

모바일·IoT 안티 해킹 솔루션
OnTrust

간편한 SW 설치로 실시간 탐지부터 관제·검사(분석)까지

2025.01

Contents

1. 제안배경
2. 제품소개
3. 기대효과
4. 적용분야
5. 인증 및 수상
6. 특허
7. 레퍼런스



AI based Cyber Security Company

 OnTrust

모바일·IoT 안티 해킹 솔루션
OnTrust

 OnAV

모바일·IoT 안티바이러스
OnAV

 OnAppScan

AI 악성 앱 자동분석 시스템
OnAppScan

 OnAV for
Linux Desktop

리눅스 OS 안티바이러스
OnAV for Linux Desktop

1. 제안배경 (1) 안드로이드 OS 취약성

안드로이드 OS, 타 OS 대비 취약점 다수 존재, 정보탈취 및 서비스거부(DoS) 유형 다수

<https://www.cvedetails.com/>

Product Search

Android

8,089

Product Type: Application Operating System Hardware

#	Product Name	Vendor Name	Number of Vulnerabilities
1	Android	Motorola	2
2	Android	Samsung	327
3	Android	Google	7449
4	Android	Android	0
5	Android Tv	Google	0
6	Android-msm	Codeaurora	11

Product Search

iOS

0 (Apple)

Product Type: Application Operating System Hardware

#	Product Name	Vendor Name	Number of Vulnerabilities
1	IOS	Cisco	615
2	IOS	Apple	0
3	Ios Rom Monitor	Cisco	1

[위험 유형별 안드로이드 OS 취약점]

Year	코드실행	탐지우회	권한상승	서비스거부	정보유출
2015	70	3	3	56	17
2016	72	33	59	106	87
2017	201	29	235	87	116
2018	58	1	63	34	106
2019	92	2	3	37	216
2020	40	14	17	49	273
2021	28	17	16	35	193
2022	17	54	69	107	290
2023	24	5	10	274	497
2024	16	0	6	65	133
2025	6	0	0	7	18
Total	624	158	481	857	1946

Cisco iOS는 시스코라우터 및 스위치용 OS로 모바일 디바이스(스마트폰/IoT)용이 아님

1. 제안배경 (2) 사이버 위협 생태계 진화

취약점 거래 산업화 및 제로데이 공격 활성화

네트워크 중간자 공격·악성 URL 이용한 피싱 등 다양한 경로로 해킹 시도

취약점 거래 전문 기업, 관련 시장 형성

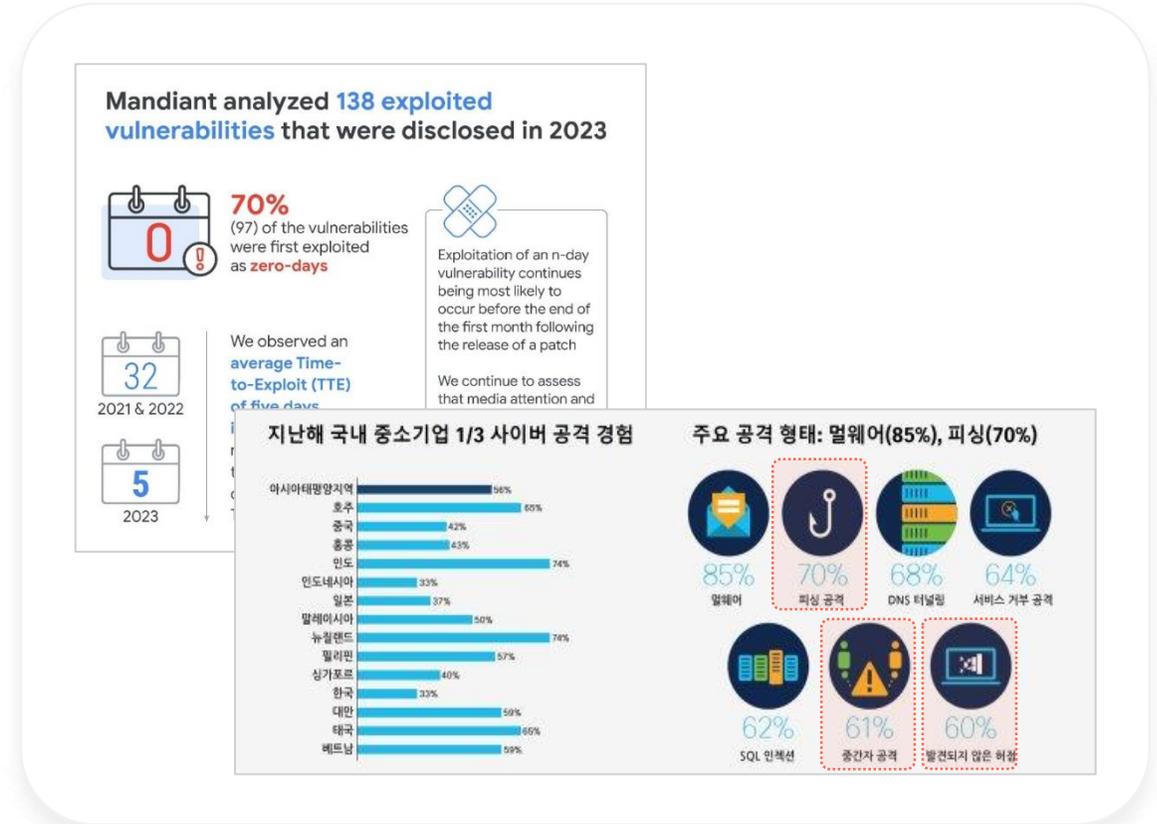
- 미국 '제로디움', 러시아 '옵제로' 등
- 경쟁적으로 취약점 매입 및 고액의 대가 지불
- 취약점 브로커 및 스파이웨어 개발사, 목적에 관계없이 취약점 판매 (그레이햇)

