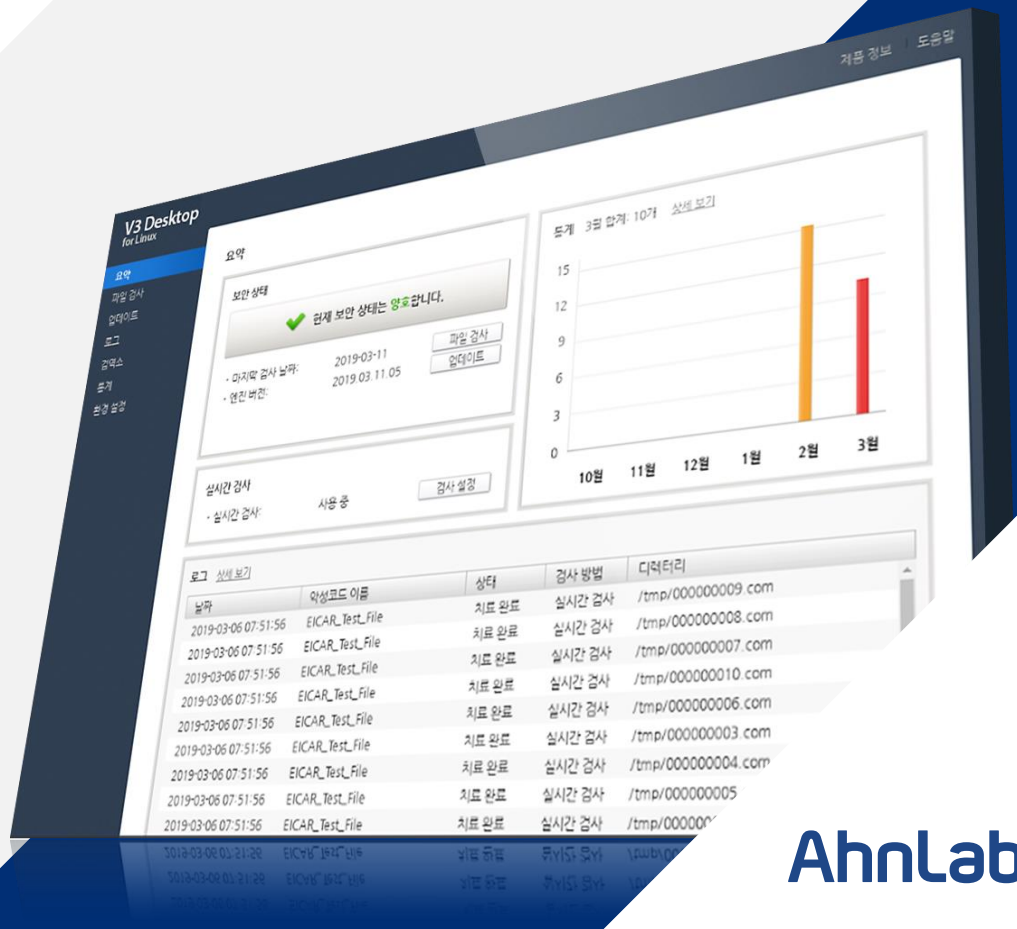
AhnLab

V3 Desktop for Linux

More security,
More freedom

개방형OS 기반의 업무용PC 보호

표준제안서



AhnLab

CONTENTS

AhnLab

1. 배경 – 개방형OS 도입에 따른 보안 필요성 대두

현재 공공기관에서 인터넷망 PC를 윈도우(Windows) OS가 아닌 리눅스(Linux) 기반의 개방형OS 도입을 적극 검토하면서 개방형OS 환경에 대한 보안 대책이 요구되고 있습니다.

디지털데일리 — 2019. 10. 23

Windows 7 기술지원 종료…
개방형 OS 도입 초읽기 나선 정부

IT Chosun — 2019. 07. 26

한글과컴퓨터, 개방형OS '구름 플랫폼' 생태계 키우기 나선다

ZDNet Korea — 2019. 07. 24

공공 PC시장 열렸다…
하모니카.구름OS.티맥스 각축

보안뉴스 — 2019. 05. 15

개방형OS 도입 추진,
정부 PC 환경에 새로운 변화 예고

2. V3 Desktop for Linux

V3 Desktop for Linux는 리눅스(Linux) 기반의 개방형OS 환경에 최적화된 보안 솔루션으로,
개방형OS 기반의 업무용 PC에 대한 악성코드 방역을 통해 안전한 비즈니스 환경 구현에 기여합니다.

