Endpoint Security

ALYac 5.1

엔터프라이즈 보안을 위한
강력한 통합백신

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**
일관적 보안 정책과 위협 시각화를 통해
신·변종 공격 등 지능형 보안 위협에 효과적으로 대응

04 **보안 강화와 비용 절감을 한 번에**
기업 상황에 맞는 엔드포인트 통합 솔루션 라인 구축
중앙 컨트롤타워 체계로 신속한 위기관리

보안 취약점 대응

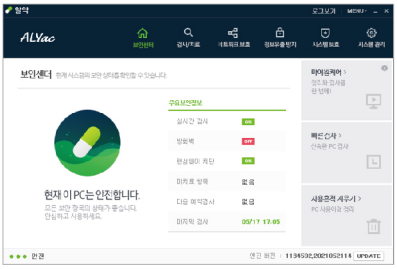
랜섬웨어 공격 대응

알약 5.1

엔터프라이즈 보안을 위한 강력한 통합백신

알약 5.1은 뛰어난 탐지율을 보장하는 2개의 듀얼엔진을 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 5.1은 보안에 대한 기업의 총체적 고민을 해결해 줄 **최상의 통합 보안 솔루션**입니다.



CPU	RAM	HDD	OS
Intel Dual Core 500MHz 이상	1GB	800MB	Windows 7 SP1 이상 (KB4490628 및 KB4474419 설치) Windows 8 / 8.1 / 10 / 11 (모든 OS 32bit/64bit 지원)

왜 알약일까요?

빈틈없는 탐지율

- 국제 인증으로 인정받은 강력한 듀얼 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 리소스 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

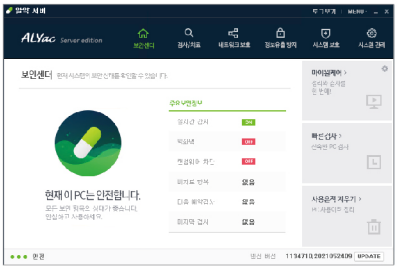
- USB 등 다양한 이동식 저장 장치 자동 검사
- 매체 제어 기능을 통해 USB 등 이동식 저장 장치를 이용한 자료 유출 사전 차단

알약 5.1 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 최적화된 알약 5.1 Server Edition은 더욱 강력한 시스템 통합보안을 위한 다양한 부가기능이 탑재되어 있어,
기업의 정보자산 보호 및 효율적인 업무환경을 보장합니다.



CPU	RAM	HDD	OS
Intel Dual Core 500MHz 이상	1GB 이상	800MB 이상	Windows Server 2008 SP2 (KB4493730 및 KB4474419 설치) Windows Server 2008 R2 SP1 (KB4490628 및 KB4474419 설치) (32bit 64bit 지원) Windows Server 2012 / 2016 / 2019 / 2022 (64bit 지원)

알약 5.1 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 수준별 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 및 IP/Port 기준으로 방화벽 규칙 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

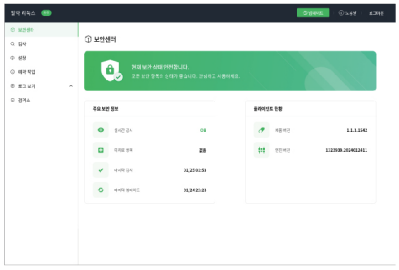
PC 관리

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

알약 리눅스/유닉스

리눅스/유닉스 서버에 최적화된 서버 보안 솔루션

알약 리눅스/유닉스는 리눅스 및 유닉스 기반 시스템을 위해 전문적으로 설계된 **서버 전용 보안 솔루션**입니다.
윈도우 환경에서 쌓인 폭넓은 경험을 바탕으로 리눅스/유닉스 환경에 맞게 최적화하여 개발되었으며,
듀얼 엔진의 강력한 탐지력과 편리한 중앙 관리 기능을 통해 기업의 핵심 데이터와 인프라를
다양한 사이버 위협으로부터 안전하게 보호합니다.



※ 본 이미지는 알약 리눅스의 웹 UI 예시입니다.

