보안 관리자를 위한 혁신적인 엔드포인트 보안 운영 전략

안랩 제품기획팀 **백민경 부장**

AhnLab

최근 유행하는 악성코드는?

AhnLab

랜섬웨어
(Ransomware)

채굴 악성코드
(Miner)

크립토 재킹
(Crypto Jacking)

공격기법 #1 워터링 홀

AhnLab

워터링 홀
Watering Hole

접근대상이 비교적 명확한 웹사이트를 공격

접속페이지 / 악의적 링크를 통한 악성코드 감염

국가기관 및 회사 기밀자료 수집/유출 /원격접속을 통한 위해행위

공격기법 #2 스피어 피싱

AhnLab

스피어 피싱
Spear Phishing

공격자가 의도한 대상에게
이메일 송부

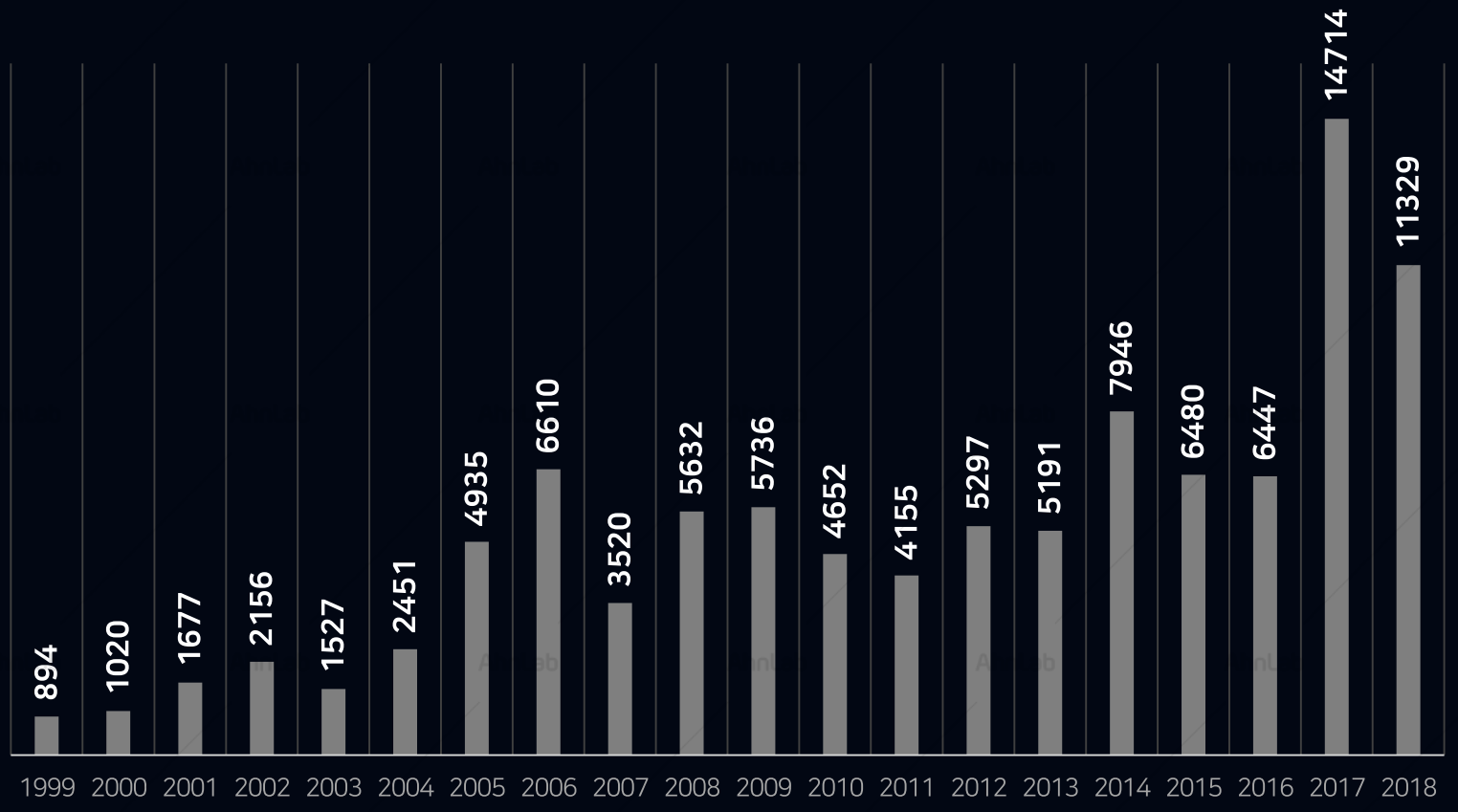
첨부파일 / 악의적 링크를 통한
악성코드 감염

국가기관 및 회사 기밀자료 수집/유출
/원격접속을 통한 위해행위

공격기법 #3 취약점 공격

AhnLab

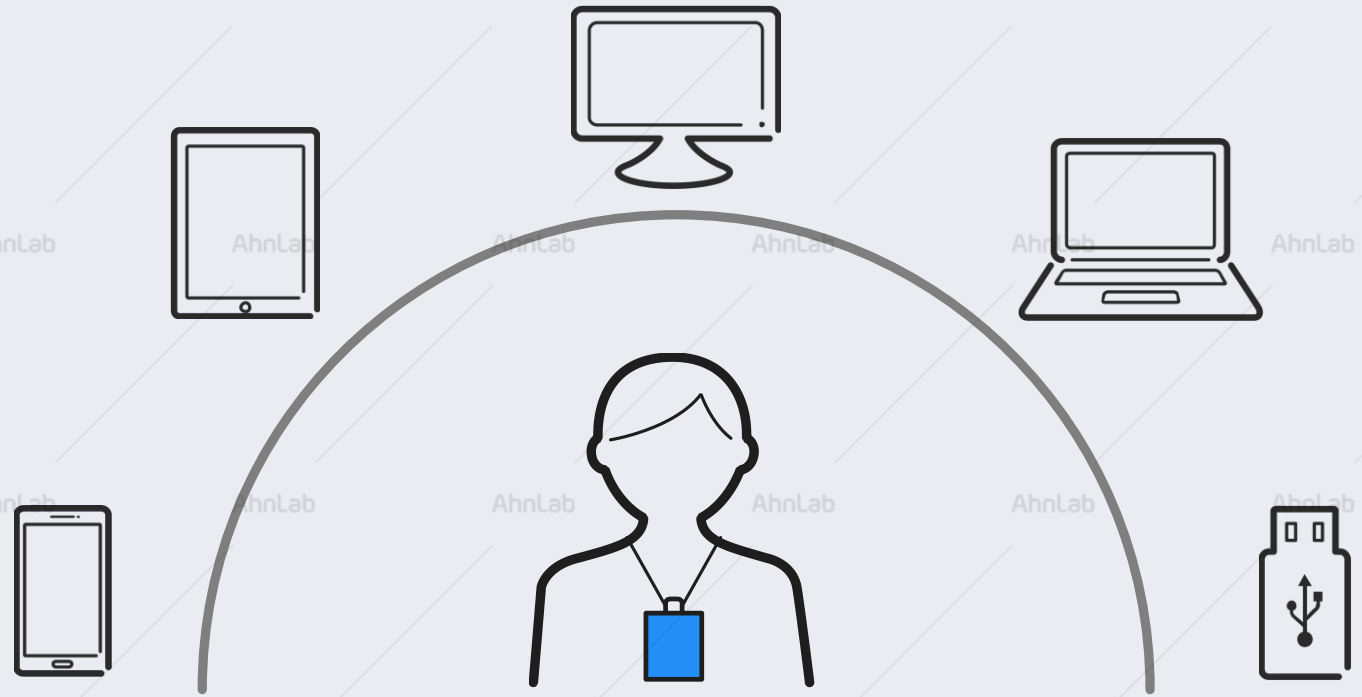
10만개 이상의 취약점



출처 : https://www.cvedetails.com

Endpoint 업무 환경

AhnLab