제로데이 취약점 악용 공격 활성화

- 구글 사이버 위협 인텔리전스 그룹 맨디언트 발표(2024.10)
- 2023년 공개된 138개 취약점 공격 중 70%가 제로데이 공격
- 제로데이 취약점 공개 후 실제 공격에 악용되기까지 걸린 기간 5일

다양한 사이버 공격 유형 혼재

- 시스코 발표, 2020년 국내 중소기업 1/3 사이버 공격 경험
- 멀웨어 공격 외에도 피싱, 중간자공격(네트워크), 제로데이 공격 등 다양한 유형 존재
- 기기 해킹 후 데이터 탈취, 음성 도·감청 등 다양한 악성 행위 진행 (ex 스파이웨어 폐가수스, 제로데이 공격으로 침투해 음성 도·감청 실행)



1. 제안배경 (3) 구형 모바일·IoT 보안 위협

보안 업데이트 종료된 구형 모바일 및 IoT 기기 사이버 공격 위협에 노출

모바일·IoT 기기 수명 연장에 따른 보안 이슈

- 기기 성능 과도화 및 고가 판매전략, 인프라형 IoT 증가 등의 요인으로 구형 모바일·IoT기기 수명 연장
- 오래된 보안 규정 반영, 업데이트 종료 등으로 보안 위협에 취약
- 업계 추산 기기 교체 수명, 스마트폰 평균 36개월

보안 위협 대응에 부적합한 '홈 네트워크 설비' 교체 주기 규정

- 2021년 월패드 해킹 사건 이후 개정된 '지능형 홈네트워크 설비 설치 및 기술기준', 망분리 등 네트워크 보안에 집중
- 공동주택관리법 장기수선계획 수립 기준 상 지능형 홈네트워크 설비교체 주기, 홈넷 기기 10년, 공용시스템 장비 20년 규정
- 공격 기술 발전 속도에 비해 지나치게 길어 최신 공격에 대응 불가



1. 제안배경 (4) 기존 기술의 한계

기존 OS 보안 솔루션, 보호 대상 기기 및 기능 한정적

솔루션 제공자 별 한계

스마트폰
제조사
제공 솔루션

특정 제조사·브랜드 단말만 보호
단말 제조사 제공 OS 보안 솔루션
해당 제조사 단말/프리미엄 모델에 국한된 보호 제공

안드로이드
OS 기업
제공 솔루션

앱 보호 목적 제한된 보호 기능
구글 '장치 무결성 검사' 기능, 루팅된 장치로
앱에 접근해 보안 우회 등의 행위를 할 수 없도록 예방
안드로이드 모바일 기기 한정, IoT기기 보호 불가

보안기업
MTD
(모바일위협방어)
솔루션

관리 및 관제 편의 기능 한계
솔루션에 따라 원격 관제, 신속검사, 해킹된 단말 복구
등 관리 편의 기능 일부 제공

스마트 환경 특성상 한계

구형 IoT 인프라
다수 존재

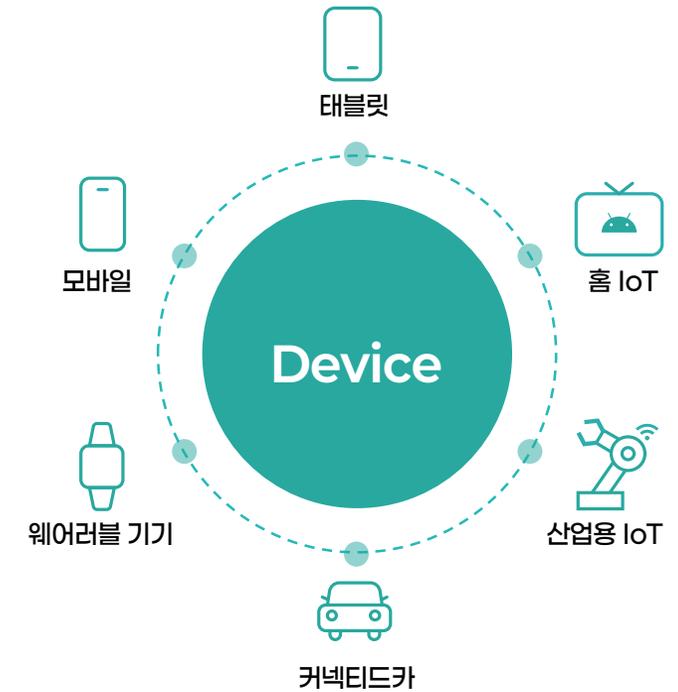
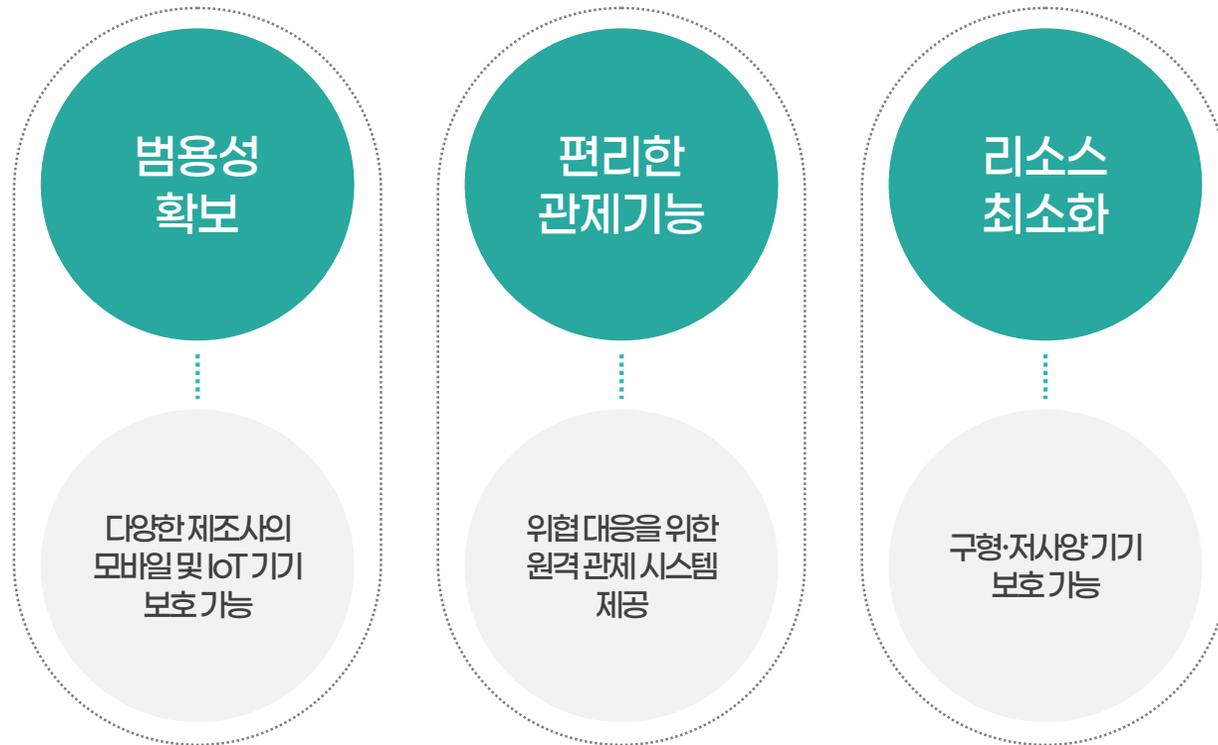
보안 업데이트 지원 불가 기기 다수 존재
기존 유통된 구형/저사양 기기에 대한 보안 공백
국내 스마트아파트 열풍 시기는 2011년 이후이나,
대다수 안드로이드 보안 솔루션은 2015년 출시된
안드로이드 6.0 이상 OS부터 지원