개방형OS 환경을 완벽하게 지원하는 PC보안 솔루션

AhnLab V3 Desktop for Linux

정확하고 신속한 PC 보안

- 실시간 검사 기능을 통한 모니터링
- 독보적인 엔진 기반의 신속하고 정확한 악성코드 진단 및 치료
- 다양한 다중 압축 파일 검사 및 치료 가능

업무용 PC 운용 극대화를 위한 다양한 정책 설정

- 효율적인 수동 및 예약 검사 기능
- 지정된 시간에 자동 엔진 업데이트를 할 수 있는 예약 기능

관리자 편의성 극대화를 통한 안정적인 보안 운영

- AhnLab EPP Management 기반의 통합 관리
- 악성코드 검사 및 치료에 대한 다양한 통계 리포트 제공
- 검사 예외 설정 기능을 통해 효율적인 방역 정책 적용 가능

3. 주요 기능

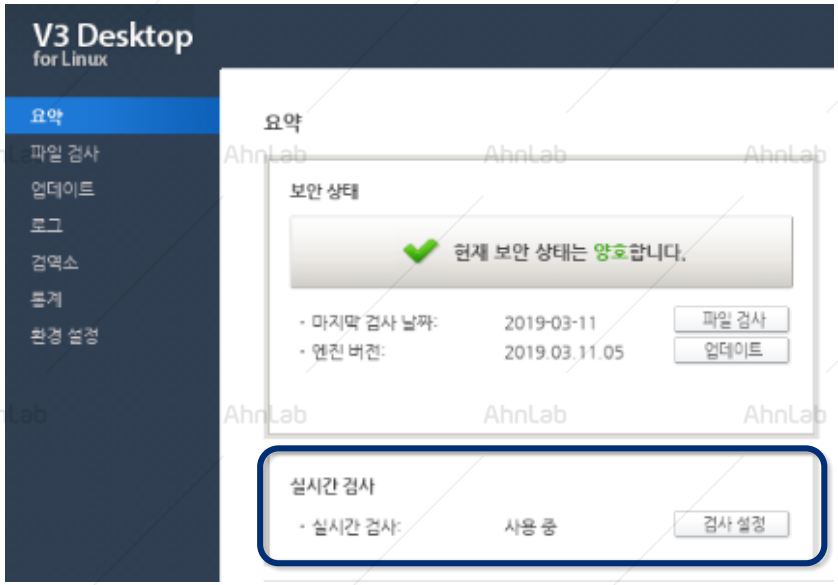
V3 Desktop for Linux는 개방형OS 기반의 업무용 PC 보안에 최적화된 기능을 제공합니다.

구분	주요 기능	상세 내용
악성코드 대응	악성코드 검사	• 실시간 검사: 실시간 검사 사용 On/Off, 실시간 검사 종료 후 자동 재시작 • 수동(정밀) 검사: 검사 대상 설정 가능 • 예약 검사: 예약 검사 목록, 예약검사 추가/수정/삭제 • DNA 스캔(Scan) 지원 • 압축 파일 검사
	엔진 업데이트	• 최신 업데이트 파일 및 패치 파일 존재 여부 확인 • 자동 업데이트: 스마트 업데이트를 이용한 자동 업데이트 및 패치 제공 • 예약 업데이트: 지정 시간에 수행하는 예약 업데이트 - 업데이트 주기 설정 가능 • 업데이트 서버 설정: 인터넷을 통한 업데이트, 사용자 정의 서버를 통한 업데이트, 로컬 디렉터리를 통한 업데이트 • 기타 업데이트 관련 설정: 업데이트 시 제품 패치, 업데이트 정보 보기, 무결성 검사
	환경설정	• 치료 방법 설정 - 악성코드 감염 파일 치료/그대로 두기, 감염 된 압축 파일 치료/그대로 두기 설정 가능 - 자동 치료 - 치료 또는 삭제 전 감염된 파일을 검역소로 보내기 • 검사 대상 설정 - 모든 파일 검사 - 감염되기 쉬운 파일 검사(실행 파일/매크로 파일/스크립트 파일), - 추가 검사 확장자 - 압축 파일 검사
관리자 기능	로그 관리/검역소	• 검사 로그, 이벤트 로그 • 검역소 목록 확인, 검역소 파일 복원
	통계	• 월별, 기간별 악성코드 발견 통계
	중앙관리	• 중앙관리 솔루션 연동을 통한 단일 콘솔 기반의 통합 관리 – V3 Desktop for Linux 외 추가 에이전트 설치 불필요

