랜섬웨어 대응 예방을 위한

화이트 시큐리티 플랫폼 W.S.P

White Security Platform

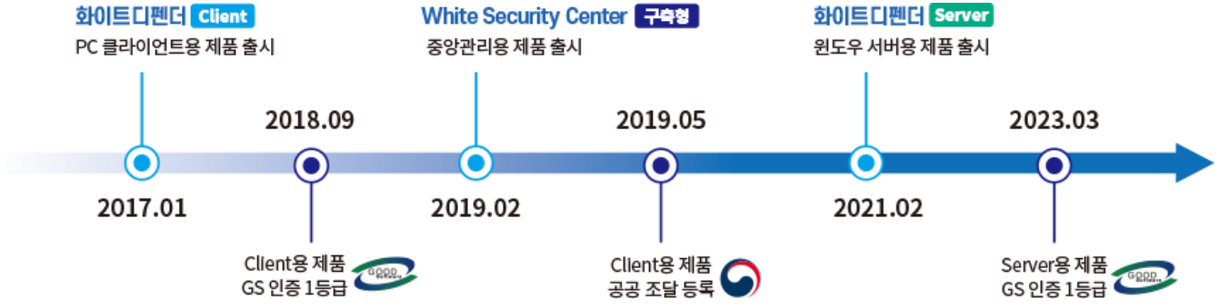
㈜ 에브리존 | 화이트 시큐리티 플랫폼

1. 개요

랜섬웨어 차단 화이트디펜더-보안 SW 개발, 20년!

보안 SW 개발에만 주력해온 ㈜에브리존은 꾸준한
연구와 개발 능력으로 다양한 제품을 출시해 왔습니다.
앞으로도 제품을 지속적으로 개선하여, 더 좋은 제품을 공급해
나가겠습니다.

2. 화이트디펜더 제품 연혁



3. 회사 연혁

2023	2023.05	"화이트디펜더 서버" 조달 등록 조달청
	2022.02	관리자용 중앙 관리 제품 "화이트 시큐리티 클라우드 플랫폼" 출시
	2021.11	롯데 렌탈, 롯데알미늄, 롯데 건설, 롯데유통사업본부 납품
	2021.08	국회도서관 납품 (서울, 부산)
2021	2021.02	"화이트디펜더" 서버 출시
2019	2020.01	"화이트디펜더" 납품 mbc / 롯데 계열사
	2019.08	터보백신 리눅스서버 출시
	2019.07	"화이트 디펜더" 조달 총판 계약 – 아이티로그 조달청
	2019.05	조달청 등록 완료 - 안티랜섬웨어 "화이트 디펜더"
	2019.02	관리자용 중앙관리 제품 "화이트시큐리티센터" 출시
	2018.07	GS인증 1등급 획득! – 안티랜섬웨어 "화이트 디펜더"
2018	2018.07	PC용 제품 – " 화이트디펜더" 출시
2017	2017.11	한국소프트웨어단체연합회 주관 '제5회 소프트웨어 산업보호 대상'
	2017.04	수상
2007	2017.03	롯데정보통신 "화이트 디펜더" 업무협약 체결
2000	2007.01	SW 자산 관리 솔루션 Audit-MAN(오딧맨) 출시(SPC SAM-DB 적용)
1999	1999.09	통합 보안 터보백신 인터넷시큐리티 출시
1994	1994.04	㈜에브리존 설립
		국내 최초 윈도우 OS 용 터보백신 개발

Table of contens

White Security Platform

I. 클라우드 보안 – 화이트 시큐리티 플랫폼

i. 화이트 시큐리티 플랫폼 소개
ii. 랜섬웨어 정책 설정
iii. 랜섬웨어 로그(탐지, 검역소, 일반, 모니터링)
iv. 보안 보고서

White Security Cloud Platform

White Security
Cloud Platform

통합 보안 관리 Platform에 오신 것을 환영합니다.

가입 및 사용 문의 안내

- 자주 하는 질문
- 문의 하기

Login

회사 아이디

아이디

비밀번호

아이디 찾기 | 비밀번호 찾기

로그인

또는

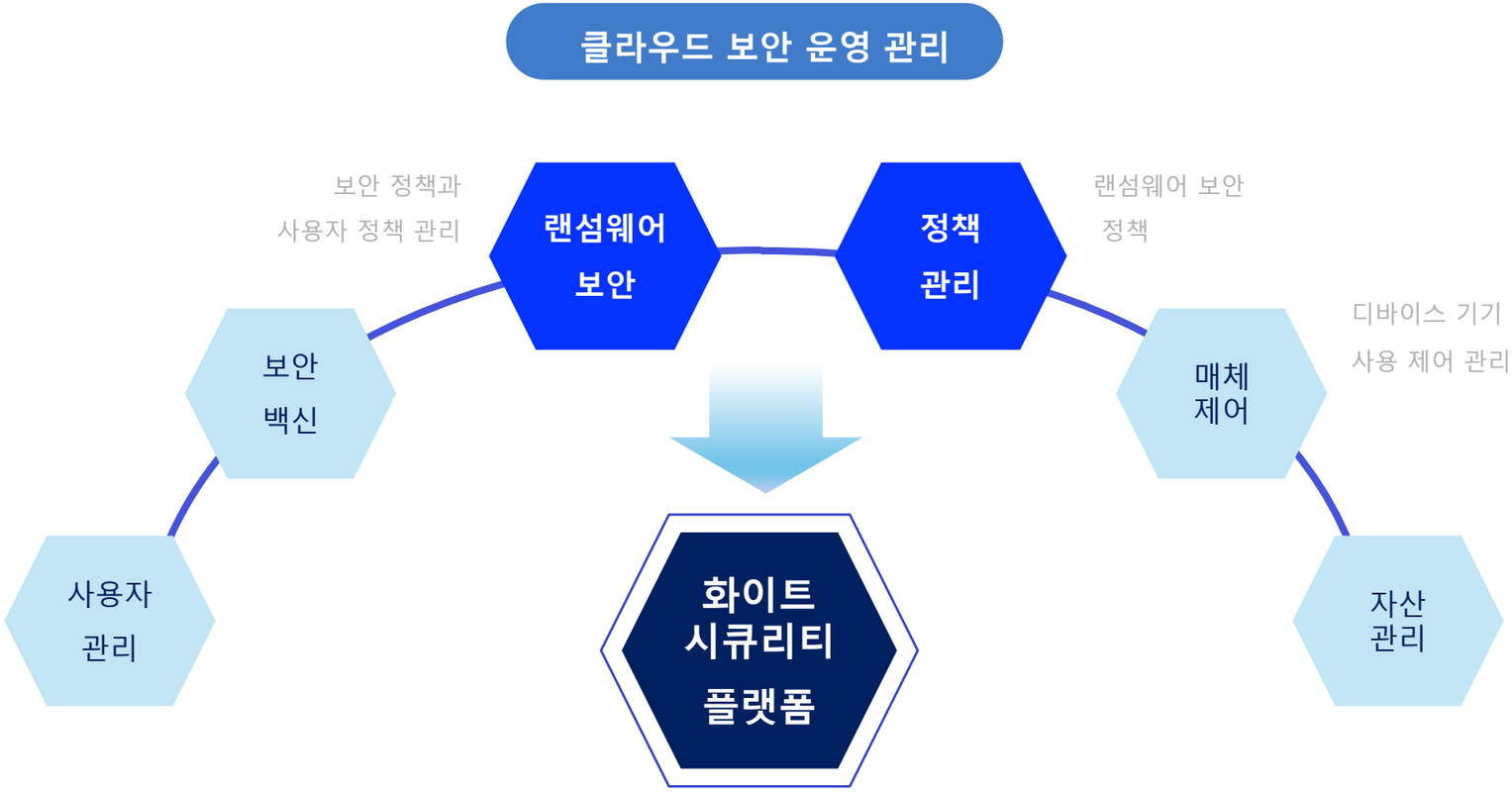
체험판 신청 하기

전체 관리자 로그인은 기업 회원 가입이 필요합니다.

White Security Platform

클라우드 보안 이렇게 관리 가능 합니다.

운영에 필요한 수많은 보안 서비스, 따로 관리 할 필요 없이 화이트 시큐리티 플랫폼에서 대시보드로 관리하세요.
보안기능을 쉽게 적용 하고 보고서로 받아볼 수 있습니다.

