엔드포인트보안, EDR로 진화하다

안랩 제품기획팀 김 창 희 팀장

AhnLab

Crime Scene

AhnLab

Crime Scene

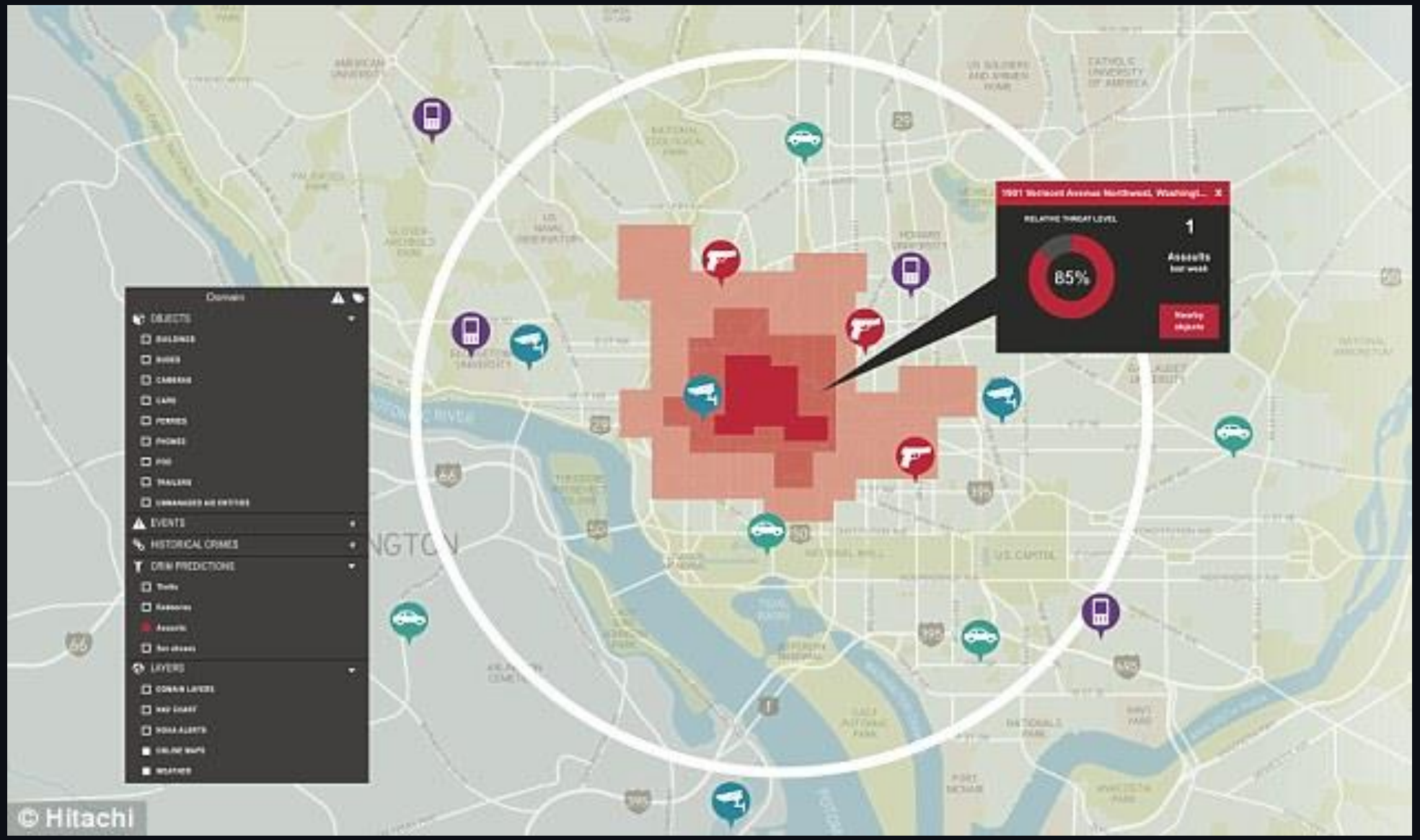
AhnLab

Crime Prediction

AhnLab

Crime Prediction

AhnLab



Contents

AhnLab

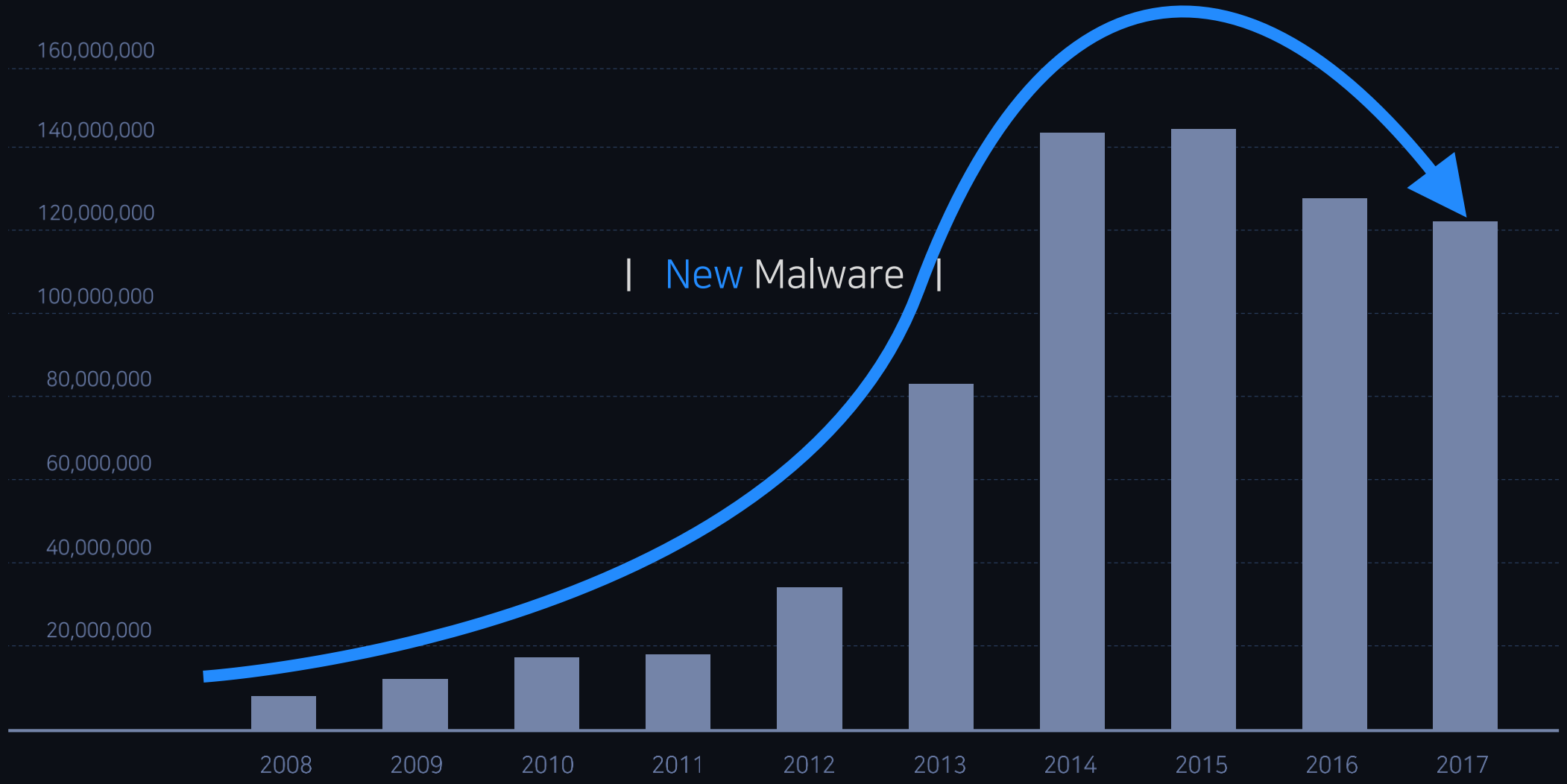
01

최근 보안 위협의 변화

AhnLab

최근 10년 동안 신종 악성코드 추이

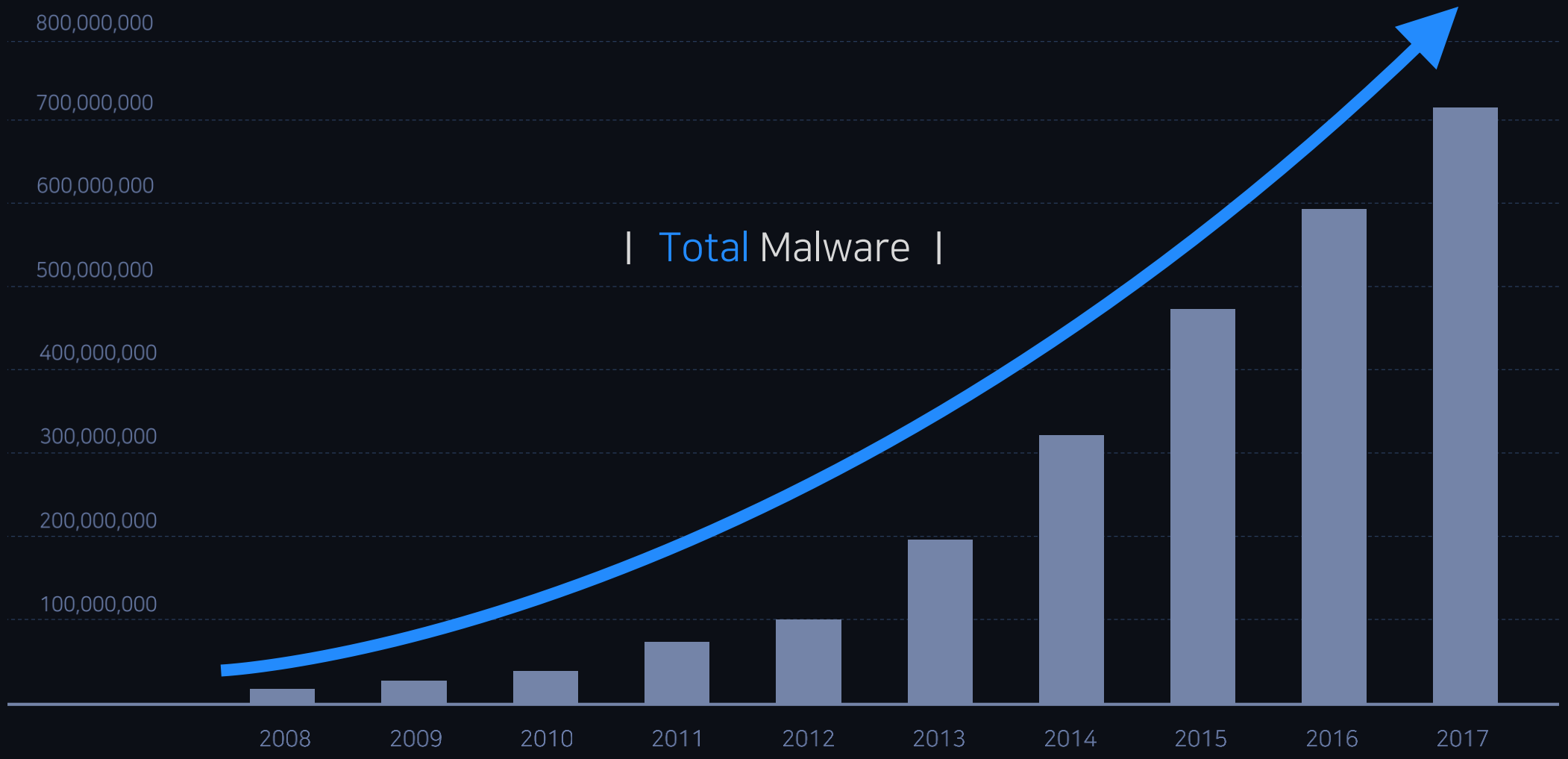
AhnLab



※ 출처: AV-TEST GmbH, www.av-test.org

최근 10년 동안 전체 악성코드 추이

AhnLab



※ 출처: AV-TEST GmbH, www.av-test.org

최근 유행하는 악성코드는?

