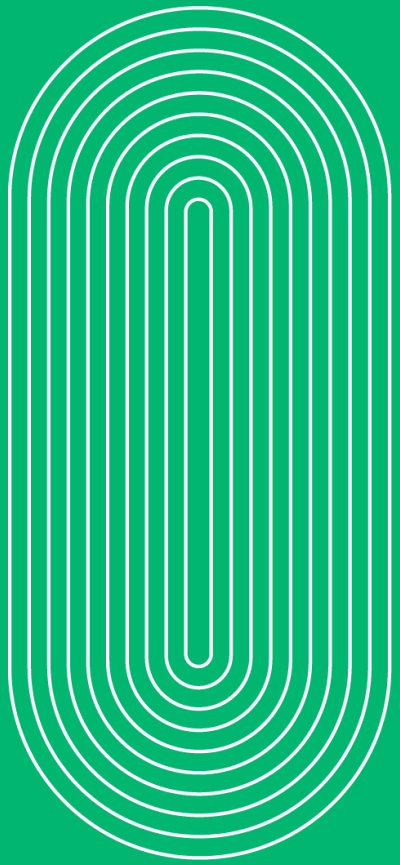
스마트한 취약점 관리 솔루션
알약 내PC 지키미



알약 내PC지키미

www.estsecurity.com

ESTsecurity

INDEX

스마트한 취약점 관리 솔루션
알약 내PC지키미

01 제안배경

- 제안 배경
- 도입 효과

02 제품소개

- 솔루션 특징
- 주요 기능

03 고객지원

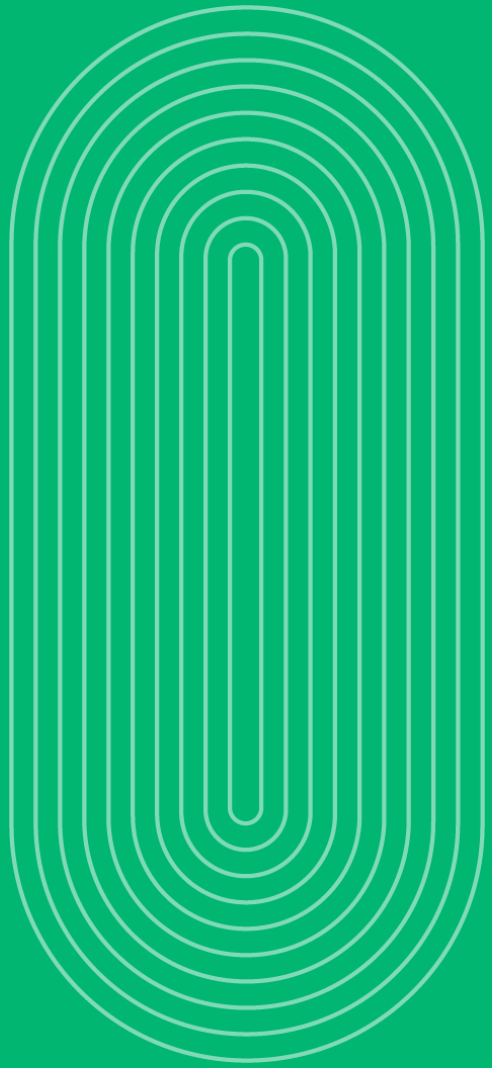
- 이스트시큐리티 대응 센터
- 고객지원 서비스

01

제안 배경

-제안 배경

-도입 효과

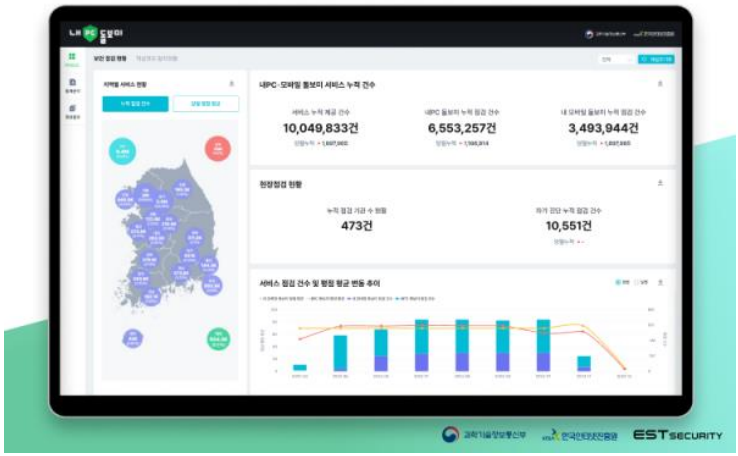


취약점으로 시작되는 보안 사고

PC,Server단말의취약점을노린침해사고의증가

- 업무용 PC, Server 단말을 통한 **침해 공격은 대부분 시스템과 애플리케이션의 취약점을 이용**
- 급증하는 취약점 공격에 사전 대비하지 못하면 해커의 위협과 정보 유출, 금전적 피해에 그대로 노출

2024년 상반기 침해 사고 신고 건수는 2023년 상반기 대비 35%증가



인터넷진흥원「내PC돌보미-PC 보안 현황 점검」

이스트시큐리티가 참여한 인터넷진흥원의 내 PC돌보미 사업의 수행 결과, PC 보안 취약점 점검 통계를 보면 **47개의 점검 항목 중 12개 항목이 취약 비율이 50% 이상**인 것으로 확인되었다.

특히 패스워드 최대·최소 사용 기간 설정과 같은 계정 관리 부문이 취약하였으며, **랜섬웨어 배포-설치에 악용될 수 있는 원격 데스크톱 포트, 공유 폴더 등의 취약한 것으로 확인**되었습니다.

출처 : https://www.datanet.co.kr

취약점 조치의 어려움

한정된 인력으로 복잡한 컴플라이언스 준수와 증가하는 장비 관리의 한계점

- 정보보안의 책임과 규제가 강화되고 각종 보안 인증에서 수 많은 단말기와 장비에 대한 취약점 조치를 요구
- 비 전문가에게는 어려운 조치 방법, 임직원들의 무관심과 비 협조로 보안 담당자의 책임과 부담은 갈수록 증가

“컴플라이언스 준수 요구”

(ISMS/ISMS-P, 전자금융감독규정, 정보보안 감사 등)





“내부의 비 협조 "

(OS, Application 별 상이한 조치법, 임직원의 무관심 등)



Microsoft

한컴오피스 2018

Adobe

취약점
점검&조치

“업무도 바쁜데..”

무관심한
임직원

“ 안 해도 모르겠지? ”



“방법을 모르겠다.”