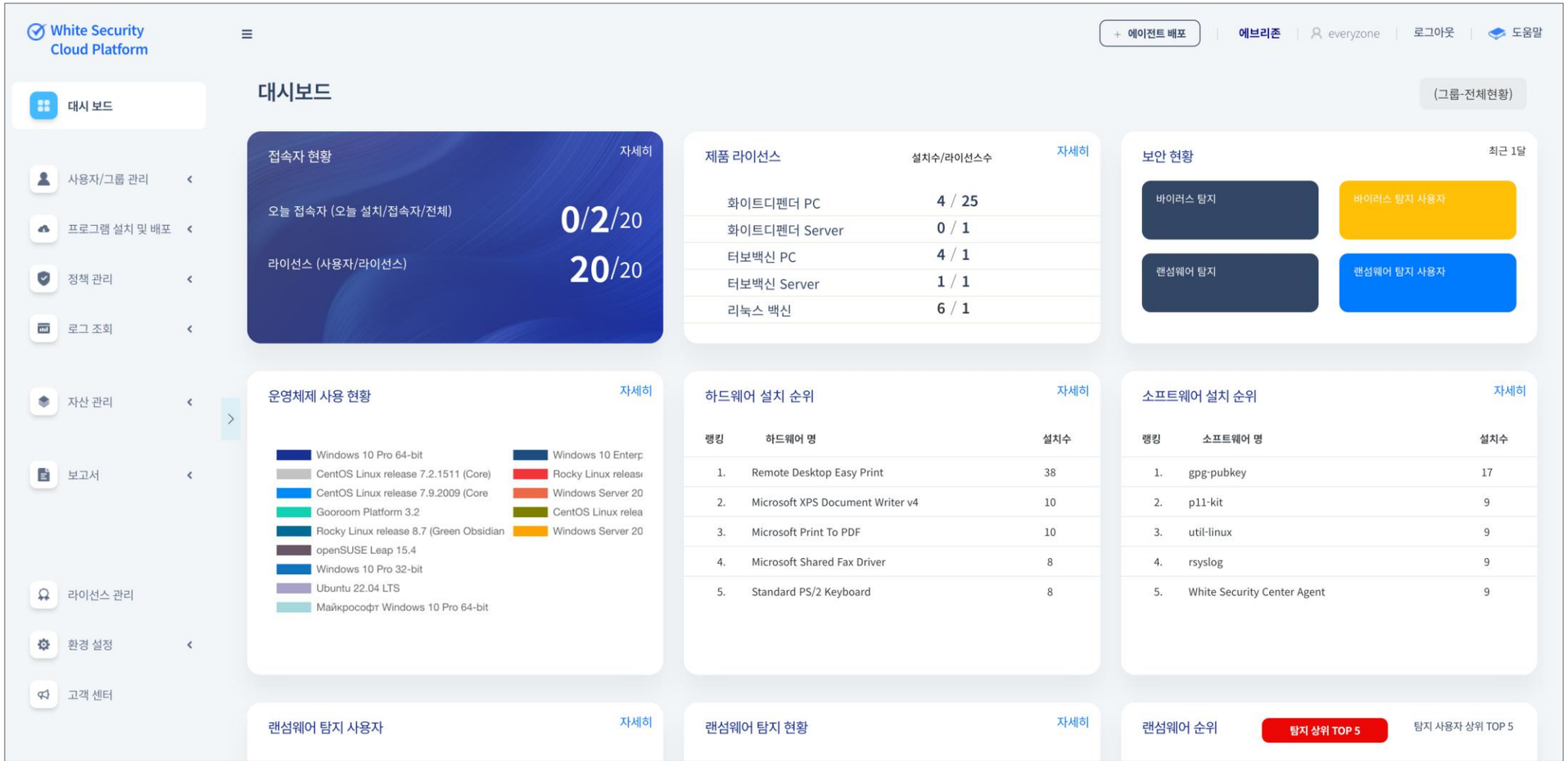


보안 관리와 현황 파악을 한곳에서 집중 관리

White Security Platform

화이트 시큐리티 플랫폼 W.S.P

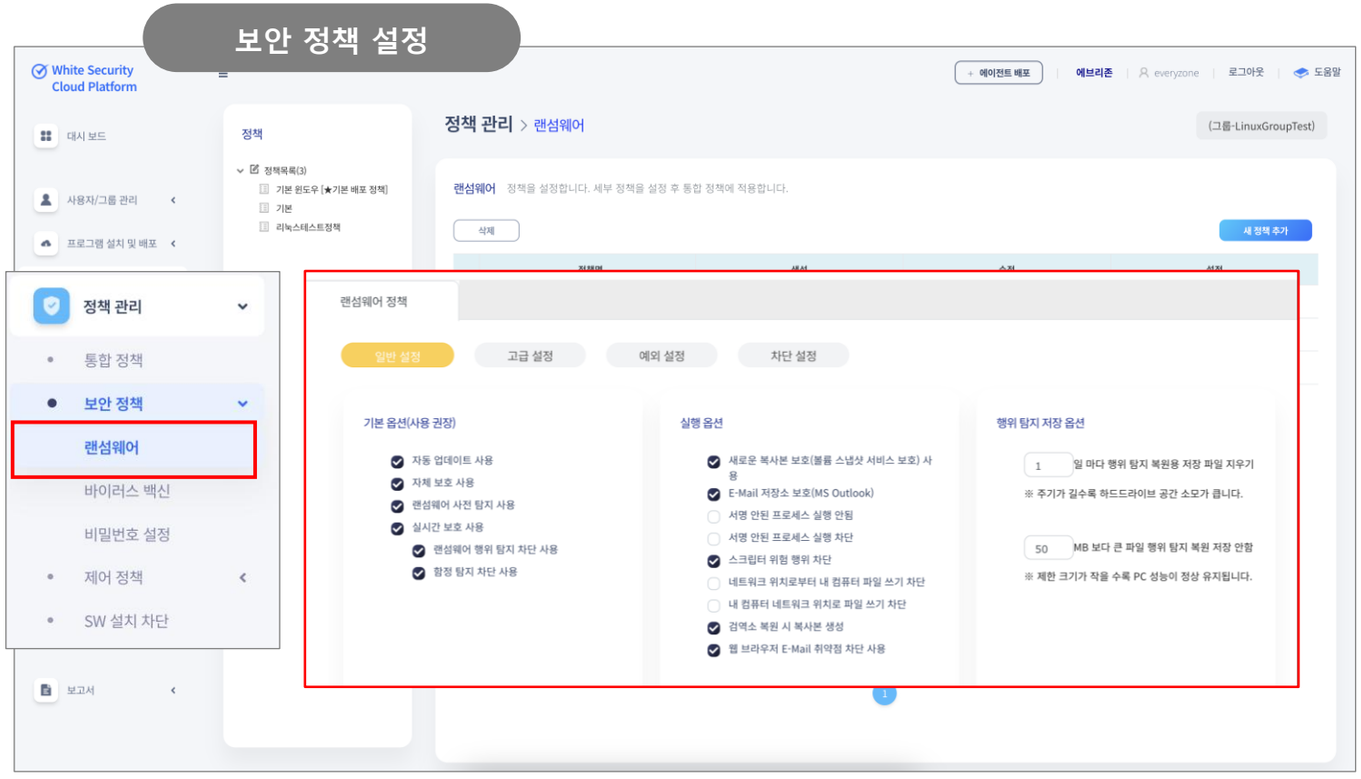
다양한 웹 브라우저 로그인을 통해 언제 어디서든 빠르게 접속하여 기업 보안 관리가 가능합니다.



White Security Platform

랜섬웨어 보안 정책

랜섬웨어 정책에 필요한 일반적인 설정과 고급 설정까지 단계별로 적용 가능합니다.
통합정책, 보안정책, 제어정책, SW설치 차단 등 다양한 정책들을 제공하여 기업의 보안이 강화될 수 있도록 지원합니다.