다양한 제조사
장비로 구성된
스마트시스템

통합 관제 및 관리 편의 확보 어려움
월패드, 도어락, IoT가전 등 스마트홈을 구성하는
장비 별, 제조사 및 도입시기(모델) 별로 보안 수준 상이
보안 관제 등 통합 시스템 구축 및 가시성 확보 어려움

1. 제안배경 (5) 해결 방안

제조사 제한 없이 OS 보호 기능을 제공하여 솔루션의 범용성을 대폭 강화

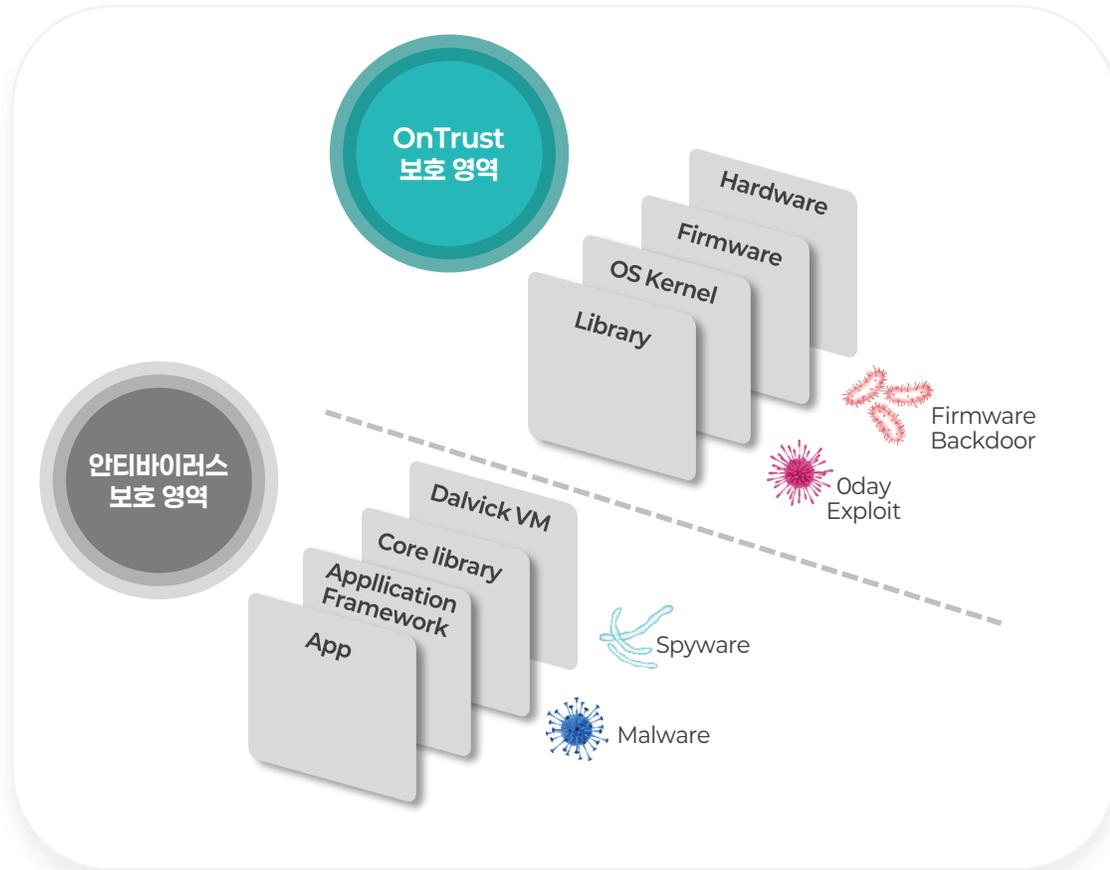


[시큐리온 OnTrust 보호 가능 기기]

