SentryAPT

차세대 보안 솔루션

에스지에이솔루션즈 전략기획팀 최종태 이사

2018. 04

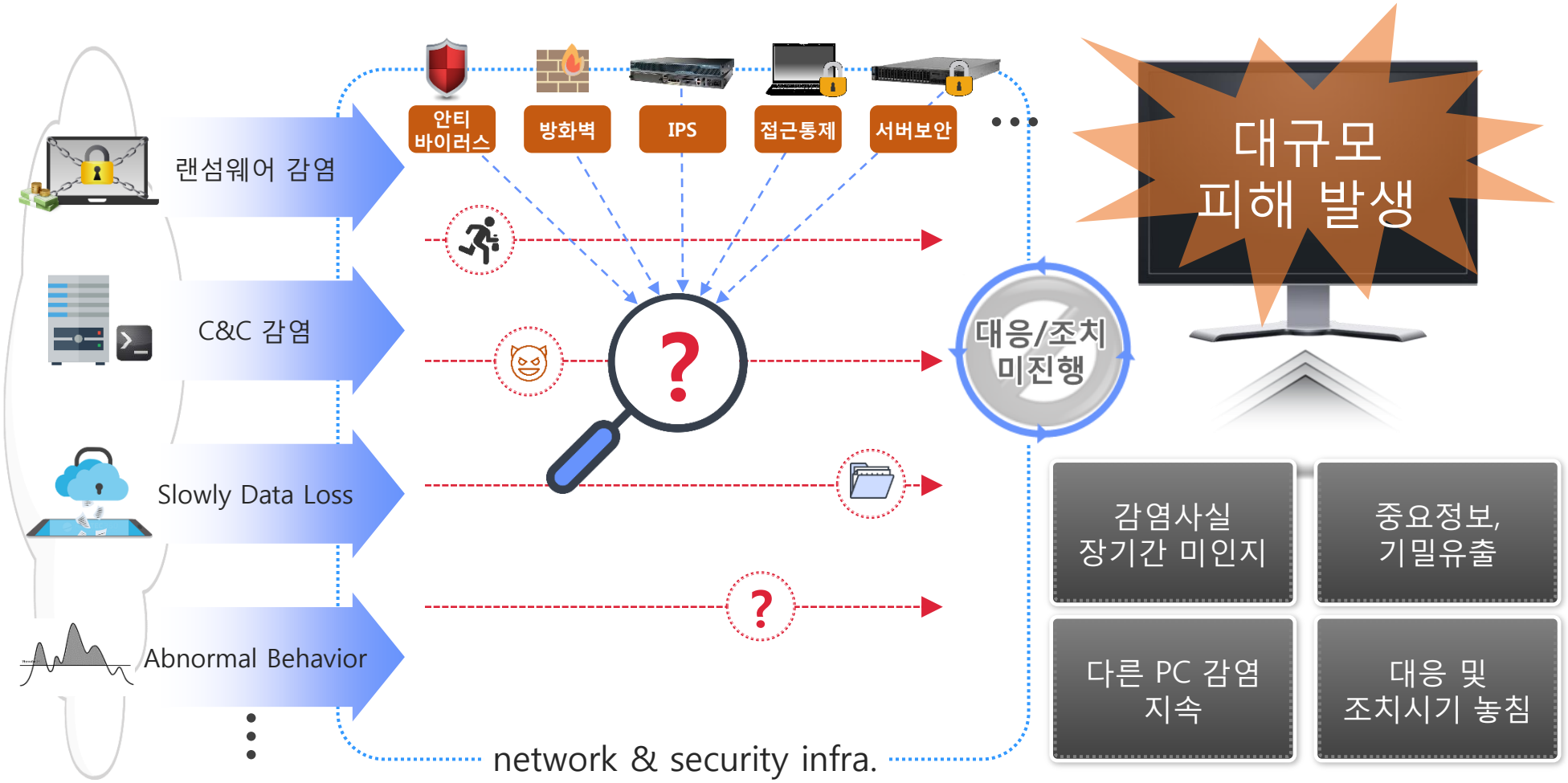
CONTENTS

Ⅰ. 최신 보안위협 및 APT

1. 보안 위협의 고도화 및 지능화
2. 기존 보안체계의 한계에 따른 피해
3. APT 공격의 정의
4. APT 공격 단계별 위협
5. 국내 APT 보안 위협의 현황
6. 국내·외 APT 공격 사례

