개방형 OS 보안 솔루션

OnTrust for Gooroom
제품소개서

pr@securion.co.kr

2024.07

1. 회사소개

AI based Cyber Security

Mobile·IoT·5G SECaaS Provider

머신러닝 기반 안티바이러스

OnAV

모바일·IoT 종합 보안 솔루션

OnTrust

악성 앱 자동분석 솔루션

OnAppScan

*지원플랫폼: Android, Linux, Gooroom

㈜시큐리온

대표자	유동훈
주력사업	AI기반 사이버 보안기업
주소	서울시 송파구 송파대로 201 송파테라타워2 A동 G129-2 OS-33호
설립일	2019.05.15
전화	02-575-3339
홈페이지	http://www.securion.co.kr/

주요연혁

2024	OnTrust 2024 우수 정보보호기술(제품) 지정
2023	**보이스피싱 악성앱 탐지 특화 OnAppScan V2.0 출시** 시큐리온 ISO9001 품질경영시스템 인증 OnTrust 2023 하반기 정보보호제품 혁신대상 수상
2021	**IoT·모바일 종합보안 솔루션 OnTrust 출시** 유동훈 대표 국가 교육정보화사업 유공 교육부장관 표창
2019	**시큐리온 법인 설립, OnAV/OnAppScan 출시**

2. 제안배경 (1) 개방형 OS 도입 배경

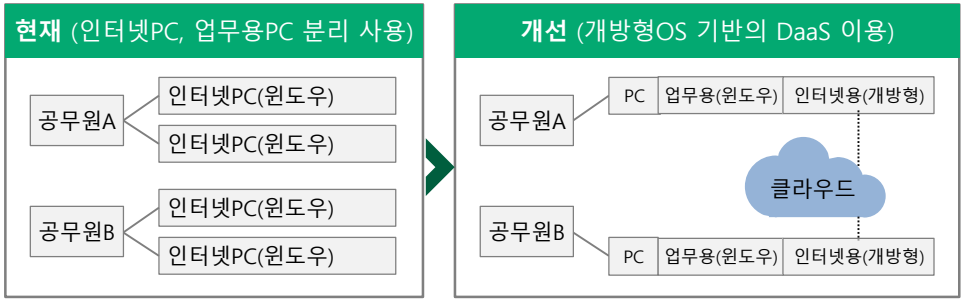
정부 주도 국내 OS 개발

특정 OS에 종속되지 않는 개방형 IT환경 구축

추진현황

시기	내용
2014	개방형OS '하모니카' 개발(NIPA지원)
2015	개방형OS '구름플랫폼' 개발 (국가보안기술연구소, 한컴/티맥스)
2020	행정안전부 개방형 OS도입계획 발표
2020~	개방형 OS 공공부문 시범도입 ~2026년까지 단계적 확대
2021~	개방형 OS 민간 시범도입 지원사업
2022~	행정안전부 '온북' 시범사업 ~2025년까지 공공기관 노트북 전면 교체