CPU	RAM	HDD	OS
Intel Dual Core 500MHz 이상	512MB 이상	2GB	**Linux** CentOS 5.x ~ 8.x, RHEL 5.x ~ 9.x, Oracle Linux 5.x ~ 9.x, Rocky Linux 8.x ~ 9.x ProLinux 7.5 ~ 8.5, Amazon Linux 1 ~ 2 Fedora 15 ~ 36 Ubuntu 14, 16, 18, 20, 22,Debian 9.3 ~ 11.2 openSUSE 12.1 ~ 15.4 SUSE Linux Enterprise Server 11.1 ~ 15.4 **Unix** HP-UX 11.31(IA64, PA-RISC) Solaris 10 ~ 11.4(SPARC) AIX 7.1(POWERPC)

알약 리눅스/유닉스의 특장점

고도화된 악성코드 탐지

- 듀얼 엔진을 이용한 강력한 탐지력
- 검사레벨 설정을 통한 탐지 수준 설정
- 터미널/웹 환경을 활용한 편리한 탐지 제외 설정 기능

실시간 파일 시스템 감시

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

자동 및 사용자 정의 업데이트

- 터미널 환경 및 웹 환경을 이용한 엔진 업데이트 지원
- 예약 작업을 통한 커스텀 스케쥴 업데이트 지원

향상된 로그 관리 및 추적

- 발생 시간, 이벤트 및 행위 주체를 포함한 상세한 로그 기록
- 미치료 로그를 별도로 분류하여 제공

중앙 관리

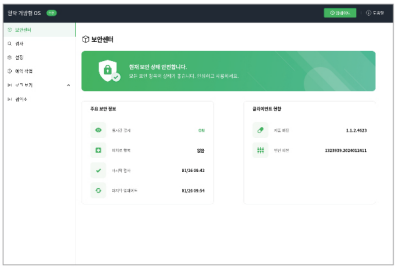
- 중앙 관리 솔루션을 연동하여 엔드포인트 보안의 통합 관리 기능 제공
- 편리한 보안 정책 설정 및 효율적인 모니터링 기능 제공

알약 개방형 OS

개방형OS를 위한 최적의 백신 솔루션

알약 개방형OS는 윈도우/리눅스 환경에서 검증된 알약의 기술력을 바탕으로 기업 내 침투한 악성코드를 검사 및 치료하는 **개방형OS 전용 백신**입니다.

관리자가 사내 보안 정책에 맞춰, 검사/업데이트 등을 효율적으로 스케줄링하여 검사 효율성을 극대화할 수 있으며,
웹 기반의 GUI를 제공하여 일반 사용자도 손쉽게 PC 검사를 진행할 수 있습니다.



CPU	RAM	HDD	OS
Intel Dual Core 500MHz 이상	512MB 이상	2GB	HamoniKR Gooroom Tmax OS

알약 개방형OS의 특장점

파일검사/치료
- 듀얼 엔진을 사용해 특정 파일 검사
- 파일 검사를 통하여 검출된 악성코드를 치료할 수 있는 기능

실시간 감시
- 실시간으로 감시하여 바이러스 및 악성코드 등에 노출되는 위협을 사전에 차단하는 기능

예약 검사/업데이트
- 정해진 시간/날짜에 검사 및 업데이트
- 예약 검사 결과는 로그에서 확인 가능

제외 처리
- 파일 이름, 파일 사이즈, 파일 확장자, 상위 디렉터리명, 특정경로의 파일 탐지명으로 제외 처리 가능

로깅
- 알약의 이벤트 로그를 웹과 터미널에서 확인 가능

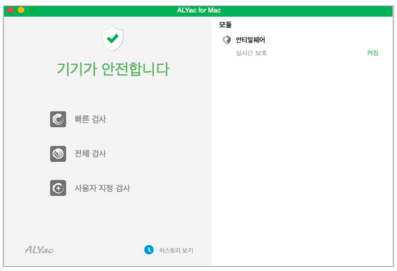
편리한 UI
- 터미널 환경에서의 CUI 지원
- 웹 기반 GUI 지원

알약 Mac

Mac OS를 위한 최적의 백신 솔루션

알약 Mac은 Mac OS를 타겟으로 하는 악성코드뿐만 아니라, Windows 환경에 대한 위협요소도 모두 탐지하여 각종 위협으로부터 시스템을 실시간으로 강력하게 보호합니다.

