IT Login White Defender EVERYZONE

# 학내망, 공공을 위한
# 보안소프트웨어
# 랜섬웨어 솔루션
# 조달 품목 리스트

# 차세대 랜섬웨어 대응 솔루션 화이트 디펜더!

# White Defender

1등급

GOOD Software

랜섬웨어 위협 24시간 대응!


## 갈수록 진화하는 랜섬웨어 공격!
## White Defender로 안전하게 보호할 수 있습니다!

- 랜섬웨어 공격 실시간 대응 및 방어
- 사전 탐지를 통한 1차 방어
- 행위 탐지를 통한 2차 방어
- 순간 백업/복구를 통한 파일 보호 3차 방어

# 주요 특징

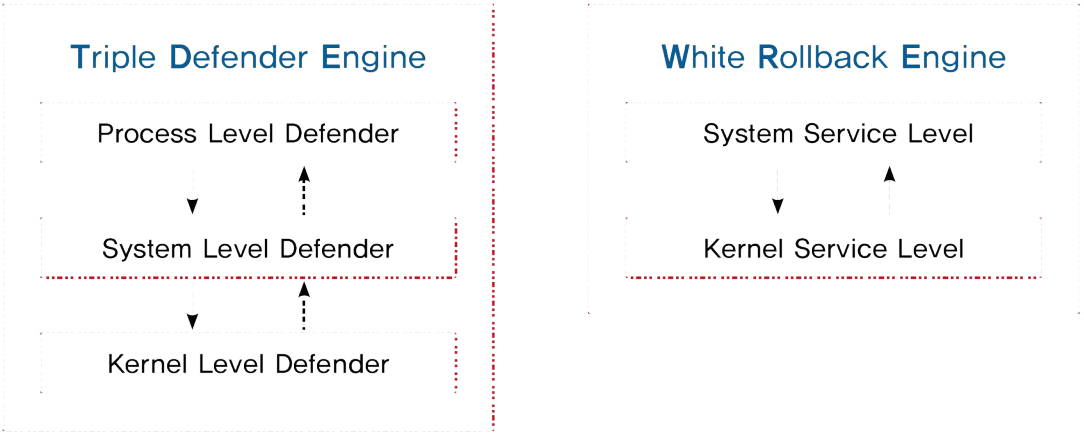
## 01 랜섬웨어 보호 메커니즘

White Defender는 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** : 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.

## 02 강력한 탐지 엔진 및 순간 복구 엔진

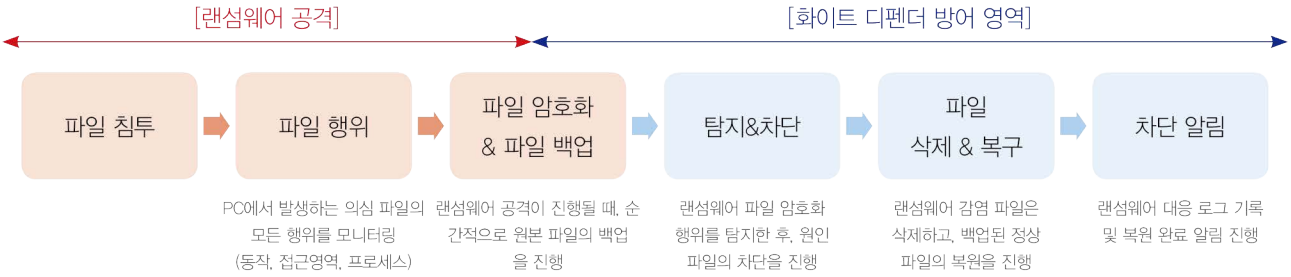
White Defender의 핵심 엔진 기술은 TDE 와 WRE 입니다. 에브리존의 독자 기술로 개발한 2개의 엔진이 유기적으로 협력하여 다양한 랜섬웨어로부터 시스템을 안전하게 보호하며, 강력한 탐지 기능으로 알려지지 않은 랜섬웨어 공격도 방어가 가능합니다.




a) **TD엔진** : 랜섬웨어의 다양한 공격 행위를 실시간으로 모니터링하고 분석하여 방어하는 탐지 엔진입니다.
b) **WR엔진** : 랜섬웨어 공격 발생시 순간적으로 파일을 백업하고 복구하는 복원 엔진입니다.

## 03 랜섬웨어 대응 프로세스

White Defender의 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.




