1등급 GOOD Software 조달청

안티랜섬웨어 차단 솔루션 화이트디펜더

www.WhiteDefender.com



화이트디펜더 / 터보백신

Industries

디지털 세상을 안전하게 설계하는 “터보백신 "

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















유지관리서비스 산업군



유지관리서비스

산업군 : 유지관리서비스

구축 사례 BRINKS

도입 전 상황

금보원 감사 조건에 맞는 서비스 구축 및 지원이 필요하고 다양한 종류의 **ATM**기기 솔루션 환경의 안정적 지원 및**ATM**기기중 저사향의 기기에서도 백신 소프트웨어를 사용해야 되며 **폐쇠망 환경에서 사용할 수 있도록 백신 업데이트 구축**과 전국에 분포되어 있는 **ATM**기기의 효율적인 관리가 필요 했습니다.

주요 도입 효과

1. 금보원 요구사항에 맞는 백신 서비스 환경 구축
2. 원활한 서비스 제공을 통해 안정적인 운영 및 비용 절감 효과 달성

SOLUTION

다양한 종류의 ATM기기 환경에 맞춘 터보백신 커스터마이징 제작
ATM 기기에 맞게 최적화된 환경으로 설치되어 동작
폐쇠망 환경에서도 최신 백신 업데이트를 진행 할 수 있도록 지원
효율적인 중앙관리를 위한 터보백신 매니저 공급

RESULTS

금보원 요구사항에 맞는 최적화된 환경으로 **폐쇄망 백신 관리 환경을 구축하여 ATM 기기에 최적화된 터보백신 사용으로 안정적인 서비스 운영이 가능해 졌으며**, 기존 발생했던 다양한 장애 현상도 터보백신으로 교체하면서 사라졌고, 이로 인해 엔지니어 현장 방문도 최소화 되면서 많은 비용절감 효과를 가져왔습니다. 또한, 터보백신 매니저에서 제공하는 다양한 기능으로 전국에 분포되어 있는 ATM기기의 효율적으로 관리가 가능해졌으며,무엇보다도 원활한 서비스 운영으로 **정기 보안 감사도 수월하게 잘 대응할 수 있게 되었습니다.**



유지관리서비스 산업군



종합병원 전체 병원 악성코드 보안 서비스 구축

산업군 : 병원 /의료

구축 사례

세림병원 Serim General Hospital

도입 전 상황

심평원 심사 조건에 맞는 보안 서비스를 구축 및 지원 하고 다양한 종류의 의료정보시스템과 충돌 없는 서비스 운영과 낮은 사양의 **PC**에서도 사용할 수 있는 백신 소프트웨어 그리고 보안 이슈 발생시 빠른 상담 지원이 필요 했었습니다.

주요 도입 효과

1. 심평원 요구사항에 맞는 백신 서비스 환경 구축
2. 다양한 의료 정보시스템과의 호환성 제공을 통해 안정적인 원내 서비스 운영

SOLUTION

다양한 종류의 의료정보시스템과 호환성을 맞춘 터보백신 커스터마이징 제작과 함께 원내 업무 환경에 맞는 최적화된 상태로 설치되어 작동 했으며 **전체 PC를 전산실에서 효율적으로 관리할 수 있도록 터보백신 매니저를 공급했습니다.**

RESULTS

심평원 요구 사항과 의료정보시스템에 최적화된 터보백신 설치를 통해 다양한 악성코드 위협으로부터 병원을 안전하게 보호 할 수 있게 되었습니다. 터보 매니저를 통해 전체 PC의 악성코드 감염 및 최신 엔진 업데이트 현황을 실시간으로 모니터링하고 있으며, 매체 제어기능을 활용하여 내부 보안을 강화했고, 원격제어, 메시지 전송, SW/HW 자산관리 기능을 통해 즉각적인 장애 대응과 함께 내부 PC관리가 수월 해졌습니다. **무엇보다도 다양한 보안 이슈 대해서 상담이 가능하고, 대응 방안에 대해 조언을 받을 수 있게 되었습니다.**

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 부분까지 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 오랜 시간 동안 이뤄지지 않는 조치 과정일 것입니다. 화이트디펜더(WD)와 중앙관리 목적의 화이트시큐리티센터(WSC)를 도입하였으며 부분적으로 발생한 간섭 상황에 대해서는 개발사에서 빠르고 적극적인 지원을 받습니다.



정유/화학 산업군



친환경 정밀화학 제품

산업군 :정유/화학

구축 사례 제조 기업 G사

담당자

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

주요 도입 효과

1. 랜섬웨어 공격에 대한 실시간 방어 및 모니터링 진행
2. 안티바이러스 제품과 호환성 확보를 통한 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 정책적으로 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 관리사무직을 포함한 포괄적 업무 환경에 대한 호환성 및 운용성 확보

SOLUTION

다수의 자체 개발 솔루션 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, 신속한 유지보수가 가능한 운영을 할 수 있게 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 정책적으로 지정할 수 있게 되어 업무 보안성과 운용성을 효율적으로 확보할 수 있게 되었습니다.

