SAMSUNG SDS

2019 . 5 . 8 . Wed . The Shilla Seoul

차세대 엔드포인트 보안요건

안호근 프로

Agenda

- 왜 엔드포인트를 강화해야 하나
- 기존 엔드포인트 방어체계의 한계
- 엔드포인트 보안의 요건
- 제안 솔루션
- Q & A

엔드포인트란?

엔드포인트의 정의

- 네트워크의 끝 단에 위치한 단말/디바이스
- 데이터 접근/처리/저장
- PC, 서버, VDI, Cloud, 모바일 등

엔드포인트의 중요성

- 해커의 최종 목적지 & 우리의 최종 방어선
- 다양한 침투경로 (USB, 피싱, 악성 이메일/URL)
- 악성행위가 실제로 발생하는 곳

→ 해커의 의도를 가장 잘 파악할 수 있는 위치

왜 엔드포인트 보안을 강화해야 하나?

네트워크 경계보안 vs 엔드포인트 보안

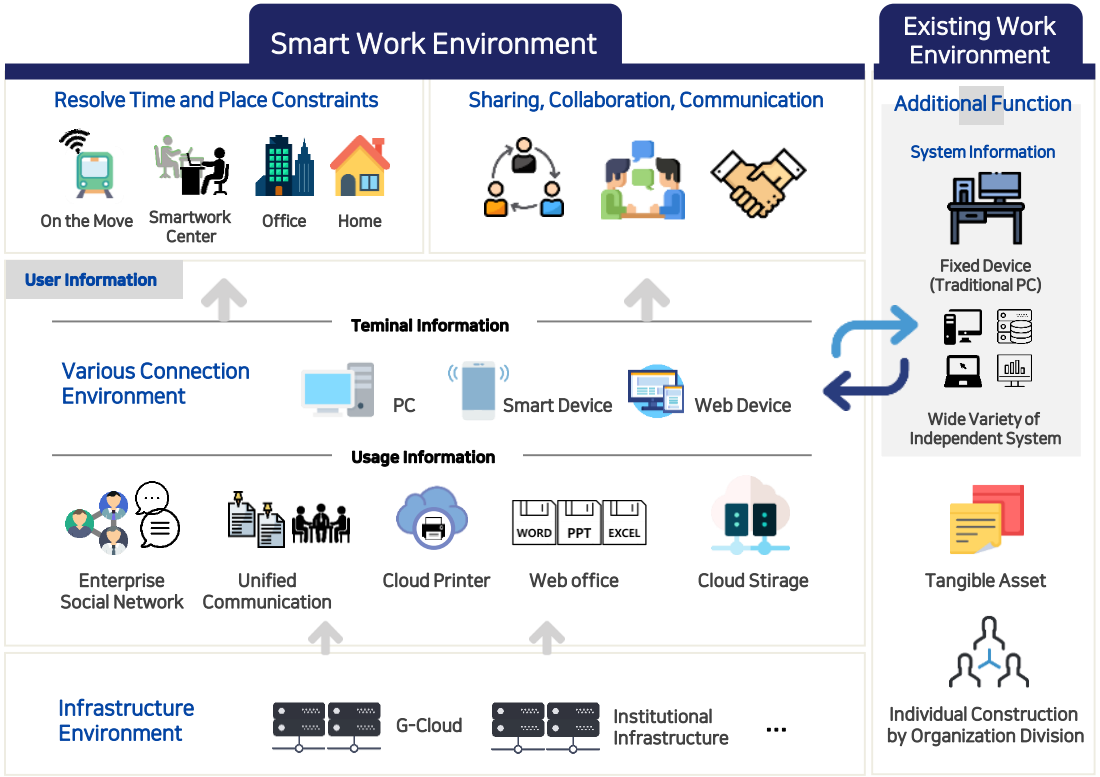
1. 사라지는 네트워크 경계

과거

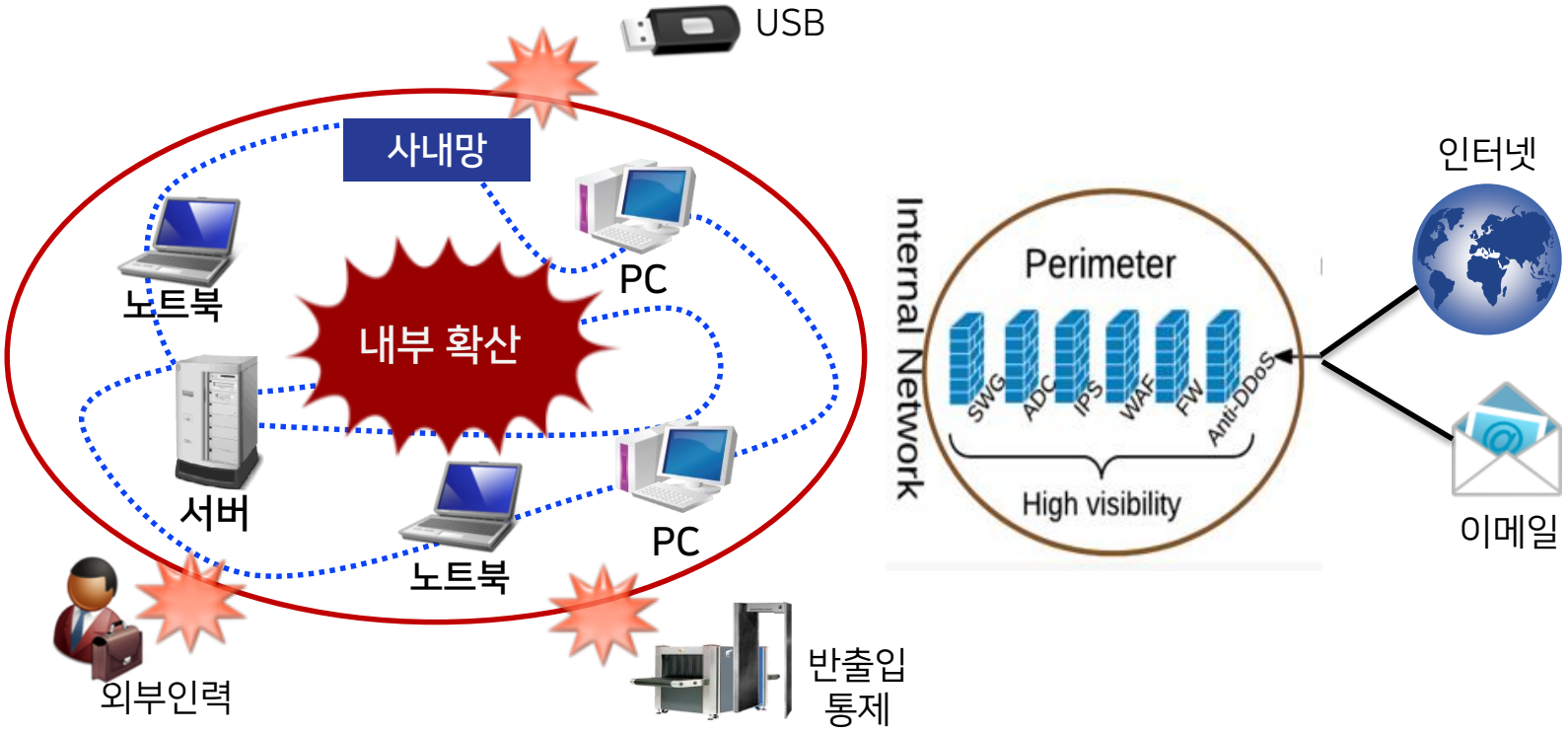
정해진 boundary내 보안
단일/소수 플랫폼
정적인 구성

현재

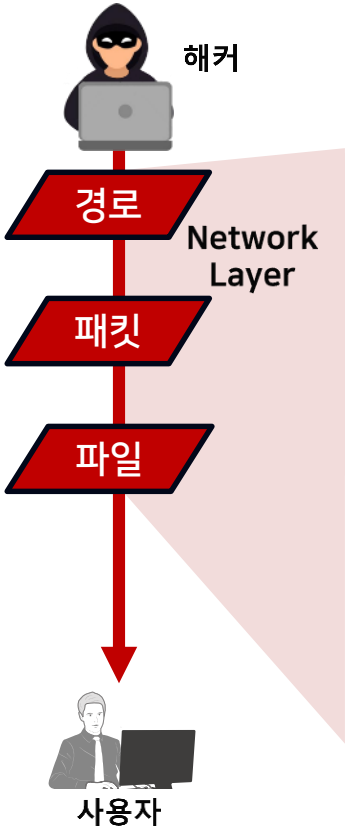
Open된 환경에서의 보안
(모바일, 클라우드, Smart Work)
다양한 플랫폼/어플리케이션
동적인 구성



2. 네트워크 경계보안의 Blind Spot 존재



3. 네트워크 경계보안을 통한 악성코드 유입/해킹 차단 한계

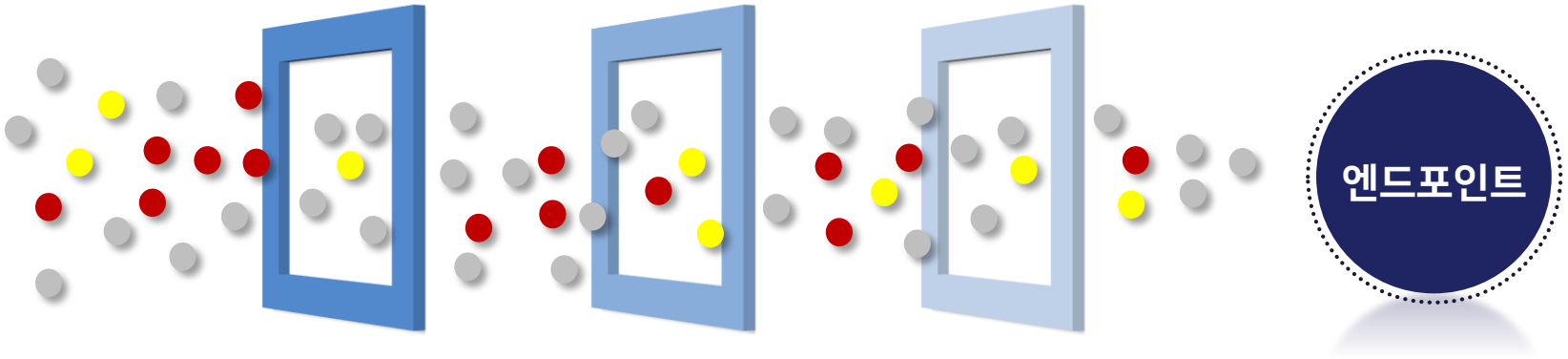


	주요 기능	솔루션	우회 공격
01 경로 차단	▶ 출발지/목적지 분석 ▶ IP, URL, URI 等	• Firewall • Proxy	1회용 주소
02 패킷 분석	▶ 통신 패킷 분석 ▶ NW 시그니처 분석	• Signature IDS/IPS • WAF	통신 암호화
03 파일 분석	▶ 패킷 조합 → 파일생성 ▶ 악성파일 여부 확인	• Sandbox	Anti-VM

3. 네트워크 경계보안을 통한 악성코드 유입/해킹 차단 한계

"네트워크 경계 보안 우회기법의 발전 "