[White Defender TD엔진 & WR 엔진 특징]

① **비확장자 기반의 행위 탐지** : 등록된 확장자를 보호하는 방식이 아닌, 기본적으로 모든 확장자를 모니터링하고 보호할 수 있음

② **암호화된 모든 파일 복구** : 일부 제품은 랜섬웨어 공격이 발생할 때, 랜섬웨어 공격으로 인지하는 임계치가 있어서, 임계치 안에 있는 파일을 복구를 할 수 없으나, 화이트 디펜더는 모든 파일의 복구가 가능함

## 제품 비교

**White Defender는 랜섬웨어에 대한 강력한 대응을 위해 사전 탐지, 함정 탐지, 행위 탐지, 자동 백업/복구, 보호 폴더 등의 보호 메커니즘이 동작하면서 PC에 있는 소중한 데이터를 안전하게 보호합니다.**

| 기능 구분 | C사 | White Defender |
|---|---|---|
| 행위 기반 인식 및 치료 | 지원 | 지원 |
| 보호 확장자 수 | 500개 제한 | 제한 없음 |
| 미끼 파일 탐지 | 지원 | 지원 |
| 비서명 파일 실행 탐지 | – | 지원 |
| 프로그램 자체보호 | 지원 | 지원 |
| MBR 보호 | 지원 | 지원 |
| 손상 파일 자동 복구 | 지원 | 지원 |
| 파일 이력 관리 | 지원 | 지원 |
| 백업 폴더 지원 | 지원 | 지원 |
| 보호 폴더 접근 탐지 | 지원 | 지원 |
| 스크립트 파일 생성 차단 | – | 지원 |
| 블랙리스트 차단 | – | 지원 |
| 화이트리스트 차단 | – | 지원 |

# 주요 기능

## 01 기본 기능

White Defender는 실시간 보호, 행위 탐지, 함정 탐지 등의 기능 통해, 랜섬웨어를 사전에 탐지하여 차단하며, 랜섬웨어가 암호화를 진행할 경우, 순간적으로 원본 파일을 백업하고, 차단 후 암호화된 파일을 복원하는 행위를 통해 데이터를 안전하게 보호합니다.

**White Defender는 실시간 보호?**

랜섬웨어 위협에 빠르게 대응하도록 실시간 방어 체계를 제공합니다.

a) 실시간 보호

**행위 탐지 차단?**

위험한 랜섬웨어 행위에 대한 내용을 지속적으로 수집하고 개선합니다.

b) 행위 탐지 차단

**함정 탐지 차단?**

랜섬웨어의 함정에 빠지지 않도록 정확한 탐지를 위해 멈추지 않습니다.

c) 함정 탐지 차단

## 02 추가 기능

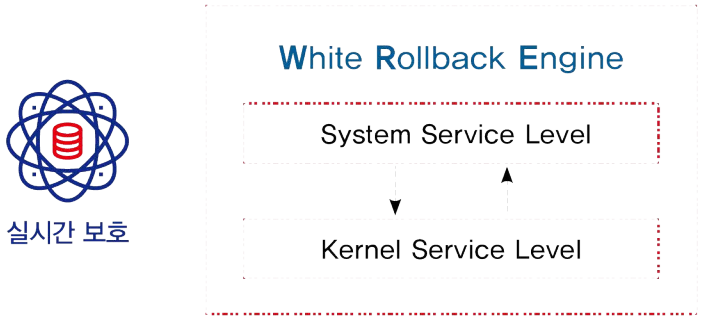
White Defender는 랜섬웨어 대응을 위해 실시간 보호, 행위 탐지, 함정 탐지 기능 외에도 다양한 기능들 제공하여 PC에 있는 소중한 데이터를 안전하게 보호합니다.

| 기능 구분 | 내용 |
|---|---|
| **자체 보호** | 프로세스, 폴더, 레지스트리 손상을 보호 |
| **새도우 복사본 보호** | 복원에 사용되는 정보에 접근하는 경우 차단 |
| **E-Mail 저장소 보호** | 대용량의 E-Mail 파일을 랜섬웨어로부터 보호 |
| **비서명 프로세스 실행 알림/차단** | 서명되지 않은 파일이 실행이 되는 경우, 알림을 통해 허용, 차단, 예외 처리 가능 |
| **스크립터 파일 생성 차단** | 스크립터에 의해서 파일이 생성이 되는 경우 차단 |
| **복원용 저장 파일 삭제** | 설정한 기간 동안 탐지된 복원용 파일을 저장하며, 이 후 날짜 데이터는 자동 삭제 |
| **행위 탐지 복원 저장 파일** | 설정한 파일보다 큰 경우, 행위 탐지 복원 파일 저장에서 제외하는 기능 (최대 100MB) |

