AhnLab

Privacy Management

More security,
More freedom

플랫폼 기반의 더 강력한 개인정보 유출 방지

표준제안서

AhnLab

CONTENTS

AhnLab
Privacy Management

AhnLab

01
제안 배경

개인정보 유출 사고 원인 및 대응 현황

사회적·제도적 변화

개인정보보호법의 요구 사항

개인정보에 특화된 보안 솔루션의 필요성 대두

개인정보 유출 사고 원인 및 대응 현황

잇따른 개인정보 유출 사고에도 불구하고 여전히 많은 기업들이 개인정보 유출 방지를 위한 적절한 대비책을 마련하지 못하고 있습니다.

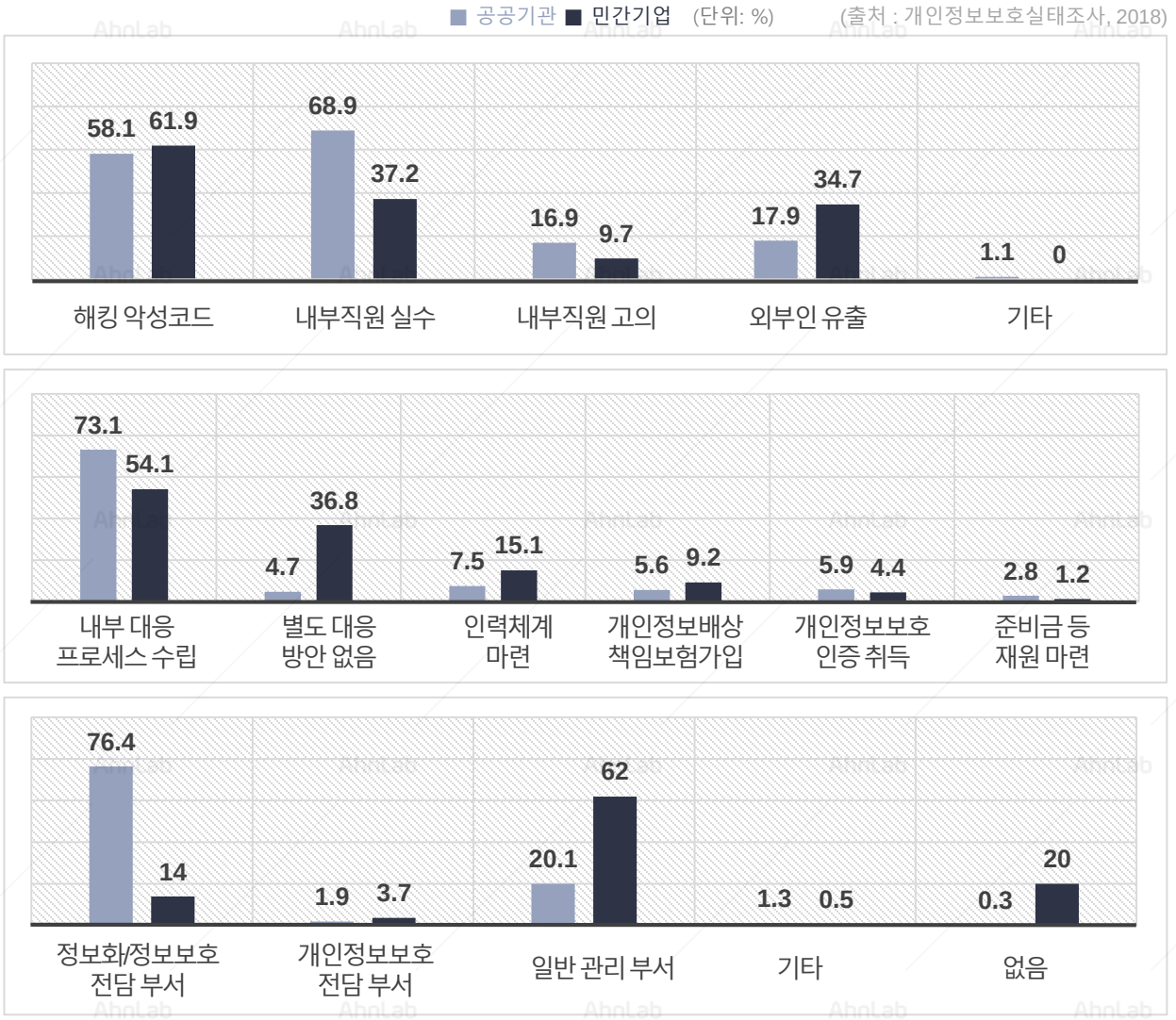
개인정보 유출 사고 원인 인식

- 공공기관: '해킹, 악성코드 등 외부 공격 ' 1순위
- 민간 기업 : '내부직원 실수로 유출' 1순위
- 전반적으로 휴먼에러에 의한 내부 직원 유출이 대다수

개인정보 유출 사고 대비 대응

- 민간 기업의 개인정보 관리 부서 현황
  - 36.8% 별도 대응 방안 없음
  - 82% 전담 부서 부재
  - 62%가 일반 관리 부서에서 담당
  - 20%는 개인정보 관리 부서 없음

(출처 : 개인정보보호실태조사, 2018)



사회적·제도적 변화(1/2)

개인정보보호법 제정 이후에도 반복되는 개인정보 유출 사고로 '개인정보보호법 개정안' 시행되었습니다.

- 개인정보의 단순 '관리'를 넘어 단 **1건의 '유출'도 책임**, 개인정보 **유출 차단 의무화**
- 매년 **위반 조건 및 처벌 강화**로 위반 사례와 과징금 증가

개인정보 유출에 대한 기업 **처벌 및 책임 강화**

개인정보가 유출 되지 않도록 사전에 탐지 및 차단하는 것이 핵심!!

2011년 개인정보보호법 제정/시행 → 2014년 주민등록번호 수집 금지(법정주의) → 2016년 주민등록번호 암호화 의무, 법적·징벌적 손해배상제 도입/처벌 강화 → 2017년 개인정보유출 신고 기준 1만→1천 건으로 조정(강화)

종류	성격	처분요건
과징금	법 위반	[제34조의2] 주민등록번호 유출 및 안전 조치 위반 시 **5억 원 이하 과징금**
과태료	법 위반	[제75조] 과태료 부과 대상 규정 위반 시 **5천~1천만 원 과태료**
시정조치	법 위반	[제64조] 침해・피해 발생 우려 시(과태료 규정 외) **침해행위 중지, 개인정보 처리의 정지, 보호 조치 명령**
징계권고	법 위반	[제65조] 개인정보 관계 법규 위반에 책임이 있는 자의 **징계 등 신분상 조치 권고**
공표	법 위반	[제66조] 위반이 심하여 공공에 경종 필요 시 명단을 전국에 보급하는 **일간신문에 게재하여 공표**
개선권고	위반 아님	[제61조] 개인정보 보호실태 개선 필요 시 **시정 조치 및 처리 실태 개선 권고**
손해배상	법 위반	[제39조의2]정보주체자에게 **300만원 이하 손해액 보상**

