SECURI ON

리눅스 OS 안티바이러스
OnAV for Linux Desktop

리눅스(구름 포함) OS 전용 악성 애플리케이션 탐지 솔루션

2025.01

Contents

SECURI ON

AI based Cyber Security Company

OnAV for Linux Desktop

리눅스 OS 안티바이러스
OnAV for Linux Desktop

OnAV

모바일·IoT 안티바이러스
OnAV

OnTrust

모바일·IoT 안티 해킹 솔루션
OnTrust

OnAppScan

AI 악성 앱 자동분석 시스템
OnAppScan

리눅스 OS 대상 악성 위협 증가 (하모니카, 구름 등 개방형 OS 포함)

랜섬웨어·트로이목마 및 신·변종 악성코드 등

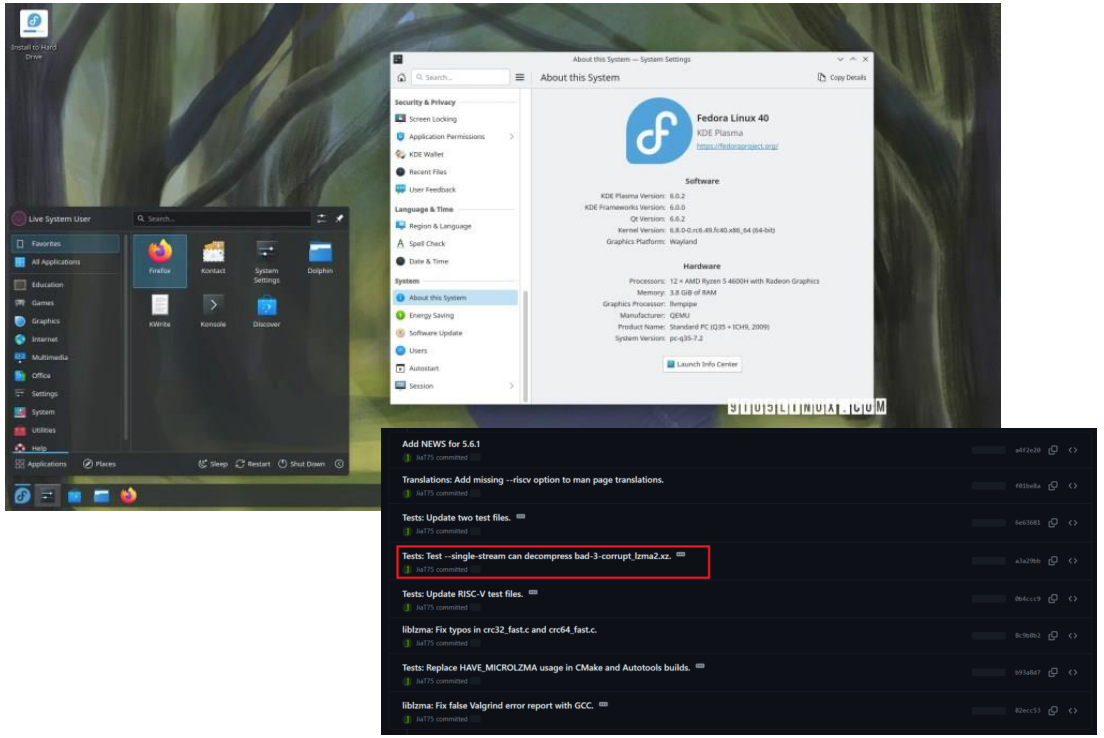
2024 발견 주요 위협 사례

리눅스 시스템 공격 악성코드 '디스고모지(DISGOMOJI)'
- 파키스탄 공격자 그룹의 인도 정부기관 대상 사이버 첩보활동
- 악성행위 실행파일을 ZIP 형태로 포함한 피싱 이메일 배포
- 악성파일 실행시 인도 국방 서비스 장교 퇴직금 관련 PDF를 미끼로 표시하며 백그라운드에서 추가 페이로드 배포

리눅스 서버 공격 악성코드 'perfctl'
- 암호화폐 채굴 목적 크립토마이닝 멀웨어
- 최근 몇 년간 수천대 리눅스 서버 감염 가능성(최소 3년 이상 활동)