User Live

화이트디펜더 제품 사용자 Live

2018년부터 랜섬웨어 대응책으로 화이트디펜더를 사용하고 있는 고객들의 숫자입니다.
2021년 3월부터 8월까지 6개월만에 10만 사용자가 증가하고 있습니다.
이후로는 더 많은 사용자가 늘어날 것 입니다.



바이러스/악성코드 솔루션

TurboVaccine 제품 소개

터보백신 제품 라인업

TurboVaccine라인업



터보백신
PC용 제품



터보배신/윈도우/리눅스
Server용 제품



터보백신중앙관리센터
중앙 관리자용 제품

Why TurboVaccine?

A) 바이러스/ 악성코드 검사, 치료 가능?

B) 검사 방법과 예약 기능(정밀/빠른/선택 검사방법)?

C) 안티 피싱-웹 실시간 보호 가능한가?

D) PC성능 최적화 가능(윈도 설정/PC 관리)?

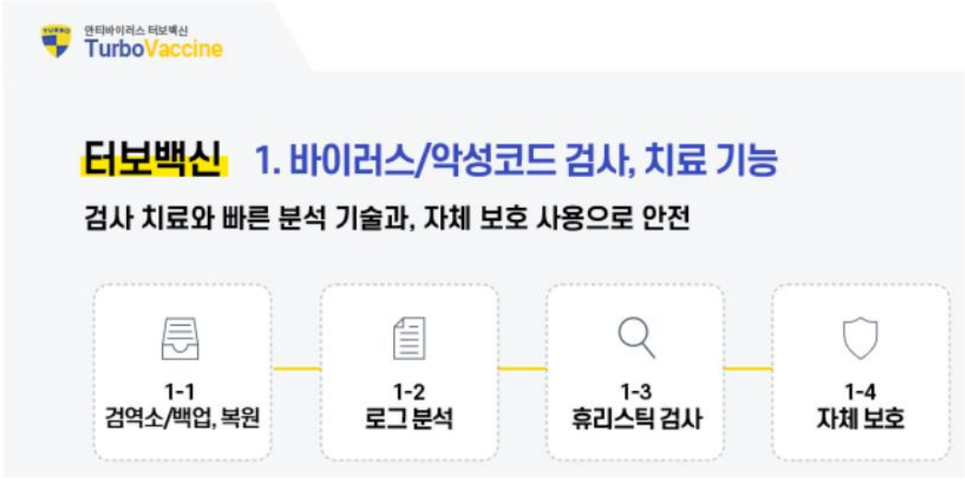
E) 실시간 보호, 고급 설정기능, 저장매체 보호가능(USB바이러스 오토런 방지)?

이 모든 질문에 **Yes!** 라고 답할 수 있는
Anti-Virus 솔루션

Turbo Vaccine!

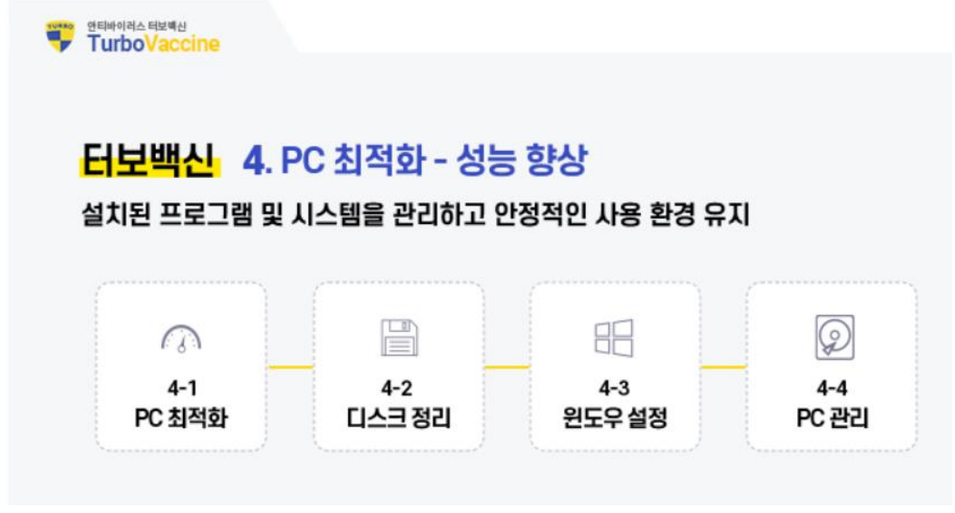


기본 동작 원리


안티바이러스 터보백신
TurboVaccine
터보백신 1. 바이러스/악성코드 검사, 치료 기능
검사 치료와 빠른 분석 기술과, 자체 보호 사용으로 안전
1-1
검역소/백업, 복원
1-2
로그 분석
1-3
휴리스틱 검사
1-4
자체 보호


안티바이러스 터보백신
TurboVaccine
터보백신 2. 검사 방법과 예약 기능
검사 모드 선택 할 수 있어 보안 점검 효율성 최대 활용
2-1
정밀 검사
2-2
빠른 검사
2-3
선택 검사
2-4
예약 검사