AhnLab

랜섬웨어
(Ransomware)

채굴 악성코드
(Miner)

크립토 재킹
(Crypto Jacking)

2016년 랜섬웨어

AhnLab

2013~2015

9종

1년 만에
18배 증가

2016

163종
(월 평균 13종)

2017년 랜섬웨어

AhnLab

2016

163종

1년 평균
163개 제작?

2017

163종

전 세계 암호화 화폐 종류

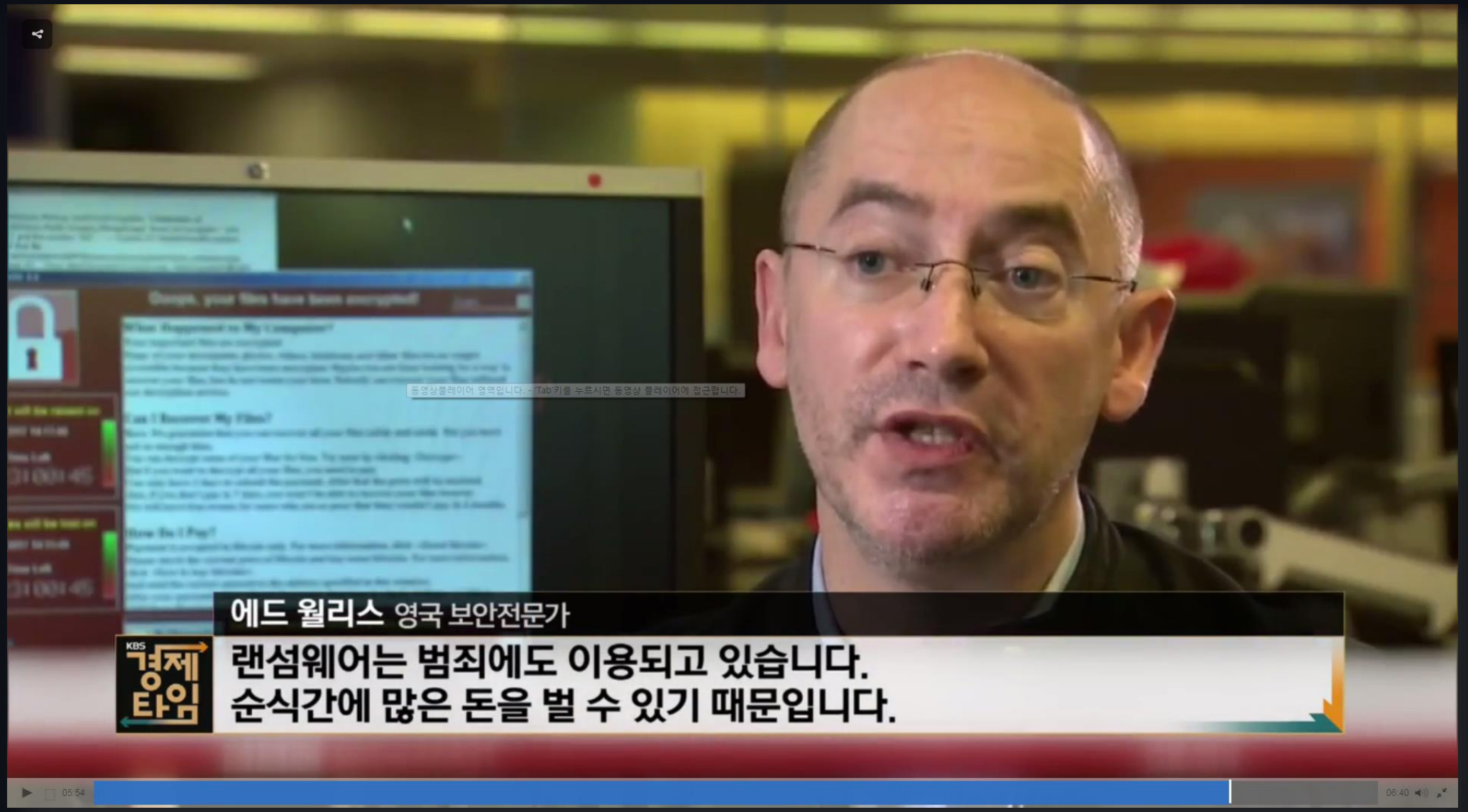
AhnLab

약 1932 종 존재

시가총액 약 400 조

랜섬웨어

AhnLab



랜섬웨어

AhnLab

최근 유행하는 악성코드는?

AhnLab

랜섬웨어
(Ransomware)

채굴 악성코드
(Miner)

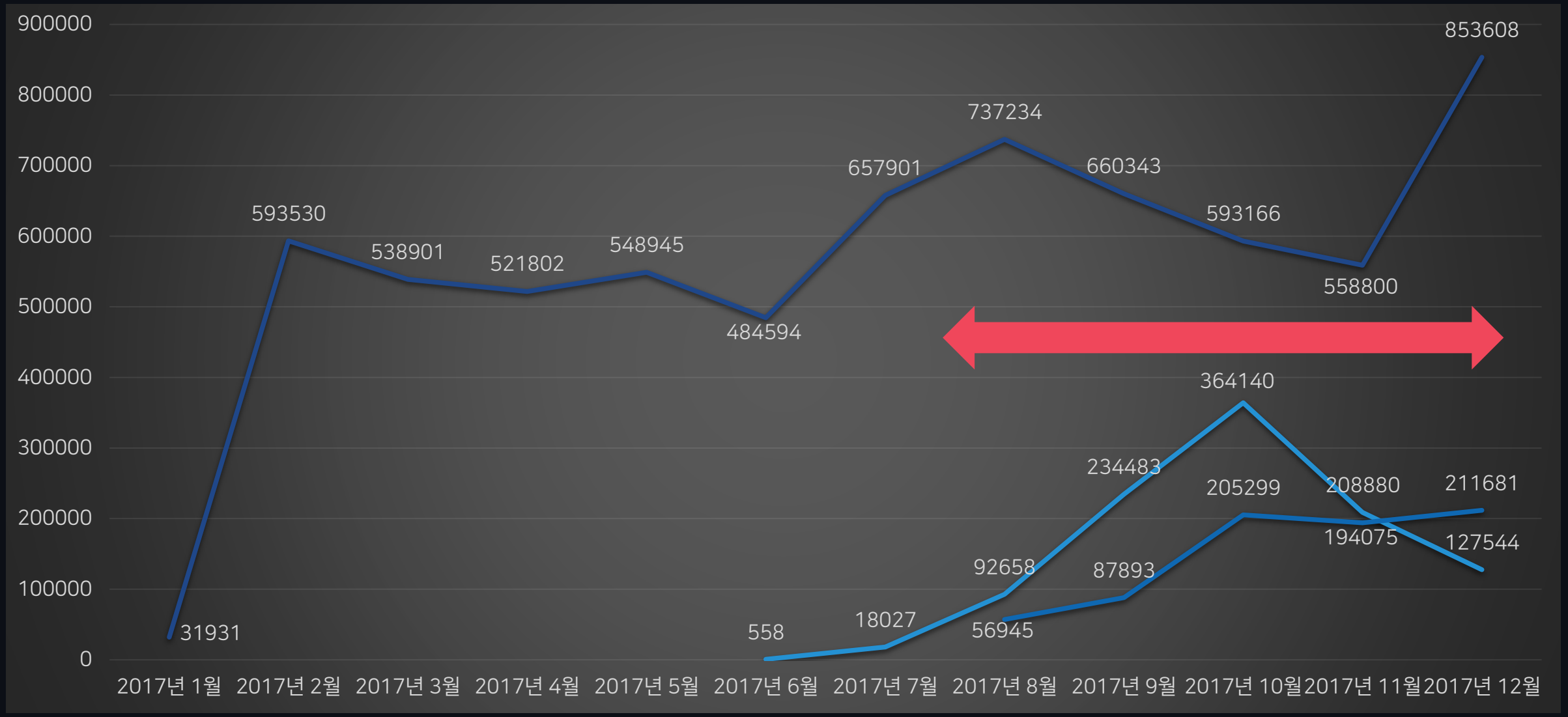
크립토 재킹
(Crypto Jacking)

2015년 부터 활동한 채굴 프로그램들

AhnLab

채굴 악성코드 흐름 (2017)

AhnLab



최근 유행하는 악성코드는?

AhnLab

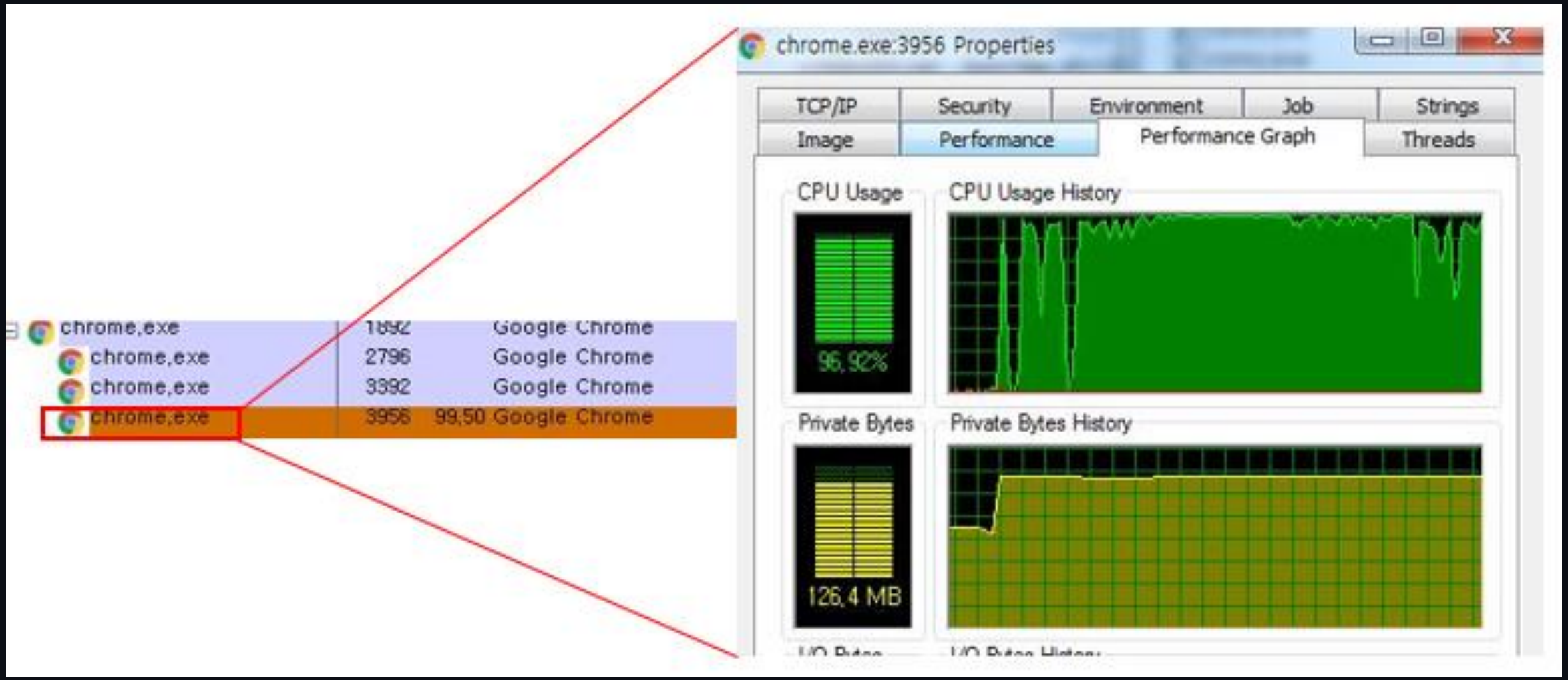
랜섬웨어
(Ransomware)

