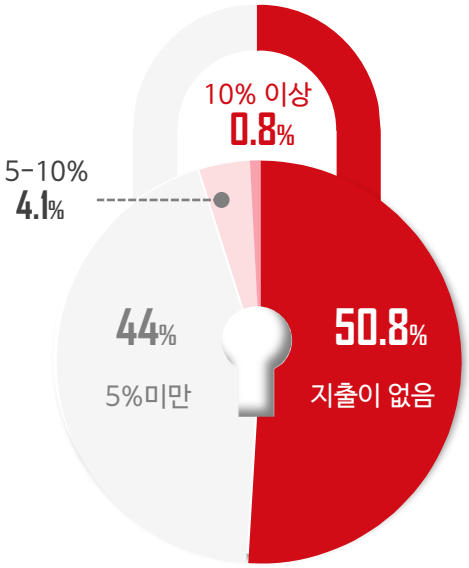

트 로 이 컷
서 비 스 소 개 서

TrojanCut

현 보안 상황

보안 지출

이대로 괜찮을까?

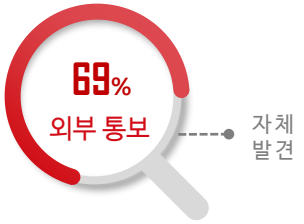


정보화 투자 대비 정보보호 투자 비율

*기준: 종사자 수 5명 이상,
네트워크로 연결된 컴퓨터 1대 이상인 사업체

불안한 지표

침해 발견까지 520일 소요



스스로 발견하기 어려운 현실

보안시스템의 96%가 우회 가능

안보 위험, 여전

기존 보안 시스템의 한계

해킹 시달리는 국토부…'기반시설' 보안 뚫릴라

하나투어, 고객 정보 얼마나 유출됐나

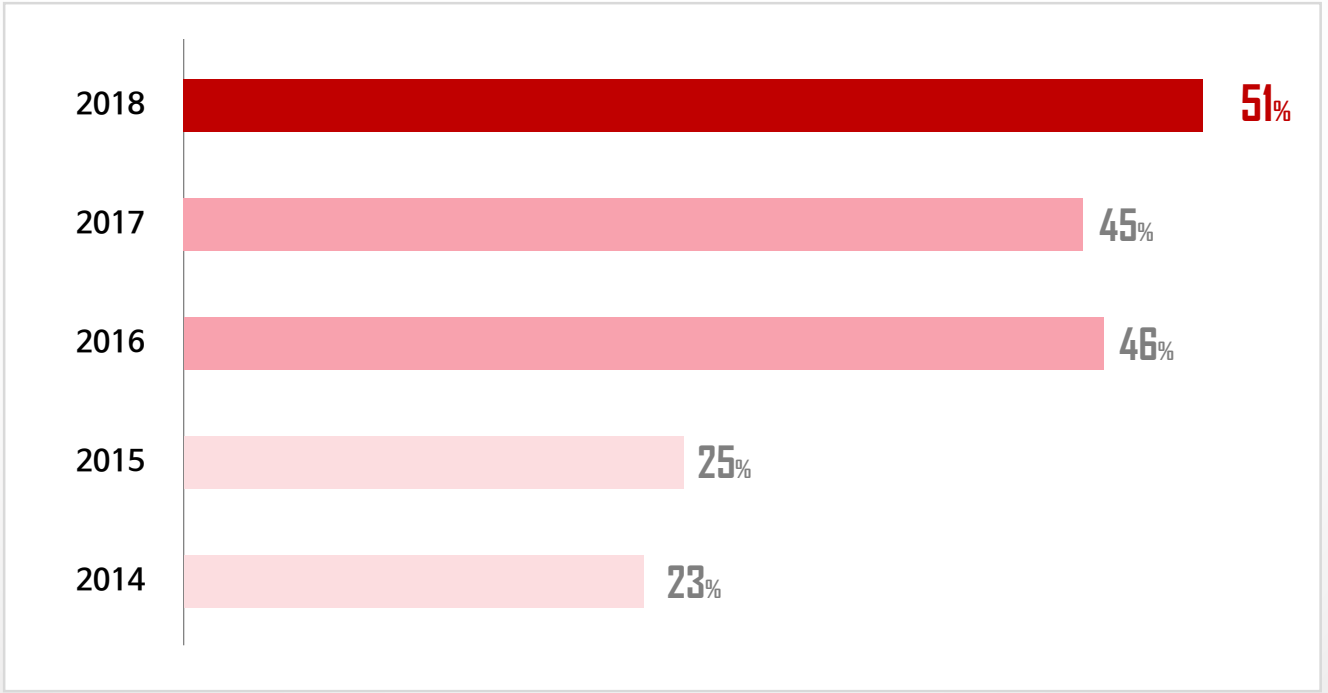
해커 호구 '대한민국'…랜섬웨어 등 '한국'만 노려

국방부 "국방망 해킹은 북한 소행"…관련자 20여 명 징계

방어기술의 현실

‘소속 조직이 사이버보안 기술 부족문제를 겪고 있는가?’라는 질문에 **‘그렇다’**고 대답한 비율

2018년,
51%의 응답자가 자신의 조직에서 사이버보안 기술 부족으로 문제가 되고 있다고 밝혔다



망 분리: 극단적 선택

극단적선택

네트워크와의 연결을 끊는 것
이외엔 대안이 없다는 결론

막대한부담

구축비와 운영비가 두 배 증가
엄청난 업무효율 저하

