표준 제안서

알약 5.1

www.estsecurity.com

ESTsecurity

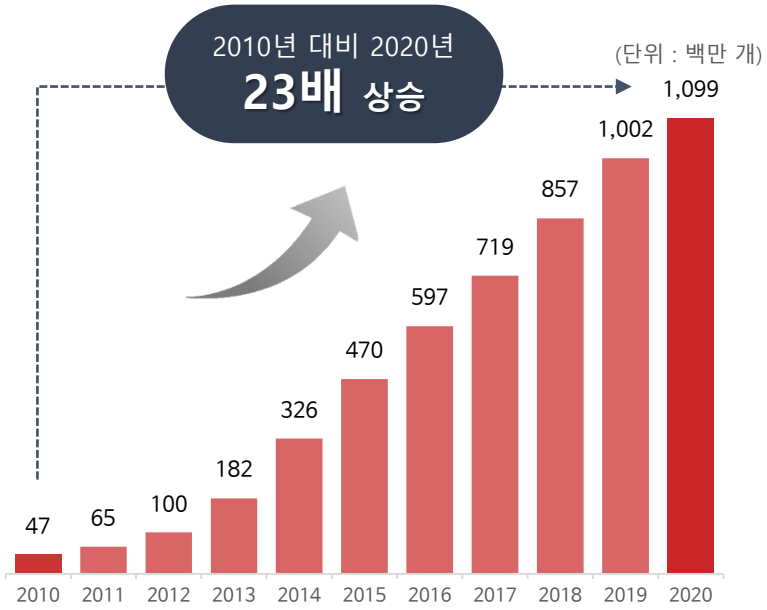
목차

1. 제안 배경

엔드포인트 보안의 중요성

대부분의 보안 사고는 엔드포인트 타겟으로 시작

- 최근 다양한 Fileless 공격 기법을 활용한 여전히 수많은 공격들이 생기고 있음
- 치밀한 방법으로 엔드포인트에 악성코드를 심는 것이 공격의 최우선 목표 → 기업 보안의 시작은 엔드포인트



출처 : AV-TEST Statistics

Fileless 공격 증가

· 블루크랩(BlueCrab) 와 메그니베르(Magniber) 랜섬웨어, 마이너(Miner, 채굴) 악성코드 등 최근 유포된 대다수가 파일리스 방식을 이용

Threat actor 공격

· 새로운 공격 기법 접목시켜 응용화
· 다양한 유입 경로를 통한 공격

엔드포인트 보안의 중요성

다양해진 경로를 통한 다양한 공격

- 이메일, 악성 웹사이트, USB, 파일 서버 등 경로는 다르지만
- 다양한 공격과 경로를 통한 해커의 궁극적인 의도는 최종적으로 결국 엔드포인트를 타겟으로 함