채굴 악성코드
(Miner)

크립토 재킹
(Crypto Jacking)

크립토 재킹 Drive by Miner (download)

AhnLab



AhnLab

타깃 공격

타깃 공격 기법 #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

주요 공격 기법 #1 워터링 홀

AhnLab

타깃 공격 기법 #2 스피어 피싱

AhnLab

스피어 피싱
Spear Phishing

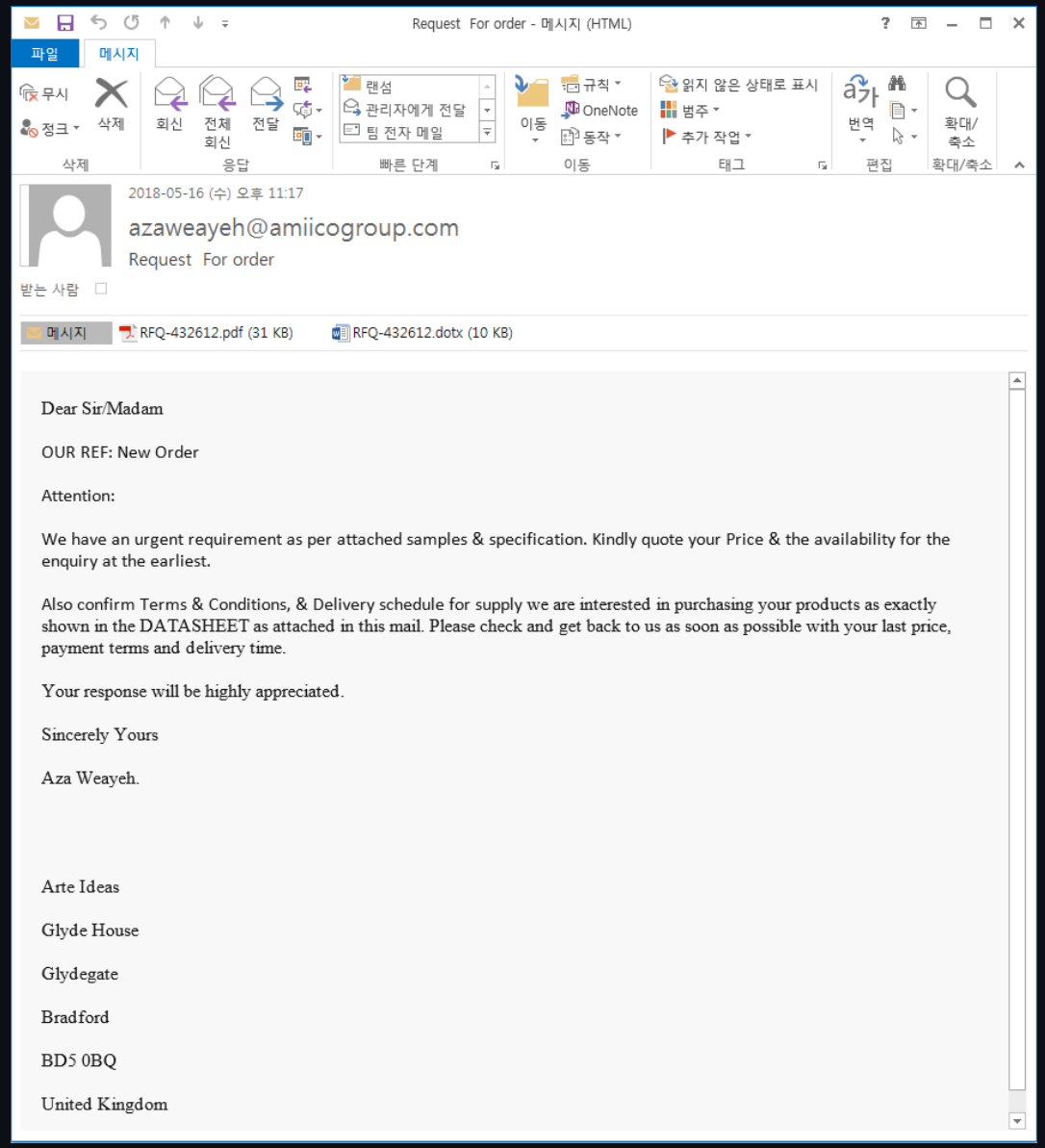
공격자가 의도한 대상에게
이메일 송부

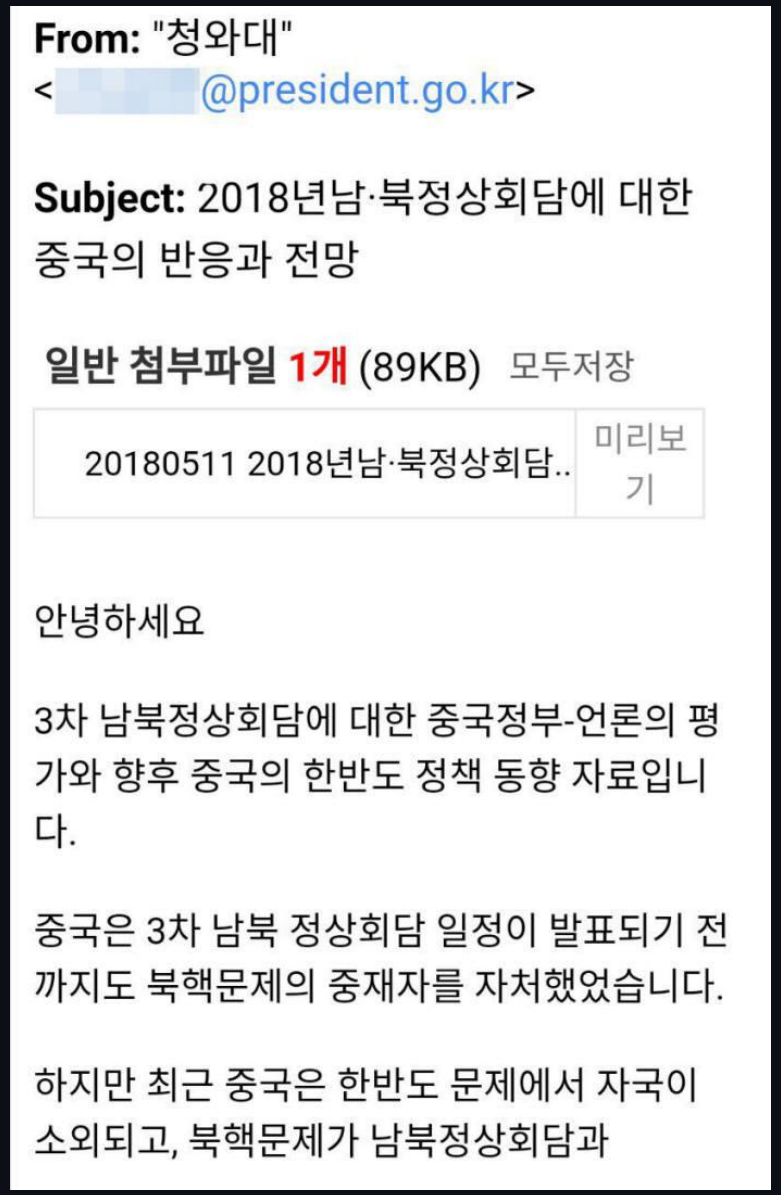
첨부파일 / 악의적 링크를 통한
악성코드 감염

국가기관 및 회사 기밀자료 수집/유출
/원격접속을 통한 위해행위

타깃 공격 기법 #2 스피어 피싱

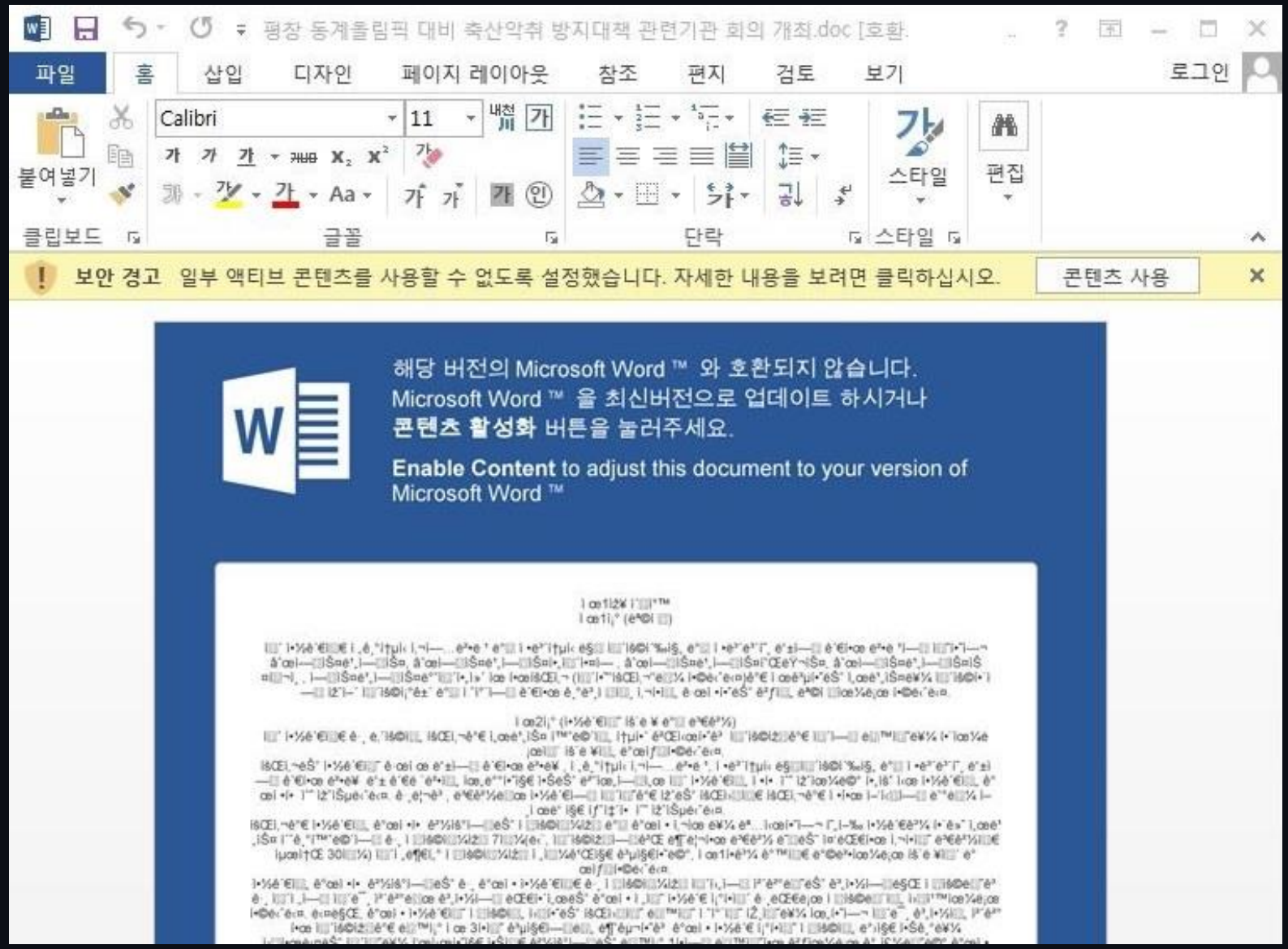
AhnLab





타깃 공격 기법 #2 스피어 피싱

AhnLab



타깃 공격 기법 #3 공급망 공격

AhnLab

공급망 공격
Supply chain attack

소프트웨어 제조 공정을 장악

정상적인 패키지 제품을 통해
기업내부에 악성코드 감염

국가기관 및 회사 기밀자료 수집/유출
/원격접속을 통한 위해행위

타깃 공격 기법 #3 공급망 공격

AhnLab

기타 – 주소 좌측 안전자물쇠도 무의미

AhnLab

02

엔드포인트 보안, EDR로 진화

AhnLab

보안 키워드의 변화

AhnLab

2014	Security Intelligence	Share, Learn, Secure Digital Business
2015	Threat Intelligence Alliance & Share	CHANGE; Challenge today's security thinking Digital Transformation
2016	Automation, Visibility	Connect to Protect The speed of Digital Transformation
2017	Business Driven Security	Power of opportunity
2018	From TRUST, To RESILENCE	Together is Power

보안 관점의 변화

AhnLab

차단, 방어 → 탐지, 대응으로 패러다임 변화