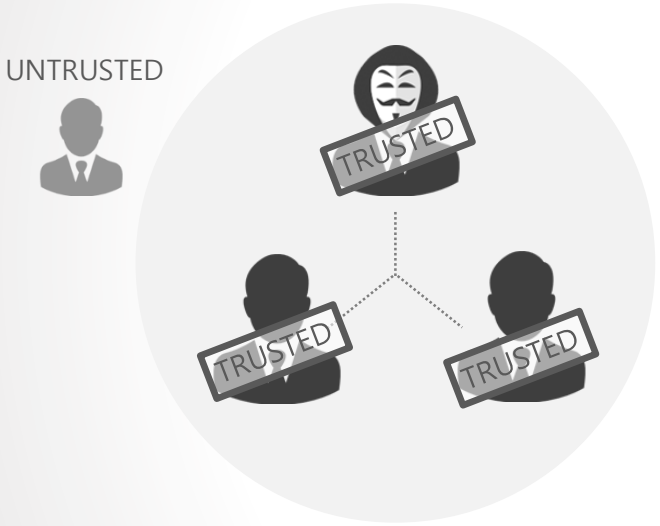
태생적한계

망과 망 사이 불가피한 접점
Human Error문제 상존

망 분리라는 특단의 선택을 한 이상,
망 분리 이전의 방어 개념은 버려야 합니다

정보보안모델의 변화

기존 모델

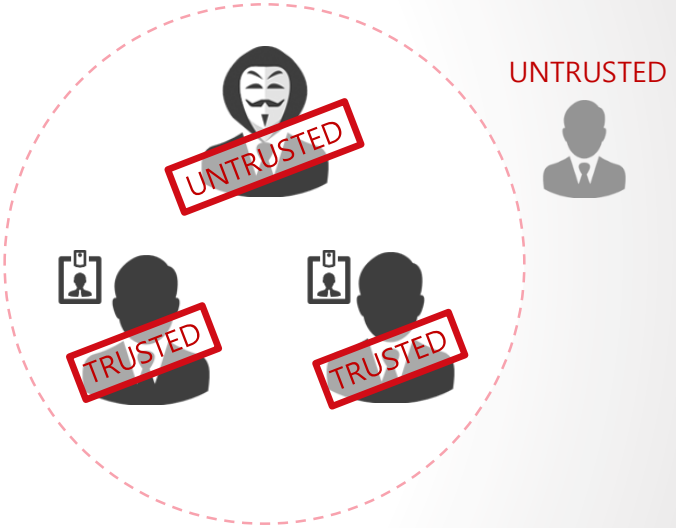


외부 침입자만 경계

내부의 적은 의심하지 않음

Security Perimeter surrounds the organization

Zero Trust Model



기존 모델의 한계 극복

내부의 적도 식별 가능

Security based on *Identity*, not on *Perimeter*

차세대 방어요건

01

우회가 가능해선 안 된다

해커는 이미
우회 방법을 알고 있다

02

패치없이 막아야 한다

아무리 빠른 패치도
해커보다 빠를 수는 없다

03

악성코드는 잊어라

일일 악성코드 100만개 시대
악성코드 없는 공격도 있다

개발 배경 (1)

"국가기관의 알려지지 않은 해킹을 막기 위한 목적으로 개발"

출처: SBS, 2004

2004년 7월 13일 국회,한국국방연구원, 해양수산부,해양경찰청,국방과학연구소,중소기업청,원자력연구소,공군대학,통일연구원, 전문연구원 등 10개 정부기관이 해킹을 당했다.