엔드포인트 보안의 중요성

변화하는 IT 근무 환경

- COVID-19 와 사내 업무 정책으로 변화로 인한 재택/원격 근무의 증가
- 취약한 환경에 노출되어있는 PC가 회사 사내 네트워크로 접근

재택/원격 근무 증가

· 다양한 장소에서 회사 네트워크 접속
· 보안이 취약한 네트워크 이용

운영 복잡성 증가

· 숙련된 IT 보안 인력의 부족
· 대응 과정의 복잡

보안 환경의 변화

· 내부 -> 외부 , 외부-> 내부
· 원격근무지에서 회사 내부 네트워크 접속
· 보안이 취약한 개인/공용 PC 이용

진화하는 위협

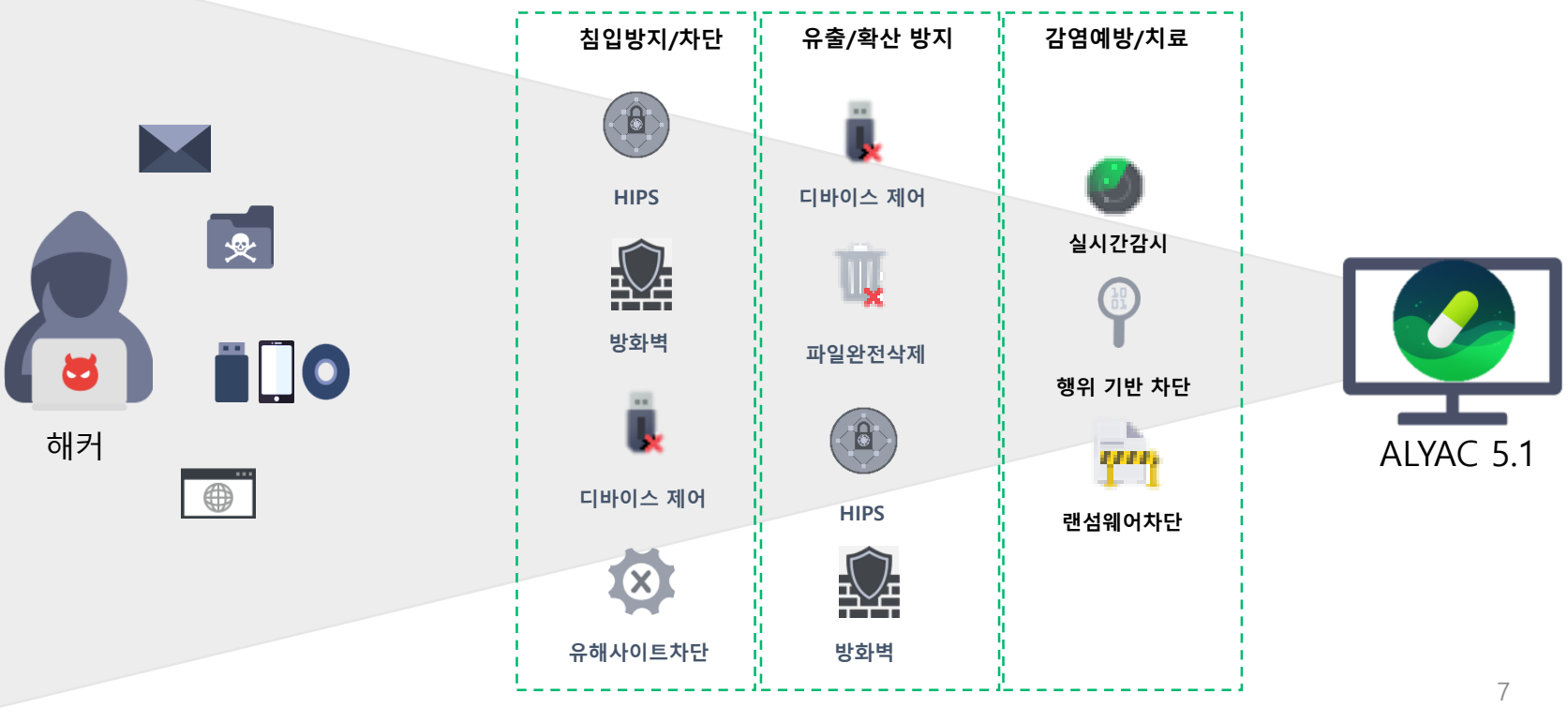
· 블루크랩(BlueCrab) 와 메그니베르(Magniber) 랜섬웨어, 마이너(Miner, 채굴) 악성코드 등 최근 유포된 대다수가 파일리스 방식을 이용

알약 5.1 도입효과

엔터프라이즈 보안을 위한 강력한 통합 백신

- 다양한 경로를 통해 유입되는 다양한 공격을 다계층 방어를 통해 실시간 대응하고 방어 할 수 있습니다.

향상 된 효율성 + 단순한 통합 보안 정책 관리 + 유연한 연동을 통한 강력한 보안



알약 5.1 도입효과

엔터프라이즈 보안을 위한 강력한 통합 백신

- 통합 에이전트를 통해 통한 효율적인 관리 대응이 가능합니다.

ALYAC 5.1

01 통합 에이전트를 통한 관리 TCO 절감

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

02 진화하는 공격에 엔드포인트 보안 대응 강화

- 백신 다계층 방어를 통해 사전에 예상되는 공격 예방 탐지, 차단
- 알려지지 않은 공격을 악성 행위 기반 탐지하고 차단

03 변화하는 환경에 대해 유연한 대응

- 원격제어, 클라이언트 관리, 파일 배포 등 다양한 환경에서 일어 날 수 있는 이슈에 유연하게 즉각 대응
- 단일 콘솔에서 각 그룹 업무 환경에 맞는 정책 즉시 적용

알약 5.1 도입효과

효율적인 보안을 단일 콘솔, 단일 에이전트 조합

- 보다 복잡해지는 IT환경에 비해 적은 보안 대응 리소스를 ASM 중앙관리 콘솔을 통해 효율적으로 신속하게 대응 할 수 있습니다.

단일
콘솔

탐지 차단(알약)

- 백신
- 디바이스 제어
- 방화벽

대응 및 분석(EDR+TI)

- 프로세스 네트워크차단
- 행위분석탐지/ 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

2. 제품 소개

이스트시큐리티

이스트시큐리티의 특장점

성공적인 보안 사업을 위한 기술, 데이터, 전문가 3요소를 모두 갖추고
14년간 축적해온 악성코드 데이터와 대응 노하우를 통해 고도화되는 위협에 효과적으로 대응하고 있으며,
최고의 악성코드 분석 기술과 인공지능 기술을 바탕으로 미래에 대비하는 새롭고 강력한 보안 솔루션을 개발하고 있습니다.

