

Endpoint Security

엔터프라이즈 보안을 위한 강력한 통합백신

알약



ESTSECURITY

알약 5.1

엔터프라이즈 보안을 위한 강력한 통합 백신
글로벌 백신 알약 5.1로 대비하세요!

알약은 위협 요소를 탐지하고 치료하는 백신 솔루션으로 바이러스와 악성코드에 대한 검사 및 치료 등 백신 기본 기능과 함께 방화벽/PC관리 기능을 부가적으로 제공합니다.

주요기능



매체제어

휴대용 저장 매체의 접근을 차단하고 사용자 맞춤형 정책 설정으로 기업의 보안 수준을 한층 강화



랜섬웨어 차단/복구

랜섬웨어 의심 행위를 사전 탐지·차단하고 변조 시 즉각적인 백업 및 복구 기능으로 파일을 안전하게 보호



유해 트래픽 /사이트 차단

강력한 방화벽과 유해 사이트/악성 행위/침입을 모두 차단하여 실시간으로 위협을 감시하고 안전한 네트워크 환경을 제공



Dual 엔진

자체 개발 엔진 테라(Tera)와 비트디펜더(Bitdefender)듀얼 엔진은 강력한 악성코드 탐지 성능으로 글로벌 위협 요소를 탐지해 사용자의 안전 보장



행위 기반

행위 기반 차단을 통해 의심스러운 행위와 알려지지 않은 위협을 탐지 및 차단



시스템 공격 차단

프로세스/메모리 검사를 통해 메모리에 로드되어 시스템을 공격하는 위협 요소를 탐지 및 차단

제품특장점



실시간 네트워크 보안

네트워크 트래픽을 실시간 감시 가능
IP/Port 기반으로 규칙 설정
행위 기반 차단으로 대응 가능



철저한 데이터 유출 방지

USB 등 다양한 휴대용 저장 매체의 접근과 사용을 제어하여 중요 정보를 안전하게 보호
허가되지 않은 데이터 이동을 차단하여 정보 유출 사고 예방



가볍고 편리한 사용

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



빈틈없는 탐지율

신속한 분석으로 알려지지 않은 의심스러운 행위를 탐지하여 차단
전 세계에서 수집되는 위협요소 DB와 국내 최대 사용자 기반 국내 위협요소 DB를 통한 포괄적 탐지

도입효과

통합 에이전트를 통한 관리 TCO 절감

엔드포인트에서 일어날 수 있는 최대한의 보안 위협을 단일 에이전트에서 대응함으로 통합 운영의 시간 절약
별도의 에이전트 설치 없이 라이선스 확장만으로 영역 확대 시간 감소

진화하는 공격에 엔드포인트 보안 대응 강화

백신 다계층 방어를 통해 예상되는 공격 예방 탐지 및 차단
알려지지 않은 공격을 악성 행위 기반 탐지 및 차단

변화하는 환경에 대한 유연한 대응

원격 제어, 클라이언트 관리, 파일 배포 등 다양한 환경에서 일어날 수 있는 이슈에 대해 즉각적이고도 유연하게 대응 가능
단일 콘솔에서 각 그룹 업무 환경에 맞는 정책 즉시 적용 가능

도입사례



OO 기관 (행정기관) 200,000 사용자 규모의 알약 백신 도입

OO 기관은 불특정 다수를 대상으로 하는 악성코드부터 특정하여 발생하는 타겟 공격까지 다양한 침해 공격에 대한 엔드포인트 대응력을 강화하고자 하였습니다.

알약 백신은 신종 변종 악성코드 뿐만 아니라 랜섬웨어와 취약점 공격도 탐지하여 차단하고 높은 수준의 기술지원 서비스를 제공할 수 있기에 해당 기관에 이상 징후 발생 시 신속 대응이 가능한 보안 체계를 구축하였습니다.