국정원은 이를 국가안보위협 사건으로 대처한다고 밝혔다.

개발 배경 (2)

"모든 공격에 준비된 솔루션"

2004

계기

정부기관 해킹 사건
국가기관의 요청

2007

솔루션 구현 (1)

자료유출 공격 차단 및
유출 증적 관리

2009

계기

7.7 디도스 사건

2009

솔루션 구현 (2)

좀비PC 차단

2011
솔루션 (1) & (2)
CC인증

2013

계기

크립토락커 성행
비트코인 요구

2014

솔루션 구현 (3)

랜섬웨어 공격 차단

2014
솔루션 (3)
CC인증

계기

해킹의 출발점

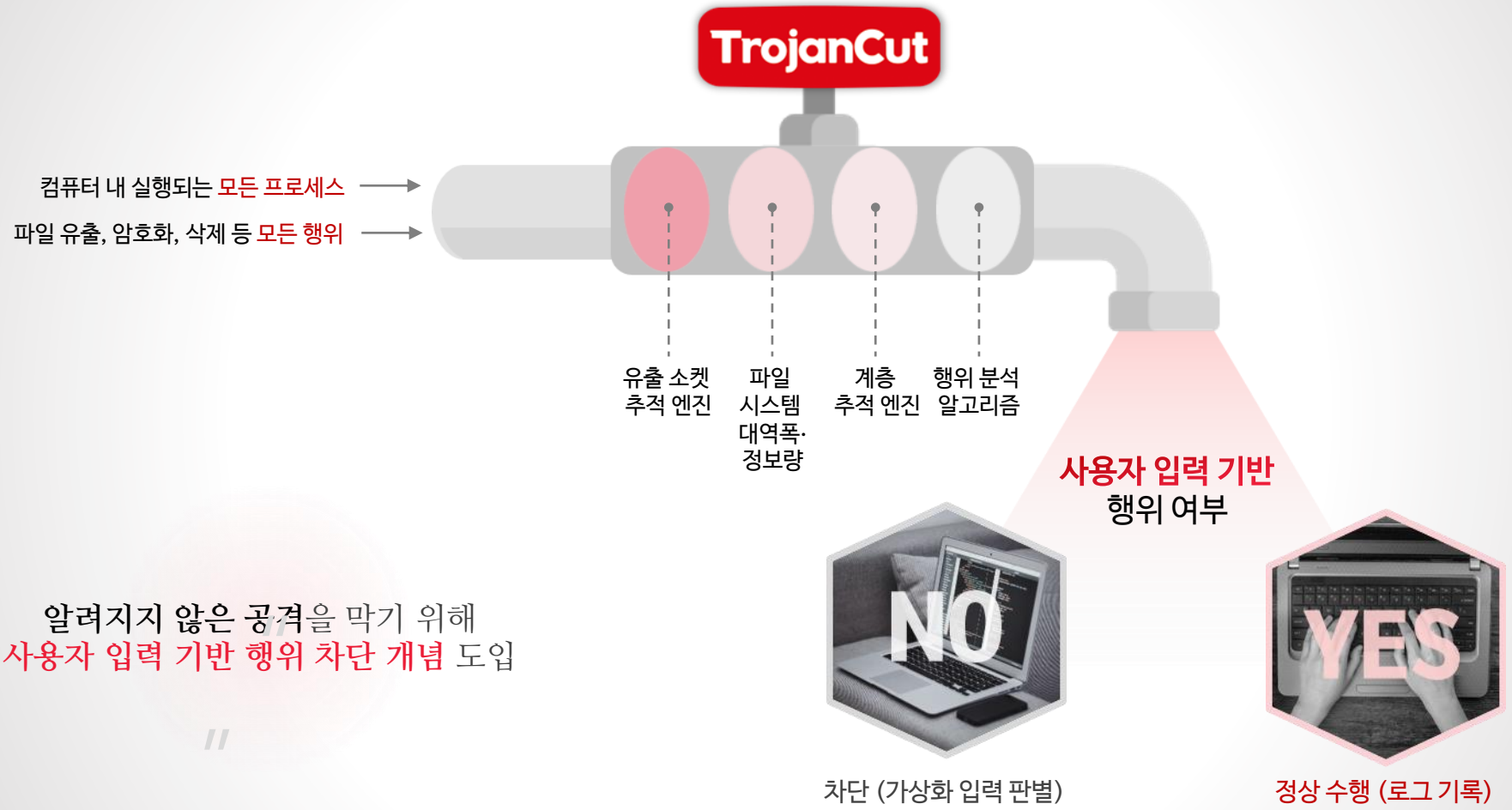
2016

솔루션 구현 (4)

