



엔터프라이즈 보안을 위한 강력한 통합백신

ALYac 5.0

ESTsecurity

진화된 알약의 위협 대응 시나리오

알약 통합 보안 솔루션은 사전 방어부터 신속한 탐지와 대응으로 고도화된 각종 위협들에 맞서, 보다 강력하고 빈틈없는 엔드포인트 통합 보안을 구현합니다. 엔드포인트에서 발생한 각종 정보들은 ASM을 통해 일괄적으로 수집 및 관리되며, 인공지능(A.I.) 기반 인텔리전스 솔루션 Threat Inside와의 연동을 통해 침해와 관련된 상세한 분석 결과를 확인할 수 있습니다.

- 01

APT 공격 유기적 대응

Threat Inside와의 연동을 통해 위협 대응 수준 고도화
- 02

효율적인 사내 보안 통합관리

다양한 엔드포인트 제품과 연동을 통한 통합 관리 기능
- 03

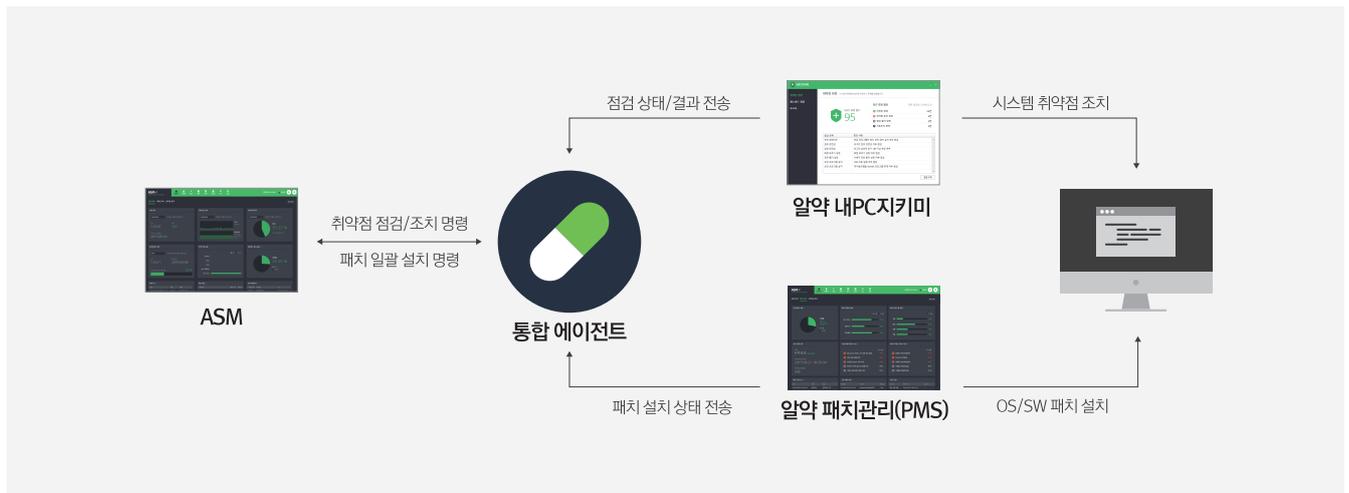
향상된 기업 보안 대응 체계 구축

일괄적 보안 정책과 위협 시각화를 통해 신,변종 공격 등 지능형 보안 위협에 효과적으로 대응
- 04

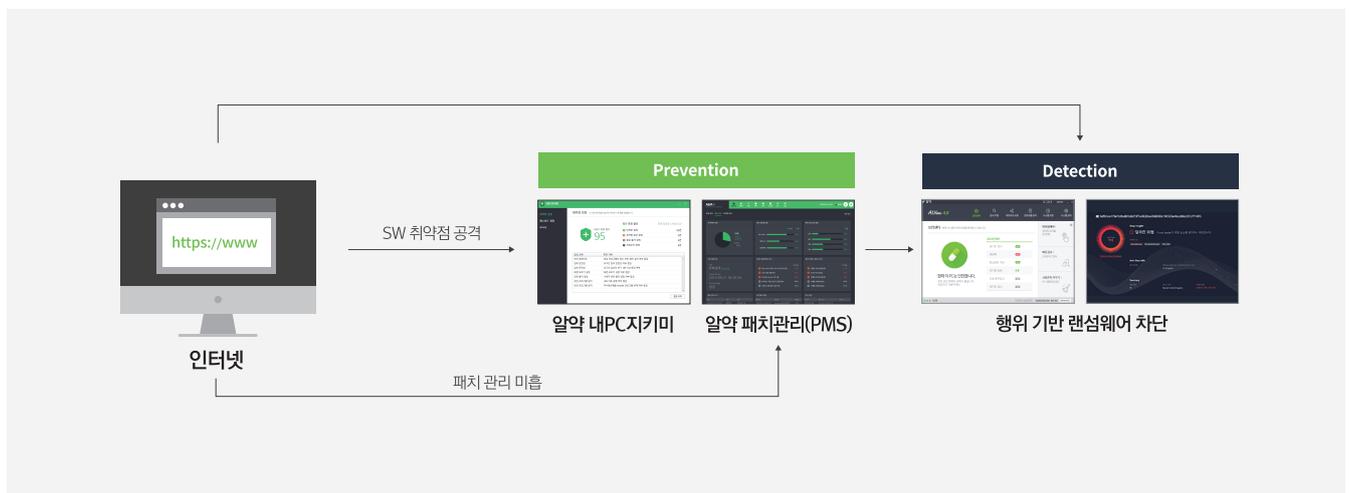
보안 강화와 비용 절감을 한번에

기업 상황에 맞는 엔드포인트 통합 솔루션 라인 구축 중앙 컨트롤타워 체계로 신속한 위기관리

보안 취약점 대응



랜섬웨어 공격 대응



알약 5.0

엔터프라이즈 보안을 위한 강력한 통합백신

알약 5.0은 뛰어난 탐지율을 보장하는 3개의 멀티엔진을 탑재하여 글로벌 위험 요소로부터 시스템을 빈틈없이 보호하고, 실시간 감시, 네트워크 보안, 매체 제어 기능을 통해 위험요소의 유입을 원천적으로 차단합니다.

