보안인증 | GS인증 | 중소기업 기술마켓 | 조달 등록 | 시범구매 제품 인증

Anti-Ransomware Solution

화이트디펜더

랜섬웨어 예방 및 대응 솔루션

행위 탐지 랜섬웨어 차단 솔루션

WhiteDefender

PC Client

www.whitedefender.com

Everyzone | Digital SECURITY Company

1. 화이트디펜더란?

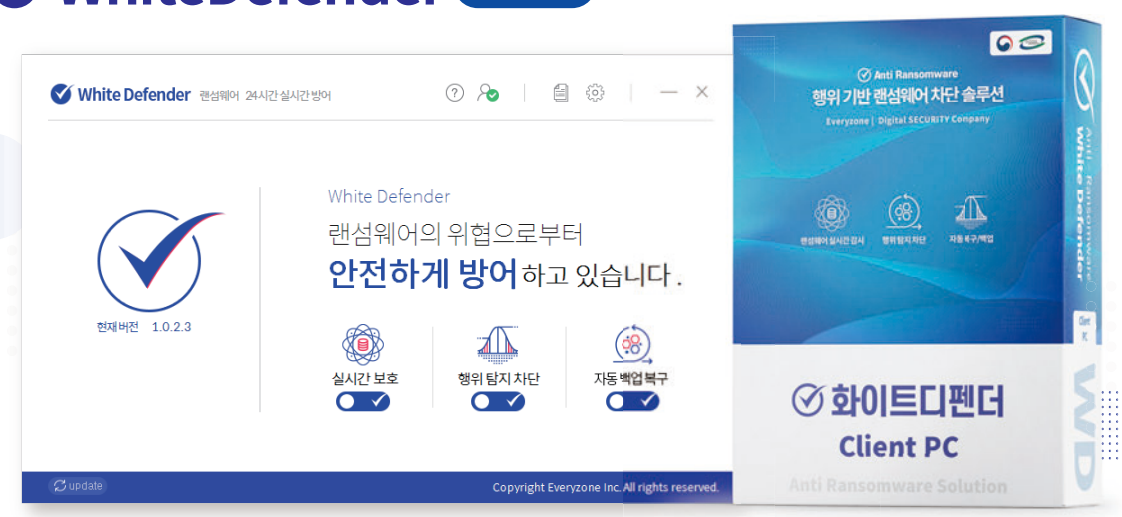
100% 행위 탐지 랜섬웨어 차단 대응 예방 솔루션입니다.

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.

랜섬웨어 위협 24시간 대응!

WhiteDefender PC



국가정보원 보안기능확인서 | GS1등급 | 중소기업 기술마켓 | 조달 등록 | 시범구매 제품 인증

화이트디펜더 랜섬웨어 대응 프로세스

화이트디펜더는 **TD엔진(행위 탐지 차단 기술)**에 의해 **랜섬웨어의 모든 행위(Read, Write, Create 등)가 모니터링되며,** 파일이 암호화되는 경우 자동으로 탐지하고 차단합니다. **WR엔진(백업, 복구 기술)**은 파일 암호화가 이루어지는 경우 공격이 이루어지는 원본 파일을 **순간적으로 안전한 공간에 백업**하고, 랜섬웨어 차단이 이루어진 후 **파일을 정상적으로 복구**하는 기능을 담당합니다.