“수많은 대상 단말기와 장비 "

(Server, PC, Notebook 등)

효율적인 관리 방안의 필요

취약점현황에대한실시간모니터링과자동점검및조치를위한방안요구

- 취약점 별 조치 방법 안내와 임직원의 협조 없이도 OS, Office 등에 대한 취약점 자동/강제화 방안 필요
- 보안 이슈 발생 시 즉각적인 취약점 조치 현황 점검 후 내부 보고를 위한 모니터링 방안 필요

답답함 불안감

조치가 필요한 수많은 점검 항목들

협조가 잘 안되는 직원들

기한이 다가오면서 느끼는 불안감

신속함 안정감

한 번 설정으로 간편하게 자동조치

자동화된 조치 유도와 명확한 안내를 통한

확실한 조치누락없는 점검 결과

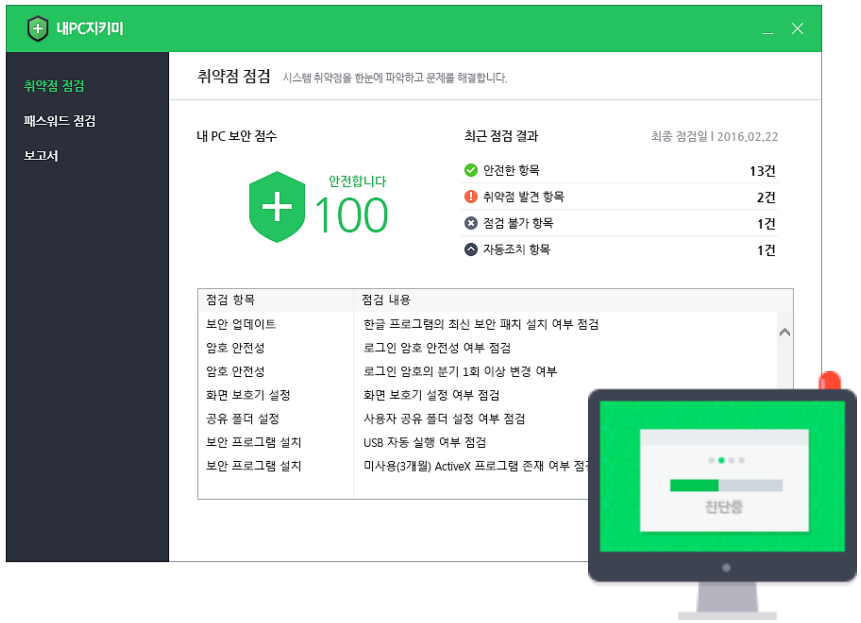
바쁜 관리자들이 **자동화된 조치**를 통해

신속하고 안정적으로 점검이 필요한 취약점을 관리할 수 있습니다

알약 내PC지키미

OS, 시스템, 주요 프로그램의 취약점 점검 및 자동 조치를 위한 취약점 관리 솔루션

EndPoint 보안 향상의 첫걸음,
알약 내PC지키미(My PC Inspector)



취약점 점검 → 진단 점수 및 조치 → 단말 보안 수준 향상

알약 내 PC지키미는 관리자가 기업 내 PC 보안 상태를 점검하고,
점검 결과에 따라 취약점을 스스로 조치할 수 있도록 지원하는
취약점 관리 솔루션입니다.

알약 내 PC 지키미 도입 시 안전하고 효율적인 PC 취약점 관리를 통해 고도화되는 위협을 사전에 예방할 수 있으며, 최소화된 운영 리소스와 비용으로 알약 및 다양한 솔루션과 연계된 통합 보안 시스템을 구축하여 보안 수준을 크게 높일 수 있습니다.

도입 효과

취약점관리솔루션으로신속하고효과적인취약점관리

- 알약 내PC지키미를 통해 수많은 IT 업무 시스템을 적은 리소스로 신속하게 점검하고 조치할 수 있습니다.



취약점 자동 조치	• 취약 항목 자동 조치로 단말기의 안전한 보안 상태 유지 • 실시간 모니터링을 통한 신속 대응 가능
취약점 현황 분석	• 단말기 별 취약점 현황 모니터링 • 보안 이슈에 대한 사내 대응 현황 및 통계 기반의 보고서 제공
보안 중앙 관리 체계 마련	• 통합 에이전트와 서버를 통해 다양한 보안 및 관리 기능 • 일관된 보안 정책 유지 가능
TCO 절감	• ASM 연동을 통한 시스템 구축 및 관리 비용 최소화 • 보안 사고 방지를 통한 기업 손실 감소 및 업무 연속성 유지

도입 효과

내 PC 지키미와 백신, 패치관리 솔루션을 단일 콘솔, 단일 에이전트로 효율적 운영

- 백신, 패치관리 솔루션과 함께 단일에이전트, 단일 관리 콘솔(ASM)로 통합하여 효율적으로 관리할 수 있습니다.



단일 콘솔

탐지 차단(알약)

- 백신
- 디바이스 제어
- 방화벽

대응 및 분석(EDR+TI)

- 프로세스 네트워크 차단
- 행위분석 탐지/차단
- 추가 분석 대응가이드 리포팅

패치 관리(PMS)

- MS 취약점패치
- 패치현황 제공

취약점 점검(MPI)

- 취약점 점검 리포팅
- 네트워크 차단

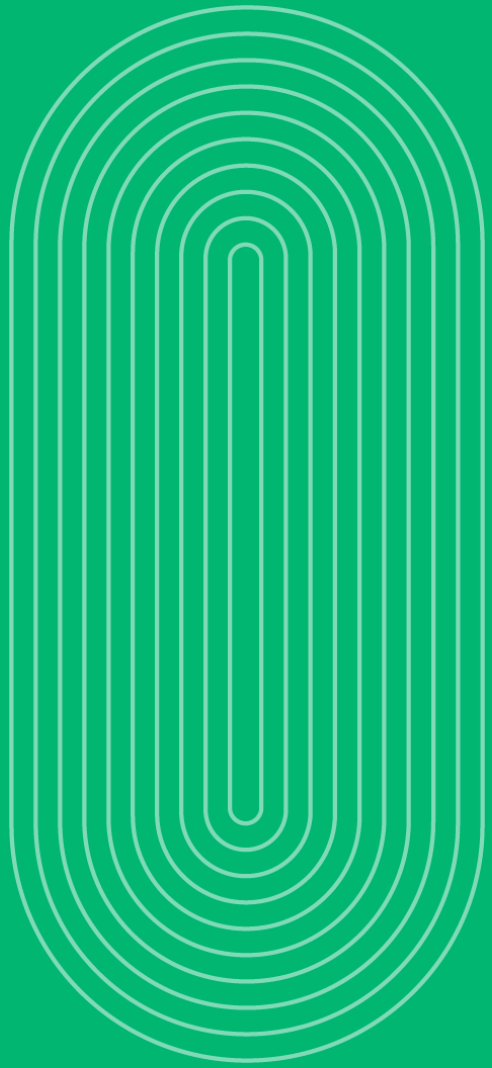
※ 알약 제품 군 도입 시 별도 서버 구축 없이 라이선스 구매만으로 사용 가능한 시스템 구축 편의성

02

주요 기능

-솔루션 특징

-주요 기능



솔루션 특징

알약 내PC지키미

바쁜 관리자들이 자동화된 조치를 통해 보다 신속하고 안정적으로 점검이 필요한 취약점을 자동 관리 할 수 있습니다.