Protection 에서 많은 정보를 얼마나 빨리 탐지하고 대응하는 지에 초점

Detection → Analysis → Response

정확한 정보 전달, 관리자가 빠른 시간 내 대처하는 것이 중요

Connect to Protect

모든 경로의 위협 모니터링, 가시화하는 제품/기능 간의 유기적 융합 강조

다양한 구성의
비즈니스 환경

+

종합적인
분석과 판단

위협 관리 및 대응 관점의 보안

AhnLab

Transformation to the Platform

AhnLab

인프라 전반에 대한 **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 경로를 통한 의심·악성 파일 유입

사회공학기법, 표적/지능형 공격

OS/SW 제로데이 취약점 이용 신·변종 악성코드 증가

03

쉬운 보안, 효과적인 EDR

AhnLab

Transformation to the Platform

AhnLab

Change
환경과 보안 위협의 변화, 진화

Transformation
보안 접근 관점과 대응의 혁신

Customer-driven Security

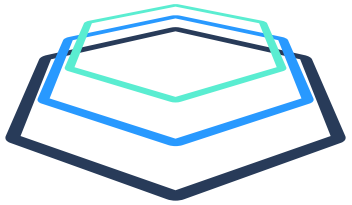
AhnLab SECURITY LADDERS

AhnLab EPP·EDR

AhnLab

AhnLab EPP

Endpoint Protection Platform



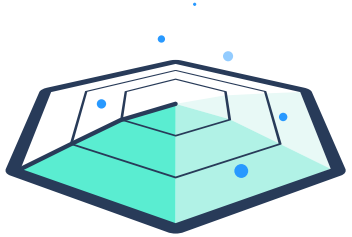
악성코드 탐지를 넘어 위협 관리/대응 플랫폼으로

Transformation to a Next Generation Endpoint Protection Platform

- 차세대 엔드포인트 보안 플랫폼
- 제품간 유연한 연계를 통한 효율적인 위협 관리/대응
- One Agent, Single Management Console

AhnLab EDR

Endpoint Detection & Response



손쉬운 EDR 도입, 올바른 엔드포인트 위협 가시성

Simple Deployment, Easy to Use

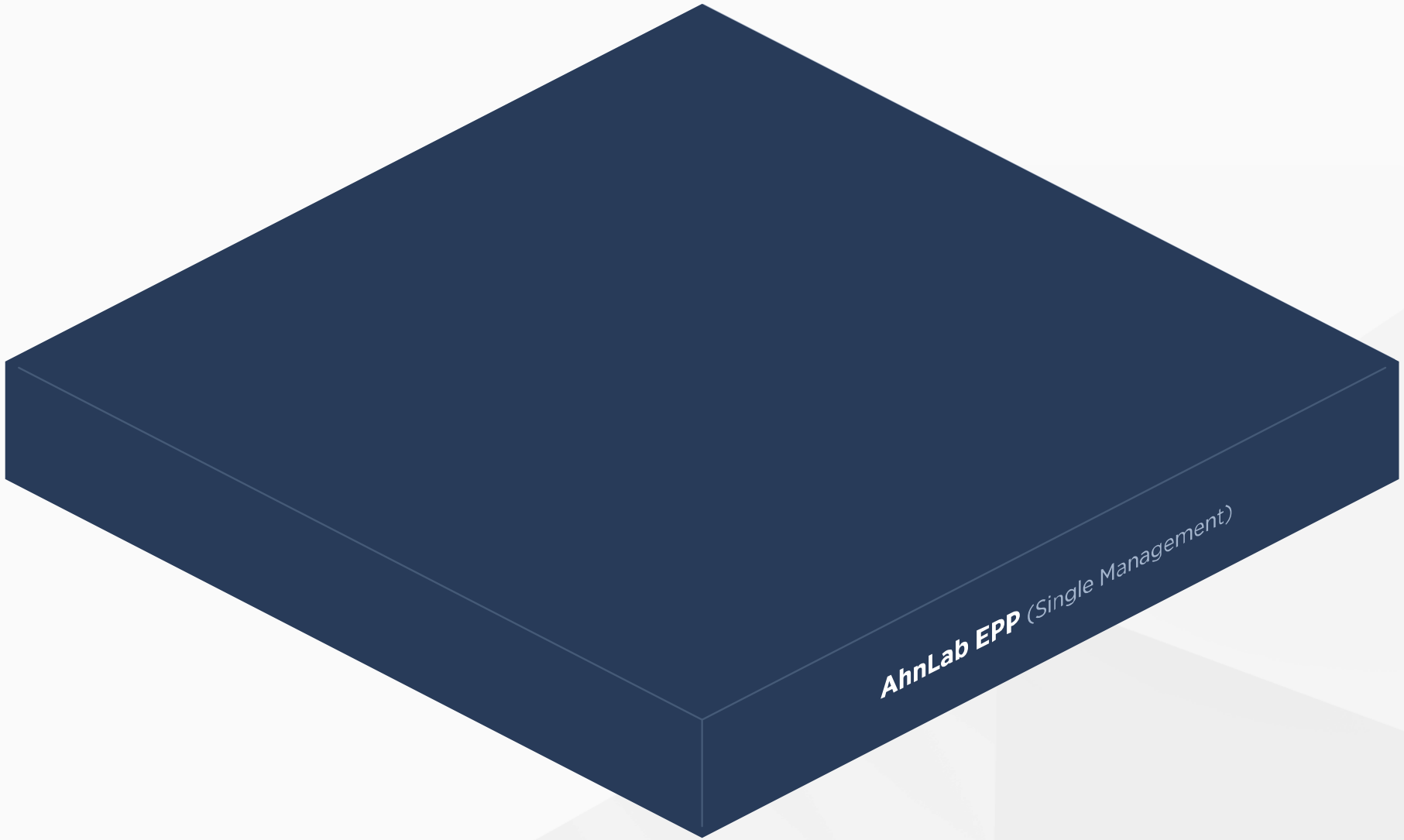
- 최고의 악성코드 전문 기업이 만든 올바른 EDR
- 국내 최초 행위 기반 엔진을 통한 행위 분석/모니터링
- 모든 엔드포인트 행위 로그 수집, 무제한 DB보존