1인 2PC ▶ 1인 1PC



- 연간 약 700억 비용 절감
- 특정 업체 기술지원 정책에 따른 업무부담 해소

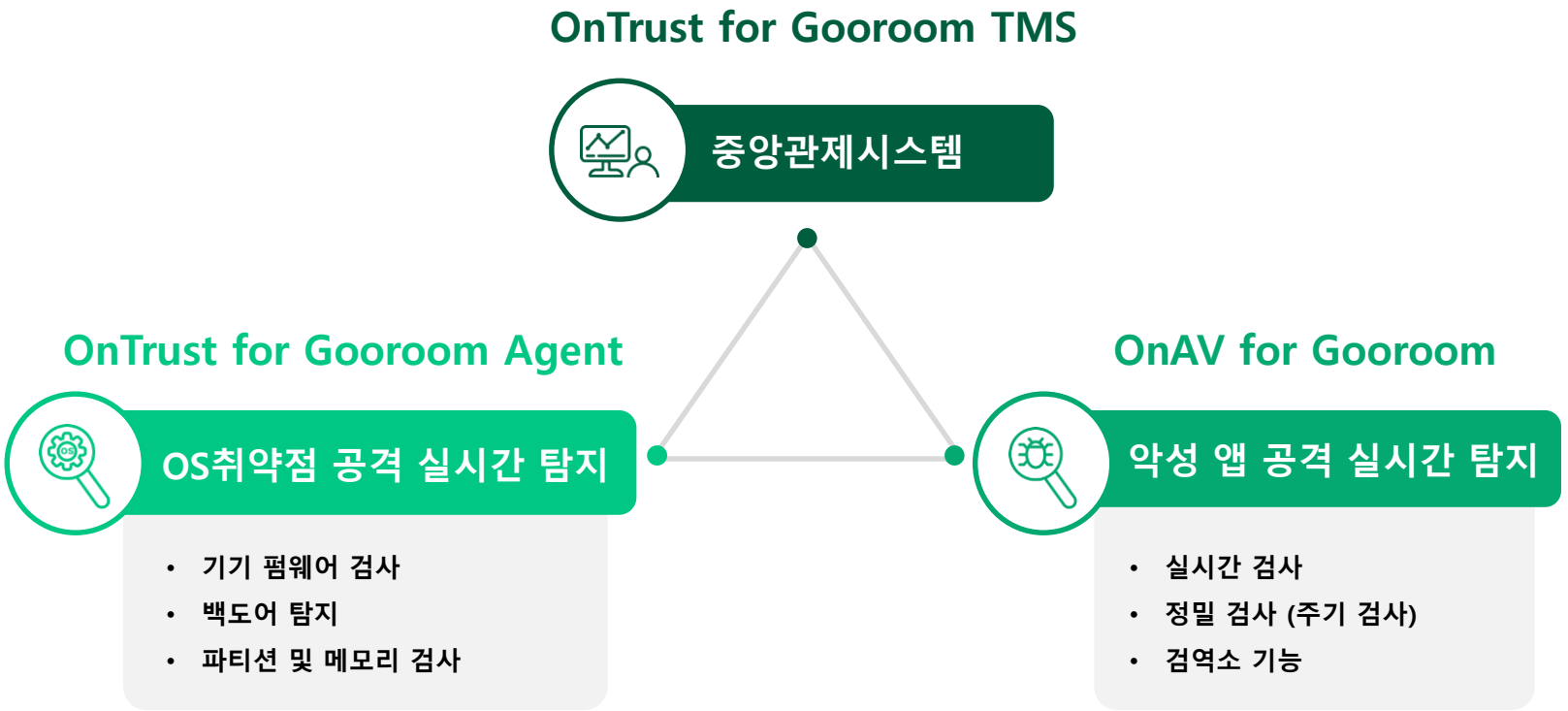
오픈소스 특성 반영된 종합보호 솔루션 필요

Risk	OnTrust for Gooroom
오픈소스 보안 취약성 다양한 OS 취약점 공격 가능성	**OS 이중 보호** 구름OS 자체보안 기능 안정성 이중 검증
각종 APP 보안성 검증 부족 개방형 OS 전용 APP 등의 보안도 초기 단계	**실시간 감시** APP과 OS영역 동시 보호
일원화된 보안대응 미흡 특정 OS사 벗어난 자체 보안 대책 필요	**위협 가시성 확보** 위협관리 및 원격관제 기능 제공

개방형 OS 탑재 데스크톱 PC 및 노트북 보안 솔루션
구름 OS 보안기능에 대한 이중검증으로 완벽한 보호 제공

Goorooom OS 보안기능		OnTrust for Goorooom 보안기능
신뢰 부팅	+	구름OS 보안상태 검사
실행파일 검증		권한 상승 및 제로데이 취약점공격 대응
OS보호		OS보호시스템 무력화 시도 탐지 대응