안티바이러스 터보백신
TurboVaccine
터보백신 3. 안티 피싱 - 웹 실시간 보호 기능
인터넷을 통해 유입되는 공격과 위험을 차단
3-1
피싱 감시
3-2
팝업 광고 차단
3-3
사이트 차단
3-4
유해 차단


안티바이러스 터보백신
TurboVaccine
터보백신 4. PC 최적화 - 성능 향상
설치된 프로그램 및 시스템을 관리하고 안정적인 사용 환경 유지
4-1
PC 최적화
4-2
디스크 정리
4-3
윈도우 설정
4-4
PC 관리

기업을 위한

터보백신 클라이언트

기업을 위한 필수 백신 솔루션
사내 환경을 외부 위험으로 부터 안전하게 보호합니다.



1 바이러스/악성코드
검사 후 진단 하고 치료 가능

인터넷을 통해 유입되는
바이러스/악성코드 를 진단하고
개별적 검사와 치료 할 수 있습니다.

Scan

2 다양한 수법의
피싱 차단과 개인 정보 보호

안티피싱.팝업차단/URL차단 기능을
통해 유해 사이트 및 불필요한 사이트로
부터 개인 정보를 보호합니다.

Anti Phishing

3 악의적으로 이용될
정보와 시스템 설정 관리

설치된 프로그램을 관리하고 불필요한
시스템 정보 삭제를 통해 안정적인 PC
사용 환경이 유지됩니다.

Cleaner

악성코드 검출 및 치료

- 컴퓨터에 유입되는 다양한 악성코드를 실시간으로 감지, 실시간 감시 창을 통해 확인 후 치료
- 원 클릭 만으로 컴퓨터에 존재하는 악성코드/스파이웨어/애드웨어에 대한 검사 및 치료
- **정밀 검사 :** 모든 파일과 모든 드라이브를 선택 검사
- **빠른 검사 :** 루트 드라이브의 시스템 파일을 우선 검사

예약 검사 및 업데이트

- 컴퓨터 부팅 시 자동으로 백신엔진 및 바이러스 패턴 업데이트가 이루어지므로 항상 최신 엔진을 유지하고 예약한 시간에 바이러스 검사 및 패턴 업데이트가 이루어지도록 자동 설정

안티피싱

- 방송통신심의위원회 권장 설정을 적용, 각종 유해 사이트의 접근을 차단하고 방문을 원하지 않는 사이트를 사용자가 임의로 추가 관리
- 유해 팝업 창 판별/차단하는 기능과 함께 다양한 피싱 사기에 대응할수 있도록 피싱 감시
- USB 메모리를 통해 감염되는 오토런 바이러스의 연결 고리를 차단하여 컴퓨터를 보호하며, 안전한 USB 메모리로 사용할 수 있도록 지원

불필요한 정보 삭제 및 데이터 정리 지원

- 데이터 정리 기능을 통해 악의적으로 이용될 수 있는 인터넷 익스플로어 및 레지스트리 정보, 윈도우의 불필요한 파일을 제거하여 로컬 디스크의 공간을 확보함과 동시에 컴퓨터 수행 속도를 향상

검역소 및 주요 활동 로그 기능

- 불필요 데이터 정리, 바이러스 치료, 스파이웨어 치료 등을 통해 발생할 수 있는 중요한 파일의 손실을 막기 위해 검역소를 만들어 삭제된 파일을 백업 후 필요 시 복구
- 빠른 검사 및 정밀 검사 / 실시간 감시, 인터넷 보안, 유틸리티, 업데이트 등의 로그를 확인

권장 시스템

분류	사양
운영 체제	Microsoft Windows 7, 8, 8.1 (64bit) / 10
하드웨어	Intel Pentium 1GHz이상 / 512MB 이상 (권장: 1GB) / IPV4,IPV6 네트워크
메시지 프로그램	MSN Messenger 7.5이상 / Windows Messenger 4.7 이상 / NateOn 3.5 이상
웹 브라우저	Microsoft Internet Explorer 7 이상 권장
이메일 프로그램	Microsoft Outlook Express 6.0 이상

윈도우 서버에 최적화

터보백신 서버

각종 보안 위협으로 부터 중요한 서버 시스템을 보호하세요.
서버로 유입되는 각종 악성코드의 침임을 감시하고 차단합니다.



1 바이러스 검사,치료
강력한 탐지력 기반

터보백신의 멀티코어 지원 기능으로 서버 시스템의 CPU 점유율을 낮춰 보다 쾌적한 환경에서 운영될 수 있습니다.

Scan

2 자동 업데이트 예약
빠르고 정확한 패턴 업데이트

자동 업데이트로 항상 최신 엔진을 유지합니다. 예약 한 시간에 자동으로 바이러스 검사 및 패턴 업데이트가 이루어지도록 설정할 수 있습니다.