1. 보안 위협의 고도화 및 지능화

최근의 악성코드 또는 행위기반의 보안 위협들은 백신 조차 무력화 할 정도로 고도화·지능화되고 있는 추세

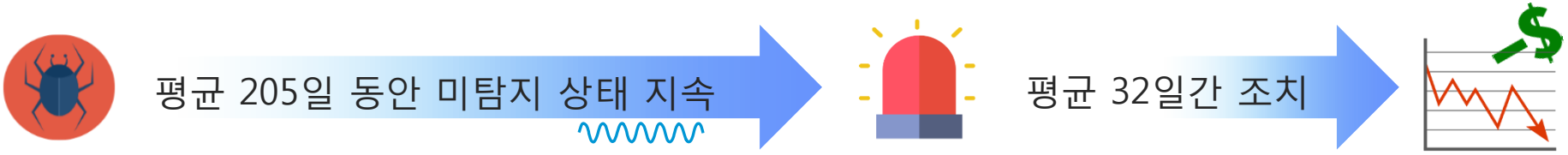


2. 기존 보안체계의 한계에 따른 피해

기존 단위 보안체계에서는 최신 위협 대응에 한계가 있으며, 이에 따른 비즈니스적 손실이 지속적으로 발생

205일	• 탐지까지 소요되는 평균 일 수
32일	• 침해 대응에 소요되는 평균 일 수
35억	• 침해사고 발생 시 평균 피해액
69%	• 피해기관은 외부로부터 침해사실을 통보 받음
100%	• 방화벽 보유, 백신 및 각종 패턴 최신버전 유지

<※ Mandiant Mtrends Report>



보안사고는 "비즈니스 가치 손실" 과 직결

3. APT 공격의 정의

APT 공격은 지능적(Advanced)이고 지속적(Persistent)으로 이루어지는 최신 보안위협 유형을 의미함

Advanced
Persistent
Threat

비즈니스 또는 정치적·악의적인 '목적'을 가지고 표적 대상에게
오랜기간 고도화된 '지능적, 지속적' 공격으로 목표를 달성할 때까지,
'은밀'하게 기밀정보 유출이나 시스템을 파괴하는 행위

APT 공격에 따른 APT Kill Chain 매핑 및 각 단계별 주요 침해행위

- 파일 송·수신/Web/E-Mail 등을 통한 악성코드 감염
- SQL인젝션, 익스플로잇
- 제로데이 취약점 이용
- 사회공학/스피어피싱을 통한 감염 등

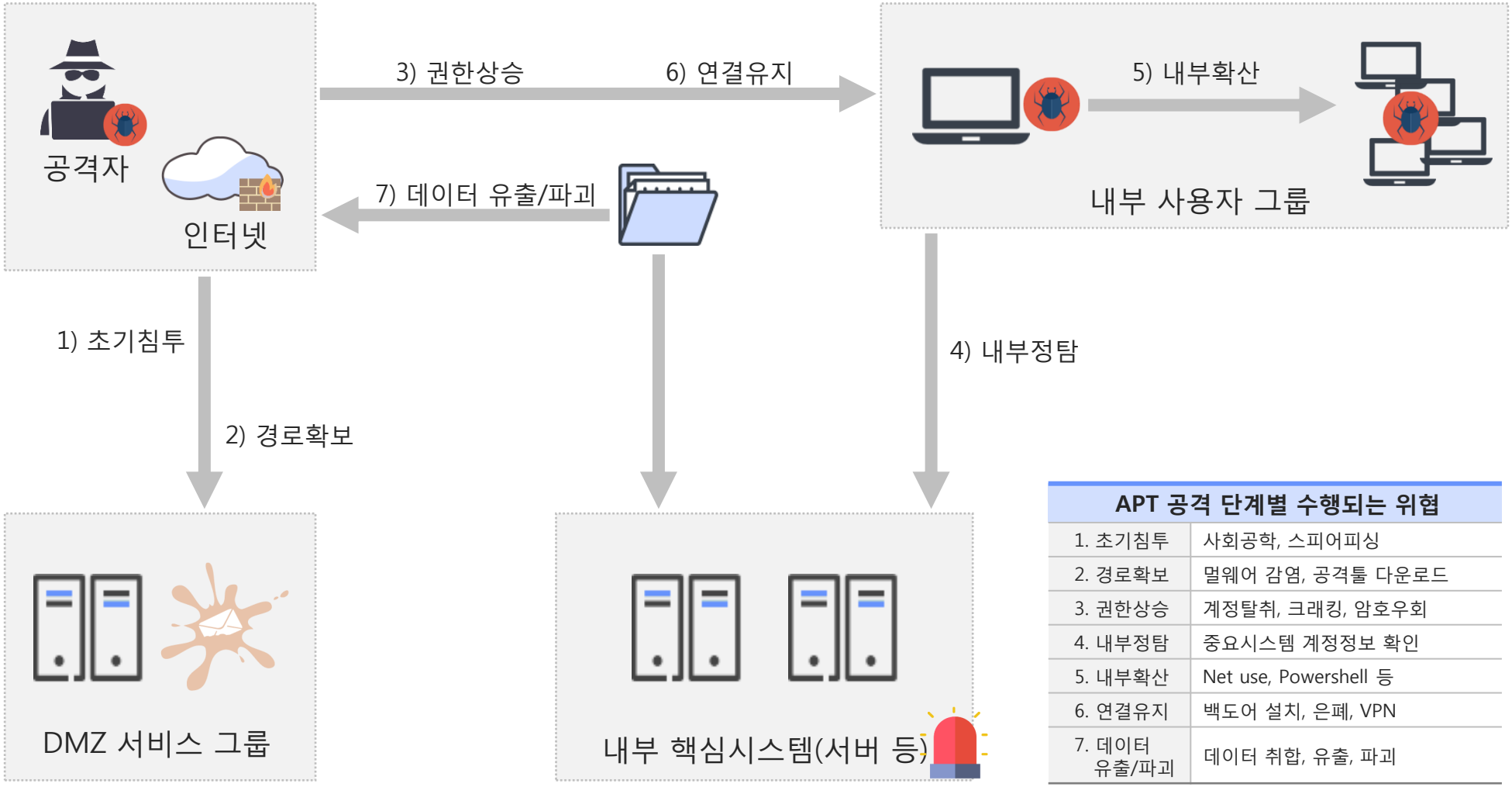
- 공격 툴 다운로드
- Run Silent 기술 (은밀히 보안탐지 등을 회피)
- 프로세스 검색 회피