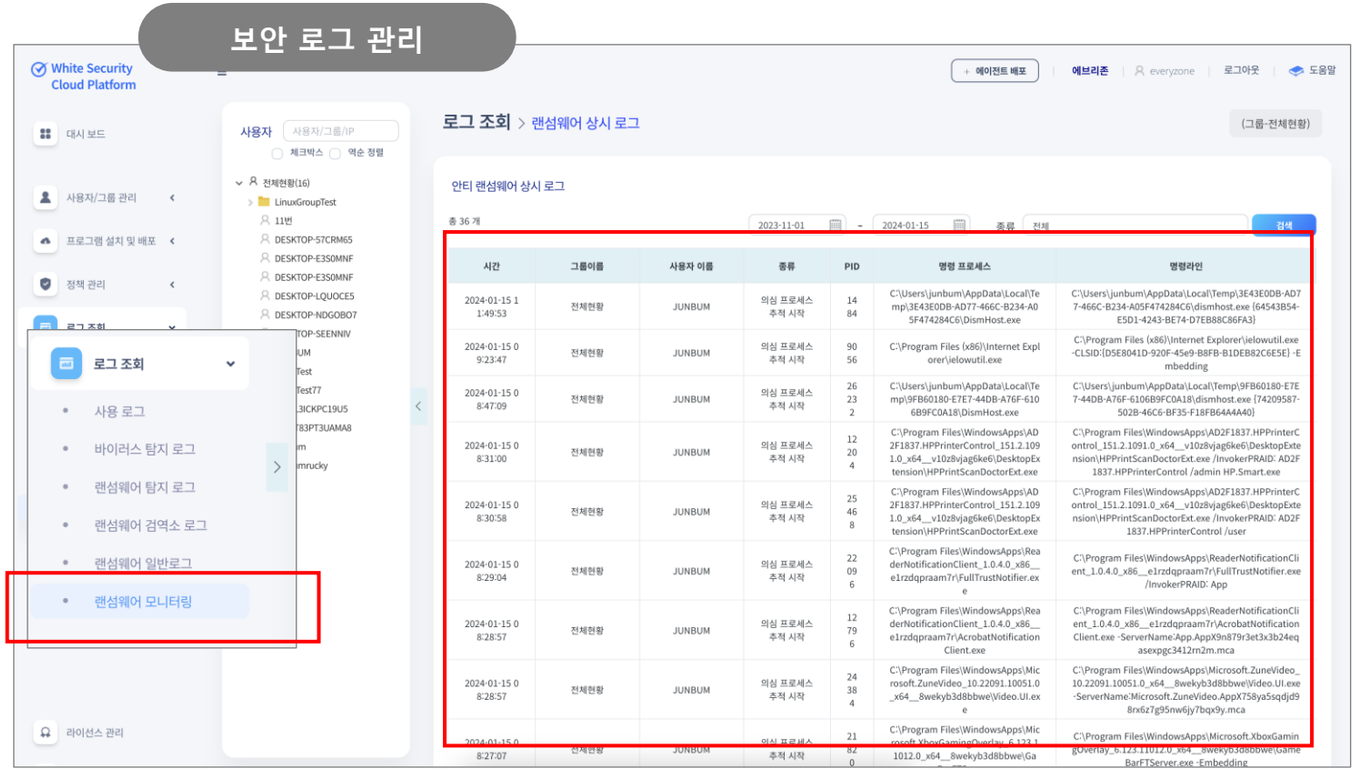
랜섬웨어 정책 관리

- **일반 설정 :** 기본 옵션(권장), 실행 옵션, 행위 탐지 저장 옵션
- **고급 설정 :** 랜섬웨어 안전지대
- **예외 설정 :** 랜섬웨어 예외 리스트 관리
- **일반 설정 :** 랜섬웨어 차단 프로세스 추가

White Security Platform

랜섬웨어 위협/탐지/차단 로그 관리

보안에 필요한 필수 로그를 확인 하고, 랜섬웨어 관련 보안 로그를 상세하게 확인 할 수 있어 보안 정책에 필요한 내용을 확인하고 적용할 수 있습니다.



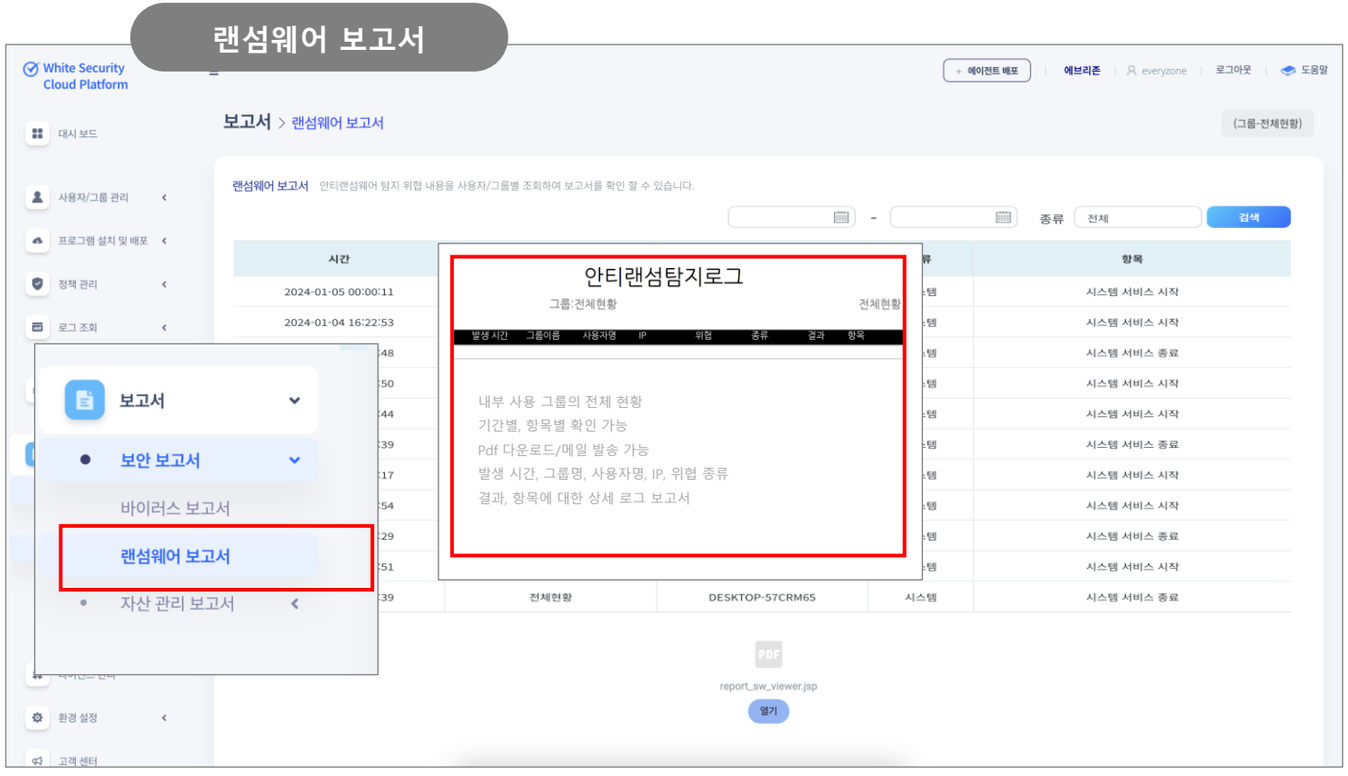
보안 로그 관리

- 랜섬웨어 탐지 로그
- 랜섬웨어 검역소 로그
- 랜섬웨어 일반 로그
- 랜섬웨어 상시 모니터링

White Security Platform

랜섬웨어 탐지 보고서

기업 내부 사용 그룹의 랜섬웨어 관련 탐지 로그 내용을 보고서로 확인 해 볼 수 있습니다.



랜섬웨어 보고서

- 내부 사용 그룹의 전체 현황
- 기간별, 항목별 확인 가능
- Pdf 다운로드/메일 발송 가능
- 발생 시간, 그룹명, 사용자명, IP, 위협 종류 결과, 항목에 대한 상세 로그 보고서

화이트디펜더 제품 Line Up

WhiteDefender

II. 화이트디펜더

i. 랜섬웨어 대응 기능

ii. 화이트디펜더 소개

White Security Platform

화이트디펜더 사용자

2017년 제품 출시 후 랜섬웨어 보안을 위해 화이트디펜더를 사용하고 있는
사용 유저 수입니다. 사이버보안이 이슈인 만큼 더 많은 사용자가 늘어날 것 입니다.

WhiteDefender

랜섬웨어 보안의 독보적인 기술- 선두업체로
발돋움 하고 있습니다.

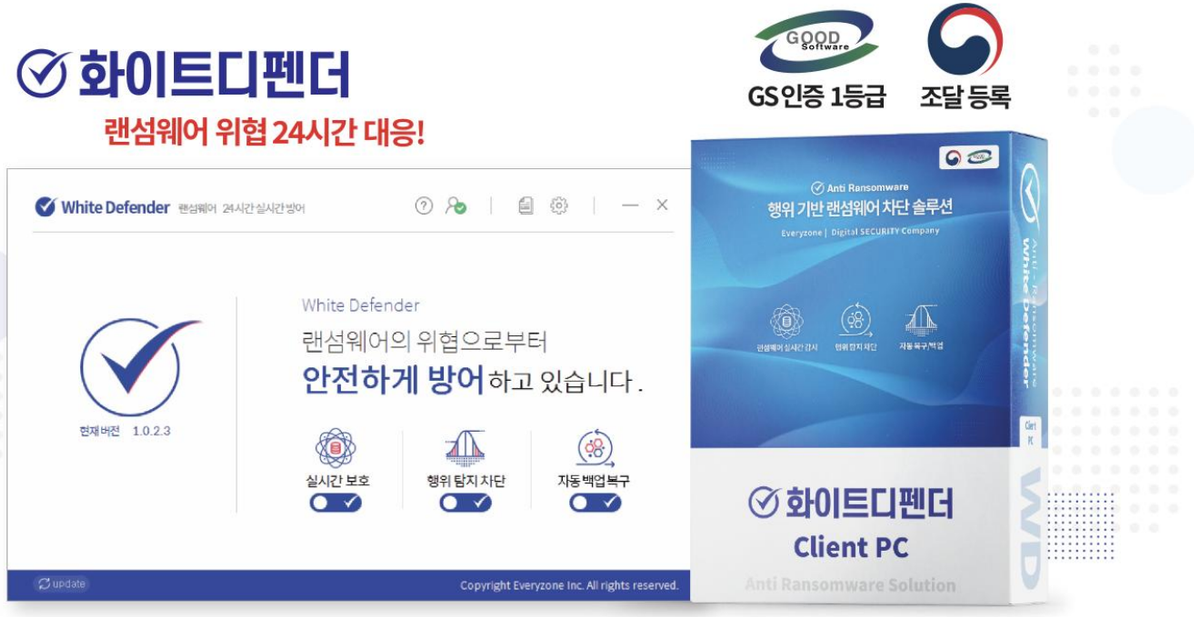
사용기업	라이브 사용자	랜섬웨어 차단
1,000+	52만명+	10만 +

화이트디펜더란?