Update

3 핵심 프로세스 보호
자가 보호 및 복원

터보백신 실행을 방해하는 위험 요소에 대응 할 수 있도록 핵심 프로세스를 보호하며, 파일이 삭제되더라도 업데이트를 통해 복원됩니다.

Protection

강력한 탐지력 기반 바이러스 검사/치료

- 터보백신의 멀티코어 지원 기능으로 서버 시스템의 CPU점유율을 낮춰 보다 쾌적한 환경에서 운영

멀티코어 기반 CPU 지원

- 멀티코어 컴퓨터에서 그래픽, 설계, DB 관련 프로그램을 사용하시는 분들은 터보백신의 멀티코어 지원 기능으로 보다 적은 CPU 점유율로 업무를 처리 가능

빠르고 편리한 자동 업데이트/예약 기능

- 컴퓨터 부팅 시 자동으로 백신엔진 및 바이러스 패턴 업데이트가 이루어지므로 항상 최신 엔진을 유지합니다. 또한, 사용자가 예약한 시간에 자동으로 바이러스 검사 및 패턴 업데이트가 이루어지도록 설정할 수 있습니다.

자가 보호 및 자기 복원

- 터보백신 실행을 방해하는 여러 가지 위험 요소에 대응할 수 있도록 핵심 프로세스를 보호하며, 알 수 없는 원인에 의하여 파일이 삭제되더라도 업데이트를 통해 복원

권장 시스템

분류	사양
운영 체제	Windows 2003 Server SP1 / 2008 / 2012/2016/2019
하드웨어	Intel Pentium 1GHz 이상

강력한 리눅스서버 보안

터보백신 리눅스서버

리눅스 서버에 최적화된 전용 백신
웹기반으로 어느 PC에서도 서버를 안전하게 운영합니다.



1 리눅스OS에서 사용 가능한 백신 엔진 탑재

터보백신 리눅스서버는 LinuxOS 뿐만 아니라 WindowsOS에서 발생한 악성코드도 탐지 및 제거 가능한 백신 엔진이 탑재되어있습니다.

Linux OS support

2 리눅스서버에 최적화 되어 있는 실시간 감시

리눅스서버를 위협하는 다양한 악성코드를 실시간 감시 기능을 통해 감시하고 치료할 수 있습니다.

Real Scan

3 모든 브라우저 웹 기반 대쉬보드 현황

웹 기반으로 어느 PC에서나 콘솔을 실행 빠르고 더 안전한 통합 관리가 가능하며, 현황까지 빠르게 파악 할 수 있습니다.

Dash board

웹콘솔

- 브라우저에서 백신을 작동/중지/설정/로그 확인

대쉬보드 기능

- 실시간 감시 상태/지원 상태 확인/최근 검사일 확인
- 자동 치료 옵션을 실시간 자동 치료로 변경 가능
- 검역소에 백업된 파일 갯수를 표시해줍니다.
- 이벤트 로그에서 최근 5개 보여주기로 현재 상태 확인
- 백신 업데이트에서 최신 서버 버전과 설치된 버전 확인
- 부팅 시 자동 업데이트 설정 가능
- 라이센스 관리 - 암호화된 라이센스 만료 기간 확인
- 나의 리눅스 OS, CPU 현황, 하드 디스크, 메모리 정보 확인

실시간 감시 기능

- 매우 강력한 실시간 감시 제공(Kernel 2.6.25 이상)
- 시스템에 부하를 주지 않고 서버 자원 사용 최소화 감시

검역소

- 바이러스 백업 파일 확인 / 복원 가능
- 삭제 기능 통한 백업 파일 삭제

환경 설정

- 예약 설정, 바이러스 검사 예외 설정
- 실시간 검사 디렉토리를 지정
- crontab 기능으로 바이러스 검사, 업데이트 예약 설정
- 예외 설정은 바이러스 검사 시 확장자별, 폴더별 설정 가능

수동 검사 기능

- 시스템 자원을 최소하하여 검사.치료 기능 수행
- 폴더 지정하여 수동 검사
- 웹 UI를 통해서 편리하게 바이러스 치료
- 검사 중지/검사 시작 선택 가능
- 검사 현황 확인 가능(치료,삭제 수)
- 감염 파일 치료 상태 확인

이벤트 로그

- 발생한 이벤트를 한 눈에 확인
- 작업/카테고리/기간으로조회
- 실시간, 수동검사, 예약 검사로 이벤트가 기록 되면 각종 설정 이벤트도 조회 가능

권장 시스템

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

분류	사양
웹 콘솔 지원 / 웹브라우저 버전	Internet Explorer 7, 8, 9, 10, 11 / Mozilla Firefox / Google Chrome / Apple Safari 등 모든 브라우저 지원
하드웨어 최소사양	Intel Pentium 코어2듀오 1.8GHz 이상 / 최소 메모리 1GB 이상 / 1GB swap(가상 메모리) 100MB 이상 하드 드라이브 설치 여유 공간 / 4GB 이상 하드 드라이브 운영 여유 공간 권장
터보백신 리눅스 모듈 컴파일 필수 소프트웨어	리눅스 커널 소스와 소프웨어 컴파일 패키지(gcc, binutils, glibc-devel, make, ld) 가 미리 설치

리눅스 지원 OS

※ 터보백신 리눅스서버가 지원하는 OS는 지속적으로 추가를 진행하고 있습니다.