보안 체계는 지능적이고 강력하게, 사용자 UI는 간결하고 편리하게, 알약 5.0은 보안에 대한 기업의 총체적 고민을 해결해 줄 **최상의 통합 보안 솔루션**입니다.



※ 소포스 엔진은 32비트 환경에서 동작합니다.

항목	CPU	RAM	HDD	OS
최소사양	Intel Dual Core 500Mhz	1GB	800MB	Microsoft Windows XP SP3 이상 / Vista SP1 이상 / 7 / 8 / 8.1 / 10 (32bit/64bit)
권장사양	Intel Dual Core 2Ghz	2GB	1GB	

왜 알약일까요?

빈틈없는 탐지율



- 국제 인증으로 인정받은 강력한 트리플 엔진 구조
- 전 세계에서 수집되는 해외 위협요소 DB와 국내 최대 사용자 기반의 국내 위협요소 DB를 통한 포괄적 탐지
- 행위/AI 엔진 기반으로 의심스러운 행위를 탐지하여 알려지지 않은 위협 차단

오탐 검증 시스템



- 오진 업데이트 전 OS 및 주요 보안 프로그램, 범용 프로그램의 설치 여부 확인 프로세스
- 오탐으로 인한 업무 중단, 복구 지원 및 비용 발생 방지

강력한 자가 보호



- 알약의 무력화 목적으로 제작된 악성코드와 각종 보안 위협에도 강력하게 보호
- 파일 및 프로세스의 자가 보호 기능 강화

높은 보안성, 빠른 검사 속도



- Smart Scan 기술을 통한 실시간 감시 및 정밀검사 시 실제 검사가 필요한 파일의 분류 기능
- 안전이 검증된 파일은 검사에서 제외하여 검사 속도 향상, 실시간 감시의 부하를 제거
- 검증된 파일이 변경 시, 악성코드 DB 신규 업데이트로 추가 검증과 지속적 관리를 통해 항상 높은 보안성 유지