2. 제품소개 (1) 개요

OnTrust, 모바일·IoT 단말 OS 보호를 위한 안티 해킹 솔루션

OS 해킹 외 네트워크 공격, 음성 도·감청 공격, 악성 URL 공격에 대한 탐지 제공

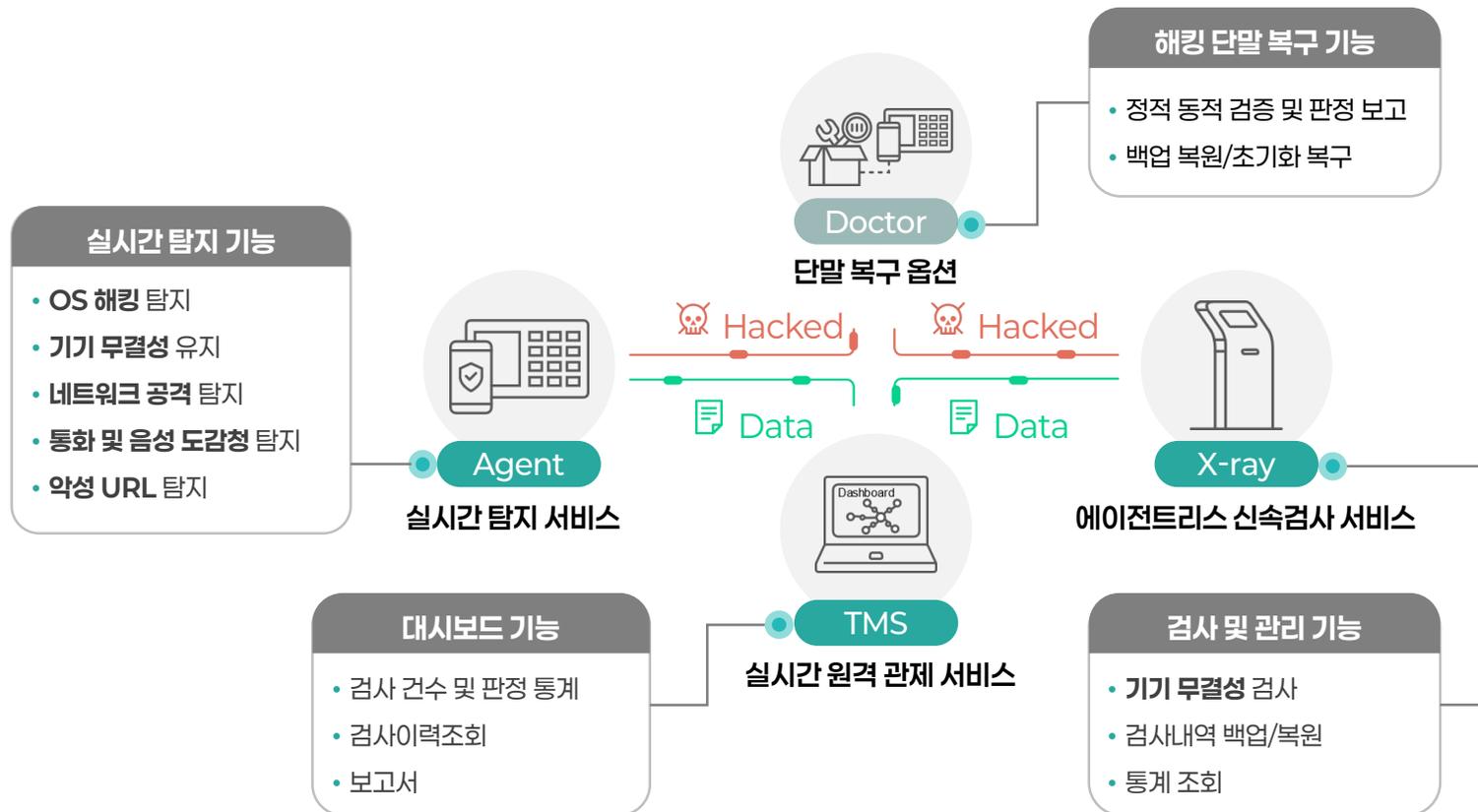


2. 제품소개 (2) 주요 기능

위협 탐지, 관제, 검사의 기능별 서비스 및 해킹 단말 복구 옵션으로 구성

실시간 위협 탐지 에이전트(App or SDK), 위협 관제(Threat Management System),

에이전트리스 방식의 신속 검사 지원



기능별 맞춤형 시스템 구성 예시

- ✓ 기업 및 기관 모바일 보안 관제 시스템
- ✓ 스마트시티·스마트아파트 IoT 보안관제 시스템
→ Agent+TMS 구성(탐지+관제)
- ✓ Agent 설치 안된 불특정 다수 단말 대상 모바일·IoT 해킹 및 백도어 검사 시스템
- ✓ 보안구역 모바일 단말 반입 통제 시스템
→ X-ray 단독구성(기기 무결성 검사)
→ X-ray+Agent 구성 (기기 무결성 검사와 모바일 단말 보호를 동시에 적용해 이중 보안 시스템 구축)

2. 제품소개 (2) 주요 기능

해킹 위협 실시간 탐지를 위한 에이전트(APP 또는 SDK) 제공

● 실시간 검사 및 위협 알림

● 항목별 검사 결과와 조치 방안 안내

The image displays six smartphone screens illustrating the OnTrust Agent's security features and results:

- Screen 1: OnTrust Agent Status**
 - OnTrust Agent: Installed (루팅이 탐지되었습니다. OnTrust Agent를 실행하여 검사를 진행한 후에 검사 결과를 확인하세요. (이 알림은 기기의 루팅이 해제되기 전까지 삭제할 수 없습니다.))
 - OnTrust Agent: Running (스마트폰을 안전하게 보호하고 있습니다.)
 - USB file transfer: Enabled (USB로 파일 전송)
- Screen 2: Wireless Security Check Results**
 - Wireless hacking prevention (무선랜 해킹 탐지): Warn (연결된 WiFi 공유기가 해킹 위험에 노출되었습니다. - 해킹 유형: ARP Redirect)
 - Wireless hacking prevention (무선랜 해킹 탐지): Warn (연결된 WiFi 공유기가 해킹 위험에 노출되었습니다. - 해킹 유형: ARP Cache Poisoning)
 - Wireless hacking prevention (무선랜 해킹 탐지): Warn (연결된 WiFi 공유기가 해킹 위험에 노출되었습니다. - 해킹 유형: 중간자(MITM))
 - Wireless authentication security status (무선랜 암호화 보안 상태): Info (연결된 WiFi 공유기가 보안에 취약한 암호화 방식을 사용 중입니다. - 현재 사용 중인 암호화 방식: [WEP][ESS])
- Screen 3: Firmware Check Results**
 - Firmware check results (펌웨어 검사 결과): Warn (변조: /system/bin/abb 경로에 파일 변조됨, 생성: /system/bin/x82 경로에 파일 신규 생성됨)
- Screen 4: CVE Vulnerability Check Results**
 - CVE-2016-0728: Warn (내용 보기) (리눅스 커널 4.4.1 이전의 security/keys/process_keys.c 의 join_session_keyring 함수는 특정 오류 발생 시 mishandles 객체를 참조해 도널 사용자 권한을 얻거나 서비스 거부할 수 있습니다.)
 - CVE-2016-2494: Warn (내용 보기) (안드로이드 OS 4.0 부터 6.0.1 중, 2016년 6월 1일 보안패치 이전의 적용 대상 중, sdcard/sdcard.c 에서 off_by_one 오류가 발생해 공격자가 Signature 또는 Signature0/System 접근 권한을 얻을 수 있습니다.)
 - CVE-2016-3861: Info (CVE 점수: 9.3)
 - CVE-2017-0781: Info (CVE 점수: 8.3)
- Screen 5: OS Check Results**
 - OS check results (OS 검사 결과): Warn (디버깅 또는 앱 후킹 탐지) (디버깅 또는 앱 후킹이 탐지되어 위험한 상태입니다.)
- Screen 6: App Security Check Results**
 - App security check results (음성, 통화 도감청 위험 검사 결과): Warn (Call Recorder) (파키지명: call_recorder.automatic.acr, 경로명: /data/app/~n9AGymyJshN4fIQ3mrpOg=/call_recorder.automatic.acr-rymizyMbGH1T6puHa_BA=/base.apk)
 - Warn (Chrome) (파키지명: com.android.chrome, 경로명: /data/app/~8oF17Ne1UbnwYEmY2g3XO=/com.android.chrome-JluJ982-kJQl2Q8Webz2=/base.apk)
 - Warn (Gmail) (파키지명: com.google.android.gm, 경로명: /data/app/~-Ys8X02CvYkPF_-fjh77FAg=/com.google.android.gm-sKm-GL76HJ9CaeVckBkMGA=/base.apk)

2. 제품소개 (2) 주요 기능

중앙 관제 TMS (Threat Management System) 기능 지원

The screenshot displays the OnTrust TMS dashboard with the following components:

- Header:** OnTrust TMS logo, navigation menu (대시보드, 사용자 관리, 검사결과, 통계), and utility buttons (비밀번호 변경, 로그아웃).
- Summary Card:** 검사건수 및 판정 통계 요약. Metrics include: 현재 검사 건수 (99), 심각 판정 기기 (34), 취약 판정 기기 (53), 미흡 판정 기기 (12).
- Line Chart:** 일간·월간 데이터. A line graph showing trends for 5개월 전, 4개월 전, 3개월 전, 2개월 전, and 1개월 전.
- Alerts List:** 당일 검사 알림 피드.

급일 검사한 Agent	1
급일 판정된 심각 기기	0
급일 판정된 취약 기기	1
급일 판정된 미흡 기기	0
- Table:** 최근 위험 판정 기기.

검사 기기	기기 보안 상태	검사일시
aa4bc302-4a7d-3125-bb94-f37a20bfa61a	● 심각	2025-02-17 02:14:08
aa4bc302-4a7d-3125-bb94-f37a20bfa61a	● 심각	2025-02-16 02:33:42
aa4bc302-4a7d-3125-bb94-f37a20bfa61a	● 심각	2025-02-15 03:27:55
aa4bc302-4a7d-3125-bb94-f37a20bfa61a	● 심각	2025-02-14 10:14:13
aa4bc302-4a7d-3125-bb94-f37a20bfa61a	● 심각	2025-02-14 03:02:36
aa4bc302-4a7d-3125-bb94-f37a20bfa61a	● 심각	2025-02-13 14:38:02
aa4bc302-4a7d-3125-bb94-f37a20bfa61a	● 심각	2025-02-13 14:14:56
aa4bc302-4a7d-3125-bb94-f37a20bfa61a	● 심각	2025-02-13 12:04:02
- Monitoring Widgets:** CPU, RAM, DISK 모니터링. Shows usage percentages for API 서버 and 관리 서버.