 # 2017년 최초 과징금 부과

총 49만 명 개인정보 유출한 여행사 접근통제・암호화 등 기술/관리적 안전조치 위반

① **과징금 3억원 부과**

② **CEO/CPO 특별 교육 및 책임에 상응하는 징계 권고**

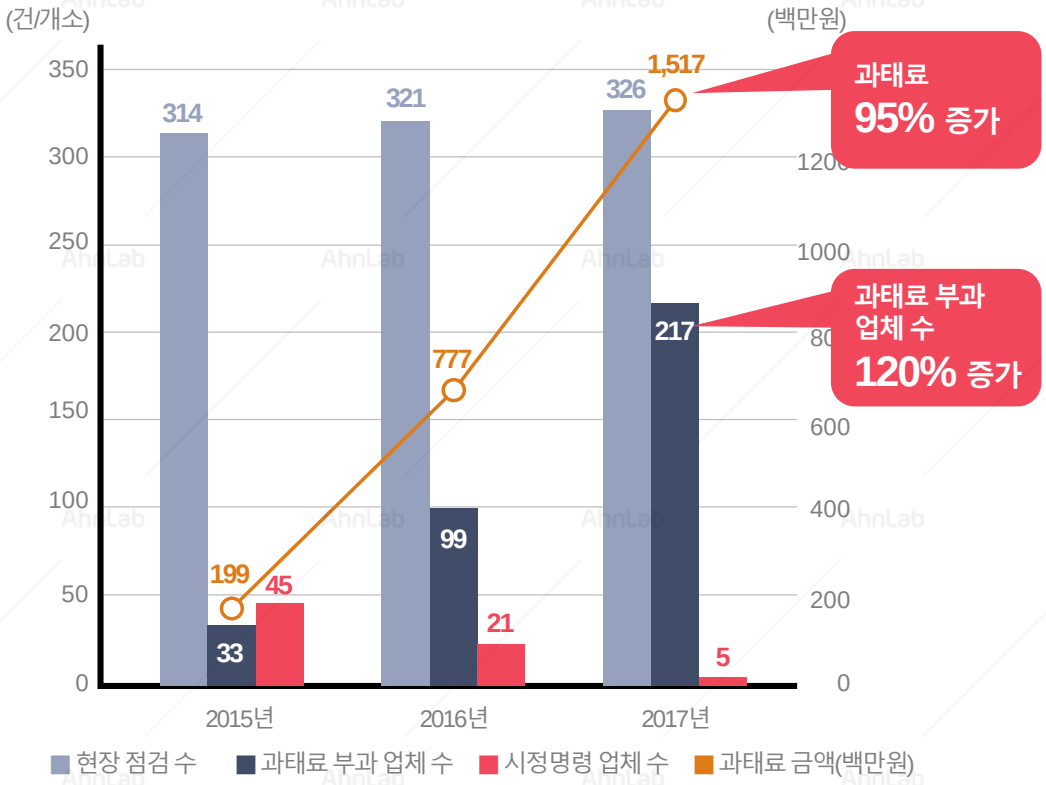
③ **주민번호/개인정보 미파기에 따른 추가 과태료 부과**

사회적·제도적 변화(2/2)

최근 기업의 개인정보 관리 현황에 대한 점검과 그에 따른 처벌이 강화되고 있습니다.

- 행정안전부에서 **개인정보 실태점검 실시**, 공공기관에서 380만 민간사업자까지 확대 (개인정보보호법 제63조, 개인정보 보호법 시행령 제60조)
  → 공공, 생활·물류, 보건·의료, 교육 등 6대 산업 분야와 통신판매업, SNS 사업자 등 온라인 서비스 분야
- 기술적, 관리적 보호 조치 여부 확인 - **위반 기업/기관에 대해 과태료 부과, 시정명령, 개선권고** (개인정보보호법 제34조의 2, 제 61조, 64~66조, 제75조)

최근 3년 점검, 과태료부과 및 시정명령 추이



최근 3년 월별 점검 분야

시기	2015년	2016년	2017년
1월	공공기관	보건・복지	산업・물류
2월	보건・복지	산업・물류	공공기관
3월	공공・교육수탁사	공공기관	시설・문화
4월	교육	의료・통신수탁사	교육
5월	수탁사(정부합동)	교육	보건・복지
6월	방송・통신	공공・교육수탁사	협회・단체 등
7월	협회・단체	중개・생활・임대	산업・물류
8월	중개・생활・임대	방송・통신	중개・생활・임대
9월	통신・산업수탁사	생활・산업수탁사	공공기관
10월	시설・문화	시설・문화	교육
11월	공공기관	공공기관	산업・물류
12월	정보・문화수탁사	문화・금융수탁사 산업・문류	보건・복지

(출처 : 행정안전부, 2018.04)

개인정보보호법의 요구 사항

개인정보보호법 및 개정안은 기술적/관리적/물리적 보호조치 수립에 대한 요구 사항을 강력하게 명시하고 있습니다.

제29조(안전조치의무)

개인정보처리자는 **개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록** 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 **안전성 확보에 필요한 기술적·관리적 및 물리적 조치**를 하여야 한다.

제24조(고유식별정보의 처리 제한)

개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 **그 고유식별정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록** 대통령령으로 정하는 바에 따라 **암호화 등 안전성 확보에 필요한 조치**를 하여야 한다.

처리하는 개인정보의 종류・규모, 종업원 수 및 매출액 규모 등을 고려하여 개인정보처리자가 **안전성 확보에 필요한 조치**를 하였는지에 관하여 정기적으로 조사하여야 한다
행정안전부장관은 전문기관으로 하여금 조사를 수행하게 할 수 있다.

제 36조(개인정보의 정정.삭제)

개인정보처리자가 제2항에 따라 **개인정보를 삭제할 때에는 복구 또는 재생되지 아니하도록 조치**하여야 한다.

개인정보보호법

개인정보에 특화된 보안 솔루션의 필요성 대두

개인정보 관련 컴플라이언스의 까다로운 기술적 보호 조치 요구사항을 준수하기 위해 개인정보에 특화된 보안 솔루션이 필요하게 되었습니다.

- 실제 개인정보가 취급되는 엔드포인트단에서의 개인정보 파일에 대한 가시성 확보 및 관리 필요
- 전사 엔드포인트에 대한 개인정보보호 인식•제고 및 기술적, 관리적 보호 체계 구현 필요
- 개인정보보호법의 기술적 조치 요구 사항은 DRM / DLP 솔루션만으로는 대응에 한계

엔드포인트 개인정보 관리에 특화된 솔루션의 필요성 대두

개인정보 수집 증가

- 기업의 개인정보 수집의 확대 • 일반화
- 마케팅을 위한 개인정보 무분별 활용

엔드포인트에서의 개인정보 관리 문제

- 개인정보보호 중요성 인식 부족
- 사용자 별 다른 PC환경에 대한 고려 필요

기존 엔드포인트 솔루션의 한계 (DRM / DLP)

- **DRM**
  - 암호화 요건만 충족
  - 개인정보 현황 파악 • 추적 불가
- **DLP**
  - 파일 단위로 추적 지원
  - 암호화와 개인정보 현황 파악 불가

02

AhnLab Privacy Management

제품 개요

특장점

도입효과

AhnLab

AhnLab Privacy Management

AhnLab Privacy Management는 개인정보에 특화된 개인정보 유출 방지 솔루션으로, 엔드포인트에 존재하는 개인정보에 대한 점검•관리는 물론 개인정보가 포함된 파일의 유출이 의심되는 행위를 원천 차단합니다. 플랫폼 기반의 더욱 편리하고 강력한 개인정보 보호를 통해 컴플라이언스 부담을 해소하고 대외 신뢰도를 향상시킬 수 있습니다.