제품 필요성

이슈	해결
증가하는 Fileless 공격 기법 스크립트, 매크로, Powershell 등을 이용한 Fileless 방식이 엔드포인트를 공격하고 있으며, 기존 방식으로는 효과적 대응이 어려움	뛰어난 탐지율을 보장하는 2개의 듀얼 엔진을 탑재하여 글로벌 위험 요소로부터 시스템을 빈틈없이 보호
재택/원격 근무의 증가 사내 업무 정책의 변화로 취약한 환경의 PC가 사내 네트워크로 원격 등으로 접근하는 경우 증가	실시간 감시, 네트워크 보안, 매체 제어 기능을 통해 위험요소의 유입을 원천적으로 차단
운영 복잡성 숙련된 IT 보안 인력이 부족하며 대응 과정이 복잡해 공격 시 대응이 어려움	보안 체계는 지능적이고 강력하게, 사용자 UI는 간결하고 편리하게, 보안에 대한 기업의 총체적 고민 해결

알약 EDR

보이지 않는 위협도 선제적으로 차단하는 완벽한 방어
차세대 엔드포인트 보안 솔루션 알약 EDR이면 문제없습니다.

알약 EDR은 이스트시큐리티의 1,600만 실사용자 데이터를 기반으로 알려지지 않은 위협까지 선차단하여 10,000개 이상의 엔드포인트를 안전하게 보호합니다.

주요기능

알려지지 않은 위협을 선차단하는 엔드포인트 위협 대응 시스템



1. 위협 인텔리전스 제공

위협 흐름도 제공
Threat Inside의 위협 식별 및 분석 정보 제공
C&C/loC 등 연관 위협 정보 제공



2. 시스템/데이터 보호 및 위협 선차단

의심스러운 활동의 자동 탐지와 규명
유해 사이트 및 C&C 차단
화이트리스트 기반 사전 방역 기능
위협 탐지/분석 및 지속적 모니터링



3. 위협 정보를 선별하여 수집 및 분석

Threat Inside를 연동한 클라우드 스캔으로
신/변종 위협까지 차단
실시간 위협 모니터링



4. 즉각적이고 실효적인 대응

Threat Inside의 위협 식별 및 연관 정보와
함께 상세 분석 정보 제공
랜섬웨어와 각종 APT 공격 대응 가이드 제공

제품특장점

- 대시보드와 상세 분석 보고서를 제공해 보다 확장된 엔드포인트 보안 가시성을 제공
- '엔드포인트 보안 위협방어-탐지-대응-예측' 4단계의 순환 프로세스를 통해 알려지지 않은 위협을 선차단
- 행위 기반 의심으로 알려진 악성코드와 악성행위의 실시간 감시/탐지부터 코드 인젝션/취약점(Exploit) 공격/랜섬웨어/자동 실행 등록 등 알려지지 않은 위협이라도 의심 행위 모두를 감시
- 1,600만 실사용자 데이터와 10년 이상의 엔드포인트 보안 노하우를 집약한 알약, 알약 패치관리(PMS)/알약 내PC지키미 등 이스트시큐리티의 엔드포인트 보안 솔루션과 완벽히 연동되어 IoC 등 Threat Hunting 정보화 체계 지원 가능
- 커널 로깅 기능으로 알약과 알약 EDR의 단일 커널 레벨 드라이버 지원으로 충돌 이슈 제거

도입효과

신속한 위협 탐지 및 대응

'엔드포인트 보안 위협방어-탐지-대응-예측' 4단계의 순환 프로세스를 통해 알려지지 않은 의심 행위를 미리 차단하여 보안 사고를 예방

확장된 엔드포인트 가시성

모든 의심 행위를 감시하고 위협 흐름을 시각적으로 제공하여 즉각적인 조치 가능

상세 분석 리포트 제공

위협 식별 정보와 분석 리포트를 통해 기업의 보안 전략을 더욱 강화

안정적인 시스템 운영

커널 로깅 기능으로 위협 관련 데이터를 안정적으로 모니터링하며 시스템 충돌 문제를 방지

효율적인 자원 활용

통합 관리로 보안 운영 비용을 절감하고
인력 자원의 효율성을 극대화

도입사례



“

OO 기관 (서비스업/중견기업) 500 유저 도입

OO 기업은 해외 및 국내 다수 기업과 협업을 하는 과정에서 이메일 등을 통해 유입되는 다양한 사이버 위협에 대응하고자 하였습니다.