100% 행위 기반 랜섬웨어 차단 대응 예방 솔루션입니다.

화이트디펜더는 **알려지지 않은 랜섬웨어**를 **원천적으로 차단**하고 안전하게 보호합니다.

엔드포인트 시스템에서 랜섬웨어 관련 의심 행위가 발생하는 경우, 랜섬웨어를 탐지- 차단하며, 랜섬웨어가 암호화를 진행할 경우, **순간적**으로 **원본 파일을 백업**하고, **차단 후 백업된 파일을 복구**하는 행위를 통해 데이터를 안전하게 보호합니다.



White Security Platform

랜섬웨어 대응(핵심 동작 원리)

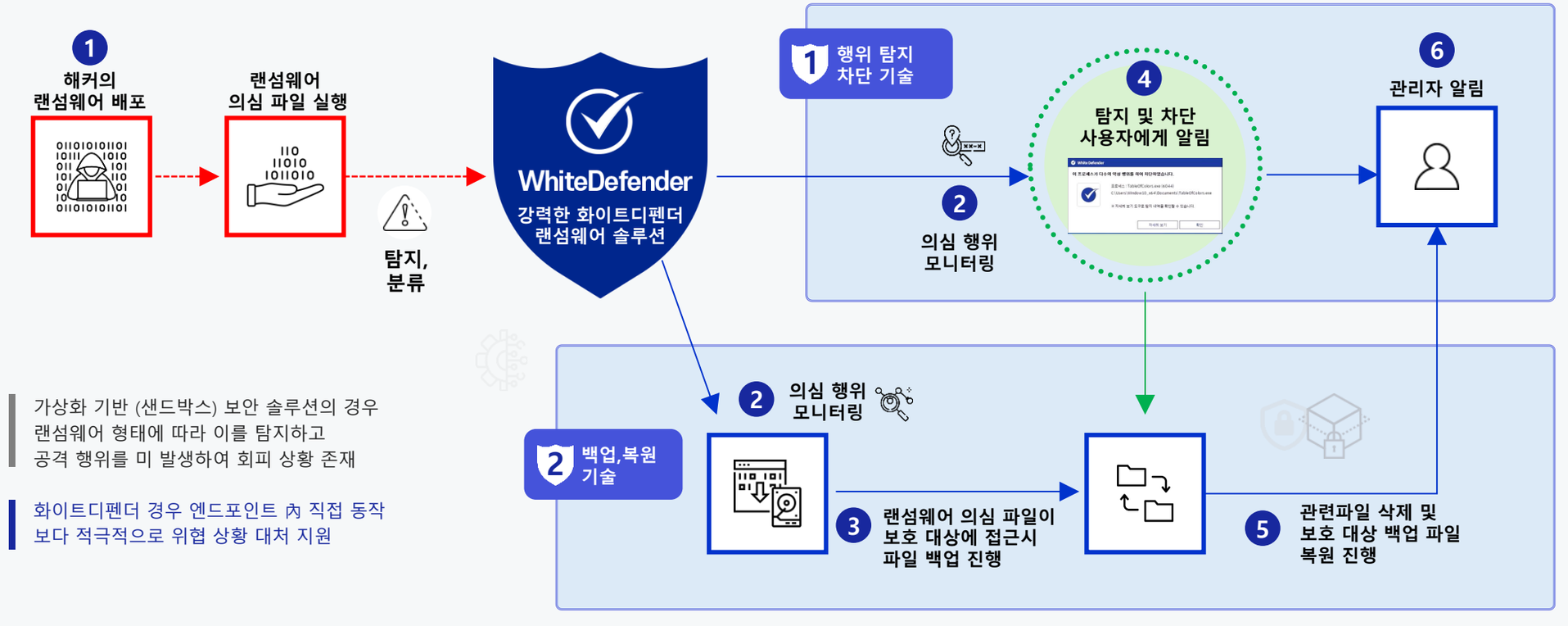
화이트디펜더는 25년 이상의 터보백신 개발, 연구 경험을 기반으로 에브리존에서 출시된 제품입니다.
랜섬웨어에 대한 적극적 대응을 목표로 **독자 기술로 개발한 3단계 (프로세스 레벨 > 서비스 레벨 > 커널 레벨) 방어 체계를 통해**
랜섬웨어를 실시간으로 모니터링 하면서 차단하고, 알려지지 않은 랜섬웨어를 방어할 수 있는 **차세대 안티랜섬웨어 솔루션**입니다.

White Security Platform

100% 행위 기반 랜섬웨어 차단 탐지 및 복원 기술!

주요 탐지 및 차단/복원을 지원하는 동작 과정에서 복합적으로 정보를 주고 받으며 위협 상황에 대한 적극적인 대응 기술입니다.

화이트디펜더의 행위 탐지 차단 기술



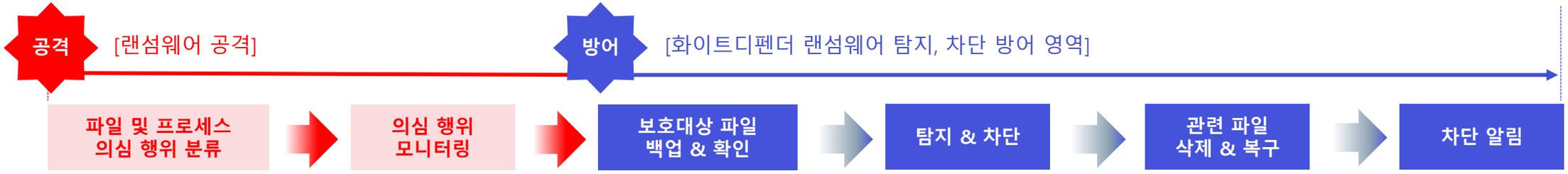
가상화 기반 (샌드박스) 보안 솔루션의 경우
랜섬웨어 형태에 따라 이를 탐지하고
공격 행위를 미 발생하여 회피 상황 존재

화이트디펜더 경우 엔드포인트 內 직접 동작
보다 적극적으로 위협 상황 대처 지원

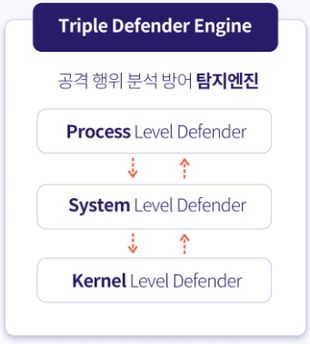
White Security Platform

화이트디펜더 - 랜섬웨어 대응 프로세스

WhiteDefender 제품군이 설치되어 있는 엔드포인트시스템에서 랜섬웨어 관련 의심 행위가 발생하는 경우, **탐지를 진행하는 TD 엔진과 보호 대상 파일에 대하여 순간 백업 및 복원을 담당하는 WR 엔진이 상호 동작**하여 랜섬웨어 대응 탐지 및 차단을 수행합니다.



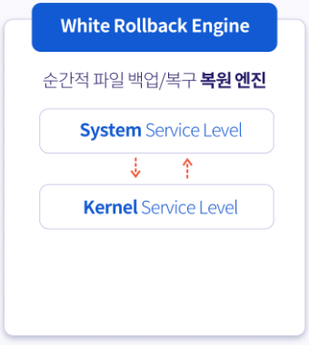
TD 엔진 (Triple Defender Engine)



1 행위 탐지 차단 기술

- 랜섬웨어의 다양한 공격 행위를 실시간으로 모니터링 하고 분석하여 방어하는 탐지 엔진
- 엔드포인트 시스템 상에서 실행된 프로세스 및 기존 프로세스에 인젝션(injection)된 다른 프로세스와 Script 형태로 실행되는 형태들이 의심 행위로 분류가 되면 해당 의심 행위들을 모니터링하면서 화이트디펜더 서비스와 드라이버가 상호 동작하며 분석 및 판단을 진행함
- 최종 탐지 및 차단이 진행되면 랜섬웨어 의심 행위로 삭제되어야 할 파일은 삭제 후 복원소로 이동시킴

WR 엔진 (White Rollback Engine)



2 백업, 복원 기술

- 랜섬웨어 공격 발생 시 의심 행위 관련 프로세스들이 접근한보호 대상 파일들을 순간적으로 백업하고 탐지 & 차단 과정이 진행되면서 순차적으로 복구하는 복원 엔진
- 랜섬웨어 의심행위에 대한 수집 정보를 **독자 구현 핵심 엔진**에서 분석 및 복원 진행함

White Security Platform

화이트디펜더, 탐지 및 차단/복원 동작 예시

랜섬웨어 의심 파일이 실행되는 주요 감염 상황별 WhiteDefender의 주요 탐지 및 차단 / 복원 동작 과정에 대한 사항입니다.