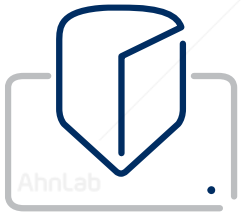
관리부터 유출 차단까지, 더 강력한 개인정보 보호

AhnLab Privacy Management

개인정보 라이프사이클 중심의 관리 및 조치

개인정보 생성 시점부터 점검 및 관리

다양한 경로를 통한
개인정보 유출 탐지 및 차단



개인정보보호법 기술적 보호조치 구현

AhnLab EPP 기반의
엔드포인트 통합 관리 체계 구현

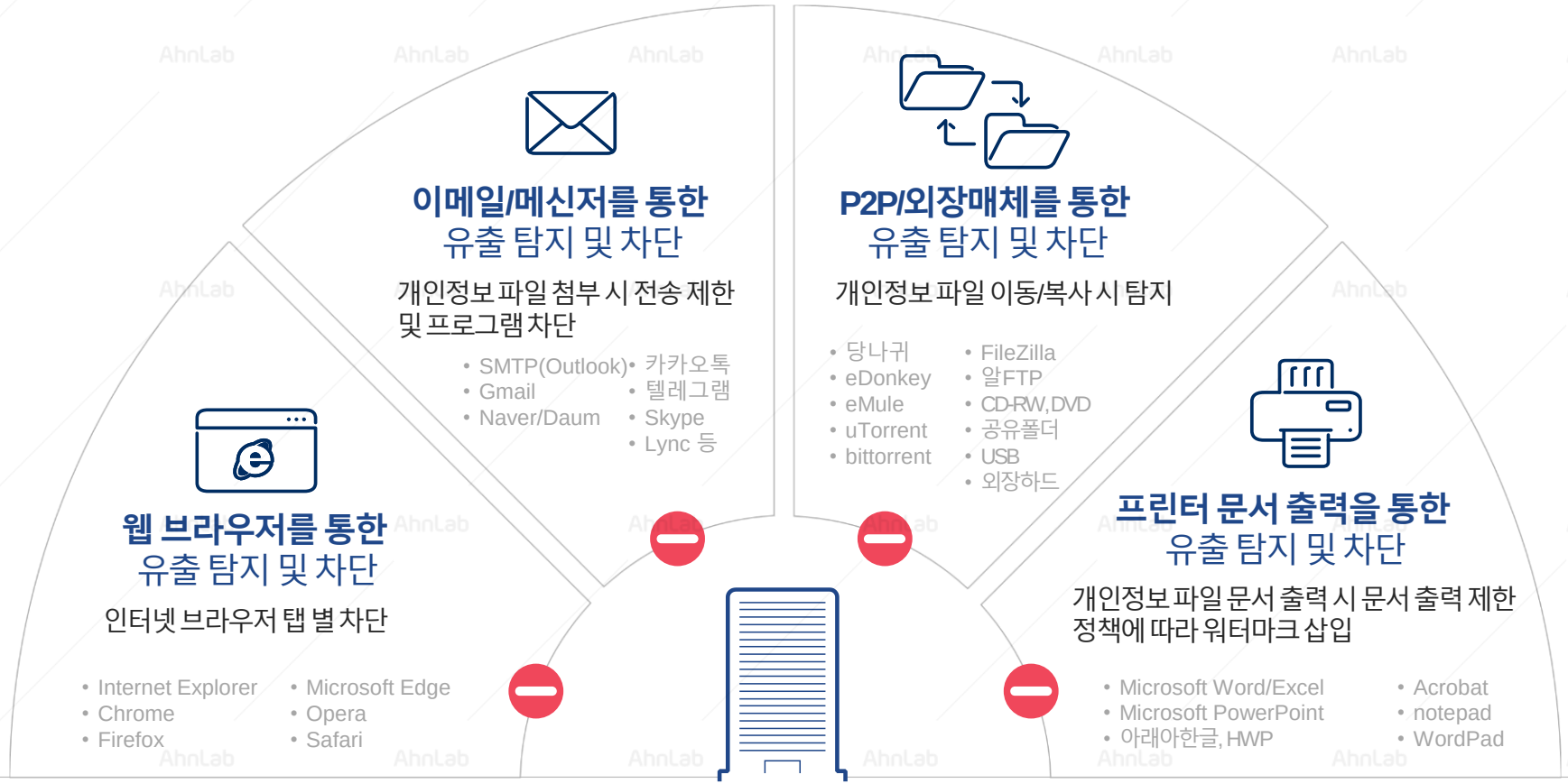
개인정보부터 백신, 패치까지
통합 관리 및 조치

단일 에이전트,단일 관리 콘솔의
탁월한 운영 및 관리 편의성

특장점(1/5) - 개인정보 유출 경로 차단

AhnLab Privacy Management는 엔드포인트의 다양한 경로를 통해 개인정보가 포함된 파일이 유출되는 것을 효과적으로 탐지 및 차단합니다.

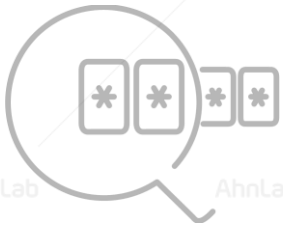
다양한 경로에서 개인정보가 포함된 파일의 유출을 시도하는 시점에 즉각 대응함으로써
안전한 기업 환경 구축에 기여합니다.



특장점(2/5) - 개인정보 관리 및 조치 강화

AhnLab Privacy Management는 실시간 검색, 자동 격리 등 다양한 기능을 제공해 개인정보 현황 파악은 물론, 유출 탐지 및 차단 등 더욱 강력한 대응 조치가 가능합니다.

기존 개인정보 관리 솔루션



검색-암호화

구분	주요 기능
관리콘솔	정책/명령/보고서/로그/모니터링
에이전트	Neuron Scan 및 수동 검색/실시간 감시/조치

플랫폼 기반의 더 강력한 개인정보 유출 방지

AhnLab Privacy Management

- 웹 메일, SMTP 메일 프로그램 유출 탐지/조치
- 웹사이트 유출 탐지/조치
- Messenger 프로그램 유출 탐지/조치
- FTP 프로그램, 공유폴더 유출 탐지/조치
- P2P 프로그램 유출 탐지/조치
- 프린터 유출 탐지/제한적 조치
- CD-RW, DVD, USB, 외장하드 유출 탐지/제한적 조치
- 사용자 지정 프로그램 유출 탐지/조치
- 프린터 워터마크 적용
- 문서 파일 관리/관리 키워드 기준 검색 및 조치

구분	주요 기능
관리콘솔	정책/명령/보고서/로그/모니터링
에이전트	Neuron Scan 및 수동 검색/실시간 감시/조치
	웹 메일 /웹 사이트 / Messenger / SMTP / FTP / P2P / 프린터 / CD-RW, DVD / USB/ 외장하드, / 사용자 지정 프로그램 유출 탐지 및 제한적 조치

