

업무중단과 정보유실*유출을 막아주는 AI기반의 랜섬웨어 보안과 DLP+보안USB+데이터금고



1. 랜섬웨어 보안 및 DLP 보안 피해 규모

배경과 필요성

해킹 사고 관련 개인정보 유출 안내



고객 여러분께 알려드립니다.

(주)골프존은 귀하의 개인정보 보호를 최우선 과제로 생각하고 그 보호를 위하여 최선을 다하여 왔습니다만, 유감스럽게도 최근 발생한 개인정보 유출 사고에 관하여 안내를 드리게 된 점 대단히 송구스럽게 생각합니다.

지난 2023년 11월 23일 당사의 서버에서 전문해커로 추정되는 공격자에 의한 랜섬웨어 감염으로 고객 유출되는 상황이 발생했습니다. 이에 당사는 고객 보호를 위해 정확한 사건 경위와 유출 규모 등을 규명 판단해 비정상적 접근이 확인된 이후 즉시 침입탐지 및 접근통제를 강화하는 등 보호조치를 보안전문업체를 통하여 조사를 진행하고 있습니다. 현재까지 파악된 바에 의하면, 해커가 당사가 탈취하였고, 해당 자료에 귀하의 성함과 휴대전화번호가 포함된 것으로 파악됩니다.

당사는 이번 사건을 인지한 직후 해커의 추가 공격을 차단하기 위한 보안 강화 조치들을 지체 없이 취하 신고 등 귀하께 피해가 발생하지 않도록 하기 위하여 최선의 노력을 다하고 있습니다.

금번 사고로 유출된 휴대전화번호를 악용한 불법적인 금전 요구나 보이스피싱, 스팸메시지 등의 불 주의하여 주시기를 당부드리며, 특히 안전성이 검증되지 않은 URL에 대한 접속은 삼가 주시기 바랍니다

금번 사고와
경우 전용성
드리겠습니다

귀하께 심려
보호조치를

감사합니다.

(주)골프존 드



현재 서비스 점검중입니다.

보다 나은 서비스 제공을 위해
서비스 점검 작업을 진행하고 있습니다.
이용에 불편을 드려 죄송합니다.

점검 완료시점에 별도 공지를 통해 재안내 드리겠습니다.

다크웹에 탈취 자료 공개

BLACK SUIT

Search query

Search

GOLFZON
Website

GOLFZON is a leading global culture of indoor golf simulator. Awarded four consecutive years from 2017 to 2020 as best golf simulator in Golf Digest's Editor's Choice, GOLFZON has a presence in 62 countries with 6,200 commercial sites around the world



1. 랜섬웨어 보안 및 DLP 보안 피해 규모

배경과 필요성

■ ‘랜섬웨어’ 시장 규모 (23조 시장 / 2023년)

글로벌 랜섬웨어 피해 금액
(단위: 억원)



글로벌 랜섬웨어 피해 시장 규모

국내 랜섬웨어 피해 신고 현황

출처: 한국랜섬웨어침해대응센터

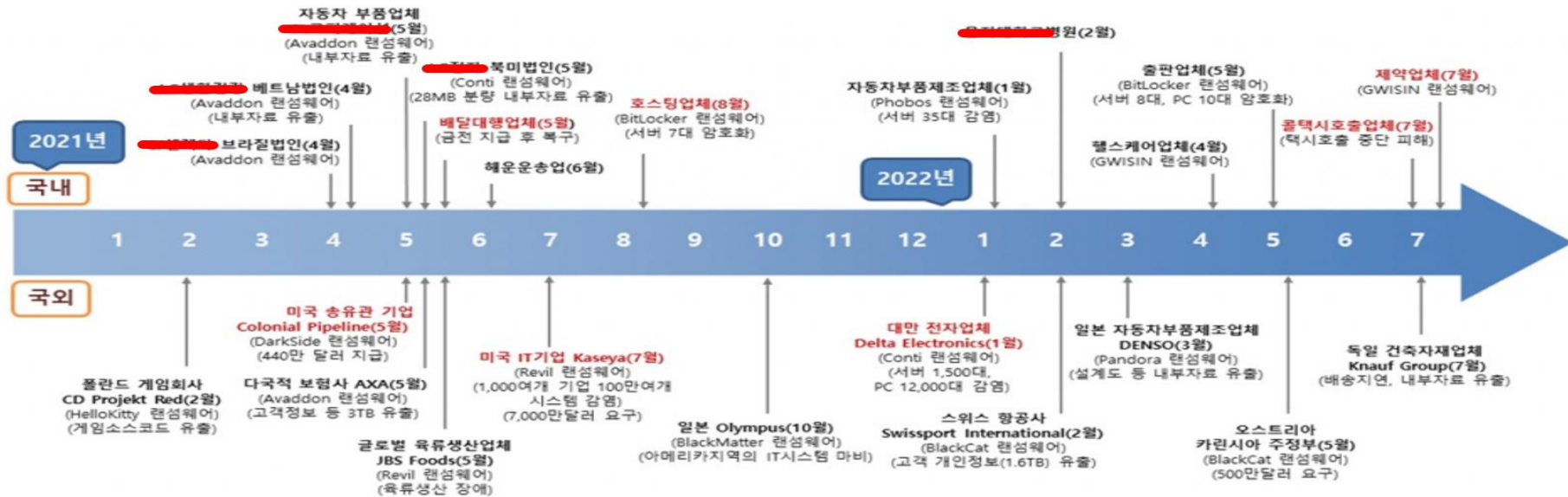


랜섬웨어 보안 + 데이터금고 필요성

- 기업/기관 대상으로 랜섬웨어로 인한 업무중단 및 데이터 유실 · 데이터 정보유출 등 피해예방목적
(정기적인 데이터 백업도 지원)
- 기업/기관의 랜섬웨어 등 사이버위협에 노출되어 있는 정보유출 및 랜섬웨어 예방 목적

1. 랜섬웨어 보안 및 DLP 보안 피해 규모

배경과 필요성



KISA-CONCERT "2021년 랜섬웨어 스페셜 리포트" 설문 조사 결과에 따르면



94.8% 랜섬웨어가 회사 비즈니스에 위협이 되고 있다.



40.27% 기업이 랜섬웨어의 피해 경험이 있다.



7.39% 공격자에게 비용 지불하였다고 응답, **43.77%** 랜섬웨어 피해가 생긴다면 공격자에게 비용 지불하거나 모르겠다.



