2020 대한민국
우수특허大賞

엔드포인트 통합보호 및 모니터링

trueEP v2.0

제품 소개서

트루컷시큐리티
TrueCut Security, Inc.

사이버 보안의 실상 : 이중고

보안 비용 급증 + 보안 사고 급증

- 보안 제품을 무력화하는 지능화된 위협에 속수무책
- 국가 안보 및 기업 생존에 대한 위협
- 개인 사생활 파괴
- 보안인력의 업무 과중에 따른 인력 수급 문제

방어 개념의 전환이 절실한 시점

악성코드 침입을 막는 개념 => 실공격 방어 개념
출입구 봉쇄 개념 => 범죄 현장 검거 개념

- 악성코드가 들어오는 것을 막는 기술은 근원적으로 존재하지 않음.
- trueEP는 악성코드의 공격 행위를 차단하도록 설계.
- trueEP는 범죄 현장에서 범인을 검거하도록 설계.

북한이 해킹으로 탈취한 주요 국내 방산기술

	해킹 대상	주요 탈취 기술
2016년	대우조선해양	콜드론치 등 SLBM 관련
2021년	한국원자력연구원	소형 원자로 관련
	대우조선해양	3000t급 잠수함 관련
	한국항공우주산업(KAI)	한국형초음속전투기 'KF-21' 관련
2023년	조선업체 4곳	함정 도면 및 설계자료
	무인기 업체	무인기 엔진자료

현대차 유럽권역본부, 랜섬웨어 공격 피해…데이터 '통째 도난' 3TB

데이터 탈취

Black Basta ransomware gang claims the hack of the car maker Hyundai Motor Europe and the theft of three terabytes of their data

출처: Security Affairs, 2024.2.9

2. 사이버 보안의 핵심은 언노운 공격 방어

언노운 공격방어를 위해 인가된 내부 사용자의 정상적인 행위인지
원격지 공격자의 악의적인 공격인지를 식별하는 알고리즘 개발

인가된 내부사용자

원하는 프로그램 실행을 위해
단말기를 직접 **조작한다**

원하는 업무 수행을 위해
단말기를 **연속해서 조작한다**

원격지 공격자

단말기를 직접 **조작하지 못한다**

사이버 공격을 진행하는 동안
단말기를 직접 **조작하지 못한다**

3. 기존 보안 제품들과의 차별성

구 분	기존 보안제품들의 방어 원리	trueEP만의 방어 원리
방어 원리	시그니처 기반 악성코드 감염 차단 - 마스크로 감염을 방지하는 방식	실시간 악성행위 실행 차단 - 자가 항체로 발병을 방지하는 방식
방어 원리 개요	유입되는 패킷에 알려진 악성코드가 포함되어 있는지를 검사하여 포함되어 있으면 방어함	내 PC(혹은 서버)에서 어떤 행위가 발생할 때 그 행위를 사용자가 실행한 건지 아닌지를 구분하여 사용자가 실행하지 않은 행위면 차단
문제점	알려지지 않은 악성코드엔 무방비 수시로 패치를 해야 함 보안 제품의 용량이 커짐	자동실행 업무 프로그램이 있으면 예외처리해야 함
특장점	거의 모든 보안기업들이 사용하는 방식으로 알려진 공격 방어에 특화	알려지지 않은 공격 방어에 특화 (알려진 공격을 하는 바보 해커는 없음) 패치가 필요하지 않음 보안 제품의 용량이 매우 작음(5MB)

4. trueEP에 의한 요구사항 충족

사이버 보안 핵심 요구사항
1. 랜섬웨어 공격 방어
2. 정보유출 방지
3. 좀비PC 방지
4. 외부 매체 사용 통제
5. 비업무 프로그램 사용 통제