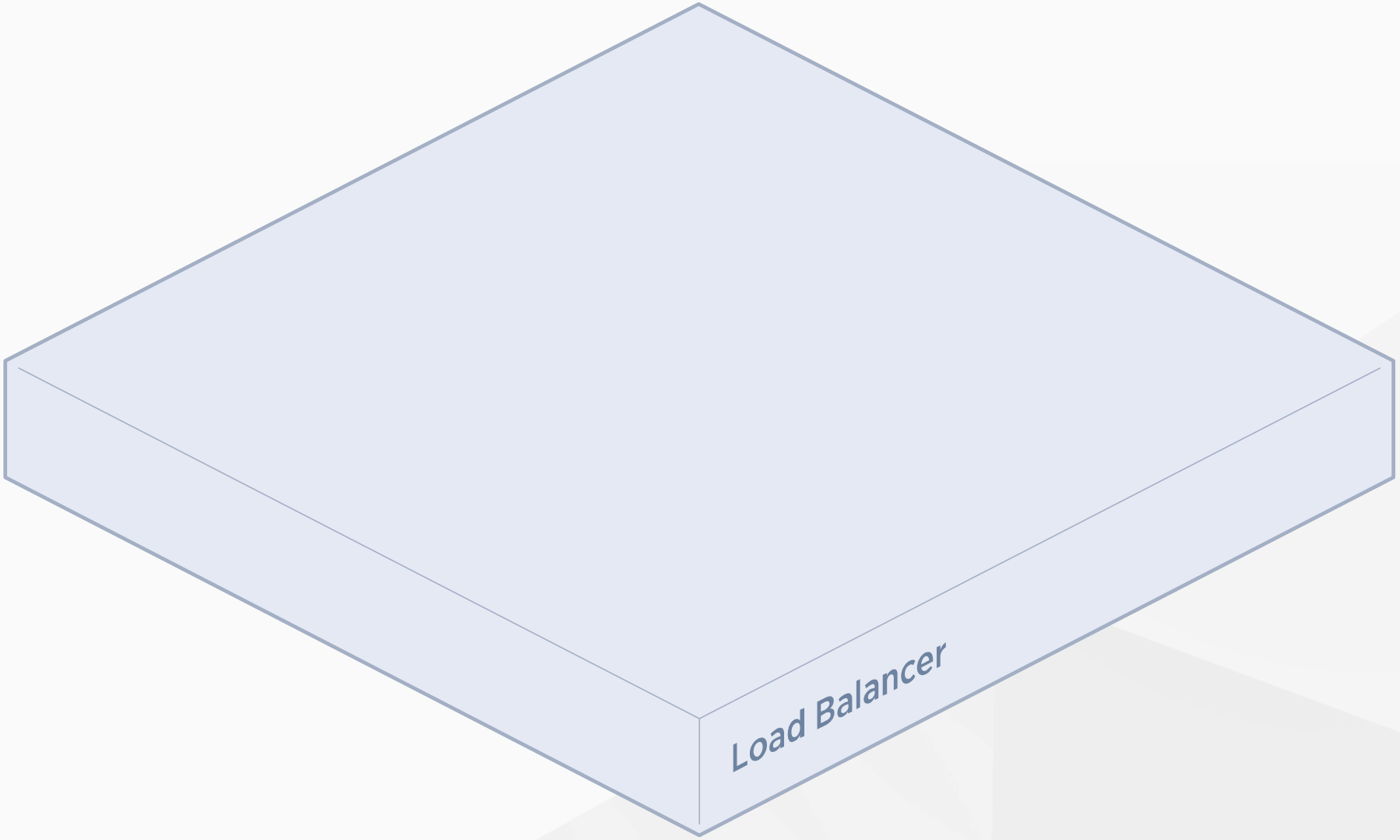
AhnLab EPP Management

AhnLab

단일 관리 콘솔을 기반으로 다수의 엔드포인트 보안 솔루션을 통합 운영 및 관리

AhnLab

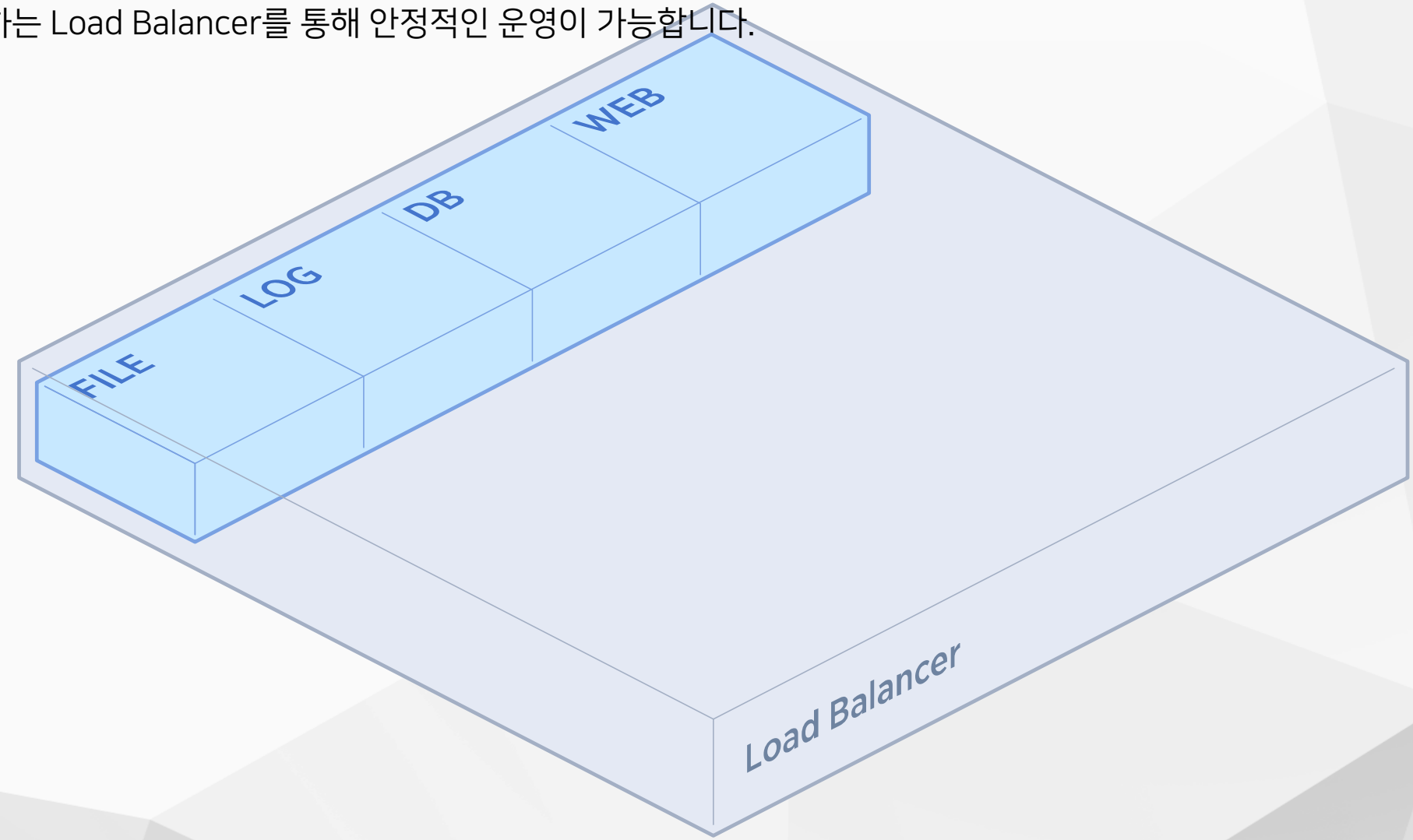




Flexibility & Stability

AhnLab

- 모듈 방식의 AhnLab EPP는 유연한 확장성을 제공하며,
- 모듈간의 부하를 방지하는 Load Balancer를 통해 안정적인 운영이 가능합니다.