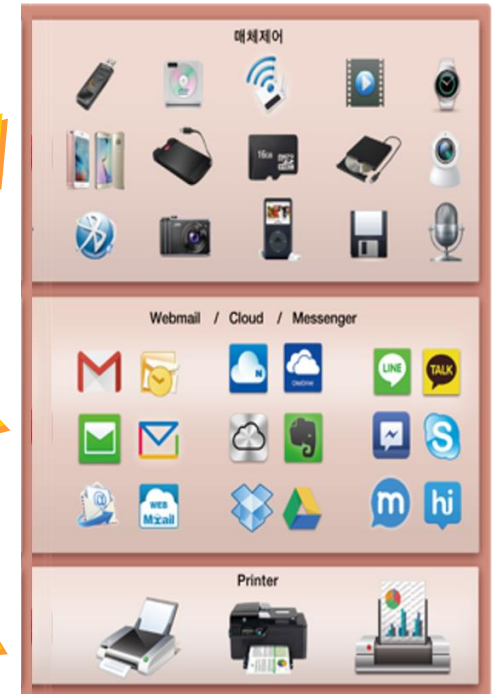
44.86% 랜섬웨어에 대한 대응을 수립하지 못하였거나 모르겠다.

1. 랜섬웨어 보안 및 DLP 보안 피해 규모

배경과 필요성



중요 정보의 유출



대표적인 3대 중요 정보 유출 경로에 보안은 최소한의 선택

1. **저장 · 통신 매체** 저장을 통한
| 휴대용 일반USB·외장HDD(SSD), CD-ROM, 스마트폰, 태더링, 무선AP, 블루투스, MTP... 등
2. **인터넷** 매체 전송을 통한
| 웹메일 / 메신저 / 클라우드 / P2P 등
3. **프린터** 인쇄를 통한
인쇄물 = 출력물
4. **안전모드, 맥·리눅스OS**를 통한

1. 랜섬웨어 보안 및 DLP 보안 피해 규모



배경과 필요성

중요정보유출 사고 사례

공개되는 범죄사실은 혐의일 뿐 확정된 사실이 아님을 유의해 주시기 바랍니다.



창원지방법검찰청

구보담당관 차장검사 김영진
전화 055-266-3311 / 팩스 055-239-4555

보 도 자 료
2014. 1. 8.(수)

자료문의 : 특수부장실
전화번호 : 055-266-3355
주책임자 : 부장검사 홍기채

제목 **카드회사 고객정보 유출 사건 중간 수사결과**

창원지검 특수부는 전산 프로그램 개발 용역 수행 과정에서 카드회사로부터 고객 인적사항정보(NF카드 약 2,500만명, KB카드 약 5,300만명, 롯데카드 약 2,600만명) 등을 불법 수집하고 그중 일부를 유출한 외부 파견직원 700과 그로부터 정보를 구입한 대출광고업자 100을 구속 기소하고, 100으로부터 정보를 구입한 대출모집인 100을 불구속 기소하였음

※불법수집된 원본 파일과 1차 복사 파일 등을 압수함으로써 외부 유출은 일단 차단된 것으로 추정됨



정보유출 카드3사, 5월 16일까지 영업정지

14일 금감원 제재심의..16일 금융위 의결 '중징계 결정'
17일 0시부터 영업정지 3개월 시작..임원 제재는 내달중 결정

"정보유출 카드3개사 집단소송 보상금 최대 1천700억"

카드사들, 카드 재발급 추가 비용부담도 200억 이상

(서울=연합뉴스) 박초롱 기자 =

입력시간 : 2014.02.03 06:19:21



CEO, 정보유출 생기면 해임까지 감수해야

[이데일리] 입력 2014-01-22 5:03 / 수정 2014-01-22 5:03

전세계 카드유출 사고 규모로 역대 3위!

이번 사고로 약 1억 4천만 명의 카드사 고객의 성명, 주민번호, 카드번호 및 유효기간, 결제계좌번호, 휴대전화, 신용등급, 타사카드 등등이 유출 되었다고 합니다. 이는 전체 경제활동 인구의 75%에 해당하는 엄청난 숫자이며, 전 세계 사고 가운데 중국의 상하이 로드웨이 D&B(2012년, 1억 5천만 건), 미국의 하틀랜드 페이먼트 시스템즈(2009년, 1억 3천만 건)에 이어 3번째 규모라고 하는군요. 그런데 정부당국이나 카드3사가 피해구제나 예방책이라고 내놓은 대책들을 보니, 영 진정성이 보이지 않네요. 대통령까지 나서 만능키 주민등록번호를 대체할 대책을 마련하라고 하는데도 '우선 소나기 피하고 보자'식인 그치는 모습이고 근본적인 문제로 지적되고 있는 주민등록번호에 대한 대책이 없습니다.

피해 시민들은 앞으로도 평생 유출된 주민번호를 사용해야 합니다. 명의도용, 부정사용 등 언제 어떻게 유출된 개인정보를 악용한 피해가 나타날지 불안해하며 살아가야 합니다.

