세계 유일 상황인식 기반 랜섬웨어 방어 솔루션

AppCheck

안티랜섬웨어

CHECKMAL

Never mind the security

AppCheck Pro / AppCheck Pro for Windows Server

상황 인식 기반 행위 탐지로 정교하고 안전하게

앱체크 프로(AppCheck Pro)는

상황 인식 기반 엔진(Context-Awareness based Ransomware Behavior Detection)을 바탕으로
고도화된 랜섬웨어 위협에 노출되어 있는 지적 자산 및 데이터를 안전하게 보호하는
종합적인 기능의 **랜섬웨어 전문 대응 솔루션**입니다. 사전 방어, 자동 복구, 자동 백업 기술로
어떠한 상황에서도 완벽하게 데이터를 보호합니다.

시그니처 없는 랜섬웨어 방어 솔루션

자체 개발한 CARB 엔진은 단 하나의 시그니처 없이
알려지지 않은 랜섬웨어를 탐지 및 차단합니다.

랜섬웨어 및 생성 파일 자동 삭제

랜섬웨어(결제안내 파일) 및 훼손 파일을 삭제하고
원상 복귀 시켜 업무 중단을 최소화합니다.

원격지에 자동 백업 및 복원으로 완벽한 보호

혹시 모를 위협에 대비하여 파일 훼손시에 실시간으로
백업하여 디스크 용량 걱정없이 안심하고 사용할 수 있으며,
지정된 시간에 원하는 폴더를 주기적으로 원격지에 백업합니다.

가볍고 효율적인 CARB 엔진

AppCheck는 타 보안 솔루션 대비 리소스를 약 73%
덜 소비하여, 안정적 시스템 이용 및 효율적 서버를
운영을 가능하게 합니다.

세계 유일 공유 폴더 보호

공유된 폴더를 원격지에서 훼손하더라도 이를
탐지 및 차단하고 손상된 파일을 자동으로 복구합니다.

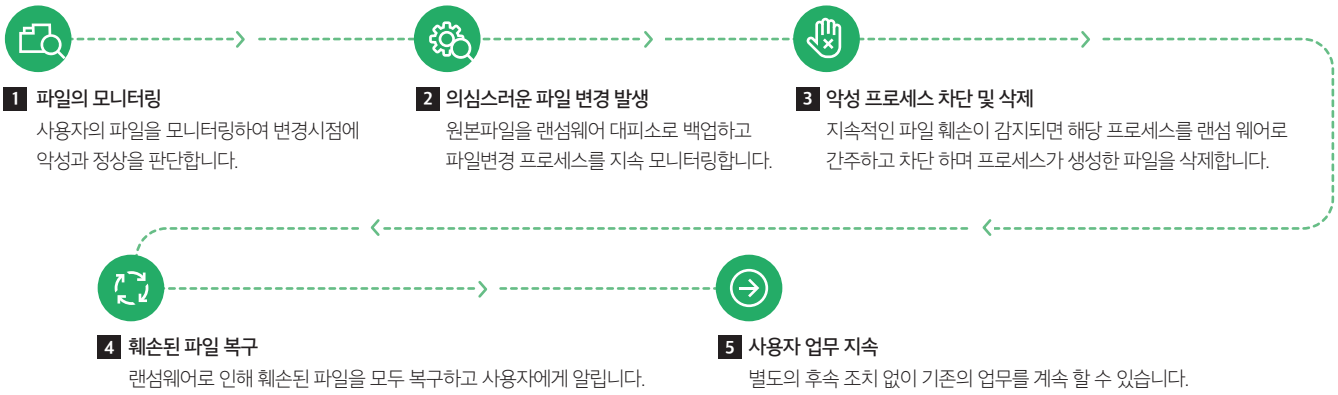
세계 유일 서버 용 랜섬웨어 솔루션

서버에서 공유된 폴더 내 파일을 원격지에서
훼손하더라도 이를 감지하고 접근을 차단하여
공유된 데이터를 안전하게 보호합니다.

