기업 정보보호 이슈 전망

CONCERT FORECAST 2018

Prevent
Detect
Response

변화하는 기술 적용 / 엔드포인트 보안의 방향성

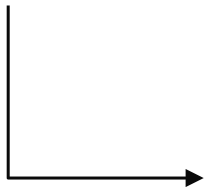
CYLANCE™

PAGO NETWORKS

공격(악성) 주체 – MALxx with File-xx Attack

MALware

MALicous Activities



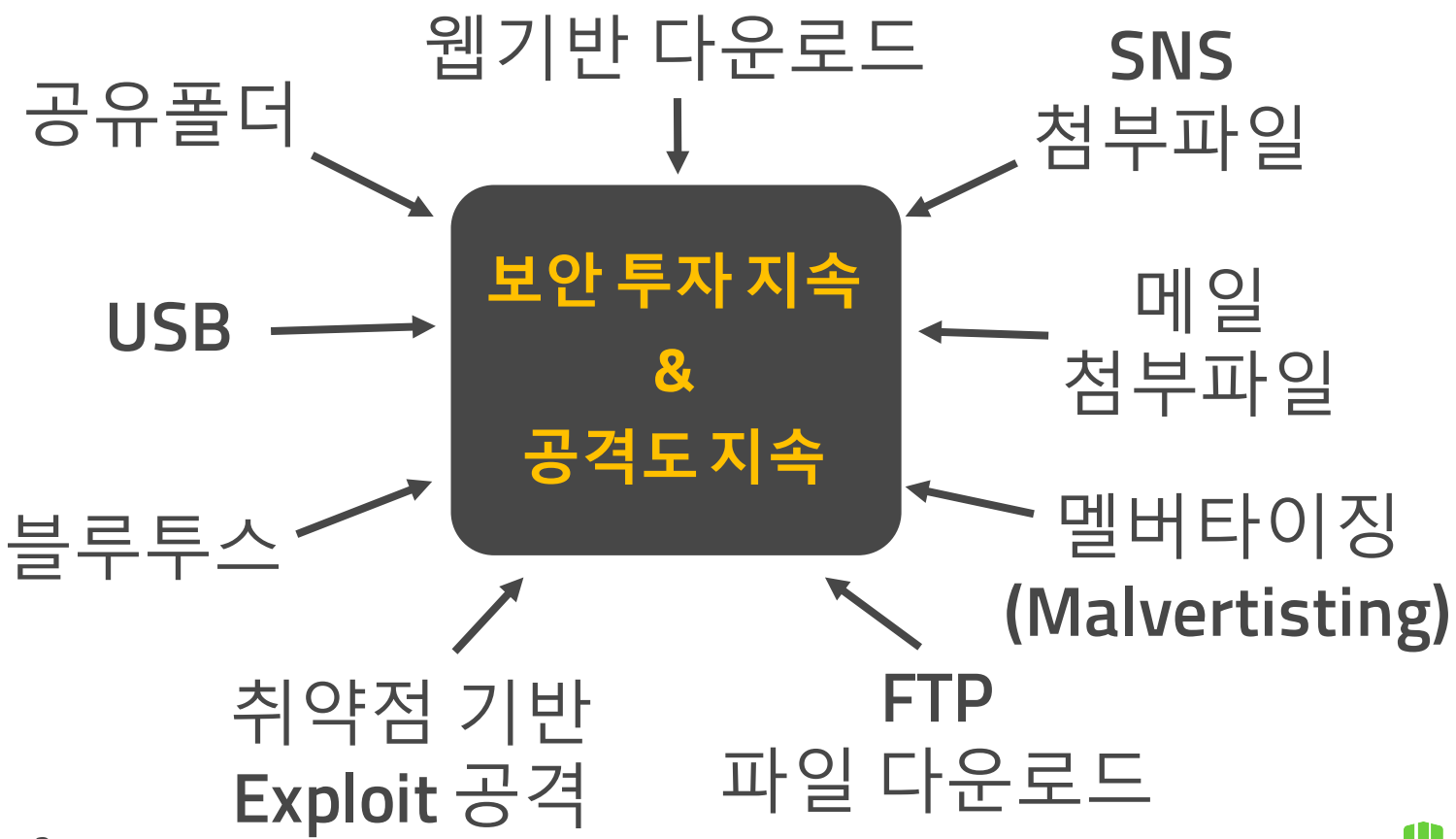
with File-based Attack

File-less Attack

* 발표자 주
  - 사용자에 의한 보안위배 활동은 주제에서 논외로 합니다.
  - "Insider Threat" 또는 "User Behavior-based Threat" 보안 영역에 더 적합합니다.

CYLANCE PAGO networks

MALxx 방어 위한, 보안 투자 위치는 ?



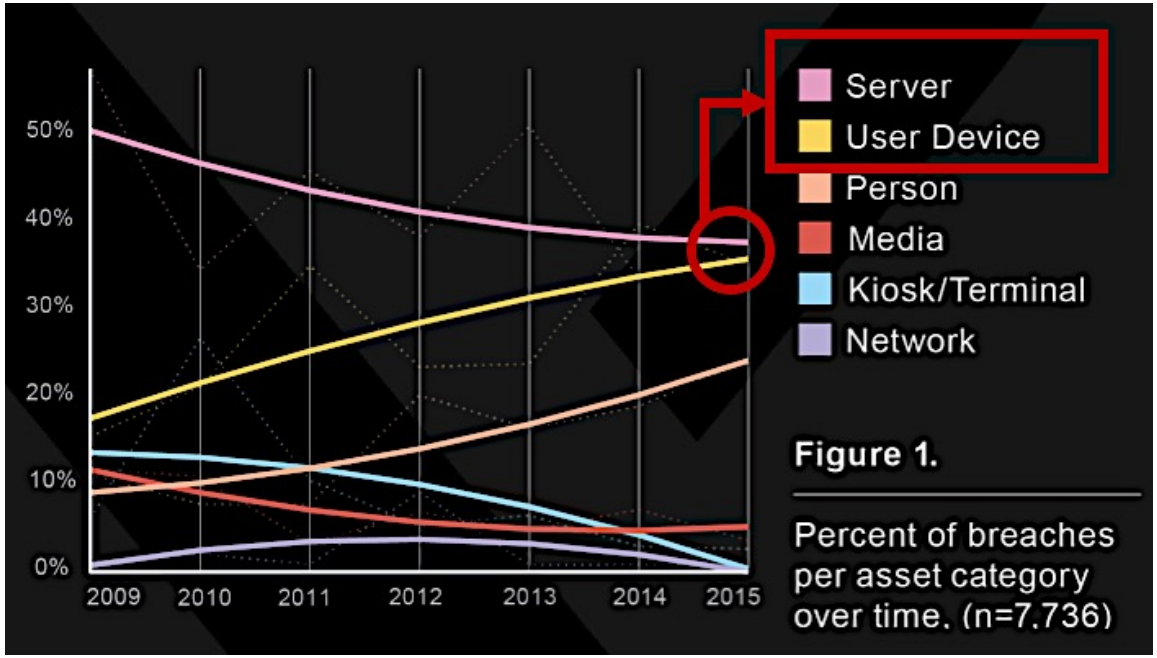
MALxx
유입 경로
방어 강화 ??