1. 랜섬웨어 보안 및 DLP 보안 피해 규모

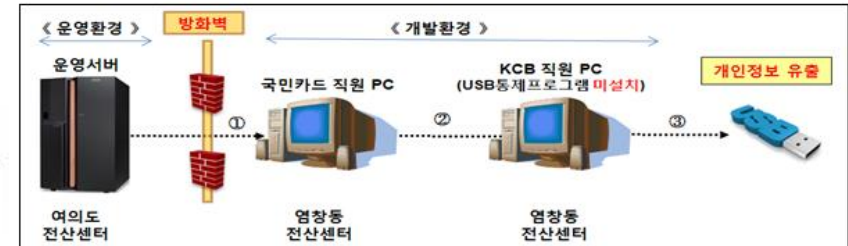
배경과 필요성

중요정보유출 사고 사례

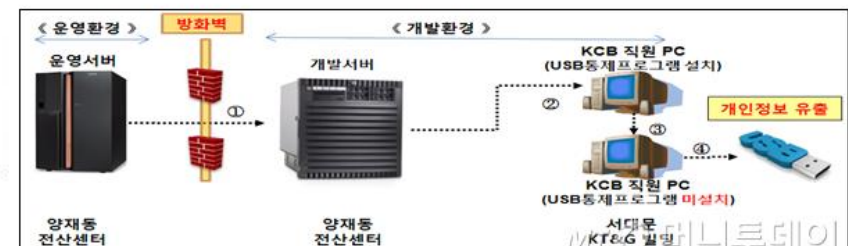
<롯데카드>



<KB국민카드>



<NH농협카드>

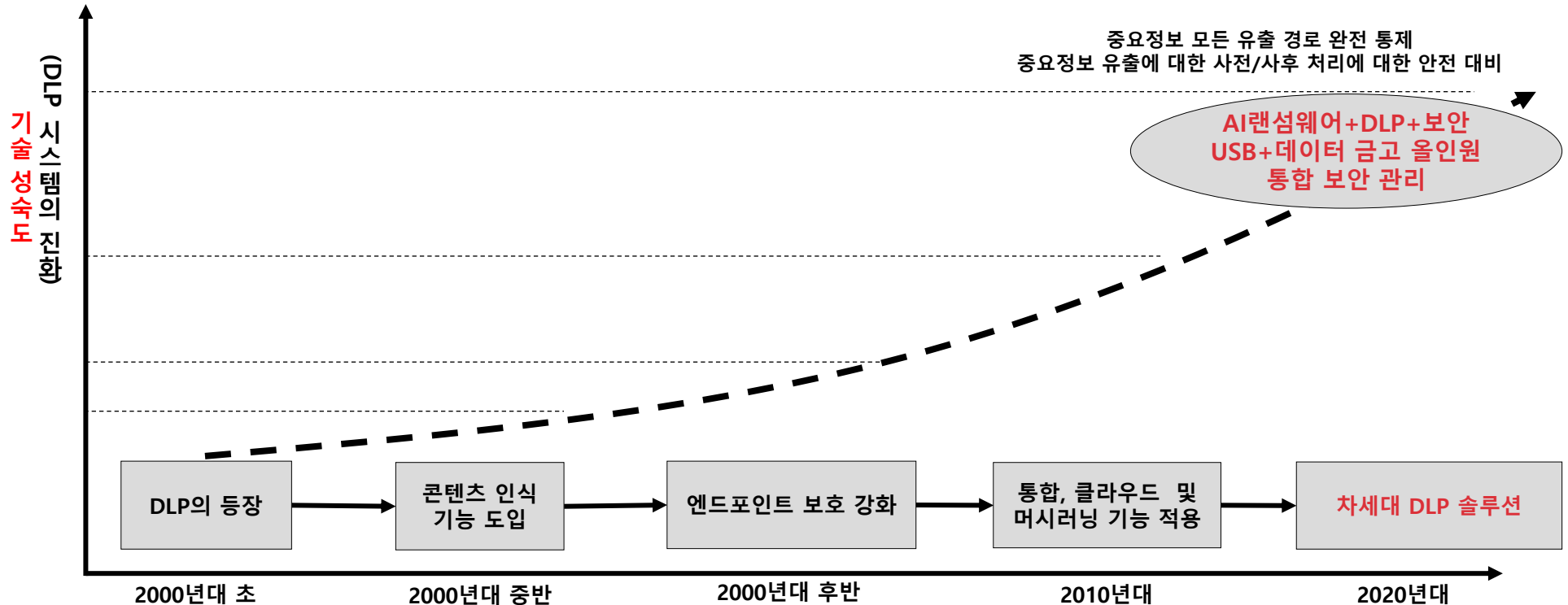


구분	KB국민카드	NH농협카드	롯데카드
미변환데이터제공시기	2013.2월 ~ 6월	2012.5월 ~ 12월	2013.11월 ~ 12월
USB복사 · 유출시기	2013.6월	2012.10월 · 12월	2013.12월
특기사항	- KB직원의 PC경유 - KCB PC 1대 이용	개발서버경유 KCP PC 2대 이용	개발서버 경유 KCB PC 2대 이용

출처: 금융감독원

2. 랜섬웨어 보안 및 DLP 보안 솔루션 동향

DLP 솔루션 동향

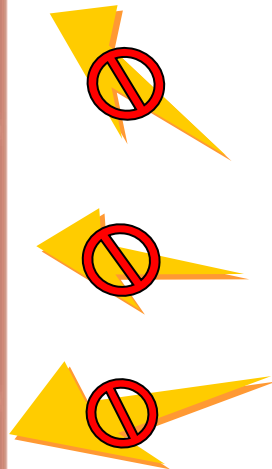


구분	DLP 등장	콘텐츠 인식 기능 도입	엔드포인트 보호 강화	통합 및 클라우드 서비스 적용 인공지능+머신러닝 적용	사전/사후 대비를 위한 올인원 통합 보안 관리
특징	<ul style="list-style-type: none"> - 네트워크 기반의 모니터링 초점 - 이메일과 같은 통신 채널 데이터 유출 감시 	<ul style="list-style-type: none"> - 콘텐츠 인식 기능 도입하여 민감 정보 식별 관리 기능 - 민감 정보에 대해 단순 패턴 매칭, 규칙 감지에서 벗어나 세밀한 데이터 보호 전략 수립 가능 	<ul style="list-style-type: none"> - 컴퓨터, 모바일 기기와 같은 엔드포인트에서의 데이터 보호 기능 강화 - 매체 제어, 출력물 관리 및 오프라인에서의 데이터 보호 기능 강화 	<ul style="list-style-type: none"> - 통합 보안 플랫폼의 일부로 발전 - IT환경 내 다양한 지점에서 데이터 보호 가능 - 머신러닝을 이용한 자동화된 데이터 보호 기능 제공 	<ul style="list-style-type: none"> - AI 랜섬웨어를 통한 데이터 변조 사전 방지 - 외부 매체, 네트워크, 출력물을 통한 데이터 유출 사전 방지 - 데이터 금고 서비스를 통한 안전 백업

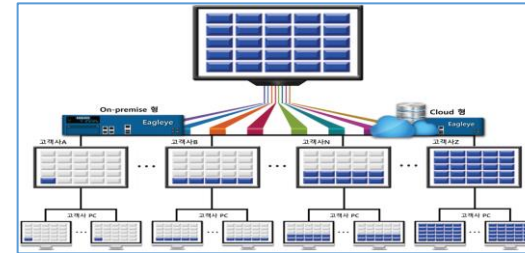
2. 랜섬웨어 보안 및 DLP 보안 솔루션 동향

차세대 올인원 통합 보안 DLP 솔루션 아키텍처

- 올인원 제품을 통한 일관된 보안정책 수립 가능!
- 일관된 인터페이스로 구성되어 있어 편의성 향상!
- 솔루션 설치부터 실 사용까지 소요 시간 최소화!