간편한 취약점 조치

- 자동조치 정책으로 사용자가 조치하지 않아도 자동으로 점검과 조치를 한 번에 진행
- 자동 조치가 불가능한 항목에 대해서는 사용자의 네트워크를 차단하여 조치 유도
- 일괄조치 및 상세한 수동 조치 안내를 통해 관리자에게 문의하지 않아도 스스로 PC 관리 가능

명확한 취약점 점검

- 누락 점검결과 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

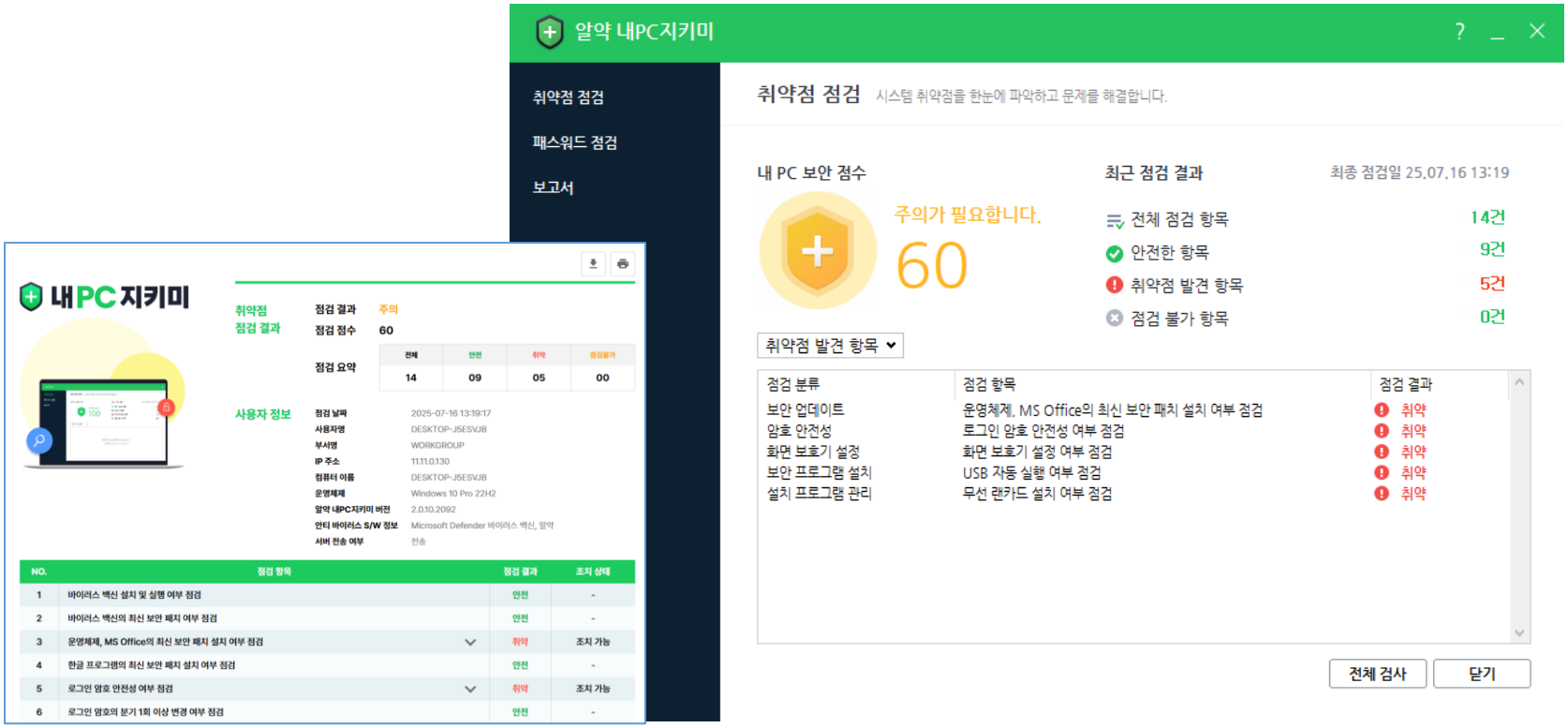
고도화된 효율성

- 알약 제품군 도입 시 별도 서버 구축 없이 라이선스 구매만으로 사용 가능한 시스템 구축 편의성 제공
- 통합 관리 솔루션 ASM5 연동을 통해 백신, 자산, 취약점 등 보안 기능 통합 관리
- 취약점 현황에 대해 빠른 파악이 가능한 시각화된 대시보드 및 보고서 제공

주요 기능

사용자 UI

알약 내PC지키미는 관리자가 설정한 점검 정책에 따라 단말기의 취약점을 점검하여 그 결과를 통합 보안 점수와 개별 항목 별로 표시합니다. 사용자는 PC 상태 및 보안 수준을 확인하고 상세 내용을 확인할 수 있습니다.

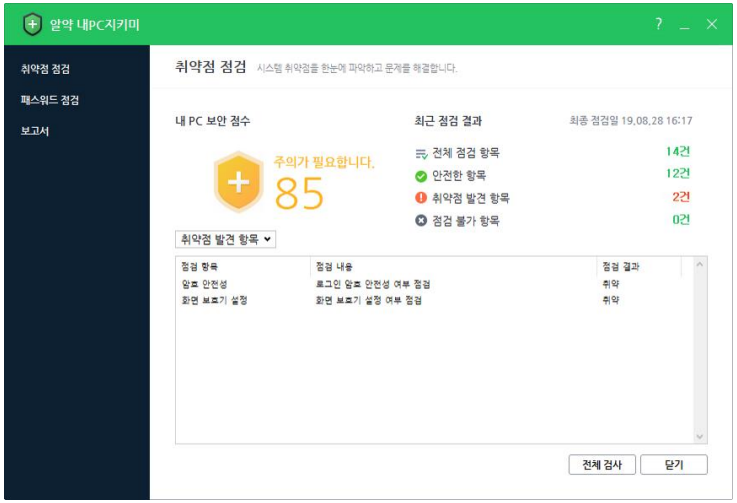


주요 기능

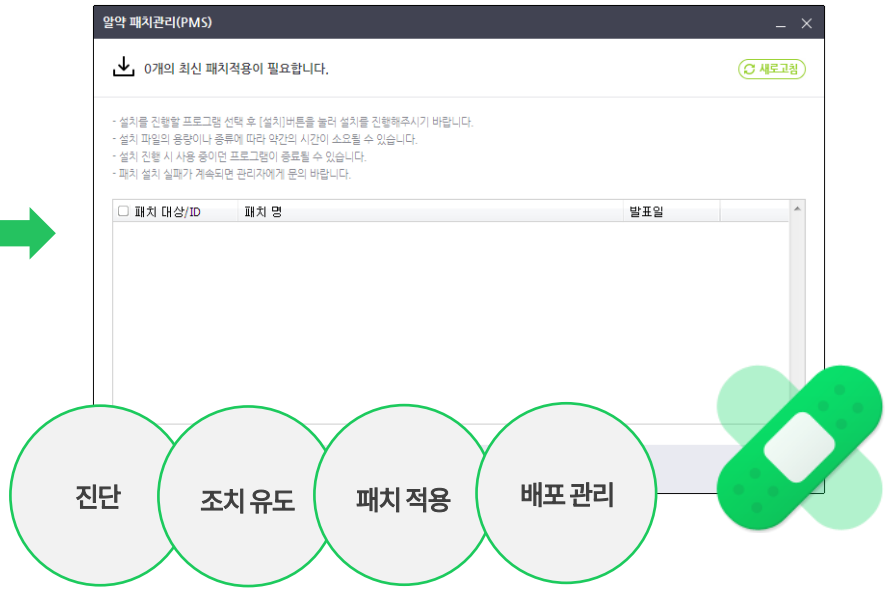
알약 백신, PMS와 연계

알약 내PC지키미는 다양한 점검 항목과 점검 설정 등 세부 정책을 통해 사용자 PC상태와 보안 수준을 효율적으로 관리할 수 있습니다. 특히 알약 패치관리(PMS)와 함께 도입 시, 알약 패치관리(PMS)와 연동되어 기업 내 PC의 윈도우 업데이트나 주요 소프트웨어의 패치 설치 현황을 실시간으로 확인하고, 신속하게 패치 파일을 배포하여 관리할 수 있습니다.