100% 해킹 방지 및 악성코드 차단은 불가능



방화벽

- 알려진 악성 IP/Port 차단
- Blocked Session

IPS

- 패턴기반의 공격차단
- Block Session

VirusWall

- Signature기반 차단
- Block Session

기존 엔드포인트 보안의 한계

“엔드포인트 보안 = 백신” 의 한계

2018 State of Endpoint Security Risk 보고서
(美 Ponemon Institute 社)

Anti-virus 백신이 현재의 엔드포인트 위협을 전부 막을 수 없다고 답변

2017년 Anti-Virus 백신을 대체하거나 보완

자동화 된 악성코드 변종 툴

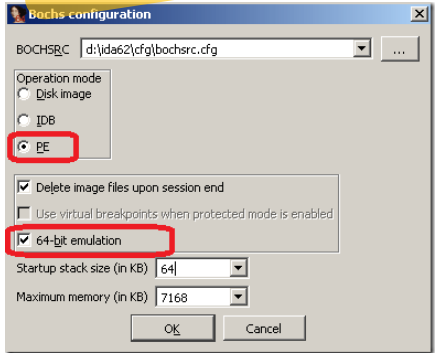
기존 악성코드를 자동화 된 툴로 변종을 만들어 시그니처 기반 백신을 **무력화**

4초에 1개꼴 기계적으로 악성코드 대량 양산

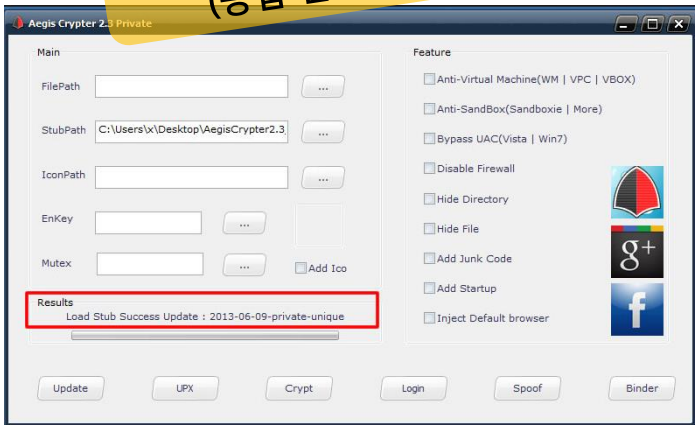
Hash Modifier (Script)

```
## Modify Hash and Rename Powershell script ##
$exeDIR = "C:\files\*.exe"
# $debuglog = "c:\files\debugging.txt"
foreach ($file in get-ChildItem $exeDIR) {
# $oldhash = get-filehash $file | Select-Object -ExpandProperty Hash
add-content $file `0
$newhash = get filehash $file | Select-Object -ExpandProperty Hash
rename-item $file "$newhash.exe"
# Add-content $debuglog "`n$file -&gt; $newhash.exe"
# Add-content $debuglog "`n$oldhash -&gt; $newhash"
remove-variable newhash
# remove-variable oldhash
}
```

