

Integrated Management Solution

빈틈없고 효율적인 사내 인프라 관리

통합관리솔루션



ESTSECURITY

ASM 5.1

회사 전체의 보안 관리를 한 곳에서
ASM으로 업무의 효율성을 높이세요!

ASM 5.1은 보안 관리자가 대규모 업무 환경에서 보안 클라이언트를 일괄 배포하고 모니터링할 수 있는 편리한 통합 중앙 관리 솔루션입니다.

주요기능



직관적인 대시보드

운영 현황을 이미지와 그래프로 한눈에 파악할 수 있는 대시보드를 제공하여 백신, 패치, 취약점 관리의 효율성 극대화



통합 작업 관리

사용자 및 조직도 기반으로 즉각적으로 백신, 패치, 취약점 관리 작업을 수행할 수 있어 신속한 대응과 운영 효율성을 보장



정책 설정 및 일괄 적용

ASM 단일 콘솔에서 다양한 정책을 손쉽게 설정하고 일괄 적용함으로써 관리의 일관성을 유지하고 시간 소모 최소화



실시간 관리 내역 확인

에이전트가 수집한 자산 및 보안 관련 내역을 즉각 확인하고 관리할 수 있어 빠른 의사결정 가능



보고서 저장 및 미리보기

자산, 백신, 패치, 취약점 관리 현황을 보고서로 저장하거나 미리보기로 확인하여 빠르게 통찰력 있는 분석을 확인 및 보고 가능



상세 로그 확인

자산 및 보안 점검의 동작 결과를 ASM 상에서 상세 로그로 확인할 수 있어 투명한 운영과 문제 해결에 기여

제품특장점



통합 보안 관리

단일 애플리케이션 및 에이전트 : 복수의 보안 서비스를 하나의 플랫폼에서 일괄 관리하여 보안 수준을 높이고 추가 제품 도입 시 별도의 서버 구축이 필요 없어 경제적