가벼워진 알약, 편리한 사용



- 엔진 최적화와 프로그램 경량화를 통해 시스템에서 차지하는 메모리와 CPU 점유율 최소화
- 친숙하고 간결한 UI, 최고의 사용 편의성

자료 유출 사전 차단



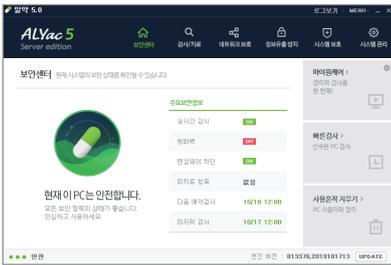
- USB 등 다양한 이동식 저장 장치 자동 검사
- 매체 제어 기능을 통해 USB 등 이동식 저장 장치를 이용한 자료 유출 사전 차단

알약 5.0 Server Edition

24시간 빈틈없는 탐지력!

서버의 경우 일반 클라이언트 PC와 달리 악성코드에 감염 시 네트워크를 통해 전사적으로 전파되기 때문에 중요 정보의 유실, 업무마비 등의 치명적인 문제를 일으킬 수 있습니다.

서버에 최적화 된 알약 5.0 Server Edition은 더욱 강력한 시스템 통합보안을 위한 다양한 부가기능이 탑재되어 있어, 기업의 정보자산 보호 및 효율적인 업무환경을 보장합니다.



※ Microsoft Internet Explorer 6.0 이상의 버전이 설치되어 있어야 합니다. 소포스 엔진은 32비트 환경에서 동작합니다.

항목	CPU	RAM	HDD	OS
최소사양	Intel Dual Core 500Mhz	1GB	800MB	Microsoft Windows Server 2003 SP2 이상 / 2008 (32bit/64bit)
권장사양	Intel Dual Core 2Ghz	2GB	1GB	Microsoft Windows Server 2012 / 2016 / 2019 (64bit)

알약 5.0 Server Edition의 주요 기능



보안 센터

- PC의 주요 보안 정보와 위험 상태를 진단하여 한눈에 확인 후 쉽게 해결
- 실시간 감시, 방화벽 설정, 검사 및 업데이트 내역 등 주요 기능을 간편하게 사용



악성코드 탐지 및 치료

- 악성코드 실시간 탐지 및 방어
- 빠른검사, 기본검사, 정밀검사 등 수준 별 검사 모드를 지원하여 필요에 맞는 효율적 검사 가능



네트워크 보호

- 네트워크 트래픽 감시를 통해 사용자의 개인정보 유출 피해 및 해킹 피해 방지
- 비정상적인 트래픽 유입을 차단하여 시스템 자원 사용 효율화
- 프로그램, IP, PORT 등 특정 규칙 별 제한 설정 가능



매체 제어

- USB 연결 및 USB를 통한 파일 복사, 이동, 생성 등 모든 동작이나 특정 동작 차단
- 차단 장치 및 차단 동작의 상세설정, 차단 예외 설정 가능



랜섬웨어 차단

- 랜섬웨어 감염으로 인한 사용자 파일 암호화를 사전에 차단
- 랜섬웨어 보호 대상 파일 백업 후 자동 복구



PC 관리

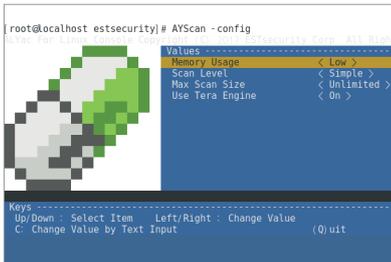
- 업데이트, 악성코드 검사, 시스템/사용기록 정리를 한 번에 실행하는 마이원케어 기능
- 미사용 파일, 연결된 파일이 없는 레지스트리의 정리 및 복구 기능
- 윈도우 임시 파일, 인터넷 임시파일, 쿠키 파일의 정리

알약 리눅스/유닉스

리눅스/유닉스 서버를 위한 최적의 백신 솔루션

알약 리눅스/유닉스는 윈도우용 환경에서 이미 검증된 알약의 기술력을 바탕으로 기업 내 서버 환경에 침투한 악성코드를 검사, 치료하는 Linux 및 Unix 서버 전용 백신입니다.