알약 EDR의 도입은 의심스러운 행위를 모니터링하여 알려지지 않는 Fileless 방식의 침해 공격도 효과적으로 탐지할 수 있어 지능형 사이버 위협에 대한 효과적인 대응 체계를 구축할 수 있게 되었습니다.

제품 필요성

이슈	해결
알려지지 않은 위협 증가로 커지는 기업 보안 리스크	알약 EDR은 행위 분석을 통해 알려지지 않은 위협을 식별하고 선차단 기업의 보안 리스크를 최소화하고, 피해를 사전 예방 가능

알약 서버 5.1

기업 정보자산 보호, 24시간 빈틈없는 강력한 서버 보안
알약 서버 5.1이 효율적인 업무환경을 보장합니다.

알약 서버 5.1은 서버에 최적화된 백신으로 기업의 정보 자산을 보호하고 효율적인 업무 환경을 보장하며 시스템 보안 강화를 위한 부가 기능을 탑재하고 있습니다.

주요기능



보안센터

PC의 주요 보안 정보와 위험 상태를 진단하여 한눈에 확인 가능

실시간 감시/방화벽 설정검사 및 업데이트 내역 등 주요 기능을 간편하게 사용



네트워크 보호

네트워크 트래픽 감시를 통해 사용자의 개인정보 유출 피해 및 해킹 피해 방지

비정상적인 트래픽 유입을 차단하여 시스템 자원 사용 효율화



매체 제어

USB 연결/파일 복사/이동/생성 등 특정 동작 차단 여부 설정 가능



랜섬웨어 차단

랜섬웨어 감염으로 인한 사용자 파일 암호화를 사전 차단

랜섬웨어 보호 대상을 설정해 의심 공격 발생 시 파일 백업 후 자동 복구



알약만이 할 수 있는 마이원케어

사용자 설정에 맞추어 클릭 한 번으로 업데이트, 검사, 시스템 정리 최적화 가능

제품특장점



보안센터

PC의 주요 보안 정보와 위험 상태를 진단하여 한눈에 확인 가능
실시간 감시/방화벽 설정검사 및 업데이트 내역 등 주요 기능을 간편하게 사용



네트워크 보호

네트워크 트래픽 감시를 통해 사용자의 개인정보 유출 피해 및 해킹 피해 방지
비정상적인 트래픽 유입을 차단하여 시스템 자원 사용 효율화



매체 제어

USB 연결/파일 복사/이동/생성 등 특정 동작 차단 여부 설정 가능



랜섬웨어 차단

랜섬웨어 감염으로 인한 사용자 파일 암호화 사전 차단
랜섬웨어 보호 대상을 설정해 및 의심 공격 발생 시 파일 백업 후 자동 복구



알약만의 마이원케어

사용자 설정에 맞추어 클릭 한 번으로 업데이트/검사/시스템 정리 최적화 가능

도입효과

빈틈없는 사전방역

매체 제어 기능을 통한 자료 유출 및 악성코드 침투 사전 차단
파일 암호화 사전 차단, 랜섬웨어 차단 기능
행위 기반 엔진으로 의심스러운 행위를 탐지하여 알려지지 않은 위협 차단
스마트 DB 기능을 통한 엔진 경량화 및 검사 속도 성능 최적화

강력한 백신 엔진

국제 인증을 통해 검증된 듀얼 엔진 구조의 높은 탐지력
악성코드의 침입 실시간 탐지 및 방어
클라우드 스캔과 연동한 AI 분석으로 신/변종 공격과 지능형 보안 위협에 효과적으로 대응

효율적인 통합 관리

ASM, 엔드 포인트 제품과의 연동을 통해 악성코드 방역 및 치료 보안 업데이트와 패치, 보안 정책 적용 가능
기업 상황에 맞는 엔드 포인트 통합 솔루션 라인 구축 가능



도입사례



OO 기업(제조업/대기업) 400 Copy 도입

업무 서비스가 다량으로 운영 중인 서버 내 백신은 안정성이 무엇보다 중요합니다.