# 기능 설명

## 01 순간 백업/복구 기능

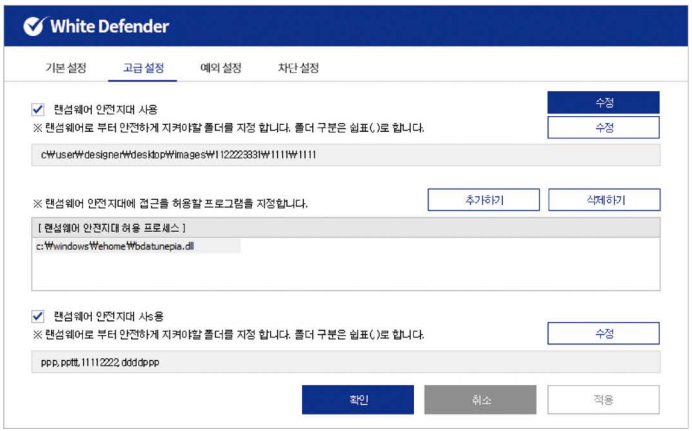
White Defender는 랜섬웨어에 의해 중요 파일이 공격을 당하는 경우, 암호화 되기 전 WR엔진이 동작하여 원본 파일을 순간적으로 안전한 곳에 백업을 하며, 랜섬웨어에 의해 암호화된 파일들이 삭제된 후 안전하게 복원이 됩니다.




화이트디펜더의 핵심 기능으로 WRE에서 담당합니다.
TDE에서 모니터링시 랜섬웨어 공격으로 인해 파일 훼손 행위가 발생할 경우, 순간적으로 파일을 백업합니다.
백업된 파일은 WRE에 의해 안전한 장소에 저장이 되며, 랜섬웨어 공격을 차단한 후, 원래의 위치로 정상적으로 복원이 됩니다.

## 02 보호 폴더 기능

White Defender는 순간적인 백업/복구를 위해 100MB 미만의 파일들을 우선적으로 보호합니다.
대용량의 파일을 보호하기 위해서 보호 폴더 기능을 제공합니다.




대용량의 파일을 랜섬웨어로부터 보호하기 위해 제공되는 기능입니다.
임의로 폴더를 지정한 후, 접근 가능한 프로세스를 등록합니다.
지정된 폴더는 등록한 프로세스만 접근이 가능하여, 랜섬웨어로부터 안전하게 보호할 수 있습니다.

# 제품 개요

## 01 Why White Defender?

a) 랜섬웨어를 빠르게 분석하고 대응할 수 있는 기술력을 보유했는가?

b) 랜섬웨어 공격 시 파일을 정상적으로 복구할 수 있는가?

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

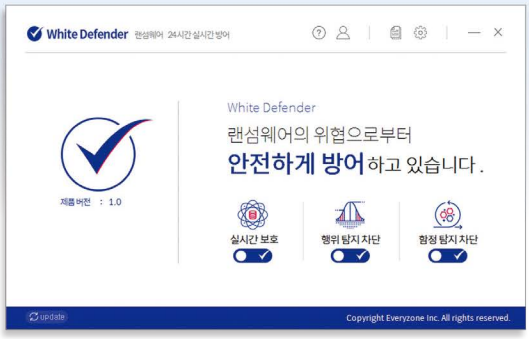
d) 내부 사용 중인 SW에 대해 빠른 호환성 해결 지원이 가능한가?

e) PC를 사용하는데, 2% 미만의 최소 점유율로 운용되는가?