- 중요 서버(DB) 또는 대고객 서비스 서버 장악
- 중요 서버의 기밀 데이터 수집

- 중요 내부 데이터의 외부 전송 (원격접속 또는 FTP)
- 대상 서버 파괴
- 로그 및 흔적 삭제

4. APT 공격 단계별 위협

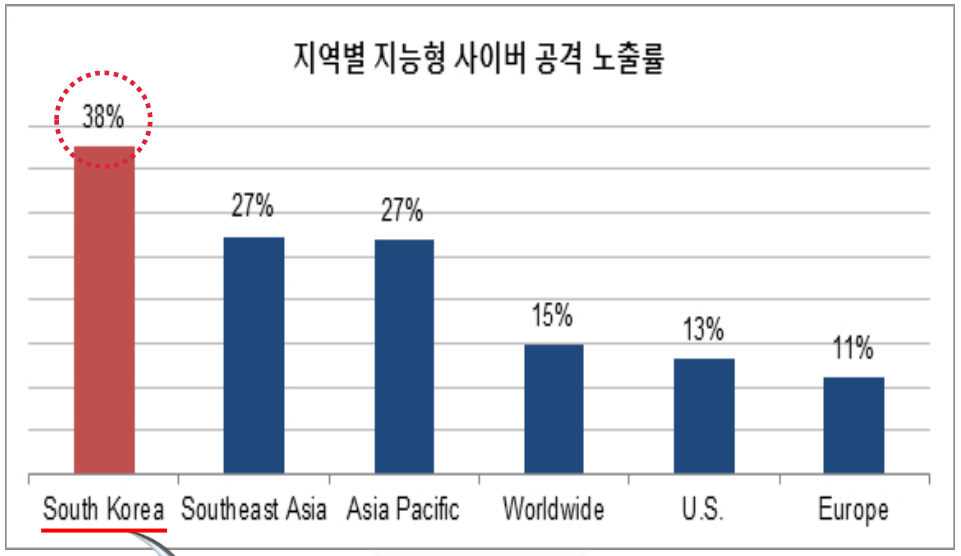
APT는 초기침투 과정부터 데이터 유출/파괴에 이르기까지 제로데이, 악성코드, 사회공학 기법 등 다양한 공격 수행



APT 공격 단계별 수행되는 위협	
1. 초기침투	사회공학, 스피어피싱
2. 경로확보	멀웨어 감염, 공격툴 다운로드
3. 권한상승	계정탈취, 크래킹, 암호우회
4. 내부정탐	중요시스템 계정정보 확인
5. 내부확산	Net use, Powershell 등
6. 연결유지	백도어 설치, 은폐, VPN
7. 데이터 유출/파괴	데이터 취합, 유출, 파괴