공격 상황별 랜섬웨어 감염

피싱 이메일 첨부파일 실행

피싱 이메일 내 첨부 파일 또는 링크를 통해
악의적인 파일을 사용자가 실행함

손상된 웹사이트 통한 공격

손상된 웹사이트 방문 및 불법 자료 검색
다운로드 등이 취약점을 통해 실행 감염됨

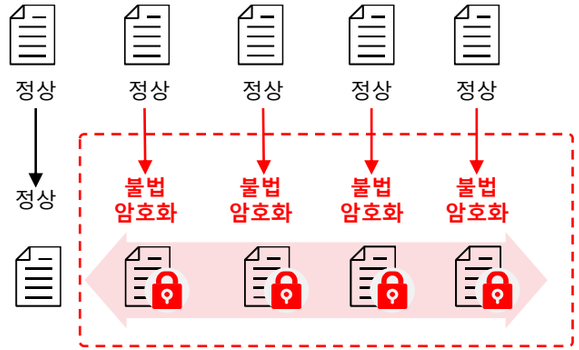
보안 취약점 악용 공격

시스템 및 어플리케이션 취약점을 노리는
악의적인 도구와 랜섬웨어로 추가 전파됨

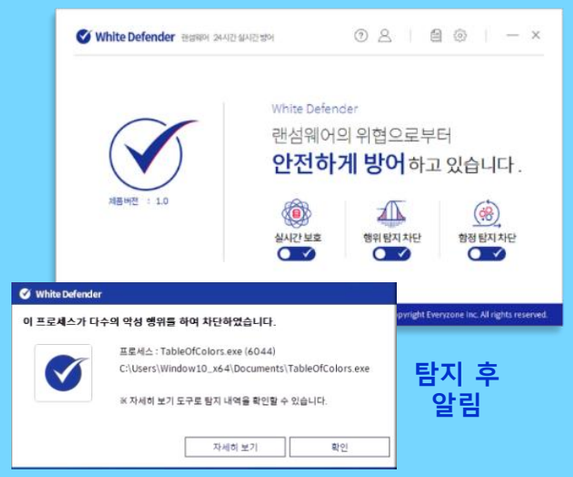
공격 랜섬웨어 공격진행

랜섬웨어 특성에 따라 암호화 공격 진행

시스템 내 랜섬웨어 의심 상황 발생 시
보호 대상 파일 감시 및 실시간 백업



방어 랜섬웨어 탐지 방어 알람



탐지 후 알림

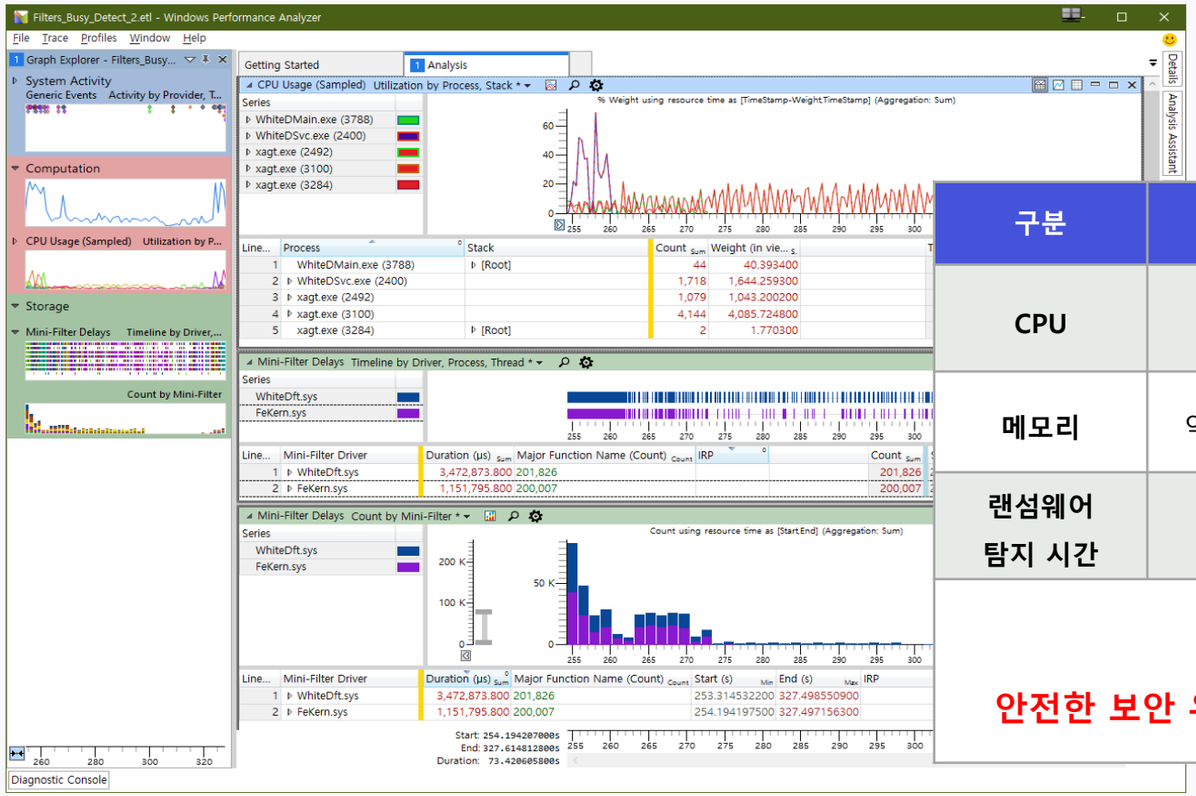
의심 프로세스에 의한 불법 암호화 상황으로
판단 시 랜섬웨어 프로세스 중지 및 피해 예상 파일
복원 완료 후 사용자 알림 진행

White Security Platform

화이트디펜더 최적의 시스템 활용

WhiteDefender 제품군은 낮은 시스템 자원 활용 수준으로 설치되어 있는 엔드포인트 시스템의 기본 운영 속도 저하를 최대한 방지

화이트디펜더의 우수한 성능



시스템 자원 활용 측정 결과

구분	평상시	탐지시	비고
CPU	약 1%	약 3 %	랜섬웨어 탐지 시 시스템 운영 속도 저하 없음
메모리	약 40 MB	약 40 MB	변동 없음
랜섬웨어 탐지 시간	0초	3.4 초	랜섬웨어를 행위 기반 탐지 후 백업, 복구까지의 시간

행위탐지 차단 진행시에도

안전한 보안 유지 및 시스템 성능을 최상의 상태로 유지됩니다.

화이트디펜더 주요 기능 및 특장점

WhiteDefender는 랜섬웨어의 안정적인 성능 유지를 위해 소프트웨어의 기능성, 신뢰성, 사용성 등을 테스트하여 GS인증 1등급을 획득했습니다.

구분	화이트디펜더 (성능 우수)
탐지 특징	1. 랜섬웨어 방어 및 파일 훼손 행위 차단 및 손상 롤백 자체 엔진 보유 2. 행위 탐지 엔진의 포렌식 검증 통해 의심 상황에 대한 오탐율 최소화 3. 랜섬웨어 대상 사전탐지 DB 사용
보안 위협 대응 형태	1. 사용자 파일 관련 의심 프로세스 동시 추적 및 모니터링 2. 의심 상황 발생 시 실시간 백업 및 변경 사항 모니터링 3. 의심 프로세스에 의한 파일 훼손 탐지 시 드라이버 연동으로 변경 관련 최대 정보 확보 및 복구 진행
동작 성격	✓ 행위 탐지 엔진 기반 능동적 ✓ 보안 기능 + 랜섬웨어에 특화된 효율성 ✓ 높은 사전탐지 기능 보안 기능 동시 제공

GS인증 1등급 획득

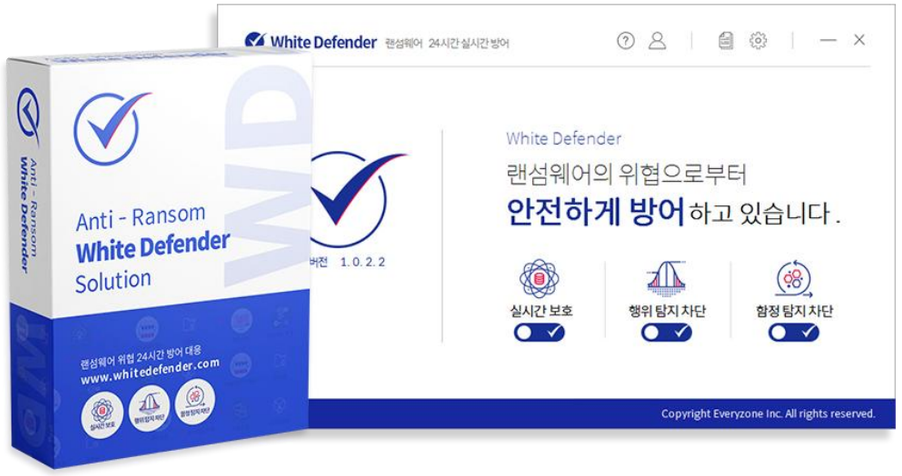
< 화이트 디펜더 (PC버전) >

< 화이트디펜더 서버 (윈도우서버 버전) >

안티랜섬웨어 실시간 보호

화이트디펜더 PC용 제품

랜섬웨어위협을실시간으로모니터링하고
알려지지않은신종랜섬웨어까지방어할수있습니다.