분류: 32/64비트 운영 체제 사양: * Red Hat® Enterprise Linux® 5.0 Server 이상 지원 / * CentOS-5.0 이상 지원 / * Debian GNU/Linux 8.0 이상 / 하모니카

기업의 관리자를 위한

터보백신 매니저

안정적인 중앙 관리 매니저로 각종 보안 위협으로부터
중요한 PC서버 자산을 보호하세요!



1 PC정보관리
및 내부 보안 정책 관리

기업의 IT/PC의 모든 정보를 중앙에서
한번에 확인하고, 매체 제어, 절전 관리,
백신 소프트웨어 관리가 가능합니다.

Manager

2 통합관리&제어
내부 원격 및 메시지 전송

내부 네트워크를 이용해 연결된 에이전트
PC들을 관리하고 원격 지원 및 안내 메시지도
전송이 가능합니다.

Remote

3 내부전체보안
내부 그룹별 관리 설정

내부 보안을 위한 바이러스 백신 관리와
사용자 그룹별 보안 수준을 각각 설정하여
관리가 가능합니다.

Security

내부 PC 자산 관리

- 선택된 에이전트 PC 또는 그룹의 S/W 정보 수집 및 원격제어 지원
- 선택된 에이전트 PC 또는 그룹의 H/W 정보 수집 (IP, MAC 주소, 운영체제 등)
- 선택된 에이전트 PC 또는 그룹의 절전모드를 설정 , 관리

원격 제어 관리

- 서버(Server) → 에이전트(Agent) PC 원격 화면 제어
- 서버(Server) → 에이전트(Agent) PC 간 원격 탐색기를 이용한 파일전송
- 정밀 검사 : 모든 파일과 모든 드라이브를 선택하여 검사
- 서버(Server) → 에이전트(Agent) PC 간 메시지 전송 및 윈도우 원격 종료

보고서 기능

- H/W 목록, 운영체제, 서비스팩, CPU, 하드디스크 등의 정보를 확인, 출력
- 에이전트 PC 또는 그룹에서 최근 검색한 S/W 정보를 확인, 출력

매체 제어

- 이동식 디스크(USB), 네트워크 공유폴더, CD/DVD 등 매체의 읽기/쓰기 기능을 허용 또는 차단하는 기능

내부 보안 백신 관리

- 선택된 에이전트 PC 또는 그룹의 불법 프로그램 차단
- 선택된 에이전트 PC 또는 그룹의 개인 사이트 관리 및 특정 URL 차단 기능

권장 시스템

분류	사양
운영체제	Windows Server 2003, 2008, 2012, 2016
하드웨어	Intel Pentium 1GHz 이상 / 512 이상 / 하드 디스크 여유 공간 최소 250MB 이상 / IPV4, IPV6 네트워크

안티랜섬웨어 솔루션

WhiteDefender 제품 소개

화이트디펜더 제품 라인업

WhiteDefender 라인업



화이트디펜더
PC용 제품



화이트디펜더
Server용 제품



화이트시큐리티센터
중앙 관리자용 제품

Why WhiteDefender?

A) 랜섬웨어를 빠르게 분석하고 대응할 수 있는 기술력을 보유했는가?

B) 랜섬웨어 공격 당한 파일을 바로 복구 할 수 있는가?

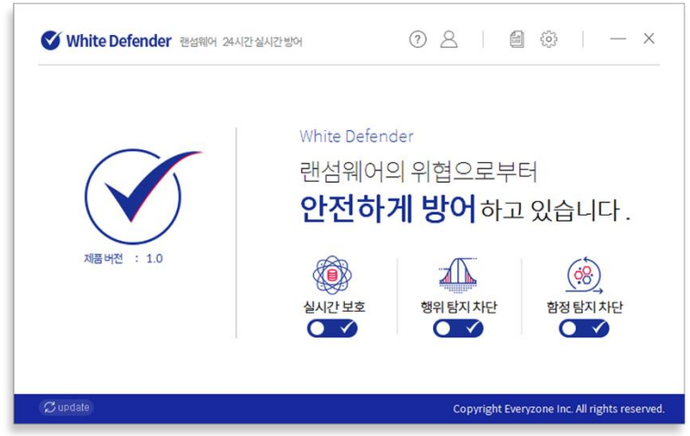
C) 랜섬웨어 진화에 맞춰 지속적인 SW 업데이트 및 패치가 가능한가?

D) 내부 사용중인 SW에 대해 빠른 호환성 해결 지원이 가능한가?

E) PC 설치 후, 2% 미만의 최소 점유율을 차지하는가?

이 모든 질문에 **Yes!** 라고 답할 수 있는
Anti-Ransomware 솔루션

WhiteDefender!