상황 인식 기반 행위 탐지 (CARB engine)

파일 변조시점에 정상·악성 판단

상황 인식 기반 랜섬웨어 탐지 기술은 파일의 변조 시점에 정상적 변경과 악의적 변경을 판단하여 별도의 업데이트 없이 신종 랜섬웨어의 사전 탐지가 가능합니다. 상황인식 기반(CARB) 기술은 파일이 변경 될 때 확인되는 정보가 매우 다양하다는 점에 착안하여, 이를 추적하고 관리하여 정상적인 파일의 변경과 비정상적 변경을 구분합니다.



1 파일의 모니터링
사용자의 파일을 모니터링하여 변경시점에 악성과 정상을 판단합니다.

2 의심스러운 파일 변경 발생
원본파일을 랜섬웨어 대피소로 백업하고 파일변경 프로세스를 지속 모니터링합니다.

3 악성 프로세스 차단 및 삭제
지속적인 파일 훼손이 감지되면 해당 프로세스를 랜섬 웨어로 간주하고 차단 하며 프로세스가 생성한 파일을 삭제합니다.

4 훼손된 파일 복구
랜섬웨어로 인해 훼손된 파일을 모두 복구하고 사용자에게 알립니다.

5 사용자 업무 지속
별도의 후속 조치 없이 기존의 업무를 계속 할 수 있습니다.

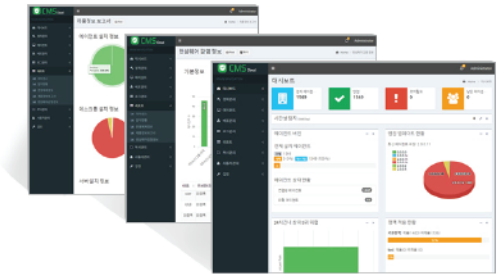
관련 솔루션 비교

상황 인식 기반 행위 탐지로 Zero-Day 랜섬웨어 탐지

상황인식 기반 (CARB) 엔진은 기존 솔루션에서 불가능했던 파일의 변화를 실시간으로 분석하여 알려지지 않은 랜섬웨어의 탐지가 가능합니다.

사전방어 탐지 세부 항목	CARB 엔진	백신	APT 솔루션
시그니처 우회 변종 파일	O	O	O
미끼 파일 포함한 파일 암호화	O	△	△
프로세스별 행위 연계 추적	O	△	△
폐쇄망 단독 탐지	O	△	X
기존 백신과 동시 운영	O	X	△
미탐시 원본파일 복구	O	X	X
미끼 파일 우회한 파일 암호화	O	X	X
확장명 우회 후 암호화 (파일 변경 추적)	O	X	X
복호화 결제 안내 파일 삭제 (파일 생성 롤백)	O	X	X
탐지전 암호화 된 파일 복구 (파일 훼손 롤백)	O	X	X
비 암호화 파일 훼손 인식	O	X	X
정상적인 파일 수정 행위 인식 (변화 분석)	O	X	X
생성/변경/덮어쓰기/삭제 상황 별 연계 분석	O	X	X
메모리 Mapped 방식 I/O 탐지	O	X	X
Hard Link 방식 파일 변조 탐지	O	X	X
원격지로부터 공유 폴더내 파일 훼손 탐지	O	X	X

CMS - 중앙 관리 솔루션



고객 맞춤형 중앙 모니터링

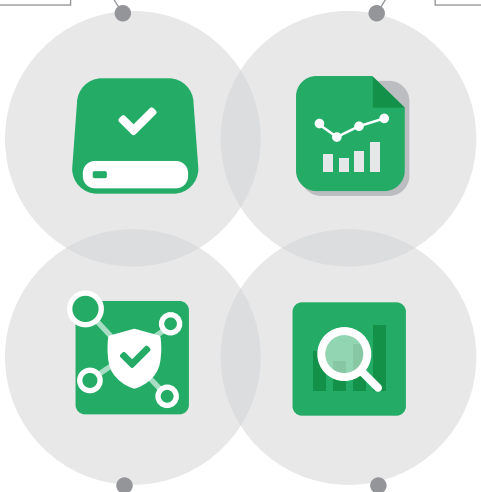
중앙관리 솔루션(CMS)은 고객사 환경에 따라
On-site/Cloud 서비스 형으로 선택하여 사용할 수 있습니다.
On-Site용 CMS Enterprise는 고객의 중요한 정보와 데이터를
추가적인 백업 중앙화 솔루션 없이 중앙에 백업할 수 있습니다.