MPress (Packer)

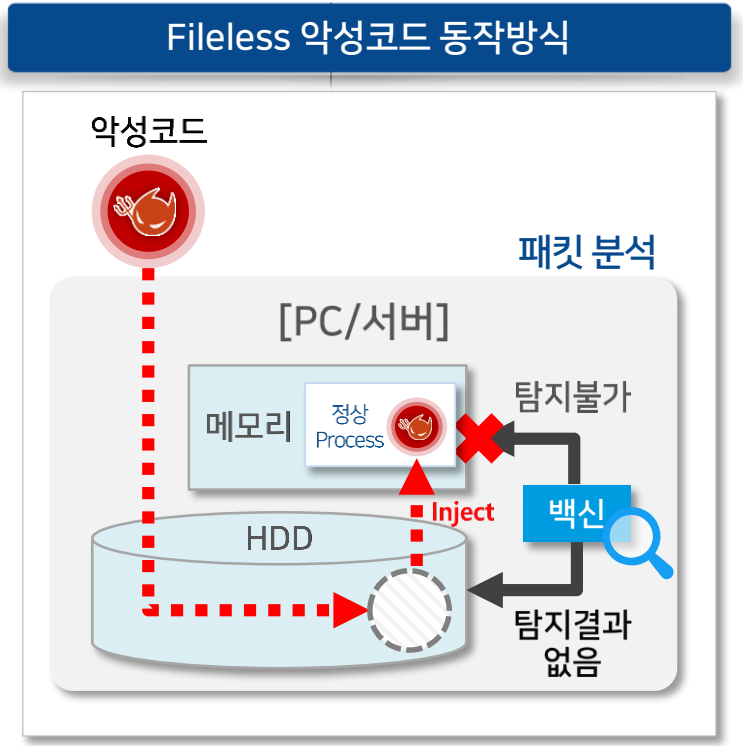


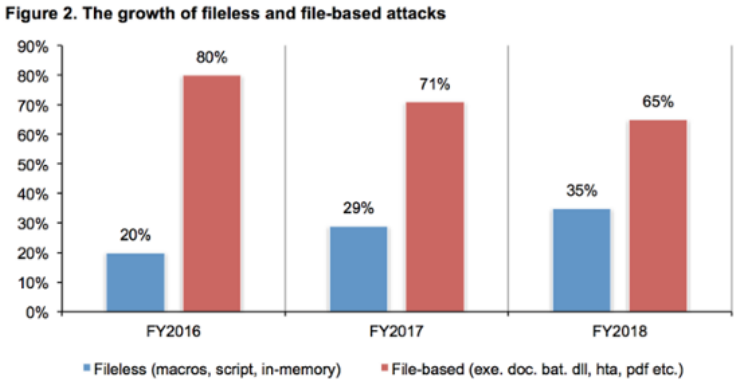
Aegis Crypter (종합 변종툴)



Fileless 악성코드

악성코드가 HDD 등에 파일이 없는 형태(Fileless)로 파일 검사 기반의 **백신 우회**





- 파일기반 공격 대비 10배 높은 성공률
- Powershell, JS, 매크로 스크립트 활용

“엔드포인트 보안 = 백신” 의 한계

시그니처 생성 속도	신종/변종 악성코드	Zeroday 공격	Fileless 악성코드
< 악성코드 생성 속도	대응 속도 느림	대응 한계	탐지 못함 (스크립트, 메모리공격)

엔드포인트 보안의 요건

보안담당자의 고민

보안위협

- 랜섬웨어
- 변종 대량 양산
- 가상화폐 채굴
- Zero-Day
- 스피어 피싱
- 소셜 엔지니어링
- Fileless 공격

보안제품

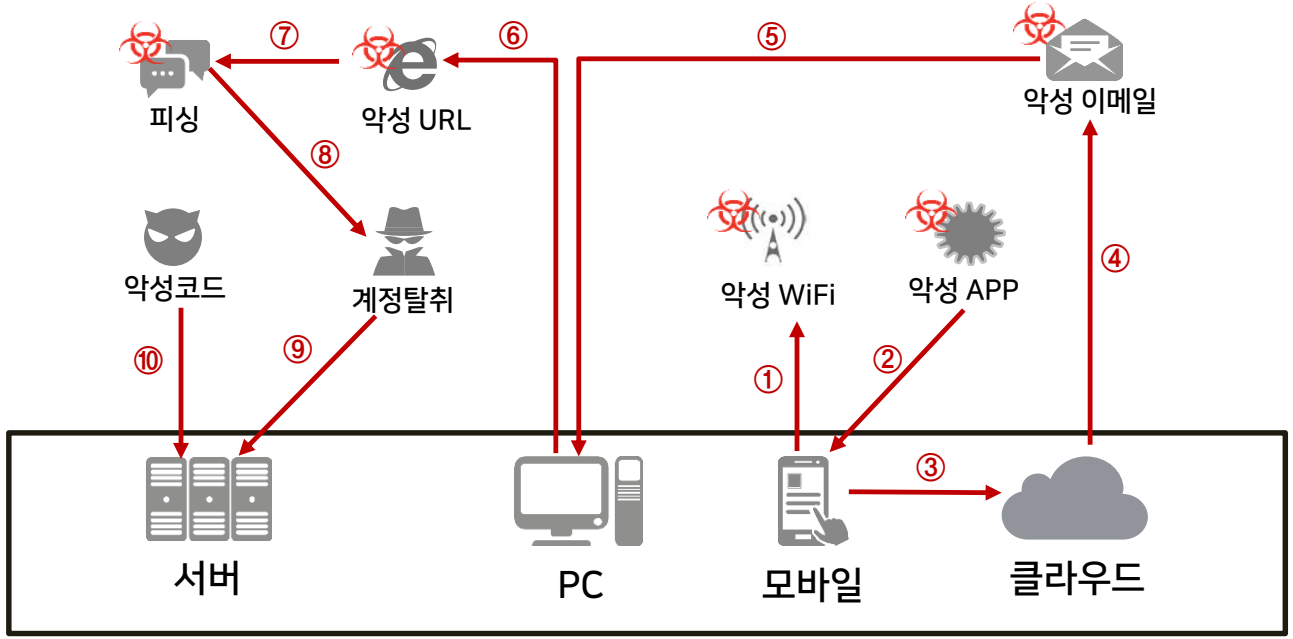
- DRM
- Anti-Ransom
- Anti-Malware
- Device Control
- DLP