가시성 높은 대시보드

실시간 모니터링 : 직관적인 그래프와 이미지로 구성된 대시보드를 통해 보안 현황을 쉽게 모니터링

다양한 보안 정보 활용 : 탐지 정보와 매체 제어 현황 등 다양한 정보를 통해 위협에 대한 가시성을 확보하고 신속한 대응 가능



간편한 PC 제어 및 관리

쉽고 빠른 사용자 PC 지원 : 관리자가 쉽고 빠르게 사용자 PC를 지원할 수 있으며 중계 서버 적용으로 안정적인 사용 환경 보장



효율적인 정책 및 자산 관리

맞춤형 정책 적용 : 부서별 및 그룹별 맞춤 정책을 통해 조직의 특성에 맞는 보안 환경 구축

다양한 정책 배포 방식 : 상하위 그룹 정책, 가상 그룹 정책, 상속 정책 등을 통해 효율적인 보안 환경 관리 지원

자산 현황 모니터링 : 전사 하드웨어 및 소프트웨어 자산 현황을 모니터링하고 통계 보고서 출력

미허가 프로그램 차단 : 허가되지 않은 프로그램의 설치를 차단하여 보안 강화



강력한 매체 제어

USB 기반 장치 통제 : 매체 제어 정책을 통해 USB 기반 장치의 사용을 통제하고 사용 내역을 중앙에서 모니터링

정보 유출 차단 : USB를 통한 기업 기밀정보 및 고객 개인정보의 유출 사전 차단

도입효과

효율적인 보안 제품 추가 구축 및 통합 관리

알약 제품 군 도입 시 별도 서버 구축 없이 라이선스 구매만으로 기능 활성화하여 관리 비용 최소화

단일 애플리케이션과 에이전트를 통해 복수의 보안 서비스를 일괄 관리하며 사내 보안 수준 강화

단일 콘솔, 단일 에이전트 기반의 보안 대응 체계

단일 콘솔 방식의 ASM 중앙관리 시스템을 구축함으로써 최소한의 비용으로 엔드포인트 보안 대응 체계의 마련 가능

보안 관리 영역의 뛰어난 가시성 제공

백신, 패치, 취약점, 매체 및 자산 등의 5가지 관리 영역에 대해 각종 현황 정보와 통계, 로그를 가시적으로 제공

이를 기반으로 관리자는 환경 분석과 정책 수립 후 일괄적인 또는 부분적으로 신속한 정책 적용 가능

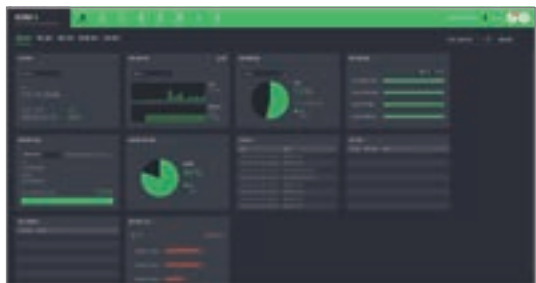
장애 대응 체계를 기반으로 안정적 운영 가능

ASM의 정상 동작 여부를 24시간 모니터링하고 장애 로그를 전송 받아 데이터베이스화된 장애 대응 체계 구축

이를 통해 장애 발생 시 즉각적인 사전 조치가 이뤄질 수 있도록 장애 대응 체계를 마련하여 안정적인 운영 가능

시연화면

대시보드



보고서 미리보기



제품 필요성

이슈	해결
한정된 인력으로 효율적인 보안 관리가 필요한 경우	통합 운영과 일관된 보안 정책 유지 지원 관리자는 ASM을 통해 실시간으로 사내 보안 현황을 모니터링하고 즉시 필요 조치 수행 가능
부서 및 그룹별 보안 정책이 달라 맞춤 정책이 필요한 경우	각 조직의 특성에 최적화된 환경을 쉽게 구축할 수 있게 하여 효율성을 높이고 리스크를 최소화
보안 관리 인력 부족	제한된 인력으로도 기업의 자산을 안전하게 보호

알약 내PC지킴이(MPI)

바쁜 관리자들을 위한 효율적인 PC 보안 관리
알약 내PC지킴이로 취약점 점검에서 조치까지 한 번에!

알약 내PC지킴이는 기업 관리자가 최소한의 리소스로 취약점을 관리할 수 있으며 통합 보안 시스템을 구축하여 고도화된 위협을 예방하고 보안 수준을 높일 수 있는 솔루션입니다.

주요기능



1. 취약점 점검

기본 점검 외 ISMS 및 PC 점검 추가
기업 특성에 맞춰 점검 항목 설정 가능



2. 보안 업데이트 관리

최신 보안 패치 설치 여부 점검 (MS, 운영체제, 바이러스 백신 등)

알약 패치 관리(PMS)와 연동해 신속한 보안 유지



3. 조치 및 관리

보안 정책에 따라 점수 기준 변경 가능
자동 조치 지원 및 수동 조치 안내 제공
점수 미달 시 네트워크 차단으로 조치 유도



4. 강제 조치 및 사용자 조치 유도

취약 시 강제 조치 기능 제공
반복 검사 및 화면 고정으로 인지 유도
안전 기준 충족 시 자동 해제



5. 점검 스케줄 설정

개인/부서별 반복 점검 스케줄 설정
진행되지 않은 점검 주기적 반복 시도
백그라운드 점검으로 사용자 부담 최소화



6. 점검 결과 관리

취약 항목 및 그룹별 진단 점수 모니터링
다양한 통계 보고서 제공
결과 누락 방지로 안정적 점검 환경 제공

제품특장점



직관적인 취약점 관리

취약점 현황 및 점검 결과 한 번에 확인 가능
점검 결과에 따른 보안 점수와 PC 상태 확인을 통해 사내 보안 수준 관리



세분화된 점검 항목

기본 점검 항목 외 ISMS 점검 및 주요 정보통신 기반 시설, PC 점검 등 취약점 정밀 진단 항목 지원
OS, 시스템, 브라우저, 네트워크 등 추가 정밀 점검 항목 지속적 확대
커스텀 점검 항목을 통해 각 환경에 필요한 점검 기준, 문구, 조치 동작 설정 가능



효과적인 보안 관리 지원

사이버 보안 진단의 날 일괄 점검 지원
보고서 양식에 맞춰 부서 및 사용자별 취약점 점검 보고서 제공



사용자의 취약점 관리 유도

점검 결과에 따른 PC 보안 점수 제공 및 상세 결과 확인을 통해 조치 유도
일괄 조치 및 상세한 수동 조치 안내를 통해 사용자 스스로 PC 관리 수준 개선
취약점 검사 반복 진행 및 화면 최상위 고정 등의 취약점 인지를 통한 조치 유도
설정된 점수 미달일 경우 사용자의 네트워크를 차단하여 완벽한 조치를 유도