고객사별 동일 버전/형상 관리 기반 자동 업데이트 플랫폼



클라우드 네이티브 및 on-premise 형의 서비스



Plug-in 방식의 올인원 에이전트

데이터금고	개인정보보호	PC 보안
PC 백업		백신
AI랜섬웨어 보안		유해 · 비업무 차단
매체제어+보안USB	출력물 보안	정보유출방지(DLP)

Multi-OS 에이전트 지원





차세대 올인원 통합 보안 DLP 솔루션 아키텍처

Dataset 수집

■ Benign/Malware Process

- virusshare.com
- 악성코드 구매
- 프로세스 수집
- ...



학습 데이터 추출

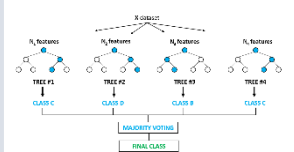
■ 프로세스 정보 추출

- raw format general information
- PE Header information
- PE Optional information
- import/export function
- PE Header section information
- String Raw feature



학습

■ Machine Learning 알고리즘으로 학습데이터 학습

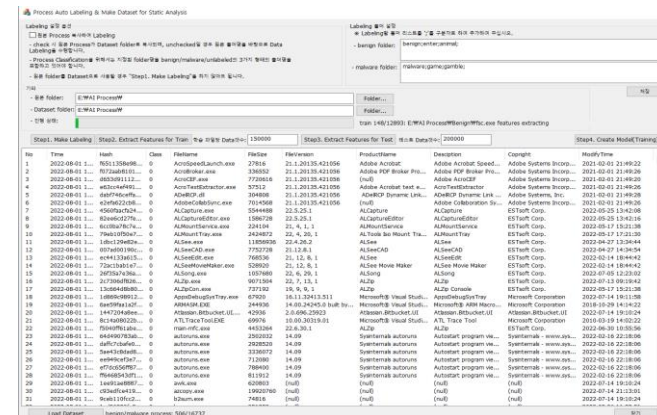


모델 테스트 및 배포

■ 모델 테스트 및 배포

[illegible]

Json type의 학습 데이터



학습 모델 생성기 메인 화면

3. 올인원 통합 보안

SaferZone V10 제품개요

- 1 **매체제어 솔루션**
| 저장 · 통신매체 정보유출방지
- 2 **인터넷 정보유출 제어**
| 인터넷(웹메일 · 메신저 · 클라우드) 정보유출
- 3 **출력물 보안**
| 워터마킹 및 프린트 제어
- 4 **중요정보 · 개인정보 보안**
| 중요정보보호 및 개인정보보호법 규제 준수
- 5 **문서보안 · PC보안 · PC백업**
| 중요 및 개인정보 문서 자동 암호화 및 보안/백업
- 6 **보안 USB**
| 국정원 인증 보안USB · 보안SSD · 보안HDD
- 7 **랜섬웨어 보안**
| AI 기반의 차세대 랜섬웨어 방화벽
- 8 **백신 보안**
| 글로벌 SDK 백신 탑재 (탐지율 최고)
- 9 **위험 · 악성 · 유해 · 비업무 사이트 차단**
| 위험 · 악성 및 유해 · 비업무 웹사이트 제어
- 10 **데이터금고 (더 안전한 보안 백업 · 복원)**
| 물리적 분리된 안전한 보안 백업 금고시스템



문서암호화(DRM)
기업의 중요한 정보가 담긴 문서 이미지 도면을 암호화



통합백업
PC생성된 모든데이터를 자동백업으로 내부문서 보호



유해사이트차단
악성코드와 유해한사이트를 차단하고, 웹 정보유출방지



랜섬웨어방지
랜섬웨어에 의한 PC내 주요 파일/폴더 암호화 변조 실시간 탐지 및 차단



개인정보보호
PC내 개인정보 검색/암호화/파기 개인정보 유출 시 차단 및 경보




정보유출방지
USB, 외장하드 CD등 매체 복사 시 외부 유출 차단

국내 **최초, 최강**
커널 기반 매체제어, 보안USB, DLP 기술

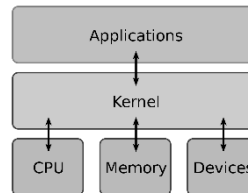
구분	세이퍼존	A사	C사	해외 G사
Windows (7, 8, 10, 11)	○	○	○	○
Mac (10.x and more)	○	X	○	○
Linux (2.6.x and more)	○	X	X	○
국산OS(구름)	○	X	X	X
국산OS(티맥스)	○	X	X	X
국산OS(하모니카)	○	X	X	X

3. 올인원 통합 보안

 통합 보안 솔루션 도입 고려사항(안전모드)

//
안전모드에서는 매체제어가
동작하지 않습니다.

커널 기반 매체제어 솔루션이
필요합니다.



