EDR을 통한
엔드포인트 보안 강화

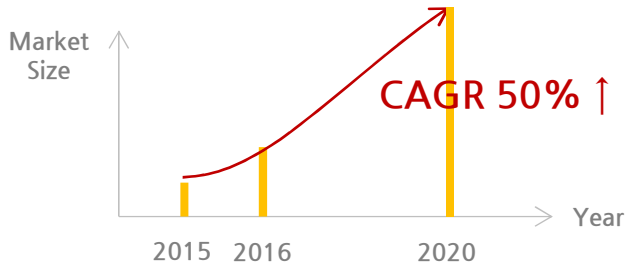
Smart Security & Service
넥스테크

Contents

EDR 시장분석 규모 및 성장

1 매출에 따른 시장 규모

- 2017년 가트너 보고서, 2015년 2억 3천만 달러에서 2016년 6억 달러로 **두배 이상 성장 추정**
- 가트너는 EDR 시장이 매년 **50% 이상의 성장률을 기록할 것**으로 예측
- 타 기관에 따르면 2016년 시장규모가 7억 5천만 달러 추정, **2020년 23억 달러에 도달할 것**으로 추정



2 배포된 EDR 엔드포인트 수에 따른 시장 규모

- 2016년 약 4천만대의 엔드포인트에 EDR 에이전트 배포
- 상위 4개 벤더의 점유율이 50% 이상을 차지

[참고자료]

- 2017.03 Gartner, Forecast Snapshot: Endpoint Detection and Response, Wolrdwide
- 2017.02 Markets And Markets: Endpoint Detection and Response Market