알약 내PC지키미



알약 패치관리(PMS)



주요 기능

점검 항목

다수의 기본 점검항목 이외에도 ISMS 등 주요 인증, 보안 점검에서 요구하는 점검 항목을 제공

	점검 항목 상세
ISMS 인증	바이러스 백신 설치 및 실행 여부 점검
	바이러스 백신의 최신 보안 패치 여부 점검
	운영체제, MS Office의 최신 보안 패치 설치 여부 점검
	로그인 암호 안전성 여부 점검
	로그인 암호의 분기 1회 이상 변경 여부 점검
	화면 보호기 설정 여부 점검
	사용자 공유 폴더 설정 여부 점검
	로그인 암호 입력 실패 횟수 초과 시 계정 잠금 여부 점검
	Everyone 사용 권한의 익명 사용자 허용 여부 점검
	Administrator 계정 사용 여부 점검
	Guest 계정 사용 여부 점검
	사용 안 함 계정 삭제 여부 점검
	로그인 암호 최대/최소 사용기간 설정 점검
	최근 사용한 로그인 암호 설정 점검
	Windows 자동 로그인 설정 점검
	FTP 서비스 사용 여부 점검
	시스템 기본 공유 폴더 설정 여부 점검
	전체(everyone) 권한 공유 폴더 설정 여부 점검

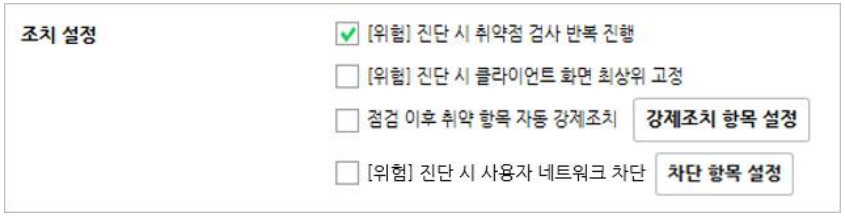
	점검 항목 상세
주요정보통신기반시설 PC 점검	바이러스 백신 설치 및 실행 여부 점검
	바이러스 백신의 최신 보안 패치 여부 점검
	운영체제, MS Office의 최신 보안 패치 설치 여부 점검
	한글프로그램의 최신 보안 패치 설치 여부 점검
	로그인 암호 안전성 여부 점검
	화면 보호기 설정 여부 점검
	사용자 공유 폴더 설정 여부 점검
	USB자동 실행 여부 점검
	미사용(3개월) ActiveX프로그램 존재 여부 점검
	PDF 프로그램의 최신 보안 패치 설치 여부 점검
	로그인 암호 최대/최소 사용기간 설정 점검
	최근 사용한 로그인 암호 설정 점검
	Windows 방화벽 사용 여부 점검
	시스템 기본 공유 폴더 설정 여부 점검
	전체(everyone) 권한 공유 폴더 설정 여부 점검
	Windows Messenger와 같은 상용 메신저 사용 여부 점검
	운영체제(OS)의 멀티 부팅 사용 여부 점검
	복구 콘솔 자동 로그인 사용 여부 점검

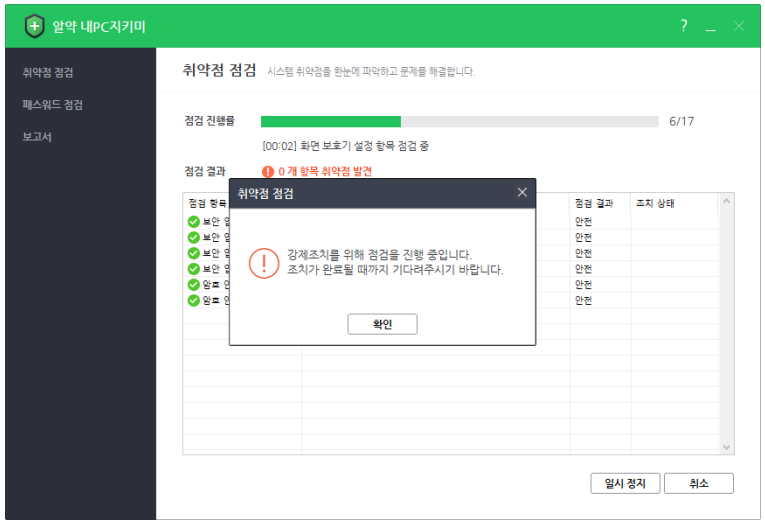
주요 기능

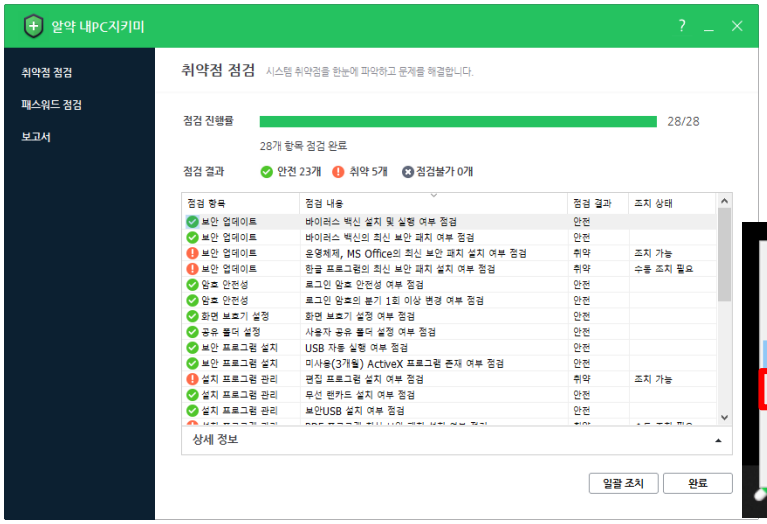
일괄 자동 조치

[자동 강제조치] 정책 설정만으로 점검 시 자동조치를 진행하여 사용자가 조치하지 않아도 자동조치 가능

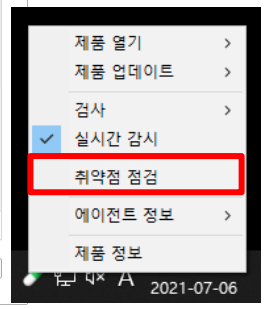
취약점 점검 결과를 항상 최신화하고 취약 항목만 조치하여 불필요한 리소스를 최소화합니다.