✔ 백업 중앙화

다양한 백업 옵션과 네트워크 드라이브 백업으로
별도 솔루션 없이 백업 중앙화 할 수 있습니다.

✔ 다양한 리포트

기간별 보고서, 통계 및 로그를 제공하며, 다양한
리포트를 손쉽게 출력할 수 있습니다.



✔ 다중 정책 및 중앙 관리

엔드포인트에 보유하고 있는 중요한 정보자산을
랜섬웨어로부터 보호하고 중앙에서 정책을
배포하여 효율적인 관리가 가능합니다.

✔ 중앙 모니터링

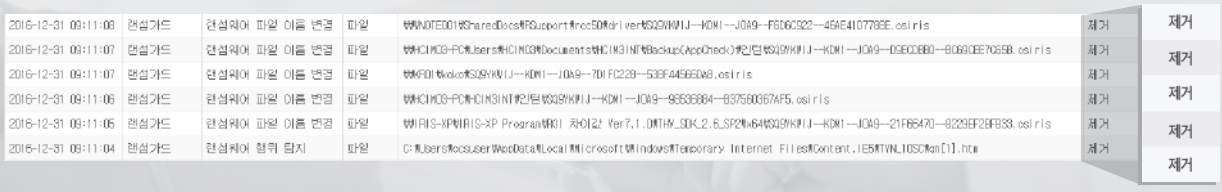
HTML5 기반의 웹 브라우저 콘솔에서 모든 기능을
제어할 수 있으며, 대시보드, 로그관리, 실시간
랜섬웨어 탐지 정보를 확인할 수 있습니다.

도입사례

AppCheck 도입 후 랜섬웨어 예방 - 국내 K병원

한달간 71대 PC 랜섬웨어 감염 차단

"해외에서 업무 관련 자료를 찾던 중에 PC가 느려지고 영문 팝업창이 떴지만 이를 광고로 생각하고 무시하고 웹사이트를 이용하였습니다.
AppCheck에서 랜섬웨어 치료 완료 알림 메시지가 나타나 관리자에게 문의하니 랜섬웨어였다는 것을 알게 되었습니다. 주위에 물어보니 랜섬웨어로
모든 파일이 암호화 되었을 거라며 앱체크가 설치되어 있지 않았더라면 어떤 피해가 발생했을지 상상만 해도 아직도 가슴이 두근거립니다."



기존 탐지 기술의 한계와 차세대 랜섬웨어 방어 전략

기존의 탐지 기술은 다양한 악성코드의 정보(URL, 파일이름, 레지스트리 값, 경로 등의 콘텐츠) 즉 콘텐츠 DB를 참조해야 하기 때문에 콘텐츠에 부합되지 않는 새로운 랜섬웨어 출현 시 탐지가 불가능하다는 한계가 있습니다. 또한 콘텐츠 기반 기술을 보완하고자 개발된 비 콘텐츠 기반 기술도 각각의 한계가 존재하므로 이러한 한계를 극복할 수 있는 원천적 기술이 필요합니다.
상황을 인식하는 랜섬웨어 탐지 기법은 기존의 보안제품처럼 랜섬웨어의 특징을 보는 것이 아닌 실제 사용자의 파일을 변조하는 상황을 종합적으로 판단하므로 새롭게 나타나는 랜섬웨어의 훼손 행위에 대해서도 시그니처 없이 정확한 탐지가 가능합니다.