EDR 시장분석 제품 유형

1 From EPP (Endpoint Protection Platform)

- EPP 제품군에서 EDR 관련 기능의 추가

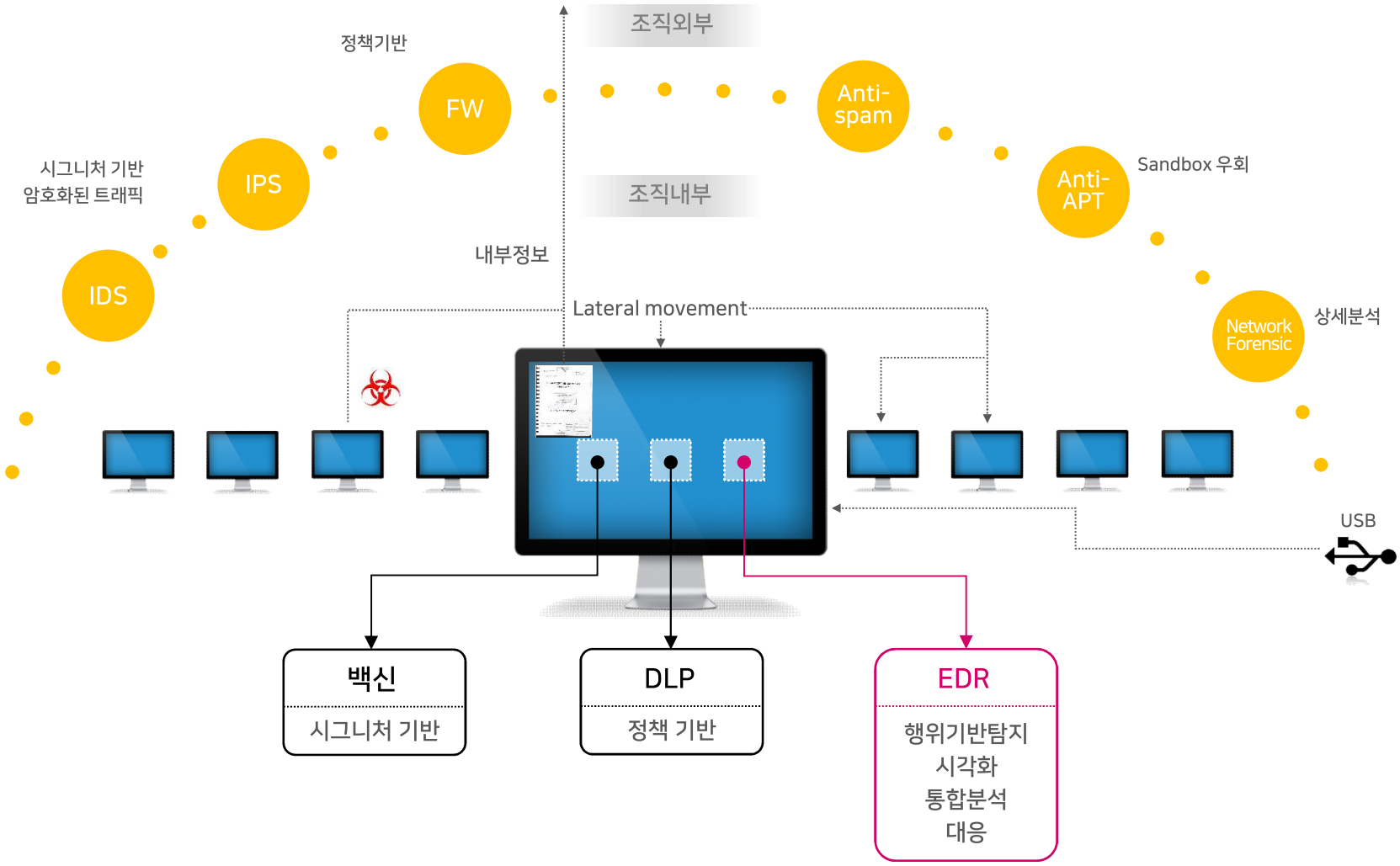
2 vs Next-generation Anti-Virus

- Signature-less 기반 악성코드 탐지
- 기존 AV 제품이 탐지하지 못하는 알려지지 않은 악성코드(Unknown Malware) 탐지
- 하지만 엔드포인트 가시성 확보 및 위협 분석 플랫폼을 제공하지 않음

3 Standalone EDR

- EDR 단독 제품 벤더들의 활약이 두드러짐
- 가볍고 빠른 에이전트와 기존 EPP 제품들과는 다른 사용자 경험 제공 (Cyber Threat Hunting 등)

새로운 보안 플랫폼의 필요성



EDR?

EndPoint

1

PC, Server

에이전트를 통한 주요 정보 수집
(파일, 네트워크, 프로세스, 레지스트리, 계정, 메모리 등)

Detection (& Analysis)

2

행위기반 탐지

머신러닝 기반 탐지

Threat Intelligence

Endpoint Threat 가시성 확보
(Cyber Threat Hunting, 실시간 모니터링)

Response

3

프로세스 차단

파일삭제

네트워크 차단

Incident Response
(사람)

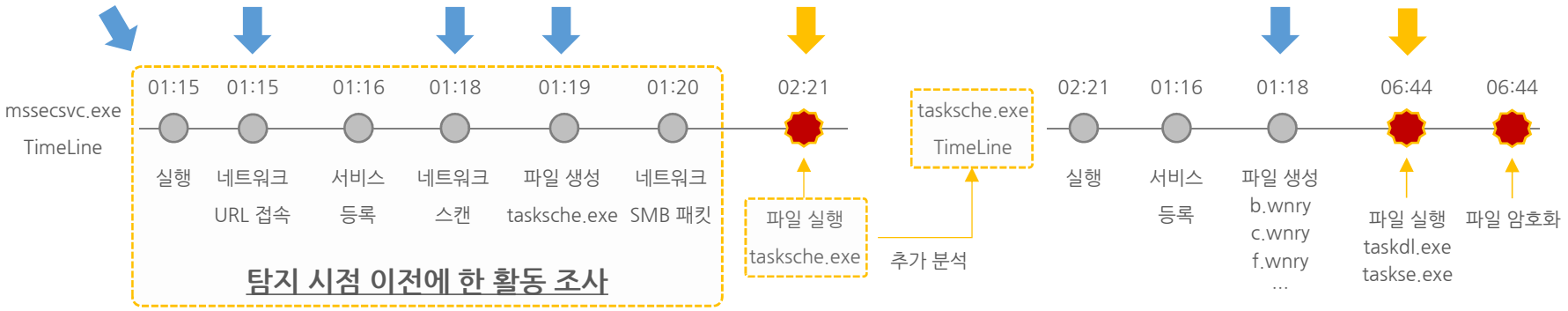
Detection (& Analysis)

