AI솔루션을 도입했는데 일이 늘어나요! 무엇이 문제인가요?

김재환 과장, 김대협 컨설턴트

포티넷 코리아

인공지능과 보안솔루션

사용자의 기대 그리고 다양한 AI솔루션들

1. 왜 인공지능(AI) 솔루션을 고려하는가?

선택 배경 “Re-Mind”

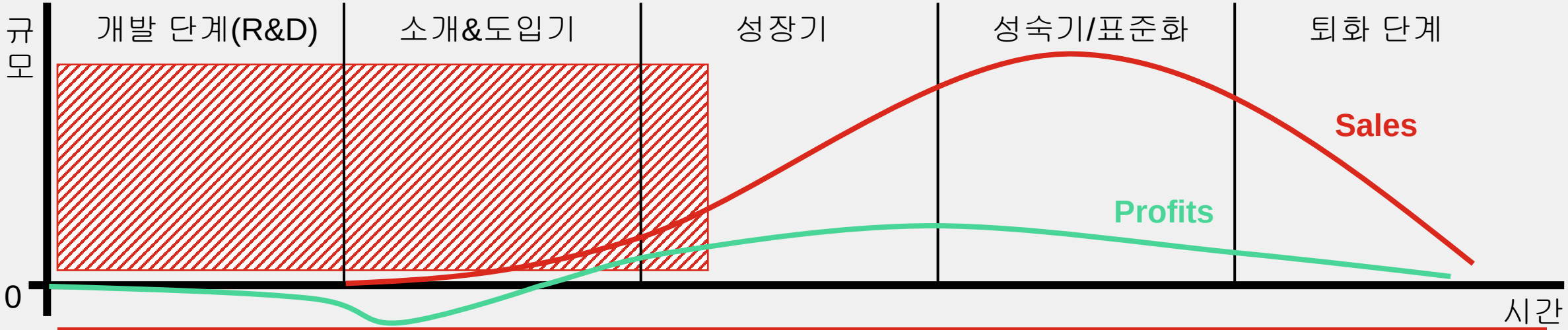
“기업 네트워크 및 인프라의 복잡성 증대“

“신종 및 변종 사이버 공격의 고도화/다양화”

“보안 침해사고 대응 인력이 겪는 난관 증대”

2. 상용 AI 보안솔루션에 대한 사용자의 기대

Think : Product Life Cycle, 시장은 어디쯤 와있을까요?



	Introduction	Growth	Maturity	Decline
시장 규모	소	중	대	중->소
시장 성장률	저	고	저	감소
시장 매력도	저	고	중	저
이노베이터 (2.5%)	**얼리어답터 (13.5%)**	**조기 수용층 (34%)**	**중간 다수층 (34%)**	**최종 수용층 (16%)**

Source : 1962, the sociologist Everett Rogers, https://en.wikipedia.org/wiki/Diffusion_of_innovations

2. 상용 AI 보안솔루션에 대한 사용자의 기대

어떤것을 기대하셨나요? 또 그것을 위해 어떤 고민과 검토를 하셨나요?

주요 기대

- **사이버 보안 영역의 기능/역량 고도화**
  - 우리 조직의 업무 환경을 학습
  - 학습된 데이터를 토대로, 사람이 놓치기 쉬운 다양한 이상행위 탐지
  - 발생하는 이벤트 데이터를 토대로, 사람이 놓치기 쉬운 연관관계 탐지

- **업무 효율성 증가를 통해 보안팀의 업무효율성 개선, 보안 업무 가속화, 사이버피로도 감소**
  - 대규모 데이터 처리, 반복 작업 처리
  - 자동 탐지 및 분석, 자동 대응, 자동 보고

기타 희망 사항

- **AI니까 자동으로 뭔가 많은 것을 해주겠지?**
  - 탐지 및 보고
  - 최적화 및 유지 관리
  - 조치 프로세스

- **AI를 샀으니까, 이제 사람을 줄여도 되지 않을까?**
  - AI 기반 업무 자동화
  - 보안인력 고용 대비 ROI 개선

- **도입과 동시에 가시적인 보안효과를 발휘하지 않을까?**
  - 조직 데이터 학습 하여, 최적화된 적용&효과
  - 제조사에서 사전학습된 고품질 데이터셋

2. 상용 AI 보안솔루션에 대한 사용자의 기대

어떤것을 기대하셨나요? 또 그것을 위해 어떤 고민과 검토를 하셨나요?

주요 기대

- **사이버 보안 영역의 기능/역량 고도화**
  - 우리 조직의 업무 환경을 학습
  - 학습된 데이터를 토대로, 사람이 놓치기 쉬운 다양한 이상행위 탐지
  - 발생하는 이벤트 데이터를 토대로, 사람이 놓치기 쉬운 연관관계 탐지
- **업무 효율성 증가를 통해 보안팀의 업무효율성 개선, 보안 업무 가속화, 사이버피로도 감소**
  - 대규모 데이터 처리, 반복 작업 처리
  - 자동 탐지 및 분석, 자동 대응, 자동 보고

기타 희망 사항

- **AI니까 자동으로 뭔가 많은 것을 해주겠지?**
  - 탐지 및 보고
  - 최적화 및 유지 관리
  - 조치 프로세스
- **AI를 샀으니까, 이제 사람을 줄여도 되지 않을까?**
  - AI 기반 업무 자동화
  - 보안인력 고용 대비 ROI 개선
- **도입과 동시에 가시적인 보안효과를 발휘하지 않을까?**
  - 조직 데이터 학습 하여, 최적화된 적용&효과
  - 제조사에서 사전학습된 고품질 데이터셋

2. 상용 AI 보안솔루션에 대한 사용자의 기대

어떤것을 기대하셨나요? 또 그것을 위해 어떤 고민과 검토를 하셨나요?

주요 기대

- **사이버 보안 영역의 기능/역량 고도화**
  - 우리 조직의 업무 환경을 학습
  - 학습된 데이터를 토대로, 사람이 놓치기 쉬운 다양한 이상행위 탐지
  - 발생하는 이벤트 데이터를 토대로, 사람이 놓치기 쉬운 연관관계 탐지
- **업무 효율성 증가를 통해 보안팀의 업무효율성 개선, 보안 업무 가속화, 사이버피로도 감소**
  - 대규모 데이터 처리, 반복 작업 처리
  - 자동 탐지 및 분석, 자동 대응, 자동 보고

기타 희망 사항

- **AI니까 자동으로 뭔가 많은 것을 해주겠지?**
  - 탐지 및 보고
  - 최적화 및 유지 관리
  - 조치 프로세스
- **AI를 샀으니까, 이제 사람을 줄여도 되지 않을까?**
  - AI 기반 업무 자동화
  - 보안인력 고용 대비 ROI 개선
- **도입과 동시에 가시적인 보안효과를 발휘하지 않을까?**
  - 조직 데이터 학습 하여, 최적화된 적용&효과
  - 제조사에서 사전학습된 고품질 데이터셋

2. 상용 AI 보안솔루션에 대한 사용자의 기대

어떤것을 기대하셨나요? 또 그것을 위해 어떤 고민과 검토를 하셨나요?

주요 기대

- **사이버 보안 영역의 기능/역량 고도화**
  - 우리 조직의 업무 환경을 학습
  - 학습된 데이터를 토대로, 사람이 놓치기 쉬운 다양한 이상행위 탐지
  - 발생하는 이벤트 데이터를 토대로, 사람이 놓치기 쉬운 연관관계 탐지

- **업무 효율성 증가를 통해 보안팀의 업무효율성 개선, 보안 업무 가속화, 사이버피로도 감소**
  - 대규모 데이터 처리, 반복 작업 처리
  - 자동 탐지 및 분석, 자동 대응, 자동 보고

기타 희망 사항

- **AI니까 자동으로 뭔가 많은 것을 해주겠지?**
  - 탐지 및 보고
  - 최적화 및 유지 관리
  - 조치 프로세스

- **AI를 샀으니까, 이제 사람을 줄여도 되지 않을까?**
  - AI 기반 업무 자동화
  - 보안인력 고용 대비 ROI 개선

- **도입과 동시에 가시적인 보안효과를 발휘하지 않을까?**
  - 조직 데이터 학습 하여, 최적화된 적용&효과
  - 제조사에서 사전학습된 고품질 데이터셋

2. 상용 AI 보안솔루션에 대한 사용자의 기대

어떤것을 기대하셨나요? 또 그것을 위해 어떤 고민과 검토를 하셨나요?

기타 희망 사항

- **AI니까 자동으로 뭔가 많은 것을 해주겠지?**
  - 탐지 및 보고
  - 최적화 및 유지 관리
  - 조치 프로세스
- **AI를 샀으니까, 이제 사람을 줄여도 되지 않을까?**
  - AI 기반 업무 자동화
  - 보안인력 고용 대비 ROI 개선
- **도입과 동시에 가시적인 보안효과를 발휘하지 않을까?**
  - 조직 데이터 학습 하여, 최적화된 적용&효과
  - 제조사에서 사전학습된 고품질 데이터셋

검토 요소

- 관련 기능이 있습니까?
- 관련 기능을 통해서 도출되는 결과가 만족할 수 있는 수준입니까?
- 구현 위한 작업이 추가로 발생하진 않습니까?

- 정확히 어떤 업무를 사람 대신 수행할 수 있습니까?
- 관리자가 전혀 필요 없는 유형의 제품입니까?
- 부가적인 작업이 필요 없습니까?

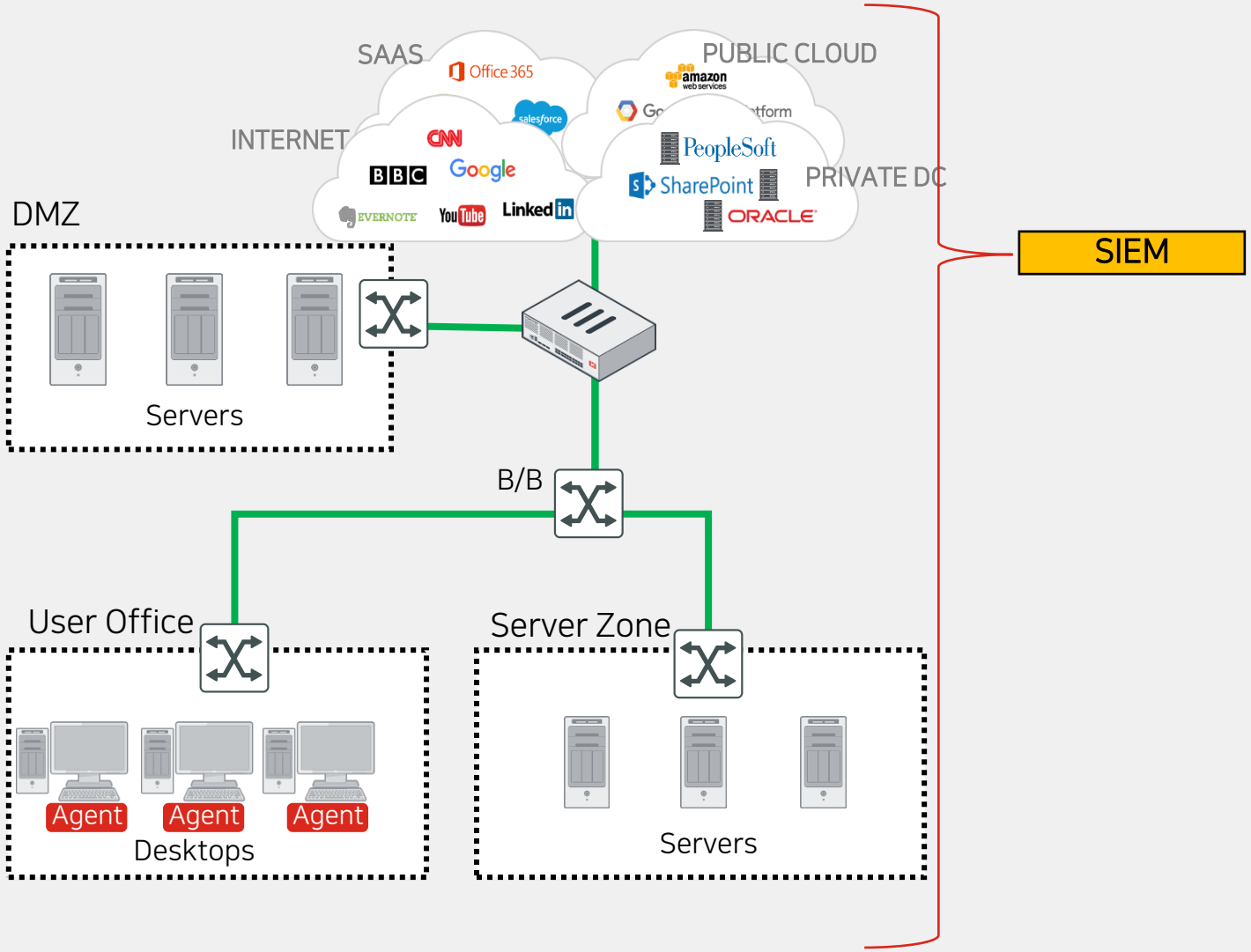
- 조직 데이터 학습이 필수적인 제품입니까?
- 조직에서 발생하는 데이터 유형 중 어떤 데이터 유형에 적용 할 수 있습니까?
- 사전학습 데이터가 신뢰할 수 있습니까?
- 제품의 설명대로 잘 동작합니까?