5. 국내 APT 보안 위협의 현황

취약점 공격 및 악성코드 감염 등의 보안 위협들을 포함하여 C&C 콜백 등 최다 APT 공격 노출



<※ FireEye>

<※ 보안뉴스(2017.01.13)>

침해사고 사례

- C&C 콜백 목적지로 가장 많이 이용된 국가
- 취약점 공격, 악성코드 감염 위협에 가장 많이 노출된 국가
- C&C 서버로의 APT 콜백이 가장 많이 발생한 국가
- 전 세계적으로 최다 APT 공격 노출율에 랭크됨

※ 주요 방송사와 은행, 카드사 등의 전산망이 마비되었던 사건

6. 국내·외 APT 공격 사례

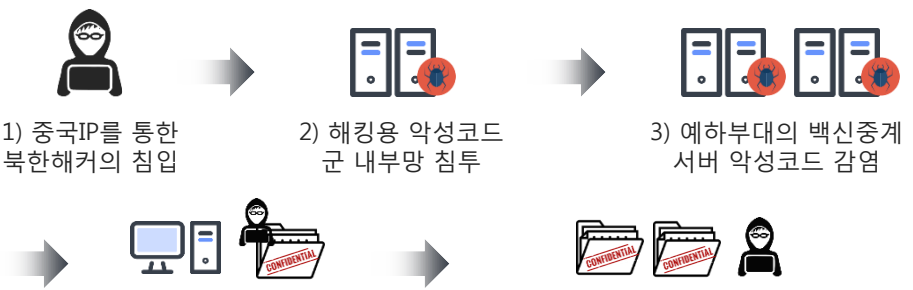
한수원, 국방부, 방송·통신 등 다양한 산업분야에서 기술결함, 회사 인프라, 구성원의 취약점을 두루 악용한 공격

한국수력원자력 정보유출 및 협박

1) 중국IP를 통한 북한해커의 침입
2) 직접접속 또는 VPN을 통한 자료유출 (직원 개인정보, 이메일, 내부PC자료)
3) 한수원 공격 시도 (악성코드 이메일 발송)
4) 공격실패
5) 대형포털 및 SNS에 자료공개 및협박

- 한국수력원자력 내부 기밀자료 및 개인정보 유출 사건(2014년)

국방부 내부 국방망 해킹 및 군 기밀자료 유출



1) 중국IP를 통한 북한해커의 침입
2) 해킹용 악성코드 군 내부망 침투
3) 예하부대의 백신중계 서버 악성코드 감염
4) 군내 PC에 저장된 기밀자료 확보
5) 군 외부망을 통한 군 기밀자료 유출 (정확한 유출내용 파악 불가)

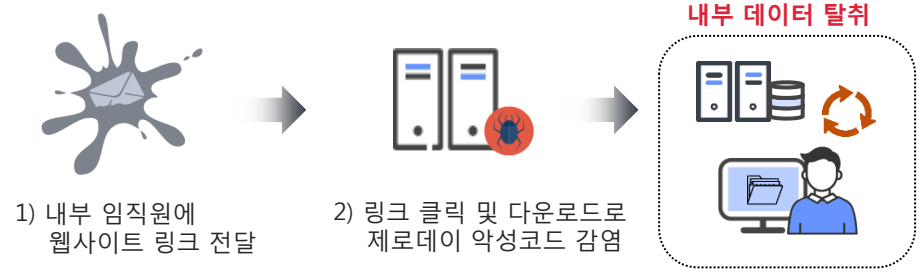
- 국방부 내부 국방망 해킹을 통한 군 기밀자료 유출 사건(2016년)

중국 기간시설 파괴 (스턱스넷)

1) 인터넷에 연결된 PC에 폭넓게 감염
2) USB를 통해 기간시설 내부망에 침투

- 중국의 댐, 공항, 철도 등 산업시설 1000곳, PC 600만대 감염

모건스탠리 사건 (오로라 사건)



1) 내부 임직원에 웹사이트 링크 전달
2) 링크 클릭 및 다운로드로 제로데이 악성코드 감염

- 구글과 모건스탠리 등에서 해킹을 통해 중요 정보를 탈취한 사건

Ⅱ. 제품 분류체계 및 포지셔닝

1. 악성행위 처리방식에 따른 APT 솔루션의 분류
2. 기존 보안위협 대응 솔루션의 한계
3. 보안위협 대응 주요 벤더사 및 제품
4. 제품의 구현 목표
5. 제품의 포지션