패스워드 유출 공격 차단

2018
솔루션 (4)
CC인증 예정

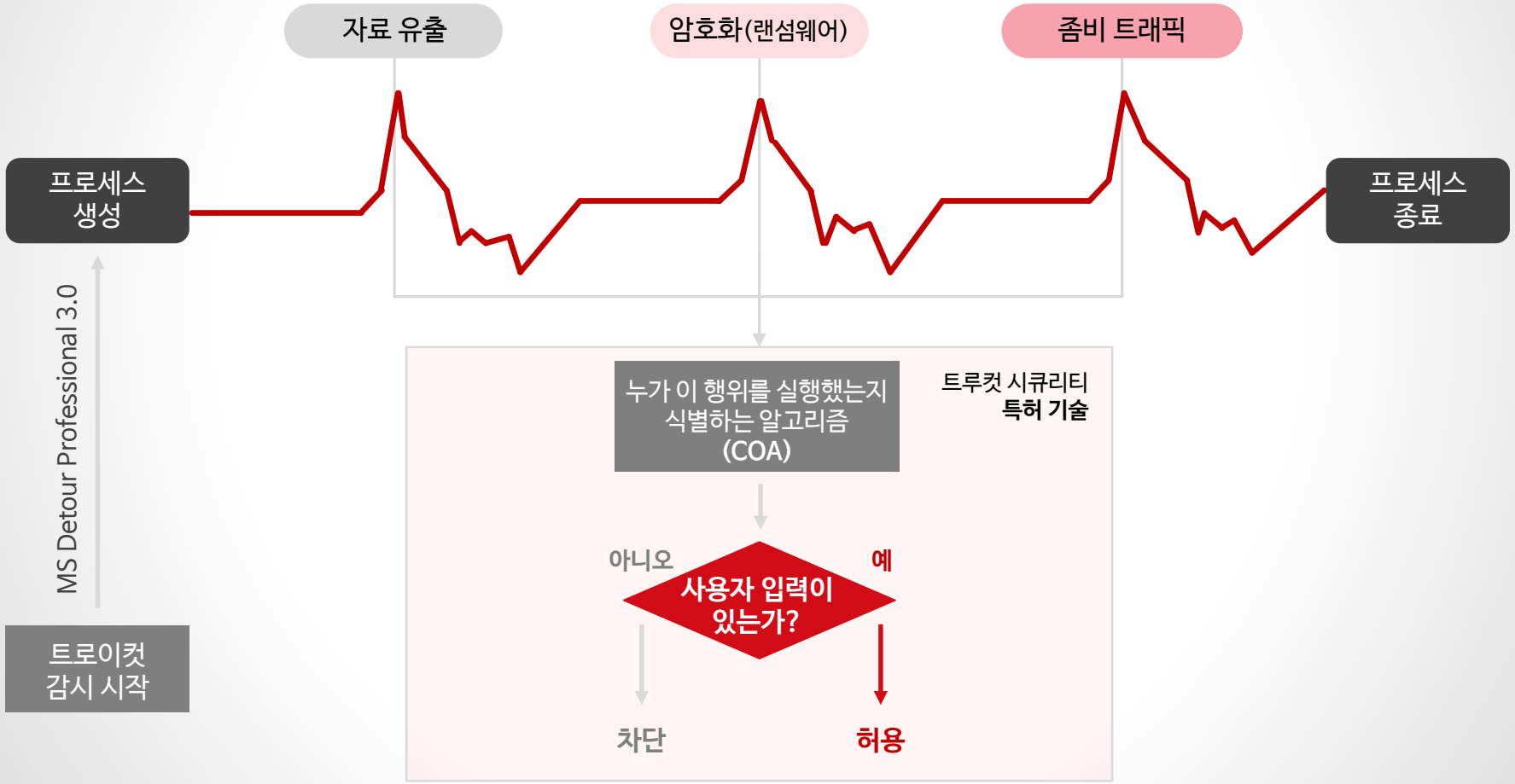
차단 개념



알려지지 않은 공격을 막기 위해
사용자 입력 기반 행위 차단 개념 도입

차단 플로우

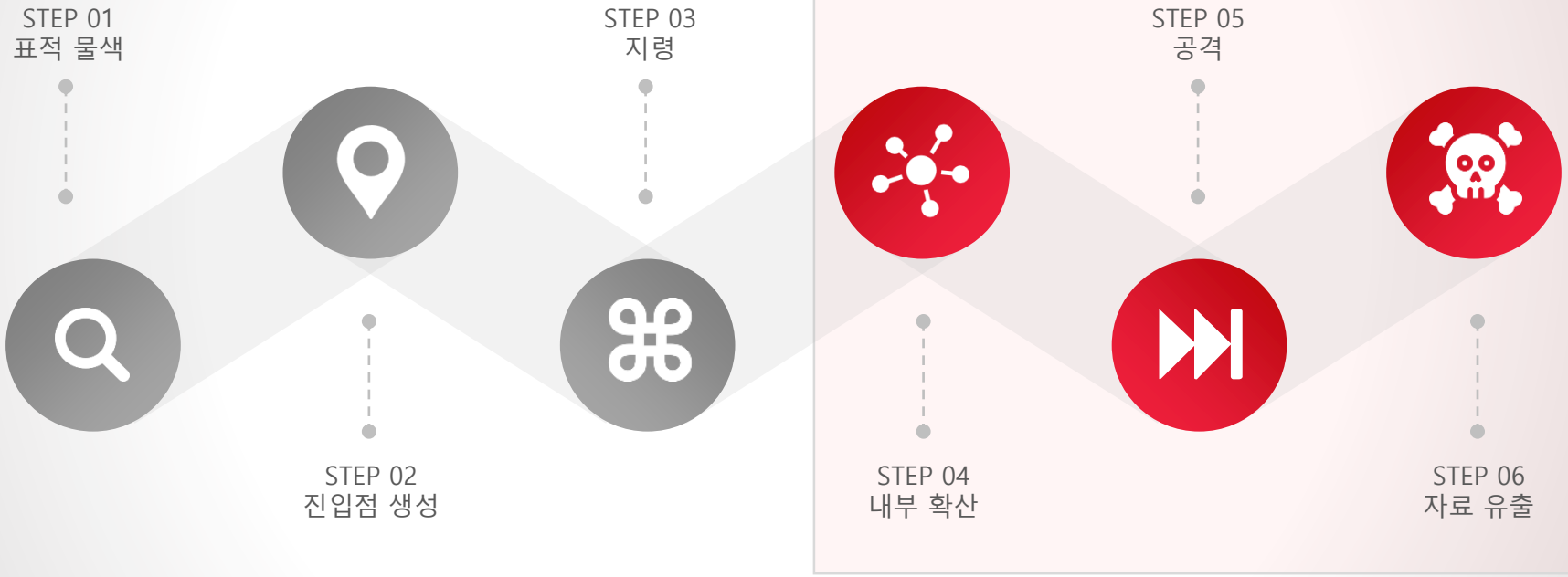
"프로세스 생애주기 감시"



APT공격의 6단계

전통적 방어체계 "정보를 알아야 막을 수 있는 기법"

트로이컷 방어체계 "정보를 몰라도 막을 수 있는 기법"



시그니처 기반 패턴 비교 · 가상머신 기반 행위 분석 · C&C 차단 등

사용자 입력 기반 악성 행위 차단

기술 수준


1세대
알려진 정보로 방어
시그니처 기반 악성코드 탐지
등록된 지문과 비교
전통 보안제품들
2세대
시뮬레이션 결과로 방어
가상공간 악성행위 탐지
실행결과를 등록 목록과 비교
가상머신 (Sandbox) 제품
3세대
학습기반으로 방어
침해 지표 탐지
침해 지표를 찾아 경고
NGAV 제품들 (차세대, AI)
4세대
실행위만을 보고 방어
리얼 공간 악성행위 차단
사용자가 의도하지 않은 행위 차단
트로이컷 특허 기술
기술이 변해야 보안이 산다!

기술 비교

"변하는 것은 기준이 될 수 없다!"