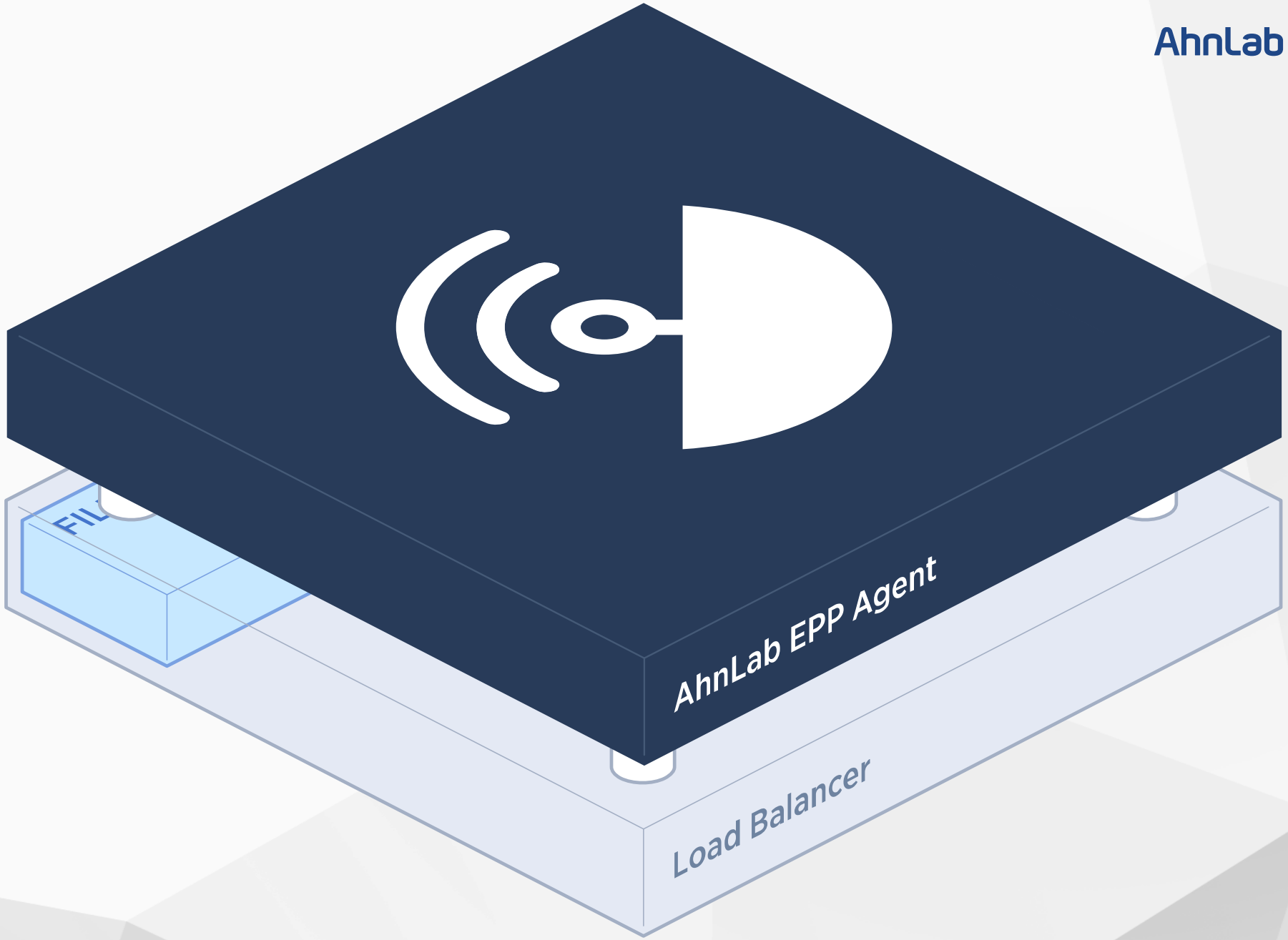


Flexibility & Stability

AhnLab

- 모듈 방식의 AhnLab EPP는 유연한 확장성을 제공하며
- 모듈간의 부하를 방지하는 Load Balancer를 통

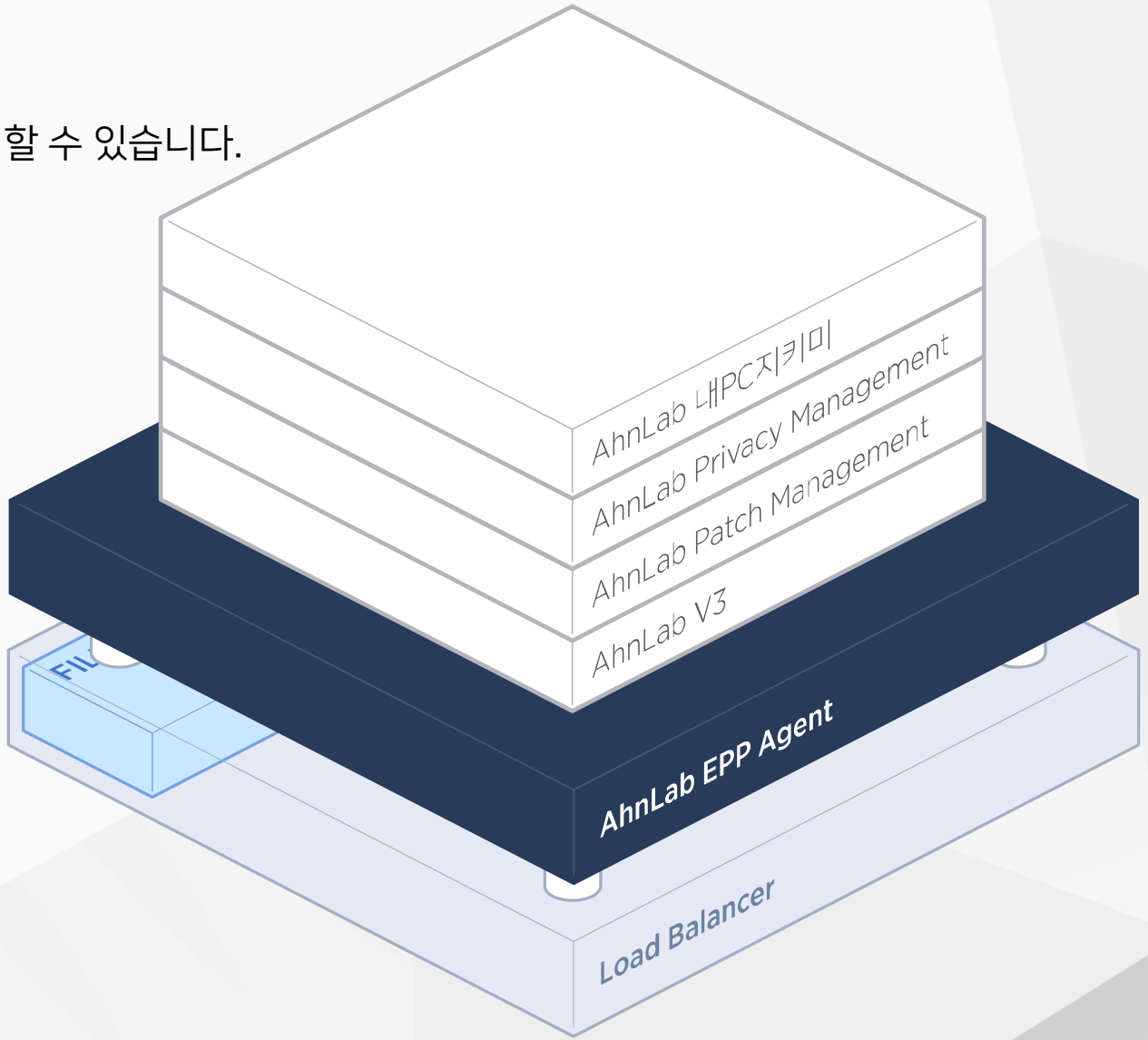
AhnLab



One Agent

AhnLab

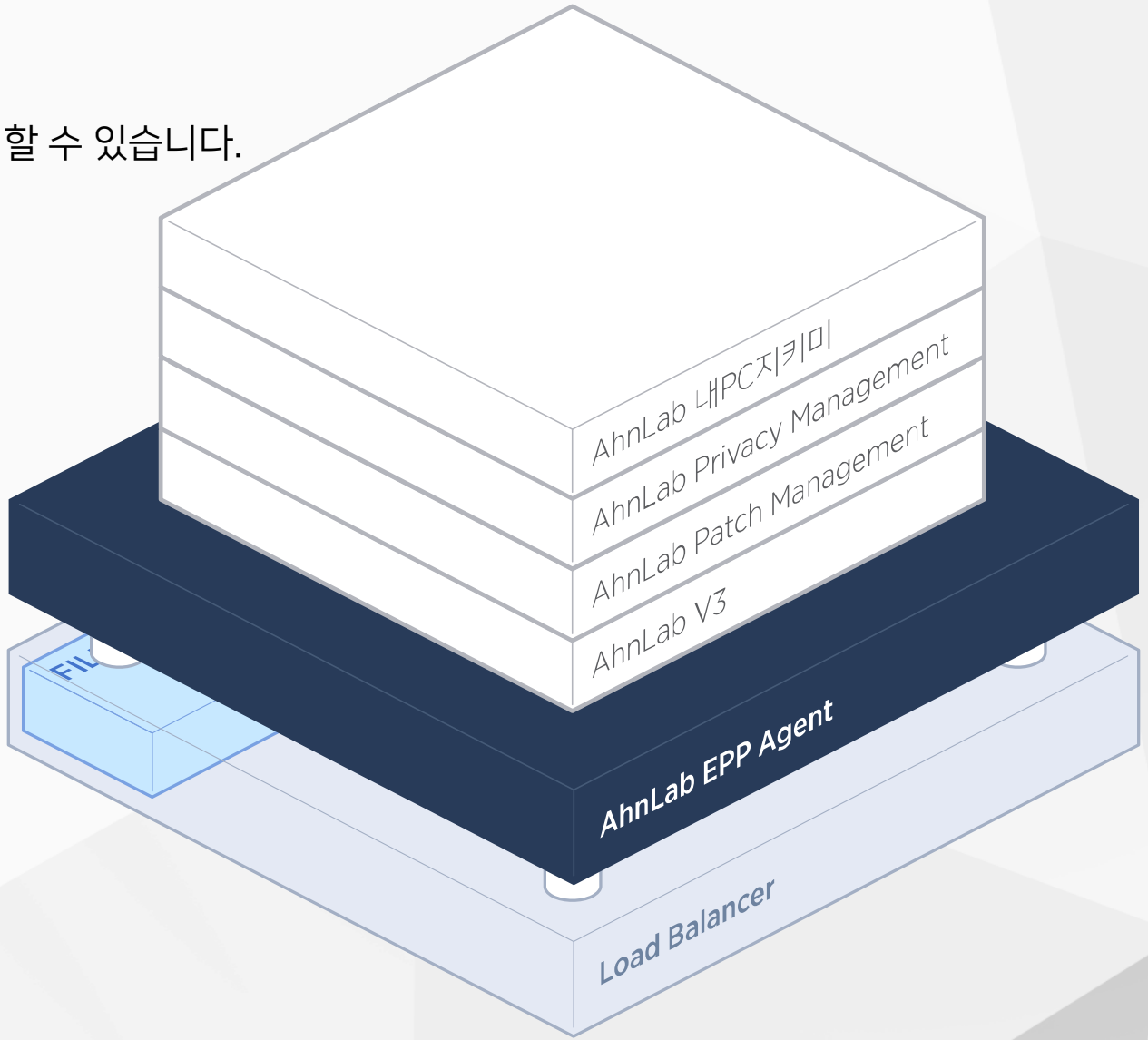
- 하나의 EPP 에이전트를 통해
- 다수의 엔드포인트 보안 솔루션을 효율적으로 통합 운영할 수 있습니다.



One Agent

AhnLab

- 하나의 EPP 에이전트를 통해
- 다수의 엔드포인트 보안 솔루션을 효율적으로 통합 운영할 수 있습니다.



