보안의 원칙을 아는 엔드포인트 통합보안 솔루션

trueEP v2.0

Anti-Hacking

1. 자료해킹 방지
2. 좀비 PC 방지
3. 인터넷 접속 통제
4. 첨부파일 통제
5. 매체사용 통제
6. 이상징후 모니터

Anti-Ransomware

1. 랜섬웨어 공격방지
2. 전자동 스마트 백업
3. 이상징후 모니터링

전세계에서
유일한
선제 방어 보안

자동백업

이상징후
모니터링

EPS
(Endpoint Protection System)

Anti-Hacking
+
Anti-Ransomware
+
Anomaly Monitoring

trueEP v2.0 IT에 관한 모든 고민을 한꺼번에 해결

IT관리자의 고민

- 업무PC에 대한 자산관리 부재
- 업무PC 비업무적 사용 통제
- 퇴직자 자료 관리 부재
- 공용PC 관리 부재
- 네트워크 구성 상황 파악 부재

보안관리자의 고민

- 해킹 사고
- 내부자의 자료유출
- 랜섬웨어 공격
- 기관 내 존재하는 좀비PC
- 보안사고가 나면 몸으로 때워야 한다
- 개인정보 보안 어떻게 하라는 건지?

사용자의 고민

- 해킹
- 랜섬웨어 공격
- P2P헤비 업로더로 도용
- 좀비PC공격에 도용
- 보안 프로그램이 너무 많음
- 실수로 삭제한 파일을 복원할 수 없을까?

IT고민 한방에 해결

IT자산 관리 및 사용 통제

- 기관 내 PC들의 리소스 사용량 정보 제공
- 기관 내 PC들에 설치된 프로그램 정보 제공
- 프로그램별 리소스 사용량 정보 제공
- PC 사용 기록 정보 제공
- 인터넷 사용 기록 정보 제공
- 비인가 프로그램 사용 차단
- 전자동 백업
- MAC, 내외부 IP 등 네트워크 정보 제공

사이버공격 방어 및 보안관리

- 관리자 개입 없이 자동 해킹 방지
- 내부자의 전송기록 로깅
- 랜섬웨어 공격 방어 및 전자동 백업
- 과다 트래픽 차단
- 자동화된 로그 분석
- 개인정보 포함 문서의 보유 및 전송기록 제공

사이버공격 방지

- 자동 해킹 방지
- 랜섬웨어 공격 방어 및 전자동 백업
- P2P 업로드 차단
- 좀비PC 공격 차단
- 올인원 보안기능 제공
- 삭제한 파일 복원

trueEP v2.0 방어원리의 차별성(특허10-0676912호)

	기존 보안 제품들의 방어 원리	trueEP 만의 방어 원리
방어 원리	시그니처 기반 **악성코드 감염 차단** 코로나 감염을 마스크로 예방하는 방식	리얼머신기반 **악성행위 실행 차단** 자기 항체로 코로나 바이러스의 활동을 억제하는 방식
방어 원리 개요	• 유입되는 패킷에 알려진 악성코드가 포함되어 있는지를 검사하여 포함되어 있으면 삭제함	• PC(혹은 서버)에서 프로세스 행위가 발생할 때 그 행위를 사용자가 실행한 건지 아닌지를 구분하여 사용자가 실행하지 않은 행위이면 차단
한계성	• 알려지지 않은 악성코드엔 무방비 • 수시로 패치를 해야 함 • 보안 제품의 용량이 커짐	• 자동실행 업무 프로그램 에 대한 예외처리
특장점	• 전통적으로 사용되어 온 기술로 언노운 공격을 근원적으로 방어하지 못함	• 언노운 공격까지 차단 • 수시 패치가 필요하지 않음 • 보안 제품의 용량이 매우 작음(10MB)