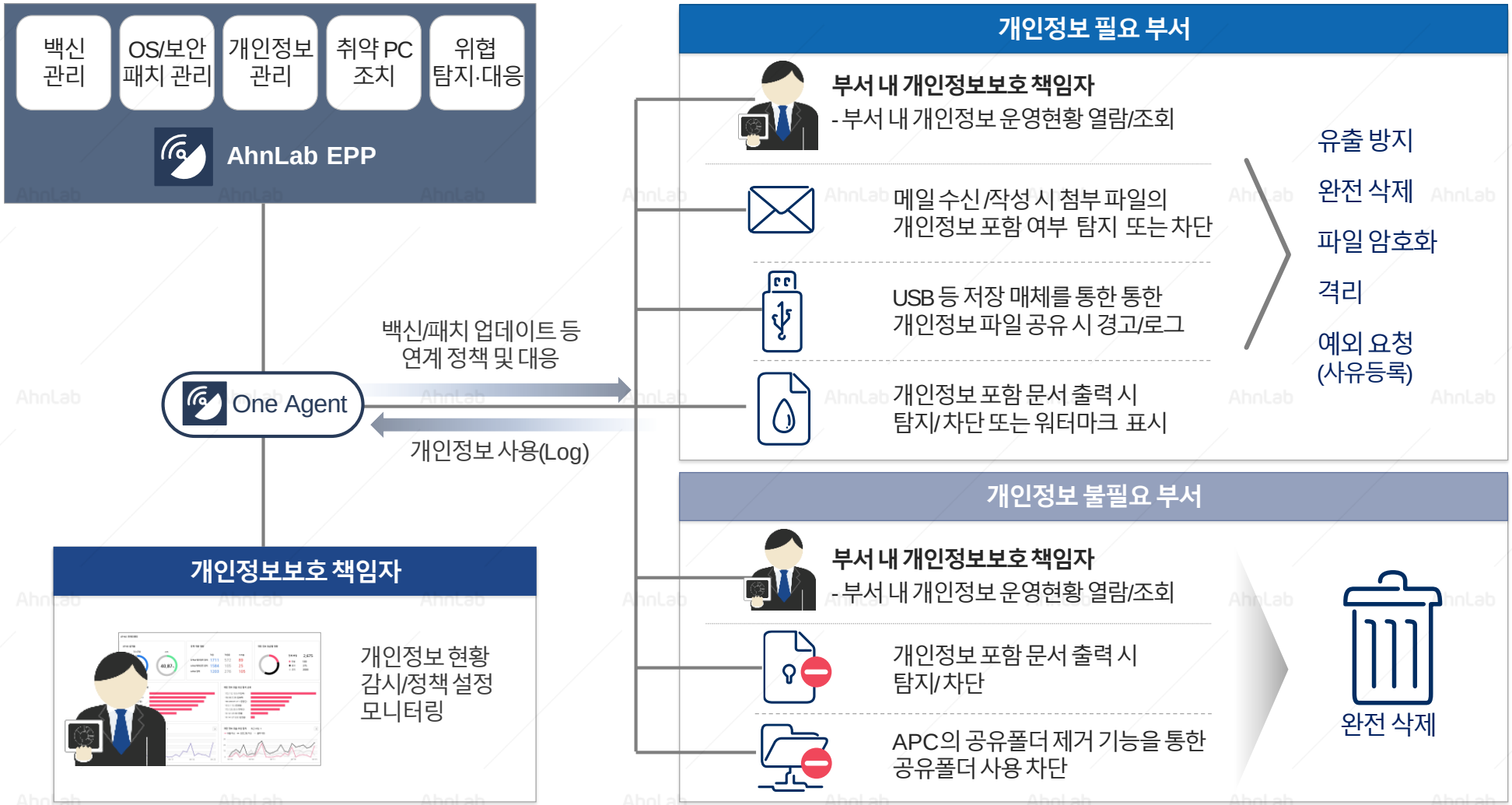
특장점(3/5) - 플랫폼 기반의 효율적인 기술적 조치

엔드포인트 보안 플랫폼 AhnLab EPP를 기반으로 개인정보 관리는 물론, 백신•패치 관리 및 취약 시스템 조치까지 개인정보보호 관련 규정에 명시된 기술적 보호 조치를 더욱 쉽고 효율적으로 준수할 수 있습니다.

- 단일 매니지먼트, 단일 에이전트를 통한 설치•운영•관리 부담 최소화
- 플러그인(plug-in) 방식 - 라이선스 적용만으로 간편하게 구축 및 다수의 보안 제품과 통합 운영 가능

특장점(4/5) - 유연한 정책 설정 및 운영 효율성

AhnLab EPP의 단일 매니지먼트•단일 에이전트를 기반으로 효율적인 정책 적용 및 보안 운영이 가능하며, 연계 정책을 통해 더욱 강력한 조치 및 엔드포인트 위협 대응을 제공합니다.

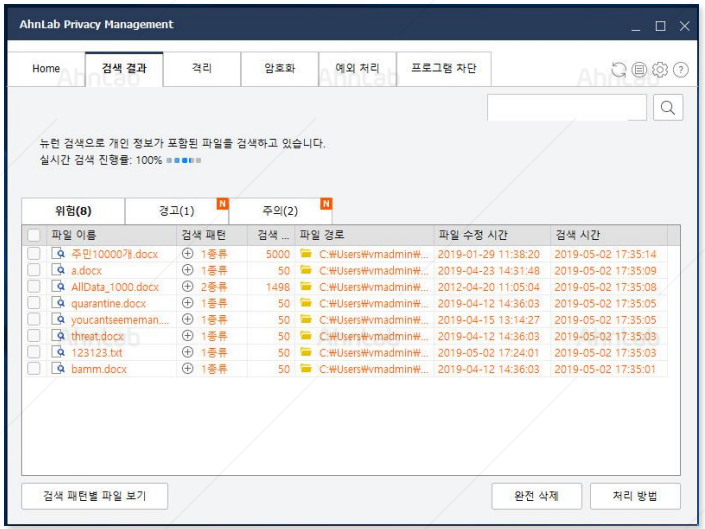


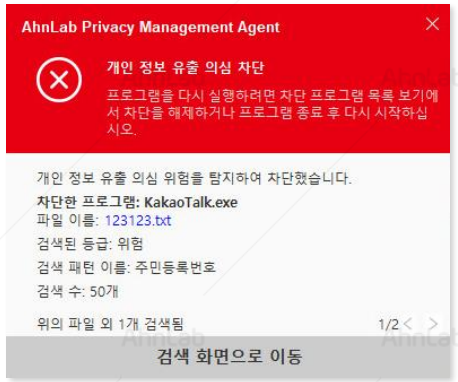
특장점(5/5) - 사용자 편의성

AhnLab Privacy Management는 개인정보 이용 및 보호에 최적화된 직관적인 사용자 화면(UI)을 통해 임직원의 업무 편의성 향상과 함께 보안 인식 제고에 기여합니다.

- 암호 입력 절차 자동화
- 사용자 거부감 최소화
- 직관적인 관리 상태/유출 현황 확인 가능
- 처리 현황 상세 정보 제공
- 패턴별 현황 제공

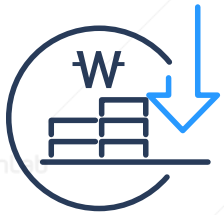
검색 현황 확인 및 검출된 문서, 개인정보 패턴에 따른 사용자 조치 가능





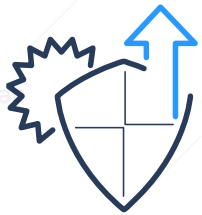
도입효과

더 강력한 개인정보 보호 및 기업 환경에 최적화된 능동적 보안



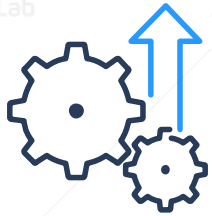
비용 절감 효과

- 비용 부담이 없는 Linux OS, DB 지원을 통해 관리 비용 절감 효과
- 통합 관리를 통한 운영 인력 비용 절감 및 관리 효율성 극대화
- 편리한 통합 운영을 통한 개별 솔루션 도입 효과 극대화
- 유연한 구성 방식을 통해 서버 확장에 따른 관리 부담 최소화
- 개인정보 유출 방지를 통한 컴플라이언스 관련 비용 부담 최소화 및 대외 신뢰도 향상



위협 대응력 향상

- AhnLab EPP 기반의 연계 정책 및 조치를 통한 강력한 위협 대응
- SIEM/통합 로그 분석 시스템 연동을 통한 보안 관제 효과 증대
- EDR 연동을 통한 엔드포인트 위협 수집 및 가시성 확보로 보안 위협 대응력 향상



업무 생산성 향상

- 중앙 제어(통합 콘솔)를 통한 신속한 사고 대응 및 업무 부담 최소화
- 중앙 관리에 필요한 시스템 설치•운영 • 관리 부담 해소
- 안전한 보안 환경 구축으로 업무 연속성•생산성 향상

03
주요 기능

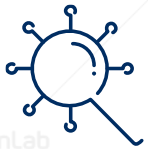
주요 기능

AhnLab Privacy Management는 개인정보에 최적화된 문서 변환, 뉴런 검색 등 독자적인 기능으로 엔드포인트 상의 개인정보를 확인하고 다양한 경로를 통한 유출 시도를 원천 차단합니다.