1,600만+

- 국내 사용자 수 1위(센서)를 통한 최다 악성코드 빅데이터 보유

딥러닝

- 알고리즘 기반 첨단 인텔리전스 보안
- 딥러닝 기반 악성코드 분석엔진으로 신변종 악성코드에 탐지에 특화

ESRC

- 국내 최고 전문성의 악성코드 분석가 풀 보유
- 전문가의 인텔리전스가 반영된 솔루션

엔드포인트

- 10년 이상의 '알약' 사업을 통한 엔드포인트 보안 전문성 보유
- 보안 운영 노하우를 통한 가시성 제공

알약 5.1 제품 특장점

알약 5.1 특장점

알약 5.1은 악성코드가 침투하기 이전에 사전 차단하고, 유입된 경우에도 강력한 탐지력으로 악성코드를 퇴치합니다.
또한 알약의 철저한 지원체계는 누구보다 빠르게 악성코드에 대응하고 있습니다.

01 빈틈없는 사전 방역

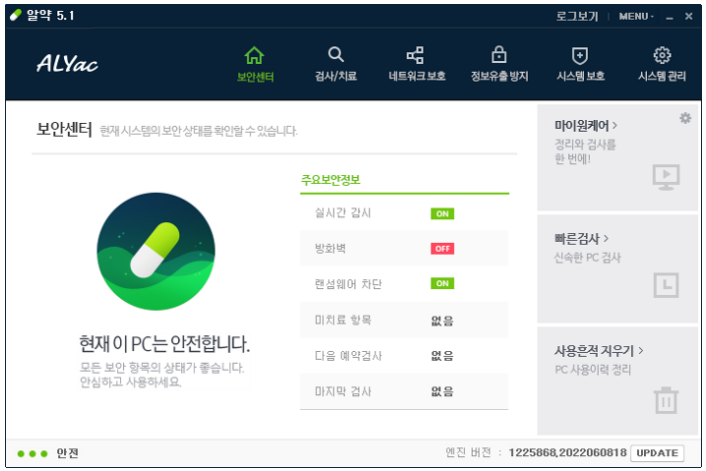
- 매체 제어 기능을 통한 자료 유출 및 악성코드 침투 사전 차단
- 파일 암호화 사전 차단, 랜섬웨어 차단 기능
- 행위 기반 엔진으로 의심스러운 행위를 탐지하여 알려지지 않은 위협 차단
- 스마트 DB 기능을 통한 엔진 경량화 및 검사 속도 성능 최적화

02 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

03 효율적인 통합 관리

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



ALYAC 5.1

주요 기능

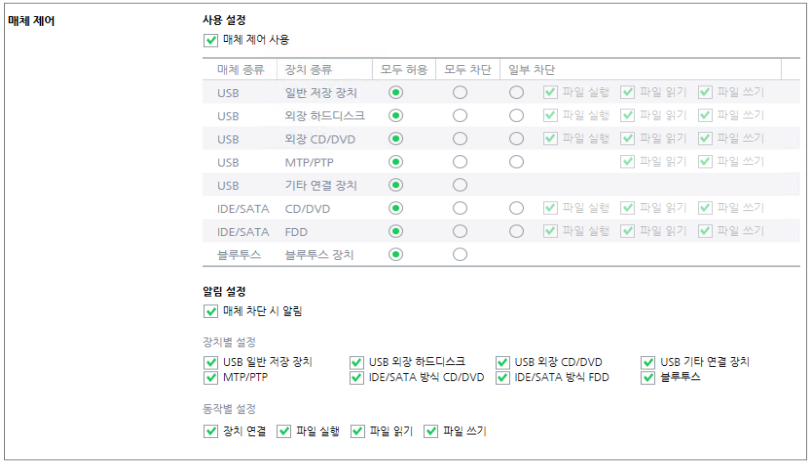
주요기능 1. 빈틈없는 사전방역_매체제어

알약은 다양한 휴대용 저장 매체의 접근 및 사용을 차단하여 내부의 중요 정보를 보호할 수 있습니다.