안전모드에서 매체제어 무용지물

- | 안전모드에서 데이터 유출 가능성 존재
- | 신규저장매체에 대한 신속한 지원 안됨



다양한
신규 저장매체에 대한 통제 필요

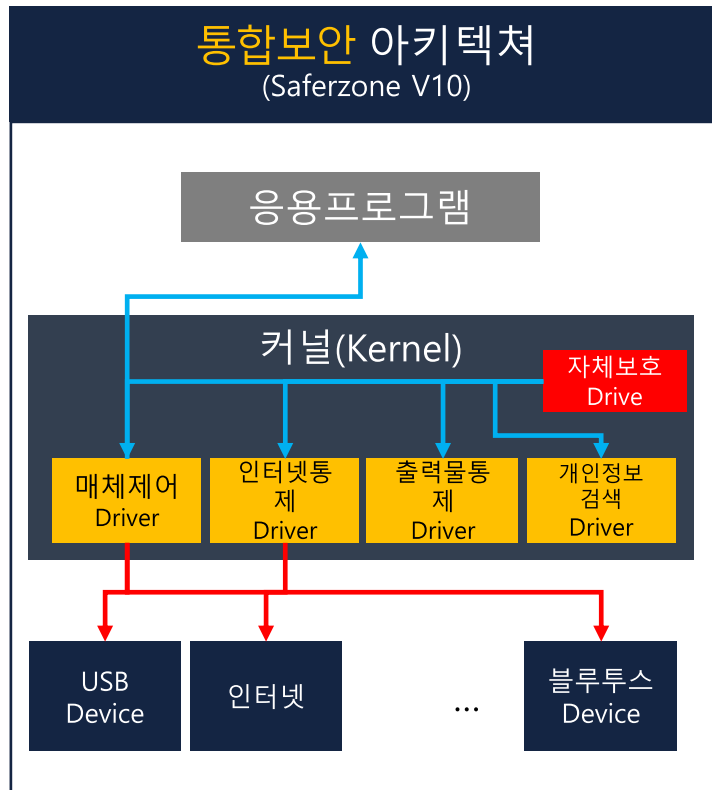


매체제어 도입 시 고려사항

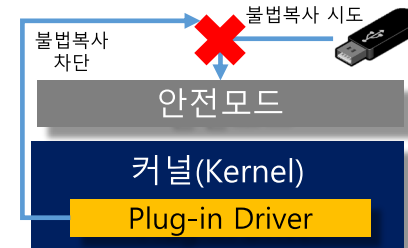
- ✔ 모든 형태의 매체제어 지원
- ✔ 안전모드 매체제어 기능

3. 올인원 통합 보안

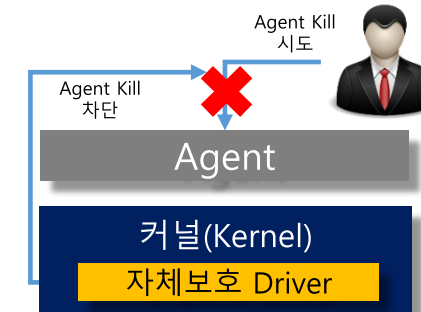
SaferZone V10 통합 보안 솔루션 기술적인 측면



이
상
적
인
통
제
방
식



OS커널에 제어 드라이버를 이식,
안전모드에서도 모든 제어



보안SW 도입 무력화 100% 원천 차단
커널 단 자체 보호 엔진

! 커널 기반
통제 필요

안전모드, 자체보호로 솔루션 보안 레벨업

3. 올인원 통합 보안



통합 보안 솔루션 도입 고려사항(자체보호)

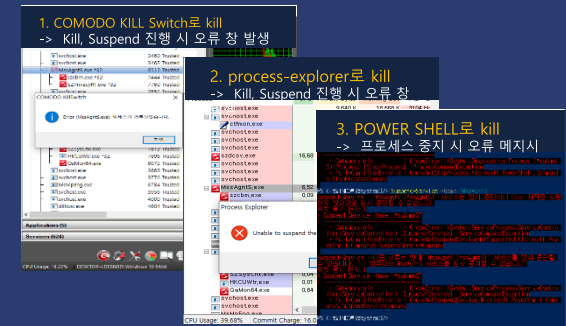
//
자체보호 무력화 취약점으로
보안이 약화되고 있습니다.

자체보호 무력화 취약점 해결책이
선행되어야 합니다. //

국정원 권고 3대 취약점

- | COMODO KILL Switch로 프로세스 종료
- | Shell script 를 통한 명령어로 프로세스 종료
- | CMD 를 통한 명령어로 프로세스 종료

국정원 권고,
'보안SW 자체보호 무력화 취약점'



매체제어 도입 시 고려사항

- ☑ Agent 강제 종료 취약점 해결 여부
- ☑ 안전모드에서도 자체보호 가능 여부

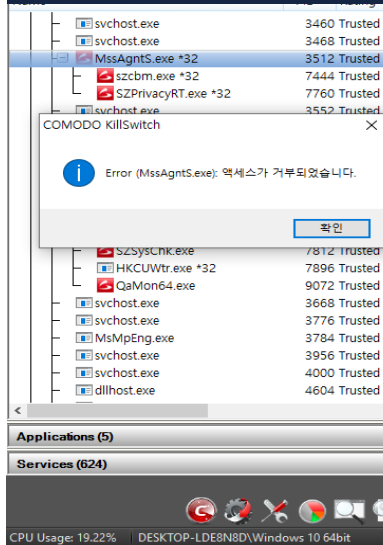
3. 올인원 통합 보안



통합 보안 솔루션 기술적인 측면

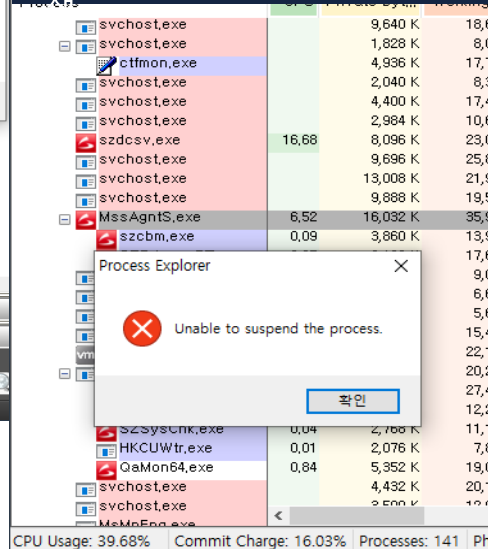
1. COMODO KILL Switch로 kill

-> Kill, Suspend 진행 시 오류 창 발생



2. process-explorer로 kill

-> Kill, Suspend 진행 시 오류 창 발

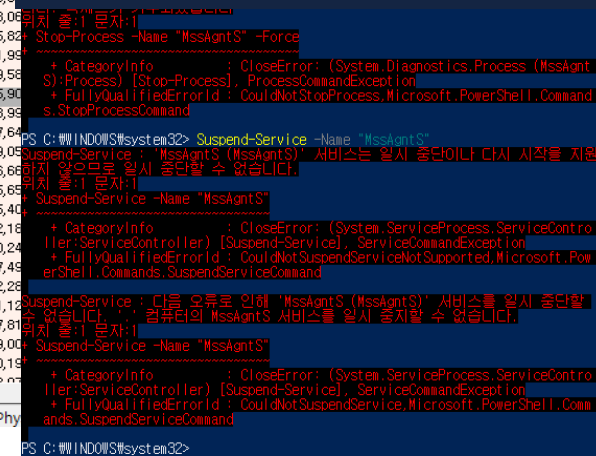


SaferZone V10,

3대 취약점 해결 완료

3. POWER SHELL로 kill

-> 프로세스 중지 시 오류 메시지




국가사이버안전센터 발표된 보안취약점

취약점 해결 필요

3대 취약점 해결로, 완벽한 데이터 유출방지 구현

3. 올인원 통합 보안

 통합 보안 솔루션 도입 고려사항(다양한OS)

//

Mac, Linux 사용자에게 대한
정보보호방안이 없습니다.