실시간 검색, 자동 격리, 유출 차단, 문서 관리까지 강력한 개인정보 보호!

다양한 경로를 통한 개인정보 유출 탐지 및 조치

- 이메일(아웃룩/웹 메일), 문서 출력(프린터) 등 다양한 개인정보 유출 경로에 대한 탐지 및 조치
- 개인정보가 포함된 파일 첨부 시, 즉각 해당 애플리케이션 차단



뉴런 검색(Neuron Search™) 기술로 탐지 정확성 및 사용자 편의성 극대화

- 실시간 검색(Real Time Scan) 및 증분 검색의 융합을 통한 신속하고 정확한 개인정보 탐지 성능
- 사용자 패턴에 최적화된 '사람 중심'의 검색 기술로 업무 불편 최소화 및 사용 편의성 향상

문서 변환 기술을 통해 다양한 문서 파일 내의 개인정보 검출

- 다양한 포맷의 문서를 txt로 변환하여 개인정보 포함 여부 탐지
- 운영체제(OS)별 방대한 문서 포맷 및 변환 기술 보유
- 관리키워드를 통한 문서파일 관리 기능

직관적인 UI를 통한 개인정보 현황 확인 및 가시성 확보

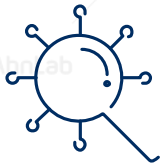
- 알기 쉬운 수치 표현으로 개인정보 파일 현황 확인 및 유출 탐지 건 수 확인
- 개인정보 탐지 및 유출 차단에 대해 색상으로 구분한 팝업창 알림 제공

상세 기능(1) 개인정보 유출 탐지

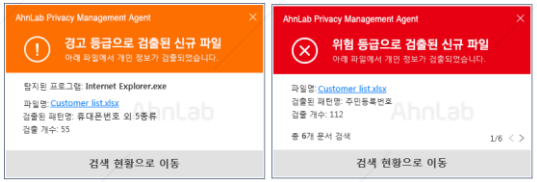
개인정보가 포함된 파일을 실시간 모니터링 하여 기업의 정책에 따라 완전삭제, 자동 격리 등의 조치가 가능합니다.
웹이나 메일, 메신저 등을 통해 개인정보가 포함된 파일 첨부 시(유출 시도 시), 실시간으로 탐지 및 차단하며, 관리자 알림을 제공해 개인정보 유출을 사전에 방지합니다.

개인정보가
포함된 문서

뉴런(Neuron) 검색
실시간/증분검색



개인정보가
포함된 문서

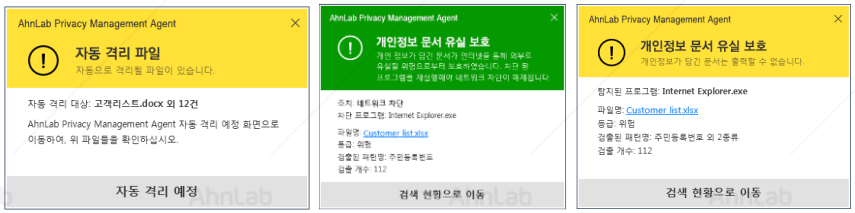


개인정보 탐지 알림 및 조치

- 파일 암호화
- 완전삭제
- 격리
- 예외 요청/처리

정책에 따른 처리

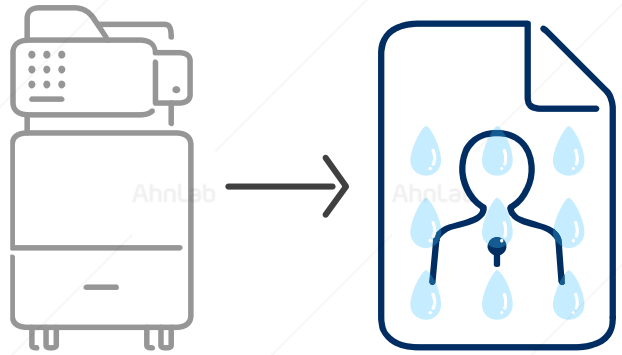
개인정보 파일 탐지/유출 탐지 및
차단 현황 제공



차단 정책 적용 시,
자동격리, 네트워크 차단, 프린터 출력 차단 및 워터마크 적용

상세 기능(2) 출력물 관리

개인정보가 포함된 파일의 프린터 출력을 제한해 개인정보 유출을 방지합니다. 프린터 출력 시 워터마크 삽입으로 개인정보 관리 및 추적이 가능합니다.



워터마크 표시 항목

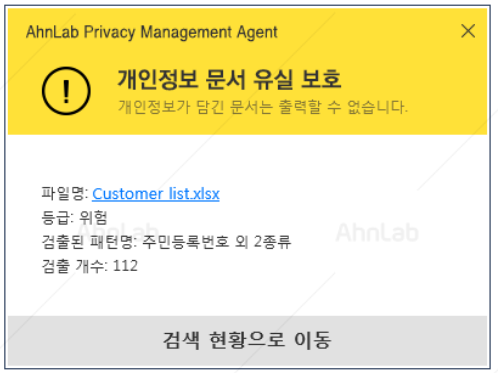
사용자 이름, 컴퓨터 이름, IP 주소, 파일 출력 번호, 사용자 입력 텍스트

워터마크 위치

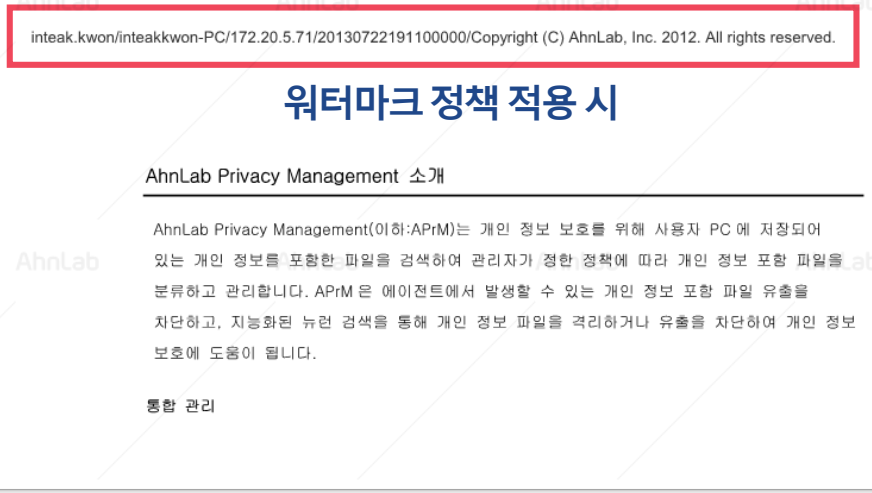
상단 / 하단 왼쪽 / 가운데 / 오른쪽

지원 프로그램

Microsoft Word, Excel, Power Point, 아래아 한글 notepad, wordpad, Acrobat Reader, Outlook