리눅스 기본 유틸리티(xz Utils) 백도어 발견
- 데이터 압축 유틸리티 XZ Utils 최신버전(5.60, 5.61) 전체 다운로드 패키지에 무단 액세스 허용 악성코드 포함
- 공격자는 2021년부터 오픈소스 프로젝트에 참여해 운영자와 신뢰를 쌓으며 의도적으로 악성코드를 삽입해 배포

XZ Utils 악성코드가 포함되어 배포된 Fedora linux 40 beta



악성코드가 포함된 XZ Utils 배포 페이지

리눅스 기반 '구름' OS, 개방형 IT 환경 구축 목적으로 공공 분야 도입 확산(2020~)

리눅스에 비해 자체 보안 강화됐으나 메일·브라우저 등을 통한 악성코드 침투 위협 여전히 존재

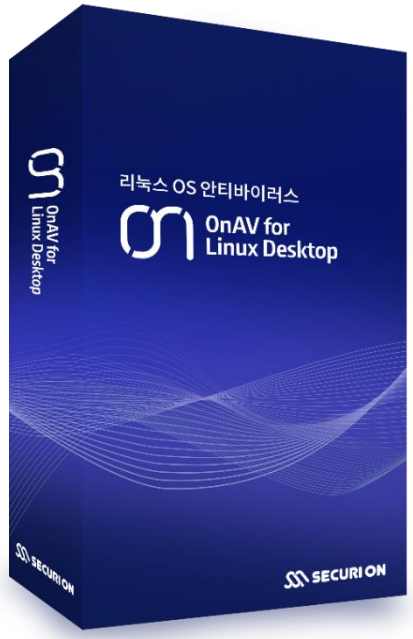
구름 OS 도입 주요 일정

- **2020** 행정안전부, 개방형 OS도입계획 발표
- **2020** 개방형 OS 공공부문 시범도입 ~2026년까지 단계적 확대
- **2021** 개방형 OS 민간 시범도입 지원사업 (2021년 11월~ 2022년 10월)
- **2023** 시범사업 결과 '온북'에 대한 긍정적 평가 확인 ~2027년까지 적용 범위 확대 예정 (공공기관 업무용 PC의 90%이상 교체 방침)

위협	대응
리눅스 OS 악성코드 위협 애플리케이션, 메일 및 브라우저 통한 악성파일	**리눅스 OS 안티바이러스 도입 필요** 악성코드 위협 실시간 탐지
리눅스 OS 해킹 위협 취약점을 이용한 OS 공격	**구름OS 자체 보호 기능 존재** 신뢰부팅/실행파일검증/OS보호
네트워크 위협 1PC 사용으로 인한 업무망 보안 취약성	**논리적 망분리+'구름플랫폼'구축** 업무 망 접속 시 보안서비스영역(VPN, 보안GW 등) '구름플랫폼'을 거치도록 시스템 설계(국가정보자원관리원 내)

OnAV for Linux Desktop, 1분 안에 전체 시스템 스캔 가능한 악성코드 탐지 엔진

방대한 악성코드 DB를 기반으로 실시간 감시 기능 강화



실시간 감시 성능 강화

브라우저를 통해 드라이브 바이 다운로드된 악성코드를 실시간으로 탐지

* 드라이브 바이 다운로드 공격
: 컴퓨터나 모바일 기기에 악성코드를 무심코 다운로드 하게 유도
: 번들웨어를 통한 다운로드 유도, 피싱(피싱사이트, 이메일 등) 수법 이용