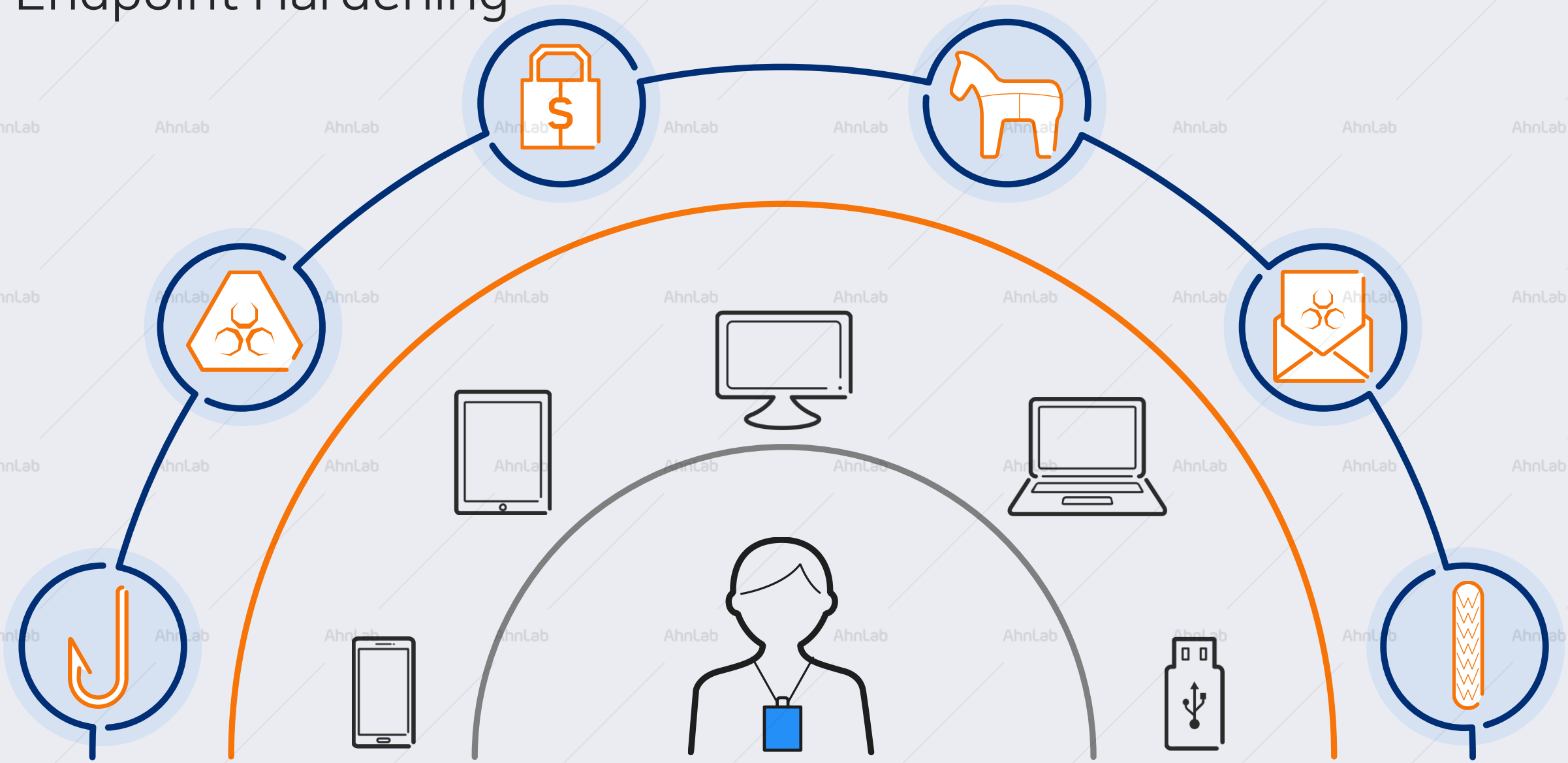


Endpoint 노리는 위협

AhnLab

Endpoint Hardening

AhnLab

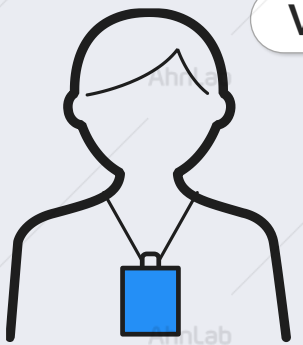


Endpoint Hardening

AhnLab

- AntiVirus
- Sandbox 분석
- 랜섬웨어 예방
- APT 대응

V3 EDR MDS



위협 탐지/대응

정보유출 예방/관리

위협 예방

보안 솔루션 관리

- 망분리
- DRM/DLP
- 매체제어
- 개인정보보호

V3 APrM

- 사용자 인증
- 취약점 패치
- 취약점 관리
- 개인방화벽/IPS

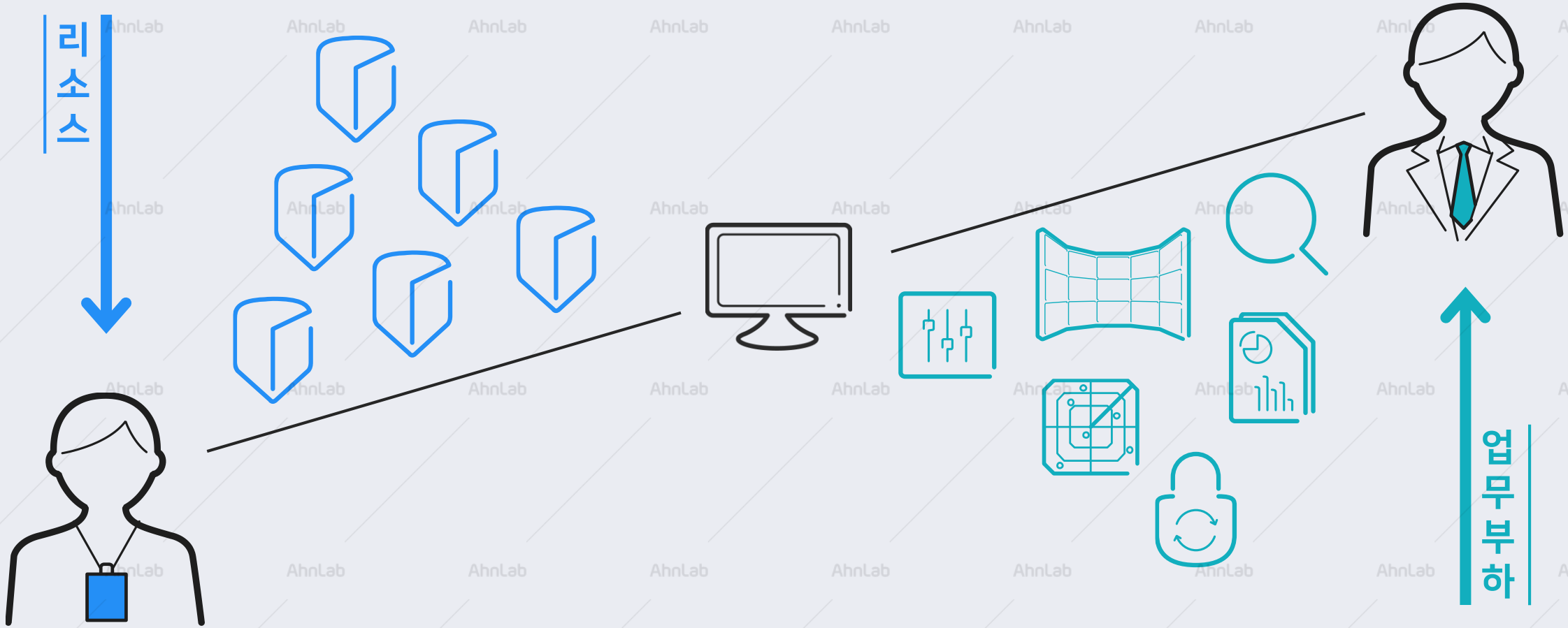
APM V3 MDS 내PC지키미

- Mgt. Console
- Web Console
- 통합로그관리

APC EMS EPP

Endpoint Hardening

AhnLab



최적의 Endpoint Hardening 방안

AhnLab

EPP

APC

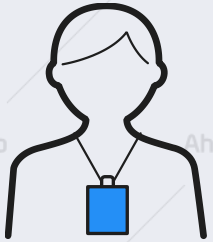
EMS

보안 솔루션 관리

위협 예방

위협 탐지/대응

정보유출 예방/관리