3. 머신러닝 기반 침해사고 탐지 관점의 보안솔루션들

"빅데이터 관제 플랫폼 기반"

예: SIEM

[기본 역량]
- 종합적인 보안 가시성 확보
- 다양한 데이터 유형 수용
- 대용량/장기간 데이터 저장
- 과거 이벤트 검색(Raw/Meta)
- 상관관계 탐지
- 기본적인 대응 액션



3. 머신러닝 기반 침해사고 탐지 관점의 보안솔루션들

"빅데이터 관제 플랫폼 기반" + "머신러닝 AI 기능"

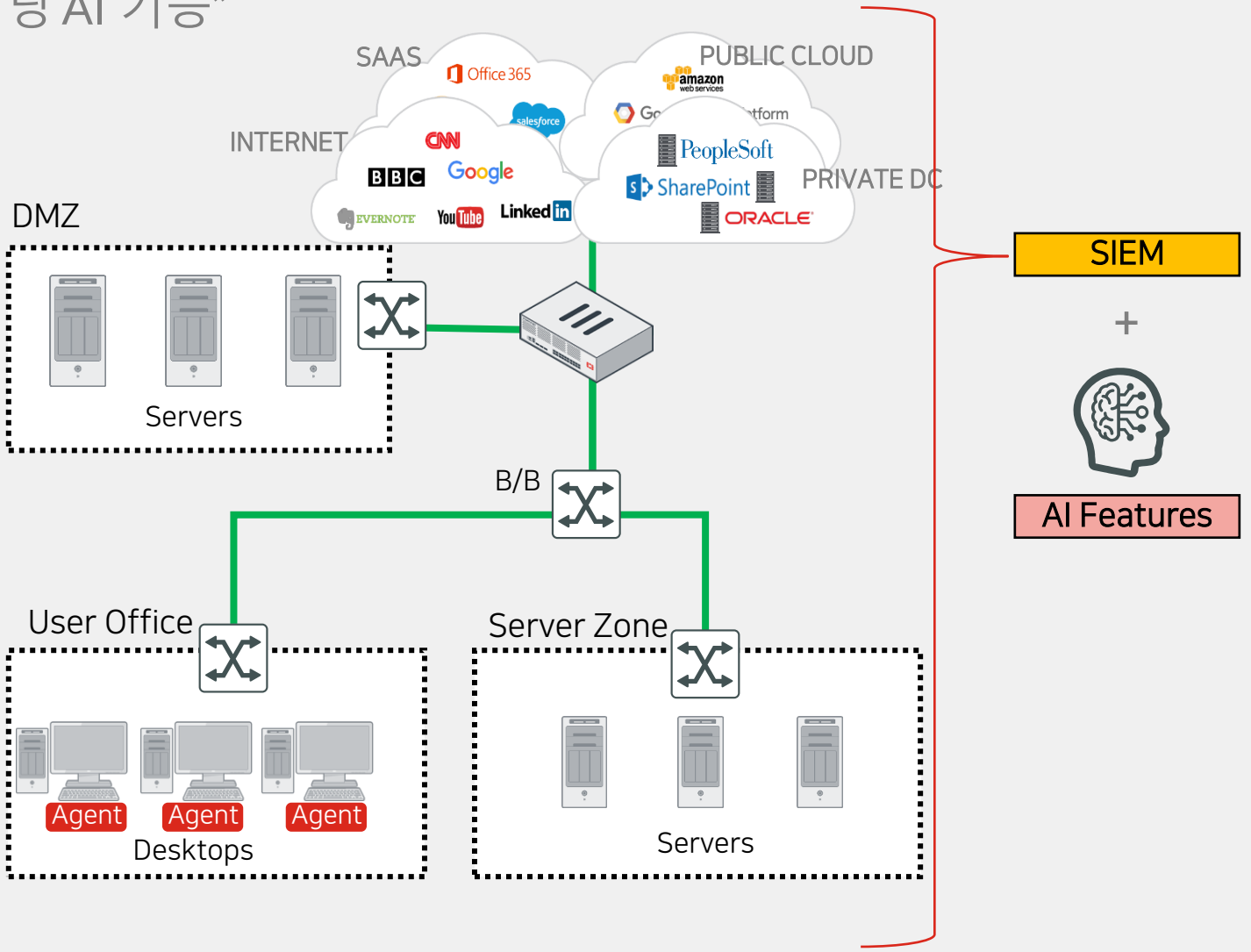
예: SIEM

[기본 역량]

- 종합적인 보안 가시성 확보
- 다양한 데이터 유형 수용
- 대용량/장기간 데이터 저장
- 과거 이벤트 검색(**Raw/Meta**)
- 상관관계 탐지
- 기본적인 대응 액션

[+머신러닝 AI 기능]

- 이벤트 스코어링
- 장치/사용자/네트워크 수준 이상 행위 경고
- 평상시 활동에 대한 베이스라인 구축
- 제품 별 상이한 탐지 기준 보유
- 제품 추가기능으로 포함 또는 독립 제품 연동



3. 머신러닝 기반 침해사고 탐지 관점의 보안솔루션들

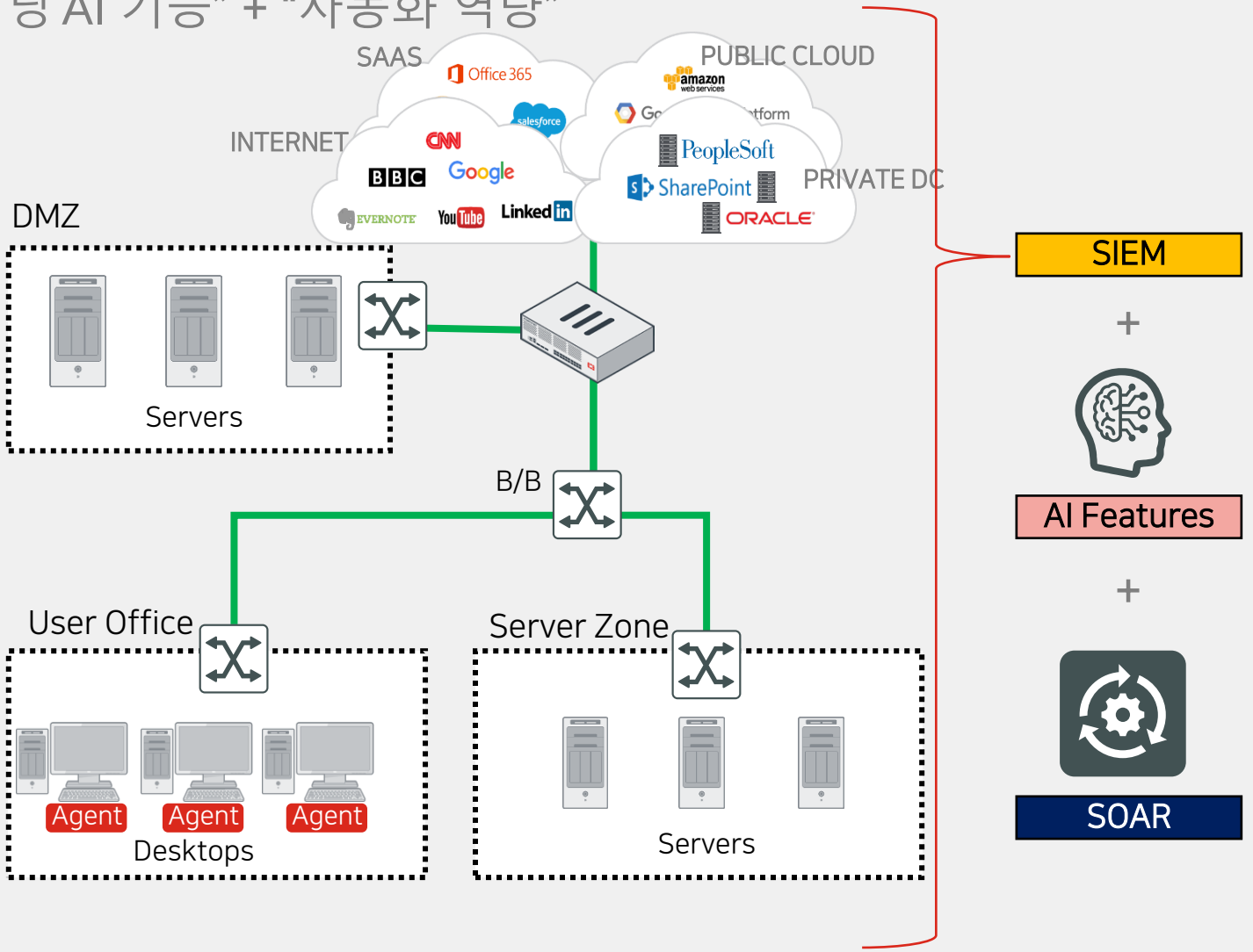
"빅데이터 관제 플랫폼 기반" + "머신러닝 AI 기능" + "자동화 역량"

예: SIEM

[기본 역량]
- 종합적인 보안 가시성 확보
- 다양한 데이터 유형 수용
- 대용량/장기간 데이터 저장
- 과거 이벤트 검색(**Raw/Meta**)
- 상관관계 탐지
- 기본적인 대응 액션

[+머신러닝 AI 기능]
- 이벤트 스코어링
- 장치/사용자/네트워크 수준 이상 행위 경고
- 평상시 활동에 대한 베이스라인 구축
- 제품 별 상이한 탐지 기준 보유
- 제품 추가기능으로 포함 또는 독립 제품 연동

[+자동화 역량]
- 플레이북 기반, 사람의 업무 절차를 자동화
- 이기종 보안시스템들과의 상호 작용
- 티켓팅/협업 기반 지능형 사고 대응 플랫폼