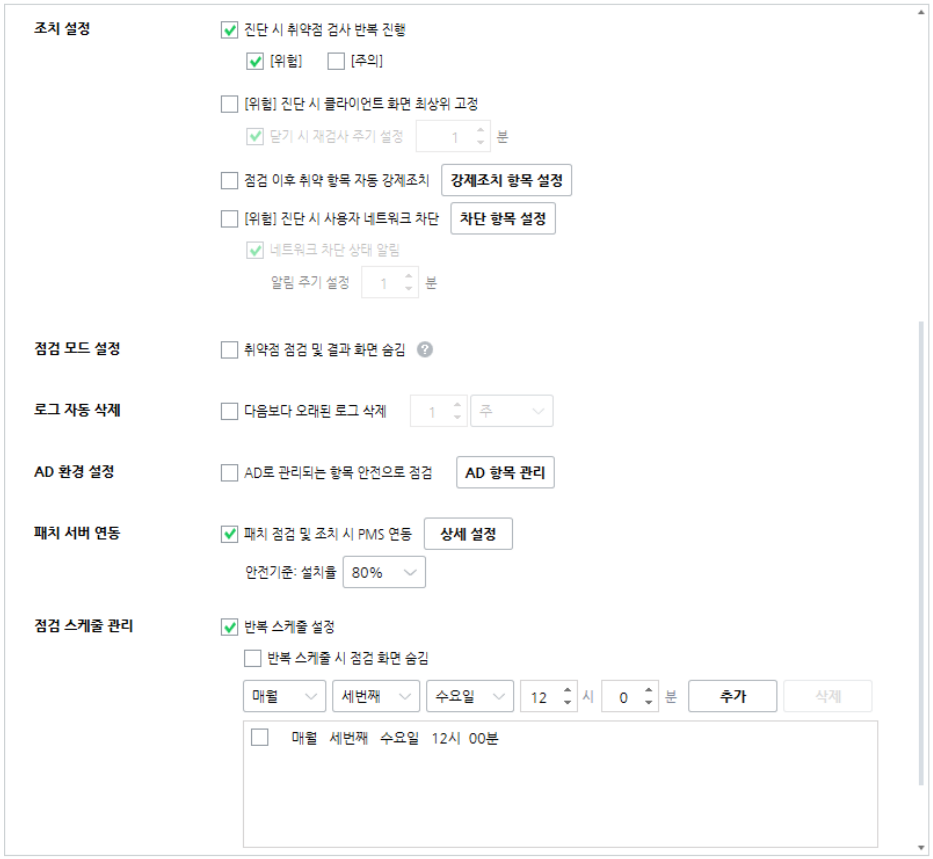
[우클릭 점검]



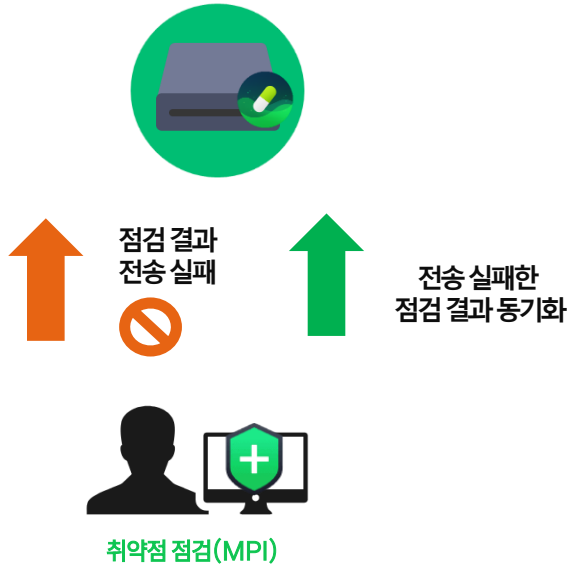
주요 기능

점검 정책 - 누락 방지

점검 스케줄관리, 취약점 검사 반복 진행을 통해 예정 된 점검일의 취약점 결과를 반영하며
점검결과 전송 실패가 발생 시 주기적인 결과 동기화를 통해서 안정적인 점검 환경 제공 합니다.



- 진단 시 취약점 검사 반복 진행
- 클라이언트 화면 최상위 고정
- 반복 스케줄 설정 (화면 숨김)

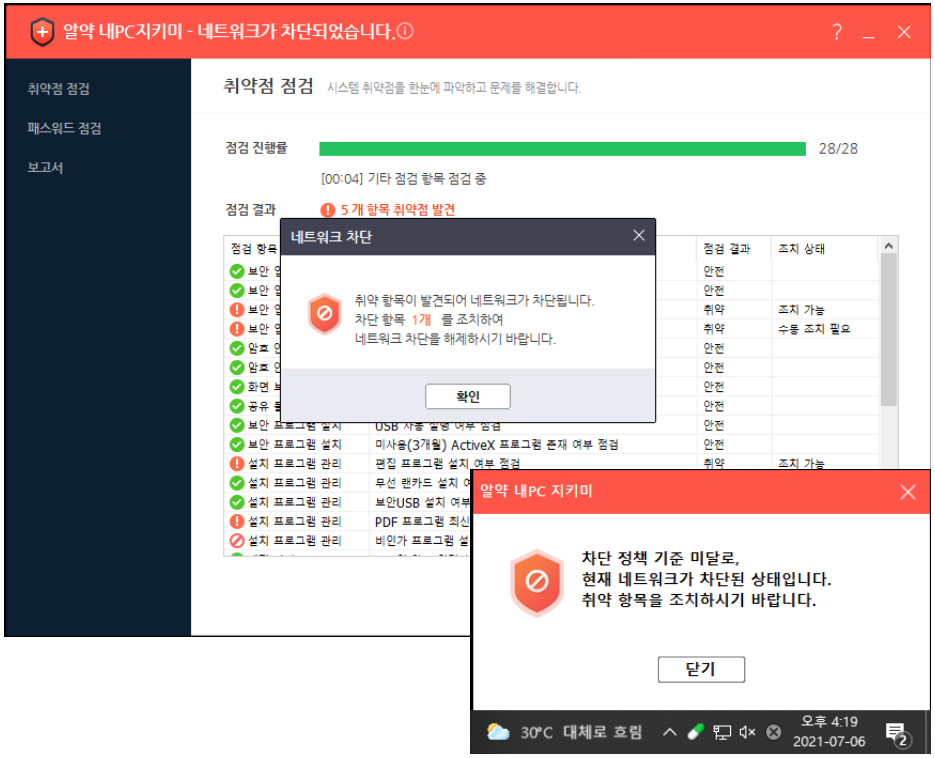


주요 기능

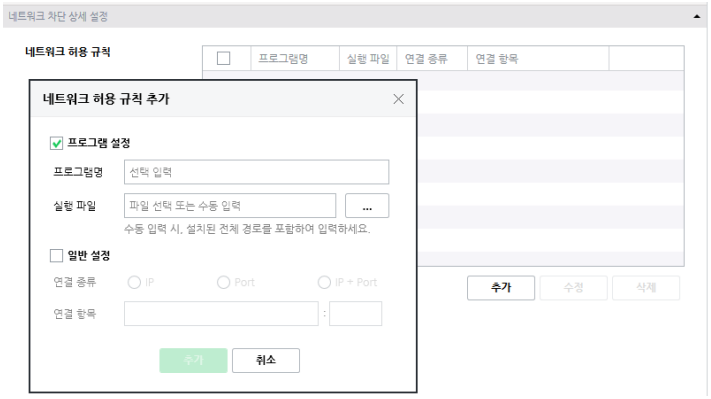
네트워크 차단

일정 점수 이하이거나 설정한 점검 항목이 취약한 경우, 사용자 PC의 '네트워크를 차단'하여 사용자 조치 유도 하고 취약한 PC를 격리 조치 합니다.