내PC지키미

APM

APrM

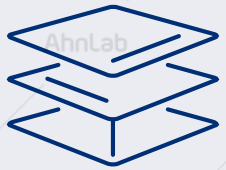
V3

EDR

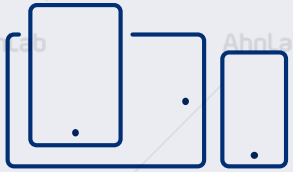
MDS

Transformation to the Platform

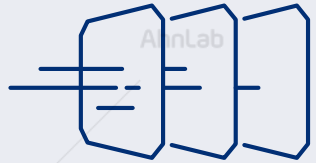
AhnLab



Multi-OS Platform



Multi-Devices

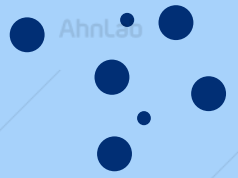


Multi-Layered Security Functions

Single Management

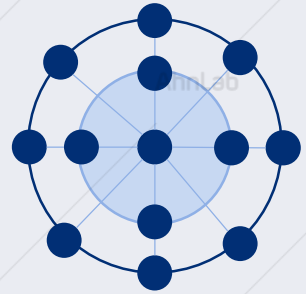
Endpoint Protection Platform

고객 지향형 보안
Customer Oriented Security



Usability / 사용성
Integrity / 안정성
Visibility / 가시성
Compatibility / 호환성

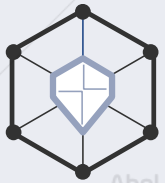
고객 주도형 보안
Customer Driven Security



