새로운 악성코드 하루 30만 개 생성 유통

백신만으론 부족합니다!



PARASOLE

엔드포인트 실시간 신규 사이버 위협 차단 솔루션 PARASOLE(파라솔)은
4단계 스마트 알고리즘을 기반으로 위협 요소 패턴 학습・분석・시그니처 비교 없이도
랜섬웨어를 비롯 30종 이상의 사이버 위협으로부터 PC・서버・키오스크・POS 등 을
보호함으로서 기업 데이터 보호, 규제 준수, 사업 연속성을 유지할 수 있도록 지원합니다.

실시간 새로운 사이버 위협엔 '파라솔'

4가지 특장점

1

실시간 미확인 위협

시그니처나 패턴 비교없이 알려지지 않은 신생 위협만 골라서 실시간 차단.

2

일당백 에이전트

안티랜섬・파일리스 해킹등 DLP, 매체제어, 자산관리 단 하나의 에이전트로 가능.

3

초경량, 강력 보안

10MB 미만 초경량 설계로 시스템 자원 최소 사용하며 높은 보안성능 제공.

4

불필요한 알림 NO

보안 업데이트, 시스템 검사 종용 등 불필요한 알림없어 업무 집중 환경 조성.

차단 솔루션 매커니즘 비교

	시그니처 기반(A/V) 저장된 패턴	행위 기반(EDR) 정의된 행위	Anti-Ransom 정의된 상황
장점	- 알려진 위협 효율적 탐지,즉각대응	-알려진 위협 패턴 식별 즉각대응	- 랜섬웨어에 특화, 백업 복구
단점	- 새로운 위협 탐지 적용 시간필요 - 지속적 보안 업데이트 필요 - 잦은 시스템 스캔으로 리소스 과점	- 오탐/과탐 가능성 - 복잡한 분석엔진,자원 과다 사용 - 도입비용 부담	- 변종대응 불확실 - 백업 복구 불완전 -암호화 동시 외부유출 차단 안됨

위협요소의 변화를 쫓는 기존 솔루션들 T..T

파라솔 선천면역 매커니즘

파라솔은 사용자가 의도한 Self 실행 여부를 식별합니다.

선천면역 매커니즘, 파라솔	후천(적응)면역 매커니즘, 백신
· 몸 속 T세포가 항원(Non-Self) 구별 후 면역 반응 · 사용자 미실행(Non-Self) 악성 행위 구별 후 차단	· 병원균 감염 후 적응, 항체 생성 면역 원리 이용 · PC 내 위협요소 시그니처 DB와 비교 멀웨어 차단

최상의 엔드포인트 보안 조합 제안!

파라솔에는 윈도우 무료 안티바이러스 MS 디팬더 통합 설정 UI 기능이 탑재되어 제공됩니다.

PARASOLE 선천면역 + 글로벌Top 안티바이러스 MS 디팬더 후천면역

파라솔이 무엇을 할 수 있나요?

- 계정탈취
- 지능형 지속 위협
- 어플리케이션 액세스 토큰
- 무차별 대입공격
- 업무 메일 침해
- 클라우드 암호화폐 채굴
- C&C공격
- 손상된 자격 증명
- 크리덴셜 덤핑
- 자격증 재사용 공격
- 멀트다운과 스펙터 공격
- 스피어피싱
- 피싱 페이로드
- 웨일 피싱
- 랜섬웨어
- 크립토재킹 공격
- DNS 증폭
- DoS 공격
- 드라이브 바이 다운로드 공격
- 내부자 위협
- IoT 위협
- 매크로 바이러스
- 악성 파워쉘
- 멀웨어
- 위장공격
- 섀도우IT
- 사회 공학적 공격
- 스파이웨어
- 공급망 공격
- 제로 데이 익스플로잇

사이버위협 30가지 끝장내기
엔드포인트 위협 요소

Anti-해킹
- 자료탈취 방지
- 좀비PC 방지
- USB 등 매체제어

Anti-랜섬웨어
- 랜섬웨어 무력화
- 전자동 스마트 백업

이상징후 모니터링
- 사이트 접속기록
- 리소스 사용
- 개인정보 사용 등

부가 기능
- PC 자산관리
- MS디팬더 통합UI
- 원격 연결 도구

(주)제이커넥트 | www.parasole.co.kr | help@parasole.co.kr