1/ 실시간 모니터링
랜섬웨어 실시간 보호

랜섬웨어 위험에 24시간 실시간 방어가 필요합니다. 다양한 보안 위험, 랜섬웨어 공격에 실기간 방어를 제공합니다.

랜섬웨어 실시간 보호

2/ 알려지지 않은 신종
랜섬웨어 행위 탐지 기능

악의적인 랜섬웨어 행위를 사전에 탐지하고
잘 알려지지 않은 신종 랜섬웨어를 행위 기반
으로 방어하고 대응합니다.

행위 탐지 기능

3/ 파일 훼손 대응
랜섬웨어 백업/복구 기능

정교한 랜섬웨어 함정에 빠지지 않도록 방어합니다.
지속적인 보안 위협에 끊임없이 대응할 수 있도록
방어 체계를 제공합니다.

자동 백업/복구

PC용 제품 기능

자체 보호
- 프로세스, 폴더, 레지스트리의 손상을 자체 보호

쉐도우 복사본 보호
- 복원 시점, 복원에 사용되는 정보에 접근 시 차단

비서명 프로세스 실행 알림/차단
- 서명되지 않은 파일이 실행될 경우 알림을 통해 허용, 차단, 예외 처리 가능

파일 쓰기 차단
- 내 PC & 네트워크 파일 쓰기 차단을 통해 랜섬웨어 감염 예방

스크립트 위험 행위 차단
- 스크립터에 의해서 위험한 파일이 생성이 되는 경우 차단

복원용 저장 파일 삭제
- 설정한 기간 동안 탐지된 복원 파일을 저장하여 이 후 데이터는 자동 삭제

행위 탐지 복원 저장 파일
- 설정한 파일보다 큰 경우, 행위 탐지 복원 파일 저장에서 제외되는 기능(최대 100mb)

PC용 제품 권장 사양

분류	사양
운영 체제	윈도우 7 이상 권고
CPU	인텔 펜티엄 i3 2.6 GHz 이상
메모리	2GB 이상
저장 공간	설치 100MB이상 / 운영 5GB 이상

※ 방화벽을 통해 프로그램의 기본 통신이 차단되는 경우, 정상적인 업데이트가 동작하지 않을 수 있습니다.

서버의 랜섬웨어 상황 실시간 모니터링

화이트디펜더 서버용 제품

윈도우서버에 최적화된 서버 전용 안티랜섬웨어 솔루션으로
안정적인 기업의 보안 환경을 구축하세요.

1/ 윈도우서버 전용 랜섬웨어 실시간 보호

다양한 보안 위험에 랜섬웨어 공격
실시간 방어 제공

서버 실시간 보호

2/ 알려지지 않은 랜섬웨어 행위 탐지 기능

랜섬웨어 행위를 사전에 탐지하고
신종 랜섬웨어를 행위 기반 방어
대응

행위 탐지
기능

3/ 파일 훼손 대응 랜섬웨어 백업/복구 기능

파일 훼손이 발생할 경우, 순간 백업,
랜섬웨어 차단 후 파일 복구로 안전

함정 탐지
기능

화이트디펜더 서버용 제품 기능

자체 보호
- 프로세스, 폴더, 레지스트리의 손상을 자체 보호

쉐도우 복사본 보호
- 복원 시점, 복원에 사용되는 정보에 접근 시 차단

비서명 프로세스 실행 알림/차단
- 서명되지 않은 파일이 실행될 경우 알림을 통해 허용, 차단, 예외 처리 가능

파일 쓰기 차단
- 내 PC & 네트워크 파일 쓰기 차단을 통해 랜섬웨어 감염 예방

스크립트 위험 행위 차단
- 스크립터에 의해서 위험한 파일이 생성이 되는 경우 차단

복원용 저장 파일 삭제
- 설정한 기간 동안 탐지된 복원 파일을 저장하여 이 후 데이터는 자동 삭제

행위 탐지 복원 저장 파일
- 설정한 파일보다 큰 경우, 행위 탐지 복원 파일 저장에서 제외되는 기능(최대 100mb)

추가 파일 보호소
- 100MB 이상 크기의 보호 확장자 파일 손상 발생시 대비 추가 보호 기능

중앙 관리 연동
- 주 서버 운영 기능에 대한 중앙 관리를 통한 예외 연동 기능으로 업무 연속성 확보

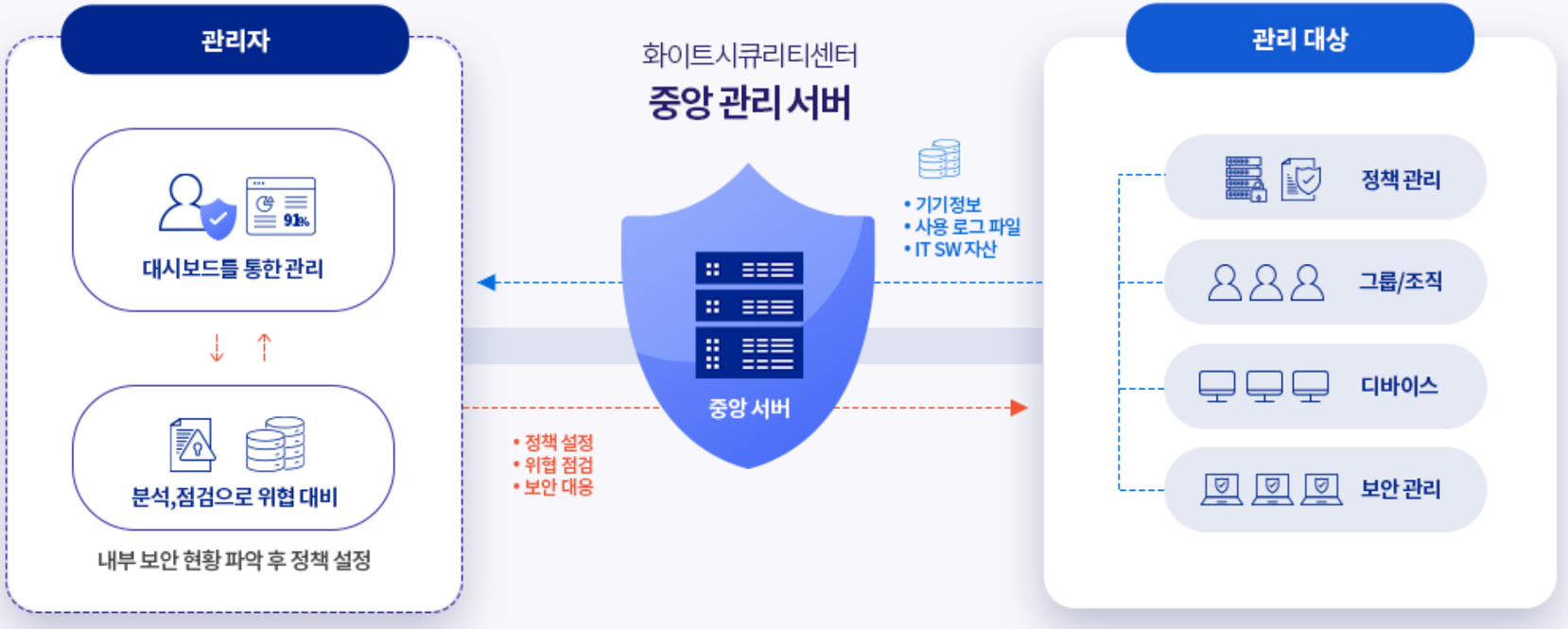
서버 권장 사양

분류	사양
운영 체제	Windows Server 2008 R2 이상 권장(64비트)
CPU	Intel Xeon Dual Core 이상
메모리	권장 메모리 4GB 이상
저장 공간	설치 100MB이상 하드 드라이브 설치 여유 공간/ 10GB 이상 하드 드라이브 여유 공간 권장
네트워크	IPv4, IPv6 네트워크 환경 권장/ *중앙관리용 WSC 서버 연동 권장

※ 방화벽을 통해 프로그램의 기본 통신이 차단되는 경우, 정상적인 업데이트가 동작하지 않을 수 있습니다.