Transformation to the Platform

AhnLab

플랫폼 기반의 통합적이고 **체계적인 위협 관리·대응 필요**



다수의 보안 솔루션의 수많은 정보를
신속하게 탐지 및 대응

정확한 정보 전달을 통한
보안 관리자 반응·대응 시간 최소화

보안 솔루션 및 기능의 유기적인 연계를 통한
엔드포인트 위협 가시성 확보

✓최신 악성코드 제어 및 대응의 한계
✓다양한 위협 경로 모니터링의 한계
✓위협 고도화에 따른 분석·대응 속도 지연

다양한 유입 경로
의심·악성 파일 유입

사회공학기법,
표적/지능형 공격

OS/SW 제로데이 취약점 이용
신·변종 악성코드 증가

AhnLab EPP Management

AhnLab

AhnLab EDR

AhnLab

행위 정보 탐지·분석을 통한
엔드포인트 가시성 확보 및 대응

AhnLab EDR

간편한 구축, 손쉬운 운영,
더 강력한 위협 대응

언제 조직 내부로 침입한 파일인가?

파일이 유입된 이후 실행된 적이 있는가?

어떻게 악성코드에 감염됐는가?

동일한 파일이 얼마나 많은 시스템에 존재하는가?

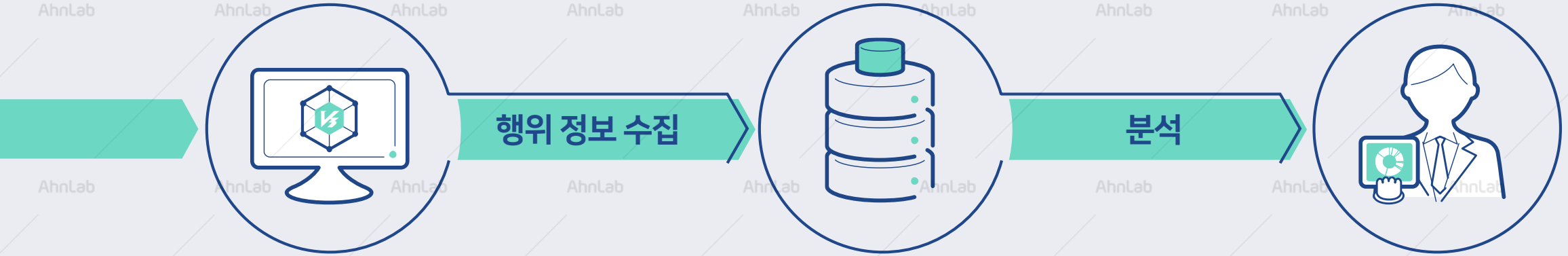
악성코드와 유사한 파일 구조를 갖고 있는가?