OO기업은 다양한 버전의 윈도우 서버 상에서 최적화된 서버 자원을 사용하며 상황 별로 적용 가능한 다양한 심화 검사 옵션을 제공하는 서버 백신을 찾고 있었습니다. 이에 알약 서버 백신을 도입해 업무 서비스의 지속성과 최적화된 보안 정책을 유지 할 수 있게 되었습니다.

제품 필요성

이슈	해결
치명적인 서버 감염	서버 감염 시 전사적으로 악성코드가 확산될 수 있어 서버 백신 무조건 도입 필요
일하기 어려운 업무 환경	강력한 시스템 통합보안과 다양한 부가기능으로 안정적인 업무 환경 제공 기업의 생산성 극대화 가능

알약 리눅스/유닉스

리눅스 취약점 공격, 윈도우 시스템까지 확산될 수 있습니다.

서버 보안에 최적화된 강력한 솔루션 알약 리눅스/유닉스로 예방하세요!

알약 리눅스/유닉스는 리눅스 및 유닉스 기반 시스템을 위해 전문적으로 설계된 서버 전용 보안 솔루션입니다.

주요기능



강력하고 유연한 악성코드 탐지

듀얼 엔진을 통한 고도화된 탐지력과 터미널/웹 환경을 활용한 편리한 탐지 제외 설정 등 사용자 맞춤 설정으로 최적의 보안 환경을 제공



효율적인 보안 관리 및 실시간 대응

24시간 실시간 파일 시스템 감시와 중앙 관리 기능을 통해 악성코드 위협을 사전에 차단하고 통합적인 보안 관리를 실현



향상된 로그 관리

발생 시간, 이벤트 및 행위 주체를 포함한 상세한 로그를 기록하고 미치로 로그를 별도로 분류하여 제공하여 관리 용이



중앙 관리

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

제품특장점



고도화된 악성코드 탐지

듀얼 엔진을 이용한 강력한 탐지와 터미널/웹 환경을 활용한 편리한 탐지 제외 설정 기능, 탐지 수준을 자유롭게 설정할 수 있어 보안 정책에 따라 효율적인 탐지를 수행



실시간 파일 시스템 감시로 24시간 보안 유지

24시간 악성코드 실시간 탐지 및 방어 위협을 사전에 차단하고 언제 어디서나 안전한 시스템을 유지



자동 및 사용자 정의 업데이트로 최신 보안 유지

터미널 환경 및 웹 환경을 이용한 엔진 업데이트 지원으로, 최신 보안 위협에 대응 예약 작업을 통한 커스텀 스케줄 업데이트를 지원해 사용자의 편의성을 높임



향상된 로그 관리로 빠른 사고 조치

상세한 로그 기록으로 보안 사고 발생 시 신속한 대응 가능
미치로 로그를 별도로 분류하여 제공하여 보안 취약점을 빠르게 파악하고 조치



중앙 관리로 효율적인 보안 관리

중앙 관리 솔루션으로 엔드 포인트 보안을 효율적으로 통합 관리
편리한 보안 정책 설정 및 효율적인 모니터링 기능으로 보안 관리자의 업무 부담 감소

도입효과

실시간으로 정보 보호

국제 인증을 통한 듀얼 엔진의 높은 탐지력으로 악성코드 침입을 실시간으로 방어해 기업의 정보 보호를 강화

사용자 친화적인 보안 관리

저사양 서버에서도 원활하게 작동하며 손쉬운 설치로 초보자도 간편하게 사용할 수 있어 보안 관리의 효율성 극대화

도입사례



OO 기업(서비스업/대기업) 200 Copy 도입

대부분의 서비스를 리눅스 OS로 운영 중인 OO 기업은 클라우드 인프라를 포함한 서버 자원을 안전하게 보호하고자 리눅스 백신 도입을 추진하였습니다. 리눅스 타겟 악성코드를 효과적으로 차단하며 운영 서비스의 영향력을 최소화할 수 있는 알약 리눅스 백신을 선택하였으며 단일 중앙관리서버(ASM)을 통해 기존 사용 중인 PC 백신과 통합하여 일원화된 보안 정책을 적용할 수 있게 되었습니다.