기본 동작 원리

WhiteDefender는 20년 이상 터보백신 개발 경험을 기반으로 에브리존에서 랜섬웨어에 대한 적극적 대응을 목표로 독자 기술로 개발한 3단계 (프로세스 레벨 > 서비스 레벨 > 커널 레벨) 방어 체계를 통해, 랜섬웨어를 실시간으로 모니터링 하면서 차단하여, 알려지지 않은 랜섬웨어를 방어할 수 있는 차세대 안티-랜섬웨어 솔루션입니다.



랜섬웨어에 대한 화이트디펜더 시스템 보호 메커니즘

WhiteDefender는 랜섬웨어의 강력한 대응을 위해 사전 탐지, 함정 탐지, 행위 탐지, 자동 백업/복구, 보호 폴더 등의 보호 메커니즘이 동작하면서 PC에 있는 소중한 데이터를 안전하게 보호합니다.

① 사전 탐지 ② 함정 탐지 ③ 행위 탐지 ④ 자동 백업/복구 ⑤ 보호 폴더

① **사전 탐지 :** 지속적으로 업데이트 되는 랜섬웨어 DB를 활용하여 알려진 랜섬웨어를 사전 탐지하여 차단합니다.

② **함정 탐지 :** 랜섬웨어 행위를 분석하여, 파일 훼손을 유도(함정)하여 탐지, 차단 후 복원합니다.

③ **행위 탐지 :** 랜섬웨어에 의해 파일 훼손이 발생할 경우 실시간으로 행위를 분석하여 탐지합니다.

④ **자동 백업/복구 :** 랜섬웨어에 의해 파일 훼손이 발생할 경우, 순간적으로 파일을 백업 후, 랜섬웨어를 차단하고 안전하게 복구합니다.

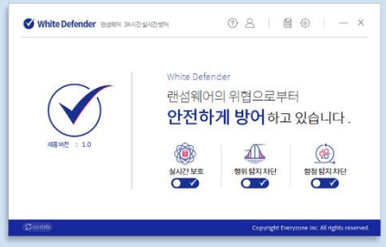
⑤ **보호 폴더 :** 대용량 파일의 경우 보호 폴더(Safezone) 설정을 통해 랜섬웨어의 파일 훼손으로부터 안전하게 보호할 수 있습니다.

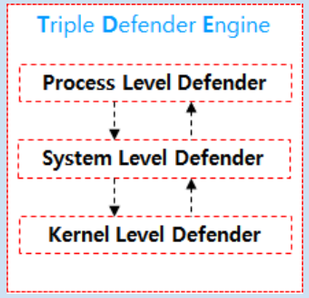
랜섬웨어에 대한 화이트디펜더 대응 프로세스

WhiteDefender의 TD엔진에 의해 랜섬웨어의 모든 행위(Read, Write, Create 등)가 모니터링되며, 파일이 암호화 되는 경우 자동으로 탐지하고 차단합니다. WR엔진은 파일 암호화가 이루어지는 경우 공격이 이루어지는 원본 파일을 순간적으로 안전한 공간에 백업하고, 랜섬웨어 차단이 이루어진 후 파일을 정상적으로 복구하는 기능을 담당합니다.

[랜섬웨어 공격] [화이트디펜더 방어 영역]

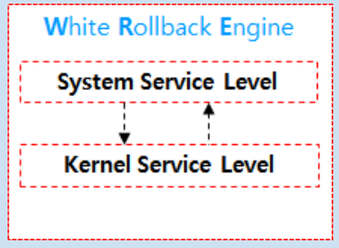
파일 침투	파일 행위	파일 암호화 & 파일 백업	탐지&차단	파일 삭제 & 복구	차단 알림
	PC에서 발생하는 의심 파일의 모든 행위를 모니터링 (동작, 접근영역, 프로세스)	랜섬웨어 공격이 진행될 때, 순간적으로 원본 파일의 백업을 진행	랜섬웨어 파일 암호화 행위를 탐지한 후, 원인 파일의 차단을 진행	랜섬웨어 감염 파일은 삭제하고, 백업된 정상 파일의 복원을 진행	랜섬웨어 대응 로그 기록 및 복원 완료 알림 진행





주요 기술 (1) TD 엔진
랜섬웨어의 다양한 공격 행위를
실시간으로 모니터링하고
분석하여 방어하는 탐지 엔진

+



주요 기술 (2) WR 엔진
랜섬웨어 공격 발생 시
순간적으로 파일을 백업하고
복구하는 복원 엔진

화이트디펜더 주요 기능 및 특장점

WhiteDefender는 랜섬웨어의 강력한 대응을 위해 사전 탐지, 함정 탐지, 행위 탐지, 자동 백업/복구, 보호 폴더 등의 보호 메커니즘이 동작하면서 PC에 있는 소중한 데이터를 안전하게 보호합니다.

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

GS 품질 인증서 1등급


1등급

소프트웨어품질인증서

Certificate of Software Quality

상호 또는 성명 : 주)에브리존(220-81-67981) EVERYZONE Co.,Ltd.