어떤 모듈(들)과 관계 있는가?

어떤 행위를 했는가?

엔드포인트 행위 정보 수집을 통한 위협 가시성 강화

AhnLab



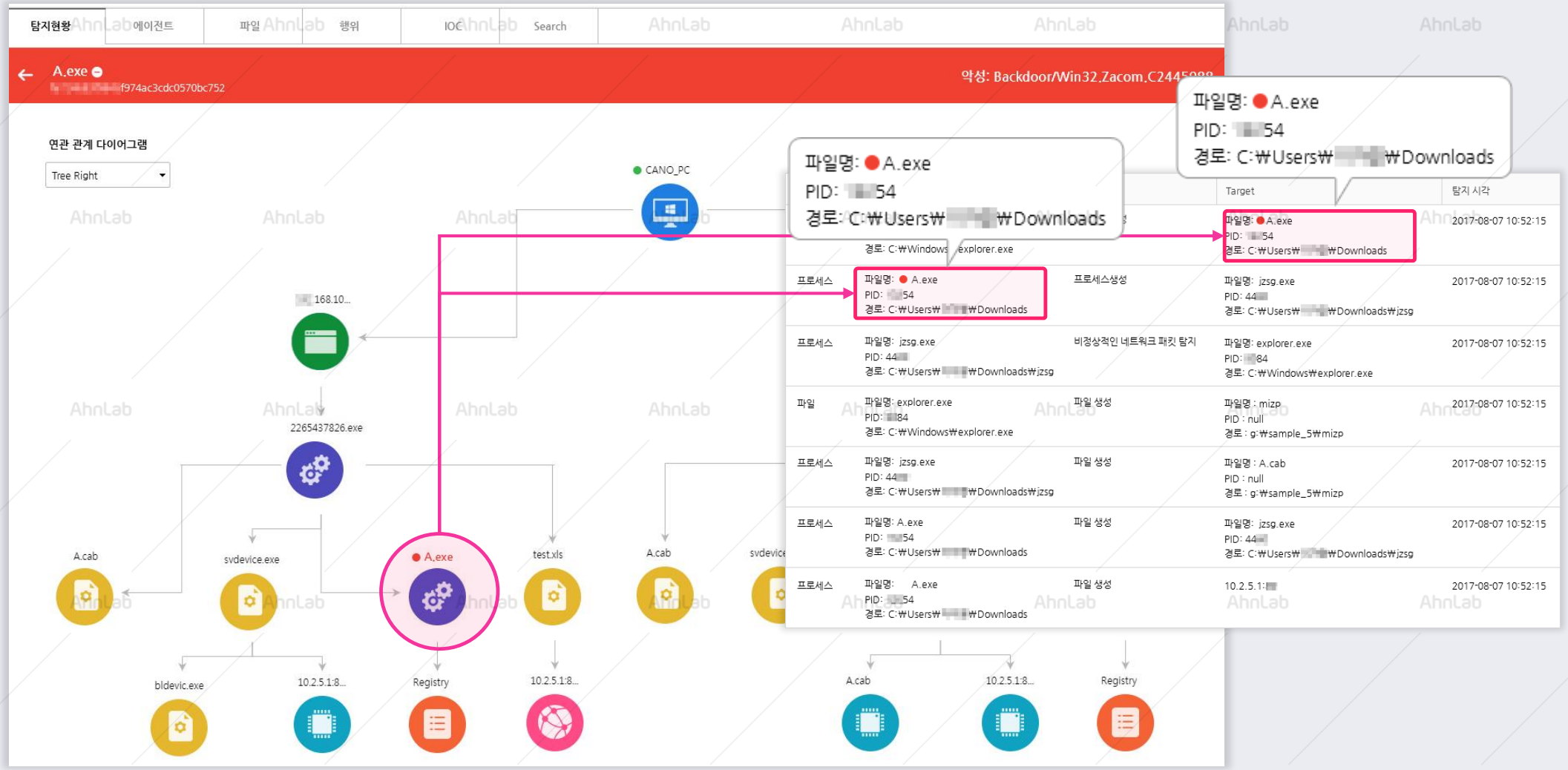
Threat Hunting

- 특정 이벤트 중심이 아닌 전체적, 연속적인 행위 정보 수집 및 저장
- 필요 시 언제든지 위협 및 관련 정보 확인 가능 - 사후 위협 분석 가능