1 알려지지 않은 위협 탐지

- 행위 기반의 위협 탐지
- 머신러닝 기반 탐지

2 Threat Intelligence

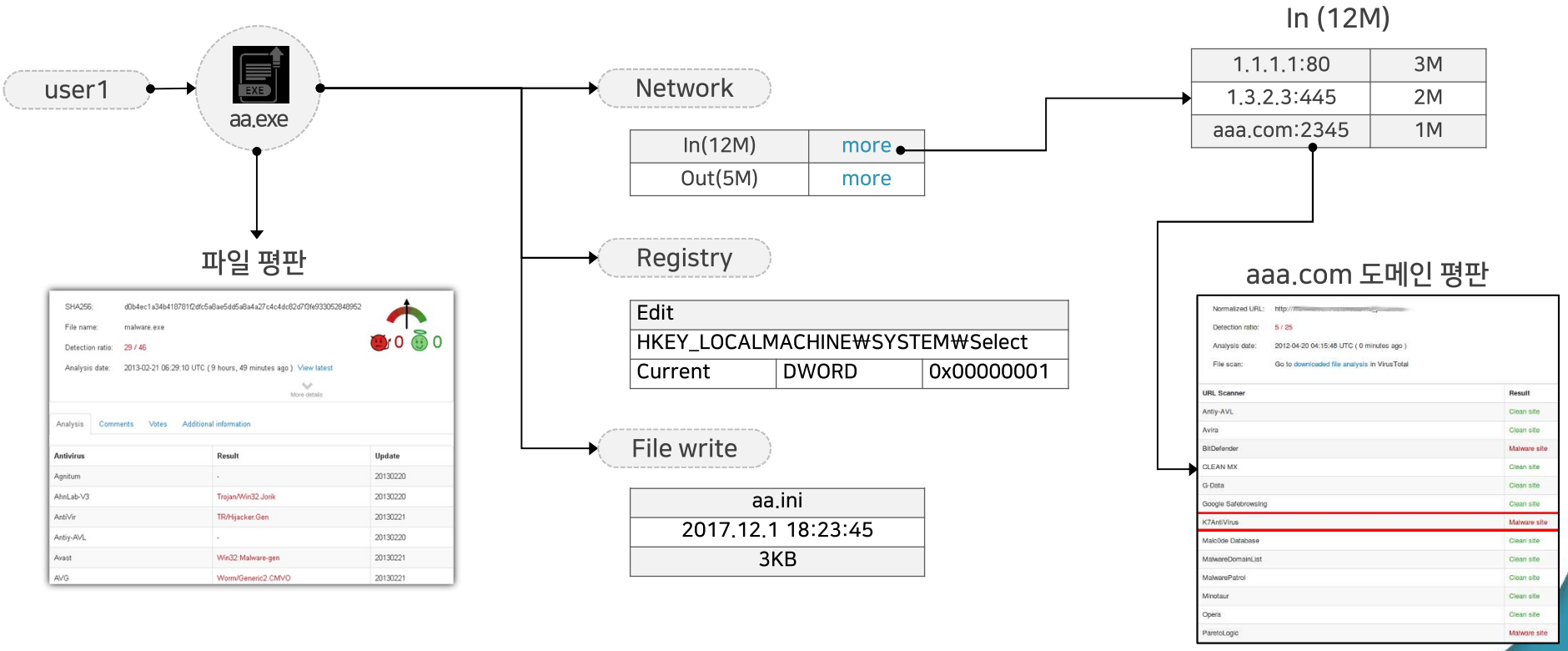
- 악성코드 해쉬값 및 악성코드 행동 정보
- IP , domain 평판 정보



Detection & Analysis

3 사이버 위협 사냥 (Cyber Threat Hunting)

- 수집된 엔드포인트 행위 데이터를 기반으로 가시성 확보
- 보안 분석 전문가가 조직내의 위협을 탐지할 수 있는 분석 플랫폼 제공



Response

1 탐지된 위협의 실시간 대응

- 위협이 탐지된 엔드포인트의 네트워크 격리, 프로세스 차단 및 삭제
- 분석을 통한 관리자 수행

2 대응 프로세스 구축

- 보안 분석 전문가가 탐지된 위협을 조사 및 분석 (사람)
- 탐지/분석 유형에 따른 대응/소명 프로세스 제공
- 유사사례 발생 시 대응 시간 최소화, 전사적 보안 인식 제고

NICSTECH EDR

1 Endpoint

- 원 에이전트 (NAC + DLP + EDR)
- 수집 : 식별 정보, HW정보, S/W정보, 사용자 정보, 프로세스/파일/레지스트리/네트워크 정보 등