1. 악성행위 처리방식에 따른 APT 솔루션의 분류

악성행위 처리 방식에 따른 분류체계와 이에 대한 명백한 차이점을 기반으로 Post-Sandbox 제품의 중요성 부각

Sandbox type

- 가상화 기반의 악성행위 샌드박싱, 모니터링, 분석
- 네트워크 영역을 기반으로 한 모니터링 및 분석

샌드박싱 형태의 대부분의 Security Solution

FireEye, paloalto NETWORKS, McAfee, TREND MICRO, lastline, AhnLab, SOPHOS, FORTINET

❖ **엔드포인트 보안영역의 제품과 결합(통합) 모색**

- 엔드포인트 벤더 인수/합병
- 서버, PC 탑재용 에이전트 개발
- 취약영역 보완 및 침해 대응력 강화

Post-Sandbox type

- 주로 PC 단위 로그 수집, 분석, 대응
- 엔드포인트 보안 솔루션 기반에서 APT 보안 솔루션으로 개선 및 확장 표방

Gartner (January 2017) 분류 → EDR, EPP

- 2019년까지 EPP 및 EDR 영역이 단일 영역의 제품으로 합쳐질 것으로 예상
(Gartner "Magic Quadrant for Endpoint Protection Platforms, 30 January 2017)

FireEye, Carbon Black., TREND MICRO, KASPERSKY, RSA, Symantec., SOPHOS, cybereason, GUIDANCE SOFTWARE, CYLANCE, SentinelOne, AhnLab, Genians, NICSTECH, NPCORE

LIGHTCYBER, VECTRA, TANIUM, splunk>, OUTLIER, VERINT → SIEM, NTA

2. 기존 보안위협 대응 솔루션의 한계

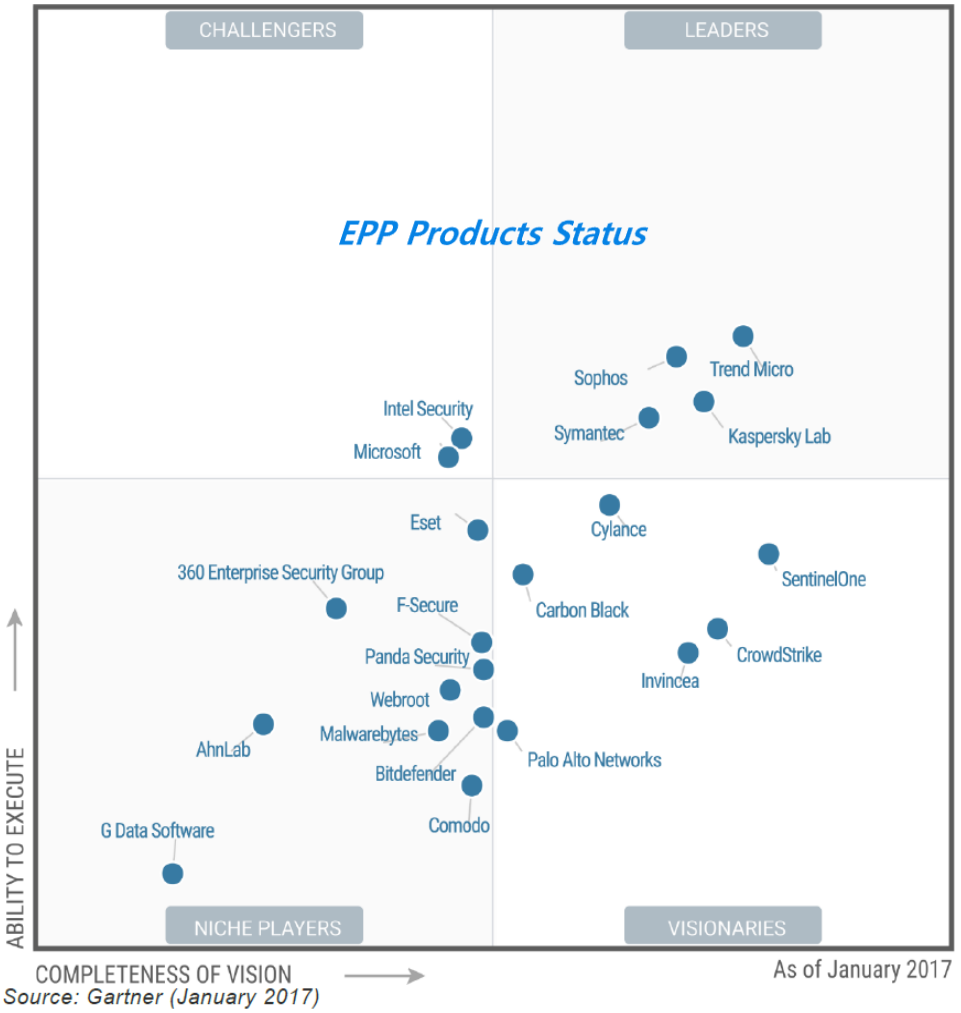
다양한 방식의 보안 위협대응 솔루션들은 해당 솔루션이 적용되어지는 특정 유형 및 영역에 대한 한계성이 있음