ESTsecurity 알약 5.1

- 사용자/그룹 별 **매체제어 정책 설정 기능 기본 제공**
- 다양한 휴대용 저장 매체(USB 기반 장치, IDE/SATA 장치, 블루투스 장치)의 **접근 및 사용을 제어 가능**

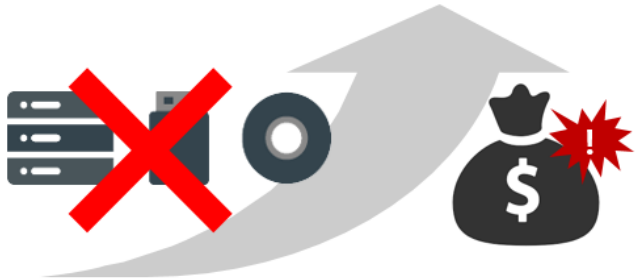
  → 매체의 연결을 포함, 파일 실행/쓰기/읽기 등 특정 동작을 차단



A社 백신

- Internet Security : 매체제어 미포함 된 보편적

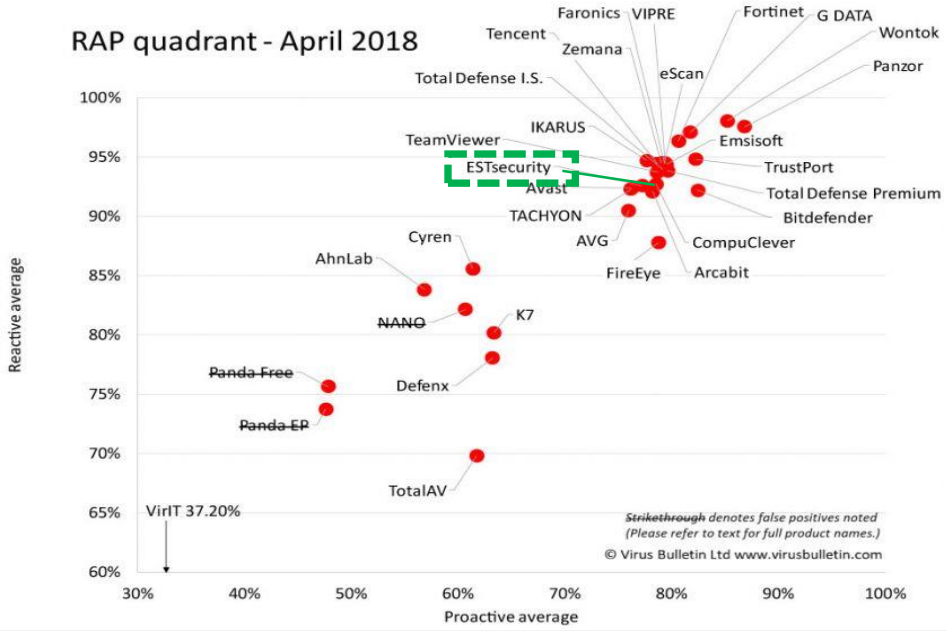
  → Endpoint Security : 매체제어 기능 추가 된 (금액 추가)



주요 기능

주요기능 2. 빈틈없는 사전방역_ 휴리스틱 검사

알약은 세계 보안 인증 테스트에서 휴리스틱 검사와 새로운 악성코드 탐지에 대한 우수성 검증 했습니다.



RAP(Reactive Detection and Proactive Detection) **Test**

- Reactive Detection : 유포된 샘플의 대응 능력, 수집 및 진단용 DB화 능력
- Proactive Detection : 휴리스틱, 제네릭 기술을 사용한 사전 방역 능력

구 분	대응능력 Reactive detection	사전방역 Proactive detection
ESTsecurity	93.8 %	77.2 %
A社	83.7 %	56.8 %