소프트웨어의 명칭 : 화이트 디펜더 V1.0 White Defender V1.0

인증등급 : 1등급

인증번호 : 18-0473

제조자 및 제조국가 : 주)에브리존/대한민국 EVERYZONE Co.,Ltd./Republic of Korea

인증연월일 : 2018년(Year) 9월(Month) 17일(Day)

기타 :

위 소프트웨어는 「소프트웨어산업 진흥법 시행규칙」 제5조제1항에 따라 인증되었음을 증명합니다.

I hereby confirm that the quality of the foregoing software has been certified under Article 5.1 of the Enforcement Decree of the Software Industry Promotion Act.

2018 년(Year) 9 월(Month) 17 일(Day)

TTA 한국정보통신기술협회장

CEO & President

Telecommunications Technology Association

안티랜섬웨어 실시간 보호

화이트디펜더 PC용 제품

랜섬웨어 위협을 실시간으로 모니터링 하고
알려지지 않은 신종 랜섬웨어까지 방어할 수 있습니다.



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 기반으로 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.

함정 탐지 기능

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.



세부품명 : 보안소프트웨어 (4323320501)

규격 : 보안소프트웨어, 에브리존, 화이트 디펜더 V1.0 (White Defender V1.0) 1년갱신

식별번호 : 23536131 3자단가계약

회사명 : (주)아이티로그인 [중소기업]

원산지 : 대한민국

계약종료일 : 2023/05/20 | 납품기한 :30일(납품요구일로부터)

현장설치도 | 전지역

우선구매대상 : 해당 없음

의무구매대상 : 해당 없음

36,600 원

조



세부품명 : 보안소프트웨어 (4323320501)

규격 : 보안소프트웨어, 에브리존, 화이트 디펜더 V1.0(White Defender V1.0), 100~499copy

식별번호 : 23499972 3자단가계약

회사명 : (주)아이티로그인 [중소기업]

원산지 : 대한민국

계약종료일 : 2023/05/20 | 납품기한 :30일(납품요구일로부터)

현장설치도 | 전지역

우선구매대상 : 해당 없음

의무구매대상 : 해당 없음

49,200 원

조



세부품명 : 보안소프트웨어 (4323320501)

규격 : 보안소프트웨어, 에브리존, 화이트 디펜더 V1.0(White Defender V1.0), 1~99copy

식별번호 : 23499971 3자단가계약

회사명 : (주)아이티로그인 [중소기업]

원산지 : 대한민국

계약종료일 : 2023/05/20 | 납품기한 :30일(납품요구일로부터)

현장설치도 | 전지역

우선구매대상 : 해당 없음

의무구매대상 : 해당 없음

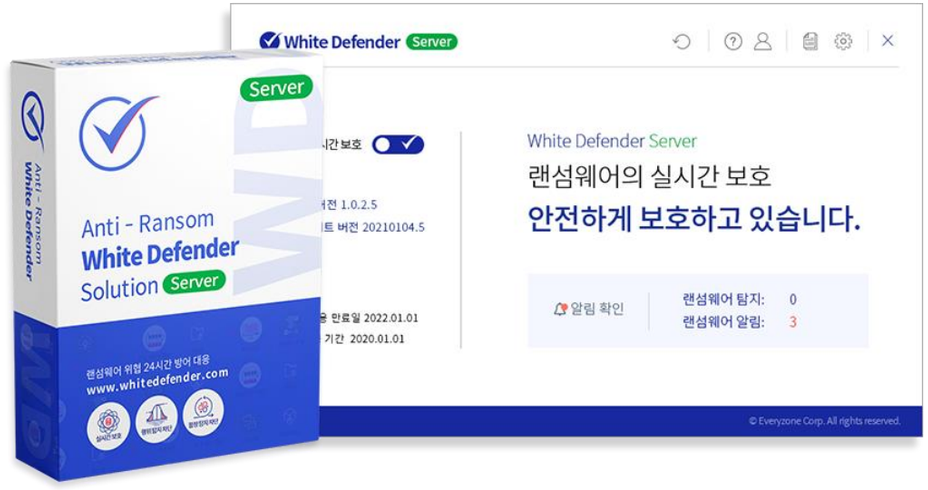
55,000 원

조

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

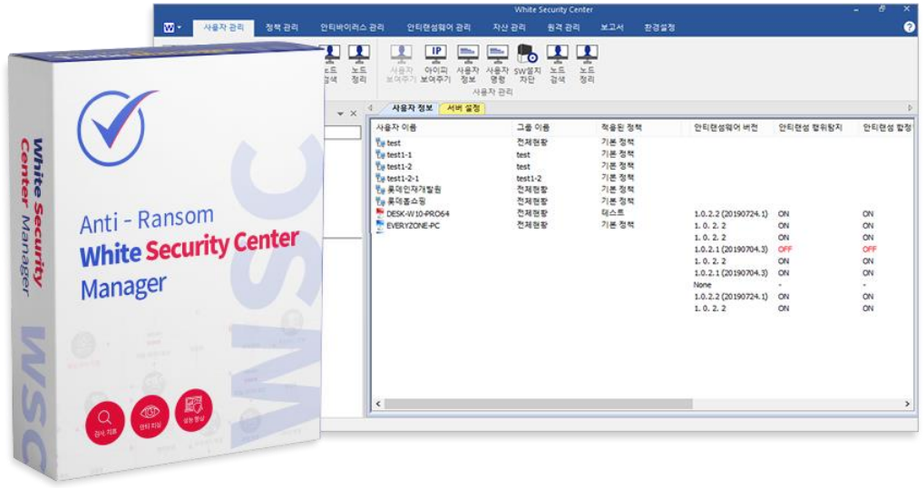
※ 방화벽을 통해 프로그램의 기본 통신이 차단되는 경우, 정상적인 업데이트가 동작하지 않을 수 있습니다.