제품군 구분	주요 기능 및 역할	기반 솔루션	한계점
NTA (Network Traffic Analysis)	• 네트워크 관문을 경유하는 트래픽 모니터링 기반 • 네트워크 수준에서의 접근통제	• Network Firewall/UTM • IPS(Intrusion Prevention System) • Web Security Gateway	• **서버, PC 자체의 취약점, 위협 탐지 불가** • **악성행위, 취약점의 근원에 대한 해결 불가**
SIEM (Security Information & Event Management)	• 보안제품들의 로그 수집, 통합 • 임계치 기반의 이벤트 도출 • 통계, 보고 및 분석이 주 용도	• 로그 수집/통합 솔루션 • 로그 관리 솔루션 • ESM 기반 관리대상의 원시로그 수집	• **보안장비, 서버들에 대한 로그수집 및 관리가 주 목적임** • **추가 분석, 위협 대응 불가 (3rd party 제품과 연동)**
EDR (Endpoint Detection & Response)	• 엔드포인트 시스템 레벨의 동작 및 이벤트 탐지(예: 사용자, 파일, 프로세스, 레지스트리, 메모리 및 네트워크 이벤트) • 알려진 위협 데이터베이스(패턴DB) 기반 침해식별 및 대응	• Anti-Virus • Anti-Malware • 개인정보보호솔루션	• **대부분 알려진 위협에 대해서만 탐지** • **Windows PC 영역에 대해서만 지원** • **EPP 영역으로 흡수/통합되는 추세임**
EPP (Endpoint Protection Platform)	• 멀웨어 방지, 개인 방화벽, 포트 및 장치 제어와 같은 기능을 갖춘 통합 솔루션	• PC Internet Security • PC Firewall • PC Device Access Control • DLP(Data Loss Prevention)	• **기업의 정보유출 방지의 목적이 강함** • **Windows PC 영역에 대해서만 지원**