멀티OS에 대한 지원이
필요합니다.

//

타OS 사용자 정보보호방안 부재

I MacOS, Linux 사용 증가로 정보보호방안 부재



통합
보안시스템

보안 관리자
(정책관리
및 모니터링)

Windows OS

Mac OS

Linux

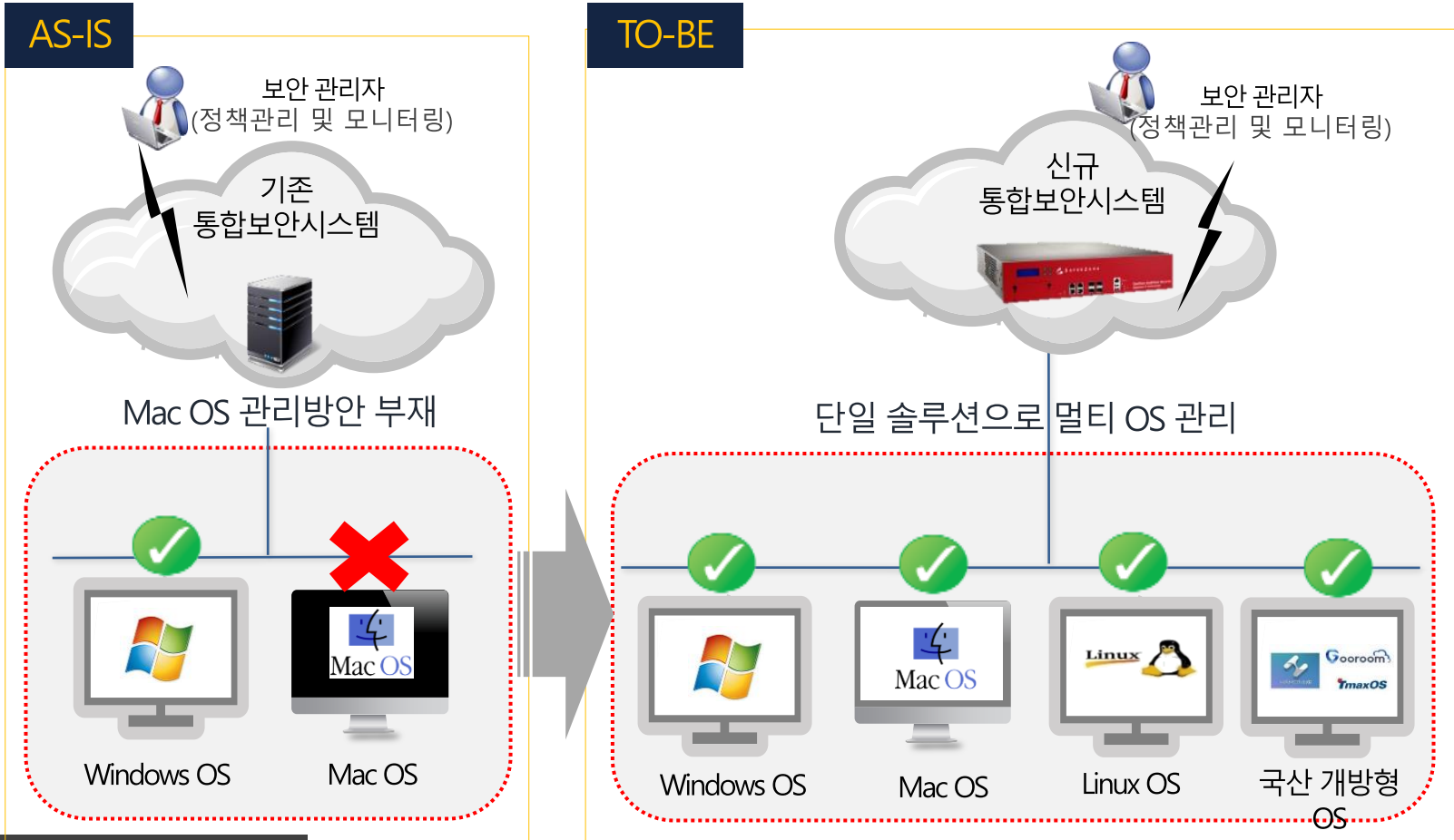
국산 개방형 OS

도입 시 고려사항

- ☑ 효율적인 운영을 위한 단일 솔루션 지원 확인
- ☑ IT 환경 변화에 따른 다양한 OS 지원 여부

3. 올인원 통합 보안

통합 보안 솔루션 기술적인 측면



멀티OS 지원 필요

국내 사용되는 모든 OS를 지원, **보안사각지대 제거**

3. 올인원 통합 보안

통합 보안 솔루션 도입 고려사항(인터넷통제)

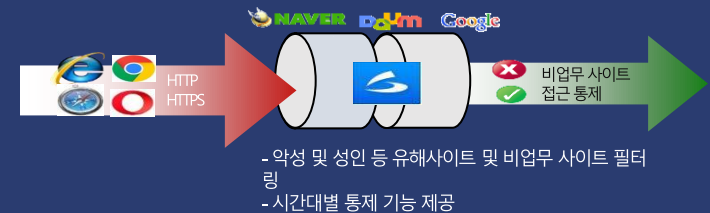
// 인터넷을 통한
비업무사이트 접속 및
파일유출이 발생합니다.