trueEP v2.0 Anti-Hacking 기능 소개

	제공 기능	trueEP 만의 방어 원리
자료유출 방지	자료 해킹 방지	• 내장 하드디스크에 저장된 파일이 사용자 입력없이 네트워크나 외장 디스크로 유출되는 경우 차단
	개인정보 포함 문서 해킹 방지	• 자료 유출 방지 시 개인정보가 포함 문서일 경우 구별하여 알림
	자료 전송 감사로그	• 내장 하드디스크에 저장된 파일이 사용자 입력에 의해 네트워크나 외장 디스크로 전송되는 경우 로깅
	개인정보 포함 문서 전송 감사로그	• 자료 전송 감사로그 시 개인정보가 포함 문서일 경우 구별하여 알림
	메일 • 메신저 파일 첨부 차단	• 메일 • 메신저에 파일을 첨부하여 전송할 수 없도록 제한
	메일 • 메신저 첨부파일 사이즈 제한	• 메일 • 메신저에 첨부하는 파일의 크기를 일정 사이즈 이내로 제한
	출력문서 워터마크 삽입	• 프린트시 워터마크를 삽입하여 출력하도록 함-이미지 혹은 문자
	인쇄기록 감사 로그	• 누가 언제 어떤 문서를 출력하였는지 히스토리 관리
좀비PC 방지	과다 트래픽 차단	• 사용자 입력없이 임계치(조절 가능) 이상의 트래픽이 발생할 경우 차단
매체사용 통제	USB장치 사용 통제	• USB 매체를 사용/사용불가/Read만 가능하도록 설정하거나, 특정 USB만 허용할 수 있음
	테더링 사용 통제	• 테더링 기능을 사용하지 못하게 막을 수 있음
	블랙리스트기반 차단	• 블랙리스트 방식으로 특정 프로그램의 실행을 차단할 수 있음
	인터넷 접속 통제	• 블랙리스트 방식으로 특정 웹사이트의 접속을 차단할 수 있음

trueEP v2.0 Anti-Ransomware 기능 소개

	제공 기능	trueEP 만의 방어 원리
랜섬웨어 공격 방지	순수 행위기반 차단 알고리즘	• 언노운 랜섬웨어 까지 방어 (유일)
전자동 스마트백업	스마트 백업	• CPU 유휴시간에만 백업 실행 • PC 사용 중에는 백업 중단 • 사용자 PC상태에 맞게 저장공간 크기 지정 • 저장공간이 부족할 경우 오래된 파일 자동 삭제 • 지정한 폴더 또는 파일만 백업되게 설정
	전자동 백업	• 사용자 개입 없이 스스로 알아서 백업 • 파일 생성 및 변경을 자동으로 인식하여 백업
	자동 복원	• 자동 복구툴 제공(복구툴에 의해서만 복구 가능) • 원래 파일 경로 또는 지정 경로를 선택하여 복원
	통합 관리 및 모니터링	• 관리서버에서 개별사용자에 대한 백업정책 설정 가능 • 개별 사용자들의 백업상태를 관리서버에서 통합 모니터링
	외부 저장장치로 백업	• FTP / NAS 방식으로 외부 백업 지원
	DB백업	• Date Base 파일 백업 지원

trueEP v2.0 이상징후 모니터링 기능 소개

제공 기능	기능 설명
PC uptime 모니터링	PC uptime을 모니터링하여 이상 가동 징후를 포착할 수 있음
웹페이지 접속기록 모니터링	웹페이지 접속기록을 모니터링하여 이상징후를 포착할 수 있음
리소스 사용량 모니터링	CPU, 메모리, 네트워크 등 사용량을 모니터링하여 이상징후를 포착할 수 있음
프로그램 설치 현황 모니터링	프로그램 설치 현황을 모니터링하여 악성코드 설치징후를 포착할 수 있음
개인정보 포함 문서 모니터링	개인정보 포함 문서 보유 상황을 모니터링하여 개인정보 보안에 대비할 수 있음

trueEP v2.0 제품 출고 형태

적용 범위		비고
기능적	범용 해킹 방지 목적	통상의 해킹 공격을 방어하고, 이상징후에 대비하려는 경우
	랜섬웨어 공격 방지 목적	랜섬웨어 공격을 방어하고, 이상징후에 대비하려는 경우
	통합보안 목적	통상의 해킹 공격과 랜섬웨어 공격을 동시에 방어하고, 이상징후에 대비하려는 경우
용도적	서버 보호 목적	보호하려는 대상이 업무용 서버 제품인 경우
	PC 보호 목적	보호하려는 대상이 업무용 PC 인 경우
	특수기기 보호 목적	보호하려는 대상이 POS, ATM, KIOSK, Smart Factory 등 특수기기인 경우
형태적	구축형	관리서버를 독자적으로 구축하여 운영하고자 하는 경우
	구독(SaaS / Cloud)	클라우드 기반의 관리서버에 접속하여 운영하고자 하는 경우