Centralization

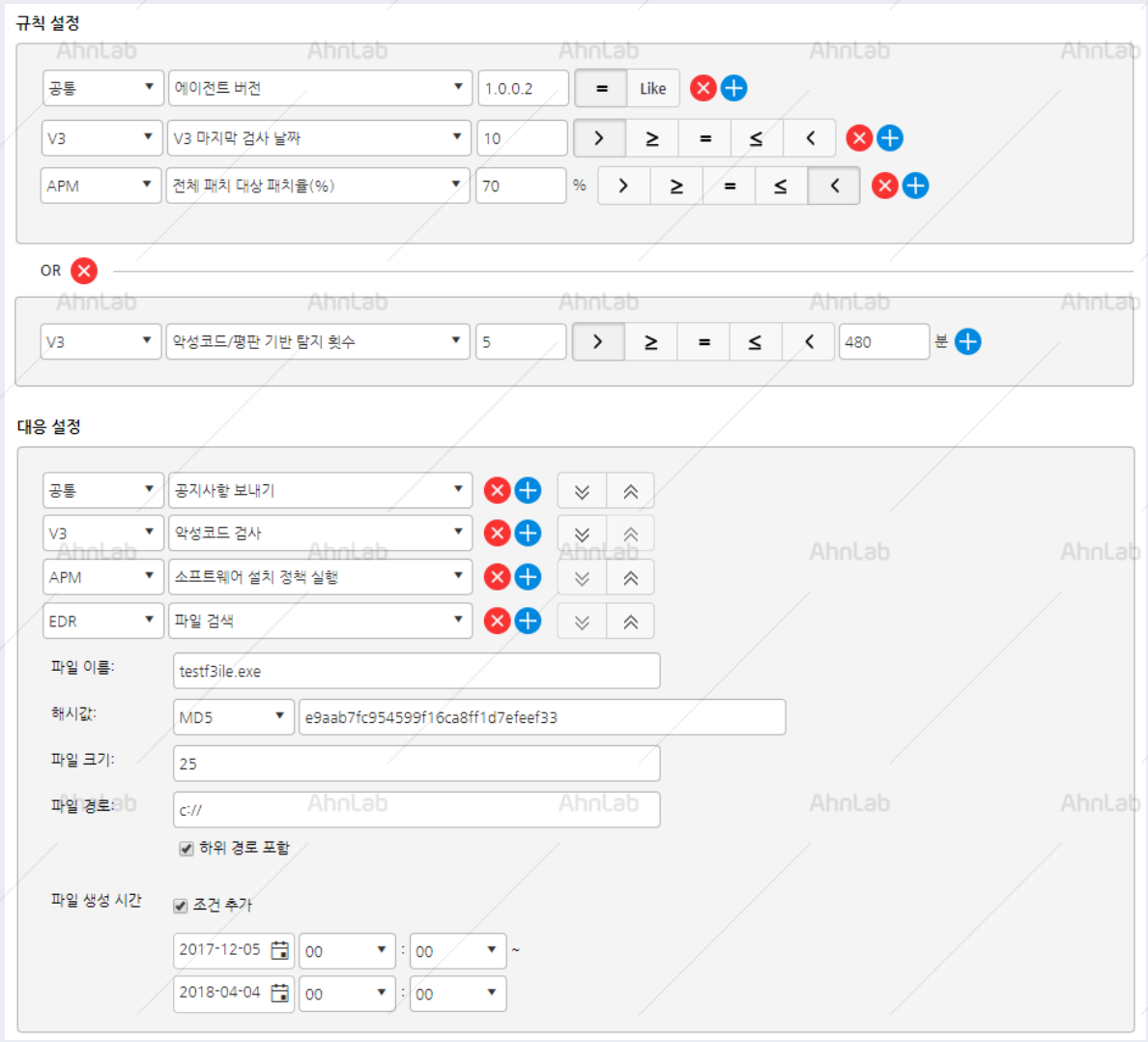
- 중앙화된 로그 저장 및 관리 - 모든 엔드포인트 로그를 중앙 서버에 저장
- 로그 관리 및 분석 편의성 향상