3. 보안위협 대응 주요 벤더사 및 제품

제품군에 따른 주요 벤더사 및 제품들이 존재하며, APT 제품을 기반으로 한 지속적인 흡수, 통합이 이루어짐

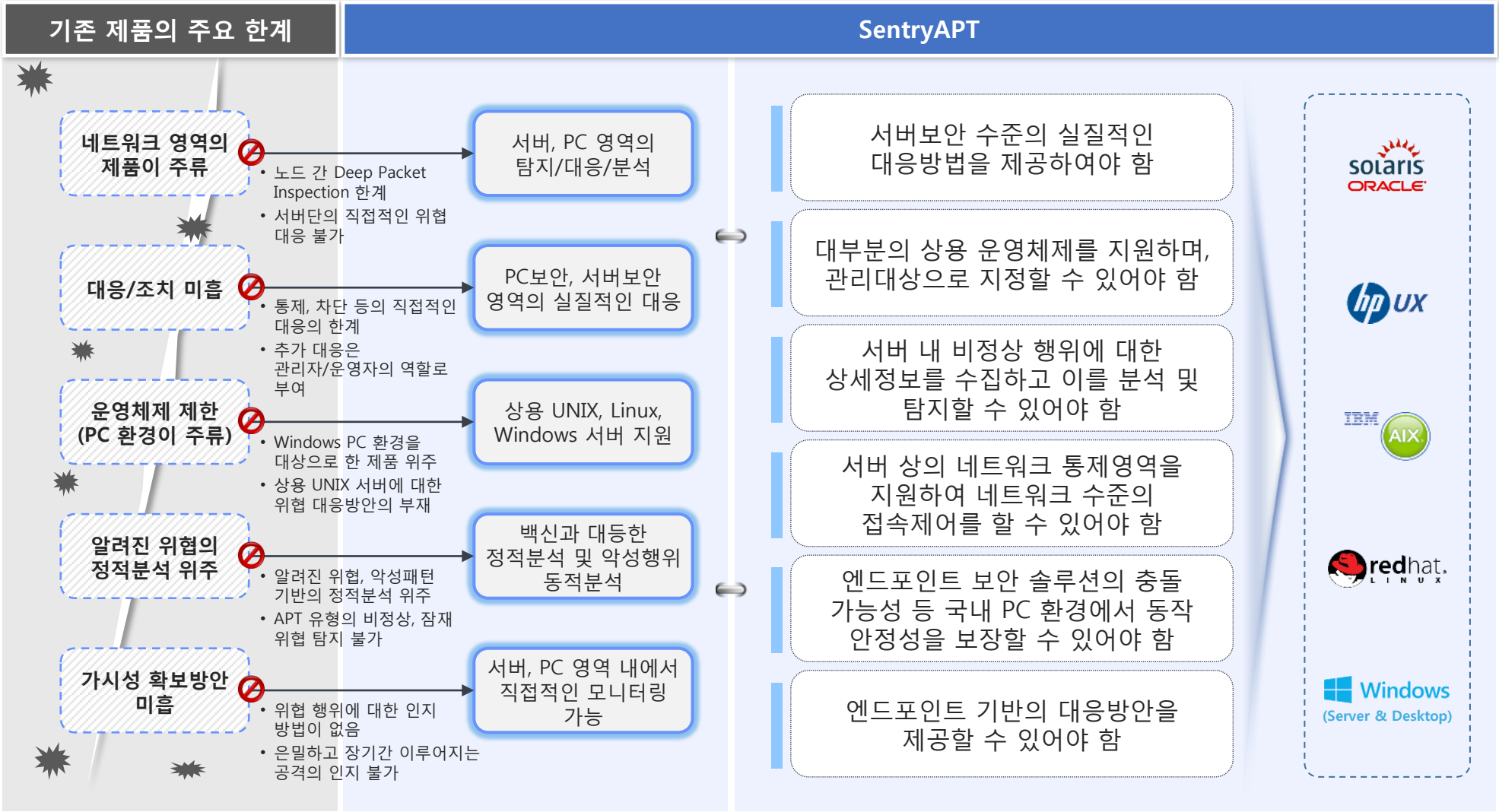
제품군 구분	대표적 제품
NTA	• NGFW(UTM 기능을 제공하는 대부분의 차세대 방화벽) • FireEye - Analysis Series (AX Series) • Fortinet - ForiGuard Security Services • Symantec - Blue Coat Secure Web Gateway Virtual appliance • McAfee - Web Gateway • Forcepoint - Web Security
SIEM	• Hewlett Packard Enterprise (HPE) ArcSight • Splunk Enterprise Security (ES) • IBM Security QRadar • AlienVault Unified Security Management (USM) • LogRhythm SIEM • McAfee Enterprise Security Manager (ESM) • Micro Focus Sentinel Enterprise • SolarWinds Log & Event Manager • Trustwave SIEM Enterprise and Log Management Enterprise • RSA NetWitness Suite
EDR	• FireEye Endpoint Security • Carbon Black Cb Response • Guidance Software EnCase Endpoint Security • Cybereason Total Enterprise Protection • Symantec Endpoint Protection • RSA NetWitness Endpoint • Cisco Advanced Malware Protection for Endpoints • Tanium • CrowdStrike Falcon Insight • CounterTack Endpoint Threat
EPP	• Carbon Black - CB Defense • Comodo - Comodo Advanced Endpoint Protection (AEP) • CrowdStrike - Falcon Endpoint Protection • Cylance - Cylance Protect • Sophos - Invincea • SentinelOne - SentinelOne • Symantec - Symantec Endpoint Protection (SEP) • Trend Micro - Endpoint Security