화이트시큐리티센터(White Security Center, WSC) 구성

[WSC 일반 구성 형태]



[운영체제] WSC Server ▶ Linux CentOS 7.2 + PostgreSQL 9.5.4 버전 이상 권장 | WSC Console & WSC Agent ▶ Windows 7 이상

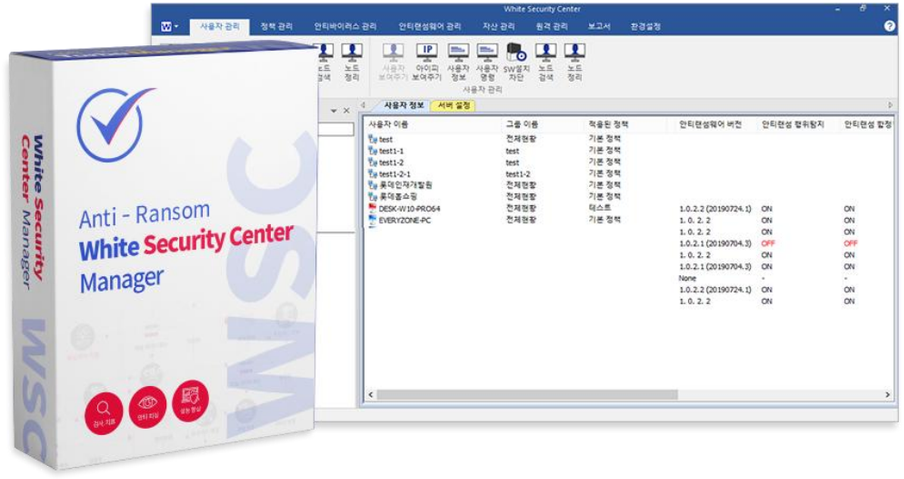
[하드웨어] WSC Server ▶ CPU – 클럭 속도 2.4GHz 이상 Intel CPU | Memory – 8GB 이상 | DISK – 200 GB 이상 여유 공간 권장 (HDD 보다 SSD 권장)

WSC Console & Agent ▶ CPU – Intel i3 2.6GHz 이상 | Memory – 4GB 이상 | DISK – 5GB 이상의 여유 공간 권장 (HDD 보다 SSD 권장)

화이트디펜더 중앙 관리자용 솔루션

화이트시큐리티센터 WSC

화이트 시큐리티 센터는 기업 내부의 랜섬웨어 위협 데이터를
수집하고 모니터링하여 랜섬웨어 위협을 관리합니다.
관리자가 기업의 보안 현황을 한눈에 파악할 수 있도록 대시보드를 제공합니다.



1/ 중앙 집중 관리
사용이 쉽고 빠른

설치된 화이트디펜더 관리와
실시간 사용 상태, PC 보안 현황 관리

중앙 집중 관리

2/ 정책 생성 관리
지속 가능한 관리

그룹 및 사용자 별로
정책 생성, 삭제, 수정/실시간 적용

정책 생성 관리

3/ 대시보드
관리자 편의성

화이트디펜더 동작 상태와 랜섬웨어
탐지 및 방어 현황 확인/보고서 출력

편리한
대시보드

화이트시큐리티센터 기능

기업 내부의 랜섬웨어 위협 데이터를 수집하고 모니터링하여 랜섬웨어 위협을 관리합니다.
관리자가 기업의 보안 현황을 한눈에 파악할 수 있도록 대시보드를 제공합니다.

대시보드

- 내부 보안 상태를 빠르게 파악하고 필요한 조치를 취할 수 있도록 관리

내부 자산 수집/관리

- 에이전트 PC 또는 그룹들을 선택하여 S/W, H/W 정보를 수집/관리

정책 설정 관리

- 에이전트 PC 또는 그룹들의 H/W 보안 수준을 설정

내부 보안 관리

- 에이전트 PC 또는 그룹들의 보안 수준을 설정하고 관리

관리 보고서

- 내부 보안 현황에 대한 정보를 리포트로 받아볼 수 있는 보고서

원격 제어 관리

- 에이전트 PC 또는 그룹들을 선택하여 원격 제어

화이트시큐리티 센터 구성 관리자가 사용할 수 있는 웹 기반의 관리 콘솔과 중앙 서버, 에이전트로 구성됩니다.

분류	사양
제품 구성 환경	관리 서버 + 관리 콘솔 + 에이전트
Server	Linux Centos 7.X, PostgreSQL DB
Console	윈도우 7 이상, 시스템 메모리 1GB 이상, 저장 공간 150MB 이상
Agent	윈도우 7 이상, 시스템 메모리 1GB 이상, 저장 및 운영 1GB 이상 권장

※ 화이트시큐리티 센터가 설치되는 서버는 고객사 환경에 따라 차이가 있을 수 있습니다.

화이트시큐리티센터(WSC) 서버 구성 시스템 권장 사양

*최신 업데이트 지원 위하여 IPv4, IPv6 인터넷 네트워크 환경 필요

OS	리눅스 CentOS 7.2 버전 권장 (운영 안정화 버전이며 최신 7.6 버전도 지원)
CPU	클럭 속도 2.4GHz 이상인 Intel CPU ➔ 최소 2 Core 이상 / 권장 4 Core 이상 운용
RAM	시스템 메모리 최소 8GB 이상 사용 가능 확보 필요 ➔ 최소 8GB 이상 여유 메모리 필요 (설치 메모리 16GB 이상 권장)
HDD	SSD 형태 하드 드라이브 200GB 이상의 여유 공간 권장 : WSC 서버 모듈 및 PostgreSQL 9.5.4 버전 설치 및 운용 / 로그 저장 ➔ 일반 HDD 보다 처리 속도 빠른 SSD 권장

화이트시큐리티센터(WSC) 관리 콘솔 설치 최소 사양

OS	Microsoft Windows 7 | 8 | 8.1 | 10 - (32비트/64비트)
CPU	Intel Pentium Core i3 2.6GHz 이상 권장
RAM	4 GB 이상 권장
HDD	설치 100MB 이상 여유 공간

WhiteDefender

제품 적용 산업군

Industries

랜섬웨어 차단 "화이트디펜더" 제품 적용 산업군

화이트디펜더는 다양한 산업군에 랜섬웨어 대응 관련 보안 시스템 구축 경험을 기반으로
물류, 제조(팩토리), 유통/커머스, 방송/미디어, 병원/의료, 호텔/빌딩, 정유/화학 등 기업 영역에
특화된 랜섬웨어 대응책을 제공합니다.

물류/제조 산업군

유통·물류 트랜드의 효과적인 대응 및 고객 서비스 선도

산업군 :물류/제조

구축 사례

롯데글로벌로지스

담당자

> **본사와 물류 영업소 간 랜섬웨어 동시 대응, 안티랜섬웨어 화이트디펜더 대응과 함께 전사 엔드포인트 현황 및 추가 정보 관리가 가능하게 되었습니다.**

주요 도입 효과

1. 엔드포인트 PC 내 중요 정보 자산에 대한 랜섬웨어 능동 대응 솔루션 확보
2. 생산직부터 관리사무직까지 포함한 포괄적 업무 환경에 대한 호환성 및 운용성 확보
3. 기존 안티바이러스 제품군을 보완한 추가적인 업무 보안성 확보

SOLUTION

최근 국내를 대상으로 한 고도화된 사이버 공격이 일어나고 있는 외부 위험 요소의 증가와 함께 사업 환경 상 다수의 자료가 외부 유출이나 불법 암호화 공격으로부터 보다 더 안전해야 할 필요성이 증가되어, 기존에 운영 중인 보안 솔루션과 함께 추가적으로 랜섬웨어 대응 기능을 보완해줄 전문 솔루션의 도입을 검토하게 되었습니다.

RESULTS

화이트디펜더(WD)와 중앙관리 목적의 화이트시큐리티센터(WSC)를 도입한 후 시스템 운영 초기 적응 단계에서 심각한 장애는 발생하지 않았고, 운영 초기에 전사 대응 정책 수립을 조정해가며 전문 엔지니어와 안정화 작업을 진행하였습니다.