랜섬웨어 공격

랜섬웨어 공격
공격이 발생하는 모든 의심 파일을 모니터링 (동작, 접근, 프로세스)

파일 암호화
랜섬웨어 공격이 진행되며 모든 파일 암호화 진행

화이트디펜더 랜섬웨어 방어 영역

탐지&차단
랜섬웨어 파일 암호화 행위 탐지 후 원인 파일 차단 진행

감염 파일 삭제/복구
감염 파일 삭제 후 백업된 정상 파일 복구 진행

차단 알림
랜섬웨어 대응 로그 기록 및 복원 완료 알림 진행

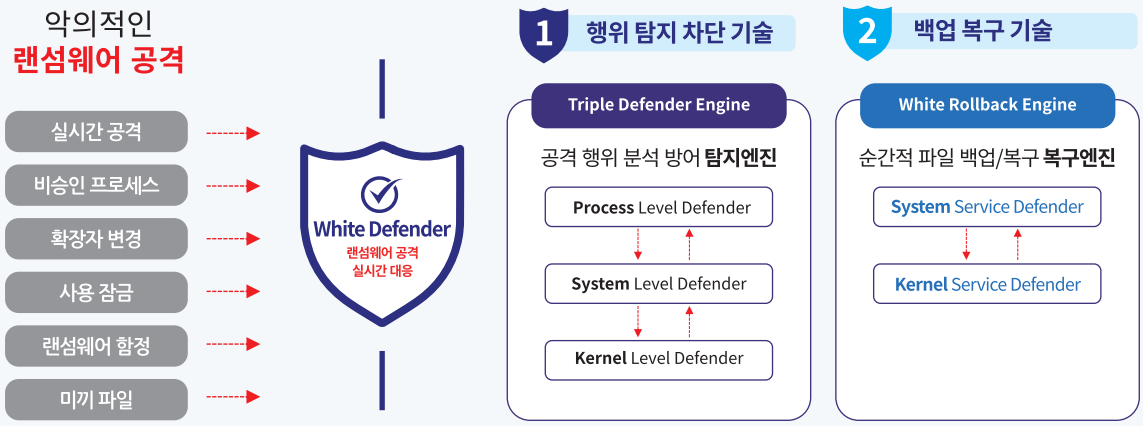
2. 화이트디펜더의 핵심 동작 원리는?

독자 개발한 랜섬웨어 탐지 - 차단 - 복구 알고리즘 기술입니다.

화이트디펜더 Triple Defender엔진 & White Rollback 엔진으로 안전하게 **대응**합니다.

랜섬웨어 위협에 대한 적극적 대응을 목표로 **독자 기술로 개발**한 **3단계 (프로세스 레벨 > 서비스 레벨 > 커널 레벨) 방어 체계**를 통해 랜섬웨어를 실시간으로 모니터링 하면서 차단하고, 알려지지 않은 랜섬웨어를 방어할 수 있는 차세대 안티랜섬웨어 솔루션입니다.

2개의 랜섬웨어 탐지 엔진



1 행위 탐지 차단 기술

- **랜섬웨어 공격 행위를 실시간으로 모니터링 하고 분석/방어하는 탐지 엔진**
- 시스템 상에서 실행 프로세스 및 기존 프로세스에 인젝션 (injection)된 다른 프로세스와 Script 형태로 실행되는 형태들이 의심 행위로 분류가 되면 해당 의심 행위들을 분석 및 판단을 진행함
- 최종 탐지 및 차단 진행시 랜섬웨어 의심 행위로 삭제될 파일은 삭제 후 복원소로 이동시킴

2 백업 복구 기술

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

100% 행위 탐지 랜섬웨어 차단 탐지 및 복구 기술

화이트디펜더 경우 엔드포인트 內 직접 동작하여 사용자, 관리자가 직접 알림을 확인 할 수 있어 빠른 대응이 가능합니다.

※ 화이트디펜더가 독자 개발한
랜섬웨어 탐지-차단-복구 알고리즘 기술

WhiteDefender
제품 Line UP

기업을 안전하게 보호할 수 있는 최적의 랜섬웨어 차단 솔루션 제품 라인업입니다.

화이트디펜더 Client
클라이언트 PC를 위한 안티랜섬웨어

화이트디펜더 Server
윈도우 Server 전용 안티랜섬웨어

화이트 시큐리티 센터 구축형
관리자를 위한 중앙 관리 솔루션

WhiteDefender
사용 환경

기업의 내부 정책에 따라 최적의 조건으로 유연하게 구축할 수 있도록 지원합니다.
화이트디펜더의 안정적인 보안 환경 구축과 설치 및 활용을 위한 권장 사양은 다음과 같습니다.