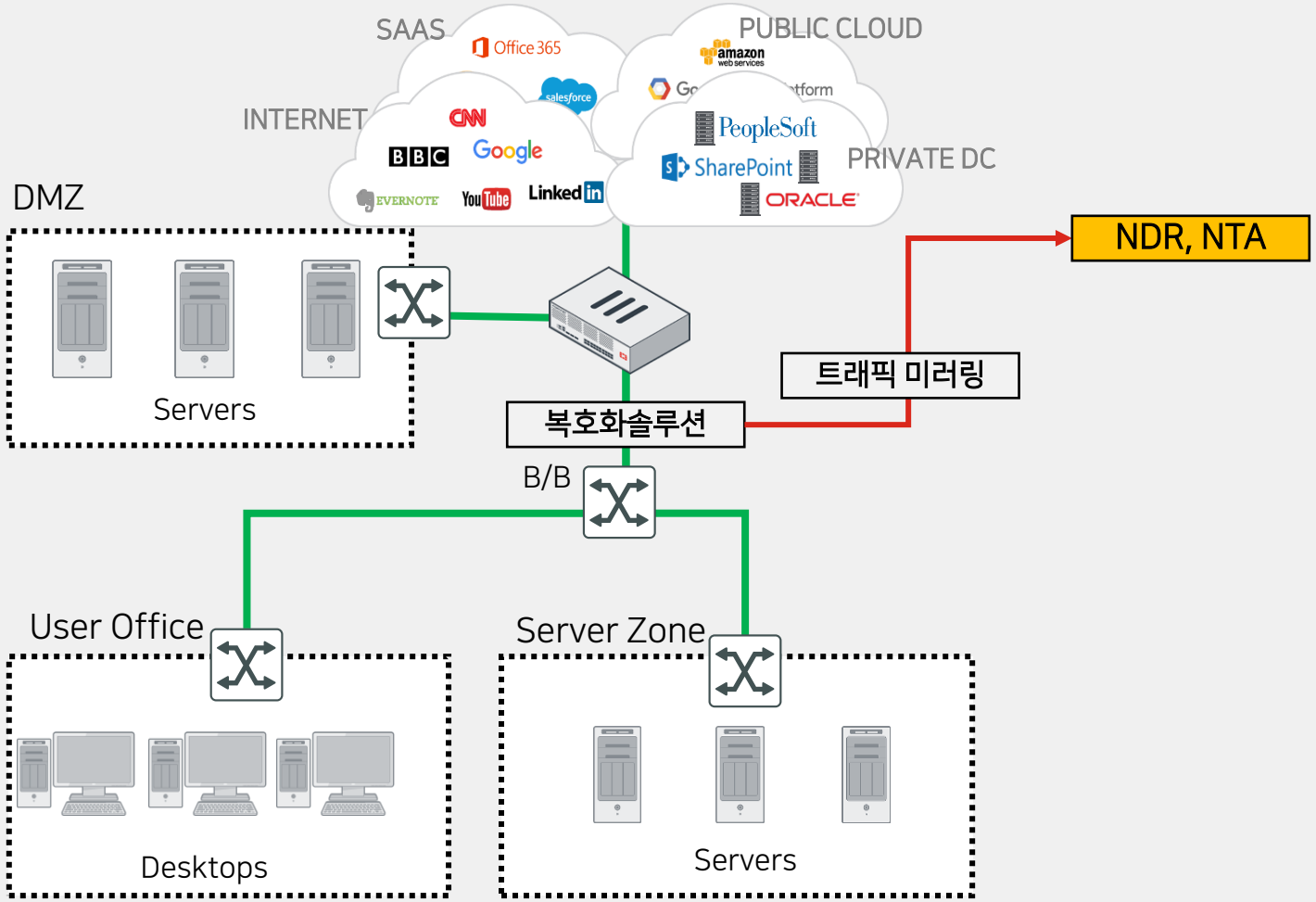


3. 머신러닝 기반 침해사고 탐지 관점의 보안솔루션들

"네트워크 트래픽 분석 기반 솔루션"

예: NDR, NTA

[기본 역량]
- 네트워크 트래픽 수집(미러링)
- **DPI** 기술기반 파싱 및 메타데이터 추출
- 네트워크 패킷 처리에 전문화
- 대용량/장기간 네트워크 저장
- 과거 이벤트 검색**(Payload or Meta-Only)**
- 룰 기반 탐지



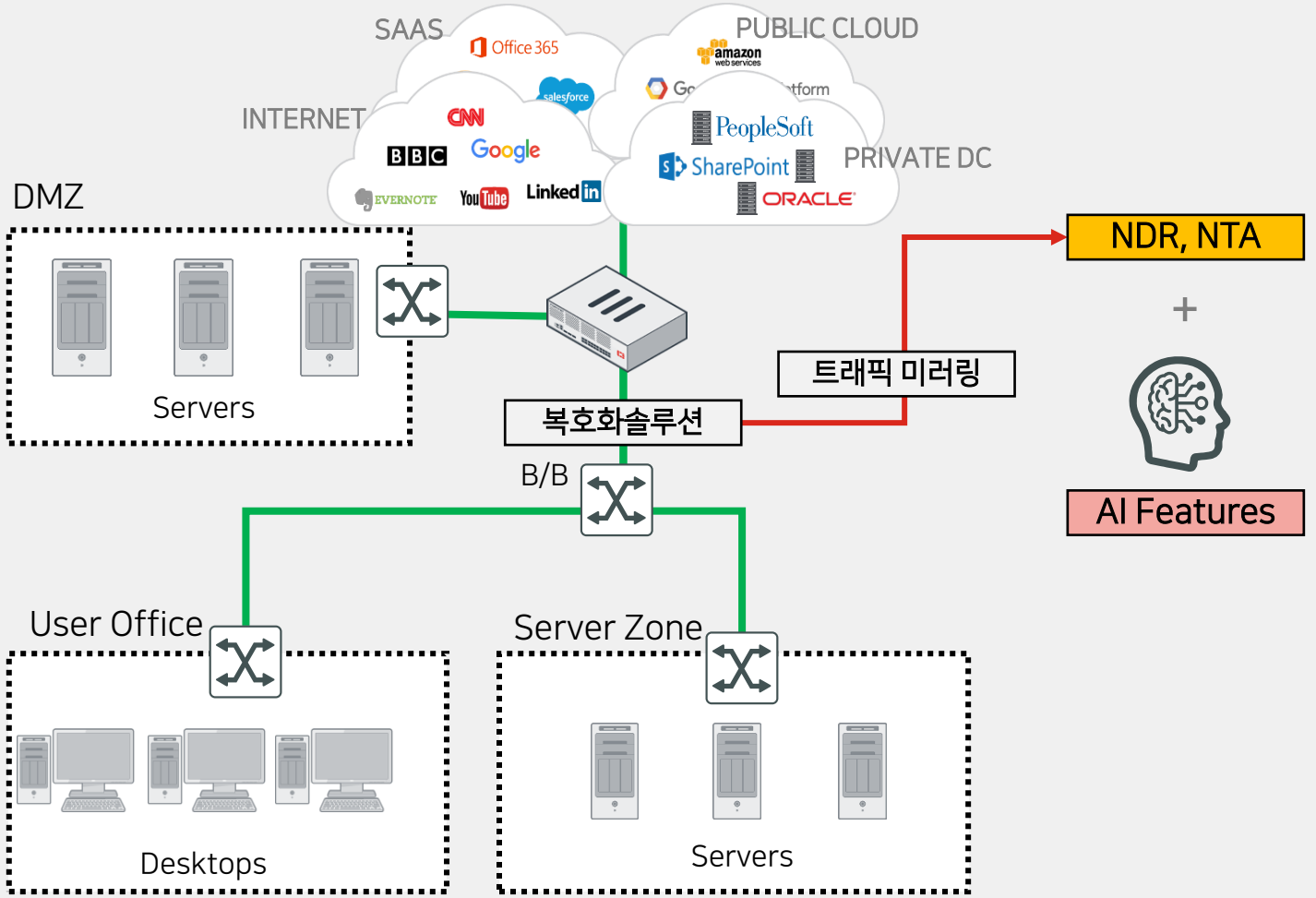
3. 머신러닝 기반 침해사고 탐지 관점의 보안솔루션들

"네트워크 트래픽 분석 기반 솔루션" + "머신러닝 AI 기능"

예: NDR, NTA

[기본 역량]
- 네트워크 트래픽 수집(미러링)
- **DPI** 기술기반 파싱 및 메타데이터 추출
- 네트워크 패킷 처리에 전문화
- 대용량/장기간 네트워크 저장
- 과거 이벤트 검색(**Payload or Meta-Only**)
- 룰 기반 탐지

[+머신러닝 **AI** 기능]
- 평상시 네트워크 활동에 대한 베이스라인 구축
- 네트워크 수준의 이상 행위 경고
- 장치/행위 별 클러스터링으로 유사군집
- 제품 별 상이한 탐지 기준 보유



3. 머신러닝 기반 침해사고 탐지 관점의 보안솔루션들

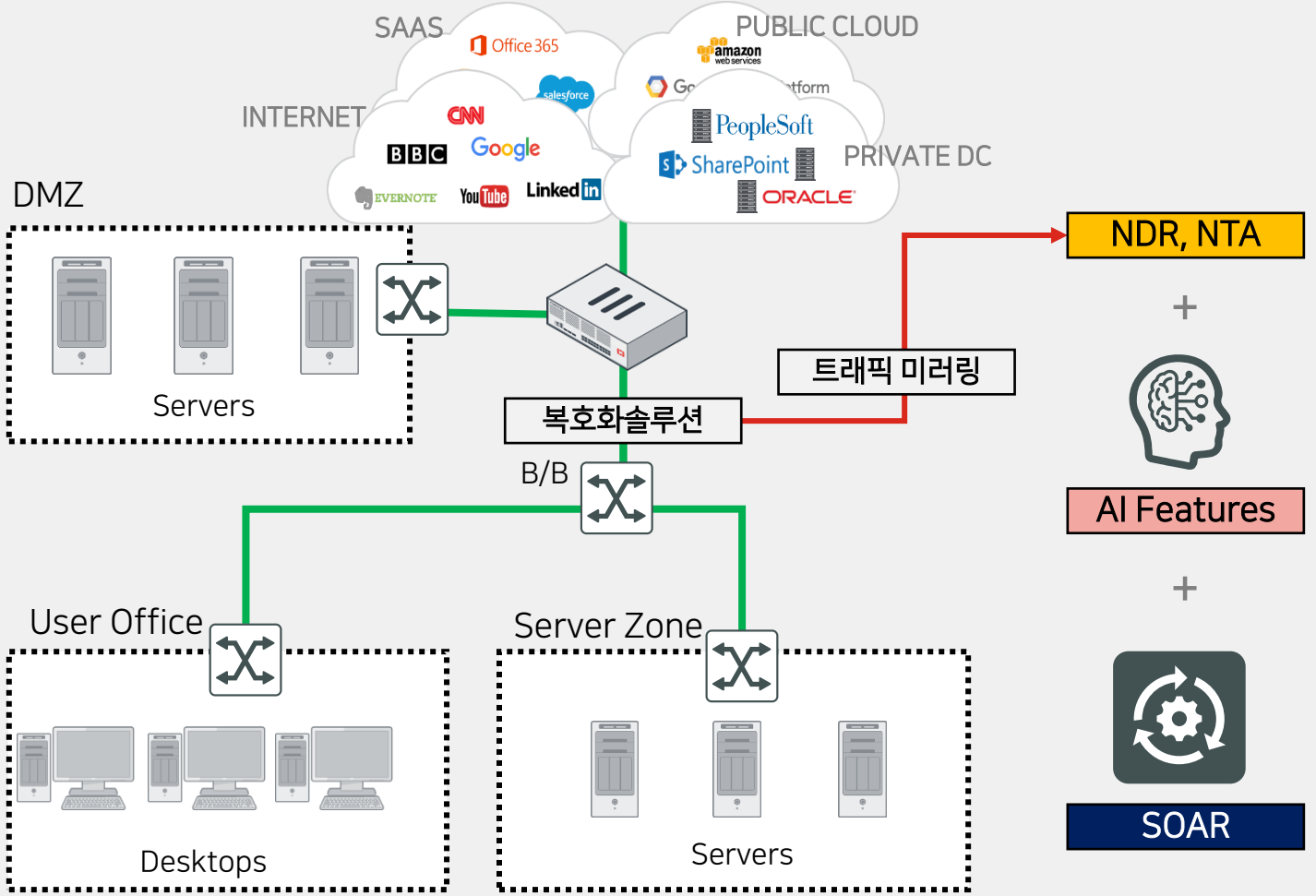
"네트워크 트래픽 분석 기반 솔루션" + "머신러닝 AI 기능" + "자동화 역량"

예: NDR, NTA

[기본 역량]
- 네트워크 트래픽 수집(미러링)
- **DPI** 기술기반 파싱 및 메타데이터 추출
- 네트워크 패킷 처리에 전문화
- 대용량/장기간 네트워크 저장
- 과거 이벤트 검색(**Payload or Meta-Only**)
- 룰 기반 탐지

[+머신러닝 AI 기능]
- 평상시 네트워크 활동에 대한 베이스라인 구축
- 네트워크 수준의 이상 행위 경고
- 장치/행위 별 클러스터링으로 유사군집
- 제품 별 상이한 탐지 기준 보유

[+자동화 역량]
- 플레이북 기반, 사람의 업무 절차를 자동화
- 이기종 보안시스템들과의 상호 작용
- 티켓팅/협업 기반 지능형 사고 대응 플랫폼