IT자원 관리 핵심 요구사항
1. 리소스 사용률 실시간 모니터링
2. PC On/Off 현황 모니터링
3. 프로그램 설치 현황 실시간 모니터링
4. PC 사용 기록 실시간 모니터링
5. 인터넷 사용 기록 실시간 모니터링
6. 개인정보 보유 현황 모니터링

trueEP에 의한 충족
1. 언노운 랜섬웨어 공격 방어
2. 전자동 스마트백업 기능 제공
3. 언노운 해킹에 의한 정보유출 방지
4. 악성 트래픽 차단
6. 외부 매체 사용 통제
7. 프로세스 실행 통제(블랙리스트)
8. 프로세스병 리소스 사용률 로깅
9. PC 사용 기록 로깅
10. 설치된 프로세스 목록 로깅
11. 인터넷 사용 기록 로깅
12. 파일 전송 기록 로깅
13. 개인정보 보유 및 전송 기록 로깅

5. 주요 기능

구 분	기능	설명
보안 기능	정보(자료) 유출 방지	알려지지 않은 해킹(APT)에 의한 정보(자료) 유출 방지 - 유일
	랜섬웨어 공격 방어	자료를 탈취하고 암호화 하여 금전을 요구하는 랜섬웨어 공격 방어 - 유일
	좀비PC 방지	디도스/스푸핑/악성트래픽 차단으로 네트워크 마비 및 속도저하 방지
	메일•메신저 보안	파일 첨부 통제 (파일 사이즈 제어)
부가 기능	전자동 스마트 백업	문서파일 + 확장자 지정 백업, 암호화 3중백업
	매체제어	USB 매체제어(특정 USB만 허용 가능) / 테더링 / 포트 접속 제어
	블랙리스트 차단	유해사이트 접속 차단 / 악성 프로그램 실행 차단
	원격 지원	원격 단말기에 대한 지원 서비스 기능 제공
	개인정보 문서	개인정보 보유 문서 전송 기록 제공
	MS백신 사용 지원	MS 디펜더 백신 사용 편의성 제공
관리 기능	자산관리 및 모니터링 (첨부 보고서 참조)	1) 운용중인 단말기 현황 파악 : 제조사/모델/CPU/Mem/Disk/수량 2) 운용중인 OS 현황 파악 : 버전/수량 3) 사용중인 프로그램 현황 파악 : 업무용/비업무용 구분 4)기간별 프로그램 추가/삭제 현황 파악 5) 사용중인 백신프로그램 현황 파악 : 제조사/제품명/수량 6) 기간별 인터넷 사용 현황 파악 : 사이트별 접속자/접속횟수 7) 기간별 단말기 사용 현황 파악 : 용도/사용자수/회수/시간 8) 개인정보 문서 보유 현황 파악 : 단말기별/개인정보별/사용구분

6. 스마트백업 기능 소개

랜섬웨어 공격 이중방어를 위해 제공

스마트한 백업 제공	trueEP의 기능
업무를 방해하지 않음	+ CPU 유휴시간에만 백업 실행 + PC 사용 중에는 백업 중단
자동 백업	+ 사용자 개입 없이 스스로 알아서 백업 + 파일 생성 및 변경을 자동으로 인식하여 백업
자동 복원	+ 자동 복원툴 제공 + 원래 파일 경로 또는 지정 경로를 선택하여 복원
저장공간 관리	+ 사용자 PC상태에 맞게 저장공간 크기 지정 + 저장공간이 부족할 경우 오래된 파일 자동 삭제
선별 백업	+ 지정한 폴더 또는 파일만 백업되게 설정
통합 관리 및 모니터링	+ 관리서버에서 개별사용자에 대한 백업정책 설정 가능 + 개별 사용자들의 백업상태를 관리서버에서 통합 모니터링
외부 저장장치에 백업	FTP / NAS 방식으로 외부에 백업 가능
DB백업	DB 파일도 백업 가능