인터넷 접속 및 파일전송 통제
개선이 시급합니다. //

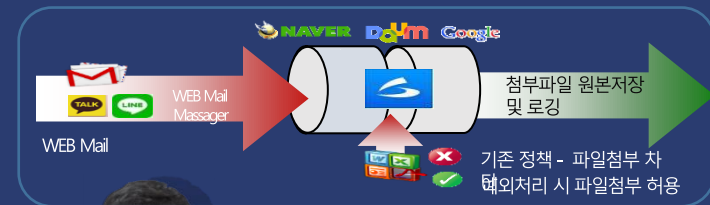
인터넷을 통한 정보유출

- | HTTP뿐만 아니라 HTTPS 웹사이트 통제 필요
- | 다양한 어플리케이션을 통한 파일전송 제어 필요

웹사이트 통제



파일전송 통제



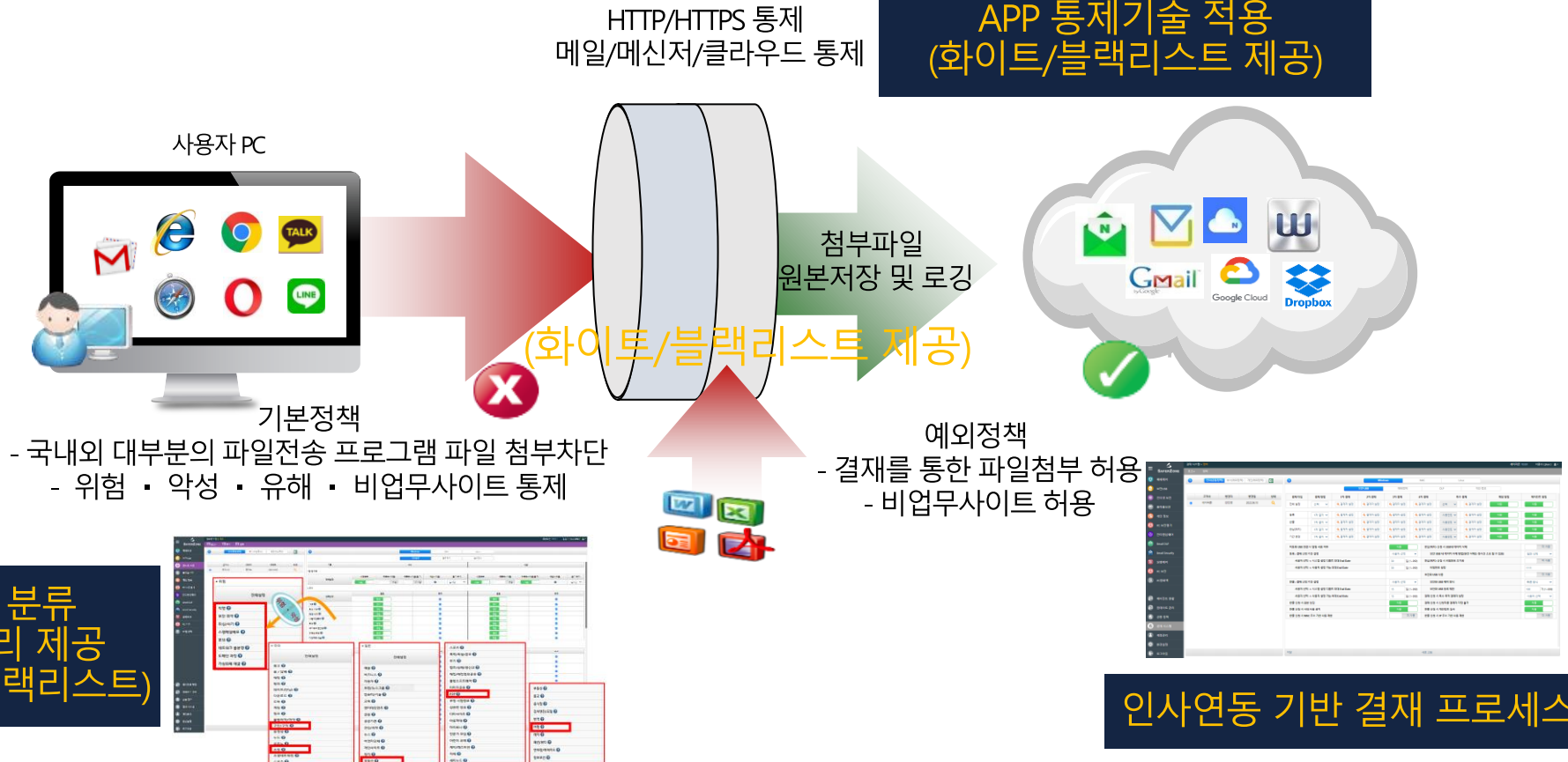
도입 시 고려사항

- ☑ 다양한 경로를 통한 파일첨부 차단 기능
- ☑ HTTP/HTTPS 차단 기능

3. 올인원 통합 보안




통합 보안 솔루션 기술적인 측면



다양한 파일첨부
통제 필요

인터넷을 통한 파일첨부차단 및 비업무사이트 통제

3. 올인원 통합 보안


 통합 보안 솔루션 도입 고려사항(자료보호)

//
자료유출과 함께 자료보호에
대한 방안이 필요합니다.

랜섬웨어 방어, 백신, 백업이
추가되어야 합니다. //

자료보호(유실) 방안 부재

- | 랜섬웨어 대응 방안은?
- | 자료 유실에 대한 방안은?