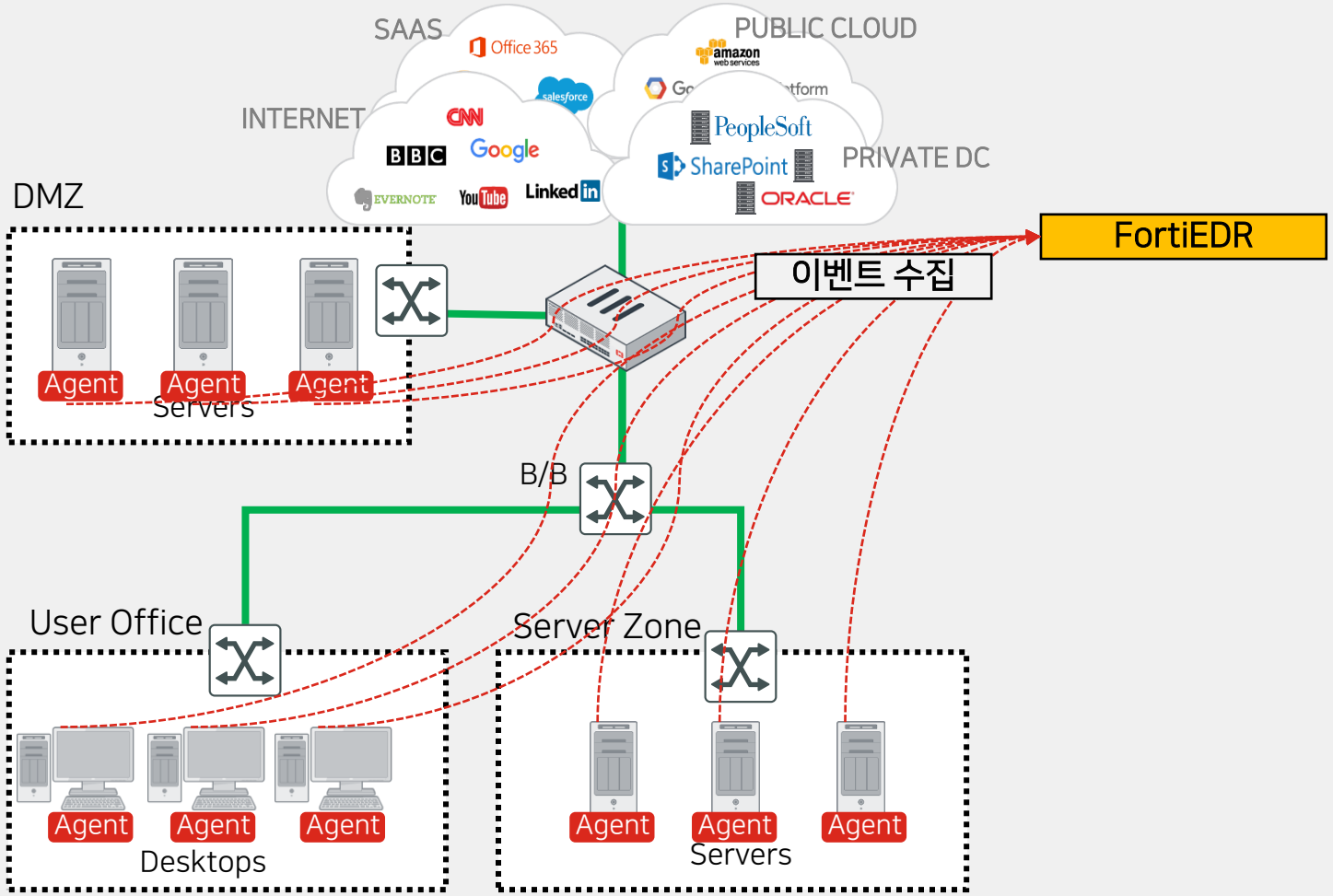


3. 딥러닝 기반 악성코드 탐지 관점의 보안솔루션들

"엔드포인트 기반 솔루션"

예: FortiEDR

[기본 역량]
- 엔드포인트 레벨 이벤트 수집(에이전트)
- 호스트수준의 깊은 데이터 가시성 확보
- 사고 추적 포렌직용 백데이터 확보
- 제품 별 상이한 수준으로 악성코드 방어 기능 탑재
- **XDR 로의 확장성**
  (Endpoint + Network + Cloud + Email…)



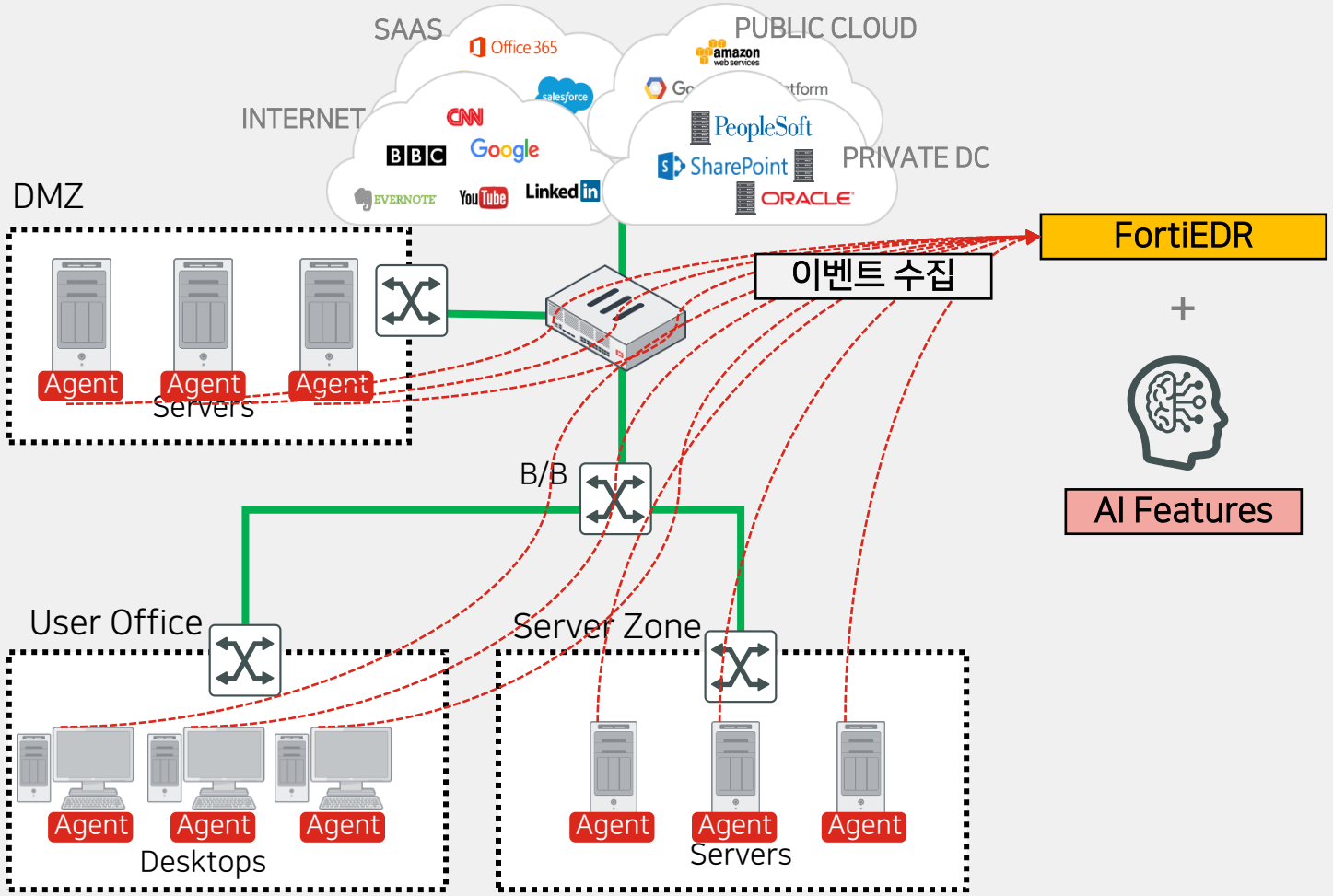
3. 딥러닝 기반 악성코드 탐지 관점의 보안솔루션들

"엔드포인트 기반 솔루션" + "딥러닝 AI 기능"

예: FortiEDR

[기본 역량]
- 엔드포인트 레벨 이벤트 수집(에이전트)
- 호스트수준의 깊은 데이터 가시성 확보
- 사고 추적 포렌직용 백데이터 확보
- 제품 별 상이한 수준으로 악성코드 방어 기능 탑재
- **XDR 로의 확장성**
  (Endpoint + Network + Cloud + Email…)

[+딥러닝 **AI** 기능]
- 딥러닝 기반 코드레벨 악성코드 탐지/차단
- 악성코드 스코어링



3. 딥러닝 기반 악성코드 탐지 관점의 보안솔루션들

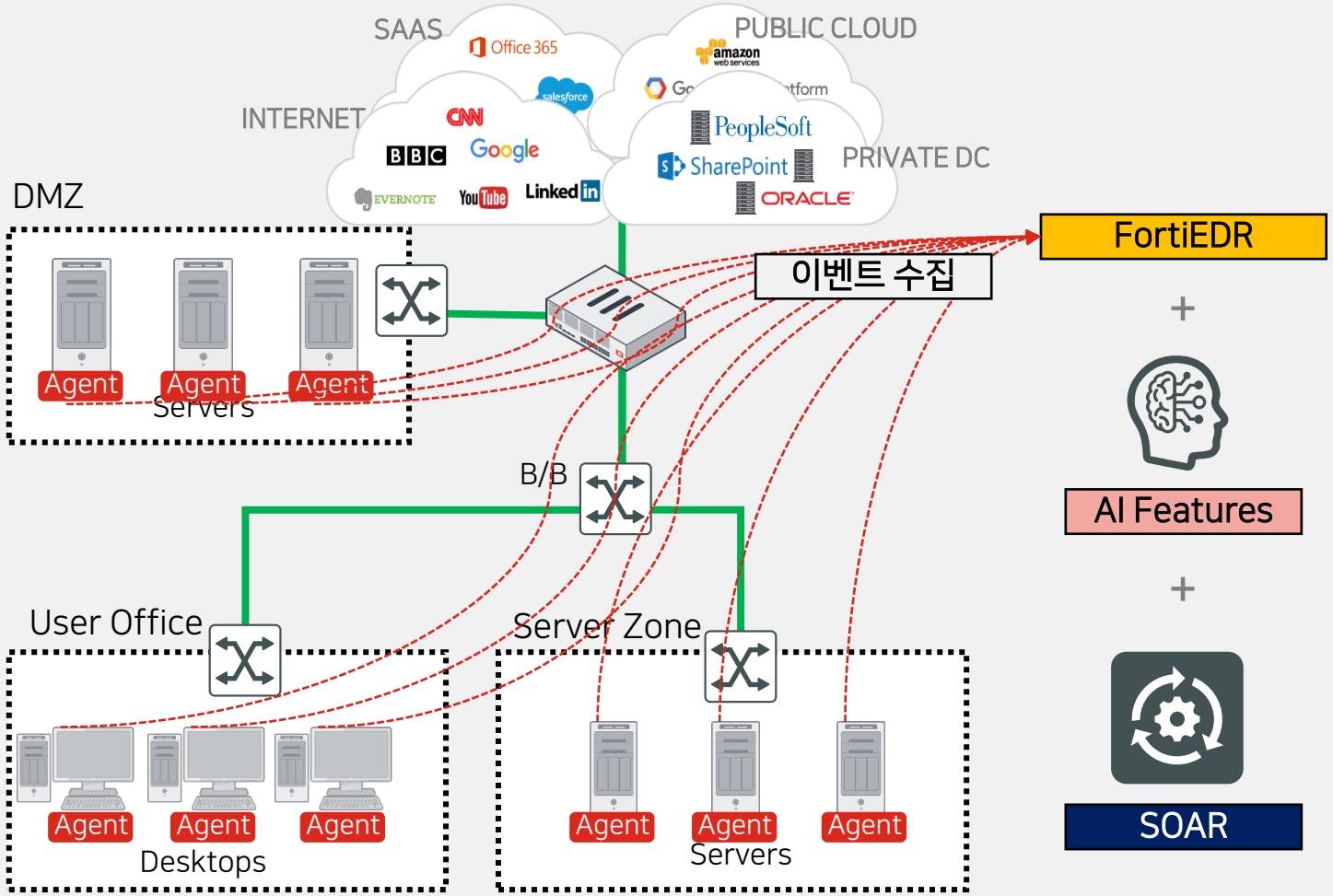
"엔드포인트 기반 솔루션" + "딥러닝 AI 기능" + "자동화 역량 "

예: FortiEDR

[기본 역량]
- 엔드포인트 레벨 이벤트 수집(에이전트)
- 호스트수준의 깊은 데이터 가시성 확보
- 사고 추적 포렌직용 백데이터 확보
- 제품 별 상이한 수준으로 악성코드 방어 기능 탑재
- **XDR 로의 확장성**
  (Endpoint + Network + Cloud + Email…)

[+딥러닝 **AI** 기능]
- 딥러닝 기반 코드레벨 악성코드 탐지/차단
- 악성코드 스코어링

[+자동화 역량]
- 플레이북 기반, 사람의 업무 절차를 자동화
- 이기종 보안시스템들과의 상호 작용
- 티켓팅/협업 기반 지능형 사고 대응 플랫폼



3. 그 외에도..