7. 원격 지원 기능 소개

trueEP가 설치된 PC나 서버를 원격으로 지원하는 기능

- 유료 원격지원 제품에 준하는 기능 제공

기능 구분	설 명
원격 화면 공유	원격지 서버나 PC의 화면 모니터링
원격 화면 인쇄	원격지 서버나 PC의 화면 인쇄
	원격지 서버나 PC의 화면 스크린샷 저장
원격 제어	원격지 서버나 PC의 실행 프로세스 종료/일시중지
	원격지 서버나 PC의 리소스 사용 모니터링
	원격지 서버나 PC에 폴더 생성
	원격지 서버나 PC로 파일 보내기 및 받기
	원격지 서버나 PC의 CMD창 사용
	원격지 서버나 PC의 작업관리자 화면 제어
	원격지 서버나 PC의 시스템 정보 표시
	원격지 서버나 PC 사용자와 실시간 화면 채팅
	원격지 서버나 PC 사용자와 실시간 화면 채팅
	원격지 서버나 PC 화면에 레이저포인터 사용
	다중 단말기에 대하여 한 화면에서 동시에 원격지원 가능

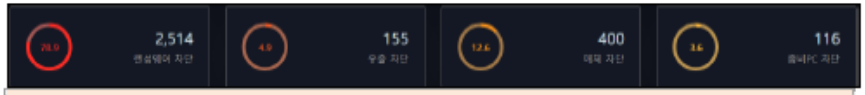
8. MS 디펜더 백신 제어창 제공

가장 강력한 무료 백신인 MS디펜더 사용 편의 제공

trueEP 02 월 점검보고서

고객명 : ABCD
점검일 : 2024.03.06 (2024-02-01 ~ 2024-02-29)
점검자 : 트루컷시큐리티 홍 길동 대리

1. 로그 분석



1.랜섬 차단 2,514, 유출 차단 155, 매체 차단 400, 좀비 차단 116 건의 로그가 발생하였음.
2.차단 로그가 발생한 사유는 해당되는 이벤트에서 사용자 입력행위가 식별되지 않은 경우임.
3.알려지지 않은 공격을 방어하기 위해 불가피하게 발생하는 과탐 로그임으로 우려하지 않아도 됨.

2. 운용 중인 PC 현황

제조사	모델명	CPU	MEM	Storage	대수
ASUSTeK	ASUS TUF Dash F15 FX516PM_FX51...	8	16GB	477GB	6
HP	HP ProBook 440 G7	8	8GB	477GB	56
	HP ProBook 450 15.6 inch G9 No...	16	16GB	239GB	98
LENOVO	20V9, 81UM	8	8GB	239GB	740
LG	15ZD90N-VX30K	4	8GB	239GB	372
SAMSUNG	340XAA/350XAA/550XAA	4	8GB	119GB	184
	900X3K	4	8GB	239GB	103
trueEP 에이전트가 설치된 PC 총 대수					**1,559**

1.귀 기관의 PC 는 5 개 제조사 총 1,559 대로 파악됨.
2.trueEP 에이전트가 설치되 않은 PC 는 집계되지 않음.

☞ trueEP 에이전트 2.0.23.1108 이후 버전에서 제공되는 기능임

3. 운용 중인 OS 현황

구분	버전	설치된 수
서버 OS	Win2003 R2 Server	1
	Win2008 R2 Server	1
	Win2008 Server	5
	Win2012 R2 Server	19
	Windows 2016 DataCenter Server	2
	Windows 2016 Server	9
	Windows 2019 Server	6
	Windows 2022 Server	6
Window Server OS 사용 총 대수		**49**
PC	Windows 10	1,099
	Windows 11	278
	Windows 7	122
	Windows 8	1
	Windows 8.1	8
	WinXP	2
PC 용 OS 사용 총 대수		**1,510**

1.귀 기관의 OS 분포는 서버는 8 종, PC 는 6 종이 사용 중인 것으로 파악됨.
2.주력 OS 로는 서버는 Win2012 R2 이고, PC 는 Windows 10 임.