빠른 검사 속도

바이트 패턴 기반 휴리스틱 검사 방식으로 검사 속도 개선

1분 안에 전체 시스템 스캔 가능

변종 악성코드 탐지 강화

대부분의 파일 시스템 및 포맷 검사 지원

검사대상 파일 시스템 및 포맷 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**

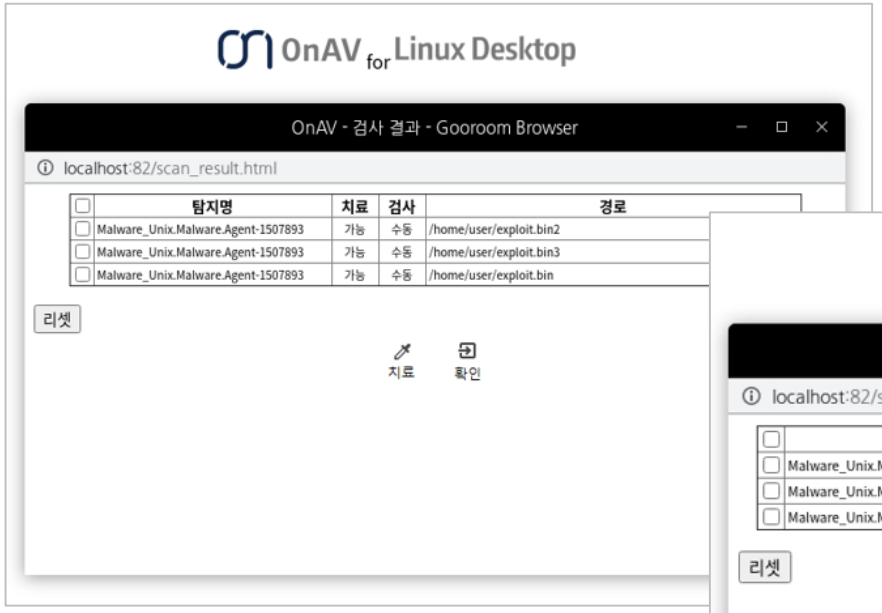
악성코드 검사, 패턴 업데이트 및 검사 결과 제공

● 메인 메뉴

- 악성코드 검사 및 치료 기능

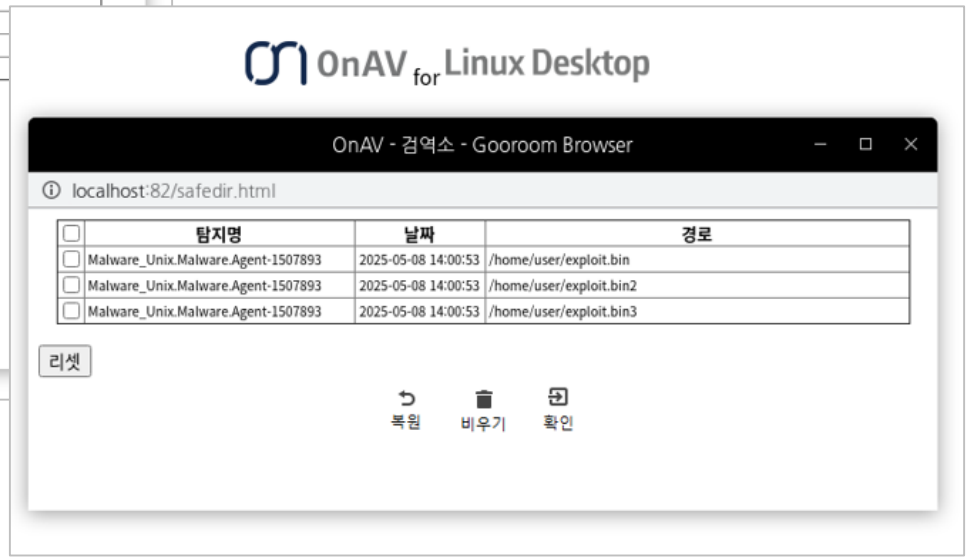
● 검사 결과

- 탐지된 악성코드를 치료
- 검역소 기능 사용 시 검역소로 이동, 사용하지 않을 시 즉시 삭제



● 검역소

- 검역소 내의 악성코드 파일을 복원하거나 삭제 가능



Clam AV , 신뢰도 높은 악성코드 DB를 보유한 바이러스 백신 툴킷

다년간 누적된 메인 DB와 매일 업데이트 되는 데일리DB 제공

Clam AV 데이터 센터,
전 세계에서 발생하는 바이러스에 대한 방대한 자료를
확보하고 이를 주기적으로 업데이트 및 공개

최소 **4시간 마다** 패턴 업데이트

업데이트 DB개수 **1일 약 2만개**

Clam AV, The 5 Best Antivirus for Linux in 2023

* wizcase test (2023.04.01)