화이트디펜더 Client

OS	MS Windows 7 SP1 이상 / 8 / 8.1 / 10 / 11
CPU	Intel Pentium Core i3 2GHz 이상
RAM	권장 메모리 4 GB 이상
HDD	10 GB 이상의 여유 공간 (백업 기능 지원은 시스템 여유 공간에 따르므로 상이함)
Network	IPv4, IPv6 네트워크 환경 권장 *중앙관리용 WSC 서버 연동 권장

화이트디펜더 Server

OS	MS Windows Server 2008 R2 SP1 이상 (64비트)
CPU	Intel Xeon Dual Core 이상
RAM	권장 메모리 4GB 이상
HDD	10 GB 이상의 여유 공간 (백업 기능 지원은 시스템 여유 공간에 따르므로 상이함)
Network	IPv4, IPv6 네트워크 환경 권장 *중앙관리용 WSC 서버 연동 권장

화이트 시큐리티 센터 구축형

제품 구성	관리 서버 + 관리 콘솔 + 에이전트
관리 서버	Linux RHEL 8.x / 9.x 기반 구성 + PostgreSQL DB 15.x 구성
관리 콘솔	윈도우 기반 OS 상 설치 : 관리 정책 및 운영 상태 확인
에이전트	화이트디펜더 제품군 설치 PC 및 서버에 설치 연동 진행

WhiteDefender
레퍼런스

주요 기관
행안부 - 스마트워크센터, 국회도서관, 부산도서관, 성북구도시관리공단, 부산시설공단, 인천시설공단
한국장애인문화예술원, 서울도시철도그린환경, 부산도시공사, 국가과학기술인력개발원, 광주광역시교육청

주요 기업
롯데하이마트, 롯데컬처웍스, 롯데면세점, 롯데캐논 , 롯데홈쇼핑, (주)한국무역정보통신
동국제약, 이원의료재단, 건일제약, 동구바이오제약, 세븐일레븐, 한국제강, 그린케미칼
오텍캐리어, MBC, 현대에이치티, 한일단조공업(주), 롯데호텔, 한국소프트웨어저작권협회
한국전파진흥원, 롯데제과, 롯데글로벌로지스, 롯데건설, 롯데월드, 고려특수선재

검색창에 “화이트디펜더”를 검색하시면, 랜섬웨어 정보를 확인 할 수 있습니다.
화이트디펜더

(주)에브리존 | 화이트디펜더
본사 : 서울 마포구 마포대로 136 지방재정회관
대표전화 : 02-3274-2700 / fax : 02-3274-2709
www.whitedefender.com
Copyright ⓒEveryzone. All rights reserved

▼ 공식 사이트 QR

보안인증 | GS인증 | 중소기업 기술마켓 | 조달 등록 | 시범구매 제품 인증

Anti-Ransomware Solution

화이트디펜더

랜섬웨어 예방 및 대응 솔루션

행위 탐지 랜섬웨어 차단 솔루션

WhiteDefender

Window Server

www.whitedefender.com

Everyzone | Digital SECURITY Company

1. 화이트디펜더 Window Server란?