4. 설치된 프로그램 현황

2024.1 월 이전	2024.02	증감
280	288	+8

1.귀 기관에는 24 년 1 월 이전까지 280 개의 프로그램이 설치되어 있었고,.
2.2 월 8 개가 추가로 설치되어 2 월말 기준 288 개의 프로그램이 설치되어 있는 것으로 파악됨.
3. OS 및 드라이버 프로그램은 제외하였으며, 설치 프로그램 현황은 별첨 참조

5. 금월 추가 혹은 삭제된 프로그램 내역

구분	프로세스명	분류	프로세스 설명	권고사항
추가	dell supportassist	관리툴	델 PC 관리 프로그램	없음
	kollus player	보조	인터넷 강의 동영상 플레이어	없음
	aomei backupper	보조	백업 및 복구 프로그램	없음
	경리스웨어	업무	경리 프로그램	없음
	xp-builder	업무	LS 전기 PLC 시뮬레이터	없음
	explorerpatcher	관리툴	윈도우 보조 프로그램	없음
	serviceipchange	업무	LS 전기 프로그램	없음
	mcafee security scan	백신	맥아피 백신 프로그램	없음

1.금월에 추가 설치된 프로그램은 모두 업무에 관련된 것으로 특별한 조치가 필요하지는 않으나,
2.향후 저작권 분쟁 등에 대비하여 정식으로 구입하지 프로그램은 삭제할 것을 권고 드림.

6. 사용 중인 백신 프로그램 현황

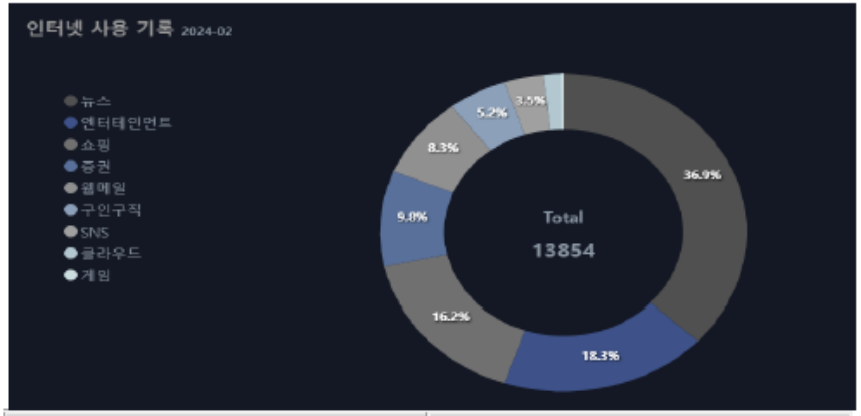
제조사	제품명	사용자 수
안랩	V3	83
이스트시큐리티	알약	105
Microsoft	디펜더	1,437

9. 보고서 예시(실 데이터)

Norton	AntiVirus	43
Avast	Free Antivirus	2
McAfee	Antivirus	7
합계		**1,677**

1.백신 프로그램은 혼재되어 사용 중이며, 중복으로 설치한 사용자도 존재함.
2.백신 중복 설치는 권장하지 않으며, MS 디펜더 백신 사용자가 압도적인 상태인데,
trueEP 의 MS 디펜더 백신 지원 기능을 활용하시면 더욱 편리하게 운용하실 수 있음.

7. 인터넷 사용 현황



구분	접속 횟수
뉴스	5,116
엔터테인먼트	2,534
쇼핑	2,251
증권	1,356
웹메일	1,156
구인구직	718
SNS	481
클라우드	211
게임	31

인터넷 접속 기록을 카테고리별로 분류한 것임.

☞ 해당하는 정책을 설정한 경우에만 이 현황을 확인할 수 있음.

8. PC 사용 현황

구분	사용횟수
웹브라우저	131,705
오피스	82,007
메신저	75,805
기타	45,999
메일 클라이언트	45,742
원격제어	2,314
화면캡처	1,528

9. 개인정보 문서 탐지 현황

사용자	개인정보 문서	구분	탐지 일시
이 XX	23 연말정산.zip	전송	2024-02-01 09:15:26
임 XX	○○산림엔지니어링.xls	전송	2024-02-01 09:15:33
최 XX	23 년 주식등변동상황명세서.xls	전송	2024-02-01 09:16:40
최 XX	주주명부.pdf	전송	2024-02-01 09:18:44
최 XX	2023 년 근로연말.zip	전송	2024-02-01 09:36:05

☞ 개인정보 정책을 설정한 경우에만 이 현황을 확인할 수 있음.