듀얼엔진의 강력한 탐지력과 손쉬운 보안 관리 기능으로 기업보안을 강화하는 **리눅스 및 유닉스 서버에 최적화된 보안솔루션**입니다.



항목	CPU	RAM	HDD	OS
최소사양	Intel Dual Core 500Mhz	512MB	800MB	CentOS 4.x ~ 8.x (32, 64bit), Redhat Enterprise 4.x ~ 8.x (32, 64bit), Ubuntu 14, 16, 18, HP-UX 11.31 (IA64), HP-UX 11.31(PA-RISC), Solaris10(SPARC), AIX7.1(POWERPC)
권장사양	Intel Dual Core 2Ghz	1GB	1GB	

알약 리눅스/유닉스의 특징점



악성코드 탐지 및 치료

- 다양한 종류의 악성코드 검사 및 치료
- 터미널 환경과 웹 환경에서의 검사 및 치료 지원
- 다양한 검사레벨을 통한 검사영역 설정 가능
- 옵션값을 통한 탐지 제외설정 가능



엔진 업데이트

- 터미널 환경 및 웹 환경을 통한 엔진 업데이트 지원
- 예약설정을 통한 주기적인 업데이트 지원



검사로그 저장

- 악성코드 검사 로그 저장
- 터미널 환경 및 웹 환경에서 로그 조회 가능
- 사용자 메일에서도 로그 확인 가능



다양한 브라우저 지원

- 별도의 플러그인 설치 필요 없음
- 모든 웹 브라우저 완벽 지원



실시간 감시

- 24시간 악성코드 실시간 탐지 및 방어
- 바이러스 및 악성코드 등에 노출되는 위협 사전 차단/처리

ASM4 알약 중앙 관리 솔루션

기업 통합 보안 관리의 중심

ASM은 관리자가 기업 내 알약 제품군이 설치된 PC에 대한 통합적인 보안 관리 및 자산관리, 보안 정책 적용 등을 수행하도록 하는 **통합 중앙 관리 솔루션**입니다.



항목	CPU	RAM	HDD	DBMS	OS
최소사양	Intel Dual Core 1Ghz	4GB	100GB	기존 DB설치 시, MSSQL만 지원	Windows Server 2003 SP2 이상 / 2008 / 2012 / 2016 (R2 포함)
권장사양	Intel Dual Core 2Ghz	8GB	200GB		Windows 7 / 8 / 8.1 / 10 (모든 OS 64bit 지원) CentOS 6.x 이상

ASM4의 특징점



보안 제품 통합 관리

- 단일 어플리케이션과 에이전트로 복수의 보안 서비스를 일괄 관리하여 사내 보안 수준 강화
- 제품 추가 도입 시 별도의 서버 구축이 필요없어 경제적인 운영이 가능



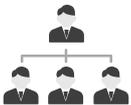
가시성 높은 대시보드

- 직관적인 그래프와 이미지로 구성된 대시보드로 실시간 보안 현황 모니터링
- 탐지 정보, 매체제어 현황 등 다양한 보안 정보를 활용하여 위협 대응을 위한 가시성 확보



간편한 PC제어

- 손쉬운 관리자의 사용자 PC 지원
- ASM4.0은 실제 데스크탑 수준의 빠른 제어 기능을 제공하며 중계 서버 적용으로 보다 안정적인 사용 환경을 제공



빠르고 편리한 정책 배포

- 부서별/그룹별 맞춤 정책 적용을 통해 조직의 특성에 맞는 보안 환경의 구축 가능
- 상하위 그룹 정책, 가상 그룹 정책, 상속 정책 등 정책 배포 방식을 통해 보안 환경 관리의 효율을 제고 가능



강력한 매체제어

- 매체제어 정책을 통해 기업 내 각종 USB 기반 장치의 사용을 통제하고 사용 내역을 중앙에서 모니터링
- USB를 통한 기업 기밀정보 및 고객 개인정보 등의 유출을 사전에 차단