APP/OS 공격 실시간 탐지 및 관제 솔루션 제공



※ OnTrust for Gooroom X-ray(신속검사 서비스),OnTrust for Gooroom Dr(해킹 단말 복구 서비스) 출시 예정

압축파일 및 난독화 파일 검사 가능

트로이 목마, 웜, 루트킷, 악성 코드, 바이러스 대응

• 최소 4시간 마다 패턴 업데이트

• 1일 업데이트 DB개수 약 2만개

» 두 가지 타입의 시그니처 패턴을 포함해 순차적 검사 진행

Step1	Step2
전체 파일과 세그먼트를 md5로 해싱 (md5 타입이 전체 패턴의 92.32%)	정규 표현식과 동일한 바이트 패턴 시그니처

지원파일 시스템 및 포멧 종류

- 대부분의 압축 파일 포맷 지원
  - ZIP, ARJ, SFX, RAR, 7ZIP, CPIO, IMG, DMG, ISO 9660, Tar, GZIP, BZIP2, OLE2, Cabinet, CHM, BinHex, PKG, SIS, XAR, XZ, EGG 등
- 대부분의 파일 시스템 지원
  - HFS+, HFSX, APM, GPT, MBR 등
- 실행 압축 및 난독화 된 파일 지원
  - AsPack, UPX, FSG, Petite, NsPack, wwpack32, MEW, Upack, SUE, y0da cryptor 등
- 문서 파일 포맷 지원
  - MS 오피스, Mac 오피스, HTML, SWF, RTF, PDF, HWP 등
- 그 밖에 대부분의 메일 파일 포맷 지원

특허 기반 '공격흔적 탐지기술'

침해사고 발생 전후 All time 위협관리

공격 흔적 탐지 프로세스

공격	조사	침해사실확인	검증 결과 보고
• 기기 잠금 해제 • OS보호 무력화 • 펌웨어변조 • 원격침입 • 권한상승 • 백도어설치 • 악성앱설치 • 정보유출	• 기기펌웨어 • 파티션상태 • 파일 시스템과 파일 • 프로세스 트리 • 메모리 상태 • 환경 변수 • 프로퍼티 변수 • 각종 보호 모듈	• 시스템 취약점 • 취약점 공격 도구 • 권한상승 공격코드 • 각종 익스플로잇 코드 • 암호화 된 페이로드 • 추가 공격 도구 • 위협적인 앱 • 백도어	

3. OnTrust for Gooroom 소개 (4) 특장점

1분 안에 전체 시스템 스캔 가능

WIZCASE 멀웨어 탐지율 TEST 90% 기록

The 5 Best Antivirus for Linux in 2023 *wizcase test (2023.04.01)

Quick Guide: 5 Best Antivirus Software for Linux

1. **Bitdefender** — **Top-tier Linux antivirus** for home and enterprise users.
2. **McAfee** — Support for a wide range of distros, but more suited for businesses.
3. **Sophos** — Lightweight Linux antivirus with real-time and on-demand scanning, but no desktop GUI.
4. **ClamAV** — Free and open-source antivirus for Linux with multi-threaded scanner daemon, but only works with CLI.
5. **Dr.Web Security** — Protects emails on Linux systems from spam, but doesn't work well on all distros.

ClamAV took less than a minute to scan my whole system

```
File  Edit  View  Search  Terminal  Help
ubuntu@ubuntu:~$ clamscan --infected --remove --recursive /home/ubuntu/Desktop/

----------- SCAN SUMMARY -----------
Known viruses: 2226383
Engine version: 0.102.2
Scanned directories: 14
Scanned files: 62
Infected files: 0
Data scanned: 9.72 MB
Data read: 4.66 MB (ratio 2.09:1)
Time: 11.842 sec (0 m 11 s)
ubuntu@ubuntu:~$ _
```

개방형 OS 환경 하에서 APP 및 OS 포괄적 보호 제공

기능	시큐리온 OnTrust	A/V 단독	제조사 보호
OS 해킹탐지	✓	✗	△
악성 앱 탐지	✓	✓	✗

✗ 불가 △ 일부 가능 ✓ 가능

3. OnTrust for Gooroom 소개 (5) 인증 및 특허

OnAV for Gooroom V1.0 엔진, GS인증 획득

소프트웨어 품질인증서
Certificate of Software Quality

상호 또는 성명 Name of Company / Name of Applicant	:	(주)시큐리온
소프트웨어의 명칭 Name of Software	:	OnAV for Gooroom V1.0
인증등급 Certification Level	:	1등급
인증번호 Certification No.	:	22-0019A
제조자 및 제조국가 Manufacturer and Country of Manufacture	:	(주)시큐리온(대한민국)
인증연월일 Date of Certification	:	2023년(Year) 02월(Month) 01일(Day)
기타 Additional Information	:	

위 소프트웨어는 「소프트웨어 진흥법」 제20조제3항,
같은 법 시행규칙 제6조제1항에 따라 인증되었음을 증명합니다.