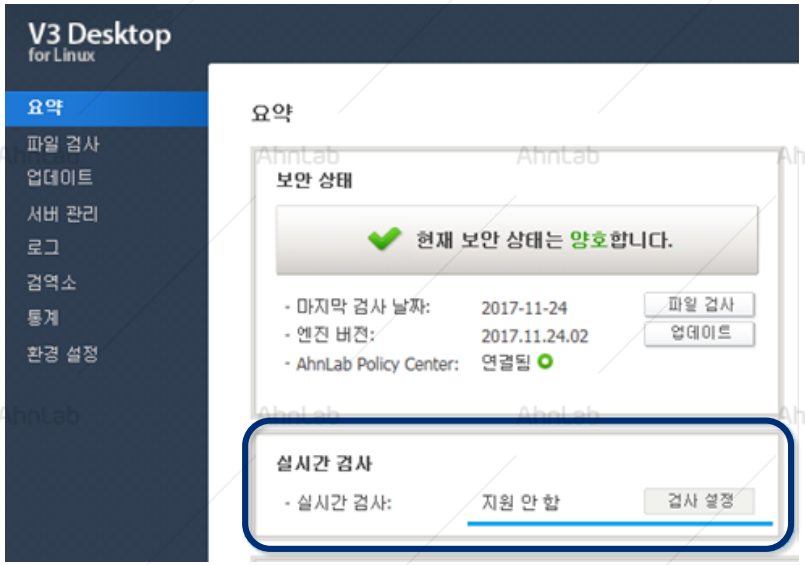
4. 특장점 – (1)실시간 검사 지원 여부 확인

V3 Desktop for Linux 제품을 설치할 때 자동으로 실시간 검사 기능이 사용 가능한 OS 여부와 커널 버전을 확인하며, 관련 정보를 관리자 웹 콘솔에 제공합니다.

실시간 검사 지원 OS인 경우



실시간 검사 미지원 OS인 경우



4. 특장점 – (2)통합 관리 및 위협 대응

V3 Desktop for Linux는 엔드포인트 보안 플랫폼 AhnLab EPP를 통해 효율적으로 통합 관리할 수 있으며,
연계 정책을 활용해 취약 시스템 점검•조치부터 악성코드 대응, 패치 관리, 개인정보 유출 방지 등 엔드포인트 하드닝이 가능합니다.

- AhnLab EPP 기반의 보안 솔루션 연계를 통한 취약 시스템 조치 및 엔드포인트 하드닝 (Endpoint Hardening) 효과

5. 사용 환경

V3 Desktop for Linux는 Linux 기반의 다양한 개방형OS 환경을 지원합니다.

운영체제

Gooroom(구름)

TmaxOS(티맥스오에스)

HamoniKR(하모니카)

메모리

512MB 이상

HDD

500MB 이상의 여유 공간

* 상기 개방형OS 이외 운영체제는 지원하지 않습니다.
* 상기 OS의 64 bit 운영체제를 지원하며, x86은 지원하지 않습니다.

별첨

1. 입체적인 대응 서비스
2. 전문 고객 지원 프로세스

입체적인 대응 서비스

※ 별첨

- 안랩의 차별화된 전문 지원 서비스
- 24시간, 365일 깨어 있는 ASEC 대응센터

AhnLab

20여 년간 축적된 악성코드 분석 능력과 대응 경험을 통해
안전한 컴퓨팅 환경 조성과 함께 기업 비즈니스 연속성에 기여합니다.

안랩은 30년간 악성코드를 분석하고 연구해온 전문 기업입니다.

안랩은 지난 1988년부터 악성코드와 바이러스 등에 대한 연구를 시작, 25년여 간 노하우를 축적해왔습니다.
국내 최대 규모의 샘플 DB를 보유하고 있으며 독자적인 기술을 확보하고 있습니다.

안랩은 다양한 분야의 기업 고객에게 위협 대응 방안을 제공하고 있습니다.

1995년 회사가 설립된 이후 다양한 레퍼런스를 통해 경험을 쌓았습니다.
다양한 기업 환경에서 발생하는 위협을 정확하게 진단해내고 있으며 적절한 대응 방안을 제시하고 있습니다.

안랩은 24시간, 365일 철저한 대응 체계를 가동 중입니다.

24시간 × 365일 ASEC 대응센터의 전문 인력이 위협을 모니터링하며 대응하고 있습니다.
일일 정기 업데이트 및 긴급 업데이트를 수행함으로써 발 빠르게 악성코드에 대처합니다.