물류/제조 산업군

국내/외 친환경 고효율 에어컨 분야 선도기업

산업군 :물류/제조

구축 사례 Carrier 캐리어에어컨

담당자

> **화이트디펜더 도입 후 생산 현장에서 경영 부문까지 랜섬웨어 대응 대비책을 확보하여 주기적인 모니터링 및 관리가 가능해 졌습니다.**

주요 도입 효과

1. 적극적 랜섬웨어 대응과 함께 전사 엔드포인트 현황 파악
2. 기존 안티바이러스 제품군을 보완하여 랜섬웨어 의심 활동에 대한 대비
3. 본사, 연구소 및 생산 현장 포함한 포괄적 업무 환경에 대한 호환성 및 운용성 확보

SOLUTION

일반 사무용 프로그램을 주로 사용하는 본사와 제조업 분야에서 많이 사용되는 제품 개발 모델링 프로그램을 주로 사용하는 연구소 및 생산 현장 등 다양한 PC 환경과 조직원 구성으로 기존에도 다양한 보안 솔루션을 도입하여 사용하고 있었으나, 해외 제조업 현장의 사례와 같이 늘어나는 랜섬웨어의 위협 속에 보다 적극적으로 대응하기 위해 도입 검토 중이었습니다.

RESULTS

새로운 보안 제품의 도입 및 적용에 있어서 보안 담당자 입장에서 가장 우려되는 부분은 기존에 운영 중인 환경 내 심각한 장애 발생 및 장시간 동안 이뤄지지 않는 조치 과정일 것입니다. 화이트디펜더(WD)와 중앙관리 목적의 화이트시큐리티센터(WSC)를 도입하였으며 부분적으로 발생한 간섭 사항에 대해서는 개발사에서 빠르고 적극적인 지원을 받습니다.

정유/화학 산업군

친환경 정밀화학 제품

산업군 :정유/화학

구축 사례 그린케미칼

담당자

“ 본사/공장 및 연구소, 서울사무소 대상으로 화이트디펜더 및 화이트시큐리티센터 도입하여 랜섬웨어 공격의 불확실성에 대한 적극적 대응 및 보호를 통한 보안성 강화를 진행하였습니다.

주요 도입 효과

1. 랜섬웨어 공격에 대한 실시간 방어 및 모니터링 진행
2. 안티바이러스 제품과 호환성 확보하여 상호 보완 운영으로 보안성 강화
3. 산업 현장 및 해외 업무 등 주요 정보 자산에 대한 엔드포인트 보호 능력 추가 확보

SOLUTION

일반 사무 환경 및 제품 생산 공장과 같은 산업 현장과 해외 관련 업무를 주로 진행하는 환경에서 점점 고도화되어 가는 랜섬웨어 공격에 대한 적극적 대응의 필요성이 점점 높아지는 가운데, 이에 다양한 보안 프로그램과 상호 충돌을 최소화하고 해당 제품의 도입과 실제 운영 시 적극적 지원을 받을 수 있는 제품을 검토하게 되었습니다.

RESULTS

보안 담당자 입장에서 화이트디펜더(WD)의 랜섬웨어 대응 활동 정보와 정책 관리를 제공하는 화이트시큐리티센터(WSC)를 통하여 조직 내 엔드포인트 PC의 운영 상태를 모니터링하고 랜섬웨어 의심 활동에 대한 정보 확인을 통해 보안 강화 조치를 중앙에서 정책으로 지정할 수 있게 되어 업무 보안성과 운용성을 효율적으로 확보할 수 있게 되었습니다.

유통/커머스 산업군

세계 최초 글로벌 편의점 브랜드 코리아 세븐

산업군 :물류/제조

구축 사례 7-ELEVEN

담당자

> **다수의 환경에 대한 호환성 및 운용성을 확보하여 랜섬웨어 방어를위한 화이트디펜더 제품군을 보완하였습니다.**

주요 도입 효과

1. 엔드포인트 PC 내 중요 정보 자산에 대응 솔루션 확보
2. 기존 보안 제품군을 보완하여 랜섬웨어 의심 활동에 대한 대비
3. 생산직부터 관리사무직까지 포함한 포괄적 업무 환경에 대한 호환성 및 운용성 확보

SOLUTION

다수의 자체 개발 솔룻ㄴ 및 외부 솔루션을 도입하여 운영하고 있는 전산 환경 상에서 기존 운영 소프트웨어와의 호환성과
시스템 부하가 낮게 유지되면서 보안성은 강화할 수 있는 솔루션을 찾던 중 국내 다수의 기업에서 좋은 평가를 받고 있는 화이트디펜더를 접하게 되어 중앙 관리 제품군과 함께 내부 테스트를 끝마치고 정식 배포를 진행하게 되었습니다.

RESULTS

안티랜섬웨어 제품 중 행위 기반 탐지와 시그니처 기반 탐지가 같이 존재하면서 실시간 보호 기능 활성화 상태에서도
PC 사용에 부담이 크게 발생하지 않은 점이 화이트디펜더 제품군의 장점으로 느껴졌으며, 유지보수에 보다 합리적인 상황으로 운영하게 된 점이 만족스러웠습니다.

방송/미디어 산업군

국내 지상파 공영 방송사

산업군 : 방송/미디어

구축 사례 MBC

담당자

“ 화이트디펜더 제품군 설치 후 랜섬웨어 적극 대응 능력 확보!
업무 보안성과, 운용성을 효율적으로 확보할 수 있게 되었습니다.

주요 도입 효과

1. 지능화된 랜섬웨어 공격과 유사 공격에 대한 대응력 강화
2. 솔루션 도입 조직 내 업무 보안성과 운용성 확보
3. 다양한 사용자 환경에 대한 빠른 분석 및 대처 능력 확보

SOLUTION

언론/방송/미디어 산업군 특성에 따라 다양한 PC 운영 환경과 프로그램을 사용하는 조직원으로 구성된 고객사에서는 점점 증가되는 랜섬웨어 공격 위험에 대응하기 위해 기존 시그니처 기반 안티 바이러스 제품군 외에 글로벌 업체의 EDR 솔루션 및 랜섬웨어 대응 전문 보안 제품군에 대한 추가 도입을 준비하고 있었습니다.

RESULTS

보안 담당자 입장에서 화이트디펜더(WD)의 랜섬웨어 대응 활동 정보와 정책 관리를 제공하는 화이트시큐리티센터(WSC)를 통하여 조직 내 엔드포인트 PC의 운영 상태를 모니터링하고 랜섬웨어 의심 활동에 대한 정보 확인을 통해 보안 강화 조치를 중앙에서 정책으로 지정할 수 있게 되어 업무 보안성과 운용성을 효율적으로 확보할 수 있게 되었습니다.

WhiteDefender

레퍼런스

많은 기업들이 화이트디펜더를 도입하여 랜섬웨어 위협으로부터 스마트하게 대응하고 있습니다.

행정안전부
국회부산도서관 NATIONAL ASSEMBLY BUSAN LIBRARY
국회도서관 NATIONAL ASSEMBLY LIBRARY
sb 성북구 도시관리공단
MIRAE ASSET 미래에셋증권 베트남
한국소프트웨어저작권협회
RAPA 한국전파진흥협회 Korea Radio Promotion Association
KTNET 한국무역정보통신
롯데멤버스
LOTTE DUTY FREE 롯데면세점
7-ELEVEN
롯데홈쇼핑
롯데글로벌로지스
롯데물산
롯데유통사업본부
Canon
MBC
세계일보
롯데하이마트
롯데컬처웍스

많은 기업들이 화이트디펜더를 도입하여 랜섬웨어 위협으로부터 스마트하게 대응하고 있습니다.

롯데렌탈 | 롯데제과 | 롯데칠성음료 | 롯데건설

롯데자이언츠 | LOTTE INEOS | 롯데월드 | 롯데알미늄

현대통신 | Carrier 캐리어에어컨 | LUCOMS | 한일단조공업(주)

KUHNIL 건일제약(주) | 이원의료재단 EONE Laboratories | 동구바이오제약 | 안국약품(주)

HANGLAS | VITZRO CELL | 그린 케미칼 | [주] 서양 네트웍스

많은 기업들이 화이트디펜더를 도입하여 랜섬웨어 위협으로부터 스마트하게 대응하고 있습니다.

Asemtech (주)아셈텍

신보운영관리(주) 신용보증기금 자회사

HANMI (주)한미철강

바르미 호텔인터불고 대구

효성병원

미즈맘병원 MIZMAM HOSPITAL

세명병원

여성아이병원

청라연세어린이병원 Cheongna Yonsei Children's Hospital

APEC Asian Power & Energy Corp.

주식회사 대호하이텍

KUNYOUNG TECH

STEEL DREAM

SHINHAN PRECISION IND.CO.,LTD

TESK Total Emission Solution Korea Co,Ltd.

김천에너지서비스 | SK E&S

㈜새날테크텍스

DASAN Machineries Co.,Ltd.

Sungbo Industries Co., Ltd.

기업外1000여개

안티랜섬웨어 차단 솔루션 **화이트디펜더**

www.WhiteDefender.com

Thank You

화이트디펜더
고객 문의

대표 번호 02-3274-2700
문의 메일 contact@whitedefender.com
홈페이지 www.whitedefender.com