

# AhnLab Xscanner

## 특수목적시스템을 위한 악성코드 진단 및 치료

실시간 검사 및 엔진 업데이트가 어려운 환경을 위한 수동 검사 기반  
악성코드 진단 및 치료 프로그램

### 제품 개요

AhnLab Xscanner는 일반 보안 솔루션 적용이 어려운 특수목적시스템에서 악성코드를 찾아 제거하기 위한 수동 검사 기반 악성코드 진단 및 치료 프로그램입니다. 기존 설치된 보안 에이전트와 충돌을 최소화하며, 운영 상황에 맞게 검사 및 치료 옵션을 설정할 수 있습니다. 시스템에 설치하지 않고 이동식 저장 매체에 탑재해 사용 가능합니다.



ICS



POS 시스템



KIOSK



BIS

- ✓ 폐쇄망 환경 지원
- ✓ 과거 악성코드 대응
- ✓ 구버전 OS, 업데이트 중단 OS 지원
- ✓ 비설치형
- ✓ 이동식 저장매체 탑재 사용

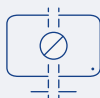
### 특수목적시스템 보안 조치

특수목적시스템은 안정적 운용에 대한 요구가 높고 정해진 프로그램만 사용해야 합니다. 또, 폐쇄망 환경 내 시스템은 악성코드 엔진 최신 업데이트가 어려운 가운데, 보안 이슈를 조치해야 하는 요구사항이 있습니다. AhnLab Xscanner는 이처럼 특수한 보안 요구사항에 맞춰 적절한 보안 조치를 취할 수 있도록 지원합니다.



일반 보안 솔루션 적용이 어려운  
특수목적시스템

- 실시간 진단 기반 즉각적인 치료가 어려운 민감 시스템
- 구버전 OS 혹은 보안 지원이 중단된 OS를 사용하는 시스템
- 기 적용된 보안 솔루션과 충돌이 우려되는 시스템
- 보안 전문가가 아닌 현장 작업자가 보안 조치에 투입되는 환경






최신 엔진 및 대규모 업데이트가 어려운  
폐쇄망 또는 저대역 네트워크 환경

- 보안 프로그램 최신 엔진 업데이트가 불가한 시스템
- 폐쇄망 환경에서 악성코드 감염이 발생한 경우
- 악성코드 삭제, 메모리 검사, 은폐 진단 등 치료 조치가 필요한 경우

## 특장점

AhnLab Xscanner는 편리한 사용성을 바탕으로 보안 전문가 뿐만 아니라 현장 작업자와 설비 담당자도 악성코드 감염 시 쉽게 대응할 수 있도록 지원합니다.

 <b>수동 검사 기반 진단 및 치료</b>	<ul style="list-style-type: none"><li>· 기존 설치된 보안 에이전트 삭제 없이 충돌 최소화</li><li>· 감염된 시스템 사후 치료</li><li>· 보안 에이전트 설치 전 사전 방역을 위한 시스템 전체 검사</li><li>· 검사 시간 단축을 위한 사용자 지정 검사 지원</li></ul>
 <b>편리한 운영을 위한 다양한 설정</b>	<ul style="list-style-type: none"><li>· 운영 상황에 맞게 대응할 수 있는 검사 및 치료 옵션 설정</li><li>· 검사 불필요 항목에 대한 예외 설정(폴더, 파일, 확장자)</li><li>· 커널 드라이버 구동이 불가능한 환경까지 지원하는 기능 제공</li><li>· GUI, CLI, Silent 모드 실행 지원</li><li>* Linux 버전은 CLI, Silent 모드 실행만 지원</li></ul>
 <b>사용 및 관리 편의성 제공</b>	<ul style="list-style-type: none"><li>· 검사 후 선택 치료 제공</li><li>· 필수 프로그램 감염으로 인한 삭제와 오진 대응을 위한 검역소 기능 제공</li><li>· 이벤트 및 진단 로그 기간별 검색어 조회 및 파일 저장 지원</li></ul>

## 주요 기능

AhnLab Xscanner는 효과적인 악성코드 검사와 치료 및 효율적인 운영을 위해 다음과 같은 기능들을 제공합니다.

 <b>악성코드 검사</b>	<ul style="list-style-type: none"><li>· 수동(정밀) 검사: 전체 검사, 사용자 지정 검사(폴더, 파일)</li><li>· 유해 가능 프로그램, 불필요한 프로그램(PUP) 검사</li><li>· 클라우드 진단</li><li>· 압축 파일 검사</li><li>· 검사 결과 조회 및 선택 치료</li><li>· CPU 점유율 설정</li></ul>
 <b>악성코드 치료</b>	<ul style="list-style-type: none"><li>· 치료 방법 설정</li><li>· 자동 치료 설정</li><li>· 치료 불가 파일 삭제 설정</li><li>· 감염된 압축파일 치료/그대로 두기 설정</li><li>· 치료 레벨 설정</li><li>· 검사 예외 설정 (폴더, 파일, 확장자)</li><li>· 검사 옵션</li></ul>
 <b>설정 기능</b>	<p><b>로그 관리</b></p> <ul style="list-style-type: none"><li>· 이벤트 로그, 진단 로그</li><li>· 날짜 별 조회, 검색어 조회</li><li>· 로그 파일 저장</li></ul> <p><b>검역소</b></p> <ul style="list-style-type: none"><li>· 검역소 목록 조회 및 내보내기</li><li>· 검역소 파일 복원</li></ul> <p><b>프로그램 종료</b></p> <ul style="list-style-type: none"><li>· 실행 프로그램만 종료</li><li>· 프로그램 제거 (검역소, 로그, 환경설정 데이터 삭제)</li></ul>