(또는)

MALxx
활동
종착 지점
방어 강화 ??

CYLANCE PAGO networks

보호를 강화해야 할, 공격 대상 – “Endpoint”

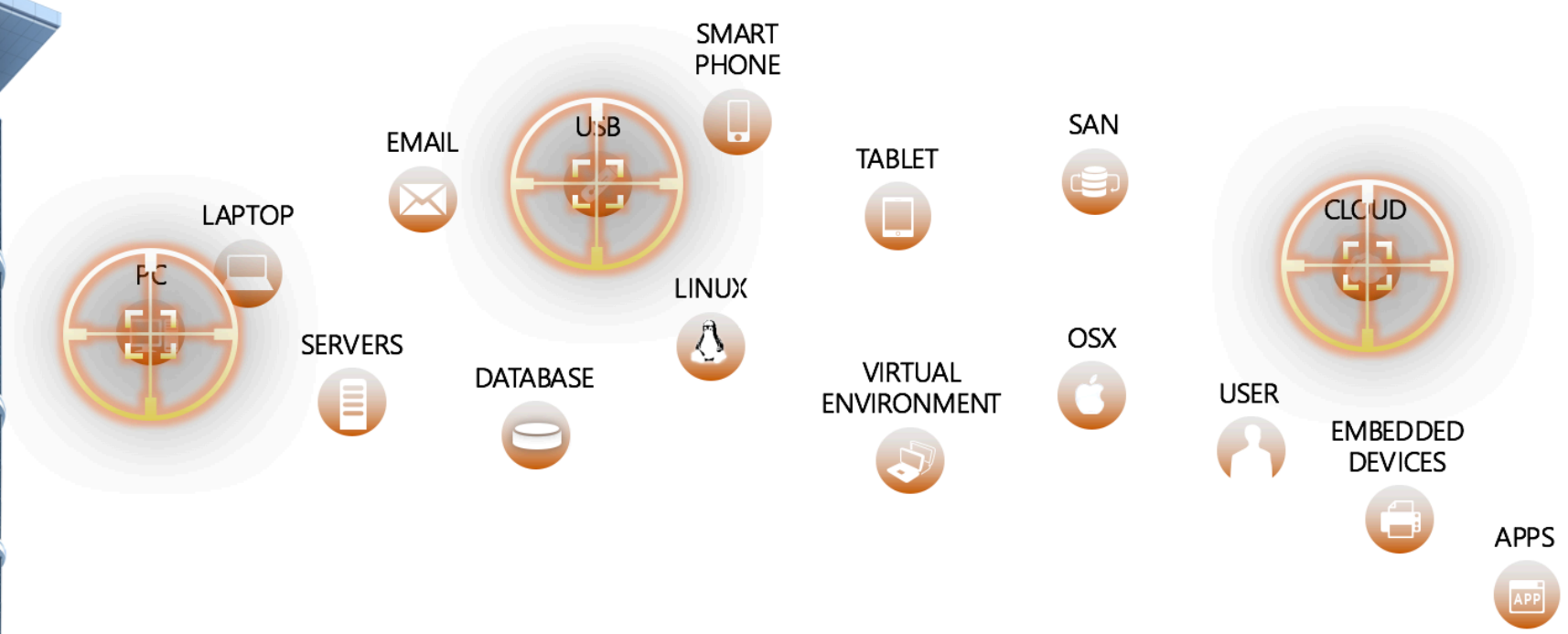


Endpoint
개념/범위 확대

Server
+
PC

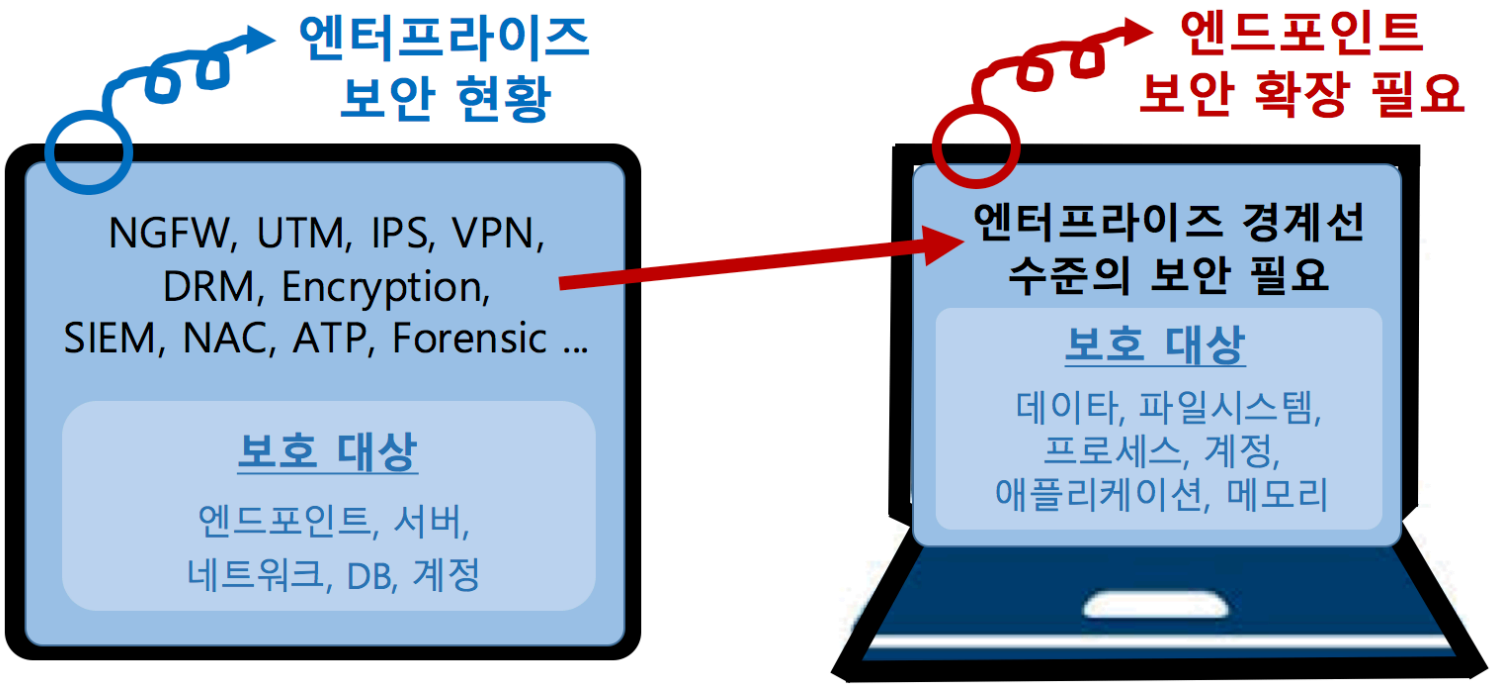
CYLANCE PAGO networks

“Endpoint” 위치 - 더 이상 논제가 아닙니다



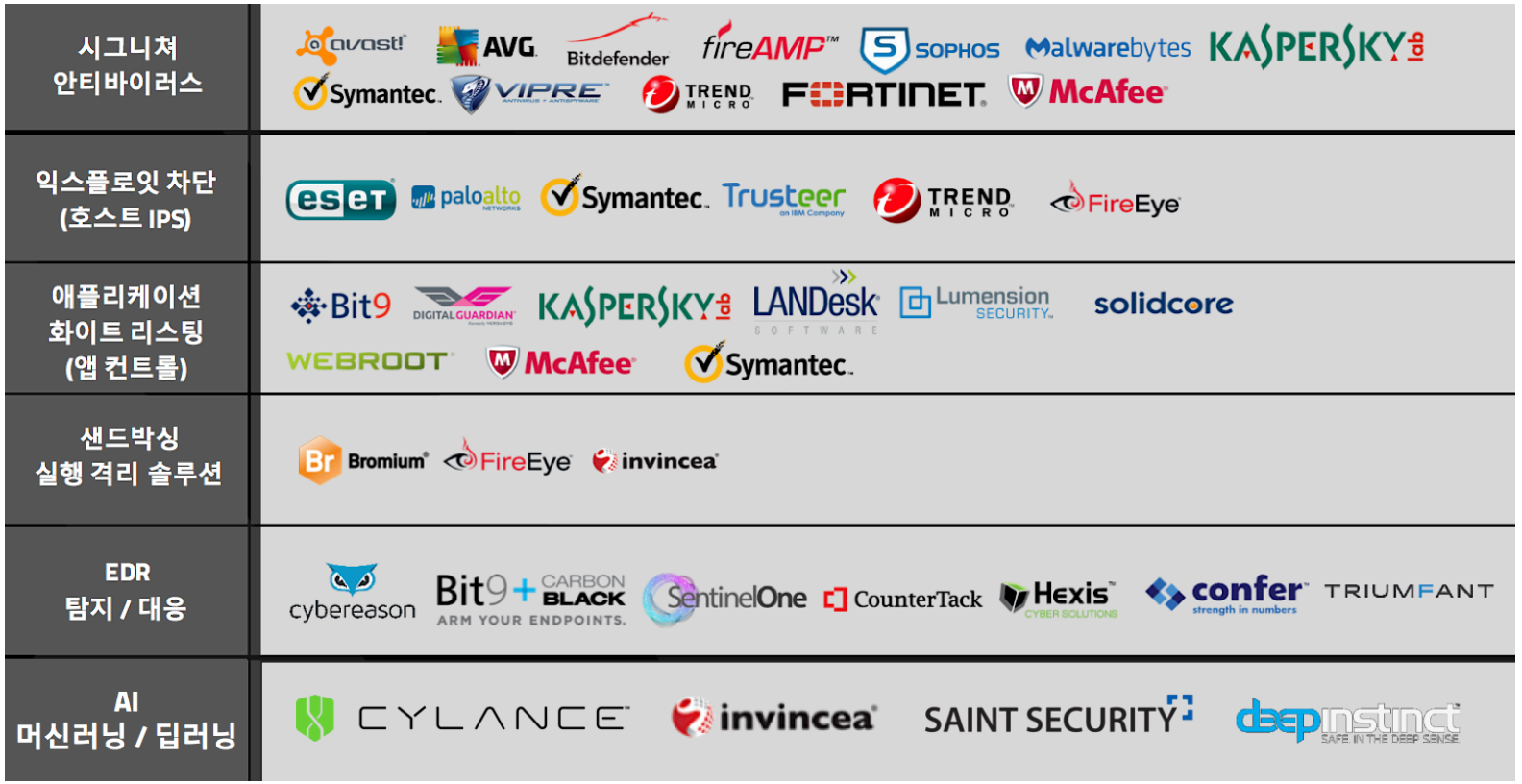
CYLANCE™ PAGO networks

“Endpoint” 보안 – 크기만 작은 엔터프라이즈



CYLANCE PAGO networks

"엔드포인트" 보안 기업 (예) - VS. MALxx



* **발표자 주** - 상기 기업 이외에도 많은 기업의 보안 솔루션이 있습니다.

CYLANCE PAGO networks

"엔드포인트" 보안기술 트렌드 - VS. MALxx

잠시 생각해 보겠습니다

Prevent 기술 경쟁? 공존? **Detect & Response 기술**

시장 벤더 측면

EPP 벤더 **경쟁!** **EDR 벤더**

Endpoint **Prevention** Platform

Endpoint **Detection** & **Response**

"시장의 논리입니다 !!!"

CYLANCE PAGO networks

EPP – 기술 출현 과정 / 현재 시장 상황

(Endpoint Prevention Platform)

Anti-Virus + **Endpoint ATP**

EPP (Endpoint Prevention Platform)

멀티레이어 보안 (기존 AV 기반, EPP)	인공지능 (AI, EPP)	확장 (EPP의 인수합병 / 자체개발)
- 시그니쳐 - 안티익스플로잇 - 행위기반 - Cloud 샌드박스 - 휴리스틱 - 평판조회 - BAD URL **- 머신러닝 추가**	**- 머신러닝** **- 딥러닝**	- 멀티레이어 보안 EPP **+ 머신러닝 EPP** 합병 **+ EDR 개발** - 멀티레이어 보안 EPP **+ EDR 합병** - 머신러닝 EPP **+ EDR 개발**

CYLANCE PAGO networks

EPP – 최근 움직임 [2017년 ~]

(Endpoint Prevention Platform)

Main 기술

"EPP"

머신러닝 기술
대부분 보유

"For Un-Known"