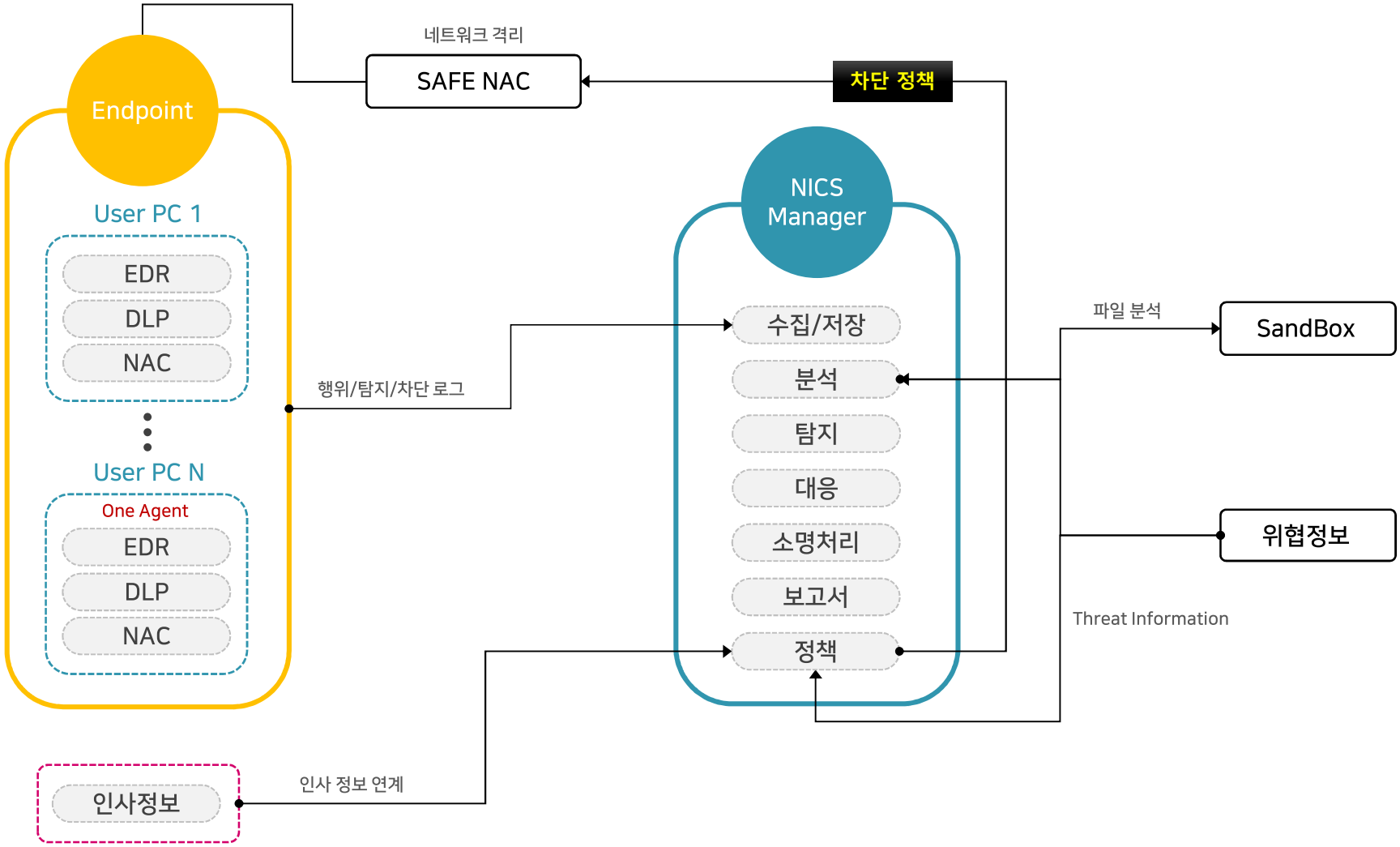
2 Detection & Analysis

- 알려진 위협 / 알려지지 않은 위협 탐지
- 이상 행위 탐지 (개인정보 오남용, 내부정보 유출)
- 룰 기반 탐지, 머신러닝 기반 탐지
- 사용자, 엔드포인트, 네트워크, 프로세스, 파일 등의 상태에 대한 가시성 확보

3 Response

- DLP, NAC 이용한 네트워크, 호스트 차단
- 악성/비정상 행위 탐지 시
  - 보안담당자에게 대응 프로세스
  - 사용자에게 소명 처리 프로세스

NICSTECH EDR 시스템 구성도



엔드포인트 위협 가시성 확보

행위 기반 위협 탐지 (내부정보유출 포함)

체계적 대응 시스템