리눅스 기반의 다양한 운영체제를 악성코드 위협으로부터 보호

지원 운영체제

Debian 계열 Linux

debian GNU/Linux

Ubuntu

Linux Mint from freedom came elegance

국내 개방형 OS

GOOROOM

Tmax구름

한컴구름

HAMONI KR

-그 외 Linux OS

사양

GUI 사양	
웹기반 GUI 사양	-Gooroom Browser 90.0.4430.212, Firefox Browser 135.0 - 화면 해상도: 최소 1024 x 768 픽셀, 권장 1280 x 1024 픽셀

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

개방형 OS 도입한 공공 부문 PC 및 태블릿, 특수 단말 보호

“제한된 조건에 맞는 커스터마이징”

사례

국가재난안전통신망 지령업무 특화 탁상 단말기
IPv6 네트워크망 사용, 폐쇄망 환경, 개방형 OS 등
제한된 조건에서 운용 가능한 보안 솔루션 필요

시큐리온, 고객사 망 내에 패턴 및 패치관리 시스템(PMS)
구축, IPv6 업데이트 지원 정기 패턴 업데이트 및
검사 기능 제공

hanswell
Exploring beyond communications

환경부
4대강 홍수통제소

OnAV for Linux Desktop V2.1

GS 인증 1등급 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 Linux Desktop V2.1
인증등급 Certification Level	:	1등급
인증번호 Certification No.	:	22-0019B
제조자 및 제조국가 Manufacturer and Country of Manufacture	:	(주)시큐리온(대한민국)
인증연월일 Date of Certification	:	2025년(Year) 04월(Month) 17일(Day)
기타 Additional Information	:	

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

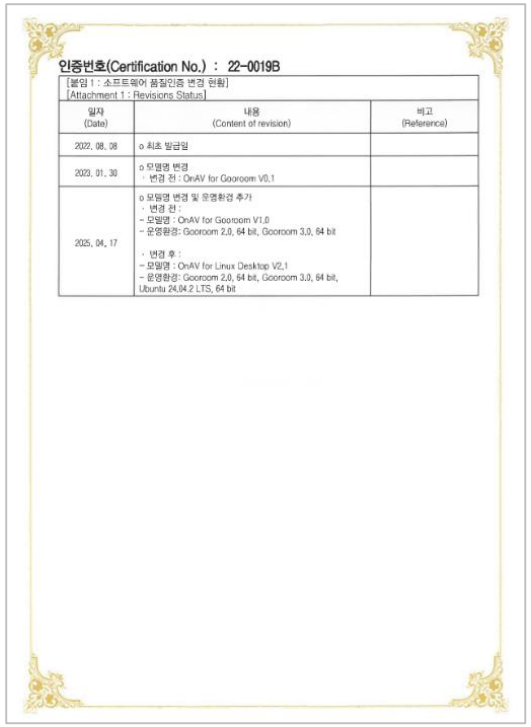
I hereby confirm that the quality of the foregoing software has been certified under Article 20.3 of the Software Promotion Act and Article 6.1 of its Enforcement Decree.

2025년(Year) 04월(Month) 17일(Day)

KTR 한국화학융합시험연구원장
KOREA TESTING & RESEARCH INSTITUTE

President of the Software Quality Certification Body
Republic of Korea

위변조 확인용 QR code



인증번호(Certification No.) : 22-0019B

[붙임 1 : 소프트웨어 품질인증 변경 현황]
[Attachment 1 : Revisions Status]

일자 (Date)	내용 (Content of revision)	비고 (Reference)
2022. 08. 08	o 최초 발급일	
2023. 01. 30	o 모델명 변경 · 변경 전 : OnAV for Gooroom V0.1	
2025. 04. 17	o 모델명 변경 및 운영환경 추가 · 변경 전 : - 모델명 : OnAV for Gooroom V1.0 - 운영환경: Gooroom 2.0, 64 bit, Gooroom 3.0, 64 bit · 변경 후 : - 모델명 : OnAV for Linux Desktop V2.1 - 운영환경: Gooroom 2.0, 64 bit, Gooroom 3.0, 64 bit, Ubuntu 24.04.2 LTS, 64 bit	