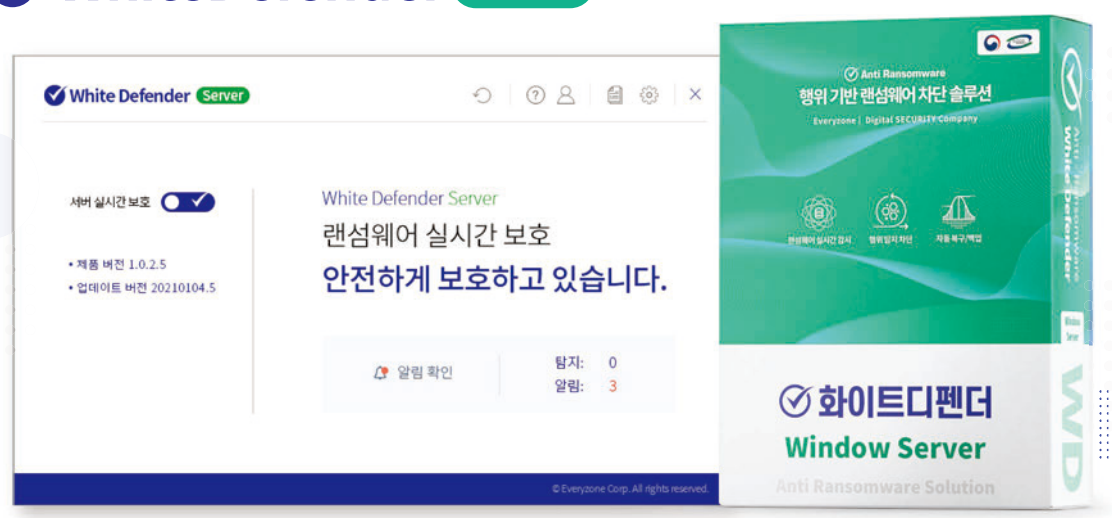
100% 행위 탐지 랜섬웨어 차단 대응 예방 솔루션입니다.

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.

윈도우 서버 랜섬웨어 위협 24시간 대응!

WhiteDefender Server



국가정보원 보안기능확인서 | GS1등급 | 중소기업 기술마켓 | 조달 등록 | 시범구매 제품 인증

화이트디펜더 랜섬웨어 대응 프로세스

화이트디펜더는 **TD엔진(행위 탐지 차단 기술)**에 의해 **랜섬웨어의 모든 행위(Read, Write, Create 등)가 모니터링되며,** 파일이 암호화되는 경우 자동으로 탐지하고 차단합니다. **WR엔진(백업, 복구 기술)**은 파일 암호화가 이루어지는 경우 공격이 이루어지는 원본 파일을 **순간적으로 안전한 공간에 백업**하고, 랜섬웨어 차단이 이루어진 후 **파일을 정상적으로 복구**하는 기능을 담당합니다.

서버 랜섬웨어 공격

랜섬웨어 공격	파일 암호화
공격이 발생하는 모든 의심 파일을 모니터링 (동작, 접근, 프로세스)	랜섬웨어 공격이 진행되며 모든 파일 암호화 진행

화이트디펜더 랜섬웨어 방어 영역

탐지&차단	감염 파일 삭제/복구	차단 알림
랜섬웨어 파일 암호화 행위 탐지 후 원인 파일 차단 진행	감염 파일 삭제 후 백업된 정상 파일 복구 진행	랜섬웨어 대응 로그 기록 및 복원 완료 알림 진행

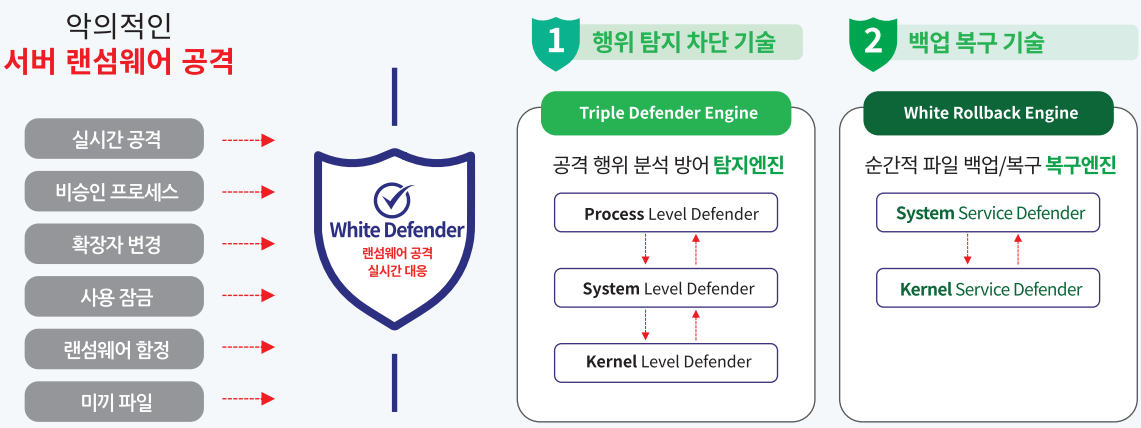
2. 화이트디펜더 Window Server의 핵심 동작 원리는?