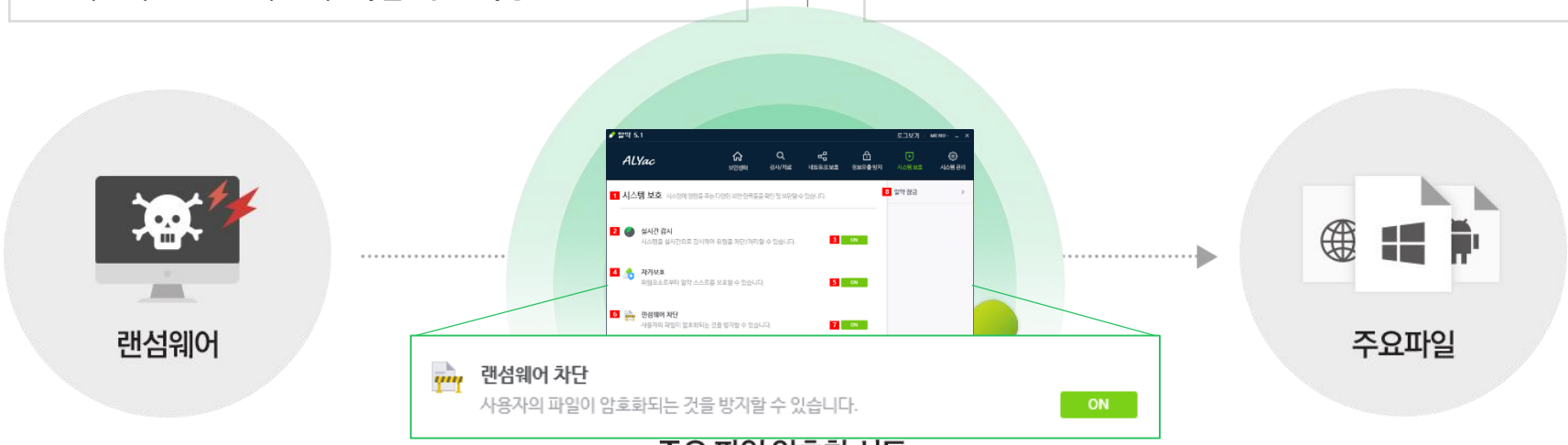
주요 기능

주요기능 3. 빈틈없는 사전방역_ 랜섬웨어 차단 / 복구

랜섬웨어 의심 행위를 사전에 탐지하고 차단하여 사용자의 파일이 암호되는 것을 방지합니다.

- 알려지지 않은 변종 랜섬웨어 위협 발생 시 백업 및 복구가 가능합니다.

ESTsecurity 알약 5.1	A社 백신
▪ 알려지지 않은 변종의 경우 트랩 폴더 생성 후 트랩 폴더 내 파일 변조 시도 시 차단 ▪ 파일 변조 동작을 감시하여 변조 시작 시점에 파일을 백업하고 실행 차단 후 **파일 복원 가능**	▪ 알려지지 않은 변종의 경우 지정된 폴더에 한해 부분 방어 가능 ▪ 랜섬웨어 감염 시 원본 파일로 **복원 불가**



주요 파일 암호화 시도
동작 감지 및 차단

주요 기능

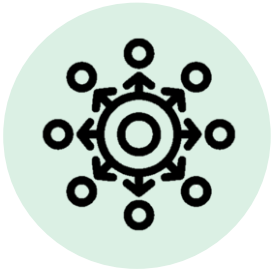
주요기능 4. 빈틈없는 사전방역_ 유해 트래픽 / 사이트 차단

사용자가 네트워크로 접근할 수 있는 유해한 사이트를 차단하거나 네트워크로 전파될 수 있는 악성 행위들을 차단/탐지합니다.

방화벽

Host F/W 을 이용한 네트워크 침입 및 전파 차단

- 실행 중인 모든 프로그램의 통신 상태를 사용자에게 알려 사용자가 모르는 사이에 통신을 시도하는 프로세스에 대한 정보를 제공하고 불필요한 프로그램이 통신을 시도하면 강제로 해제 강제로 해제



네트워크 침입차단

행위기반 침입 차단 을 이용한 네트워크 공격 차단

- IP 스푸핑 : 변조된 IP 주소가 포함된 패킷을 탐지
- MAC 스푸핑 : 변조된 MAC 주소가 포함된 패킷을 탐지
- ARP 스푸핑 : ARP 응답 패킷의 MAC 주소 변조를 탐지