사라지는 네트워크 경계

- 클라우드 IaaS, PaaS, SaaS
- 스마트워크 원격근무, 모바일 오피스, VDI
- 모바일
- IoT
- 스마트 팩토리 Industry 4.0

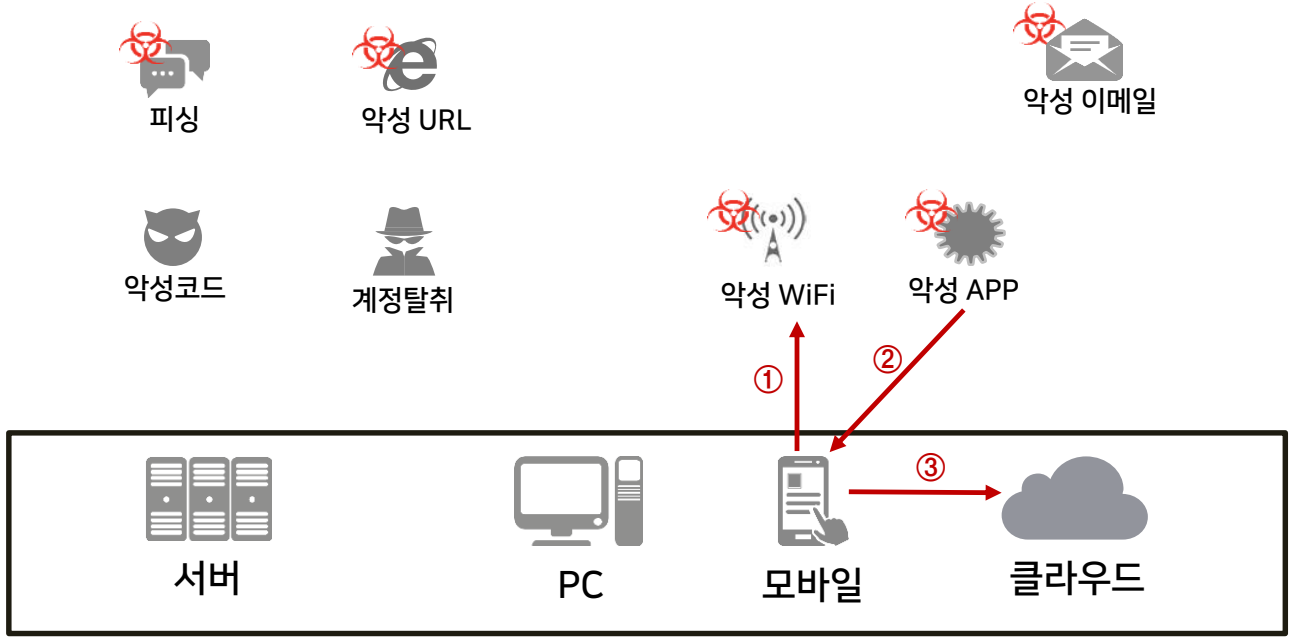
보안요건 1. 통합 플랫폼의 필요성

APT 공격 시나리오



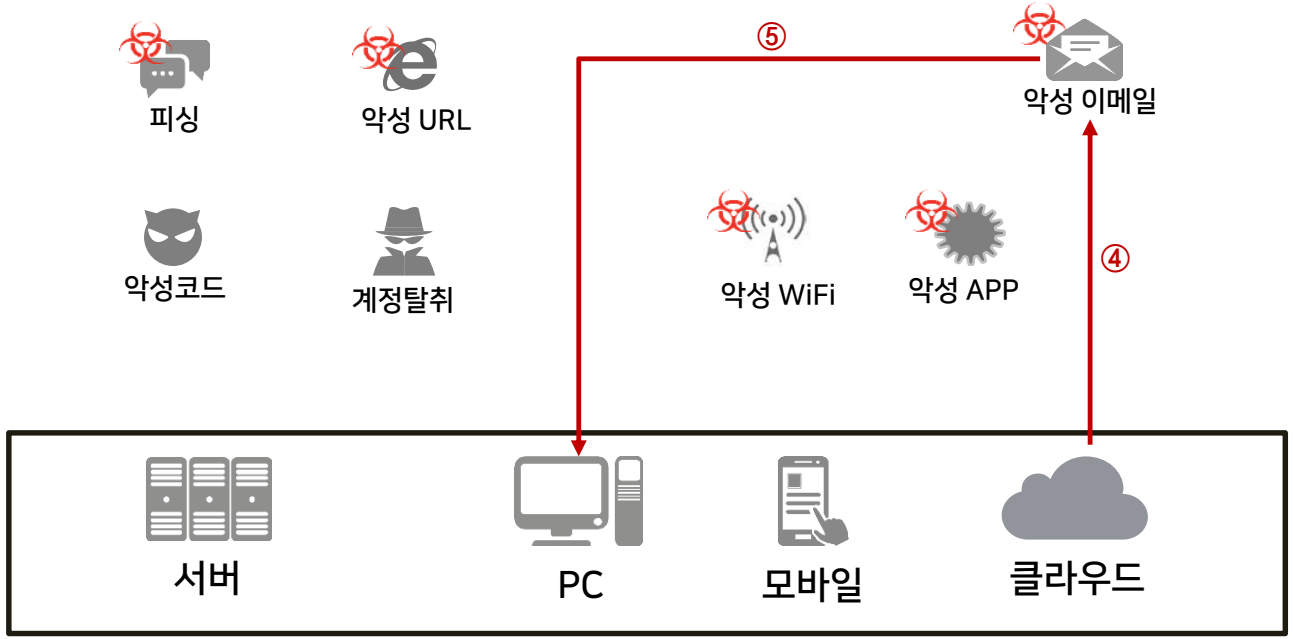
보안요건 1. 통합 플랫폼의 필요성

APT 공격 시나리오



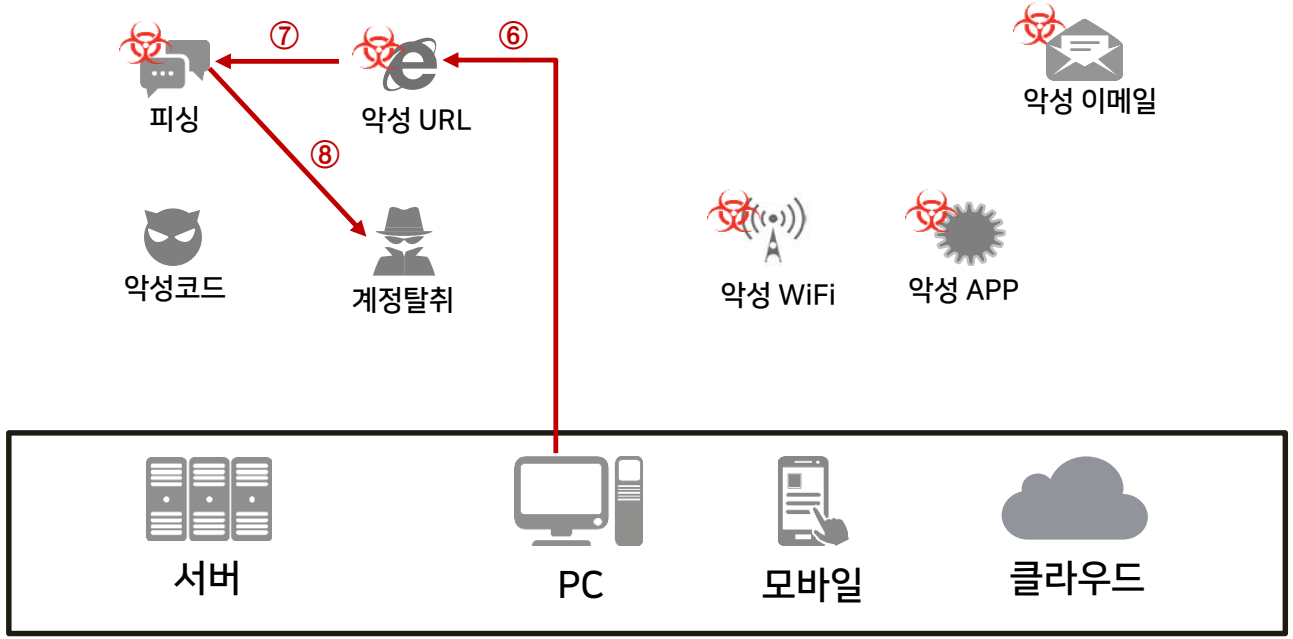