독자 개발한 랜섬웨어 탐지 - 차단 - 복구 알고리즘 기술입니다.

화이트디펜더 Triple Defender엔진 & White Rollback엔진으로 안전하게 **대응**합니다.

랜섬웨어 위협에 대한 적극적 대응을 목표로 **독자 기술로 개발**한 **3단계 (프로세스 레벨 > 서비스 레벨 > 커널 레벨) 방어 체계**를 통해 랜섬웨어를 실시간으로 모니터링 하면서 차단하고, 알려지지 않은 랜섬웨어를 방어할 수 있는 차세대 안티랜섬웨어 솔루션입니다.

2개의 랜섬웨어 탐지 엔진



1 행위 탐지 차단 기술

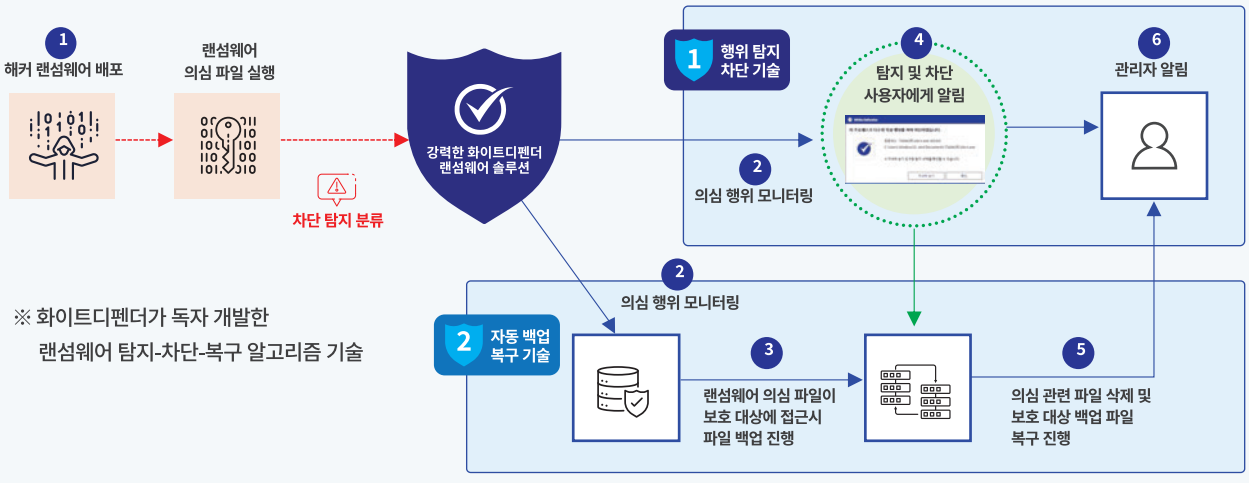
- **랜섬웨어 공격 행위를 실시간으로 모니터링 하고 분석/방어하는 탐지 엔진**
- 시스템 상에서 실행 프로세스 및 기존 프로세스에 인젝션(injection)된 다른 프로세스와 Script 형태로 실행되는 형태들이 의심 행위로 분류가 되면 해당 의심 행위들을 분석 및 판단을 진행함
- 최종 탐지 및 차단 진행시 랜섬웨어 의심 행위로 삭제될 파일은 삭제 후 복원소로 이동시킴

2 백업 복구 기술

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

100% 행위 탐지 랜섬웨어 차단 탐지 및 복구 기술

화이트디펜더 경우 엔드포인트 內 직접 동작하여 사용자, 관리자가 직접 알림을 확인 할 수 있어 빠른 대응이 가능합니다.