유해사이트차단

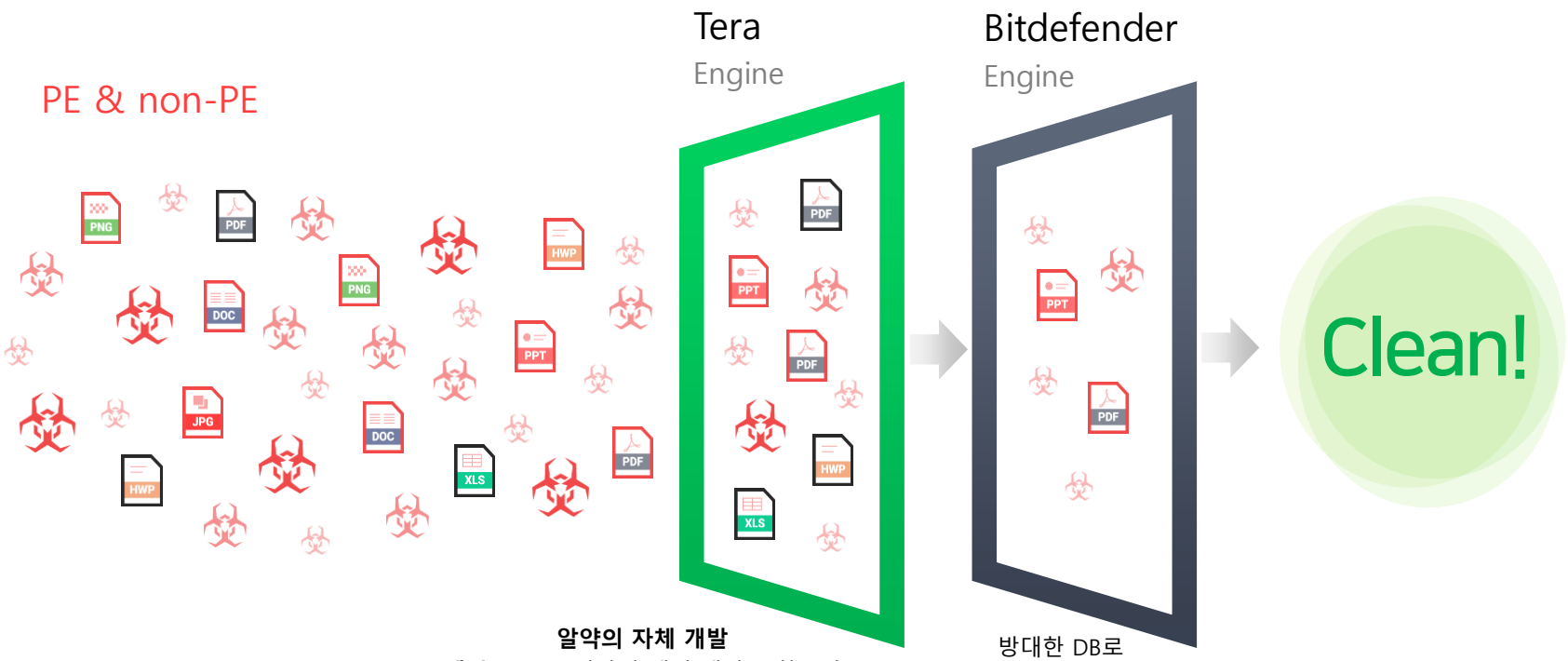
DB 를 이용한 유해사이트 접근 차단

- 악성,피싱,파밍 등 사용자에게 유해한 접근을 차단
- 사용자가 직접 설정한 사이트 허용/차단 목록 관리 침입차단 or T.I 인텔리전스 자체 유해 사이트 DB 를 활용

주요 기능

주요기능 5. 강력한 백신 엔진_ Dual 엔진

국제 인증을 통해 검증 받은 듀얼 엔진을 통해 강력한 악성코드 탐지
전세계에서 광범위하게 수집되는 해외 위협요소 DB와 국내 최대의 사용자를 기반으로 구축된 국내 위협요소 DB를 통한 포괄적 탐지



알약의 자체 개발
엔진 으로 10년간의 엔진 개발 노하우와
DB 분석 팀의 패턴 업데이트를 통해
악성코드를 빠르고 정확하게 탐지

방대한 DB로
전세계 악성코드에 대응하며
알려지지 않은 악성코드를 탐지하는
사전 방역 능력 우수

주요 기능

주요기능 6. 강력한 백신 엔진_국제 인증을 통해 검증 받은 엔진

VB100 인증 Virus Bulletin

전 세계적인 악성코드 목록인 WildList에 대한 100% 검출 및 오탐지 0% 조건 충족 시 부여하는 세계 3대 국제보안인증

- 2013.08 : Windows 7
- 2013.10 : Windows Server 2008
- 2013.12 : Windows 8.1
- 2014.04 : Windows 7
- 2014.08 : Windows 8 Professional
- 2014.10 : Windows Server 2008 R2
- 2014.12 : Windows 7
- 2015.14 : Windows 8.1
- 2015.16 : Windows Server 2012
- 2015.18 : Windows 7
- 2015.10 : Windows Sever 2008 R2
- 2015.12 : Windows 10
- 2016.04 : Windows 8.1
- 2016.06 : Windows Server 2012
- 2016.08 : Windows 10
- 2016.12 : Windows Server 2016
- 2017.04 : Windows 7, 10
- 2017.10 : Windows 7, 10
- 2017.12 : Windows 7, 10
- 2018.02 : Windows 7, 10
- 2018.04 : Windows 7, 10
- 2018.06 : Windows 7, 10
- 2018.10 : Windows 7, 10
- 2018.12 : Windows 7, 10
- 2019.02 : Windows 7, 10
- 2019.04 : Windows 7, 10
- 2019.06 : Windows 7, 10
- 2019.08 : Windows 7, 10

CheckMark 인증 Westcoast labs

Virus Bulletin 100% Award, ICSA와 더불어 세계 3대 국제보안인증으로 정보보호 제품의 효율성에 대한 품질을 테스트

- 2011.07 : Windows 7
- 2012.08 : Windows 7
- 2013.12 : Windows 7
- 2014.01 : Windows 7
- 2014.02 : Windows 7
- 2014.03 : Windows 7
- 2014.09 : Windows 7
- 2014.10 : Windows 7
- 2015.11 : Windows 7
- 2016.01 : Windows 8