트로이컷		타 제품
사용자 입력 유무	판단 기준	설정된 시나리오 혹은 상황과의 일치 여부
컴퓨터 내에서 실행되는 행위에 대해 사용자가 직접 실행시킨 것인지 아닌지 판단	설명	컴퓨터 내에서 실행되는 행위에 대해 업체가 설정해 둔 범주에 드는지 아닌지 판단
사용자입력은 불변의 조건 해커가 알아도 우회가 불가능함	차별성	'업체가 설정한 범주'는 업체의 생각일 뿐 해커가 그대로 한다는 보장이 없음
컴퓨터의 동작원리에 기반한 "근원적 차단 기술"	가치	계속 업데이트 해야 방어가 가능한 "비근원적 차단 기술"

주요기능

자료해킹 차단

- 해킹에 의한 자료유출 차단
- 사용자 모르게 일어나는 유출사고 (APT공격) 차단

좀비PC 차단

- 업무PC에 의한 좀비PC 공격차단
- 원인미상의 네트워크 마비 트래픽 (DDoS공격) 방어

랜섬웨어 공격 방어

- 파일 암호화(랜섬웨어) 공격 차단
- 접근 경로와 무관, 실제 행위시 차단
- 전자동 스마트 백업기능 지원

패스워드 유출차단

- 사용자 PC계정정보 탈취 차단
- 관리자 권한 및 접근 권한 탈취 차단

사고추적

- 자료전송 사고추적(증적관리)
- 해킹에 의한 유출 관리 뿐 아니라 정상적 전송 증적관리 가능

화이트 리스트

- 인가된 프로세스만 접근허용
- POS, ATM기기 전용

랜섬웨어 차단(1)

방어대책	방식	한계성
악성행위 차단 방식 (트로이컷)	▪ **트로이컷만의 독자적 방식** ▪ **사용자가 실행하지 않은 암호화행위 차단**	▪ **알려지지 않은 공격까지 근원적으로 방어가 가능한 유일한 기술**
백업 방식	▪ 데이터 복사본을 저장하는 방식	▪ 공격 자체를 방어하는 개념이 아님 ▪ Doxware(암호화+자료유출)공격에 무방비
랜섬차단 방식	▪ 알려진 랜섬웨어 차단 ▪ 미끼파일 이용 / 평판기반 차단 / 임계치기반 차단	▪ 알려진 정보를 갖고 그 정보에 기반하여 차단 ▪ 알려지지 않은 신, 변종 랜섬웨어에 무방비

랜섬웨어 이중 방어

랜섬공격 실시간 차단

- 랜섬웨어 종류와 상관없이 실시간 차단
- 랜섬공격 프로세스 및 실행 파일 삭제

스마트 백업

- 전자동 스마트 백업
- 파일 수정 시점, 전자동 증분 백업
- 전용 복구 툴만 접근 허용 영역

랜섬웨어 차단(2)

"랜섬공격 완벽방어를 위한 스마트백업"

01

보호 문서에 대해
실시간 스마트 백업 기능 제공

02

최초 설치 시
1회 **전자동 Full 백업**

03

스마트 백업 영역
Stealth & Access **Protection**

04

파일이 수정될 때마다
해당 파일 **전자동 증분 백업**

05

백업공간
크기 조정 가능

06

백업 룰(Rule)
설정 가능

07

전용 복구툴에 의해서만
접근 가능

특장점


01
배포파일 크기 10MB 미만
실행파일 크기 2MB 미만
CPU 사용률 최대 3% 미만
메모리 사용 4MB
초 경 량
02
시그니처 DB 없음
Rule 테이블 없음
업데이트
최 소 화
ALL
-IN-
ONE
검사실행
불 필 요
04
실시간 악성행위차단 알고리즘
COA (Cut On Active) 방식
03
No Process · No Folder
No Pop-up · No Icon
No Registry
스 텔 스
모 드
다 용 도
05
웹서버·POS·ATM 유출 차단
웹서버·POS·ATM 전송 감사
웹서버·POS·ATM 위변조 차단