구분	+AI 역량
이메일	스팸, 악성 이메일 위협 탐지, 스코어링
데이터 유출 / 컴플라이언스	사용자/장치 행위 기반 내부자 정보유출/보안컴플라이언스 위반 감지
금융 사기 탐지	머신러닝 기반 학습 행동 패턴 대비 사기 위협 탐지
웹방화벽	머신러닝 기반 악성 봇 공격 탐지, 신종 패턴 컨텍스트 공격 대응
APT 샌드박스	기존 동적 분석 + 딥러닝 기반 코드레벨 악성코드 분석 보강
…	…

4. 일이 많아지는 AI솔루션의 몇가지 특징

- ✓ ***전에는 보이지 않던 새로운 이벤트가 탐지된다.***
  > 기계의 학습데이터를 기준으로 평시 활동과 상이한 행위 이벤트를 보여주므로, 놓치던 이벤트를 보게 되어 보안은 강화되는 효과가 있지만, 실무자 입장에서는 처리해야 하는 이벤트가 늘어나는 셈

- ✓ ***제품 최적화에 어려움이 있다.***
  > 모델/룰/정책을 직접 커스터마이징 할수 없거나, 화이트리스트 적용 등의 기능이 부족하여, 동일 유형의 이벤트를 매번 수동 처리 해야 하는 경우

- ✓ ***기존 패턴매칭(시그니쳐 등) 솔루션에 비해, 회색(Grey) 영역의 결과물이 많다.***
  > 사람이 재검증 하여야 하는 경우가 자주 발생

- ✓ ***평상시 대비 이상행위를 경고로 발생 시켜주지만, 정오탐을 판단할 백데이터가 부족한 경우가 많다.***
  > 탐지된 결과를 또다시 수동 분류하고, 수동으로 제3의 보안시스템 또는 Threat Intelligence에 조회해야 하는 경우가 다수 발생

- ✓ ***학습이 불가능한 수준으로 데이터 적거나, 수시로 다변화되는 환경에서 발생하는 이벤트를 신뢰할 수 없다.***
  > 상용 제품은 학습 기준에 대한 설정 변경을 할 수 없는 경우가 다수로, 결국 사람이 정밀 분석 해야 하는 것으로 이어지는 경우 발생

인공지능 침해사고 보안솔루션 선택 전략

1. 인공지능 침해사고 보안솔루션 선택 전략

(1) 트렌드만 따라가지 않고, AI 솔루션 도입 시 명확한 기대 효과&목표를 선정

목표 예시

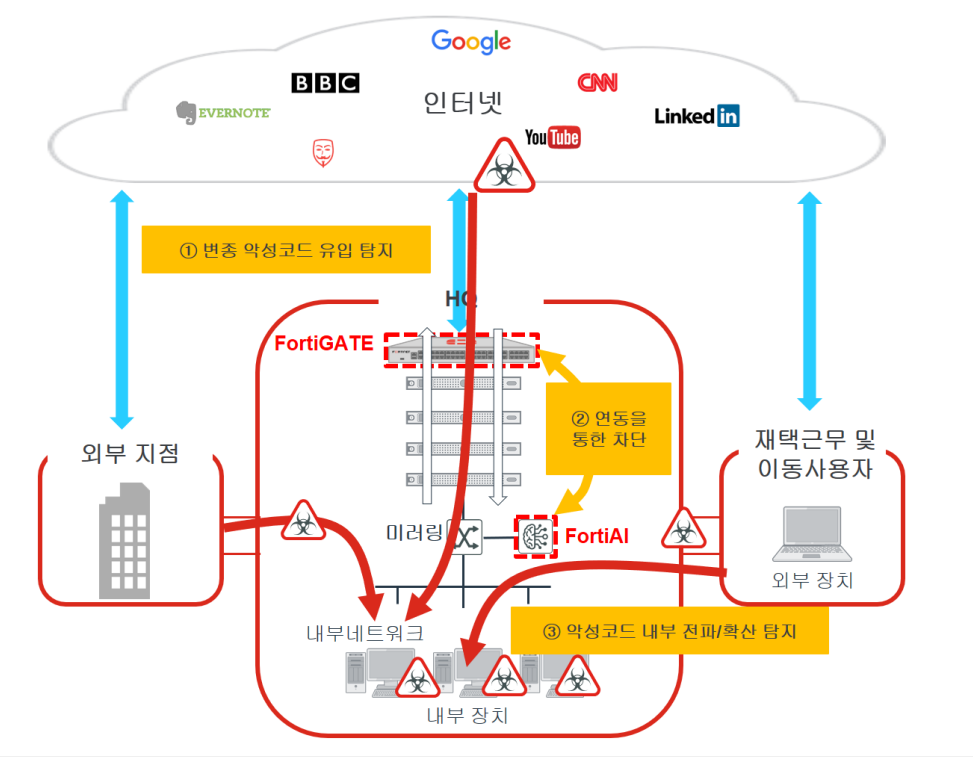
- 탐지 영역 고도화, 보완 가능한 제품으로 Security Hole을 최대한 예방하겠다.
- 서비스 영향도가 적은 형태로 구성하겠다.
- 자동화 기능을 통해 업무로드를 최소화하고 적은 인력으로 사용하겠다.
  - 분석 및 대응 부분 또는 전체 업무자동화
  - 사고 발생시 자동 추적, 연관 데이터 자동 집계
  - 보고서 자동 생성
- 탐지결과 중 위협도가 높은 것은 차단시스템 연동을 통해 우선 격리/차단 하겠다.

1. 인공지능 침해사고 보안솔루션 선택 전략

(2) 목적에 따라 AI기술 및 제품 후보 선택

검토 예시

- 침해사고의 주범인 “신/변종 악성코드” 를 탐지
- 네트워크 구간에 설치하여, 악성코드 유입/확산 탐지



포티넷의 딥러닝 기반 악성코드 탐지 시스템 FortiAI

구 분	APT 시스템	FortiAI
처리 성능(파일)	약 2,500개/1시간	약 100,000개/1시간
분석 시간	2~10분	1초>
트래픽 속에서 파일 직접 추출	▲	O
알려지지 않은 PE 악성코드 탐지	O	O
알려지지 않은 HTML 악성코드 탐지	X	O
File-less 형태 악성코드 탐지	X	O
알려지지 않은 Javascript 악성코드 탐지	X	O
알려지지 않은 VBS / VBA 형태 악성코드 탐지	X	O
알려지지 않은 오피스 문서 형태 악성코드 탐지	▲	O
내부 전파 행위 탐지	X	O
내부 전파 경로 파악 보고서 제공	X	O

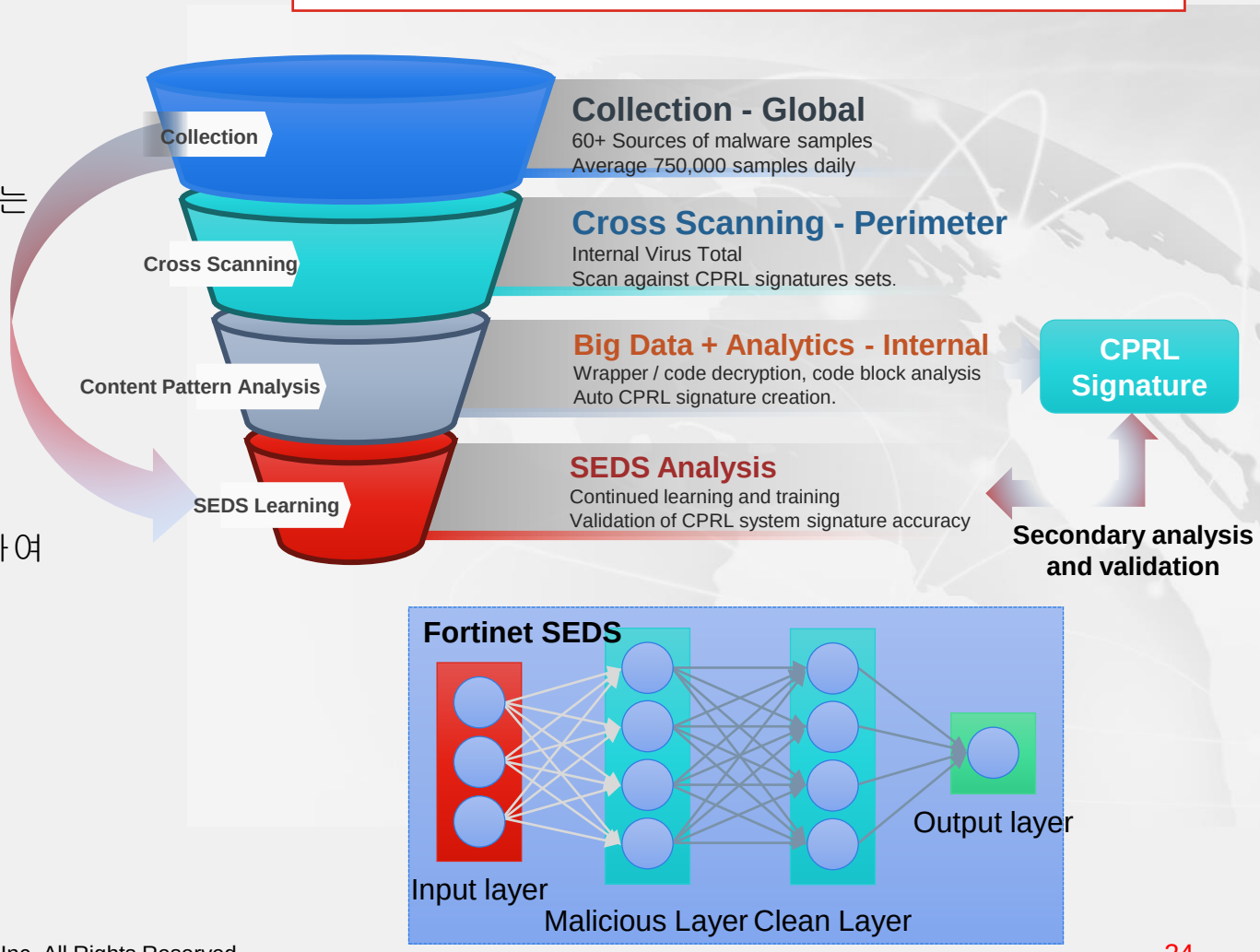
1. 인공지능 침해사고 보안솔루션 선택 전략

(3) 목표에 적합한 양질의 데이터 활용이 가능한 제품인지 검토

검토 예시

- 딥러닝 기반 제품
  - 정확하고 충분한 양의 사전 학습 데이터셋을 학습 할 수 있는 시스템이 제조사에 갖춰져 있는가
  - 온프레미스 자가학습, 적극적인 패치 등을 통해 탐지 DB를 개선할 수 있는가
- 머신러닝 기반 제품
  - 조직에서 발생하는 다양한 데이터 소스를 어디까지 수용 하여 학습에 반영 할 수 있는가
  - 인풋 데이터에 따라 제품의 설계 의도대로 학습되며, 아웃풋 데이터가 적합하게 나오는가 (Drop, 손실, 성능, 기능 제약 여부)