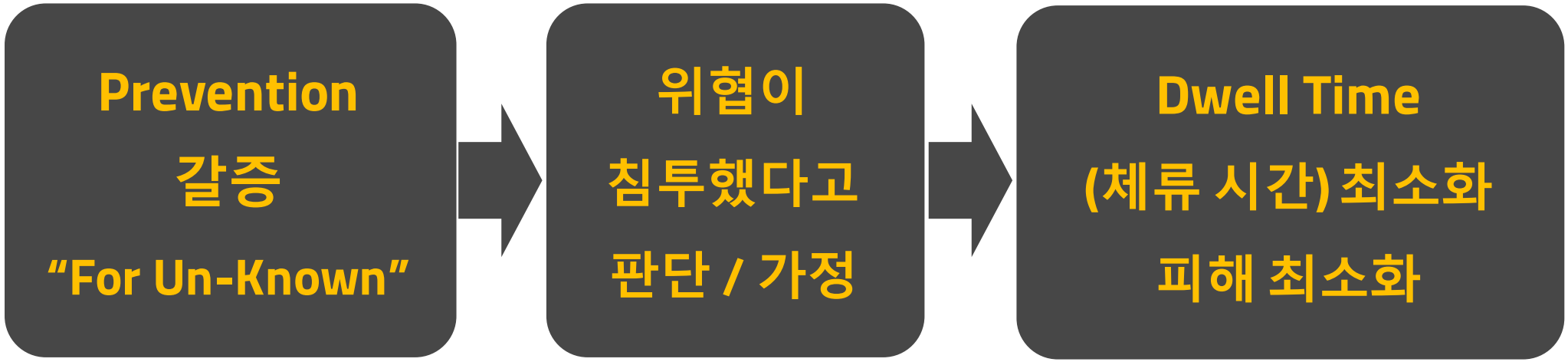
추가 방향성

"EDR"

"File-less 공격 대비"
"Unknwon 행위기반
공격 대비"

CYLANCE PAGO networks

EDR – 기술 출현 배경 (시장 요건)
(Endpoint Detection & Response)



CYLANCE PAGO networks

EDR – 정식 기술 명명
(Endpoint Detection & Response)

2013년 6월

Anton Chuvakin – 가트너 시니어 애널리스트

ETDR (Endpoint Threat Detection & Response)

After a long *agonizing* process that involved plenty of conversations with vendors, enterprises and other analysts, I have settled on this generic name for the tools primarily focused on detecting and investigating suspicious activities (and traces of such) other problems on hosts/endpoints: Endpoint Threat Detection & Response.

2014년 11월

가트너 공식 리서치 발표 (EDR로 정식 명명)

EDR (Endpoint Detection & Response)

Gartner®

CYLANCE PAGO networks

EDR – 가트너 정의 (2014년 11월)
(Endpoint Detection & Response)

- **Continuous detection and response to advanced threats**
- Security monitoring, **threat detection** and **incident response**
- **Record** many detailed endpoint and network events
- **Store** all information in a centralized DB
  for deep detection analysis, investigation reporting and alerting
- **Analytic** tools are used to continuously search
- **Early identification** of ongoing threats
- **Rapidly respond** to detected attacks

CYLANCE PAGO networks

EDR – Detection / Response 의미 이해
(Endpoint Detection & Response)

Detection → **Response** → **Remediation (Action) "EDR 관점"**

- Advanced Threats
- On-going Threats

- IR (Incident Response)
- Forensic

- Alerting
- Kill Process
- Quarantine Device
- Remove File

- SIEM 연동 / 검색 / 대쉬보드 / 레포팅
- 외부 Threat Intelligence 연동

CYLANCE PAGO networks

EDR – 도입 효과는 ?
(Endpoint Detection & Response)

- **Endpoint** 위협 가시성 확보 **(확장)**
- 새로운 개념의 실시간 대쉬보드 **(SIEM** 연동의 확장**)**
- **File-less Attack** 대응 **(**행위 기반**)**
- **Un-Known Attack** 대응 **(**행위 기반**)**

- **그런데, EDR만으로도 10% 모자랍니다 !!!**
  Incident Response (사후 처리)이므로 !!!

CYLANCE PAGO networks

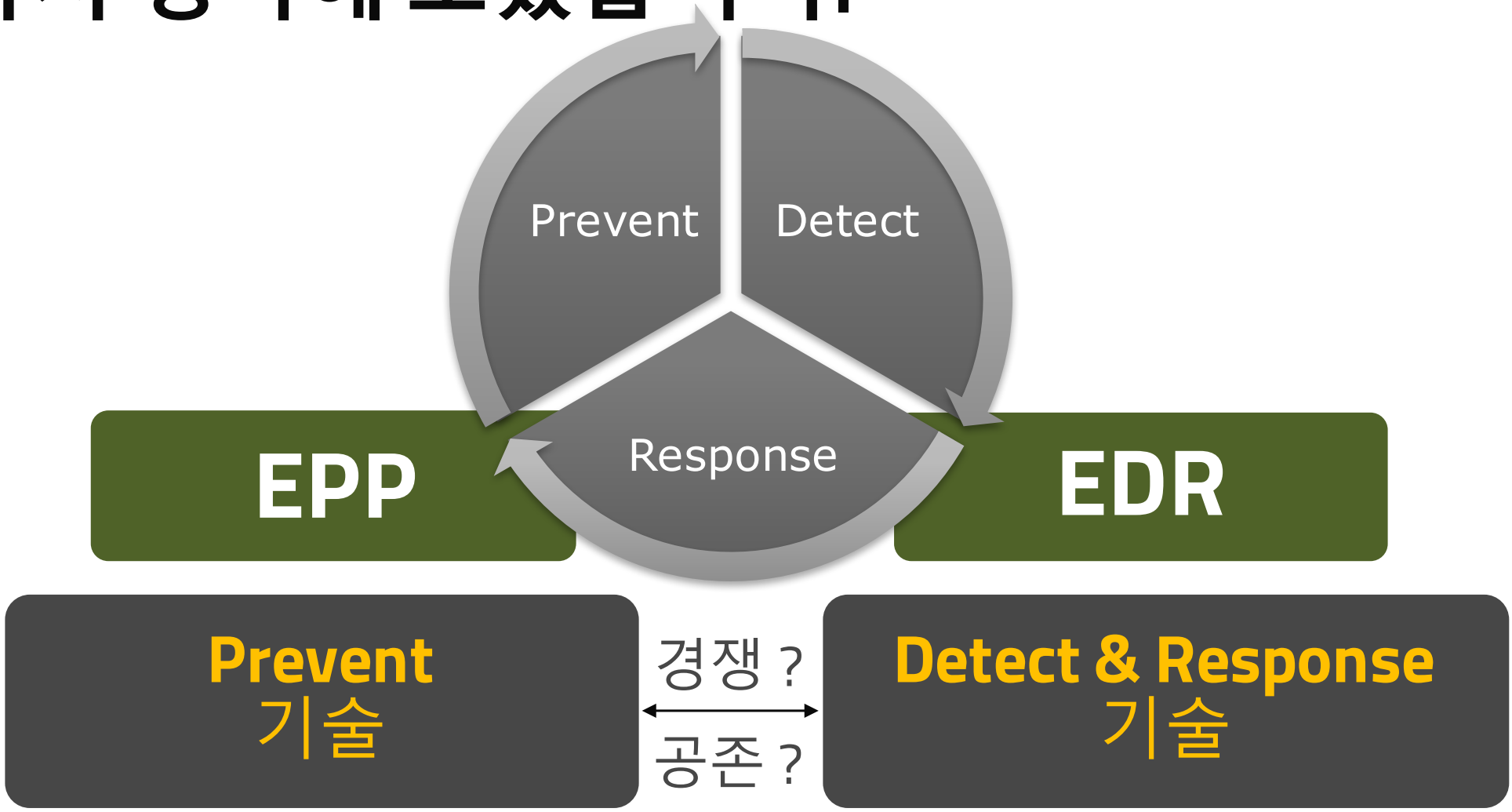
EDR – 최근 움직임 [2017년 ~]

