빗 클라우드 "리자드 클라우드"출시
2010	-(주)이노티움 설립

특허증 및 인증서

엔파우치 특허증

특허 / 인증

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

레퍼런스

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

경상남도 GYEONGNAM | 문화체육관광부 | 특허청 KOREAN INTELLECTUAL PROPERTY OFFICE | SAMSUNG ELECTRONICS | 한화시스템 | KORAIL 한국철도공사

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

rancert 한국랜섬웨어침해대응센터

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

유비무환

有備無患

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