● 당일 검사 알림 피드

● CPU, RAM, DISK 모니터링

2. 제품소개 (2) 주요 기능

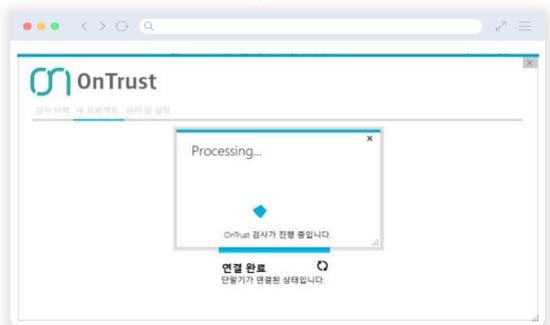
OnTrust X-ray, 에이전트 App 또는 SDK가 설치되지 않은 모바일 단말도 검사 가능

◆ 신속 검사 방법

1. OnTrust X-ray가 설치된 PC 또는 키오스크에 스마트폰, 태블릿 등 검사 대상 단말을 연결



2. 단말 검사



○ 단말기 정보		
단말기	모형명	수집일시
R3CN800595Z	SM_N981N	2021-08-12 03:54:27
○ Package Scan		
파일명	/data/app/com.sktelecom.tguard-MqJf9unGVAHLKFTi-KQm7Q==/base.apk	● 정상
검사결과	normal	
검사이름	null	
○ Device state total scan		
운영체제 버전 검사	안드로이드 7 버전 이상	● 정상
보안 업데이트 검사	보안 업데이트 존재	● 정상
최신 운영체제 사용 여부 검사	1년 이내에 볼드 된 최신 운영체제 사용	● 정상
마지막 업데이트 검사	1년 내 보안 업데이트 내역 있음	● 정상
사용자 데이터 영역 암호화 지원 여부	지원	● 정상
앱 설정 검사	알려진 앱만 설치하도록 설정	● 정상
기기 루팅 검사	정상 단말기	● 정상
SELinux 설정 검사	정상 : enforcing	● 정상
SELinux 상태 검사	동적중	● 정상
펌웨어 상태 검사	이상 없음 (기기 잠금 상태)	● 정상

● APP/SYSTEM/DEVICE 종합 검사 결과 보고서 제공

- 운영체제 버전 검사
- 보안 업데이트 검사
- 최신 운영체제 여부 검사
- 마지막 업데이트 검사
- 사용자 데이터 영역 암호화 지원 여부
- 앱 설정 검사
- 기기 루팅 검사
- SELinux 설정 검사
- SELinux 상태 검사
- 펌웨어 상태 검사

2. 제품소개 (3) 핵심 기술

실시간 해킹 탐지 '공격 흔적 조사 기술'

기기의 상태 변경에 기반한 이상 징후 추적 방식, 제로데이 공격에도 효과적 대응

공격 흔적 탐지 원리



실시간 보호

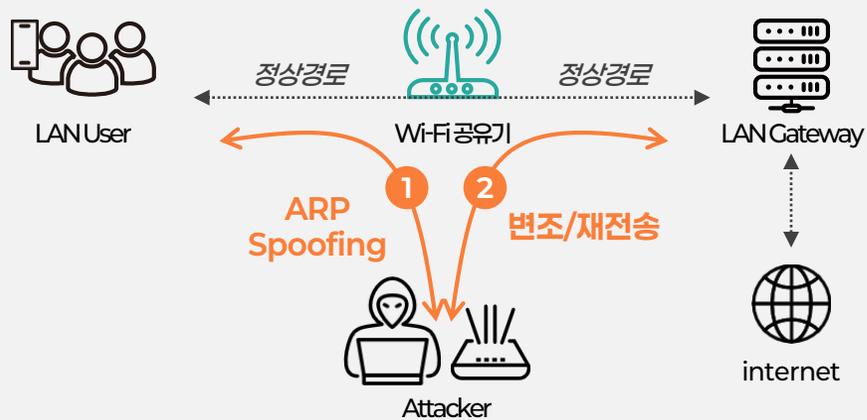


2. 제품소개 (3) 핵심 기술

연결된 유, 무선 네트워크 공격 실시간 탐지

각종 스푸핑, MITM 공격에 효과적인 대응 (일반 권한 동작)

Wi-Fi 해킹 기법(MITM) 개념도

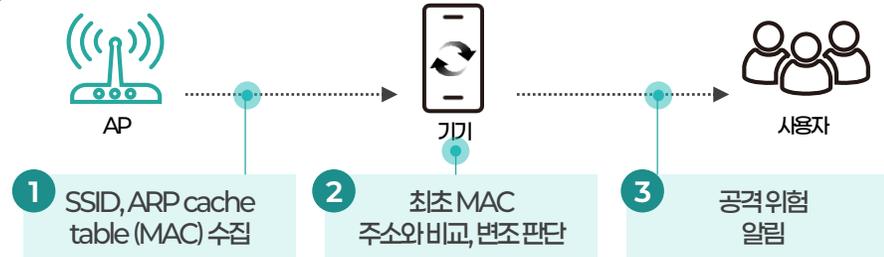


ARP (주소 결정 프로토콜) Spoofing 공격 기술

- ① 가짜 ARP 패킷을 통해 상대방의 데이터 패킷을 중간에서 가로채는 MITM 공격 (Man In The Middle, 중간자기법)
- ② 가로챈데이터를 유출하거나 변조후 재전송하여 계정 도용 등 불법행위가능

OnTrust Network Detection API

- 01 WLAN_AP_Scan
: 위험한 네트워크 감지
- 02 DNS_Spoof_Scan
: DNS 스푸핑 공격 탐지
- 03 MITM_Scan
: 중간자 공격 탐지
- 04 ARP_Attack_Scan
: ARP 리다이렉트 공격, ARP 캐시 변조 탐지