(Endpoint Detection & Response)

Main 기술	추가 방향성
"EDR" 엔드포인트 상관분석 "For Un-Known"	"EPP" "10% 모자라는 부분에 대한 갈증 해소"

CYLANCE PAGO networks

다시 생각해 보겠습니다.


Prevent
Detect
Response
EPP
EDR
Prevent
기술
경쟁 ?
공존 ?
Detect & Response
기술

Prevent + Detect + Response 공존 가능

엔드포인트 보안을

강화할

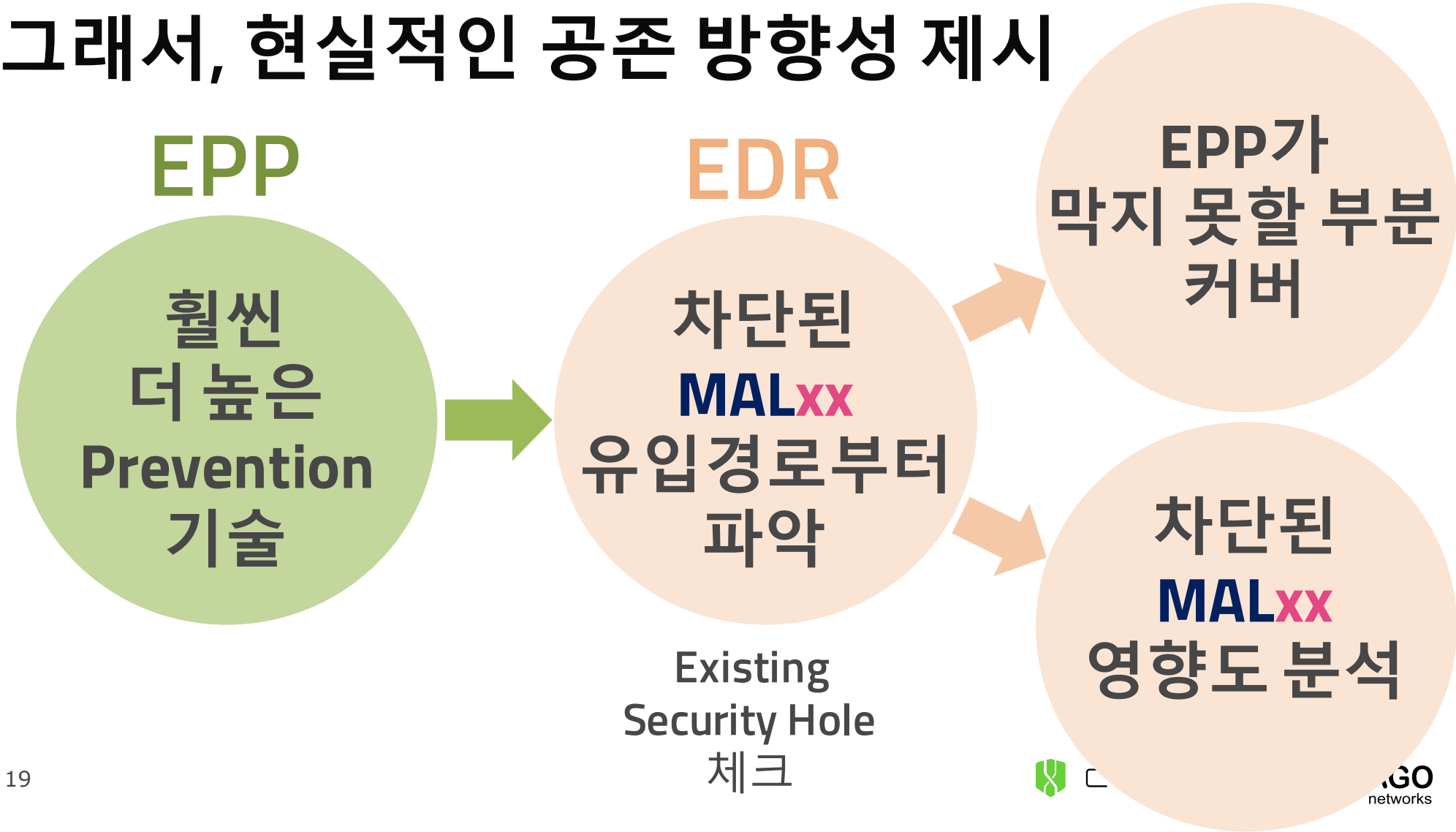
우선 순위는?