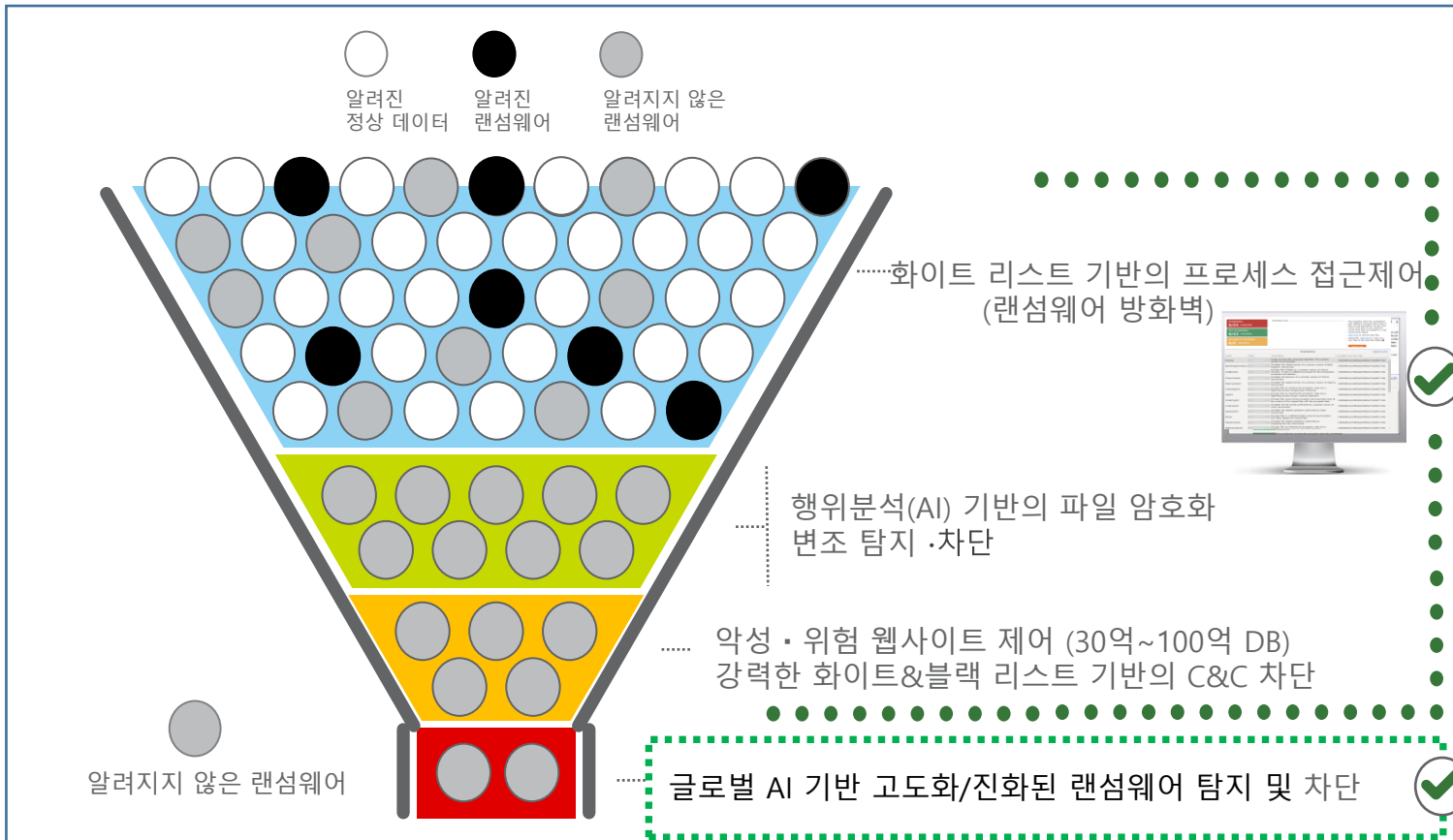


도입 시 고려사항

- ☑ 자료유출 이외 자료보호방안 여부
- ☑ 내부자료 백업 기능 여부

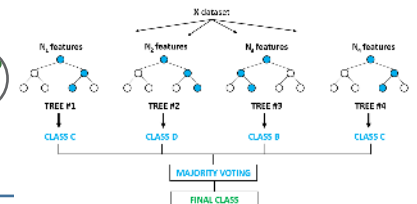
3. 올인원 통합 보안

통합 보안 솔루션 기술적인 측면



Real-Time Protection

안티 랜섬웨어 엔진	0n
AI 랜섬보안 엔진	0n
안티 바이러스 엔진	0n
AI 보안백업 엔진	0n
웹 방화벽 엔진	0n
PC 방화벽 엔진	0n
정보유출 엔진	0n
자체 보호 엔진	0n



자료 보호
필요성

추가 기능으로, 랜섬웨어, 악성코드 방어

3. 올인원 통합 보안



통합 보안 솔루션 기술적인 측면

PC 영역 : 1차 백업 (보험1)

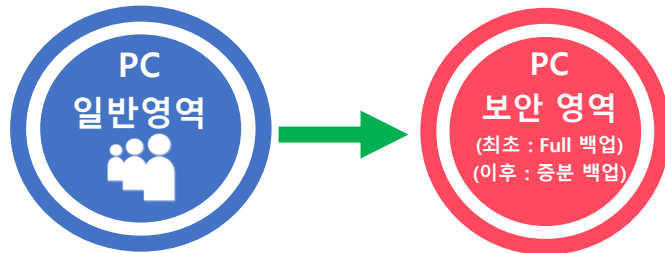


1단계 백업 보안 : PC 방화벽 (In/Outbound)

2단계 백업 보안 : 랜섬웨어 보안 + 백신

3단계 백업 보안 : 보안영역 백업

4단계 백업 인증 · 식별 : 로그인

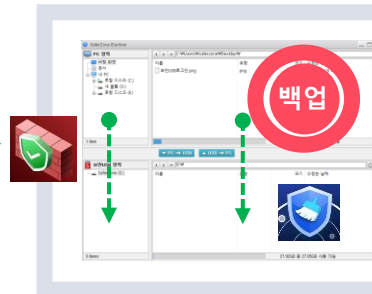


실시간 데이터 백업
(Full + 증분만 백업)

Multi-OS Platform (PC, Server 다양한 운영체제 지원)



5단계 백업 보안 : 암호화 통신



NAS 영역 : 2차 백업 (보험2)

6단계 백업 보안 : NAS 방화벽

7단계 백업 보안 : NAS 백신

다양한 보안 NAS



2-Bay



4-Bay



8~12 Bay

자료 보호
필요성

자료 보호를 위한 , 스마트 백업으로 자료보호까지

3. 올인원 통합 보안



통합 보안 솔루션 도입 고려사항(충돌, 리소스관리)

//

Agent간 충돌, 리소스문제가
심화되고 있습니다.

근본적인 해결책이
필요합니다.

//

보안제품별 Agent 설치

- | 서로 다른 제조사의 Agent 다수 설치
- | 제조사간 Agent 충돌문제 책임회피
- | 사용자PC의 리소스 문제 발생



도입 시 고려사항

- ☑ Agent 통합이 가능한지 여부
- ☑ Agent간 충돌은 없는지 여부

3. 올인원 통합 보안

통합 보안 솔루션 기술적인 측면



Plug-in 방식의 올인원 에이전트

데이터금고	개인정보보호	PC 보안
PC 백업		백신
AI기반 랜섬웨어 보안		유해 · 비업무 차단
매체제어+보안USB		정보유출방지(DLP)
출력물 보안		

Multi-OS 에이전트 지원



! 통합 Agent 필요

보안Agent 통합으로, **충돌 및 리소스 문제 해결**



감사합니다.



1577 - 3110

Sales@SaferZone.Com