2. 제품소개 (3) 핵심 기술

스마트폰 마이크/카메라 해킹을 통한 음성 및 통화 도·감청 행위 탐지

카메라, 마이크 등 해킹 위협

※ 월패드 카메라 유출 사례, 페가수스 spyware에 의한 음성 도청, 통화 감청 사례 대응

OnTrust MIC/Call Record Detection API

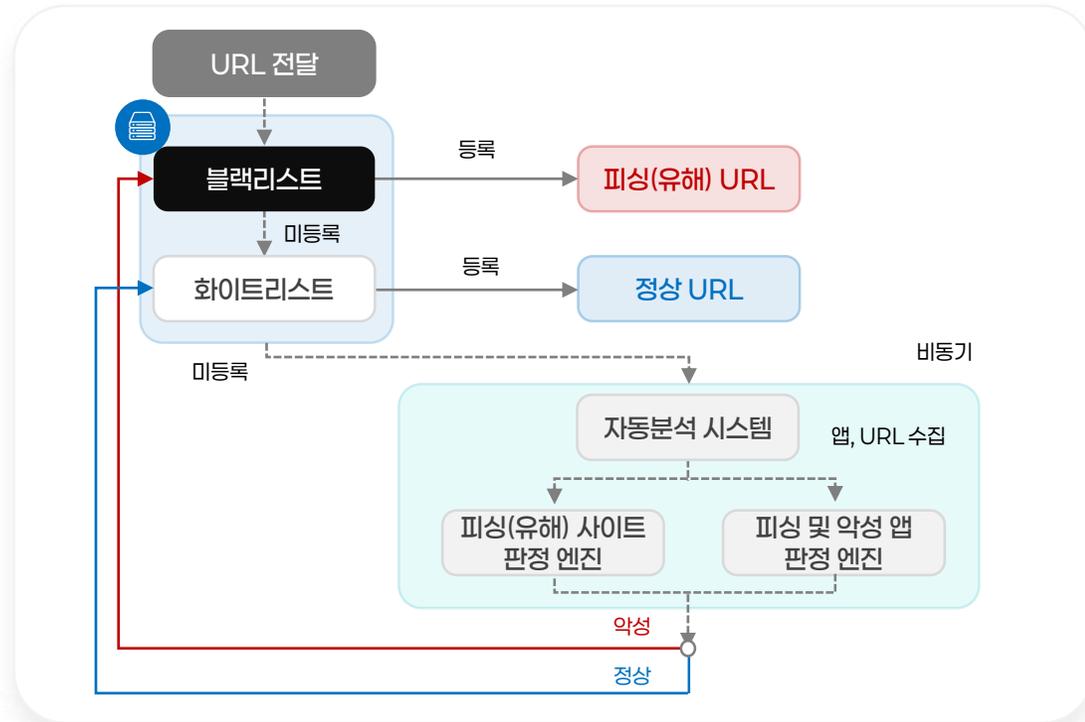
- 01 Record_Prevention**
: 실시간 도·감청 방지
- 02 Camera_Record_Scan**
: 촬영 시 녹음 기능 작동 여부 검사(수동)
위험 발생 시 해당 권한 보유 앱 리스트 제공
- 03 MIC_Record_Scan**
: 마이크를 통한 녹음 기능 작동 여부 검사(수동)
위험 발생 시 해당 권한 보유 앱 리스트 제공
- 04 Call_Record_Scan**
: 접근성 권한을 이용해 통화 녹음이 가능한
앱 리스트 제공

※ 음성 도감청 기능: 동시 녹음 미지원 기기에서 지원
통화 도감청 기능: Android 9이상에서 지원

2. 제품소개 (3) 핵심 기술

URL 자동 판정 기술로 악성 URL 탐지, 스미싱 대응

셀레니움(웹 수집/테스트 도구) 기반 URL 및 앱 자동 수집 기술 적용



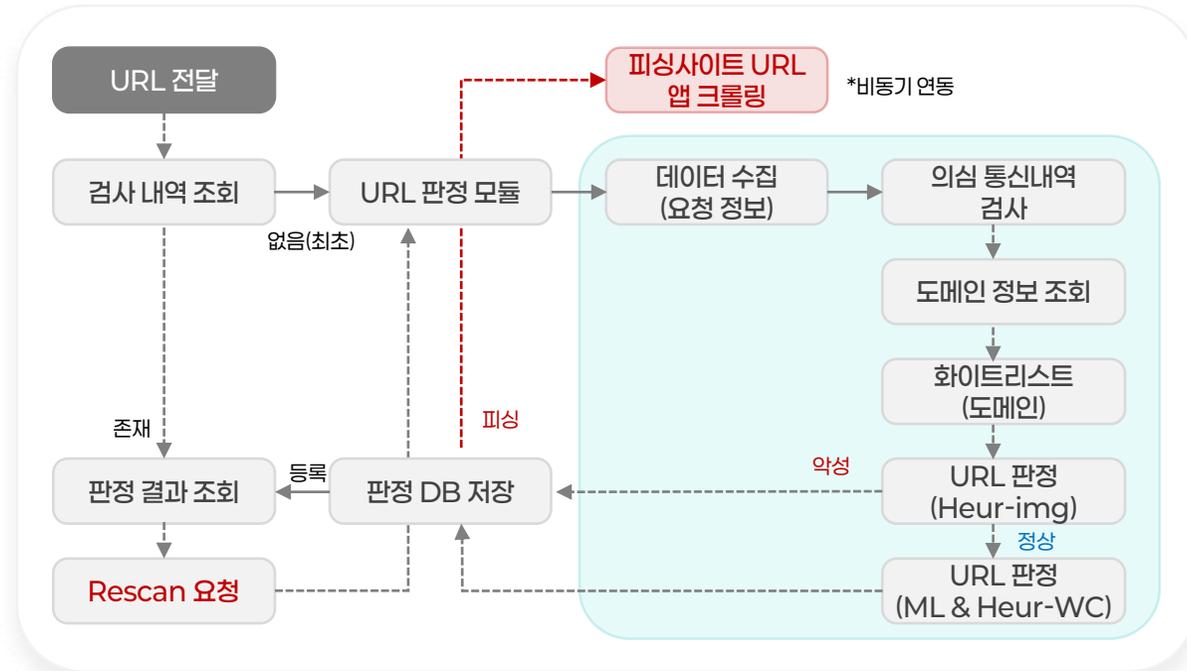
[피싱 사이트 자동 판별 및 악성 앱 수집 시스템 병렬 구성]