현재 엔드포인트 보안 시장

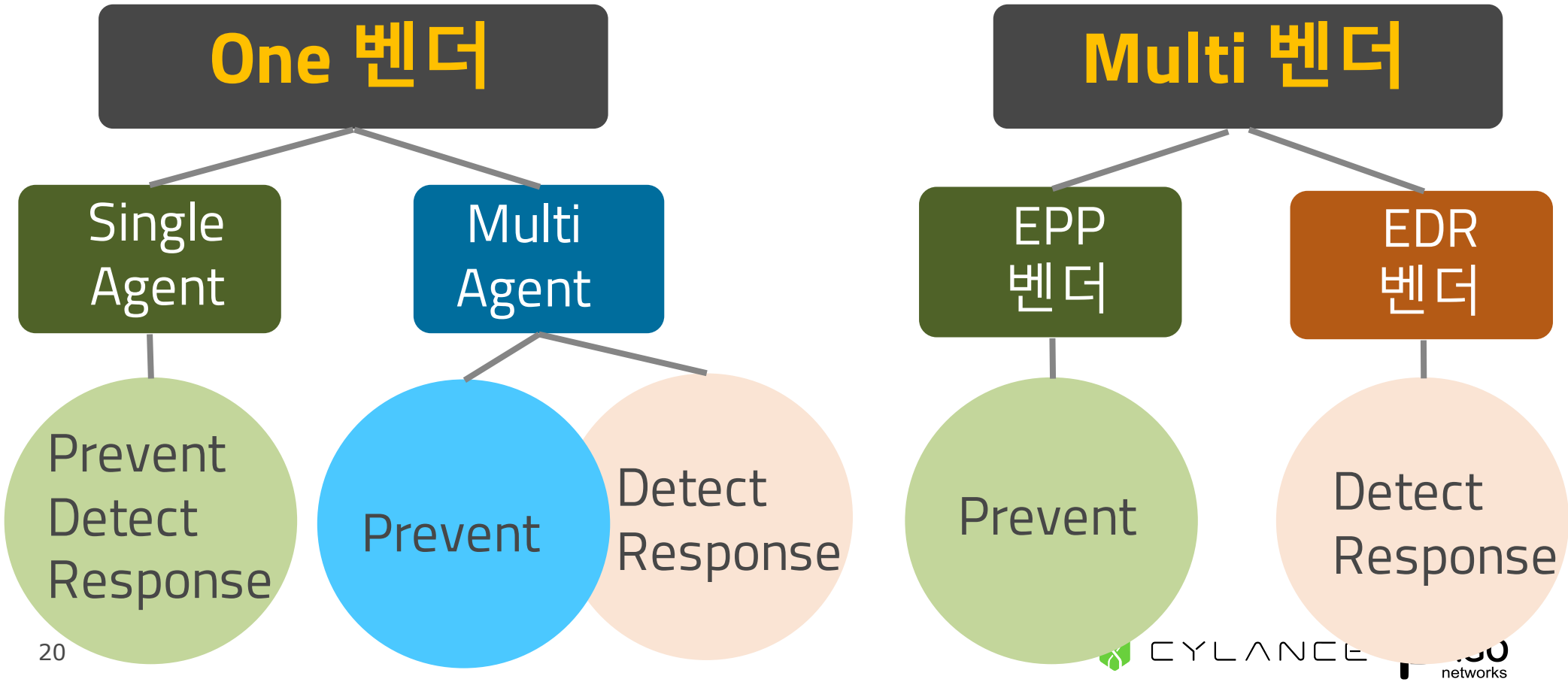
"춘추전국시대"

CYLANCE PAGO networks

그래서, 현실적인 공존 방향성 제시



EPP + EDR 구성 방안 (다양한 케이스)



EPP + EDR 동시 구성, 현실적 고려 사항

예상 가능한 고려사항

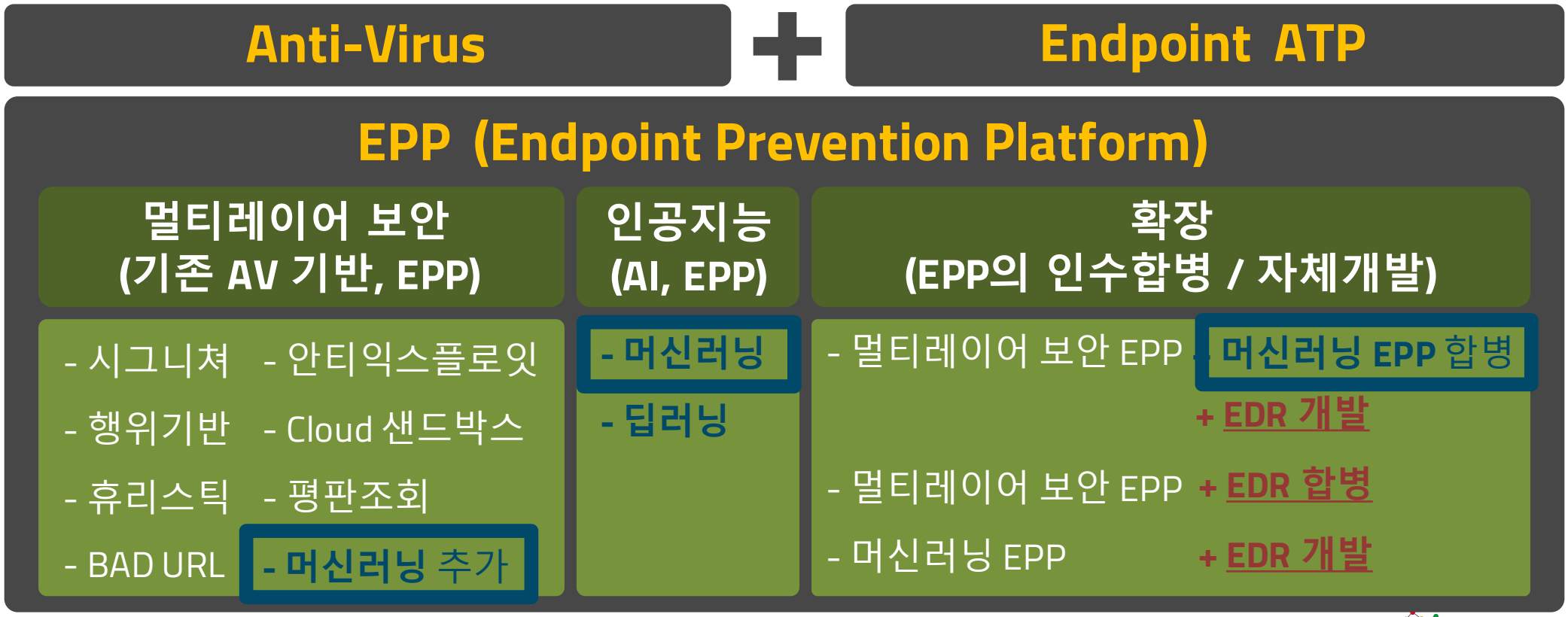
- 무거워 지고,
- 이슈가 많아지고,
- 비용이 많이 늘어나고,

현실적인 요건

- 성능 이슈 ⬇
- 충돌 이슈 ⬇
- 비용 이슈 ⬇

CYLANCE PAGO networks

주목해야 할 엔드포인트 보안 기술 (머신러닝)



CYLANCE PAGO networks

머신러닝이 탐지/차단하는, MALxx

차단 대상
for More Prevention

랜섬웨어	바이러스	다운로더	드롭퍼
백도어	익스플로잇	루트킷	트로얀
웜	봇	리다이렉터	패스워드 크랙툴
키로거	스크린샷툴	키젠 크랙툴	게임핵 툴
전자화폐 채굴 멀웨어	애드웨어	툴바	포터블 툴

Vs.