[네트워크 차단]



- 네트워크 차단 대상 점검 항목의 설정
- 네트워크 허용 규칙 추가
- [위험] 진단 시 강제 조치

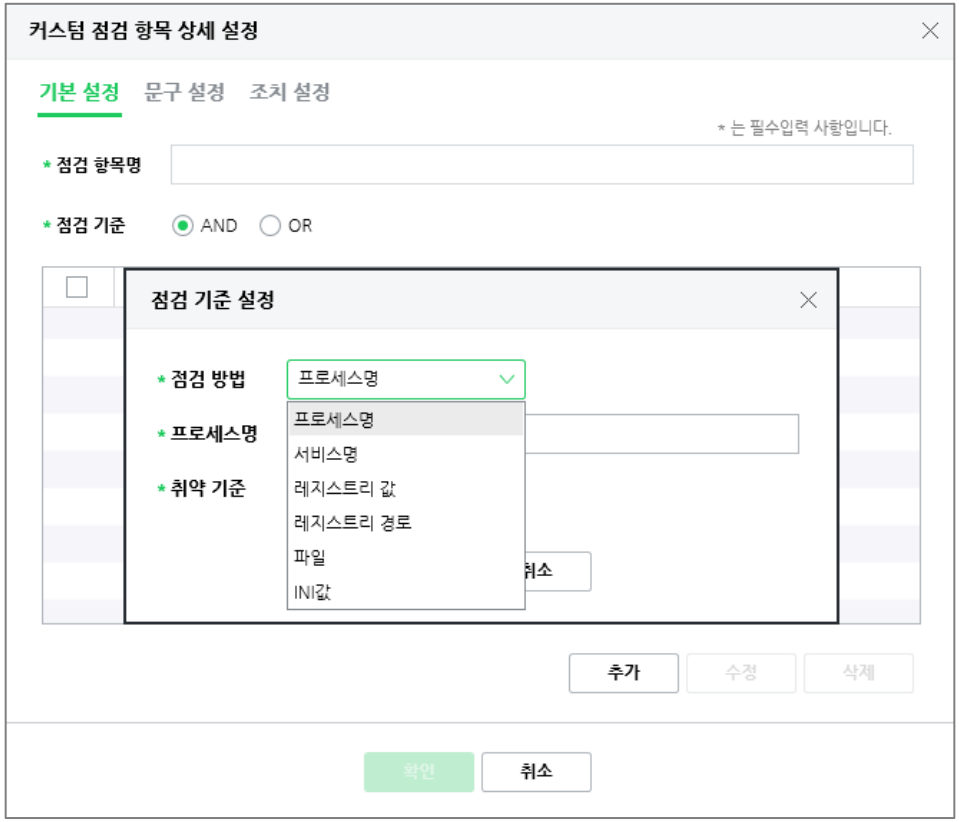


[네트워크 허용 규칙 설정]

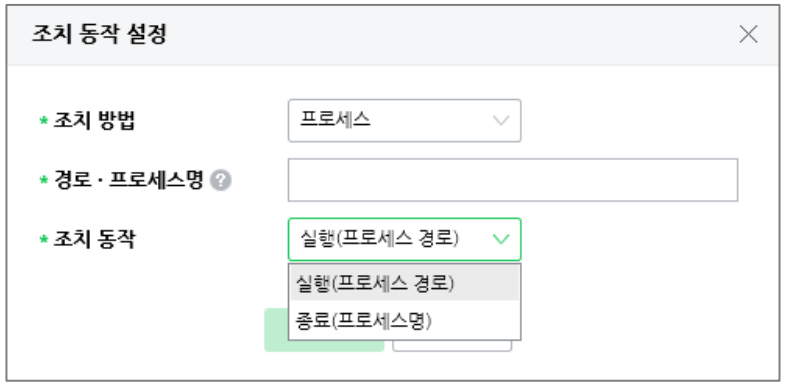
주요 기능

커스텀 점검

프로세스, 레지스트리, 서비스, 파일, INI값과 관련된 다양한 조건을 지정하여 취약 항목으로 점검하고 자동 조치하기 위한 커스텀 점검 기능을 제공합니다.



- 프로세스, 레지스트리, 서비스, 파일, INI 값을 점검하여 조건이 일치하는 경우 취약으로 검출
- 점검 시 사용자에게 노출되는 문구 등록
- 프로세스, 레지스트리, 서비스, 파일, INI 값을 지정된 동작/값으로 조치
- AND, OR 조건으로 조합하여 점검 항목 생성



주요 기능

중앙 관리

통합 관리 솔루션 ASM을 통해 취약점 점검 명령, 현황, 사용자 정보 등 사용자 PC의 취약점 통합 관리하여 운영의 편의성과 대응의 신속함을 제공합니다.



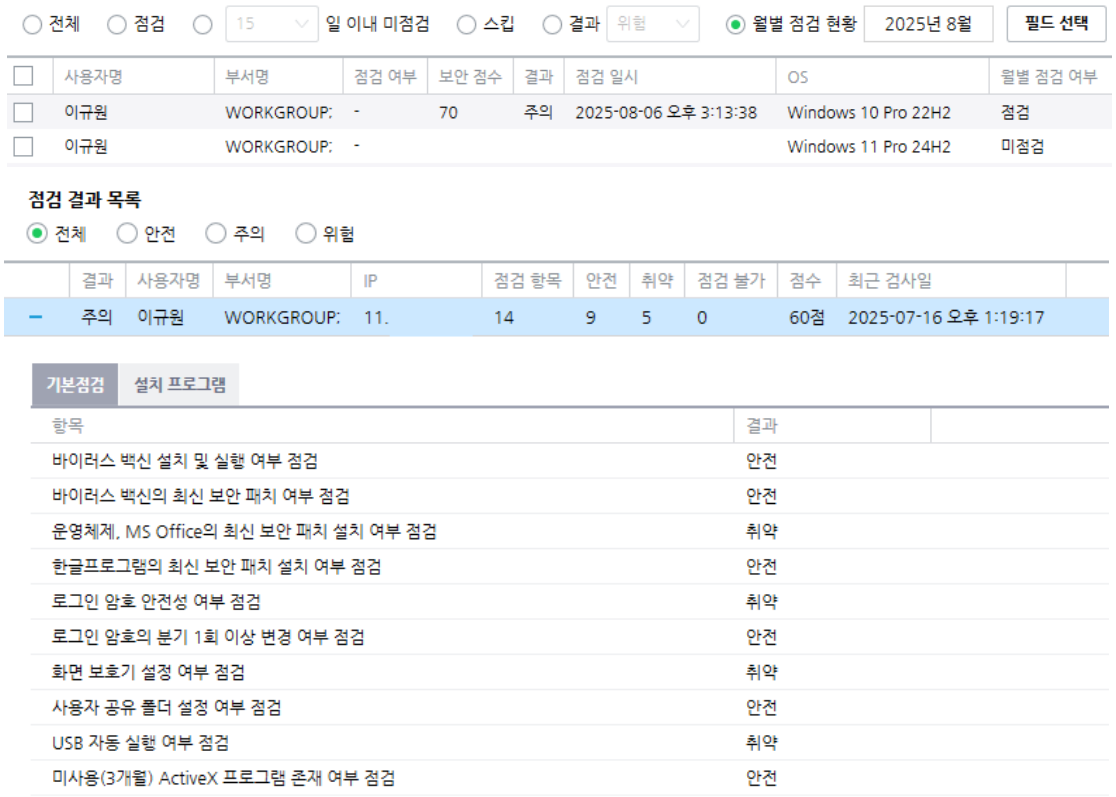
- 대시보드를 통한 실시간 관리 정보 확인
  (서버 성능, 에이전트 접속 현황, 장기 미접속자 등)
- 메시지 전송 및 회신, 원격 제어 가능
- 필수 SW에 대한 자동 배포 및 설치 유도
- 서버 로그 및 클라이언트별 이벤트 로그 관리

- 취약점 현황
  (점검여부, 보안점수, 결과, 점검 일시 등)
- 우 클릭으로 사용자 점검 명령
- 네트워크 차단 일시 해제
- 취약점 정보 가져오기

주요 기능

점검 현황 모니터링

에이전트 별로 수행된 점검 일시와 보안 점수, 월 별 점검 수행 여부를 실시간 모니터링하고 특정 에이전트를 지정하여 각 세부 점검 항목 별로 점검 결과를 확인할 수 있습니다.