효율적인 자산관리

- 전사 하드웨어/소프트웨어 자산 현황 모니터링 및 통계보고서 출력
- 미허가 프로그램 관리 기능을 통해 허가되지 않은 프로그램을 임의로 설치하지 못하도록 차단

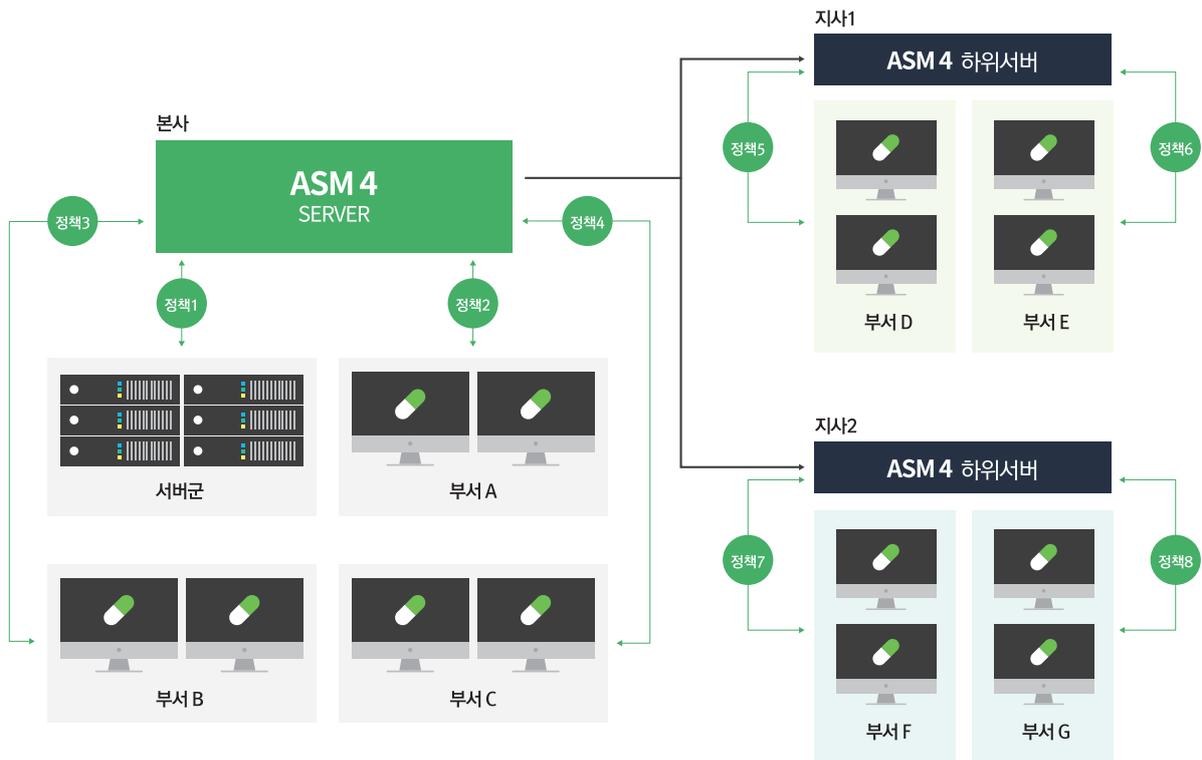
ASM4 도입 효과

ASM 도입으로 기업의 전체 보안 현황과 자산 현황을 한눈에 파악할 수 있으며, 각종 보안 위협 상황에 즉각적인 조치와 대응을 통해 안정적인 기업 보안을 가장 효율적으로 완성할 수 있습니다.



ASM4 구성도

관리자는 ASM을 통해 사내 보안 현황을 실시간으로 모니터링하고 필요한 조치를 취할 수 있으며, 맞춤 정책 적용을 통해 부서 및 그룹별로 최적화된 보안 환경을 손쉽게 구축할 수 있습니다.



주요고객사

기업

5,000여 기업



공공

1,000여 기관



교육

2,000여 기관



구매문의

[기업/공공기관/교육기관]

ESTsoft

이스트소프트
02-3470-2970