현황판
로그
정책
사용자
이상징후 모니터링
리포트
설정
History
최근 24시간
차단
22 Total
14.3
3
랜섬웨어 차단
0
유출 차단
0
매체 차단
85.7
18
DDoS 차단
랜섬웨어 차단
월별 주별 일별
유출 차단
월별 주별 일별
DDoS 차단
월별 주별 일별
위험도 0 위험도 1 위험도 2 위험도 3
에이전트 운영 모드
Total
1215
8.6%
15.5%
76.0%
차단 탐지 미관제 미사용
실시간 로그 보기
2023-01-19 22:58:57 z: 192.168.123.108 excel.exe 국내영업팀보(23年-1月)-신규서식.xlsx network drive
2023-01-19 22:51:26 0 192.168.123.108 notepad.exe behavior blocking - 7962397a4d... ransomware
2023-01-19 22:51:02 z: 192.168.123.108 excel.exe 23년_종합일일영업현황 - 01월.xlsx network drive
2023-01-19 22:40:08 movable-mounted 192.168.0.31 newgendbserver.exe octlog.log movable/usb
2023-01-19 22:40:08 movable-mounted 192.168.0.31 newgendbserver.exe octlog.dbs movable/usb
2023-01-19 22:40:08 movable-mounted 192.168.0.31 newgendbserver.exe octlog.dbs-wal movable/usb
2023-01-19 22:40:08 movable-mounted 192.168.0.31 newgendbserver.exe octlog.dbs-shm movable/usb


현황판
로그
정책
사용자
이상징후 모니터링
현황판
인터넷 사용 기록
설치된 프로그램
PC 사용 기록
개인정보 전송/차단
리포트
설정
History
인터넷 사용 기록
2020-01-20 ~ 2023-01-20
쇼핑
뉴스
엔터테인먼트
구인구직
SNS
증권
Total
2346973
3.7%
22.2%
45.0%
25.7%
설치된 프로그램
2020-01-20 ~ 2023-01-20
총 설치된 수 최근 7일 내 최근 30일 내
건수(건)
건욱장
태호드
건성이
태프PC
김정호
PC 사용 기록
2020-01-20 ~ 2023-01-20
Application
클라우드
FTP Rush
오피스 제품군
SMM_HyperCam.exe
WebhardExplorer
오피스
Total
455054
4.7%
19.2%
43.1%
30.0%
개인정보 전송/차단
월별 주별 일별
건수(건)
2023-01-11 2023-01-12 2023-01-13 2023-01-14 2023-01-15 2023-01-16 2023-01-17
탐지 차단 개인 정보


현황판
로그
정책
사용자
이상징후 모니터링
리포트
현황판
탐지 내역
탐지 예약
설정
History
리포트
다운로드
2023.01.19 ~ 2023.01.26
76 Total
위협도 0
58 76.3%
위협도 1
17 22.4%
위협도 2
1 1.3%
위협도 3
0 0%
차단 / 탐지
차단 탐지
건수(건)
2022-03 2022-04 2022-05 2022-06 2022-07 2022-08 2022-09 2022-10 2022-11 2022-12
유형별 차단
건수(건)
유출 차단 랜섬웨어 차단 매체 차단 DDoS 차단
에이전트 운영 모드
차단
923
탐지
188
미관제
104
미사용
0
버전별 에이전트 설치 수
810
118
91
57
44
40
16
15
14
10
0 200 400 600 800 1000
OS별 에이전트 설치 수(top 10)
Total
1192
49.8%
27.6%
8.6%
4.4%
2.5%
Windows 10 Pro x64
Windows 10 Home x64
Windows 7 Pro x64
Windows 11 Home x64
Windows 11 Pro x64
Windows 7 Home x64
Windows 7 Home
Windows 7 Pro
Win2012 R2 Server x64
Windows 8.1 Pro x64

trueEP v2.0 시스템 구성도

구 분	에이전트 요구 사항	매니저 요구 사항
CPU	Pentium 133Mhz 이상	Quad Core 2Ghz 이상
메모리	5MB 이상	16GB 이상
디스크	10MB 이상	SSD 500GB 이상
OS	Windows XP / 7 / 8 / 10 / 11(32/64bits)	Window 2019 / 2022 권장

개발사

㈜트루컷시큐리티
www.truecut.co.kr

서울특별시 서초구 강남대로 525, 14층
TEL. 02.3448.0880 FAX 02.3448.0804

판매협력사

아이비즈(주)

황기주이사
010-4331-5554 / kj@ibiz.kr
www.ibiz.kr