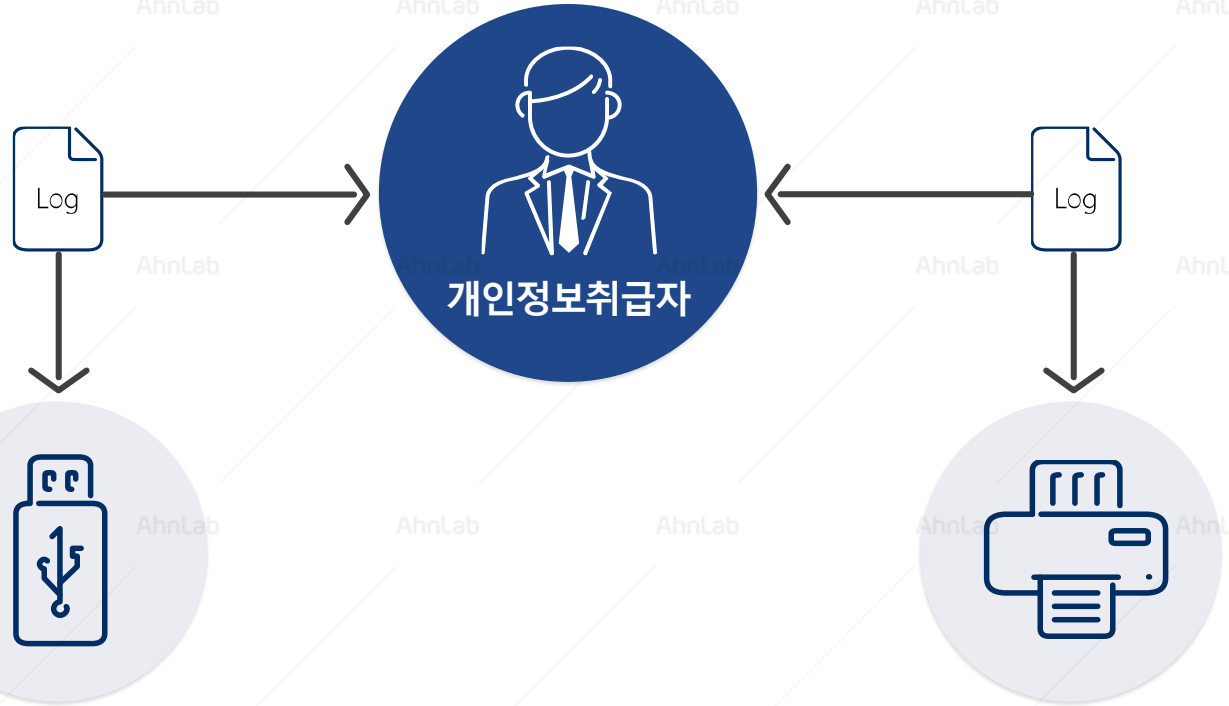
프린터 출력 방지 정책 적용 시



워터마크 정책 적용 시

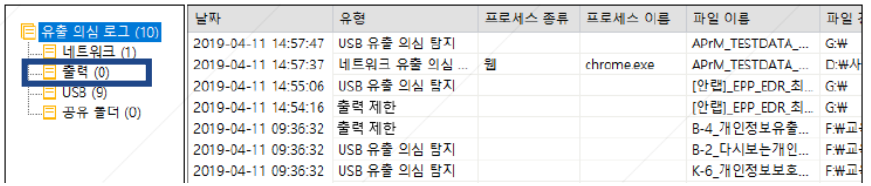
상세 기능(3) 개인정보취급자(실무자) 기능

상세한 로그 정보를 제공해 실무자(개인정보취급자)가 직접 내용을 확인하고 해당 개인정보 파일을 관리할 수 있습니다.



유출 행위가 시도된 경로 및 조치 내역 확인 가능

프린트 출력 제한 및 유출 탐지에 대한 로그 확인 가능



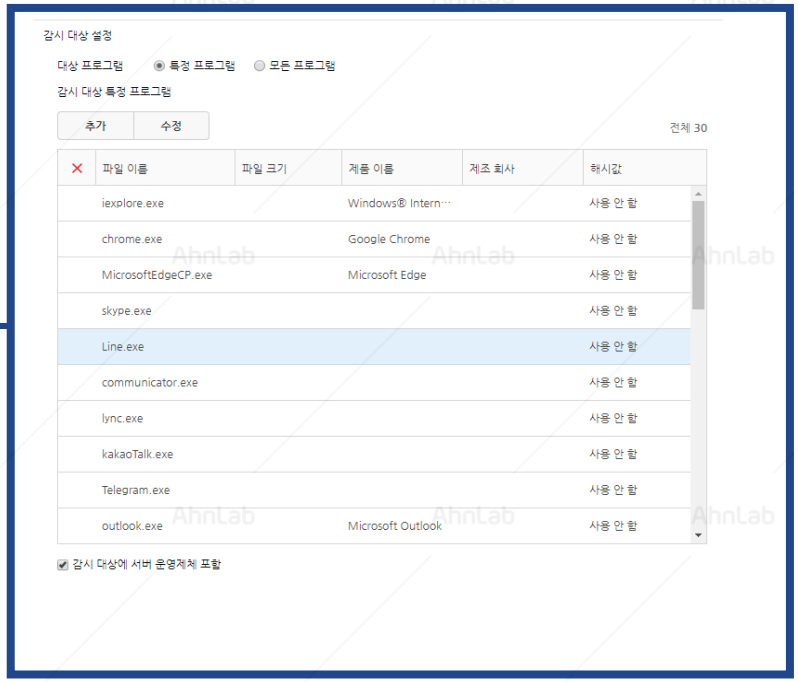
상세 기능(5) 관리자 정책 설정 1

기업의 내부 정책에 따라 프로그램에 대한 감시 대상 또는 예외 설정을 통해 유연하고 효과적인 개인정보 관리가 가능합니다.