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.

2023년(Year) 02월(Month) 10일(Day)

KTR 한국화학융합시험연구원장
KOREA TESTING & RESEARCH INSTITUTE

President of the Software Quality Certification Body
Republic of Korea

위변조 확인용 QR code

BEYOND ASIAN HUB, TOWARD GLOBAL WORLD

TEST REPORT

성적서 번호 : CGS-2023-000001

신청자 ㅇ 회 사 명 : (주)시큐리온
ㅇ 주 소 : 서울특별시 송파구 송파대로 201, 에이동 지129-2 OS-33호(문정동, 송파테라타워2)
ㅇ 대표자명 : 유동훈, 이성권

시험성적서의 용도 : 소프트웨어 품질인증용

제품명 : OnAV for Gooroom V1.0

시험기간 : 2023년 01월 05일 ~ 2023년 01월 11일

시험방법 : 과학기술정보통신부고시 제2021-101호

시험결과 : 시험결과 참조

비 고 : 1. 이 성적서는 의뢰자가 제시한 시료 및 시료명으로 시험한 결과로써 전체 제품에 대한 품질을 보증하지 않으며,
성적서의 진위확인은 홈페이지(www.ktr.or.kr) 또는 QR code로 확인 가능합니다.
2. 이 성적서는 홍보, 선전, 광고 및 소송용 등으로 사용될 수 없으며, 용도 이외의 사용을 금합니다.
3. 이 성적서는 원본(재발행 포함)만 유효하며, 사본 및 전자 인쇄본/파일본은 결과서 참고용입니다.

작성자 : 윤정훈
Tel : 02-2092-3883

기술책임자 : 박호준
Tel : 1577-0091

2023 년 01 월 31 일

KTR 한국화학융합시험연구원장
KOREA TESTING & RESEARCH INSTITUTE

위변조 확인용 QR 코드

KTR-QI-Y10053-F27(00)

A4(210 X 297)

검증된 리눅스 OS 커널 보호 기술


특허증
CERTIFICATE OF PATENT
특 허 제 10-1064164 호
제 10-2011-0018467 호
2011년 03월 02일
2011년 09월 05일
위의 발명은 「특허법」에 따라 특허등록원부에 등록되었음을 증명합니다.
This is to certify that, in accordance with the Patent Act, a patent for the invention has been registered at the Korean Intellectual Property Office.
2021년 02월 26일
특허청장
COMMISSIONER,
KOREAN INTELLECTUAL PROPERTY OFFICE
김 용 래
특허청
Korean Intellectual Property Office


특허증
CERTIFICATE OF PATENT
특 허 제 10-2324950 호
제 10-2019-0031547 호
2019년 03월 20일
2021년 11월 05일
위의 발명은 「특허법」에 따라 특허원부에 등록되었음을 증명합니다.
This is to certify that, in accordance with the Patent Act, a patent for the invention has been registered at the Korean Intellectual Property Office.
2022년 04월 26일
특허청장
COMMISSIONER,
KOREAN INTELLECTUAL PROPERTY OFFICE
김 용 래
특허청
Korean Intellectual Property Office


특허증
CERTIFICATE OF PATENT
특 허 제 10-2070010 호
제 10-2019-0023742 호
2019년 02월 28일
2020년 01월 20일
위의 발명은 「특허법」에 따라 특허원부에 등록되었음을 증명합니다.
This is to certify that, in accordance with the Patent Act, a patent for the invention has been registered at the Korean Intellectual Property Office.
2022년 04월 29일
특허청장
COMMISSIONER,
KOREAN INTELLECTUAL PROPERTY OFFICE
김 용 래
특허청
Korean Intellectual Property Office