시큐리온 품질경영 인증 획득

Certificate of Registration

품질경영시스템 인증서
(주)시큐리온
ISO 9001:2015

Certificate of Registration

SECURION Co., Ltd.
ISO 9001:2015

품질경영시스템 ISO 9001 국제표준

- 2023년 06월 인증 획득
- 국제표준화기구(ISO)에서 제정, 시행하는 품질경영시스템에 관한 국제 규격
- 제품 및 서비스를 생산, 공급하는 과정에 대한 품질 보증 체계

대표 사례

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

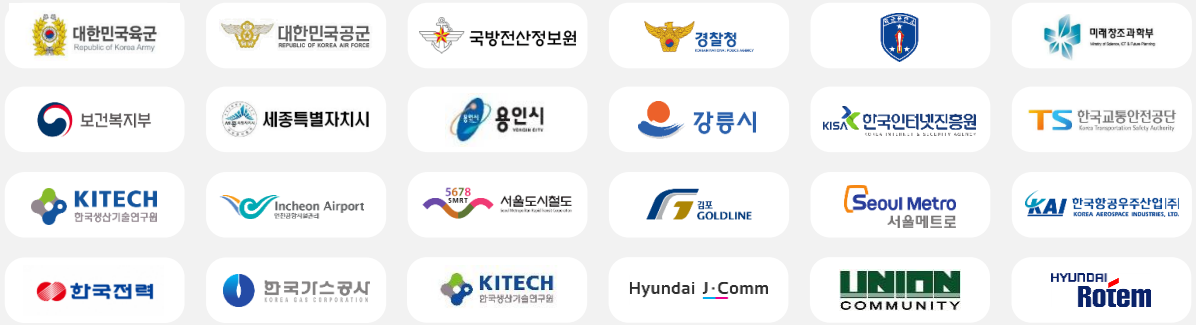
국가재난안전통신망 재난대응 8대 분야 특수단말 보안

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

5. 레퍼런스

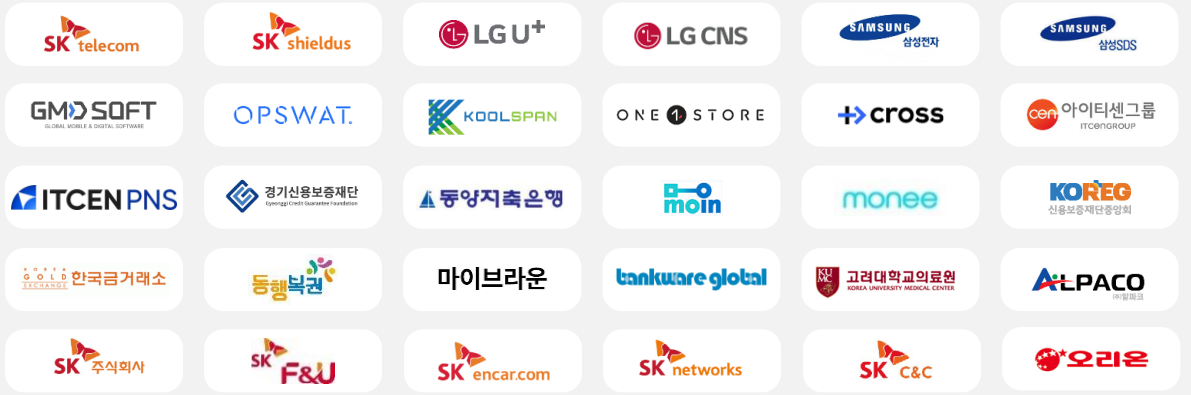
공공 보안

1. 주요 시설 폐쇄망
2. 스마트시티
3. 스미싱 대응



민간 보안

1. 엔드포인트보안
2. 앱 서비스 보안
3. 이용자 단말 보안



Thank you

문의 pr@securion.co.kr

SECURI ON

A : 서울시 송파구 송파대로 201 송파테라타워2 A동 G129-2 OS-33호 | T : 02-575-3339 | W : https://www.securion.co.kr