시연화면

보안 센터(보안현황 및 요약)



수동 검사



제품 필요성

이슈
리눅스 서버에 대한 공격은 주로 윈도우로 이루어진 클라이언트로 확산되어 네트워크 전체에 영향을 미칠 수 있음
클라우드 인프라의 확산으로 리눅스에 대한 공격 또한 증가

해결
윈도우용 환경에서 오랫동안 검증된 알약의 기술력을 바탕으로 만들어진 리눅스/유닉스 전용 백신
신종 악성코드에 대한 빠른 대응과 안정적인 탐지 능력

알약 개방형 OS

저사양 PC 걱정하지 마세요!

최적의 백신 솔루션인 알약 개방형 OS가 있습니다.

알약 개방형 OS는 윈도우/리눅스 환경에서 쉽고 빠르게 악성코드를 검사 및 치료하는 가벼운 개방형 OS 최적화 백신입니다.

주요기능



강력한 파일 검사 및 치료 기능

강력한 듀얼 엔진을 활용하여 정밀 검사 후
검출된 악성코드를 즉시 치료



편리한 실시간 감시

실시간 감시 기능을 통해 바이러스와 악성코드의
위험을 24시간 동안 차단하고 즉각 대응 가능



예약 관리 및 예외 처리

정해진 시간에 자동으로 검사 및 업데이트를
진행하며 예약 검사 결과는 로그에서 간편하게
확인

파일 이름, 사이즈, 확장자, 상위 디렉터리명,
특정 경로의 파일 및 탐지명으로 제외 처리가
가능해 사용자 맞춤 관리 가능



편리한 UI

터미널 환경에서의 CUI와 웹 기반 GUI를 지원

직관적인 사용자 인터페이스로 편하고
효율적으로 보안 설정과 검사 결과 확인 가능

제품특장점



검증된 탐지력과 24시간 방어

테라(Tera)엔진과 비트디펜더(Bitdefender)엔진을 탑재한 듀얼 엔진 기반의 강력한
악성코드 스캔

성능 조정 옵션을 통해 최적화된 스캐닝 속도 설정 가능

실시간 감시로 24시간 동안 안전하게 시스템 보호



사용자 편의성 증대

리눅스 및 유닉스 환경에 최적화된 install 및 sh 형태로 제공

CLI와 GUI 모두 지원하여 관리 용이

파일 이름, 파일 사이즈, 파일 확장자, 상위 디렉터리명, 특정 경로의 파일 탐지명으로
제외 처리 가능

사내 보안 정책에 맞춰 검사/업데이트 등을 효율적으로 스케줄링 가능



리소스 효율성 극대화

검사 성능 조정 기능으로 저사양 PC에서도 원활하게 작동

시스템 리소스를 최소화하여 효율적으로 사용 가능

도입효과

강력한 악성코드 탐지로 안전성 확보

국제 인증을 통해 검증된 듀얼 엔진 구조의 높은 탐지력으로 악성코드를 실시간으로 탐지하고 방어하여 기업의 데이터 안전성을 극대화

손쉬운 보안 관리로 효율성 증대

리소스 최적화를 통해 저사양 PC에서도 원활하게 사용 가능하며 GUI 제공으로 간편한 보안 관리가 가능하여 기업의 보안 정책에 맞춘 효율적인 업데이트와 스케줄링을 지원

시연화면

보안 센터(보안현황 및 요약)



예약 검사



제품 필요성

이슈	해결
개방형 OS의 사용은 증가 중이지만 개방형 OS 환경에 맞춰진 Anti-Virus가 부재	개방형 OS에서도 사용자 친화적인 UI를 제공하는 Anti-Virus
복잡한 사내 보안 정책 맞춘 백신 필요	사내 보안 정책에 맞춰 검사/업데이트를 효율적으로 스케줄링 가능

알약 Mac

Windows와 Mac 모두를 보호하는 크로스 플랫폼 탐지
알약 Mac으로 안전하게 지키세요!