01

리눅스 커널 무결성 검사 및 데이터 복구

02

취약점 탐지 아키텍처로 구성된 메모리 관리 기술

03

취약점 보완을 위한 바이너리 패치 장치

다양한 개방형 OS 적용 가능

권장사양(H/W)	
CPU	Intel Dual Core 500 GhZ 이상
RAM	512MB 이상
HDD	800MB 이상
NIC	10/100/1000MB Ethernet

운영환경	
지원 운영체제	-Debian 계열 Linux (Ubuntu 등) -HarmoniKR -Hancom Gooroom -TmaxOS -그 밖의 Gooroom OS 계열
웹기반 GUI 사양	- Gooroom Browser 90.0.4430.212 - 화면 해상도: 최소 1024 x 768 픽셀, 권장 1280 x 1024 픽셀

4. 인증 및 수상

시큐리온 AI탐지 시스템(OnAV) 글로벌 Top 3 인증·OnAV for Gooroom GS 인증 획득

독일 | 오스트리아 | 영국 | 대한민국 | 중국 | 중국

OnTrust 2023 하반기
정보보호제품 혁신대상 수상

OnTrust, OnAV for Gooroom
한국지능정보사회진흥원 인증

OnTrust 2024
우수 정보보호 기술(제품) 지정

시큐리온 ISO9001
품질경영시스템 인증

5. 레퍼런스


SK telecom
SK networks
SK encar.com
SK C&C
SK infosec
SK 주식회사
SK shieldus
SAMSUNG 삼성SDS
SAMSUNG 삼성전자
NSOK
F&U
오리온
cen 시큐센 secucen
cen 아이티센 ITCEN
미래창조과학부
보건복지부
5678 행복미소 서울도시철도
Seoul Metro 서울메트로
김포 GOLDLINE
세종특별자치시
kt
KAI
한국가스공사
한국전력
KOREA GOLD EXCHANGE 한국금거래소
KUMC 고려대학교의료원 KOREA UNIVERSITY MEDICAL CENTER
ALPACO
OPSWAT.
cross
ONE 1 STORE
LG유플러스
KISA 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY
국방전산정보원
GMD SOFT GLOBAL MOBILE & DIGITAL SOFTWARE
STraffic
(주)가보테크 GABOTECH Co.,Ltd
(주) 한스웰
AM Telecom
BLUEBIRD
CYBERTEL bridge
Incheon Airport 인천공항시설관리
용인시 YONGIN CITY
KOREG 신용보증재단중앙회
동양지축은행
Hyundai J·Comm