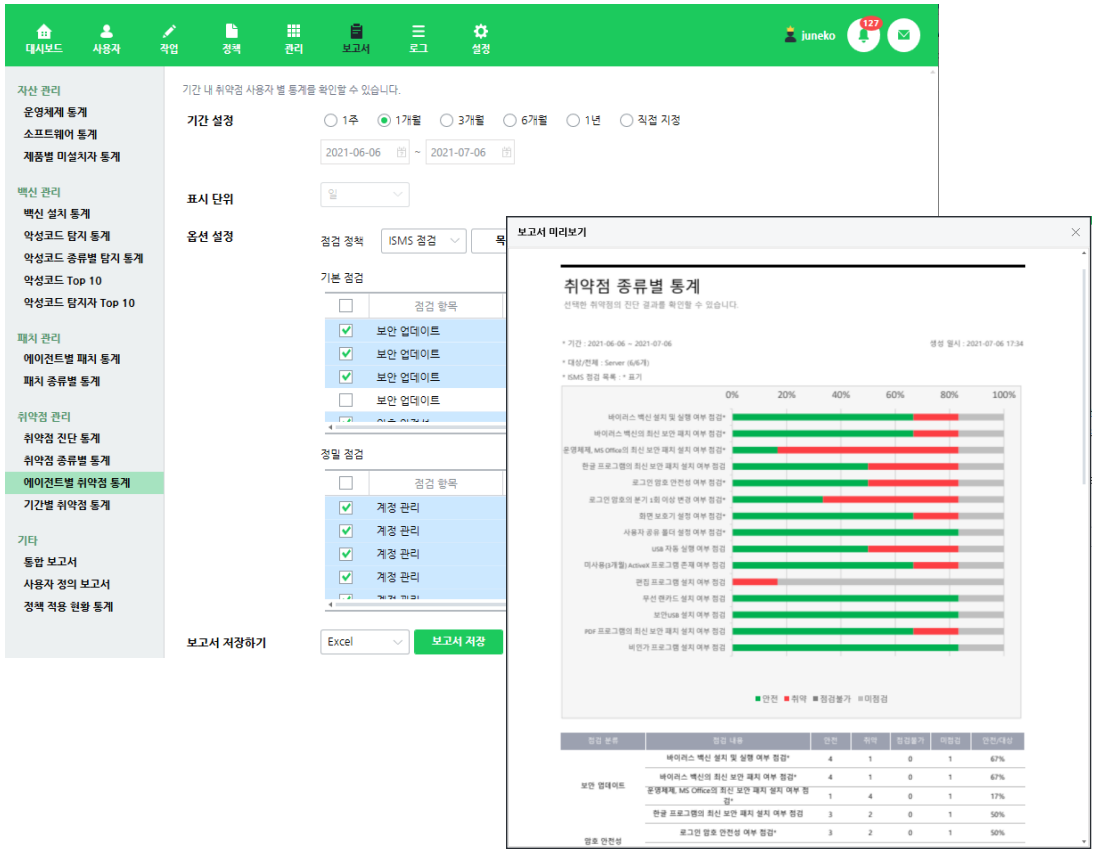


- 점검 일시
- 점검 여부
- 보안 점수 및 결과
- 사용 운영체제
- 월별 점검 여부
- 점검 항목 별 결과
- 접속 중인 IP
- 안전, 취약, 점검 불가 항목
- 다양한 조건으로 조회(검색)

주요 기능

보고서

취약점 점검 통계, 에이전트별 취약점 통계등 다양한 보고서를 저장하거나 미리보기를 지원합니다. 또한 사용자 정의 보고서를 통해 지원되지 않는 종류의 보고서를 직접 내보내기 할 수 있습니다.

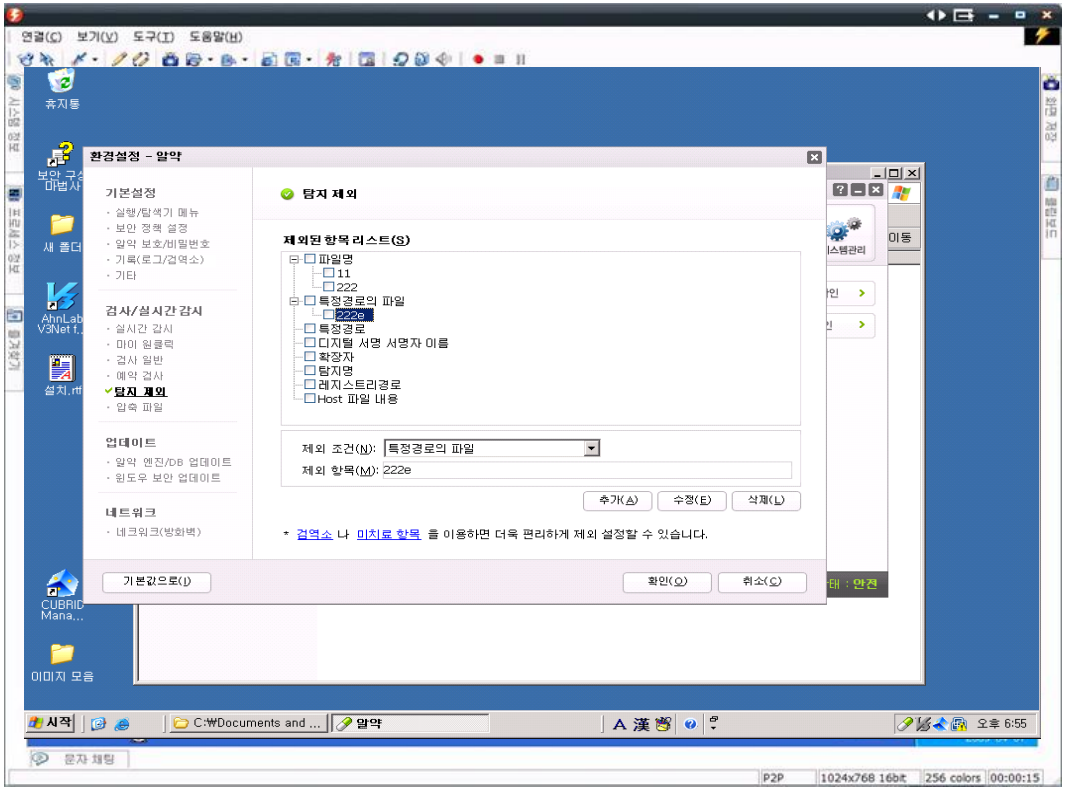


- 취약점 진단 통계
- 취약점 종류별 통계
- 에이전트별 취약점 통계
- 기간별 취약점 통계
- 통합 보고서
- 사용자 정의 보고서
- 보고서 저장 (Excel , 미리보기)

주요 기능

중앙 관리를 위한 부가 기능

ASM 관리 콘솔을 통해 개별 에이전트를 대상으로 원격 PC 제어, 파일 배포, 메시지 전송 등 관리를 위한 부가 기능을 이용하거나 조직도 연동 등으로 보다 효율적인 관리 업무 환경을 제공합니다.