특정 프로그램 감시

감시 할 프로그램 선택

- 네트워크 사용 시 감시 대상에 포함



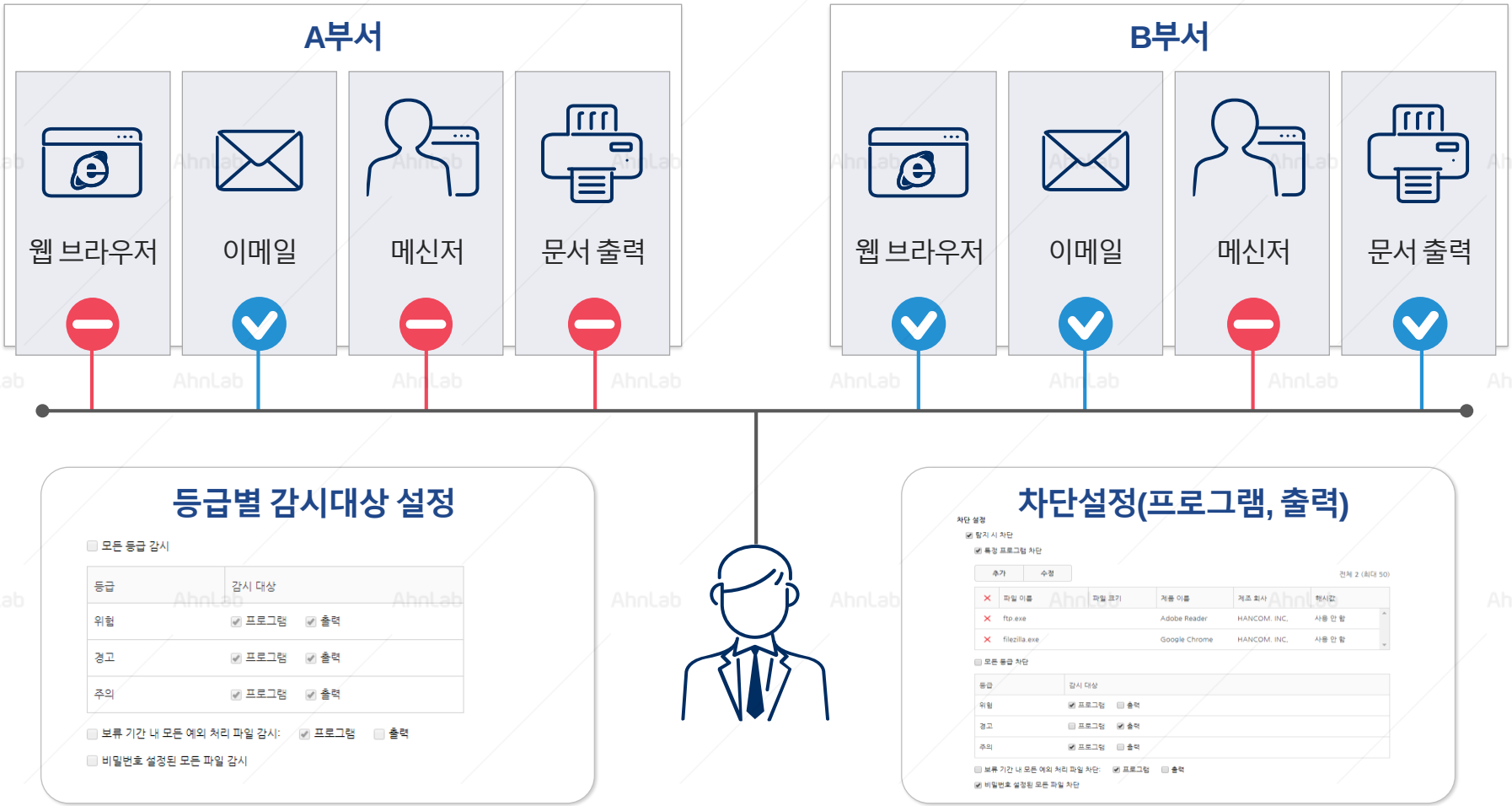
모든 프로그램 감시

선택 시 모든 프로그램 감시

- 감시에서 제외하고자 하는 예외 프로그램 지정

상세 기능(6) 관리자 정책 설정 2

각 실무 부서별 업무에 따라 특정 또는 모든 프로그램에 대해 감시 설정, 차단 설정 선택 적용 등 효율적인 정책 설정이 가능합니다.
또한 유출 시도가 탐지된 프로그램에 대해 네트워크 제한, 출력 제한 및 관리 등의 조치가 가능합니다.



04
도입 방식

AhnLab EPP 기반의 구축 및 운영

유연한 서버 구성을 통한 확장

운영 환경

AhnLab EPP 기반의 구축 및 운영

AhnLab Privacy Management는 모듈 방식으로 구성된 차세대 엔드포인트 플랫폼 AhnLab EPP를 통해 간편하게 구축 및 운영할 수 있으며, 필요 시 유연하게 확장할 수 있습니다.

- AhnLab EPP 모듈 구성: 로드 밸런서, 파일, 로그, DB

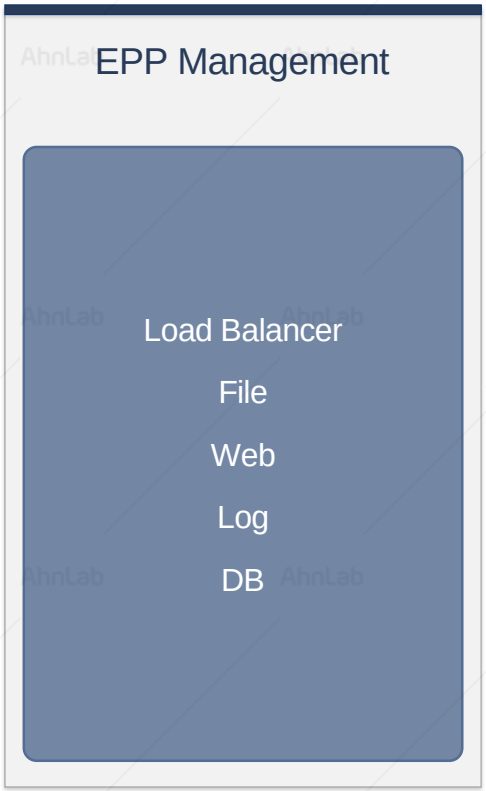
  * EDR 모듈은 EDR 사용 시에만 필요

유연한 서버 구성을 통한 확장

AhnLab EPP 기반으로 운영하는 AhnLab Privacy Management는 고객사 환경에 따라 시스템을 유연하게 구성할 수 있는 다양한 옵션을 제공합니다.

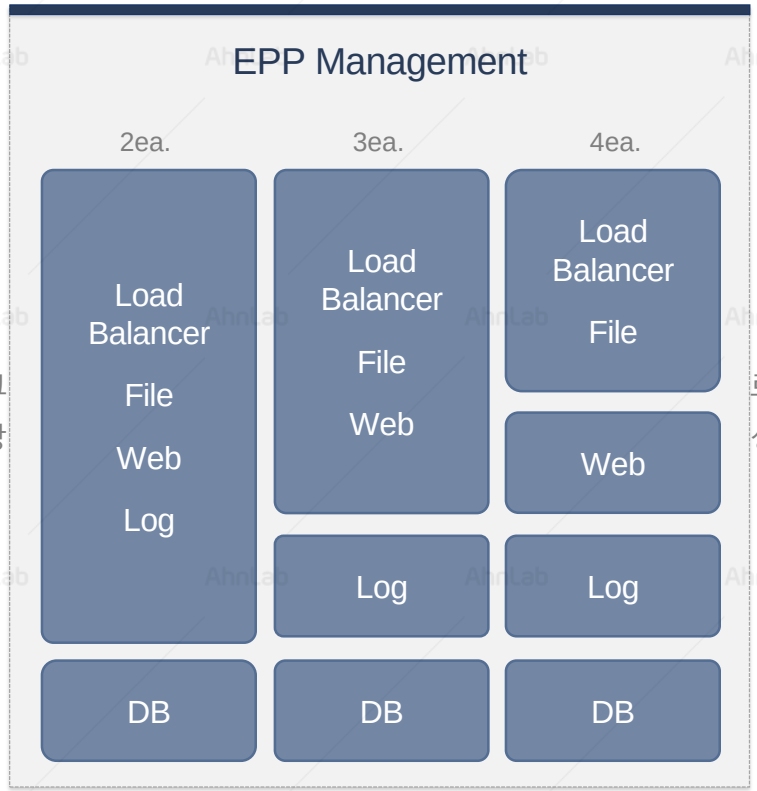
- 최적화된 초기 구축 비용 및 확장 편의성: 사용자 수, 데이터베이스 사용량 등 고객 환경에 따른 시스템 구성
- 에이전트 확대, DB 증가에 따라 모듈별 서버 확장 가능
- Load Balancer / File 서버의 경우 네트워크 별로 확장 구성 가능