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

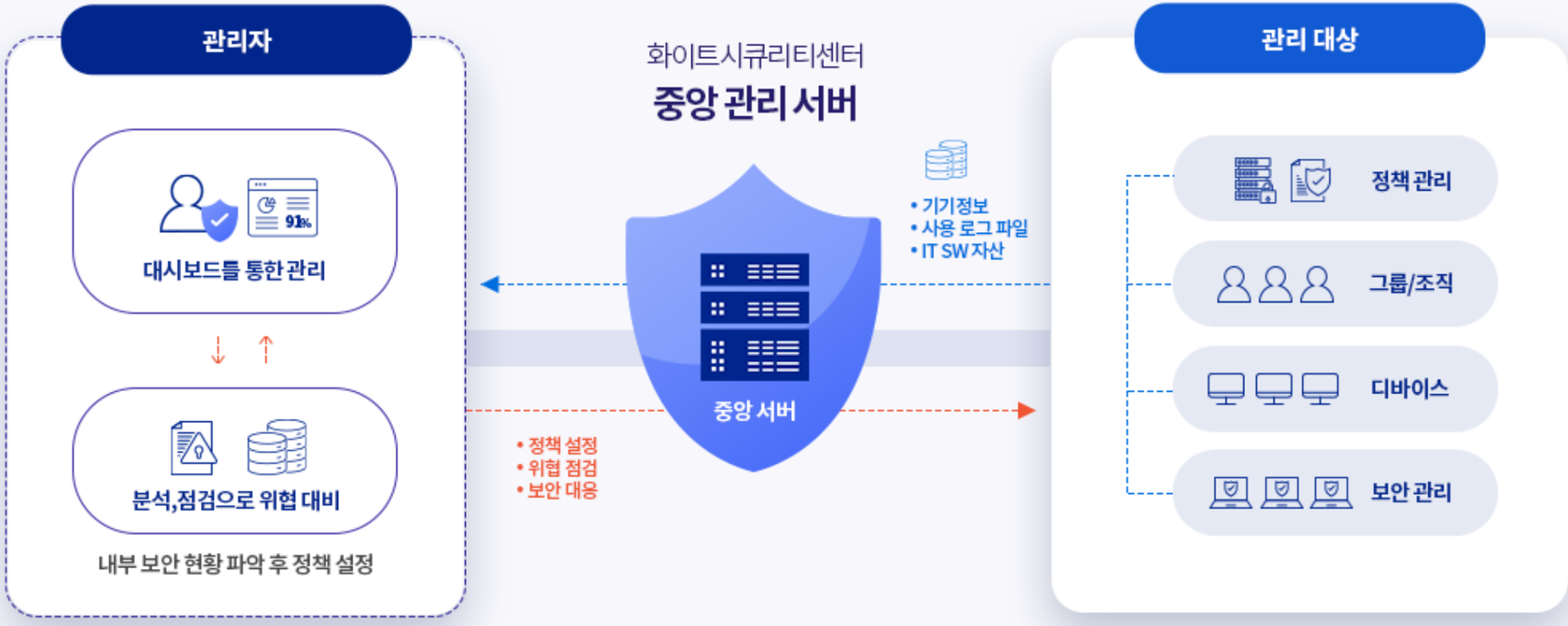
화이트시큐리티 센터 구성관리자가 사용할 수 있는 웹 기반의 관리 콘솔과 중앙 서버, 에이전트로 구성됩니다.

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(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)

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

안티랜섬웨어 솔루션

WhiteDefender 레퍼런스

많은 기업들이 화이트디펜더를 도입하여 랜섬웨어 위협으로부터 스마트하게 대응하고 있습니다.

롯데하이마트 | MBC | 7-ELEVEN | 한국소프트웨어저작권협회

KTNET 주식회사 한국무역정보통신 | 롯데컬처웍스 | Carrier 캐리어에어컨 | 롯데홈쇼핑

sb 성북구 도시관리공단 | RAPA 한국전파진흥협회 Korea Radio Promotion Association | 롯데유통사업본부 | 행정안전부

한일단조공업(주) | Canon | 동구바이오제약 | 롯데인재개발원

부산도서관 | LOTTE DUTY FREE

기업 外 300여개

안티랜섬웨어 차단 솔루션 화이트디펜더

www.WhiteDefender.com

Thank You