원격 PC 제어

- 에이전트가 설치된 특정 사용자의 PC를 원격 제어하기 위한 기능 제공

파일 배포

- 특정 사용자에게 파일을 배포하고 실행 가능

메시지 전송

- 사용자/부서 대상 공지 메시지를 송신

조직도 연동

- 인사 DB를 연동하여 조직도에 반영하고 사용자 정보를 자동 생성/관리

OTP 연동

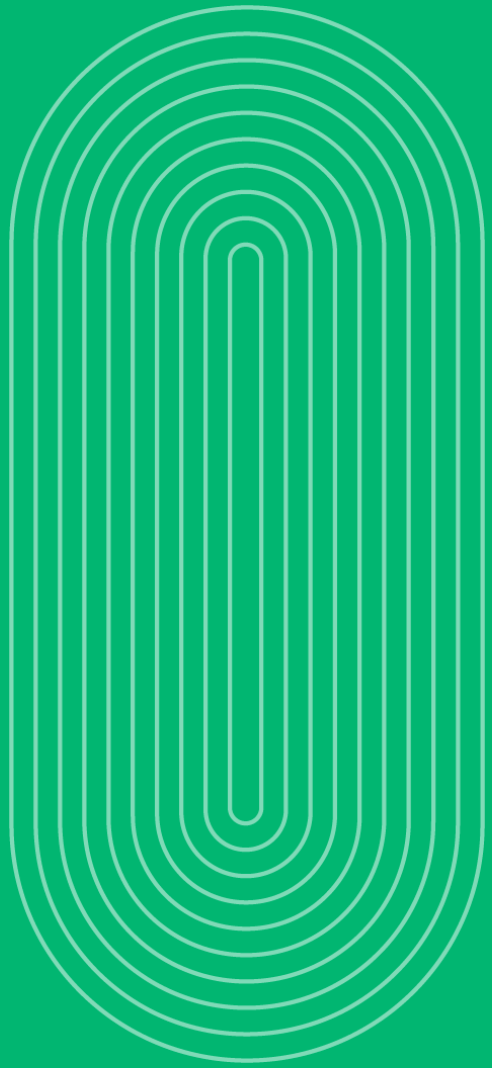
- 구글 OTP와 연동을 통해 2차 인증 적용 가능

03

고객 지원

-이스트시큐리티 대응 센터

-고객지원 서비스



ESRC

이스트시큐리티 대응센터 ESRC

국내 보안 사고는 주로 국내 사정을 잘 알고 있는 집단이 조직적이고 계획적으로 진행하여 이뤄졌습니다.

국내 최고 전문가들로 구성된 이스트시류티리 대응센터(ESRC)는 정부 주요 기관들과 연계한 **상시 대응 체계**를 유지하여,

국내에 특화된 APT 공격과 랜섬웨어 등 각종 위협에 **가장 빠르게 대응**하고 있습니다.





ESRC
이스트시큐리티대응
센터

+

커널개발 &
분석

+

A.I. Solution
개발

신종 위협 대응

고객지원 서비스

지원 센터

시큐리티 대응센터

실시간 모니터링 체계를 구축하여 국가기관과 연계한 상시 대응 체계를 유지하고 있습니다. DDos, 해킹, 랜섬웨어 등 긴급상황 발생 시 고객사를 포함한 민간의 피해를 최소하하고자 하며, 전용 백신 개발 및 배포를 통해 위기 상황에 신속하게 대응하고 있습니다.

기술 지원 센터

기업 고객들을 위한 전문 기술 지원 센터를 운영하고 있습니다. 기술지원 요청 시, 원격 지원은 물론 방문 지원 서비스 등 특화된 지원 서비스를 기업 고객들께 제공하며, 기술지원 핫라인을 24시간 운영하여 빈틈없는 보안 서비스를 제공하고 있습니다.

지원 시스템

오류 보고 시스템

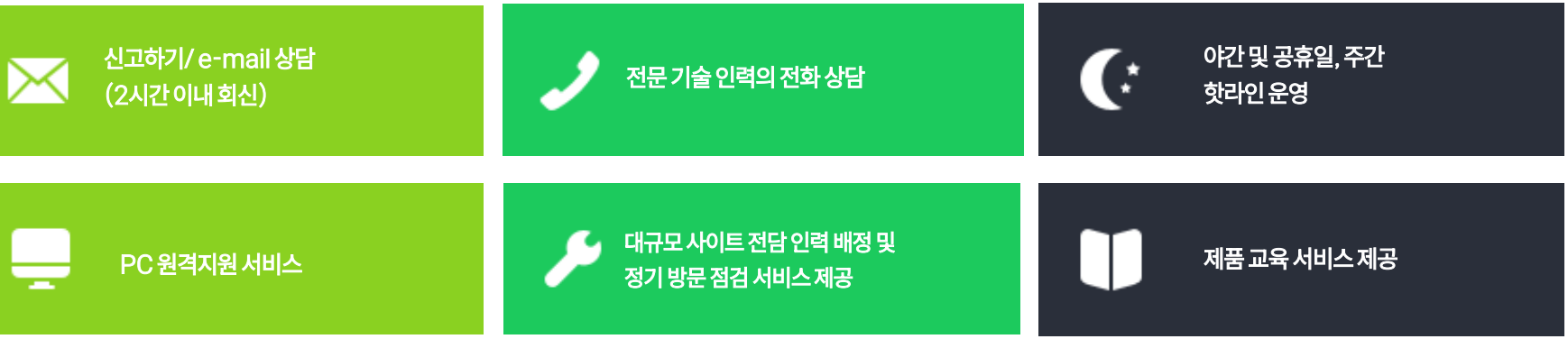
알약과 ASM은 오류 발생 시 이를 자동으로 신고하여 가장 빠르게 조치 받을 수 있는 시스템을 지원합니다. 오류 보고 시스템을 통해 관리자는 장애 상황 발생 시 신속한 선조치 및 긴급 복구 서비스를 제공받게 됩니다.

장애 모니터링 시스템

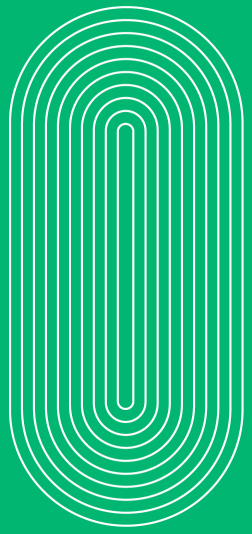
전문 보안 기술 인력들이 기업용 모니터링 시스템을 통해 고객사의 알약 및 ASM 동작 상태를 24시간 체크합니다. 모니터링 시스템을 통해 관리자가 인지하기 전에 장애 조치를 제공받고 조치 결과를 안내 받을 수 있습니다.

고객지원 서비스

전문 기술 인력이 체계적이고 신속한 고객 지원 서비스를 제공합니다.



- 구매문의 : 02-583-4616
- 고객센터 : 1544-9744
- 홈페이지 : https://www.estsecurity.com/enterprise/product/alyac-mpi



알약 내PC지키미

ESTsecurity 문의처 TEL : 02-583-4616 홈페이지 : www.estsecurity.com