▶ 알약의 VB100 인증 최근 테스트 결과

구분	2018.12	2019.02	2019.04	2019.06	2019.08	2019.10
WildList Detection	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
False Positive rate	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%
Diversity Test rate	100.00%	100.00%	99.06%	99.90%	99.79%	100.00%

주요 기능

주요기능 7. 강력한 백신 엔진_ AIS + A.I 신속한 분석 대응

Threat Inside

의심파일

1. 신종, 변종 악성코드 탐지

2. 의심 파일 정보 분석 서버 전송

악성파일

정상파일

3. 분석 및 진단 결과 확인

4. 악성코드 치료, 위협 대응

ALYac Intelligence Scan(AIS)

알약 듀얼 엔진에 존재하지 않는 악성코드 정보에 대해서 고도의 클라우드 서버 시스템을 사용하여 신종 악성코드, 변종 악성코드 발견 시에도 신속한 대응과 악성코드 위협 분석이 가능

A.I. + 전문가 분석

알약에서 행위 기반 차단이나 랜섬웨어 차단 기능을 통해 실행 차단된 의심 파일들을 AI 엔진 서버로 전송하여 **상세 분석을 진행하고 악성 여부를 확정하며 알려지지 않은 악성코드에 빠르게 대응**

Unkown 영역 대한 신속한 대응

ALYac Intelligence Scan(AIS)

(듀얼엔진에 존재하지 않는 미탐지 파일 전송)

분석

(A.I. + ESRC 전문 인력을 통한 상세 분석)

업데이트 자동화

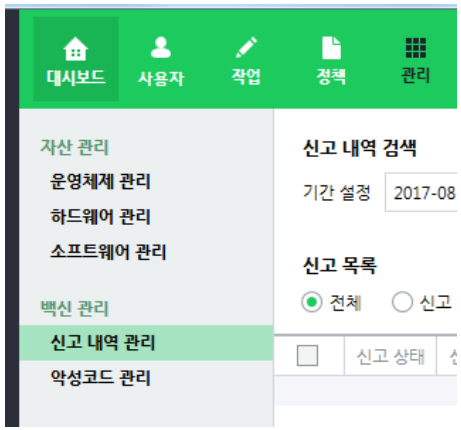
(자동 전송되어 분석을 마친 파일을 DB에 적용)

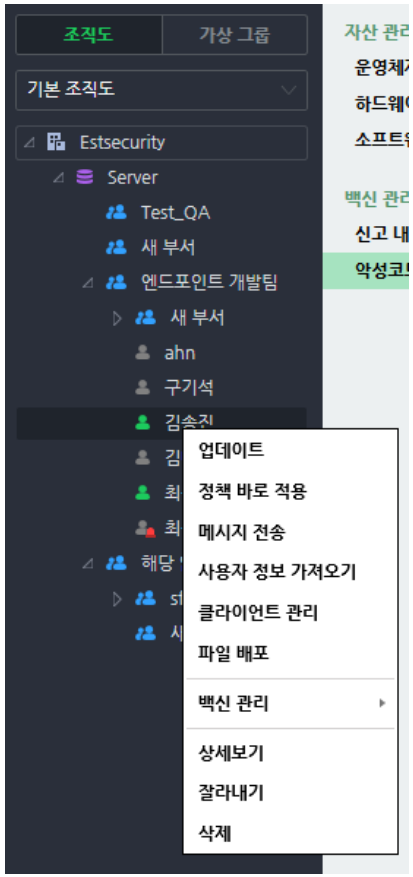
주요 기능

주요기능 8. 효율적인 통합 관리_ ASM

ASM(중앙관리솔루션) 연동을 통해 백신, 자산, 취약점 등 보안 기능 통합 관리 및 대응이 가능합니다.

ASM





직관적이고 차별화된 사용성

통합 에이전트를 통한 클라이언트 일괄 관리

- 실행, 업데이트, 수집, 로그, 사용자/서버 정보 관리 가능

손쉬운 시스템 관리

- ASM 전체 시스템을 컨트롤할 수 있는 서버 매니지먼트 제공
- ASM 장애 시 외부 지원 없이 원클릭 장애 복구 가능

조직도 연동 기능

- 조직도 항시 노출 및 주요 메뉴와의 연동 기능 제공
- 조직도를 통한 주요 작업 명령 및 실시간 제품 설치 상태 확인

메시지 및 알림 기능

- 주요 보안 위험 및 ASM 사용 관련 실시간 알림 기능 제공
- 사용자와 메시지 송수신 가능

주요 기능

주요기능 9. 효율적인 통합 관리_ 통합 솔루션 라인 확장

별도의 서버 구축 없이 라이선스 구매만으로 ESTsecurity의 엔드포인트 제품을 활성화 하고

단일 에이전트를 통해 복수의 보안 서비스를 일괄 관리하며 사내 보안 수준을 강화할 수 있습니다.