통합 보안 시스템 구축

ASM 연동을 통한 일괄설치 및 클라이언트 최신 업데이트유지
사용자 및 부서별 일괄사내 보안 정책 유지
별도의 서버 구축 없이 라이선스 구매만으로 시스템 구축 가능
알약 패치관리(PMS)와의 연동을 통한 빠르고 간편한 보안 수준 유지

도입효과

간편한 취약점 조치

자동 조치 정책으로 사용자가 조치하지 않아도 자동으로 점검과 조치를 한 번에 진행

자동 조치가 불가능한 항목에 대해서는 사용자의 네트워크를 차단하여 조치 유도

일괄 조치 및 상세한 수동 조치 안내를 통해 관리자에게 문의하지 않아도 스스로 PC 관리 가능

명확한 취약점 점검

누락 점검 결과 방지를 통해서 안정적인 점검 환경 제공

한눈에 파악 가능한 취약점 현황과 점검 결과를 통해 사용자 관리 가능

점검 결과에 따른 보안 점수와 PC상태 확인

사이버 보안 진단의 날, ISMS 인증 등 다양한 컴플라이언스 점검 항목 지원

효율성 고도화

알약 제품군 도입 시 별도 서버 구축 없이 라이선스 구매만으로 사용 가능한 시스템 구축 편의성 제공

통합 관리 솔루션 ASM 연동을 통해 백신, 자산, 취약점 등 보안 기능 통합 관리

취약점 현황에 대해 빠른 파악이 가능한 시각화된 대시보드 및 보고서 제공

도입사례



“

OO 공단(정부기관) 1,200 Copy 도입

제로데이 공격에 대응하기 위한 윈도우 업데이트, 운영체제 취약점 설정을 기존에는 수동 조치하였으나 수많은 PC의 복잡한 보안 설정을 한정된 관리 인원과 비전문가인 사용자가 점검하고 조치하는 것은 한계가 명확하여 알약 내 PC지킴이 도입을 통해, 중앙관리서버(ASM)을 통해 일원화된 점검 실시 및 자동 조치/조치 유도를 수행할 수 있게 되었습니다.

제품 필요성

이슈	해결
고도화되는 취약점 공격 기업의 업무용 PC에 발생하는 악성코드 공격이 증가, 공격의 대부분은 시스템 및 애플리케이션의 취약점 이용	MPI를 통해 스스로 PC 상태와 보안 수준 확인 가능 해킹으로 인한 사용자 PC 정보 유출 피해 예방 및 보안 의식 제고 가능
급증하는 엔드포인트 보안 공격 적절한 대응을 취하지 못하는 기업은 정보 유출, 금전적 피해, 시스템 파괴 등의 위협에 그대로 노출	다양한 PC 취약 항목을 주기적으로 점검하며 사용자 PC의 안전을 지켜 피해를 최소화

알약 패치관리(PMS)

50여 종의 SW 패치도 부하 없이 빠르게
알약 패치관리(PMS)로 전사를 안전하게 보호하세요!

알약 패치관리(PMS)는 관리자가 기업 내 PC의 Windows 업데이트와 주요 소프트웨어 패치 현황을 실시간으로 확인하고 신속하게 배포 및 관리할 수 있는 솔루션입니다.

주요기능



1. 모니터링

패치 항목별 설치 진행률, 적용 상태를 보여주는 대시보드로 실시간 모니터링 가능

미설치 패치가 많은 사용자 순위 제공



2. 정책 설정

패치 종류, 설치 주기/환경, 배포 예외 패치 등 그룹별 맞춤 정책 설정

패치 롤백, 패치 적용/금지 시간 등 다양한 설치 옵션 제공

우선순위가 높은 패치를 선순위로 설치 가능



3. 패치 배포

MS OS 및 제품군 외 50여 종의 다양한 SW 패치 제공 (Adobe, 한글, Java, 크롬 등)