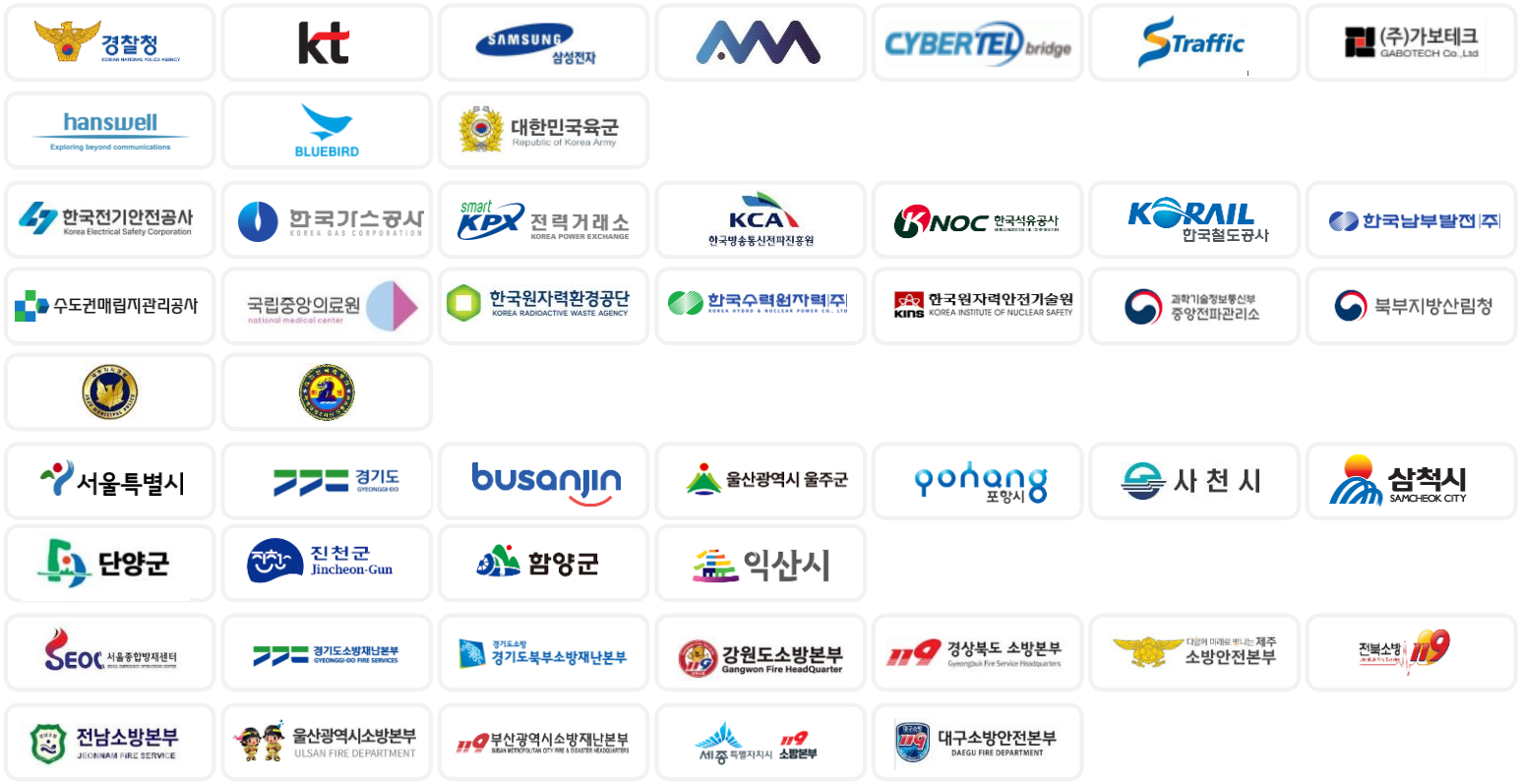
7. 레퍼런스

hanswell
Exploring beyond communications

한스웰 리눅스 앱 보호 특화 보안 솔루션

- 국가재난안전통신망 납품용 특수단말(지령업무 특화 탁상형 단말기) OnAV for Gooroom 도입
- 폐쇄망 환경에서도 정기적인 백신 업데이트로 강력한 보안
- GS인증 1등급, NIA인증 획득

국가재난안전통신망



7. 레퍼런스

공공


대한민국육군
Republic of Korea Army
대한민국공군
REPUBLIC OF KOREA AIR FORCE
국방전산정보원
경찰청
미래창조과학부
보건복지부
세종특별자치시
용인시
강릉시
한국인터넷진흥원
한국교통안전공단
KITECH
한국생산기술연구원
Incheon Airport
서울도시철도
김포 GOLDLINE
Seoul Metro
서울메트로
한국항공우주산업㈜
한국전력
한국가스공사

민간


SK telecom
SK networks
SK C&C
SAMSUNG 삼성전자
SAMSUNG 삼성SDS
LG U+
아이티센그룹
ONE STORE
SK F&U
cross
monee
한국금거래소
KOREG
신용보증재단중앙회
경기신용보증재단
동양지축은행
moin
SK shieldus
SK 주식회사
SK encar.com
시큐센
오리온
GMOSOFT
OPSWAT.
KOOLSPAN
고려대학교의료원
ALPACO

감사합니다

서울시 송파구 송파대로 201 송파테라타워2 A동 G129-2 OS-33호
T : 02-575-3339 F : 02-575-3340 W : www.securion.co.kr