손쉽게 중앙 관리가 가능한 알약 Mac은 시스템의 영향을 최소화한 Mac OS에 최적화된 보안솔루션입니다.



Mac OS	RAM	HDD
macOS 10.14 (Mojave) ~ 14 (Sonoma)	2GB 이상	8.8GB 이상

알약 Mac의 특장점

강력한 악성코드 탐지

- 방대한 DB로 전세계 악성코드에 대응하며 알려지지 않은 악성코드를 탐지하는 사전 방역 능력 우수
- 악성코드의 침입 실시간 탐지 및 방어
- 빠른 검사, 전체 검사, 사용자 지정 검사 등의 다양한 검사 옵션 제공

크로스 플랫폼 탐지

- Mac OS 타겟 멀웨어와 Windows에 대한 위협요소를 모두 탐지하는 크로스 플랫폼 탐지로 다양한 루트로 침입하는 각종 위협 방어

효율적인 통합 관리

- ASM과의 연동을 통해 악성코드 방역 및 치료
- 로그 보기와 예약 검사 등 보안 정책 적용 가능
- 사내 보안 정책에 맞춰 업데이트, 스케줄링 진행
- 기업 상황에 맞는 엔드포인트 통합 솔루션 라인 구축 가능

알약 EDR 엔드포인트 위협 대응 솔루션

가장 진보된 엔드포인트 위협 대응

알약 EDR은 백신 제품인 알약과 악성코드 위협 인텔리전스 솔루션인 Threat Inside와 결합하여 이상적인
차세대 엔드포인트 보안 체계를 완성합니다.

CPU	RAM	HDD	OS
Intel Dual Core 1GHz 이상	4GB 이상	2GB 이상	Windows Server 2008 SP2 (KB4493730 및 KB4474419 설치) Windows Server 2008 R2 SP1 (KB4490628 및 KB4474419 설치) Windows Server 2012 Windows Server 2016(R2 포함) Windows 7 SP1(KB4490628 및 KB4474419 설치) Windows 8 / 8.1 / 10(모든 OS 64bit 지원)

고도화된 알약 EDR의 특장점

가시성을 극대화한 위협 흐름도

- 악성/의심 프로세스와 연관된 요약 흐름도, 상세 흐름도 및 진단 행위에 대한 상세한 표기 제공
- 데이터 수집 서버 구축 시 대시보드에서 데이터 양과 추적 범위 확대 가능

'행위 기반 의심'으로 탐지력 강화

- 위협 종류를 세분화하여 알려진 악성코드의 실시간 감시/탐지부터, 확실한 악성 행위의 차단뿐만 아니라, 의심 행위 모두를 감시함
- 코드 인젝션, 취약점(Exploit) 공격, 랜섬웨어, 자동 실행 등록 등 의심 행위 감시로 보안 대응 범위 확장

차세대 EDR의 필수요소, 위협 인텔리전스 서비스 통합

- Threat Inside의 AI 분석 및 다차원 분석 결과를 통한 정확한 악성코드 식별/분류와 상세 위협 인텔리전스 정보 제공
- IoC 등 Threat Hunting 정보화 체계 지원 가능
- 탐지 및 위협 카테고리 표준 MITRE ATT&CK 프레임워크가 반영된 위협 인텔리전스로 구체적이고 실효적인 대응 방안 제시

커널 로깅 기능으로 안정적인 운용 가능

- 강력한 커널 로깅 기능으로 위협 관련 데이터를 모니터링하며 알약과 알약 EDR의 단일 커널 레벨 드라이버 지원으로 충돌 이슈 제거

1개의 통합 에이전트로 엔드포인트 보안 솔루션 통합관리

- 알약, 알약 패치관리(PMS), 알약 내PC지키미 등 엔드포인트 보안 솔루션과 연계
- 엔드포인트에서 발생하는 위협 행위에 대한 안정적이고 효율적인 정보 수집 및 분석 가능