[유포 URL 외 악성 앱과 연계된 서버 내역 제공]

2. 제품소개 (3) 핵심 기술

URL에 연결된 유해 사이트 판정, 스크린샷·HTML 대상 ML 및 휴리스틱 기술 활용



[피싱 사이트 자동 판별 및 악성 앱 수집 시스템 직렬 구성(상세)]

기준	설명
정상	정상 사이트
도박	토토, 바카라 등을 포함한 불법 도박 사이트
성인	성인물 약물 판매 등을 포함한 성인사이트
로또	로또 관련 사기 사이트
투자	부동산/주식과 관련된 투자 사기 사이트
피싱	유형별(부고장, 정부24, 건강보험, 청약장 등) 피싱 사이트

[유해 사이트 및 피싱 사이트 URL 판정 기준]

3. 기대효과

고도화된 모바일·IoT 위협 대응 시스템 구축

침해 사고 발생 전 대응부터 발생 후 탐지, 분석까지 All-Time 위협관리



- Agent 설치 후 OS 취약점 공격 실시간 대응
- 사내 부서별 실시간 이용 통계 확인 및 전반적인 기기 운용 상태 파악 가능
- 검사 항목 별 점검 결과 보고서 제공
- 기기별 보안 등급, 침해 위협 요약 정보 제공, 보안 대응 업무 효율성 증가
- 실시간 기기 상태 확인 후 해킹된 기기는 OnTrust Doctor로 복구 가능(옵션)

4. 적용 분야

모바일·IoT 기기가 활용되는 다양한 산업 현장에 적용

기업 및 기관 원격근무 환경 보안

업무용 엔드포인트 보안 및 임직원 스마트폰, 태블릿 등 외부기기를 통한 업무 환경 접속 시 제로트러스트 환경 구현



교육 및 의료, 기타 특수 단말 활용 분야

원격 학습을 위한 교육용 태블릿, 의료용 IoT 기기, 재난안전통신망 단말 (무전기) 등 특수 목적으로 관리되는 단말 보안 관제 시스템 구축



아파트 월패드 해킹 검사, 보안 관제

월패드 해킹 여부 검사 및 아파트 단지별 월패드 디바이스 보안 관제 가능한 솔루션 제공

앱 비즈니스 이용자 보호

결제 등 금융 기능 포함 앱 서비스 운영 시, 이용자 기기 검사 및 보호로 안전한 서비스 이용 보장



보안구역 기밀 유출 방지

사육, 연구소, 대외비자료보관실, 군부대, VIP 전용출입 구역등에해킹된기기반입통제/보안구역출입통제 장치 (태블릿, 키오스크등)에대한보안



VIP 스마트폰 해킹 검사

기업 민감 정보를 다루는 C레벨 임원 및 연구 인력, 국가 지도자 등의 스마트폰에 대한 해킹 검사 및 복구 시스템 구축

스마트시티, 팩토리 IoT 보안

다양한제조사, 다양한사양의IoT 단말이복합적으로 사용된스마트시티및 스마트팩토리보안관제기능 (안드로이드OS기기에 한함)

백도어·공급망 공격 이슈 대응

에이전트리스 방식의 기기 무결성 검사 서비스를 통해 단말 안전성 확인 후 현장 투입 가능



5. 인증 및 수상

국내외 인증 및 수상으로 기술력 검증



OnTrust Agent V2.0GS 인증 1등급



OnTrust 2025
신SW상품대상 수상(2월 상)



OnTrust 2024
우수 정보보호 기술(제품) 지정



OnTrust 2024
중소기업기술마켓 인증



OnTrust 2023 하반기
정보보호제품 혁신대상 수상



OnTrust, OnAV for Gooroom
한국지능정보사회진흥원 인증

AI 시스템 CVS 글로벌 인증(OnAV)



독일



오스트리아



영국



중국



중국

시큐리온 ISO9001 품질경영시스템인증



6. 특허

핵심기술 국내 IP 확보



리눅스 커널 무결성 검사 및 데이터 복구



현대 단말에서의 악성코드 진단 및 제거



취약점 탐지 아키텍처로 구성된 메모리 관리 기술



취약점 보안을 위한 바이너리 패치 장치



머신러닝 이용 이상거래 탐지 장치 및 그 방법



유사도 기반 악성 어플리케이션 탐지 방법 및 장치



위험도 기반 악성 어플리케이션 탐지 방법 및 장치



악성 어플리케이션 탐지 방법 및 그 장치

7. 레퍼런스

국가재난안전통신망 재난대응 8대 분야 특수단말 보안

- 1 무전기·태블릿·지령장치 보안
- 2 폐쇄망 지원
- 3 중앙관제 시스템 제공



7. 레퍼런스

공공 보안

- 1 주요 시설 폐쇄망
- 2 스마트시티
- 3 스미싱 대응



민간 보안

- 1 엔드포인트 보안
- 2 앱 서비스 보안
- 3 이용자 단말 보안
- 4 악성 앱 자동분석시스템 구축



Thank you

문의 pr@securion.co.kr