시그니처/ 행위 기반 탐지 기법의 한계

파일을 진단할 때 사용되는 탐지 방법으로 주로 파일내 특정 부분을 해시로 변환하여 참조하는 방법으로 랜섬웨어 유포자가 인터넷에 알려져 있는 시그니처 테스트 후 이를 우회한 악성코드를 유포하기 때문에 신종 랜섬웨어에 대한 탐지가 불가합니다.
상황인식 기반 랜섬웨어 탐지 기법은 최종적으로 파일을 암호화 하는 단계에서 파일이 변경되기 전과 후를 지속적으로 모니터링하여 관리하므로 시그니처 없이 순수한 행위만으로 방어가 가능합니다.

네트워크/ 미끼/ 익스플로잇 기반 탐지 기법의 한계

네트워크상의 통신 정보를 기반으로 악성코드를 탐지하는 방법은 암호화된 네트워크를 통해 공격자가 명령을 전송할 경우에는 이를 탐지하기가 어려우며, 임의의 파일을 생성하고 이를 랜섬웨어가 암호화 하였을 때 탐지하는 디코이(Decoy) 기반 탐지 기법도 랜섬웨어는 간단하게 우회가 가능합니다.
상황인식 기반 랜섬웨어 탐지 기법은 랜섬웨어의 최종 목적인 파일을 실시간으로 모니터링함으로써 모든 변조에 대한 탐지가 가능합니다.

랜섬웨어 방어 실패시의 대안

랜섬웨어는 매우 높은 수준의 암호화 기법을 사용하여 사용자의 파일을 암호화 하기 때문에 이를 복호화 하기에는 매우 어렵습니다. 따라서, 기존의 탐지기법은 탐지에 실패할 경우 훼손된 파일에 대해서 복구가 불가능합니다. 상황인식 랜섬웨어 탐지 기법은 파일을 훼손하는 시점에 실시간으로 원본을 백업하기 때문에 복구가 가능하며, 통합된 자동 백업으로 사용자의 파일을 이중화하여 보관하므로 방어에 실패하더라도 사용자의 파일은 안전하게 복원할 수 있습니다.

랜섬웨어 대피소 및 자동 백업

한번 훼손된 파일은 복원이 불가능하므로, AppCheck는 파일이 훼손되기 이전의 원본을 실시간으로 랜섬웨어 대피소에 백업합니다. 랜섬웨어 대피소는 의심스러운 파일의 훼손 행위가 일어날 때 파일을 임시로 대피시키며 향후 랜섬웨어로 판단되는 경우에 이를 복원합니다. 또한 자동백업 기능으로 사용자의 파일을 지정한 시간마다 백업하여 혹시 모를 상황에 2중으로 안전하게 보호합니다.
백업 보관 폴더는 드라이버 수준에서 보호되므로 혹시 모를 랜섬웨어의 위협에도 안심할 수 있습니다.

체크멀의 기술력

다양한 사용자 환경/ GS인증으로 검증된 안정성

커널 레벨에서 동작하는 랜섬웨어의 상황인식 기반 엔진은 속도와 안전성 그리고 호환성을 보장해야 하며 제한된 환경에서 다양한 기능을 추가하는 일은 높은 기술적 난이도를 요구합니다. AppCheck는 월 15만의 활성 사용자를 보유하였고, 이를 통해 다양한 사용자 환경에서 검증되었습니다. GS인증 1등급 획득으로 제품의 안정성과 기술력을 인정 받았습니다.

GS인증

벤처기업확인서

저작권 등록증

2016년 2월
- AppCheck Pro 출시

2016년 4월
- Primer 투자유치
- **법인 설립**

2016년 7월
- 판교 사무실 이전

2016년 8월
- TIPS 프로그램 선정
- **총판 계약 체결** HCINFO 지란지교소프트

2016년 11월
- AppCheck Pro for Windows Server 출시
- CMS 출시

2016년 12월
- 월 활성 사용자 15만명 달성

주요 납품 고객사

국회도서관 · 경희의료원 · 서울아산병원 · 대구광역시버스운송사업조합 · Cellab
DAEHAN · 롯데건설 · KOREA RATINGS · 유한양행 · 주식회사 성진포머

CHECKMAL

(주)체크멀
경기도 성남시 분당구 대왕판교로 660,
유스페이스1 A동 303호. 우) 13494
031-724-2580 · contact@checkmal.com