편의성

업 무 지 속 가 능

01

실시간 원격 차단모드 해제
실시간 원격 감시모드 해제
실시간 원격 실행 종료
실시간 원격 설치 제가

02

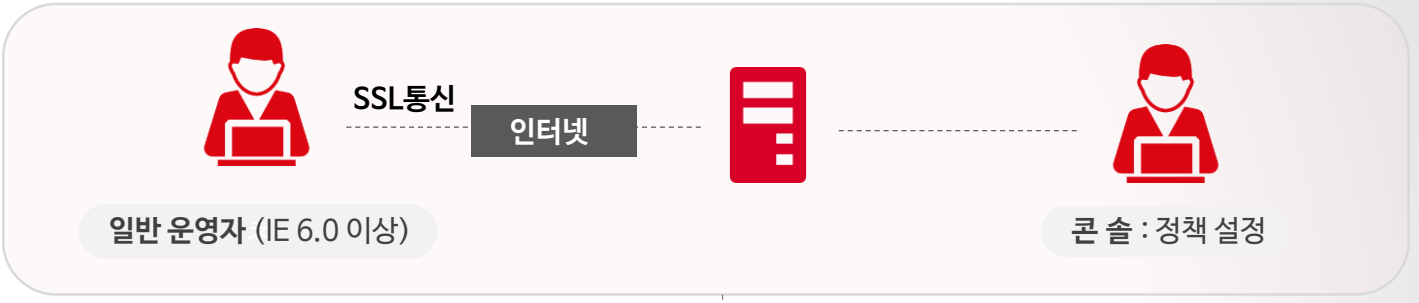
예외처리대상 자동 검출
개발사 등록 출고
고객 자체 등록
권장사항 제공

예 외 처 리 등 록

제품 구성

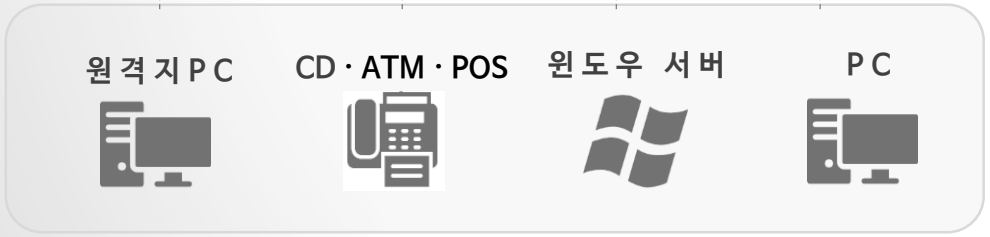
서버데몬 + 관제 웹

전송/차단 현황 조회
에이전트 접속 현황 및 관리기능
기간 설정 자동 보고서 작성 기능
운영자 접속 통제 기능 수행



SSL통신

인터넷



서버와 통신
실시간 탐지 · 차단 기능 독자적 수행
실시간 정책 반영 : Full/Push 방식 제공
관제 서버 DB에 실시간 로그인, 팝업 등 수행

클라이언트에이전트

통합관제화면


LOG
PROCESS
DESTINATION
USER
TIME
CHINA
AMERICA
16 1942
세계최초 신개념 악성행위 차단 시스템

특허 및 인증

2007 01.25

특허 제10-0676912호

차세대 '사용자입력 행위기반'의
악성행위 차단 기술

2007 10.09

GS 인증 제07-0171호

사용자입력 행위기반'의
악성행위 차단 메커니즘 유일 인증

2010 01.11

중소기업청 인증

산업보안기술개발 사업 성공판정

2011 01.14

국정원 CC인증 CISS-0293-2011

알려지지 않은 악성코드에 의한
자료유출방지 및 좀비PC 무력화 기능 유일 인증

2015 06.02

국정원 CC인증 CISS-0609-2015

악성 행위 및 랜섬웨어 공격 차단 기능 유일 인증

레퍼런스

대한민국 보안 1등 기관과 기업은 모두 트로이컷을 사용하고 계십니다

국가, 공공

금융

방위산업

기업

병원, 학교

POS보안 롯데마트

보안관제협약 청주상공회의소

SECURITY BIBLE

보안의 시작은 상황을 제대로 인식하는 것이다

해커는 제약이 없고 막는 자에겐 제약투성이다

도둑을 잡으려 하지 말고 도둑질을 당하지 않도록 해라

일일 악성 코드 백만 시대

제품 평가의 핵심은 내일도 막을 수 있는 지 확인하는 것이다

랜섬 공격 앞에 침묵을 지키는 전통 보안의 실체를 바로 알자

㈜비즈엠티

- 제품문의: 02-701-4994
- 이메일: Marketing@bizmt.co.kr
- 담당자 :최준원 상무