위협 이벤트 및 공격 흐름도 제공



엔드포인트 제품간 연계 정책을 통한 위협 대응

AhnLab



특·장점 : V3 기반의 안정적인 도입 운영

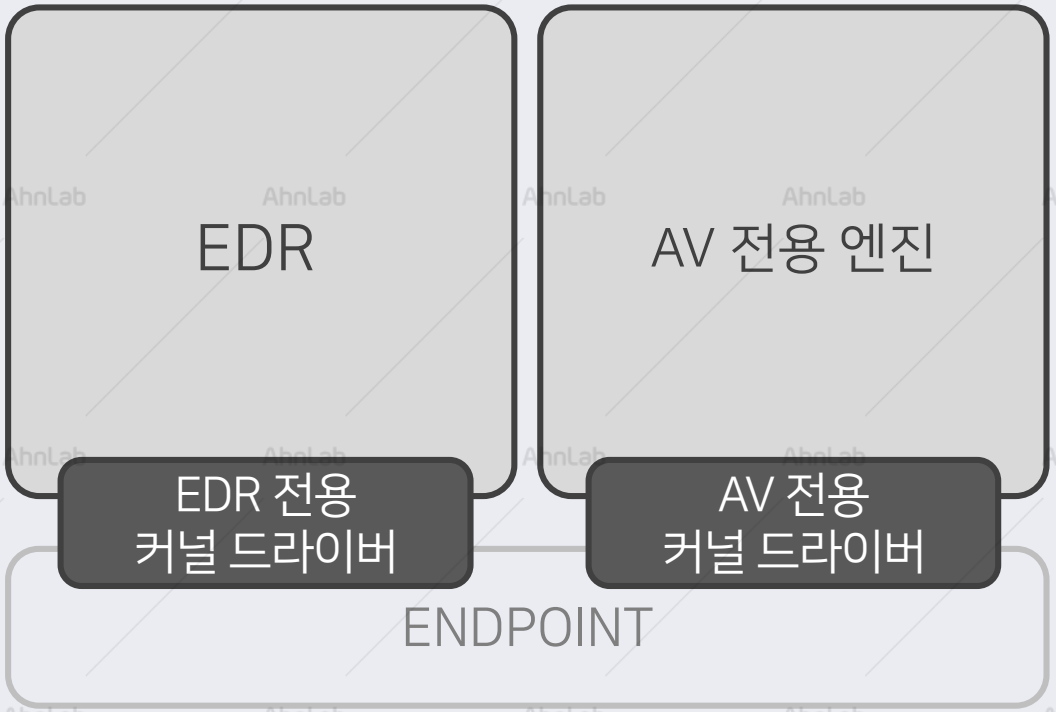
AhnLab

AhnLab EDR

- V3 행위 분석 엔진 연계
- 엔드포인트 행위 분석을 위한 커널 드라이버 추가 설치 불필요

타사 EDR

- 운영체제 커널 기반의 행위 정보 모니터링을 위해 AV와 EDR 운영을 위한 개별 커널 드라이버 설치 및 관리 필요
- 별도의 AV 사용으로 인한 커널드라이버 중복 설치 및 이에 따른 엔드포인트 성능 이슈 발생



특·장점 : 단일 매니지먼트 기반의 관리

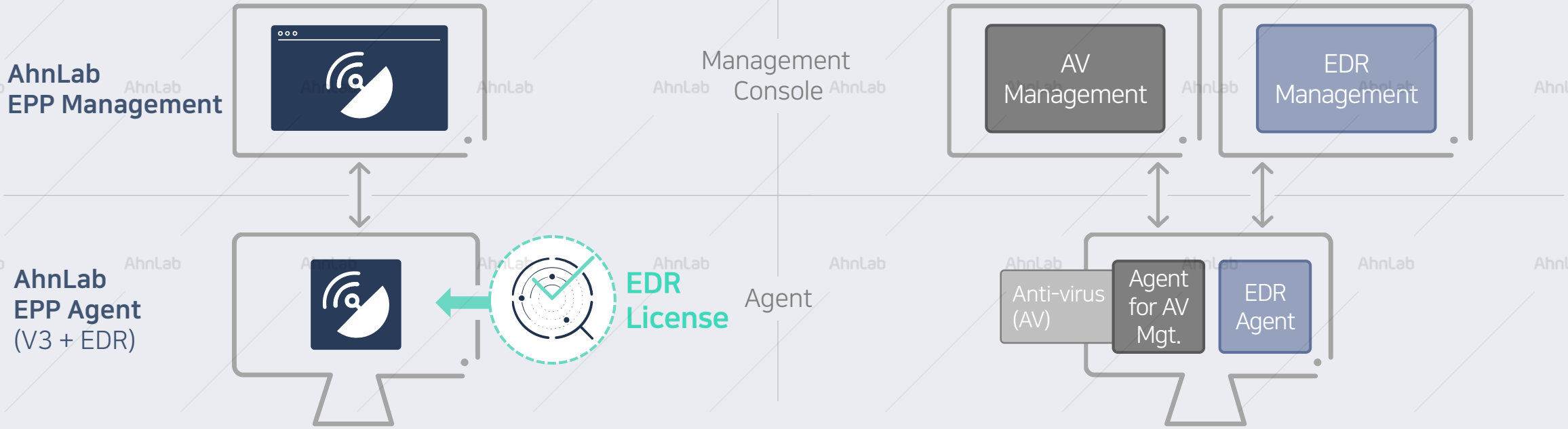
AhnLab

AhnLab EDR

- 단일 에이전트, 단일 매니지먼트 기반의 효율적인 보안 운용
  (One Agent, Single Management Console)
- V3 기 사용 시 EDR 라이선스 추가만으로 즉각적인 운영 가능
- EDR 운영을 위한 에이전트 추가 설치 불필요
  (로그 저장 등을 위한 DB 서버만 추가)

타사 EDR

- 백신(AV), EDR 및 그 외 엔드포인트 보안 솔루션 운영을 위한 개별 에이전트, 개별 매니지먼트 콘솔 필요
- EDR 전용 장비 구매 및 구축 필요
- 백신 추가 사용 시 개별 설치 및 관리 필요