머신러닝 적용된
EPP

스코어링 기반

예측 기반

CYLANCE PAGO networks

엔드포인트 보안, 머신러닝 적용 의미

- 시그니쳐
- 휴리스틱
- URL 블랙리스트

For Known MALxx

- 행위기반
- 평판조회
- 안티익스플로잇
- 클라우드 샌드박스
- **머신러닝**
- 주기적인 작동
  - 시그니쳐 업데이트
  - 풀스캐닝

For Un-known MALxx

인공지능 / 머신러닝

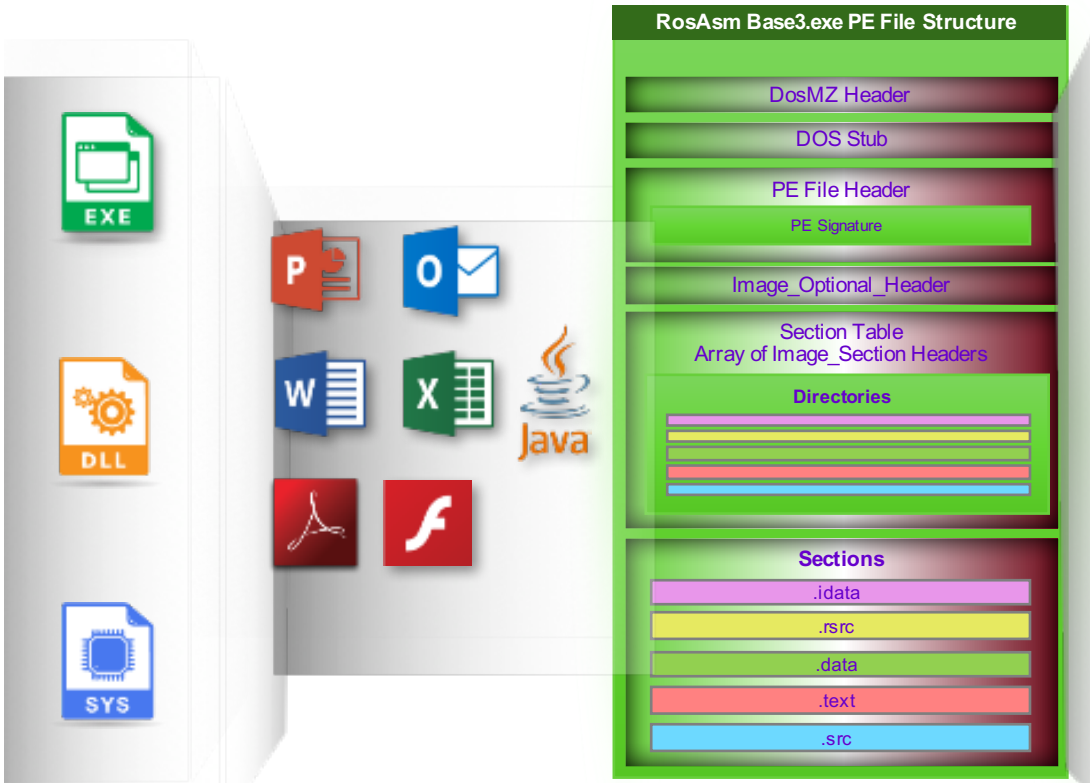
- 멀티레이어 보안 + 머신러닝
- 머신러닝 Only

- **Known**
- **Un-Known**

상관없이
방어하는 것이 목적

CYLANCE PAGO networks

머신러닝 기술 1



DOS Header
NT Header
File Header
Section Headers
Export Directory
Import Directory
Resource Directory
Relocation Directory
Debug Directory
Packer Used
Compiler Type
Compiler Language
File size
PE size
Image section headers
Image imports
Functions called
Kernel hooks
Image Paths
Image Resource Directory
Bitmaps
Icons
Strings
RCData
Icon Groups
Version Info

```
lea     rcx,[rdi+20h]
mov     qword ptr [rdi+8],r13
mov     qword ptr [rdi+10h],r13
mov     qword ptr [rdi+18h],r13
mov     qword ptr [rcx+20h],r12
mov     qword ptr [rcx+18h],r13
lea      rdx,[rsp+258h]
or       r9,0FFFFFFFFFFFFFFFFh
xor      r8d,r8d
mov     word ptr [rcx+8],r13w
mov     ebx,r14d
```

CYLANCE
PAGO networks

머신러닝 기술 2

- **DOS Header**
- NT Header
- File Header
- Section Headers
- Export Directory
- Import Directory
- **Resource Directory**
- Relocation Directory
- Debug Directory
- Packer Used
- Compiler Type
- **Compiler Language**
- File size
- PE size
- Image section headers
- Image imports
- **Functions called**
- Kernel hooks
- Image Paths
- Image Resource Directory
- Bitmaps
- Icons
- Strings
- RCData
- Icon Groups
- Version Info

```
lea     rcx,[rdi+20h]
mov     qword ptr [rdi+8],r13
mov     qword ptr [rdi+10h],r13
mov     qword ptr [rdi+18h],r13
mov     qword ptr [rcx+20h],r12
mov     qword ptr [rcx+18h],r13
lea      rdx,[rsp+258h]
or       r9,0FFFFFFFFFFFFFFFFh
xor      r8d,r8d
mov     word ptr [rcx+8],r13w
mov     ebx,r14d
```

• **x**=[1007013456] **X**

Matrix

x=[1602111430]
x=[2819209111]
x=[3220101036]
x=[9910192839]
x=[2201920391]
x=[8819102999]
x=[5778492200]
x=[0001928311]
x=[7564778203]
x=[9928183918]
x=[9929192839]
x=[0019376471]
x=[0093810292]
x=[0019102922]
x=[6657749100]

$$\frac{e^{a+bX}}{1+e^{a+bX}} = P$$

Unsafe

Safe

CYLANCE

PAGO networks

머신러닝 기술 3

아래 사진은 무엇입니까? **(멀웨어 분석 관점에서 살펴보겠습니다)**

CYLANCE PAGO networks

머신러닝 기술 4

아래 사진은 무엇입니까? (멀웨어 분석 관점에서 살펴보겠습니다)

플랜테인
(Plantains)

플랜테인	바나나
채소	과일
풀 맛	단 맛
바나나보다, 크다	플랜테인보다, 작다
두꺼운 껍질	얇은 껍질
검정색 → 녹색 → 노란색	녹색 → 노란색

CYLANCE PAGO networks

머신러닝 기술 (스코어링 샘플 1)

짧은 머리, 문신, 파란 반바지 **(Un-Known 파일 2개 처리 과정)**

Vs.