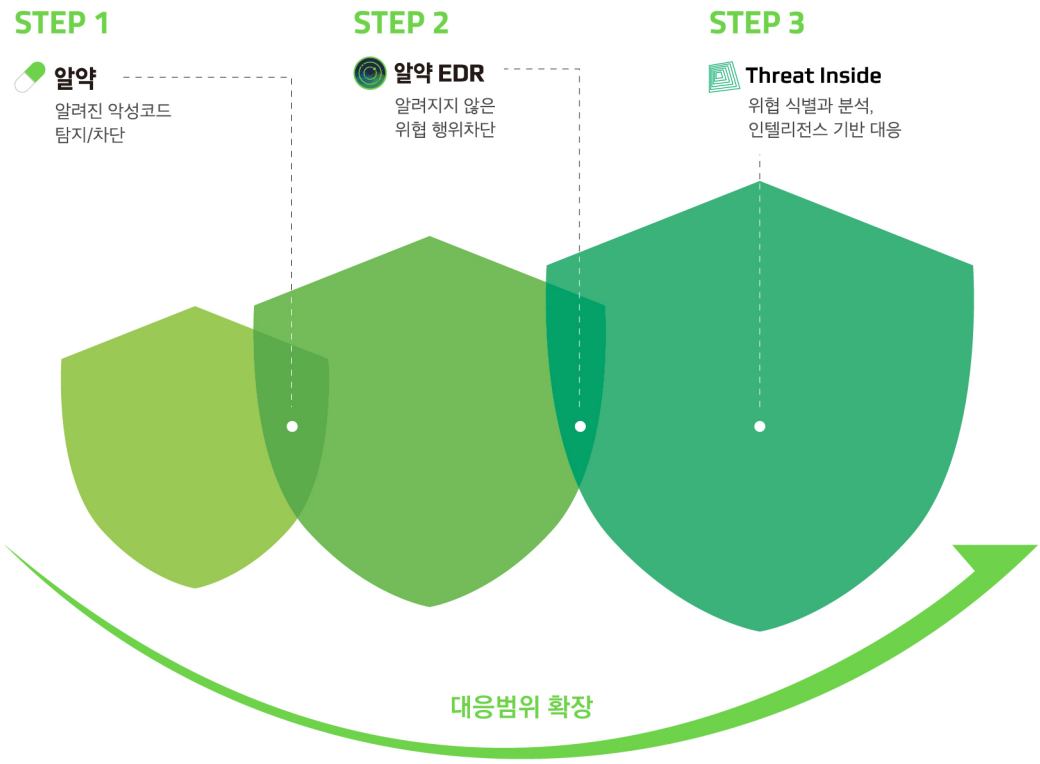
차세대 엔드포인트 보안을 위한 3단계

알약 EDR은 알려진 공격의 실시간 감시/탐지부터, 알려지지 않은 의심 행위의 선제적인 차단이 가능합니다.
또한 이스트시큐리티 1,600만 실사용자 데이터와 10년 이상의 엔드포인트 보안 노하우를 집약한 위협 인텔리전스 솔루션과 완벽히 연동되어 정확한 위협 식별 정보와 상세한 분석 리포트까지 제공하며, 대응 범위의 확장과 즉각적인 조치가 가능합니다.

1단계 **알약을 통한 알려진 악성코드 위협 탐지/차단**

2단계 **알약 EDR을 통한 알려지지 않은 위협 행위차단**

3단계 **Threat Inside를 통한 위협 식별과 분석, 인텔리전스 기반의 대응 정책 설정**



이스트시큐리티라서 가능한 고도화된 위협 대응

1,600만+국내 최다 사용자

1,600만 이상의 실사용자를 통한
악성코드 빅데이터 보유

30+ESRC 분석 전문가

국내 특화 위협에 빠르게 대응하는
악성코드 전문 인력

10+년 백신 운영 노하우

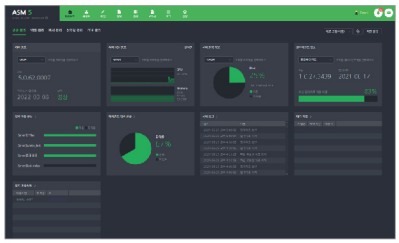
최근 2년간 탐지한 악성코드 3억 7천만 건
최근 4년간 랜섬웨어 행위 차단 850만 건

ASM5

ASM5 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.