포티넷의 FortiGuard 연구소 – AI 학습 체계



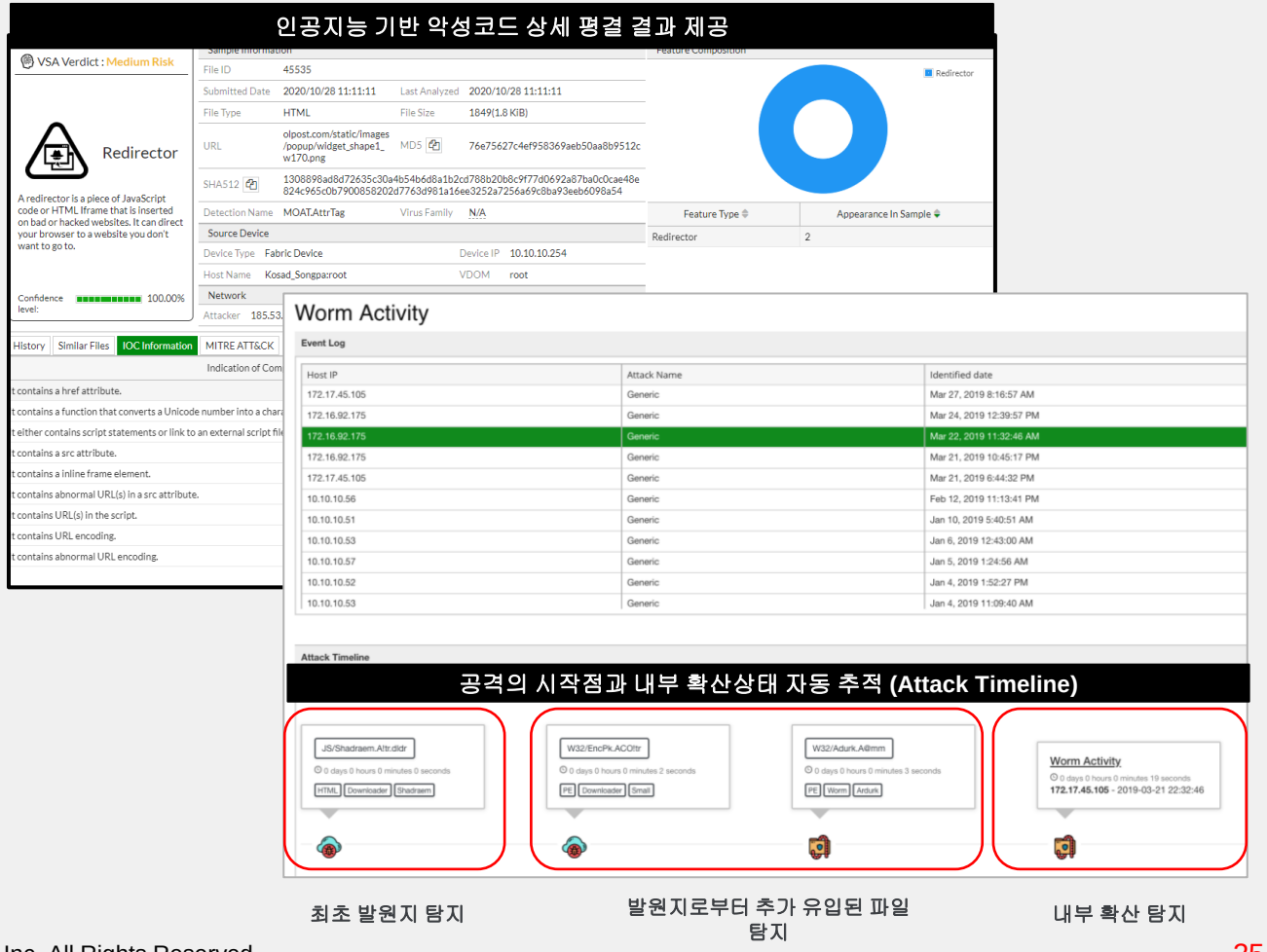
1. 인공지능 침해사고 보안솔루션 선택 전략

(4) 결과를 직관적으로 제공하는지 검토

검토 예시

- 탐지 결과에 대한 명확한 정의
  - 유형: 비정상행위, 사용자 이상행위, 변종 악성코드분석 등
  - 내용: 유사도 또는 벗어난 정도, 프로파일링 데이터, 매칭 특징
- 결과 검증을 위한 상세 데이터 제공
  - 상세 탐지근거/분석결과 등의 보강데이터
  - 상관관계, 연관데이터 등의 분석용 백데이터
  - 사고 자동 추적에 대한 이벤트 데이터

포티넷 딥러닝 기반 악성코드 탐지 시스템 FortiAI 화면



1. 인공지능 침해사고 보안솔루션 선택 전략

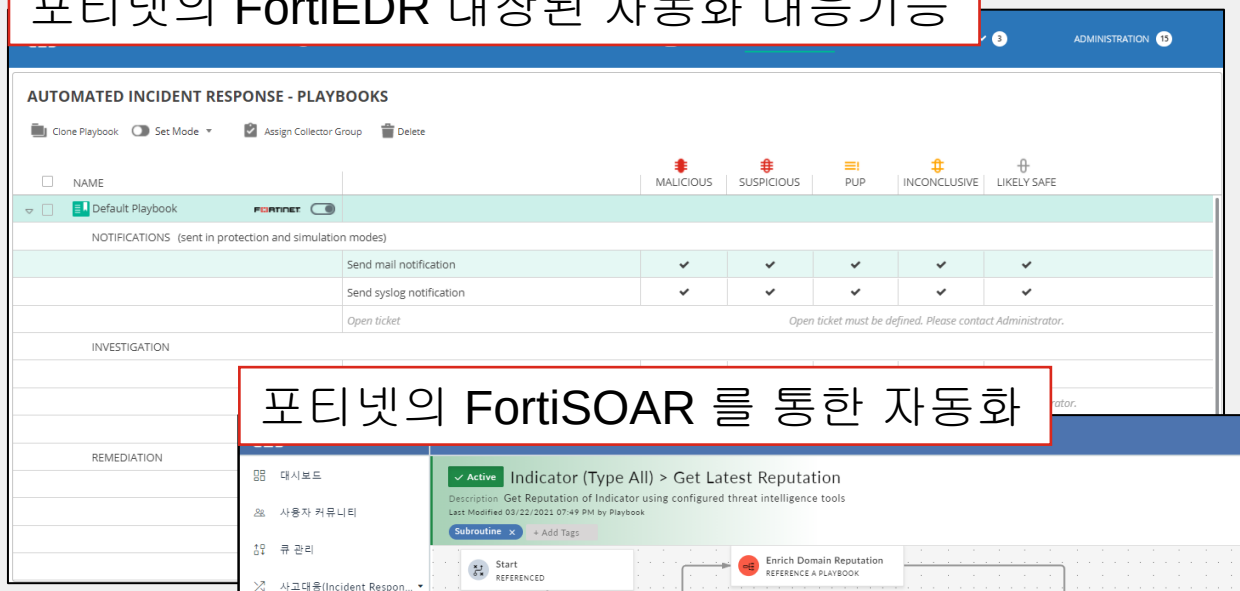
(5) 업무로드를 최소화할 수 있는 역량으로 적은 인력으로도 사용이 가능한지 검토

검토 예시

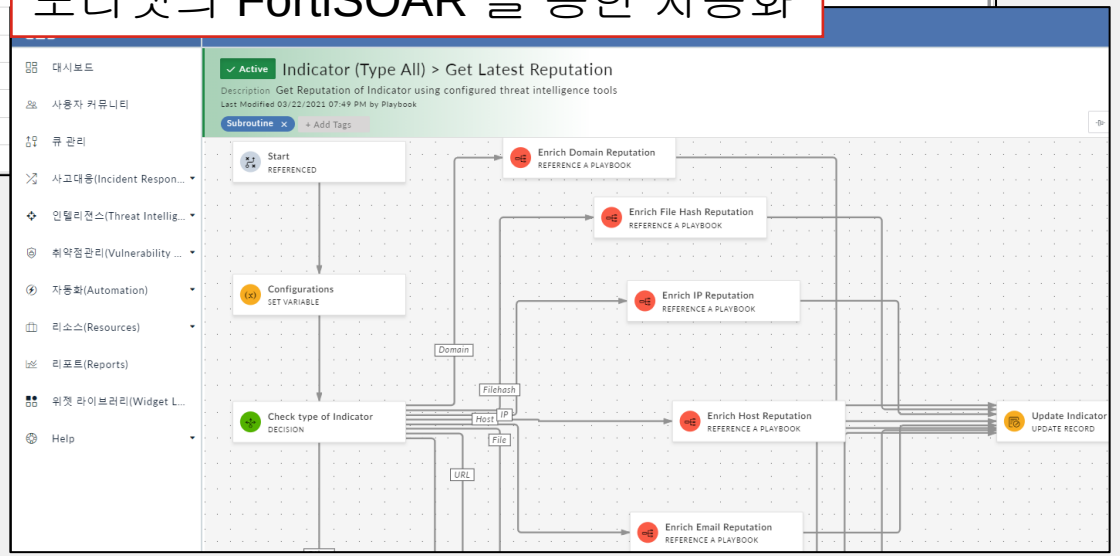
- 빠른 조치를 위한 환경을 제공하는가
  - 위협도/유사도/악성코드의 특징 정보 제시하여 대응 우선순위 제공
  - 유입/확산/추가다운로드 이력 추적 자동 보고서 제공