알약 Mac은 손쉽게 중앙 관리가 가능하고 시스템의 영향을 최소화한 Mac OS 최적 보안 솔루션입니다.

주요기능



강력한 악성코드 탐지

방대한 DB로 전세계 악성코드에 대응하며
알려지지 않은 악성코드를 탐지

악성코드의 침입 실시간 탐지 및 방어

빠른 검사, 전체 검사, 사용자 지정 검사 등의
다양한 검사 옵션 제공



크로스 플랫폼 탐지

Mac OS 타겟 악성코드와 Windows에 대한
위험요소를 모두 탐지하는 크로스 플랫폼
탐지로 다양한 루트로 침입하는 각종 위협 방어



효율적인 통합관리

ASM과의 연동을 통해 악성코드 방역 및 치료

로그 보기와 예약 검사 등 보안 정책 적용 가능

사내 보안정책에 맞춰 업데이트, 스케줄링 진행

기업 상황에 맞는 엔드포인트 통합 솔루션 라인
구축 가능

제품특장점



강력한 악성코드 탐지

방대한 데이터베이스를 바탕으로 전세계 악성코드에 대응하며 알려지지 않은
악성코드에 대한 사전 방역 능력 출중

실시간으로 악성코드 침입을 탐지하고 방어하는 기능을 제공하며 빠른 검사,
전체 검사, 사용자 지정 검사 등 다양한 검사 옵션으로 사용자 편의 극대화



크로스 플랫폼 탐지

Windows에서 제작된 악성코드와 감염 파일을 Mac에서도 탐지할 수 있는 크로스
플랫폼 탐지 기능을 제공하여 모든 환경에서의 위협 요소를 효과적으로 관리



효율적인 통합 관리

ASM과 연동하여 악성코드 방역 및 치료 로그를 쉽게 확인할 수 있으며 예약 검사
및 보안 정책 적용 가능

기업 상황에 맞춘 업데이트와 스케줄링을 통해 통합 솔루션 라인을 구축할 수 있어
보안 관리의 효율성 증대

도입효과

포괄적인 보안 강화

알려진 위협과 새로운 위협 모두에 대한 강력한 방어로
기업의 디지털 자산 보호

크로스 플랫폼 탐지로 모든 시스템에서 일관된 보안 수준
유지

운영 효율성 증대

다양한 검사 옵션으로 기업 환경에 최적화된 보안 전략 구현

통합 관리 시스템을 통한 중앙집중식 보안 정책 적용 및 모니터링

비용 절감

사전 방역 능력으로 잠재적 보안 사고로 인한 피해 최소화

단일 솔루션으로 다양한 플랫폼을 보호하여 별도 솔루션
구매 비용 절감

규정 준수 지원

강력한 엔드포인트 보안으로 각종 데이터 보호 규정 준수 지원

상세한 로그 기능으로 보안 감사 및 리포팅 간소화

기업 이미지 제고

최신 보안 기술 도입으로 고객 신뢰도 향상

데이터 유출 위험 감소로 기업 평판 보호

시연화면

메인화면



검사화면



제품 필요성

이슈

증가하고 있는 Mac OS의 위협

해결

알약 Mac은 Mac OS를 타겟으로 하는 악성코드뿐만
아니라 Windows의 위협요소를 모두 탐지하여 각종
위협 방어

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

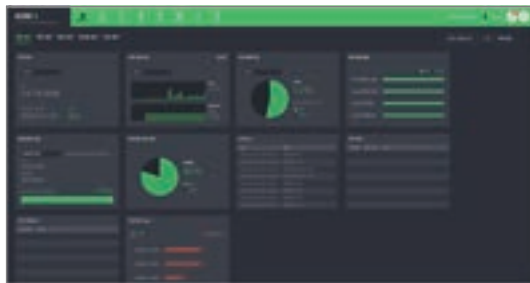
장애 대응 체계를 기반으로 안정적 운영 가능

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



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

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