PC 환경과 상태에 맞춰 패치 설치

부하분산 기능을 통한 빠른 다운로드 및 배포 진행



4. 보고서

패치 및 업그레이드 관련 통계 보고서 제공

기간, 파일 양식, 에이전트 및 패치 종류별 설정 가능



5. Windows OS 업그레이드

Windows OS에 대한 빌드 업그레이드 패치 제공 및 설치

업그레이드 대상 및 목표 Windows 버전 선택 옵션 제공

업그레이드 관련 다양한 설치 옵션 및 진행 상황 모니터링 관리 가능

제품특장점



우수한 안정성

자체 검증 및 테스트 후 안전한 패치 파일 배포
PC 환경 및 상태별 패치 자동 설치
다운로드 대역폭 설정을 통한 QoS 보장



효율적인 패치 관리

패치 금지 시간, 대기일, 용량 제한 등 다양한 패치 스케줄 및 설치 옵션 제공
패치 롤백 및 배포 예외 처리 등을 통해 긴급 상황에 대한 예외 처리 가능
사용자 설치 유도를 위한 다양한 관리 옵션 제공
부하 분산 기능을 통해 시스템 부하 감소 및 사용자 간 빠른 파일 배포 가능



차별화된 사용성

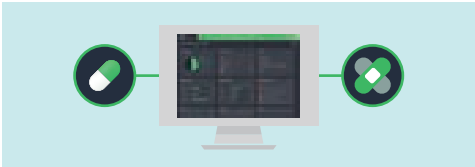
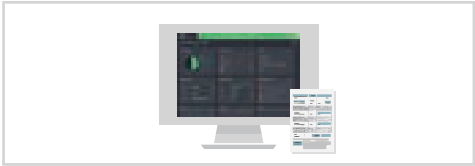
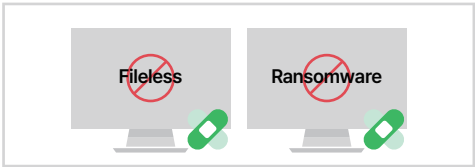
패치 현황에 대해 빠른 파악이 가능한 시각화된 대시보드와 통계 보고서
용도 및 목적에 따라 대시보드 커스터마이징 가능
조직도 연계된 직관적인 작업 및 정책 명령 프로세스 지원



통합 보안 시스템 구축

ASM 연동을 통한 일괄 설치 및 클라이언트 최신 업데이트 유지
사용자 및 부서별 일괄 사내 보안 정책 유지
별도의 서버 구축 없이 라이선스 구매만으로 시스템 구축 가능
알약 제품군과의 연동을 통해 백신, 자산, 취약점 등 보안 제품 통합 관리

도입효과



안전한 보안 환경 구축

완벽한 일괄 패치로 취약점을 이용하는 악성코드 감염 예방
실시간 모니터링을 통한 신속 대응 가능

효율적인 보안 솔루션 통합 관리

ASM 연동을 통한 시스템 구축 및 관리 비용 최소화
보안 사고 방지를 통한 기업 손실 감소 및 업무 연속성 유지

TCO 절감

통합 에이전트와 서버를 통해 다양한 보안 기능 사용
일관된 보안 정책 유지 가능

도입사례



OO 기관(정부기관)
350,000 Copy 도입

OO 기관은 산하 기관과 사무소가 전국 각지에 위치하고
있습니다.

각 거점별로 개별 운영/관리되는 PC의 윈도우 운영체제를
최소화된 리소스와 비용으로 최신 보안 상태로 항상 유지하기
위해 알약 패치관리 SW를 도입했으며 이를 통해 보안 위협에
대한 적절한 대응뿐만 아니라 PC의 성능과 안정성까지 효과적
으로 확보할 수 있게 되었습니다.

제품 필요성

이슈	해결
제로데이 취약점 제로데이 취약점 공격 사상 최대 기록 시스템 및 애플리케이션의 취약점 악용	빠른 패치 배포 및 현황 파악으로 대비 가능
지능/조직화된 APT 공격 새로운 공격 기법을 접목시켜 응용화 다양한 유입 경로를 통한 공격	패치 적용만으로도 많은 위협 감소
수동 보안/관리의 한계 비 표준화된 다수 시스템 대응 한계 한정된 담당 인력으로 관리 미흡	알약 사용 시 PMS와의 연동을 통해 제품 보안 통합 관리 가능



이스트시큐리티(주) 서울시 서초구 반포대로 3 이스트빌딩 (우)06711

T : 02-583-4616 F : 070-4850-9024 E : bizcenter@estsecurity.com www.estsecurity.com