구성 1. **올인원** (단일 장비)



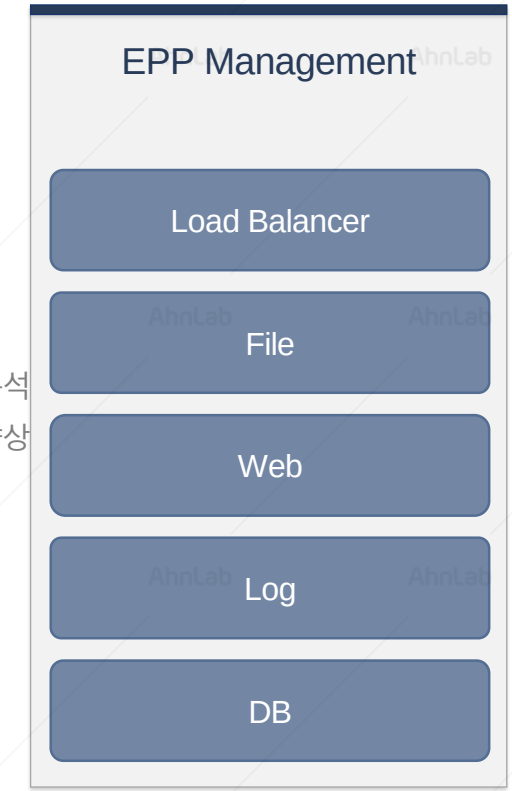
관리·로그
성능 향상

구성 2. **분리형** (개별 장비)



로그·분석
성능 향상

구성 3. **전체 독립형** (개별 장비)



운영 환경

AhnLab Privacy Management는 차세대 엔드포인트 보안 플랫폼 AhnLab EPP Management를 기반으로 효율적인 통합 관리를 제공합니다.

- AhnLab Privacy Management 에이전트 설치 환경

구분	상세 버전
운영체제	Windows XP SP3 / Vista / 7 / 8(8.1) / 10 Windows Server 2003 SP1 이상 (R2 포함) Windows Server 2008 / 2012 – 공통 사항: R2 포함 Windows Server 2016 / 2019 *상기 OS의 64bit 호환 모드 지원
지원 언어	한국어, 영어, 중국어(간체), 일본어

- 관리 콘솔(AhnLab EPP Management) 운영 환경

구분	상세 버전
웹 브라우저	Internet Explorer 11 이상 Chrome 최신 버전
지원 언어	한국어, 영어, 중국어(간체), 일본어

- 권장 서버 하드웨어 사양 (AhnLab EPP Management 설치 환경)

구분		관리 에이전트 수						
		최대 300개	최대 1,000개	최대 5,000개	최대 10,000개	최대 15,000개	최대 30,000개	최대 50,000개
CPU		4	4	8	16	16	16	16
메모리		32G	64G	64G	128G	192G	256G	384G
HDD	기본	500G	500G	1TB	1TB	1TB	1TB	2TB
	APM 사용 시	1TB	1TB	1TB	1TB	1TB	1TB	1TB

* APM 사용 시: HDD 2개 이상 물리적 분리 구성 필수, 에이전트와 서버간 네트워크 대역폭 최소 32mbps 이상 권장

별첨

1. 개인정보보호 솔루션 vs. 기존 엔드포인트 솔루션

개인정보보호 솔루션 vs. 기존 엔드포인트 솔루션 (1/3)

※ 별첨

DRM, DLP 솔루션만으로는 개인정보보호법 등에서 요구하는 기술적 보호 조치를 구현하는데 한계가 있습니다.

	AhnLab Privacy Management	DRM	DLP
주체	개인	회사	회사
정보	개인정보	회사의 저작권	회사자산유출 메일, 웹메일,메신저,외장매체
주요기능	✓ 개인정보 검색, 관리 키워드 검색 암호화, 완전삭제	암호화	유출방지 (Endpoint, Network)
암호화	파일 암호화	파일 접근 권한 통제 (후킹)	데이터 Rule 분석 (파일 모니터링)
개인정보 보호법 준수	✓ 개인정보보호법에서 요구하는 사항 준수	• 암호화 요건만 충족 • 개인정보 현황 파악 • 추적 불가	• 파일 단위로 추적 지원 • 암호화와 개인정보 현황 파악 불가
차별점	• 개인정보 파악/관리, 유출 방지 가능 • 개인정보보호법 요구 사항 준수 • 관리키워드를 통한 문서파일 관리 가능 • 실무자(개인정보 사용자) 업무 효율성 확보	• 모든 파일에 대한 관리, 암호화 제공 (DLP 유출 방지 기능 제공) • **'개인정보보호법'의 조치 조건 충족 불가**	

개인정보보호 솔루션 vs. 기존 엔드포인트 솔루션 (2/3)

※ 별첨

AhnLab Privacy Management는 **개인정보에 특화된 솔루션**으로, 개인정보를 효율적으로 관리 및 감시하고 개인정보의 유출을 사전에 방지합니다.

	AhnLab Privacy Management	DLP
대상	✓ 개인정보 한정 / 문서 종류 일부 제약	모든 문서
판별유무	개인정보 룰(rule), 관리 키워드 룰(문서파일관리)	Undefined된 문서에 대한 일반화된 룰 정의
엔진	AhnLab Privacy Management 전용 엔진	DLP 엔진
감시방식	파일 생성 시 개인정보 유무판별 *행위기반 탐지로 인해 탐지 범위가 넓음 (URL, 멀티 브라우저, SSL등의 제약 없음)	상시 패킷 모니터링 유사패턴 검출
룰 생성방식	실행 프로세스별 정형 파일포맷 감시	패킷 비정형 룰 감시
감시대상	원하는 프로세스만 감시 예) IE, 메신저 등 또는 All	모든 것을 차단 후 허용 예) 모든 프로세스 차단 등록된 프로세스만 허용
동작	감시/차단 (해당 세션 Block / 차단)	감시/차단 (해당 세션 Block / 차단)

*행위기반 데이터의 패킷 패턴을 보는 것이 아니라 개인 정보 파일에 접근하는 프로세스를 감시하는 형태로 탐지

개인정보보호 솔루션 vs. 기존 엔드포인트 솔루션 (3/3)

※ 별첨

개인정보보호법은 단순 암호화만 요구하는 것이 아니기 때문에 암호화 솔루션만으로는 개인정보보호법의 기술적 보호조치를 준수하기 어렵습니다.

개인정보보호에 특화된
AhnLab Privacy Management

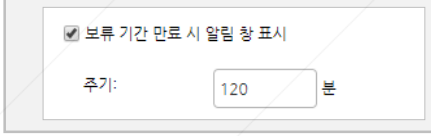
사용 기간, 용도가 맞는 경우에 한해서
'암호화'하여 보관

암호화 대상이 아닌 파일은
'완전삭제'

사용 기간을 입력하는 것과
일정 기간이 지나면 지워야 하는 것도 명시

<개인정보보호법 제30조>
명시 사항

단, 안내창 등이 불편한 경우를 대비하여 아래와 같이 보류창이 나타나지 않도록 정책 처리 가능



More security,
More freedom

㈜안랩
경기도 성남시 분당구 판교역로 220 (우)13493
대표전화 : 031-722-8000 | 구매문의 : 1588-3096 | 전용 상담전화 : 1577-9431 | 팩스 : 031-722-8901 | www.ahnlab.com

AhnLab
Privacy Management

AhnLab