스코어링 = 15

스코어링 = 100

CYLANCE PAGO networks

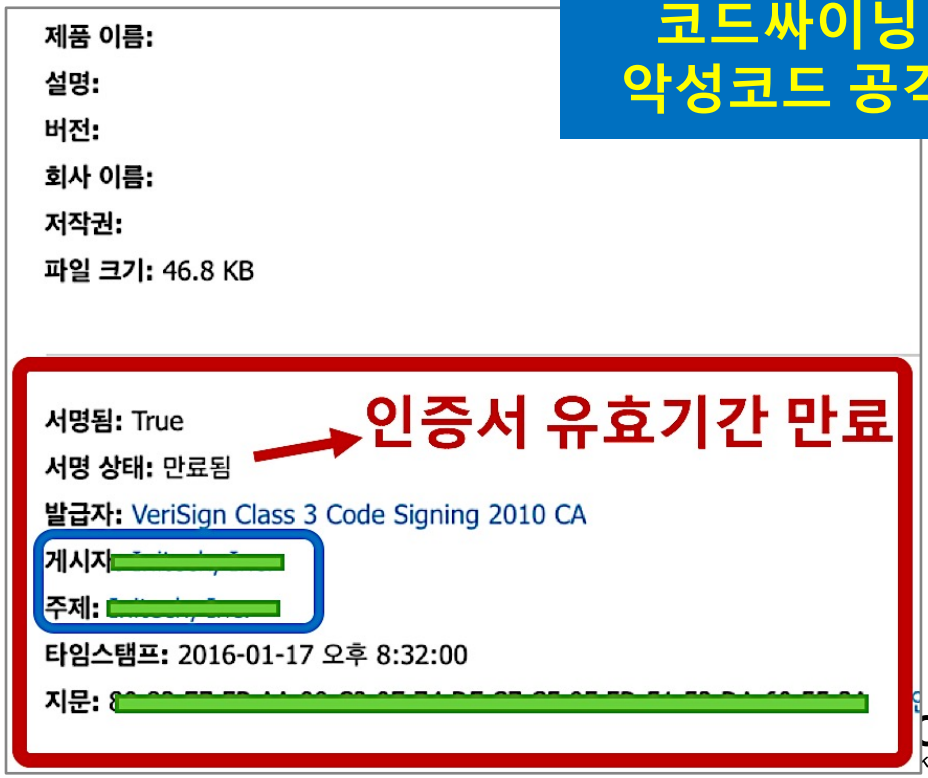
머신러닝 기술 (스코어링 샘플 2) – 오탐 ?

파일1 – Un-Known

정상적인
보안 SW

파일2 - Unknown

보안 SW
"인증서 탈취"
코드싸이닝
악성코드 공격



머신러닝 기술 (스코어링 샘플 3)

기존 "멀티레이어 보안 – No 머신러닝"	머신러닝 엔드포인트 대응
• **1차 백도어 사용** - 일부 백신 시그니처 보유 => 2017.09.25 시그니쳐, (VT-43/64) - 고객사 기존 AV도 시그니처 보유 (abc.JPG) → **(AV 입장 : Known)**	→ **탐지 / 격리 성공**
• **2차 백도어 사용 (Un-known)** - 일부 백신 시그니처 보유 => 2017.09.25 시그니쳐, (VT-14/63) - 단, 고객사 기존 AV 시그니처 없음 (abc.EXE) → **(AV 입장 : Un-known)**	→ **탐지 / 격리 성공**
• **3차 백도어 사용 (Un-known)** - 모든 백신에서 시그니처가 없도록, 멀웨어 자체 제작 : 의도적으로 코드벡터 수정 및 Unknwon 으로 생성 - 악성툴의 "특정 문자 스트링" 1개 수정 : **DoS mode → DtS mode**	→ **탐지 / 격리 성공**
• **4차 백도어 사용 (Un-known)** - 백신 시그니처도 없지만, 추가적인 회피 기능 추가한 멀웨어 제작 : 의도적으로, 샌드박싱 / VM 환경의 분석 방해 기능 추가 : 샌드박싱 / VM 회피 기능	→ **탐지 / 격리 성공**

머신러닝 기술 – 살펴볼 사항 (고려 사항)

- **Pretict (예측 기반)**
- **Scoring (스코어링 기반)**
  - **머신러닝은 만능 기술이 아닙니다.**
    - ✓ EPP / EDR (NW 보안에 적용된 모든 머신러닝 기술 포함) 상관 없이
    - ✓ 예측 기반 스코어링
  - **판단 (Judgement Staff) 필요**
    - ✓ "악성코드 같아요 (looks like malware)"
    - ✓ 전천후, 자동 시스템이 아님
    - ✓ 최종적으로 한번 더 들여다 봐야 할,
      "파일 (특히 Un-Known)"을 골라 줌

CYLANCE PAGO networks

CONCERT FORECAST 2018 – "발췌 내용"

"'자동화'라는 말에 꽂혀서 도입을 결정했던 것이 결정적인 실수였어요. 많은 부분이 자동화가 되어 있고, 인텔리전스를 이용해 알아서 해주는 부분이 많이 있지만, 어쨌거나 발생하는 모든 상황에 대해 최종적인 판단은 사람이 해야 한다는 사실을 미처 생각하지 못했습니다. 같은 실수를 되풀이하지 않기 위해 올해 사업계획에서는 이를 운용할 인력을 가장 먼저 확보했습니다."

CYLANCE PAGO networks

“EPP에 적용된 머신러닝 / EDR” 공통 고려 사항

- 내부 운용 인력

(또는)

- 외부 제안사/제조사 서비스

CYLANCE PAGO networks

신규 리서치 (EMA – NGES)

신규 리서치 (EMA – NGES)

NGES (Next-Generation Endpoint Security)

Prevent + **Detect** + **Response**

- No 시그니쳐 기반
- No 패턴 기반

- ProActive Detect
- **Alert / Notification 에 대해서는 "별도 팀이 대응" 해야만 함 (Let someone know)**

CYLANCE PAGO networks

신규 리서치 (EMA – NGES : 요건

- Prevention / Detection 의 통합 서비스
- Threat Hunting / Forensic 기능
- 관리자에 의한 엔드포인트 검색 / 관리 기능
- NGES 소프트웨어 중앙 업데이트 (타 배포 솔루션 사용 가능)
- 모든 엔드포인트 상태를 중앙 콘솔에서 관리
- 중앙 데이터 수집 / 위협 분석
- 실시간 / 거의 실시간 – 위협 대응 기능
- 변종 / APT / 타겟 공격, 제로데이 또는 취약점 기반 등장하는 공격 식별
- 엔드포인트 공격 / 침투 발생 시, 보안 담당자가 감지할 수 있는 컨텍스트 제공
- Incident Response 개념의 Mitigation 기능 제공
- 운영 / 관리 기반의 레포팅

"발표자 정리"

- **더 효율적인 Prevention > Detect > Response**

- **One 벤더 / Multi-벤더 상관없이**
  - 성능 이슈 최소화
  - 충돌 이슈 최소화
  - 비용 이슈 최소화
  - 보안 성능 최대화

그리고

"전문 Team"

"전문 Service"

CYLANCE PAGO networks

기업 정보보호 이슈 전망

CONCERT FORECAST 2018

Q&A

기업 정보보호 이슈 전망

CONCERT FORECAST 2018

PAGO NETWORKS

(주) 파고네트웍스

- 영업 문의 : sales@PAGOnetworks.com
- 기술 문의 : tech@PAGOnetworks.com