- 자동화 가능 여부(Built-In 또는 연동)
  - 고위험 이벤트 발생, 관제 부재시 대응을 위한 자동화 기능

포티넷의 FortiEDR 내장된 자동화 대응기능



포티넷의 FortiSOAR 를 통한 자동화

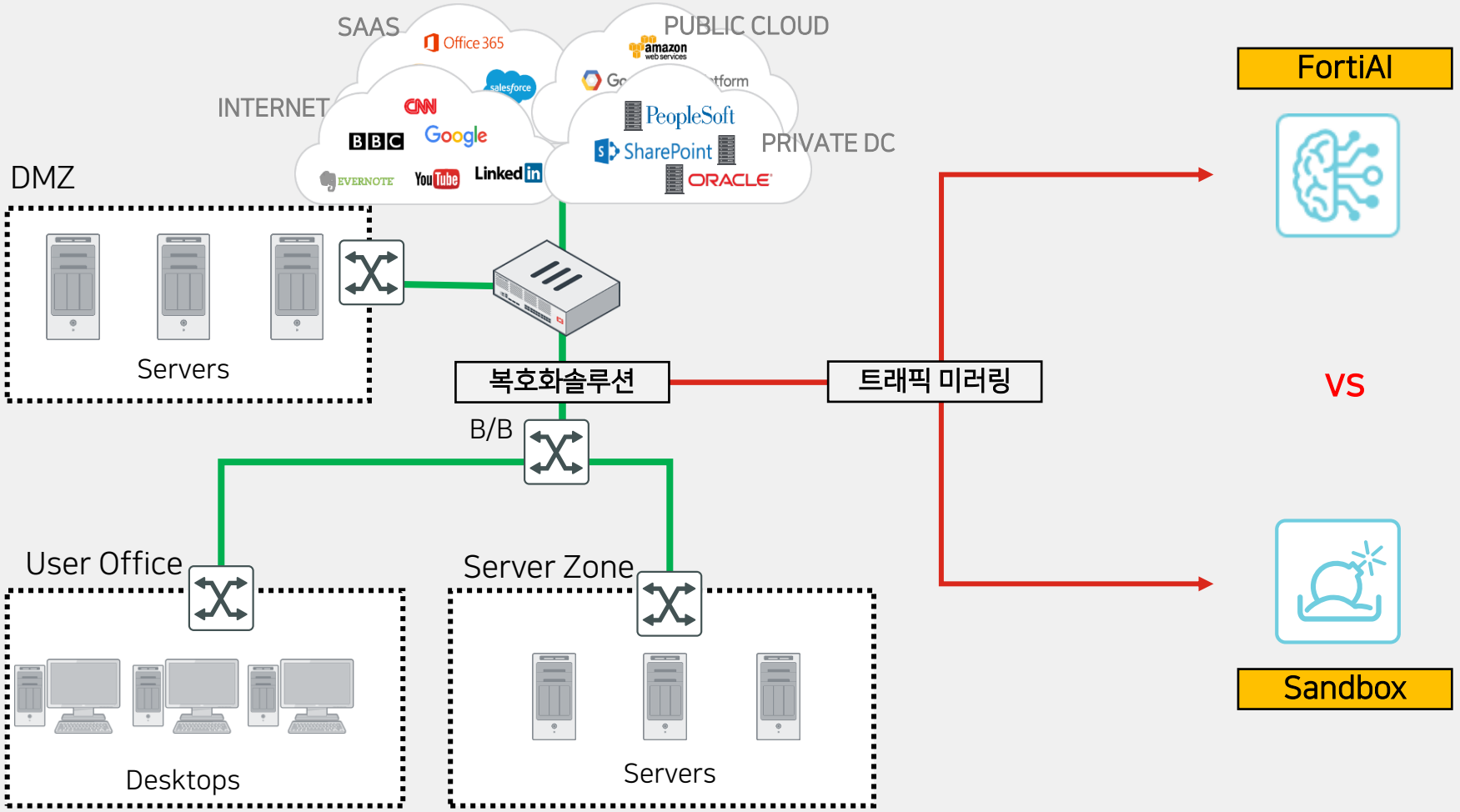


포티넷 AI 솔루션 데모

FortiAI & FortiSandbox

FortiAI & FortiSOAR & FortiEDR

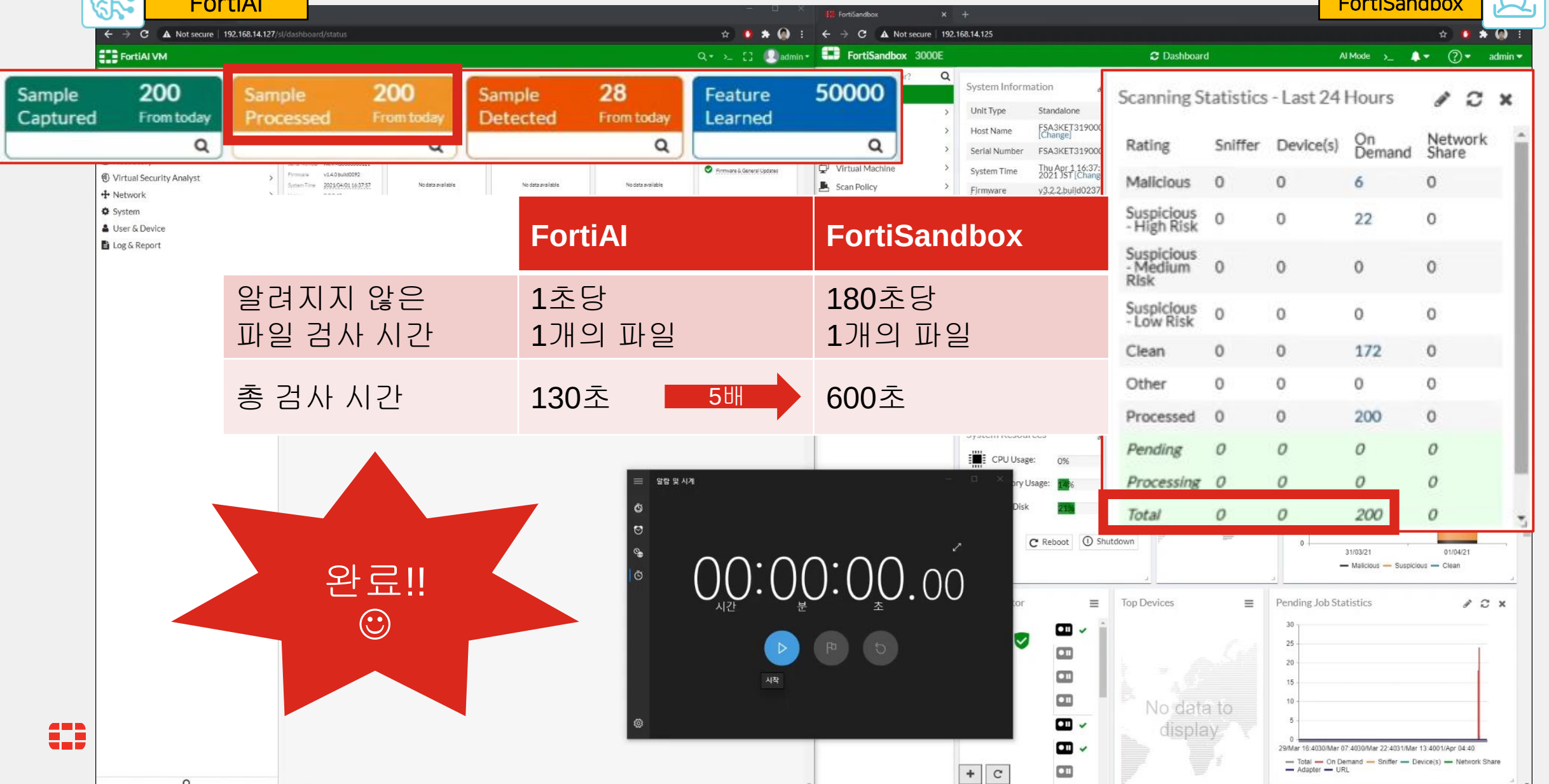
FortiAI & FortiSandbox 데모구성도



FortiAI & FortiSandbox 비교 데모

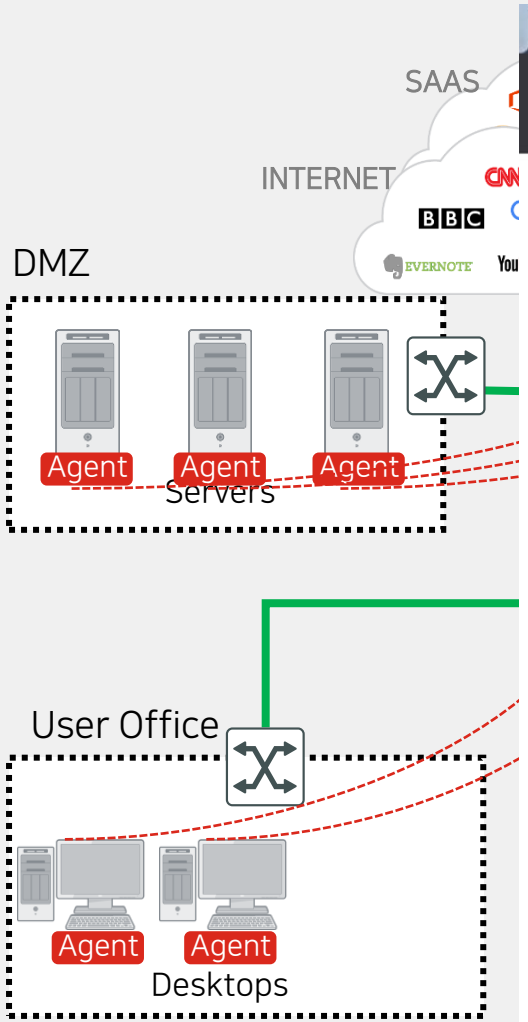
FortiAI

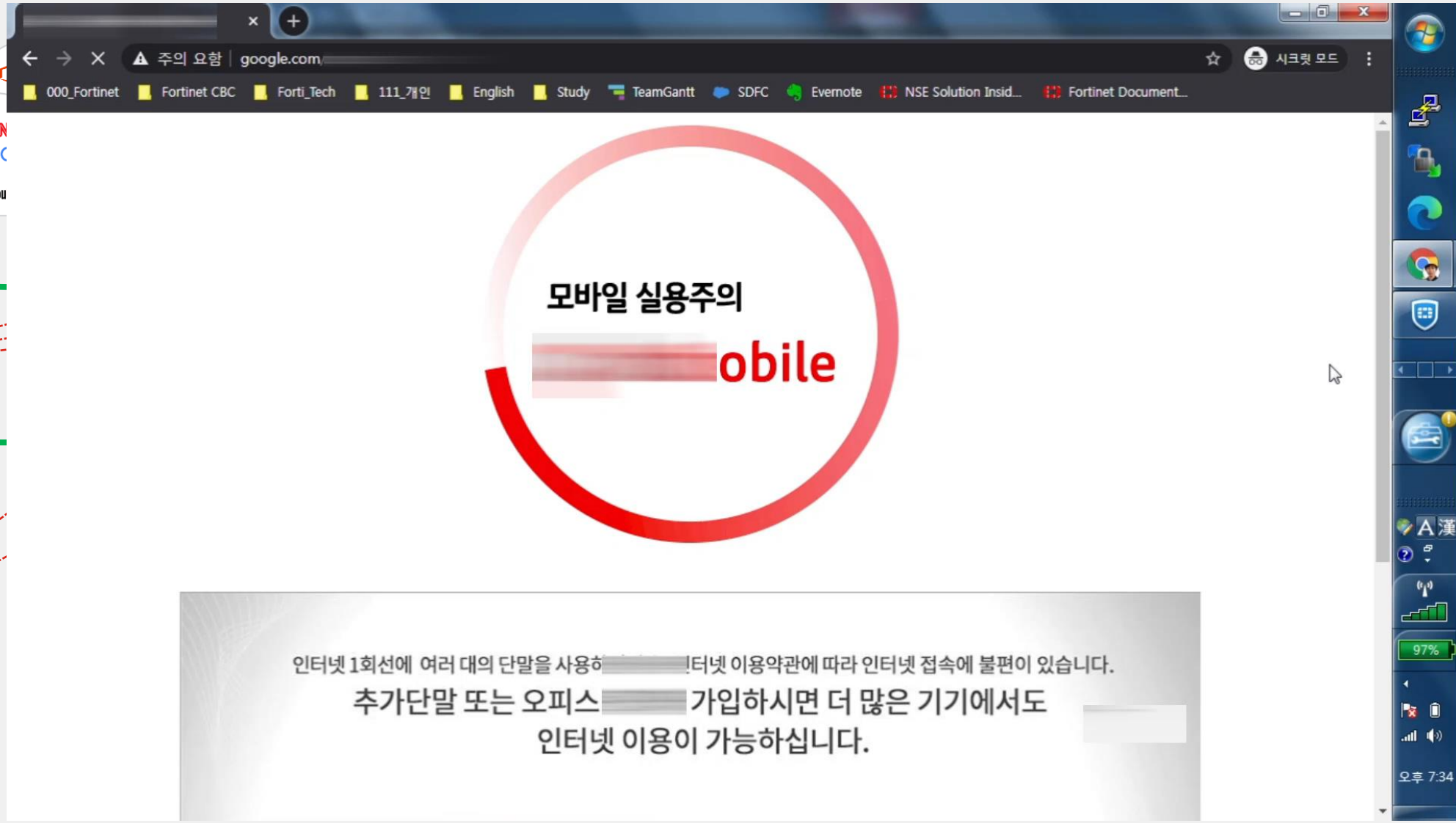
FortiSandbox



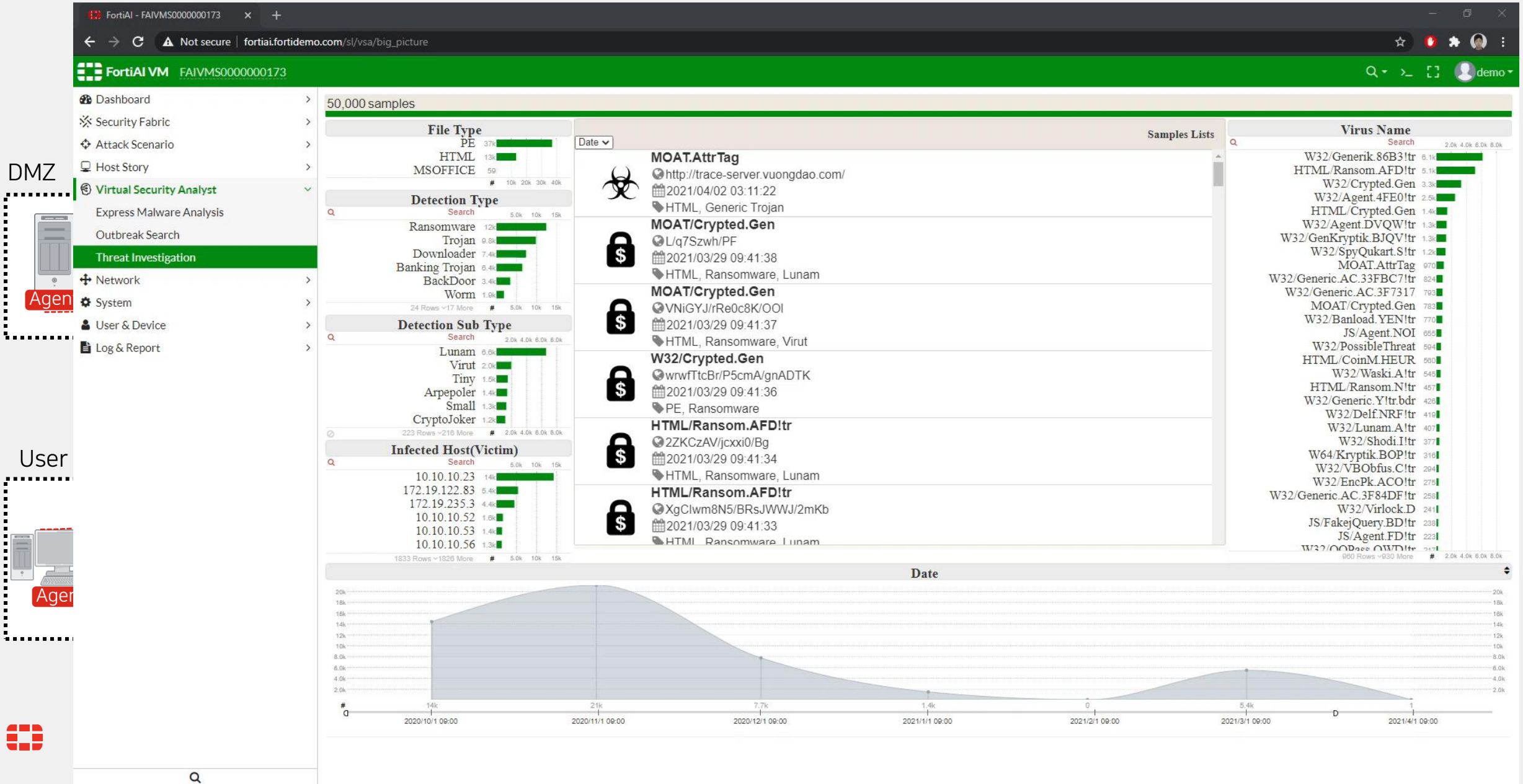
	FortiAI		FortiSandbox
알려지지 않은 파일 검사 시간	1초당 1개의 파일		180초당 1개의 파일
총 검사 시간	130초	5배	600초

FortiAI + FortiEDR + FortiSOAR 시나리오

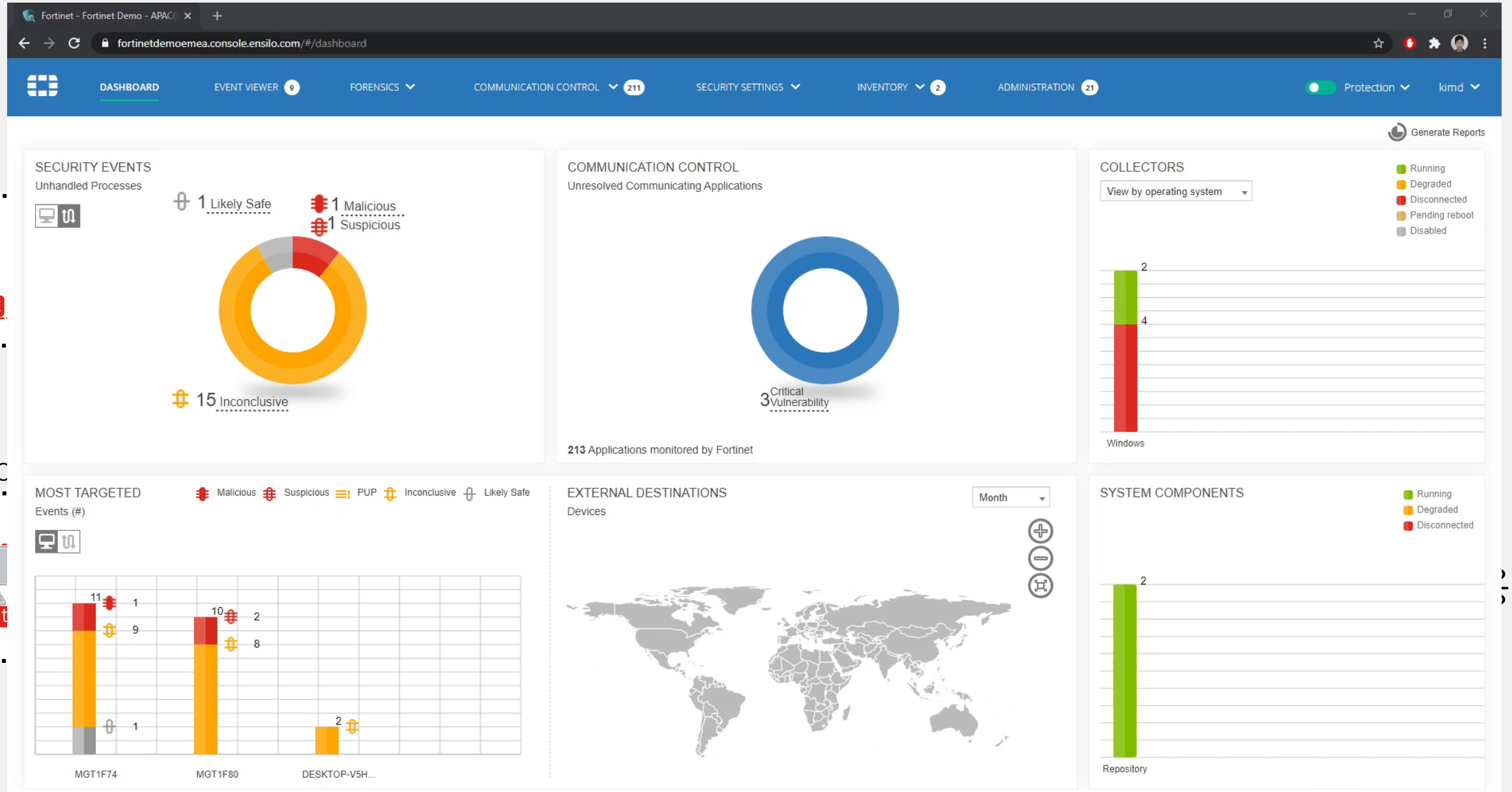




FortiAI + FortiEDR + FortiSOAR 시나리오