이 모든 질문에 *yes!* 라고 답할 수 있는

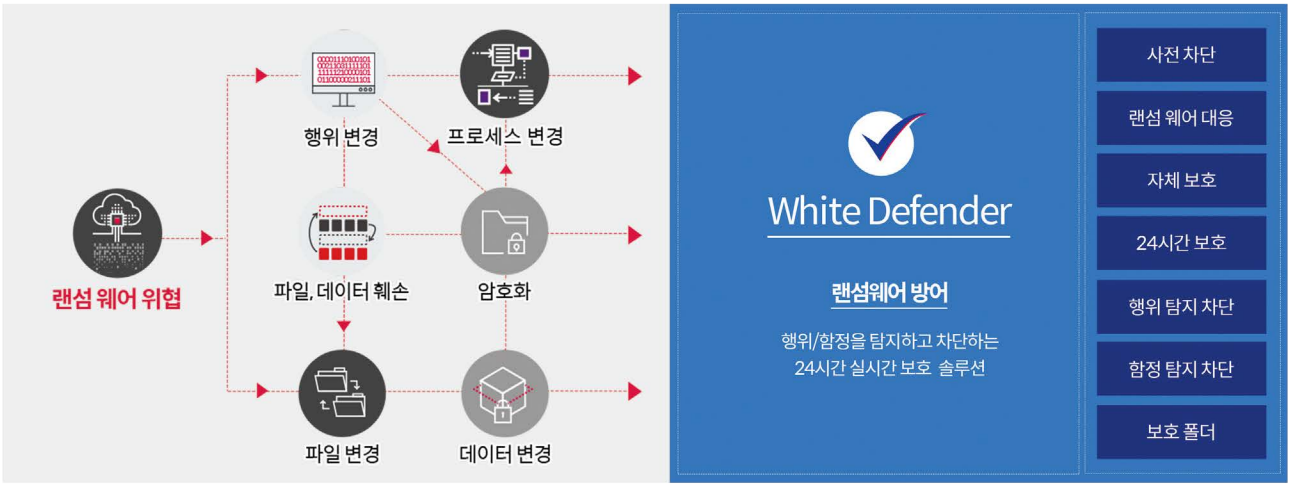
Anti-Ransomware 솔루션

**White Defender**




## 02 기본 동작 원리

White Defender는 3단계 (프로세스 레벨 > 서비스 레벨 > 커널 레벨) 방어 체계를 통해, 랜섬웨어를 실시간으로 모니터링 하면서 차단하며, 알려지지 않은 랜섬웨어를 방어할 수 있는 차세대 안티-랜섬웨어 솔루션입니다.



# 사용 환경

| [1] 시스템 최소 사양 | |
|---|---|
| OS | MS Windows 7 SP1 / 8 / 8.1 / 10 |
| CPU | Intel Pentium Core 2 Duo 2GHz 이상 |
| RAM | 2 GB 이상 |
| HDD | 프로그램 기본 설치 20 MB 이상 (백업 기능 지원은 시스템 여유 공간에 따르므로 상이함) |

| [2] 시스템 권장 사양 | |
|---|---|
| OS | MS Windows 7 SP1 / 8 / 8.1 / 10 |
| CPU | Intel Pentium Core i3 2GHz 이상 |
| RAM | 4 GB 이상 |
| HDD | 10 GB 이상의 여유 공간 |

# 보안소프트웨어, 에브리존, 화이트 디펜더 V1.0 (White Defender V1.0)

1년갱신형

물품식별번호 **23536131** 조달등록가격 **₩36,600**

영구형 1~99사용자

물품식별번호 **23499971** 조달등록가격 **₩55,000**

영구형 100~499사용자

물품식별번호 **23499972** 조달등록가격 **₩49,200**

| 제조사 | | |
|---|---|---|
| 인증 | | GS인증 1등급 인증번호 18-0473 |
| 권장 설치사양 | CPU | Intel Core i3 2.6Ghz 이상 |
| | 메모리 | 4GB이상 |
| | 디스크 여유 공간 | 설치 100MB 이상 확보 권장 |
| | 운영 | 운영 5GB 이상 확보 권장 |
| 설치 운영사양 | 1. 지원 OS(운영체제) | – Windows 7 SP1 이상 (32비트 / 64비트 지원)<br>– Windows 8 / 8.1 (32비트 / 64비트 지원)<br>– Windows 10 (32비트 / 64비트 지원) |
| | 2. 지원 웹 브라우저 | – Internet Explorer 8 이상,<br>– Chrome, FireFox, Edge 등 |

## 주요 구매기관

- 행안부 – 스마트워크센터

## 제품특징

- 랜섬웨어 행위/사전/함정 탐지 기능
- 랜섬웨어 사전 자동 백업/복구 기능
- 보호 폴더(안전지대) 기능
- 섀도우 복사본(볼륨 스냅샷 서비스) 보호
- E-Mail 저장소 보호 (MS Outlook)
- 비서명 프로세스 알림 및 차단
- 스크립터 위험 행위 차단
- 네트워크 위치로부터 내 컴퓨터에 파일 쓰기 차단


조달 총판

**(주)아이티로그인**

서울시 용산구 원효로 138 403호(원효로3가, 청진빌딩 4층)

02) 711-1175 | itlogin@itlogin.co.kr

개발사

**(주)에브리존 | 화이트디펜더**

서울 특별시 마포구 마포대로 136 지방재정회관

02) 3274-2700 | support@whitedefender.com


IT Login | EVERYZONE 화이트디펜더