AhnLab Xcanner는 단독 사용도 가능하지만 AhnLab EPS와 연동해 사용하면 더 강력하고 정밀한 악성 코드 방어가 가능합니다. EPS 연동 시 Xcanner의 검사 및 치료 로그를 중앙화하고 관리 콘솔에서 모니터링 할 수 있습니다. 또한, EPS의 Unlock 설정 없이도 Xcanner를 실행할 수 있어 운영 효율성을 높이고 악성 코드 감염 위험을 줄일 수 있습니다.



**탐지 영역 확대**

- 실행형/비실행형 파일 악성코드 탐지 및 치료
- 클라우드 기반 ASD 서버에서 파일 안전성 자동 분석(\*폐쇄망 미지원)
- 메모리 및 프로세스 사전 검사
- 은폐형 악성코드 진단



**EPS Lock Mode 상태에서 악성코드 진단 및 치료 지원**

- Xcanner 사용을 위한 Lock Mode 해제 및 전환 불필요
  - 락모드 해제 시 발생할 수 있는 악성코드 감염 위험 최소화
- \*EPS 독립 실행형(Standalone) 미지원  
\*시스템 운영 상황에 따라 선택적 사용 권장



**EPS 관리자 웹 콘솔에서 중앙 관리 지원**

- 관리자가 EPS 웹 콘솔에서 Xcanner로 탐지된 악성코드 치료 결과 조회
  - Xcanner 최신 버전 다운로드 지원
  - Xcanner 라이선스 관리
  - Xcanner 사용 현황 모니터링 및 정책 관리
- \*Linux 버전은 EPS 연동을 지원하지 않습니다.

**사용 환경**

**AhnLab Xcanner for Windows**

구분	권장 사양	
하드웨어	CPU	최소 운영체제(OS) 시스템 요구 사항에 따름 (Intel 계열의 CPU 지원)
	MEM	최소 운영체제(OS) 시스템 요구 사항에 따름 (권장: 128MB 이상)
	HDD	1GB 이상의 여유 공간
운영체제	Embedded OS	Windows XP Embedded Windows Embedded Standard 2009 Windows Embedded Standard 7 Windows Embedded POSReady 2009 Windows Embedded POSReady 7 Windows Embedded 8.1 Industry (Pro, Enterprise) Windows 10 IoT Enterprise
	Client OS	Windows 2000 Professional Windows XP (Professional) Windows Vista (Enterprise, Ultimate) Windows 7 (Enterprise, Professional, Ultimate) Windows 8/8.1 (Enterprise, Pro) Windows 10 (Enterprise, Pro) Windows 11 (Enterprise, Pro)
	Server OS	Windows 2000 (Server, Advanced Server) Windows Server 2003 / 2003 R2 (Standard, Enterprise) Windows Server 2008 / 2008 R2 (Standard, Enterprise) Windows Server 2012 / 2012 R2 (Essentials, Standard) Windows Server 2016 (Essentials, Standard) Windows Server 2019 (Essentials, Standard) Windows Server 2022 (Essential, Standard) Windows Server 2025 (Essential, Standard)

\* 상기 OS의 32 / 64 bit 지원

구분		권장 사양
하드웨어	CPU	최소 운영체제(OS) 시스템 요구사항에 따름 (Intel 계열 CPU 지원)
	MEM	최소 운영체제(OS) 시스템 요구사항에 따름 (권장: 300MB 이상)
	HDD	500MB 이상 여유 공간
운영체제	Cent OS	Cent OS 3.3 ~ 3.9, 4, 5, 6, 7, 8
	Red Hat Enterprise Linux	RHEL 3.3 ~ 3.9, 4, 5, 6, 7, 8.0 ~ 8.1, 9.0 ~ 9.5
	AntiX Linux	AntiX Linux 13.2, 16.2 AntiX Linux 15-1, 15-V AntiX Linux 17.2
	Ubuntu	Ubuntu 10.04, 11.04, 11.10, 12.04, 14.04, 18.04, 20.04, 22.04, 24.04
	SUSE Linux	SUSE Linux 9.2, 10.3, 12.1 ~ 12.3, 13.2
	Fedora	Fedora 8, 14
	Debian	Debian 8.9
	Redhat	Redhat 9
	Scientific Linux	Scientific Linux 6.7
	Ruby Duck	Ruby Duck 5.6, 5.6.5.x