보안요건 1. 통합 플랫폼의 필요성

APT 공격 시나리오



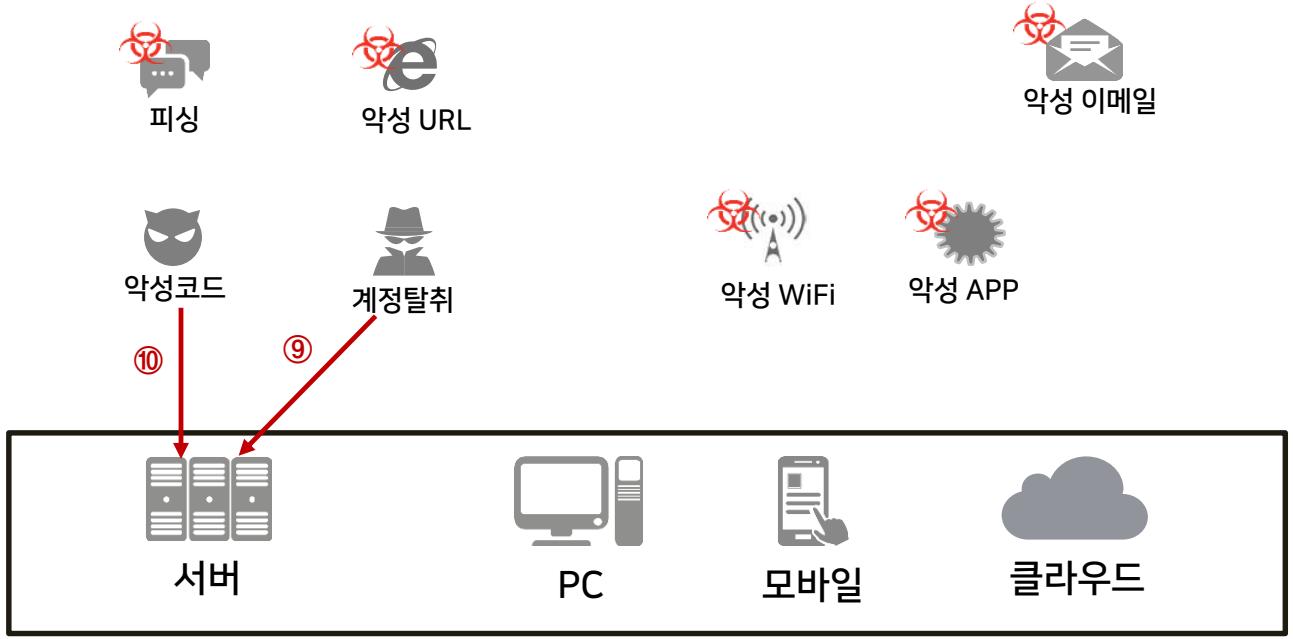
보안요건 1. 통합 플랫폼의 필요성

APT 공격 시나리오



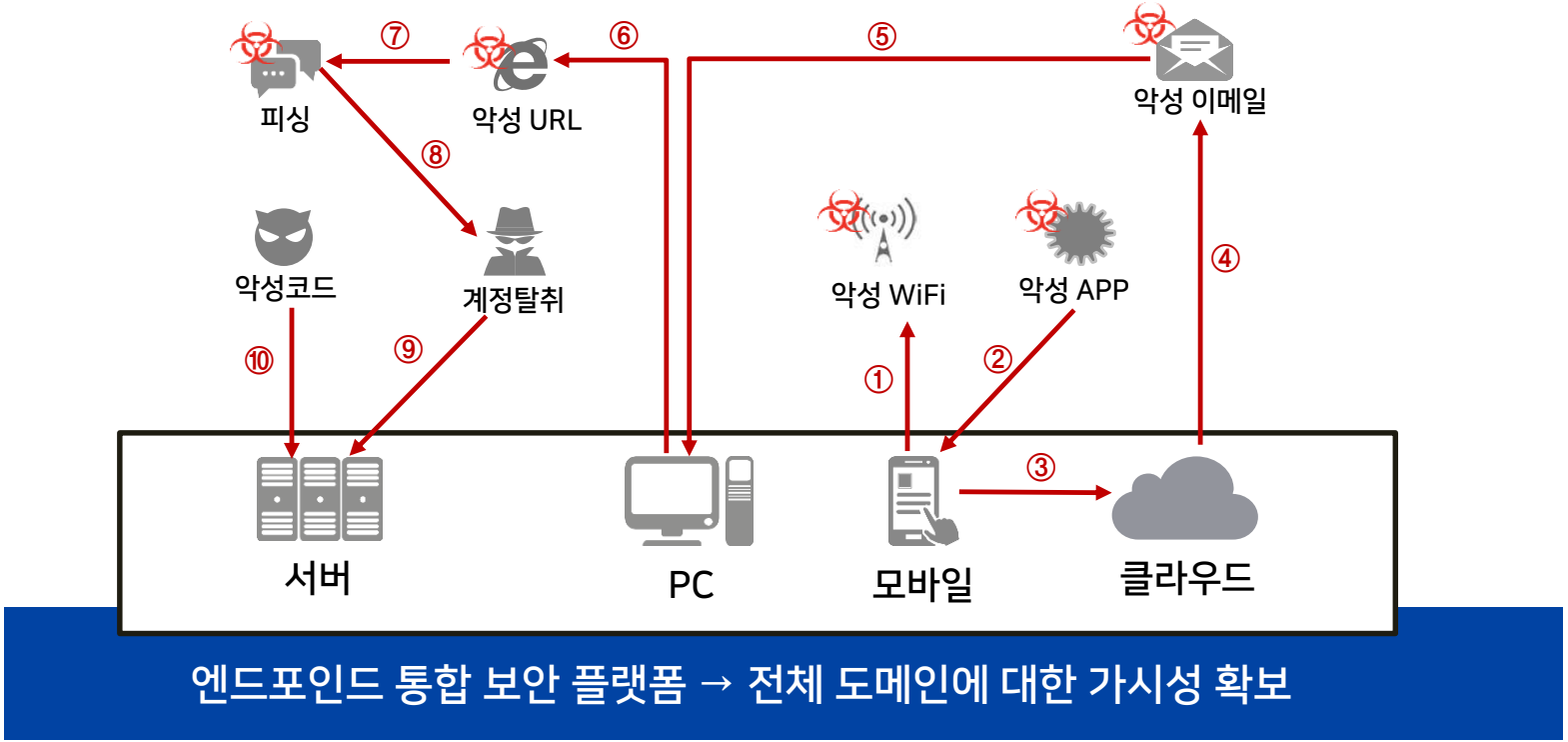
보안요건 1. 통합 플랫폼의 필요성

APT 공격 시나리오



보안요건 1. 통합 플랫폼의 필요성

APT 공격 시나리오



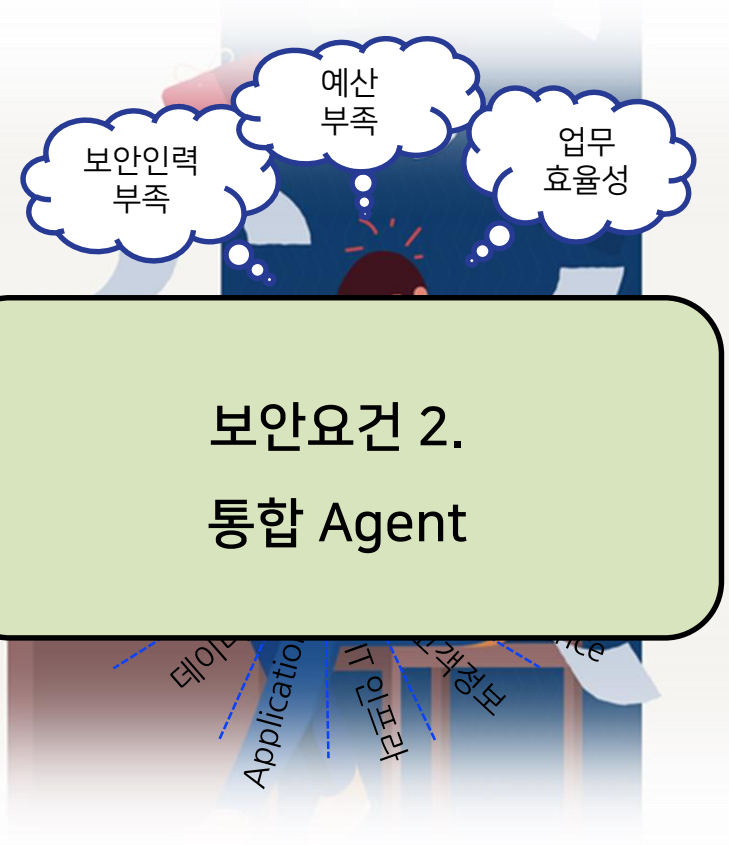
보안담당자의 고민