10. trueEP 운영 현황

버전별	설치 대수
2. 0. 23. 1023	1,559
합계	**1,559**

운용 모드	운용 대수
차단 모드	0
탐지 모드	1,559
미관제 모드	0
미접속	0

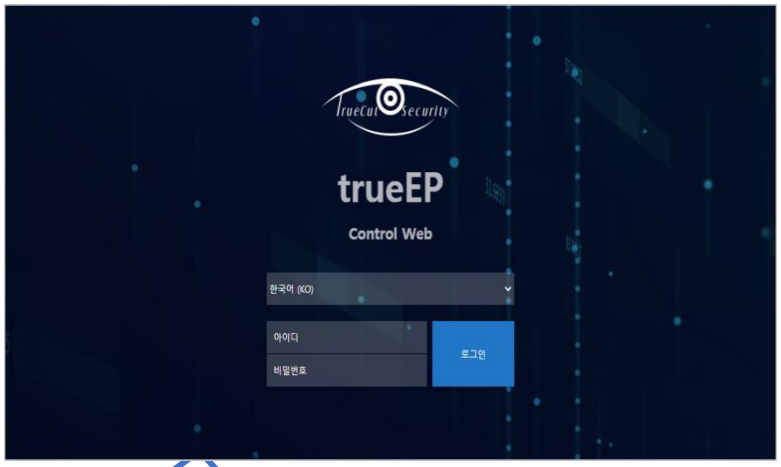
■ trueEP 최신 버전은 2.0.23.1023 이며, 최신 버전으로 운영하실 것을 권장합니다.
☞ trueEP 는 차단 모드로 운영하실 것을 권장합니다.

10. 제품 구성도

에이전트 - 보안기능 수행

에이전트
+ 각각의 엔드포인트에 설치
+ 실제 보안기능을 수행
+ 오프라인일 경우에도 보안기능 수행
+ 스텔스 모드 설치 시는 보이지 않음
+ Windows XP/7/8/10(32/64bits) 지원
+ WindowSVR 2003/2008/2012/2018 지원

매니저 - 통합관제 및 정책설정



매니저웹
+ 차단로그 검색 및 분석
+ 사용자 정보 관리
+ 접속 관리자 통제
+ 전체 혹은 그룹별 정책 설정
+ Agent Patch 작업
+ 기타 Agent 관리

대시보드 - 모니터링

대시보드
+ 상황별 차트그래프
+ 실시간 로그 동적 디스플레이

11. 인증서 (보안기능확인서 / GS인증서)

보안기능확인서

Verification of Security Function Test

발급구분	신규발급	발급번호	VSFT-KSEL-20240007
제품유형	엔드포인트 보호 제품	제 품 명	trueEP v2.0
S/W 명칭	trueEP v2.0 Manager.exe tureEP v2.0 Agent.exe		

H/W 모델

소프트웨어 제품으로 해당사항 없음

※ 발급 제품이 탑재되는 모든 H/W모델은 '시험결과보고서'에 기재되어 있음

신청기관	(주)트루컷시큐리티	제 조 사	(주)트루컷시큐리티
효력만료	2029년 03월 20일		

상기 제품이 국가용 보안요구사항에서 요구하는 보안기준을 만족하였음을 확인합니다.

2024년 03월 21일

KSEL (주)한국아이티평가원 대표이사

Level 1

GOOD Software

Certificate of Software Quality

Name of Company / Name of Applicant	:	Truecut Security,Inc.(211-87-85895)
Name of Software	:	trueEP V2.0
Certification Level	:	Level 1 (Level 1 is higher than level 2.)
Certification No.	:	21-0093
Manufacturer and Country of Manufacture	:	Truecut Security,Inc./Republic of Korea
Date of Certification	:	2021. 2. 18
Additional Information	:	

Level 1

Software

I hereby confirm that the quality of the foregoing software has been certified under Article 20.3 of the Software Promotion Act and Article 6.1 of its Enforcement Decree.

2021. 2. 18

TTA CEO & President
Telecommunications Technology Association

트루이피는
세계에서 가장 작고, 유일한
능동형 보안제품 입니다

트루컷시큐리티
TrueCut Security, Inc.