FortiAI + FortiEDR + FortiSOAR 시나리오



DMZ

Agent

User C

Agent

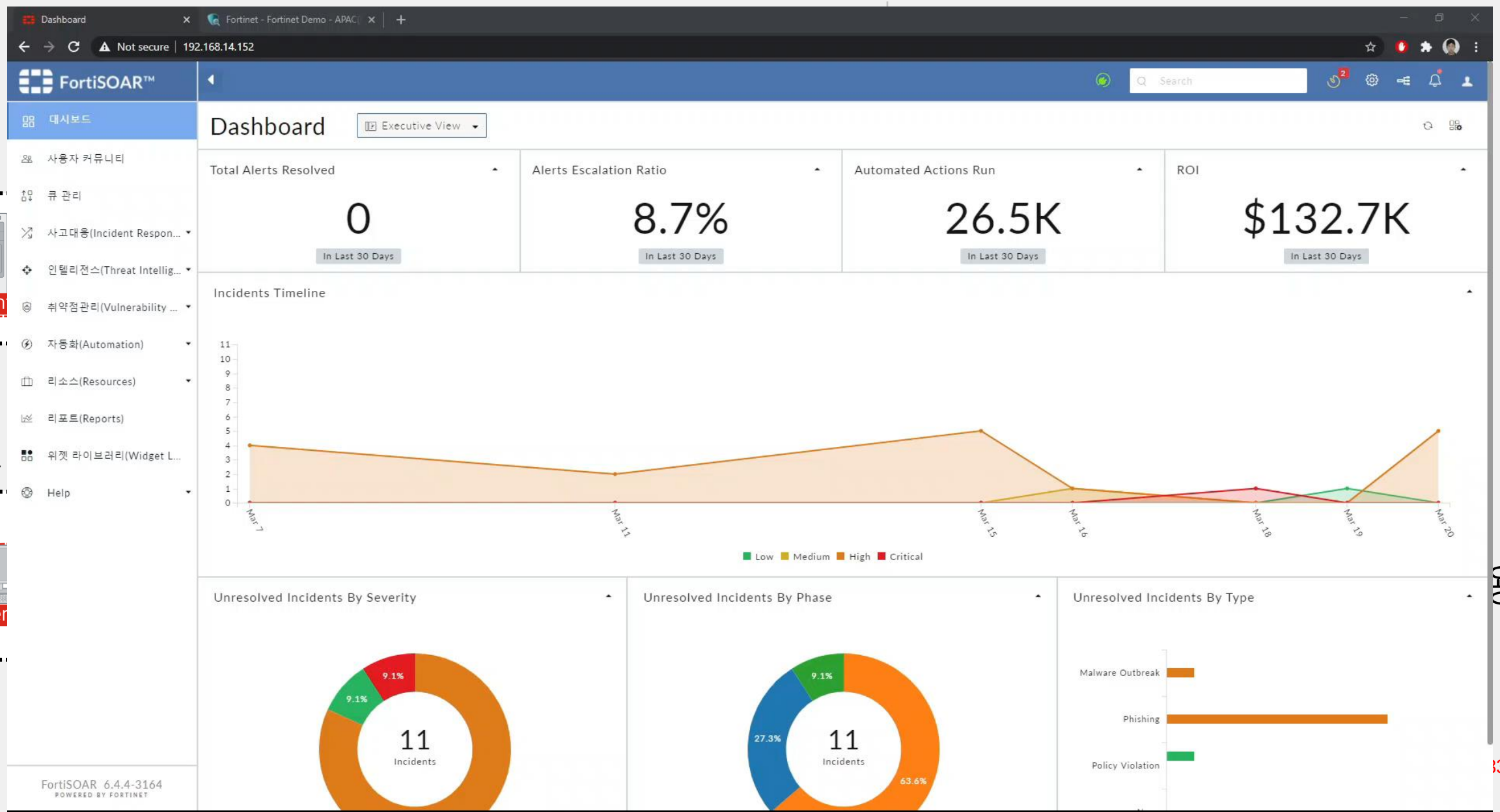
FortiAI + FortiEDR + FortiSOAR 시나리오

DMZ

Agent

User

Agent



(옵)

Summary

요약

요약 정리

- ✓ **AI** 상용 보안솔루션 시장은 성장해 가는 단계이며, 제조사들은 다양한 분야에 대해 기능의 일부로써 또는 제품자체로서 많은 상품화 시도가 이루어지고 있다.

- ✓ 이 시점에서, **AI** 기술 트렌드라는 물결에 휩쓸려 급하게 도입하게 되는 경우, 오히려 일이 많아 지거나, 기대 효과에 전혀 미치지 못하는 형태가 될 수 있다.

- ✓ 성공적인 **AI** 보안상용솔루션 도입을 위해서는 잘 설정된 목표를 기준 삼아, 충분한 검증 과정을 거쳐, 구축 환경 및 용도에 적합한 제품을 선택하여야 한다.
  - 기대 효과 정리 -> 목표 설정 -> 목표에 적합한 **AI** 기술 체크 -> 제품 후보군 조사 -> 기능 체크 -> 데모를 통한 검증

- ✓ 데이터 활용이 가장 **Key**가 되는 중요한 영역이므로, **AI** 동작 방식에 따라 데이터를 잘 활용 할 수 있는 시스템 체계를 갖추었는지, 제조사가 그런 체계를 공급할 수 있는 역량이 있는지 살펴보아야 한다.


FORTINET