보안위협

- 랜섬웨어
- 변종 대량 양산
- 가상화폐 채굴
- Zero-Day
- 스피어 피싱
- 소셜 엔지니어링
- Fileless 공격

보안제품

- DRM
- Anti-Ransom
- Anti-Malware
- Device Control
- DLP

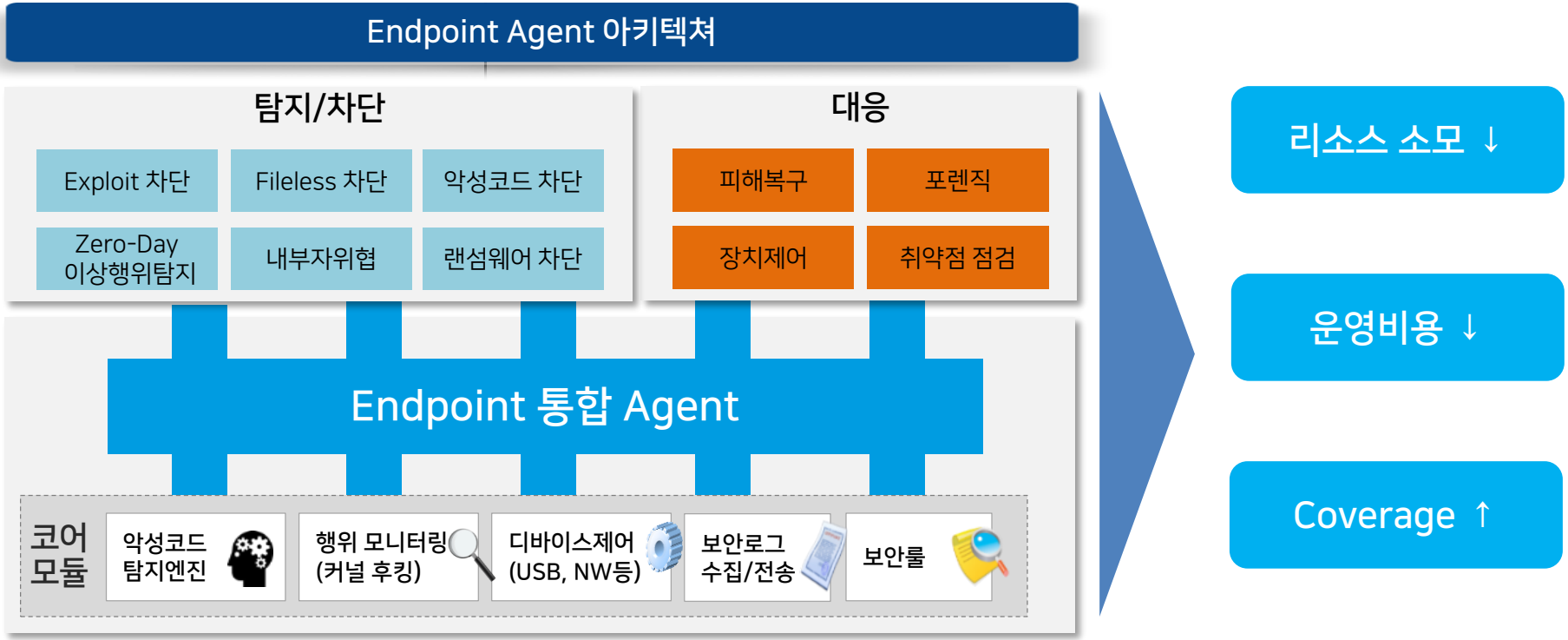


사라지는 네트워크 경계

- 클라우드 IaaS, PaaS, SaaS
- 스마트워크 원격근무, 모바일 오피스, VDI
- 모바일
- IoT
- 스마트 팩토리 Industry 4.0