Scale Out

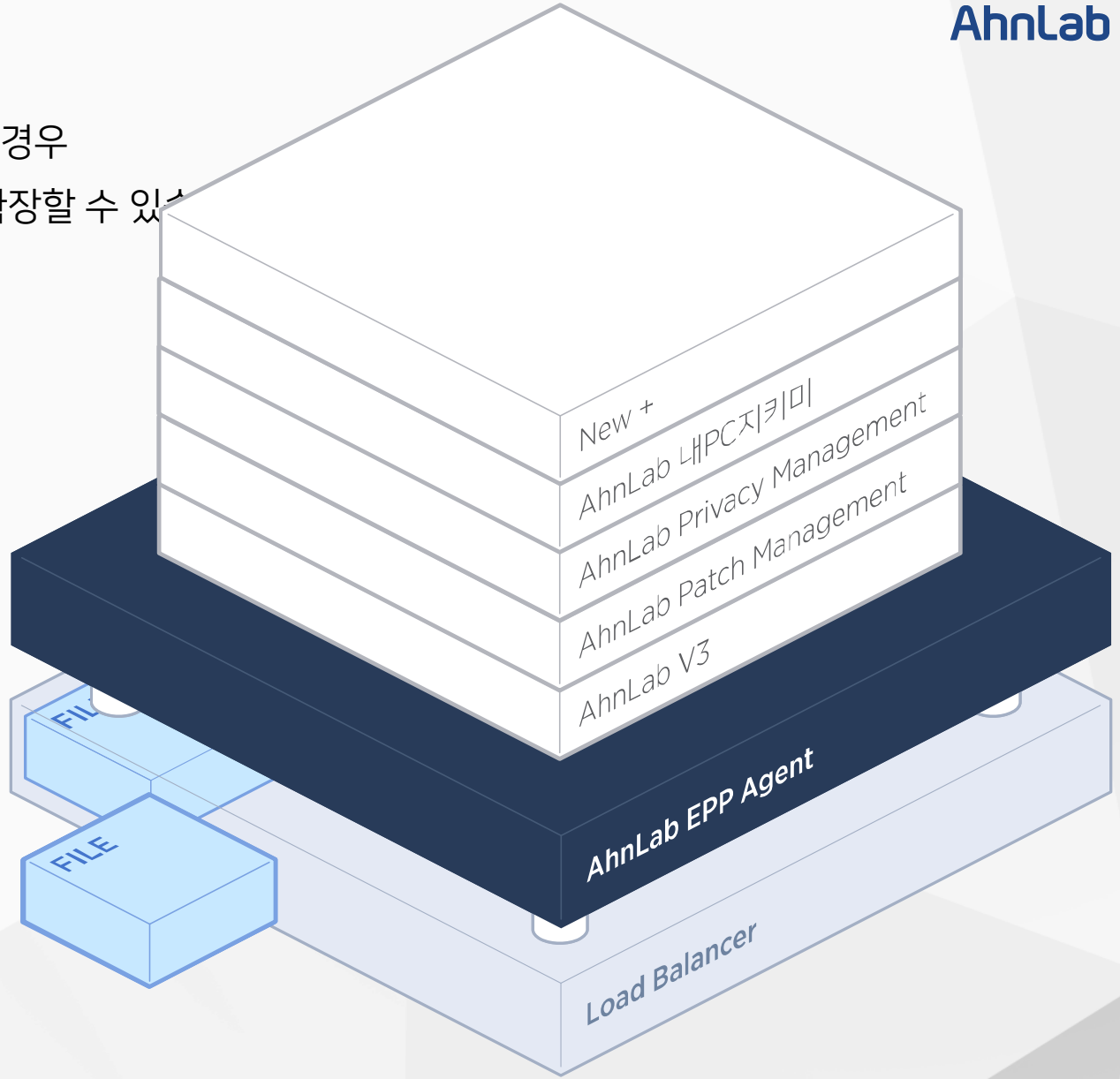
AhnLab

- 인프라 변화 및 트래픽 증가 등으로 서버 증설이 필요할 경우
- 상위 서버 교체 없이 병렬(Scale-out)로 손쉽게 추가, 확장할 수 있

올인원(단일 장비) 구성

분리형(개별 장비) 구성

전체 독립형 (개별 장비) 구성



Scale Out

AhnLab

- 인프라 변화 및 트래픽 증가 등으로 서버 증설이 필요할 경우
- 상위 서버 교체 없이 병렬(Scale-out)로 손쉽게 추가, 확장할 수 있

올인원(단일 장비) 구성

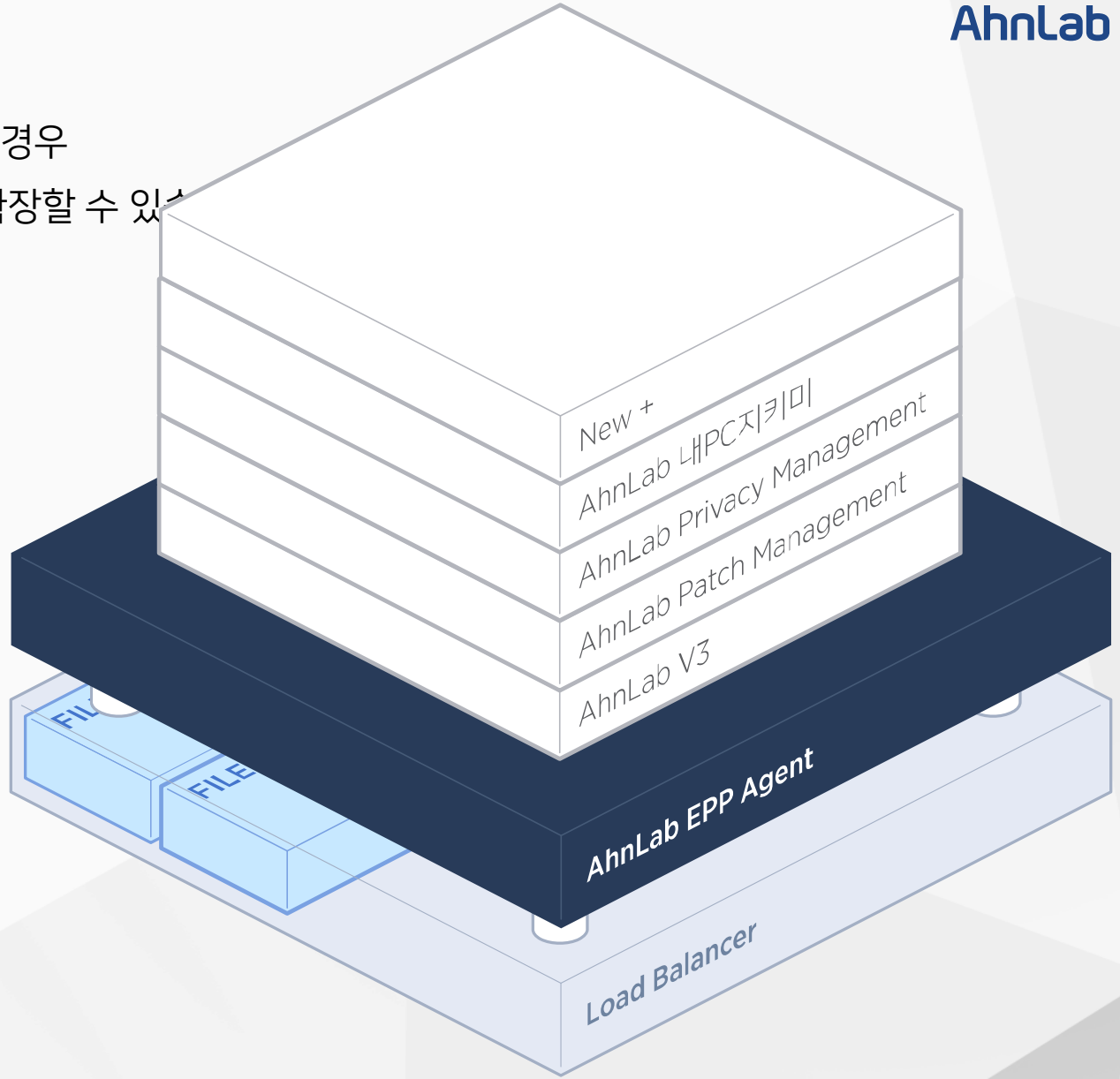
Load Balancer	File	Web	Log	DB

분리형(개별 장비) 구성

Load Balancer	File	Web	Log	DB

전체 독립형 (개별 장비) 구성

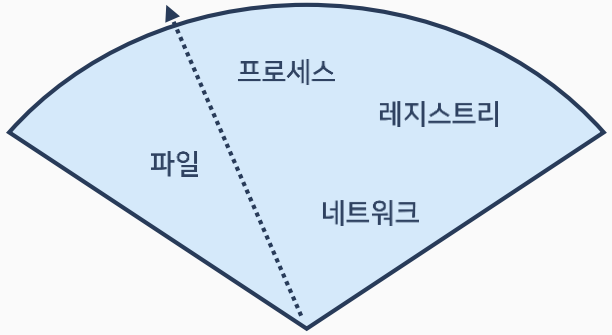
Load Balancer	File	Web	Log	DB



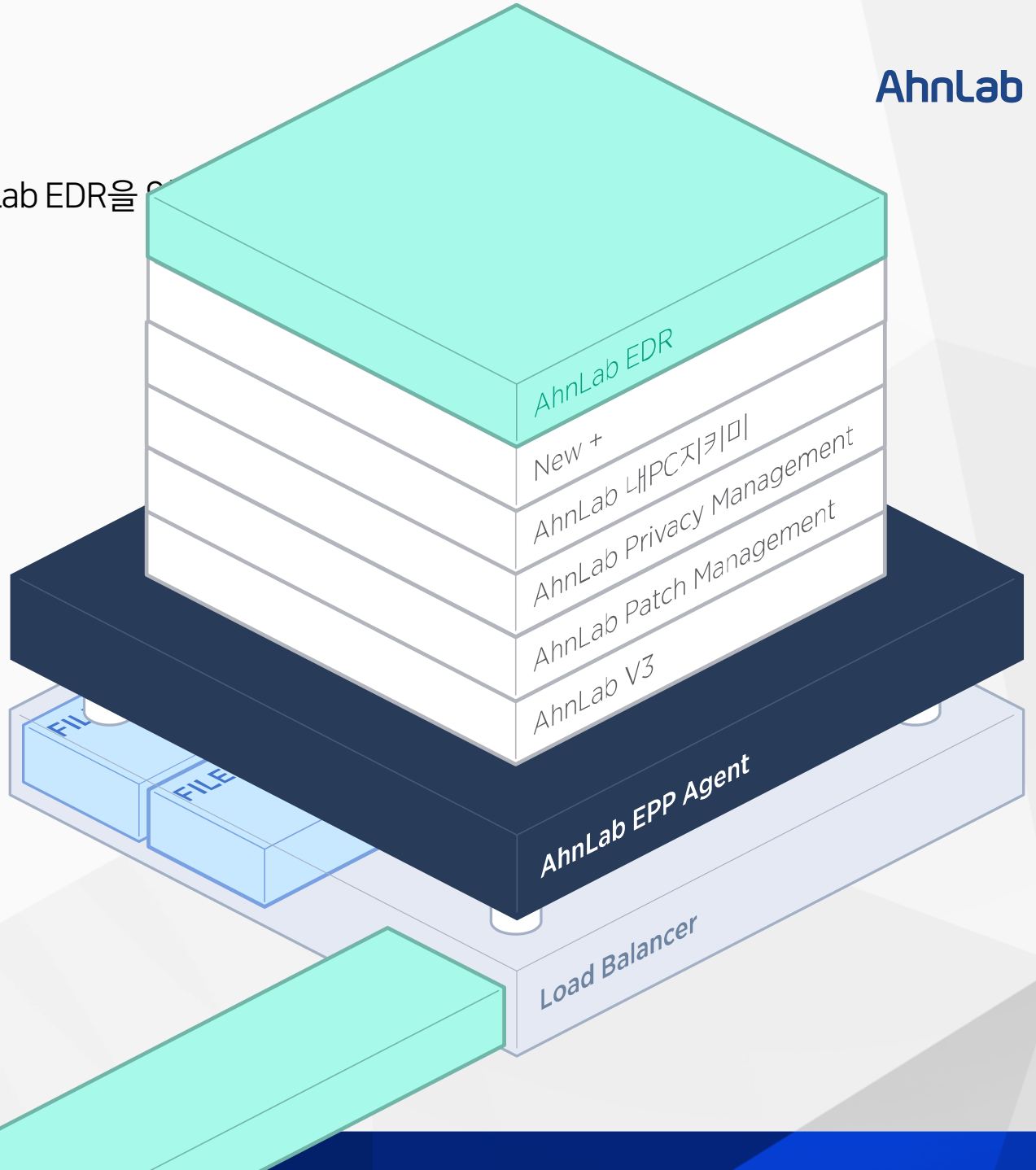
AhnLab EDR

AhnLab

- 라이선스를 추가하는 것만으로 쉽고 간편하게 V3와 AhnLab EDR을
- 더 강력한 엔드포인트 위협 대응이 가능합니다.
- (*V3 기 사용 시)



One Agent
Single Management Console



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?

어떻게 악성코드에 감염됐는가?

악성코드와 유사한 파일 구조를 갖고 있는가?

어떤 행위를 했는가?

파일이 유입된 이후 실행된 적이 있는가?

동일한 파일이 얼마나 많은 시스템에 존재하는가?

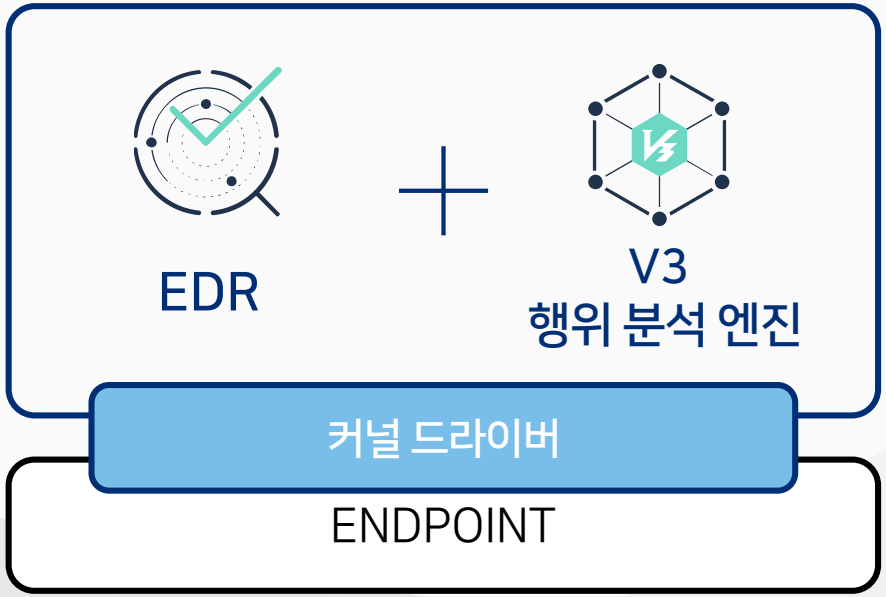
어떤 모듈(들)과 관계 있는가?