ASM 5

라이선스 추가

백신

확실한 위협을 탐지/차단

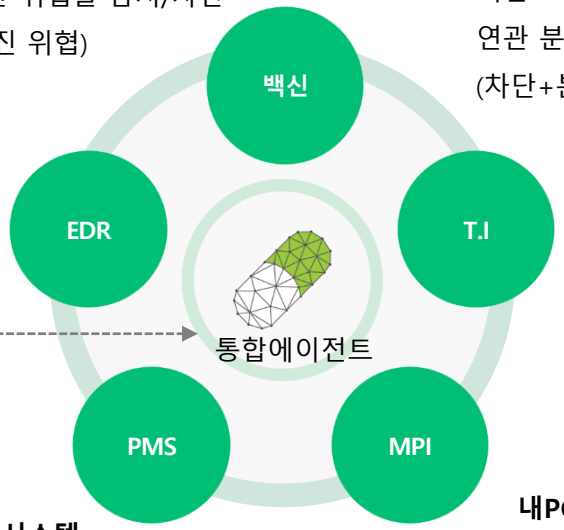
(알려진 위협)

인텔리전스

의심스러운 위협을

연관 분석된 증거들로 해석

(차단+분석+대응)



EDR

의심스러운 위협을 탐지

(알려지지 않은 위협)

패치관리시스템

OS/SW 패치업데이트 관리

내PC지키미

취약점 점검(일괄, 자동 조치)

3. 기술 지원

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 체계를 유지하여,

국내에 특화된 APT 공격과 랜섬웨어 등 각종 위협에 가장 빠르게 대응하고 있습니다.

ESRC 이스트시큐리티 대응센터 + 커널개발 & 분석 + A.I. Solution 개발

신종 위협 대응

고객지원 서비스

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

고객지원 서비스

전문 기술 인력이 체계적이고 신속한 고객 지원 서비스를 제공합니다.

신고하기/ e-mail 상담
(2시간 이내 회신)

전문 기술 인력의 전화 상담

야간 및 공휴일, 주간
핫라인 운영

PC 원격지원 서비스

대규모 사이트 전담 인력 배정 및
정기 방문 점검 서비스 제공

제품 교육 서비스 제공

- 구매문의 : 02-3470-2970
- 고객센터 : 1544-9744
- 홈페이지 : https://www.estsecurity.com/enterprise/product/alyac-enterprise

래퍼런스

공 공

외 1,000여 기관

금 융

기 업

외 5,000여 기업

교 육

한양대학교, 한국과학기술원, 서울대학교 병원, 고려대학교, 연세대학교, 순천향대학교, 성균관대학교 포항공과대학교, 한국교원대학교, 중앙대학교, 단국대학교, 부산대학교, 숙명여자대학교 홍익대학교, 경희대학교, 경북대학교, 전남대학교, 인하대학교, 경상대학교, 전북대학교 여주대학교, 영남대학교, 한국전통문화대학교, 한서대학교, 진주보건대학교, 한세대학교, 가톨릭대학교, 한국산업기술대학교, 수성대학교, 부천대학교, 경인교육대학교

제품 사양

HW 설치환경

		CPU	RAM	HDD
서버	최소	알약 운영을 위한 서버의 HW 권장 사양은 고객사 환경에 따라 차이가 있습니다. 별도의 상담을 통해 내용 확인이 가능합니다.		
	권장			
관리콘솔	최소	Intel Dual Core 1Ghz	1GB	1GB 이상 여유공간
	권장	Intel Dual Core 2Ghz	2GB	2GB 이상 여유공간
에이전트	최소	Intel Dual Core 1Ghz	512MB	800MB 이상 여유공간
	권장	Intel Dual Core 2Ghz	1GB	1GB 이상 여유공간

SW 설치환경

	OS	비고
관리 서버	Windows Server 2008 R2 SP1 (KB4490628 및 KB4474419 설치) Windows Server 2012 (R2 포함) / 2016 / 2019 CentOS 6.x 이상	
에이전트	Microsoft Windows 7 SP1(KB4490628 및 KB4474419 설치) Microsoft Windows 8 / 8.1 / 10 / 11 (모든 OS 32bit, 64bit 지원)	

ESTsecurity

감사합니다.

Make world more secure with A.I.