Endpoint 통합 Agent

One Agent로 모든 기능 제공



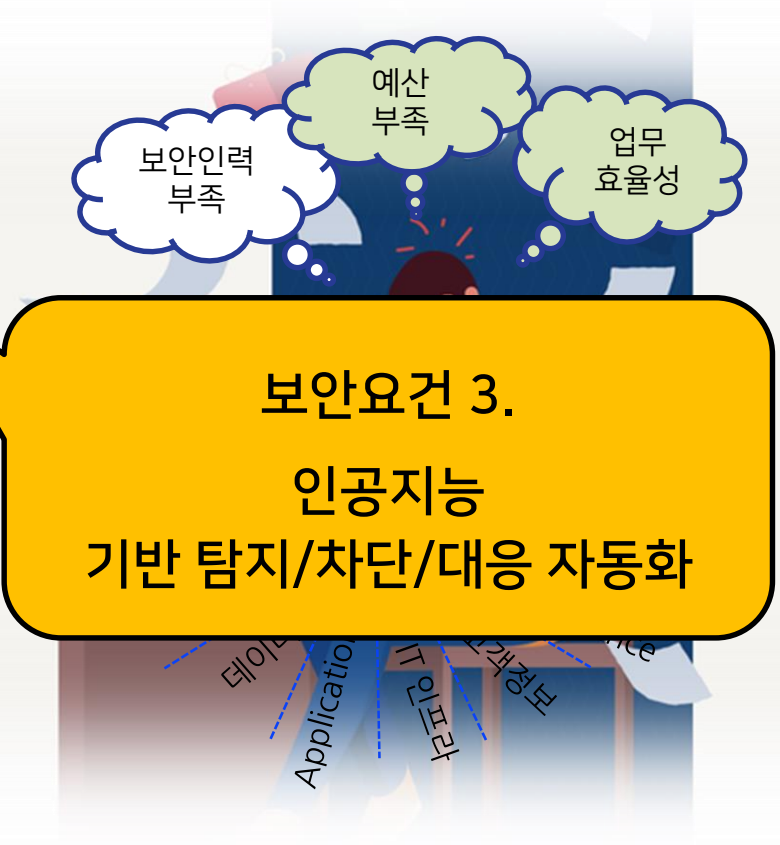
보안담당자의 고민

보안위협

- 랜섬웨어
- 변종 대량 생산
- 가상화폐 채굴
- Zero-Day
- 스피어 피싱
- 소셜 엔지니어링
- Fileless 공격

보안제품

- DRM
- Anti-Ransom
- Anti-Malware
- Device Control
- DLP



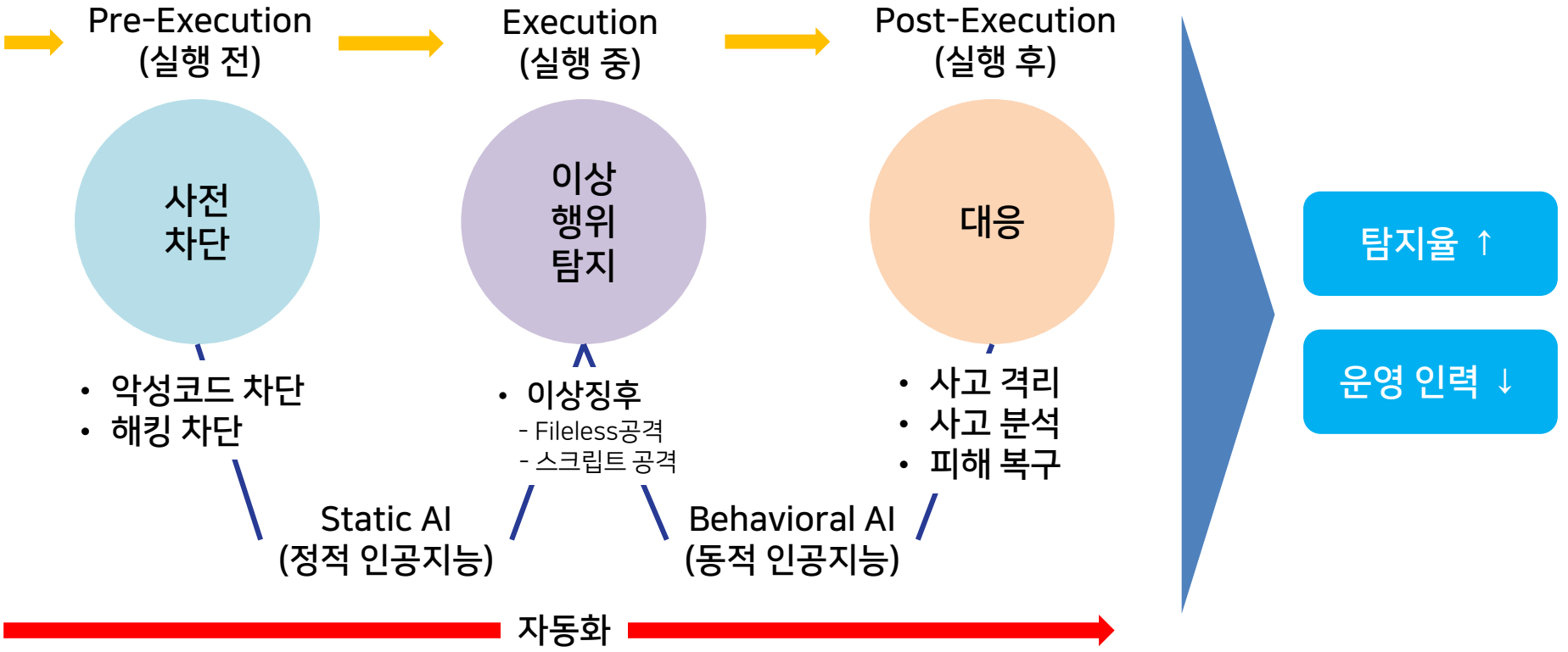
보안요건 3.