특·장점 : V3 기반의 안정적인 도입 운영

AhnLab

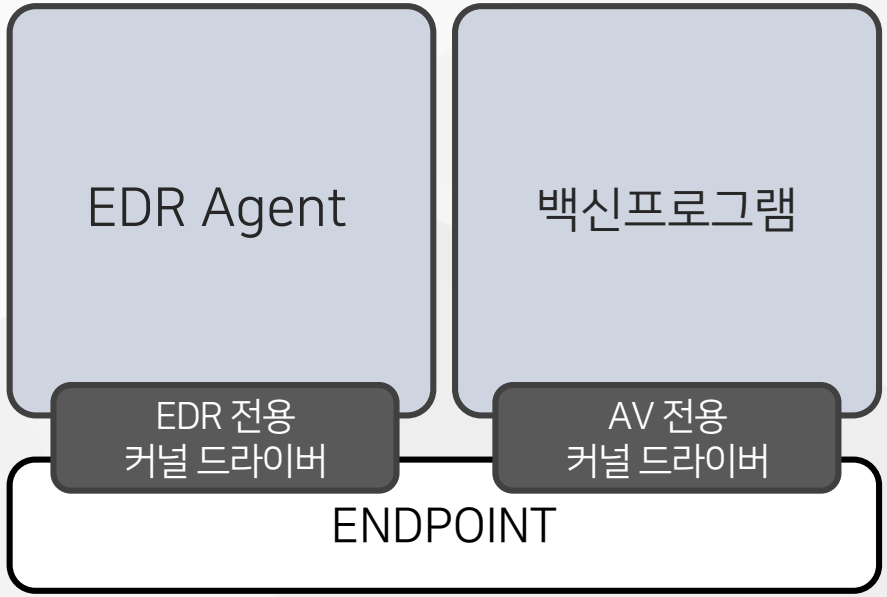
AhnLab EDR

- 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

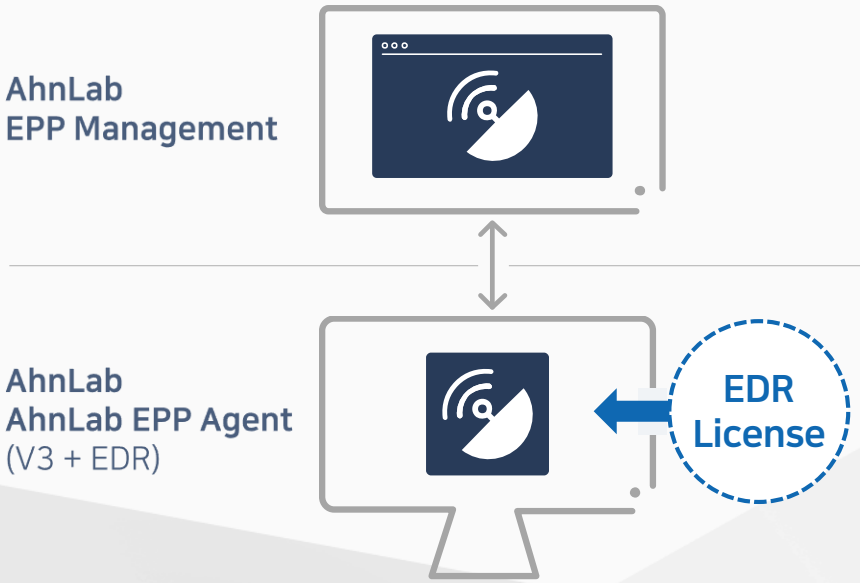


특·장점 : 단일 매니지먼트 기반의 관리

AhnLab

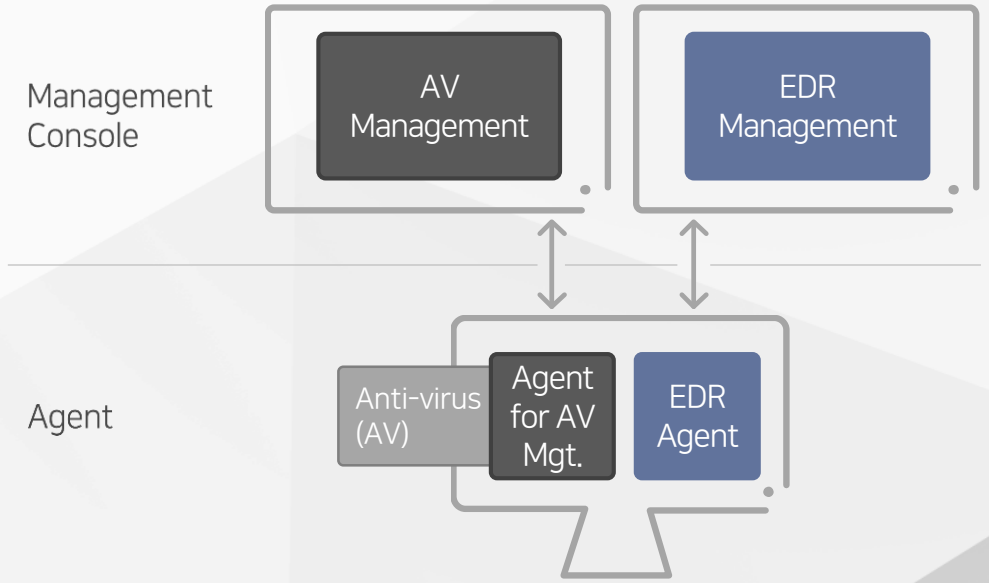
AhnLab EDR

- 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)



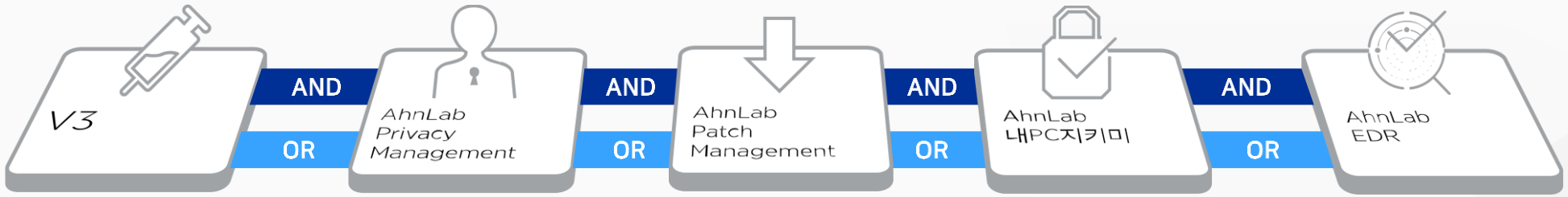
타사 EDR

- 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

AhnLab



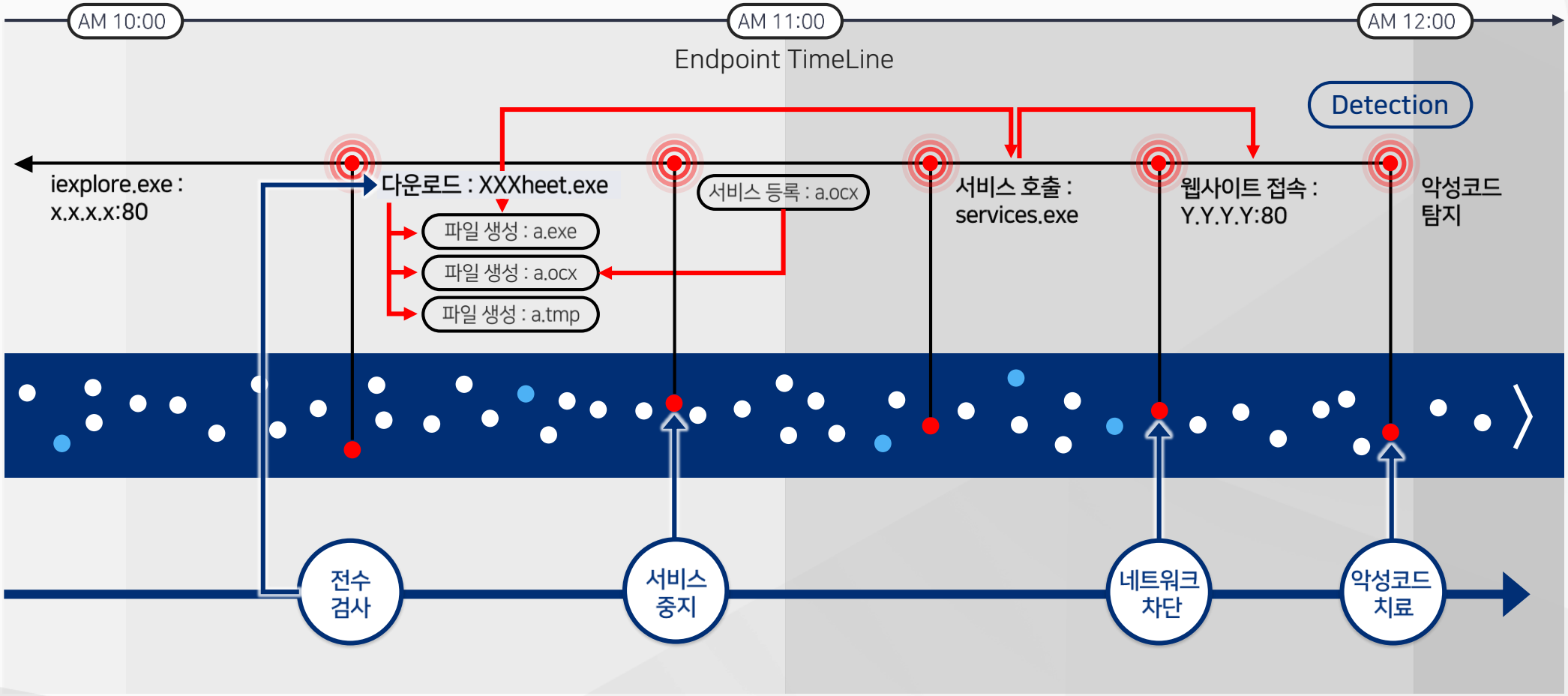
One Agent

연계 규칙 위반 시스템에 대한 순차적 대응 정책 적용

공통(관리)	V3	EDR	APM
공지사항 보내기	**V3 수동 업데이트**	**프로세스 종료**	**배포 실행**
SW/HW 정보 수집	보안 제품 배포 실행	특정 파일 수집	**전체 패치 적용**
에이전트 설치/삭제	**네트워크 완전차단**	**특정 파일 검색**	권장 패치 적용
공유폴더 정보 수집	네트워크 완전차단 해제	Artifact 수집	패치 정보 수집
공유폴더 해제	**악성코드 검사**	AhnReport 수집	소프트웨어 저작권 검사
메일 알림	시스템 최적화		특정 소프트웨어 설치
보고서 생성			

엔드포인트 가시성 확보

AhnLab



AhnLab

AhnLab Endpoint Detection & Response

분석 및 대응

- 위협에 대한 유입 경로 분석 및 대응 가능
- 국내 최고의 악성코드 분석 능력

플랫폼

- V3 기반의 안정성 및 확장성 확보
- One Agent/Single Management

진화형

- 고객 주도적 실행 보안
- 고객과 함께 진화하는 EDR

More security, More freedom

AhnLab