전문 고객 지원 프로세스

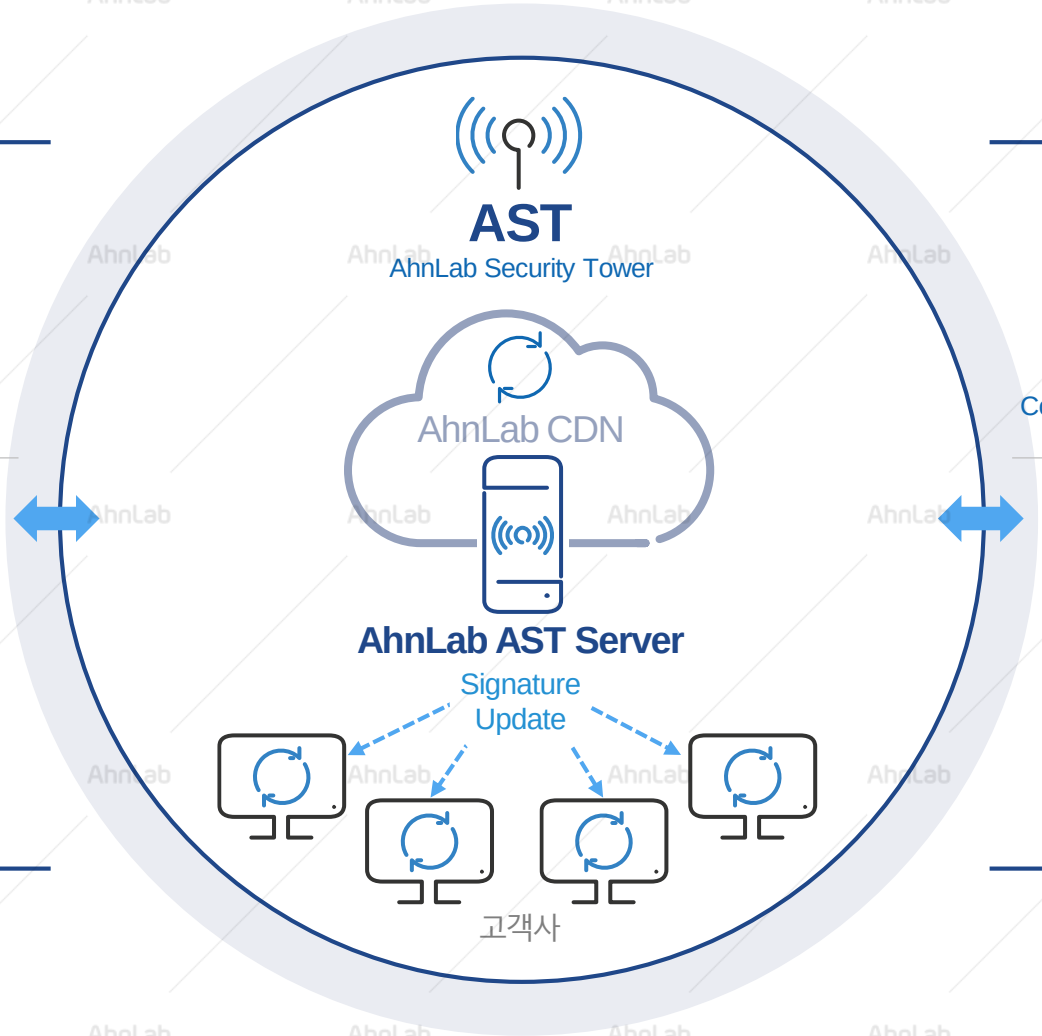
※ 별첨

위협 분석 및 대응에 대한 오랜 노하우와 경험을 토대로 체계적이며 전문적인 지원 서비스 제공을 약속합니다.

ASEC

AhnLab Security E-response Center

- 보안 위협 모니터링
- 악성코드 수집 및 분석
- 피해 접수 및 대응
- V3 엔진 개발
- 네트워크 분석/모니터링
- 사전 대응



CERT

Computer Emergency Response Team

- 관제 고객 대상 실시간 공격/위협정보 수집
- ASEC에 실시간 공격/위협정보 전달

More security,
More freedom

㈜안랩
경기도 성남시 분당구 판교역로 220 (우)13493
대표전화 : 031-722-8000 | 구매문의 : 1588-3096 | 전용 상담전화 : 1577-9431 | 팩스 : 031-722-8901 | www.ahnlab.com

AhnLab
V3 Desktop for Linux

AhnLab