특·장점 : 연계 정책을 통한 위협 대응

One Agent

연계 규칙 위반 시스템에 대한 순차적 대응 정책 적용

공통(관리)

- **공지사항 보내기**
  - SW/HW 정보 수집
  - 에이전트 설치/삭제
  - 공유폴더 정보 수집
- **공유폴더 해제**
  - 메일 알림
  - 보고서 생성

V3

- **V3 수동 업데이트**
  - 보안 제품 배포 실행
- **네트워크 완전차단**
  - 네트워크 완전차단 해제
- **악성코드 검사**
  - 시스템 최적화

EDR

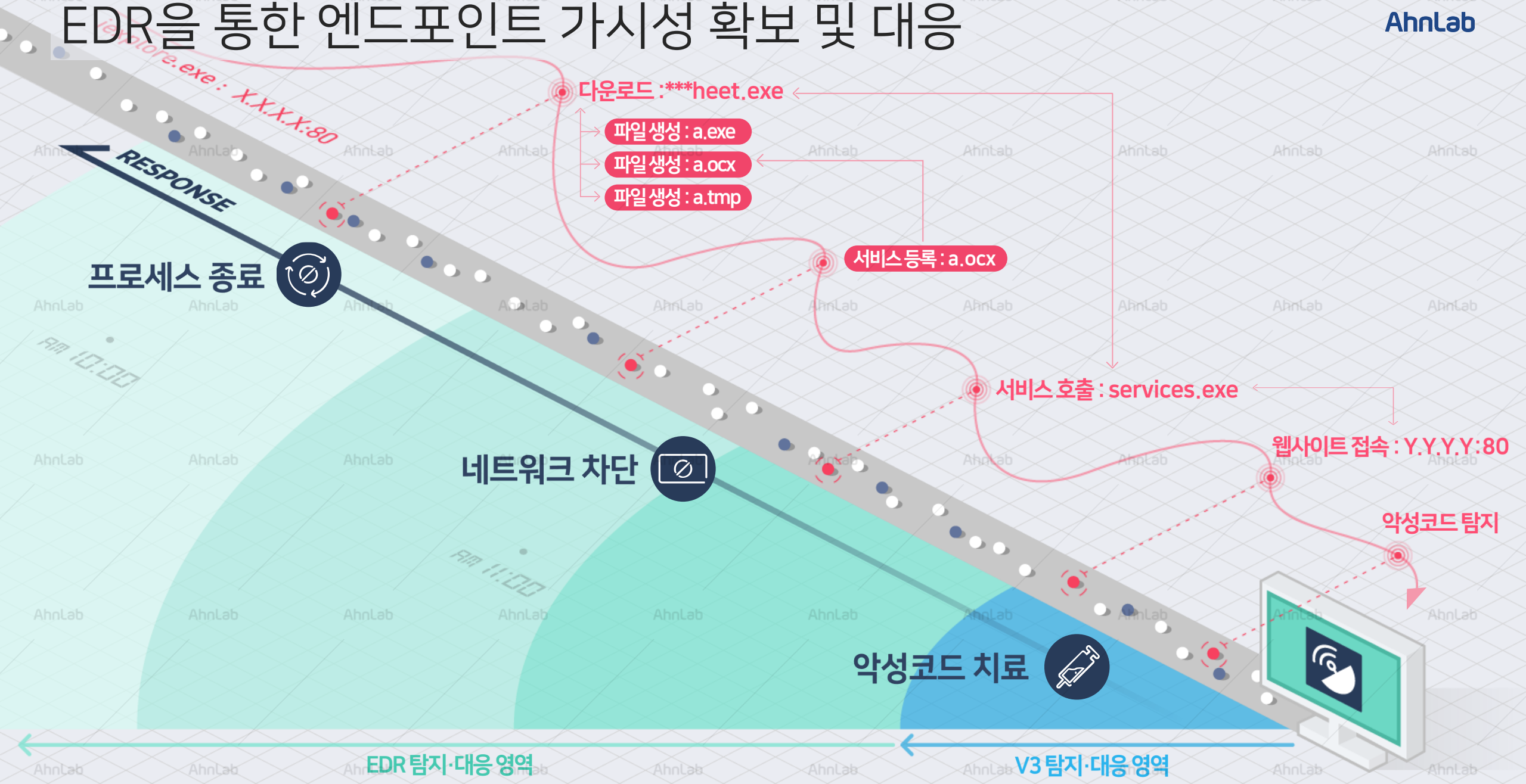
- **프로세스 종료**
  - 특정 파일 수집
- **특정 파일 검사**
  - Artifact 수집
  - AhnReport 수집

APM

- **배포 실행**
- **전체 패치 적용**
  - 권장 패치 적용
  - 패치 정보 수집
  - 소프트웨어 저작권 검사
  - 특정 소프트웨어 설치

EDR을 통한 엔드포인트 가시성 확보 및 대응

AhnLab



More security, More freedom

AhnLab