인공지능 기반 탐지/차단/대응 자동화

사라지는 네트워크 경계

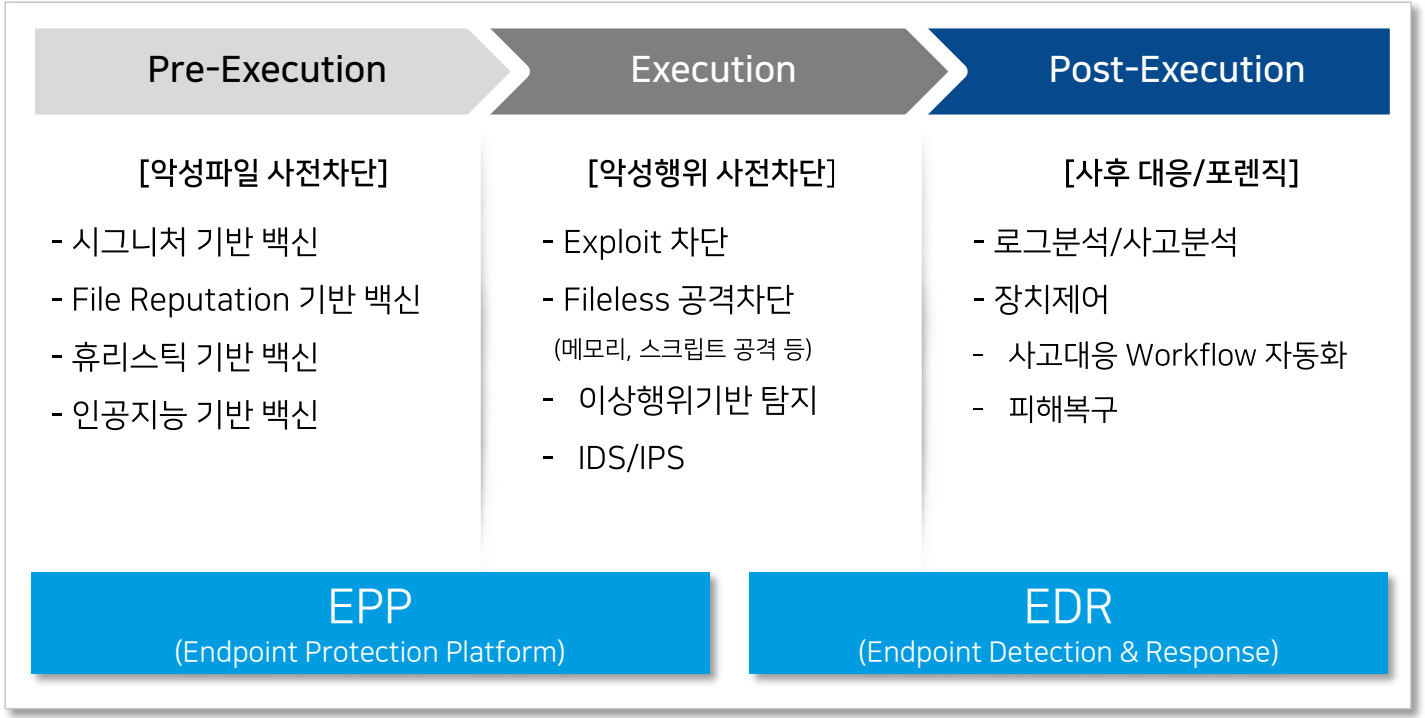
- 클라우드 IaaS, PaaS, SaaS
- 스마트워크 원격근무, 모바일 오피스, VDI
- 모바일
- IoT
- 스마트 팩토리 Industry 4.0

인공지능 기반 탐지/차단/대응 자동화

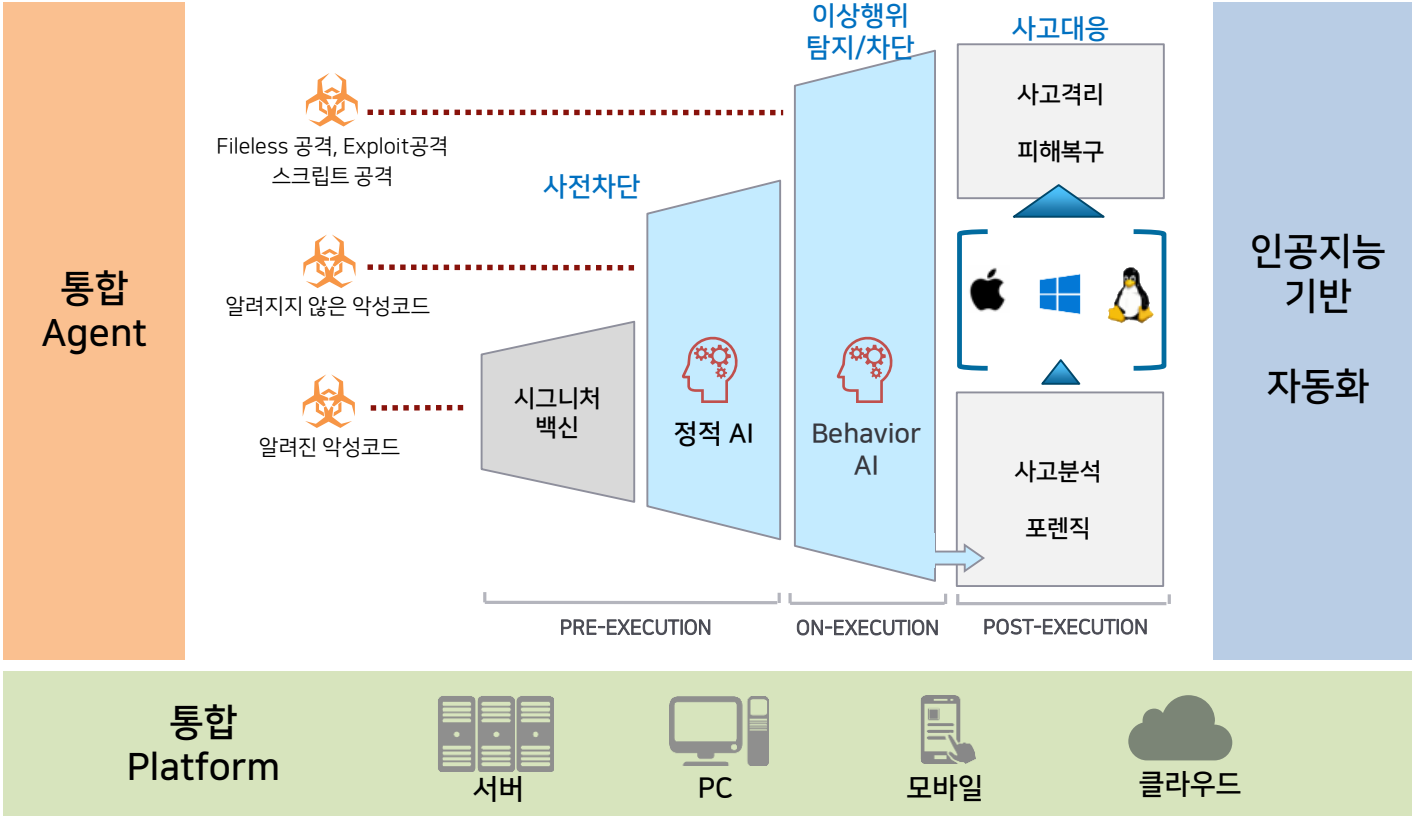


제안 솔루션
(EPP + EDR)

EPP(Endpoint Protection Platform) + EDR(Endpoint Detection & Response) 통합 솔루션



EPP+EDR 통합솔루션



Thank you

Q&A