ASM5 관리 서버

※ ASM 관리 서버 사양은고객사의 제품, Agent 수에 따라 별도의 컨설팅이 필요합니다.

OS
Windows Server 2008 R2 SP1(KB4490628 및 KB4474419 설치) Windows Server 2012(R2 포함) Windows Server 2016 Windows Server 2019 Windows Server 2022 CentOS 6.x 이상 Oracle Linux 7.x 이상 Rocky Linux 8.x (모든 OS 64bit 지원)

ASM5 관리 콘솔

CPU	RAM	HDD	OS
Intel Dual Core 1GHz 이상	2GB 이상	5GB 이상	Windows Server 2008 SP2(KB4493730 및 KB4474419 설치) Windows Server 2008 R2 SP1(KB4490628 및 KB4474419 설치) Windows Server 2012(R2 포함) Windows Server 2016 Windows Server 2019 Windows Server 2022 Windows 7 SP1(KB4490628 및 KB4474419 설치) Windows 8 / 8.1 / 10 / 11(모든 OS 64bit 지원)

ASM5의 특장점

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 구성 된 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
- ASM5는 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

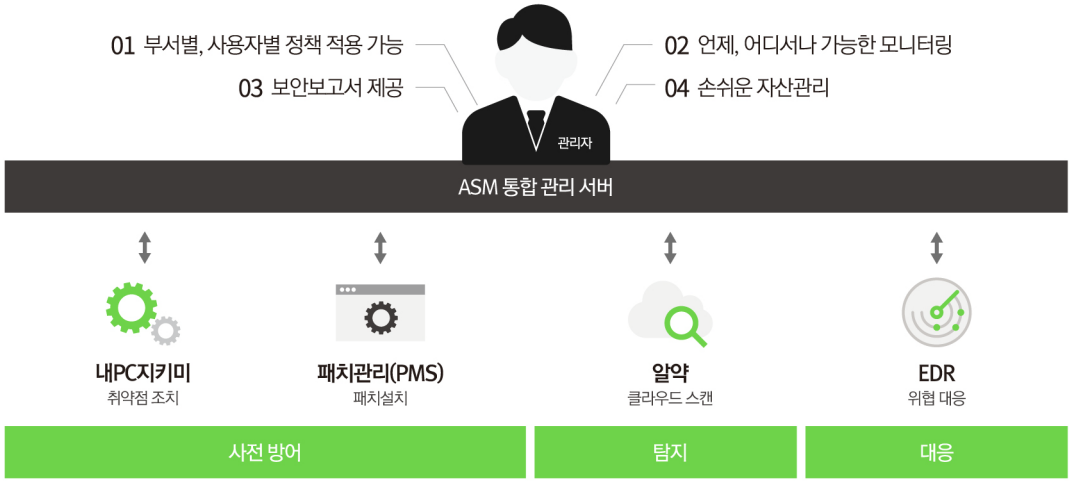
- 매체제어 정책을 통해 기업 내 각종 USB 기반 장치의 사용을 통제하고 사용 내역을 중앙에서 모니터링
- USB를 통한 기업 기밀정보 및 고객 개인정보 등의 유출을 사전에 차단