※ 화이트디펜더가 독자 개발한
랜섬웨어 탐지-차단-복구 알고리즘 기술

WhiteDefender
제품 Line UP

기업을 안전하게 보호할 수 있는 최적의 랜섬웨어 차단 솔루션 제품 라인업입니다.

화이트디펜더 Client
클라이언트 PC를 위한 안티랜섬웨어

화이트디펜더 Server
윈도우 Server 전용 안티랜섬웨어

화이트 시큐리티 센터 구축형
관리자를 위한 중앙 관리 솔루션

WhiteDefender
사용 환경

기업의 내부 정책에 따라 최적의 조건으로 유연하게 구축할 수 있도록 지원합니다.
화이트디펜더의 안정적인 보안 환경 구축과 설치 및 활용을 위한 권장 사양은 다음과 같습니다.

화이트디펜더 Client

OS	MS Windows 7 SP1 이상 / 8 / 8.1 / 10 / 11
CPU	Intel Pentium Core i3 2GHz 이상
RAM	권장 메모리 4 GB 이상
HDD	10 GB 이상의 여유 공간 (백업 기능 지원은 시스템 여유 공간에 따르므로 상이함)
Network	IPv4, IPv6 네트워크 환경 권장 *중앙관리용 WSC 서버 연동 권장

화이트디펜더 Server

OS	MS Windows Server 2008 R2 SP1 이상 (64비트)
CPU	Intel Xeon Dual Core 이상
RAM	권장 메모리 4GB 이상
HDD	10 GB 이상의 여유 공간 (백업 기능 지원은 시스템 여유 공간에 따르므로 상이함)
Network	IPv4, IPv6 네트워크 환경 권장 *중앙관리용 WSC 서버 연동 권장

화이트 시큐리티 센터 구축형

제품 구성	관리 서버 + 관리 콘솔 + 에이전트
관리 서버	Linux RHEL 8.x / 9.x 기반 구성 + PostgreSQL DB 15.x 구성
관리 콘솔	윈도우 기반 OS 상 설치 : 관리 정책 및 운영 상태 확인
에이전트	화이트디펜더 제품군 설치 PC 및 서버에 설치 연동 진행

WhiteDefender
레퍼런스

주요 기관
행안부 - 스마트워크센터, 국회도서관, 부산도서관, 성북구도시관리공단, 부산시설공단, 인천시설공단
한국장애인문화예술원, 서울도시철도그린환경, 부산도시공사, 국가과학기술인력개발원, 광주광역시교육청

주요 기업
롯데하이마트, 롯데컬처웍스, 롯데면세점, 롯데캐논 , 롯데홈쇼핑, (주)한국무역정보통신
동국제약, 이원의료재단, 건일제약, 동구바이오제약, 세븐일레븐, 한국제강, 그린케미칼
오텍캐리어, MBC, 현대에이치티, 한일단조공업(주), 롯데호텔, 한국소프트웨어저작권협회
한국전파진흥원, 롯데제과, 롯데글로벌로지스, 롯데건설, 롯데월드, 고려특수선재

검색창에 "화이트디펜더"를 검색하시면, 랜섬웨어 정보를 확인 할 수 있습니다.
화이트디펜더

(주)에브리존 | 화이트디펜더
본사 : 서울 마포구 마포대로 136 지방재정회관
대표전화 : 02-3274-2700 / fax : 02-3274-2709
www.whitedefender.com
Copyright ⓒEveryzone. All rights reserved

▼ 공식 사이트 QR