

White Defender

랜섬웨어 위협 24시간 방어, 안티 랜섬웨어 화이트 디펜더

화이트디펜더는 랜섬웨어의 대응을 위해 실시간 보호, 행위 탐지, 함정 탐지 및 다양한 기능들의 제공을 통해 소중한 데이터를 안전하게 보호합니다.



White Defender 주요 기능



- ① 지속적으로 업데이트 되는 랜섬웨어 DB를 활용하여 알려진 랜섬웨어를 사전 탐지하여 차단합니다.
- ②랜섬웨어의 파일 훼손을 유도(함정)하여탐지, 차단 후 복원합니다.
- ③랜섬웨어에 의해 파일 훼손이 발생할 경우 실시간으로 행위를 분석하여 탐지합니다.
- ④랜섬웨어에 의해 파일 훼손이 발생할 경우 순간적으로 파일을 백업 후 랜섬웨어를 차단 하고 안전하게 복구합니다.
- ⑤대용량 파일의 경우 보호 폴더(Safezone) 설정을 통해 랜섬웨어의 파일 훼손으로부터 안전하게 보호할 수 있습니다.

White Defender
제품 소개

화이트 디펜더는 **3단계**(프로세스 레벨 > 서비스 레벨 > 커널 레벨) **방어 체계를 통해**, 랜섬웨어 위협을 실시간으로 모니터링 하여 알려지지 않은 랜섬웨어까지 방어할 수 있는 **안티-랜섬웨어 솔루션**입니다.



White Defender
특장점

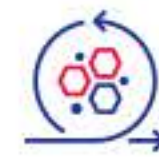
화이트디펜더는 실시간 보호, 행위 탐지, 함정 탐지 등의 기능 통해 랜섬웨어의를 사전에 탐지하여 차단하며 랜섬웨어가 암호화를 진행할 경우, 순간적으로 원본 파일을 백업 - 차단 - 복원하여 데이터를 안전하게 보호합니다.



24시간 실시간 보호
화이트 디펜더의 실시간 보호 기능은 행위 탐지/함정 탐지를 기반으로 24시간 실시간 보호 합니다.



행위 탐지 차단
모니터링을 통해 랜섬웨어로 인한 파일 훼손 행위가 발생할 경우 탐지후 차단합니다.



함정 탐지 유도 차단
랜섬웨어 행위를 분석하여 제일 먼저 감염이 될 수 있도록 유도(함정)하여 탐지 후 차단합니다.

White Defender
고급 기능



자체 보호
프로세스, 폴더, 파일, 레지스트리의 손상 보호



쉐도우 복사본 보호
복원 시점등의 복원에 사용되는 정보 접근 시 차단



비서명 프로세스 실행 알림/차단
서명되지 않은 파일이 실행 될 경우, 알림을 통해 허용, 차단, 예외



스크립터 위험 행위 차단
스크립터에 의해서 위험한 파일이 생성이 되는 경우 차단



행위 탐지 복원 저장 파일 크기 설정
설정 값보다 파일이 큰 경우, 행위 탐지 복원을 위한 파일 저장 제외



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



복원용 저장 파일 삭제
설정 기간 탐지된 복원 파일을 저장후 기간 내 삭제

White Defender
사용 환경

분류	권장 사양	최소 사양
운영 체제	윈도우 7이상 권장	윈도우 Vista SP1 이상
CPU	인텔 펜티엄 코어 i3 2.6GHz 이상	인텔 펜티엄 코어 2듀오 1.8GHz 이상
메모리	2GB 이상	1GB 이상
저장 공간	설치 100MB 이상 / 운영 5GB 이상	설치 100MB 이상 / 운영 1GB 이상