효율적인 자산관리

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

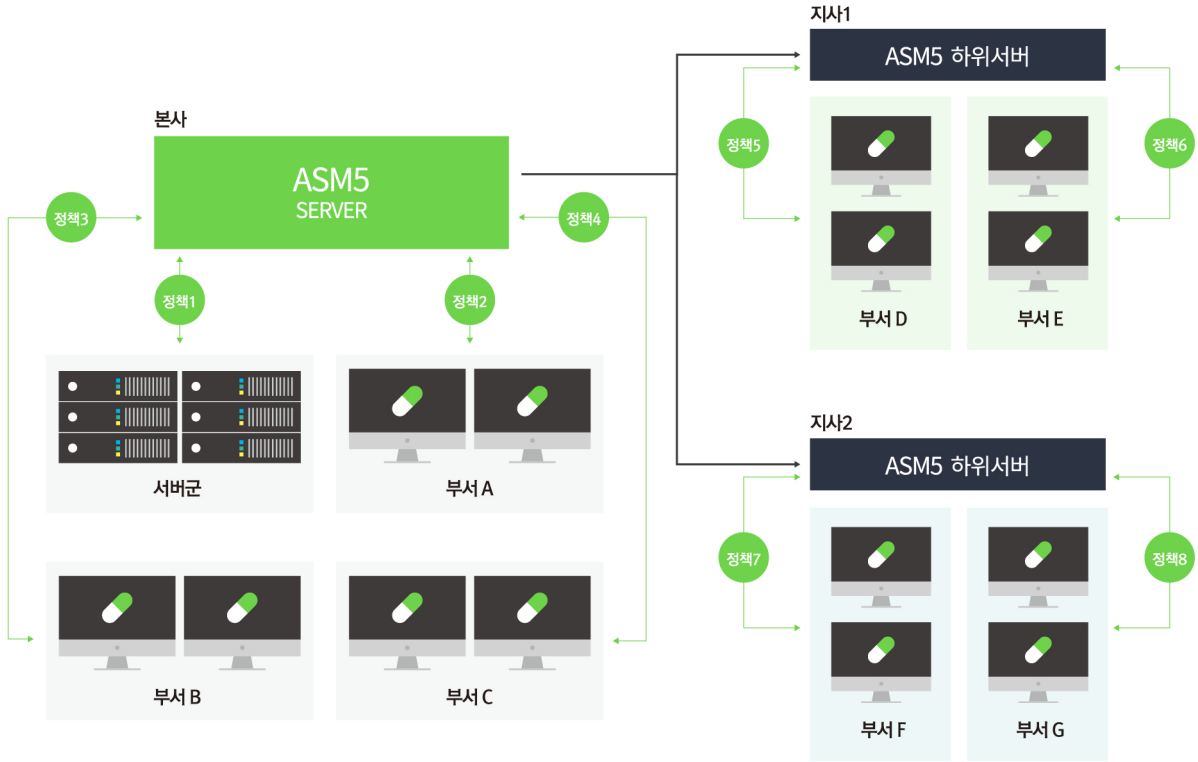
ASM5 도입 효과

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.



ASM5 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

posco
posco 포스코인터내셔널
KOREAN AIR
GS 칼텍스
S-OIL 에쓰-오일
부영그룹 BOOYOUNG GROUP
SAMSUNG 삼성전자
SOOSAN 수산아이앤티
NEXEN 넥센타이어
DAEKYO 대교CNS
SHINSEGAE CHOSUN HOTEL
ORANGELIFE
DUTY FREE HYUNDAI DEPARTMENT STORE
NICE평가정보 NICE
MIRAE ASSET 미래에셋생명
Hanwha
하림
유진투자증권
coop
JT친애저축은행

공공
1,000여 기업

행정안전부 국가정보자원관리원
해양수산부
한국수력원자력
중소벤처기업부
문화체육관광부
국민권익위원회
국토교통부
행정안전부
산림청
특허청
통계청
소방청
감사원
한국은행 THE BANK OF KOREA
KISA 한국인터넷진흥원
경상남도 GYEONGNAM
제주특별자치도
인천광역시
DAEGU 대구광역시
울산광역시
금융감독원

교육
2,000여 기업

대전광역시교육청
전라남도교육청
제주특별자치도교육청
고려대학교 KOREA UNIVERSITY
연세대학교 YONSEI UNIVERSITY
서울시립대학교
서울교육대학교 Seoul National University of Education
삼육대학교 SAHMYOOK UNIVERSITY
동덕여자대학교
용인대학교 YONG IN UNIVERSITY
상명대학교
아주대학교
충북대학교 CHUNGBUK NATIONAL UNIVERSITY
청주대학교 CHEONGJU UNIVERSITY
대전대학교
건양대학교 KONYANG UNIVERSITY
한림대학교 HALLYM UNIVERSITY
전주대학교
POSTECH 포항공과대학교
순천향대학교 SCH

ESTSECURITY

이스트시큐리티(주)

서울시 서초구 반포대로 3 이스트빌딩 (우)06711 www.estsecurity.com
T : 02-583-4616 F : 070-4850-9024 E : bizcenter@estsecurity.com

ALYac 5.1