<※ Magic Quadrant for Endpoint Protection Platforms 2017>

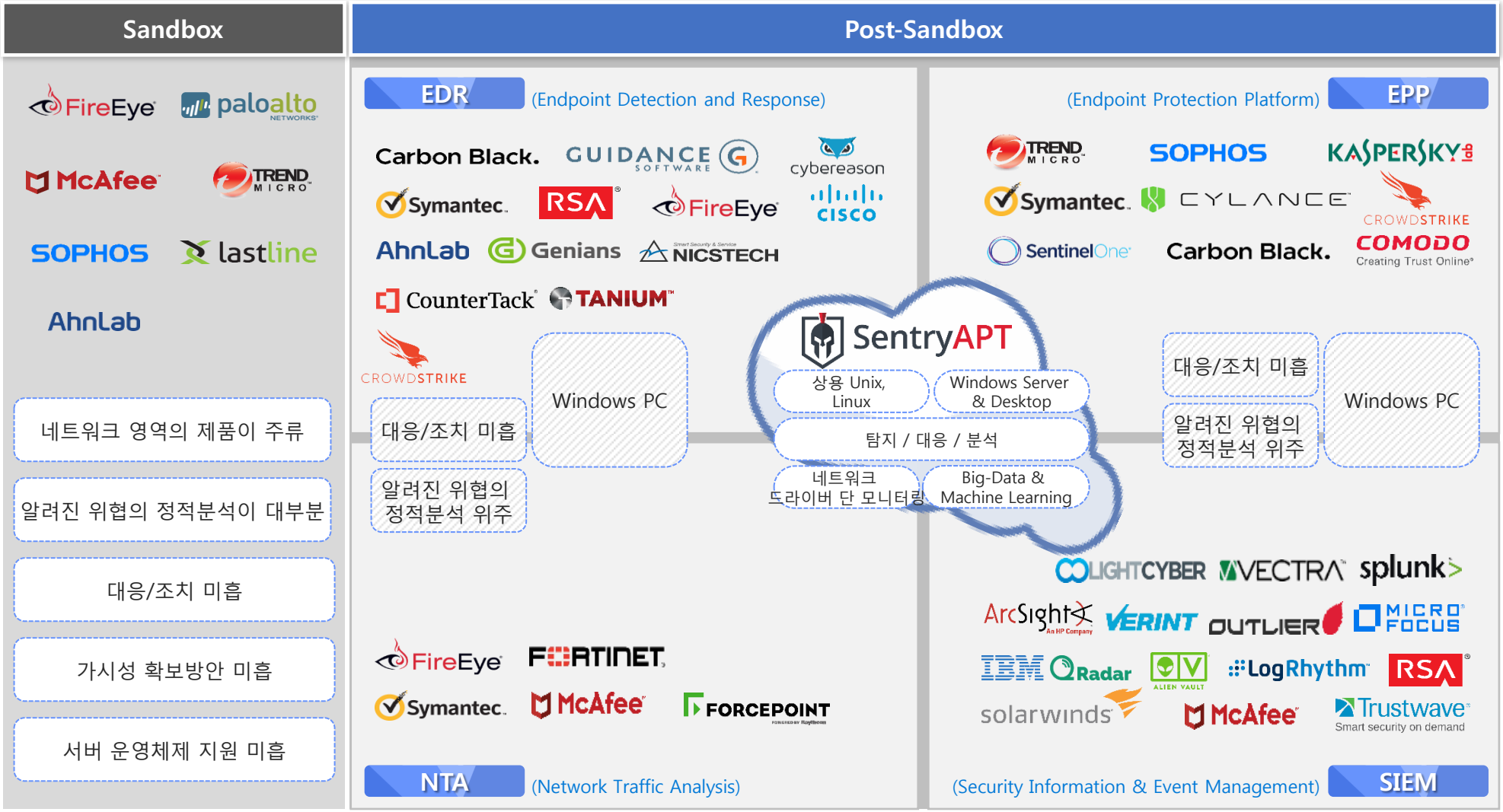
4. 제품의 구현 목표

기존 APT 제품들의 한계, 취약점을 커버하고 실질적인 대응이 가능한 차세대 APT 위협 대응 솔루션을 구현



5. 제품의 포지션

APT 제품에서 상대적으로 취약한 상용 서버군을 포함하여 "탐지/대응/분석"의 위협 대응 보안 프레임웍을 제공



Ⅲ. 제품의 주요 기능

1. 제품의 주요 특징
2. 시스템 동작 개요
3. 시스템 핵심기능 및 구성
4. 시스템 핵심기능
5. 시스템 아키텍처
6. 시스템 상세 구성
7. 주요 기능 화면

1. 제품의 주요 특징

서버 및 엔드포인트 영역의 보안 위협에 대해 실질적인 대응 방안을 제공하는 차세대 APT 위협대응 보안 솔루션

SentryAPT

서버보안 기술력 기반의 실질적인 대응방법 제공

- 서버 접근제어
- 비정상, 악성 프로세스 Kill
- 명령어 통제, 세션 통제
- 중요 파일/데이터 접근 차단

대부분의 주요 상용 운영체제 지원

- 상용 Unix & Linux
  - Solaris, HP-UX, AIX
  - RedHat(CentOS), Oracle, SUSE, Asianux
- MS Windows Server & Desktop

시스템 내 비정상 행위에 대한 상세정보 수집

- 로그 수집
- APT 킬체인 매핑
- 위협 프로파일링, 위협 레벨링
- 룰셋 기반의 탐지
- Big Data 기반 Machine Learning 지원

서버 상의 네트워크 통제영역 지원

- 네트워크 레벨 모니터링 및 통제
  - Server Firewall 기능
- 서버 내에서 직접적인 모니터링

엔드포인트 보안 기술력 반영

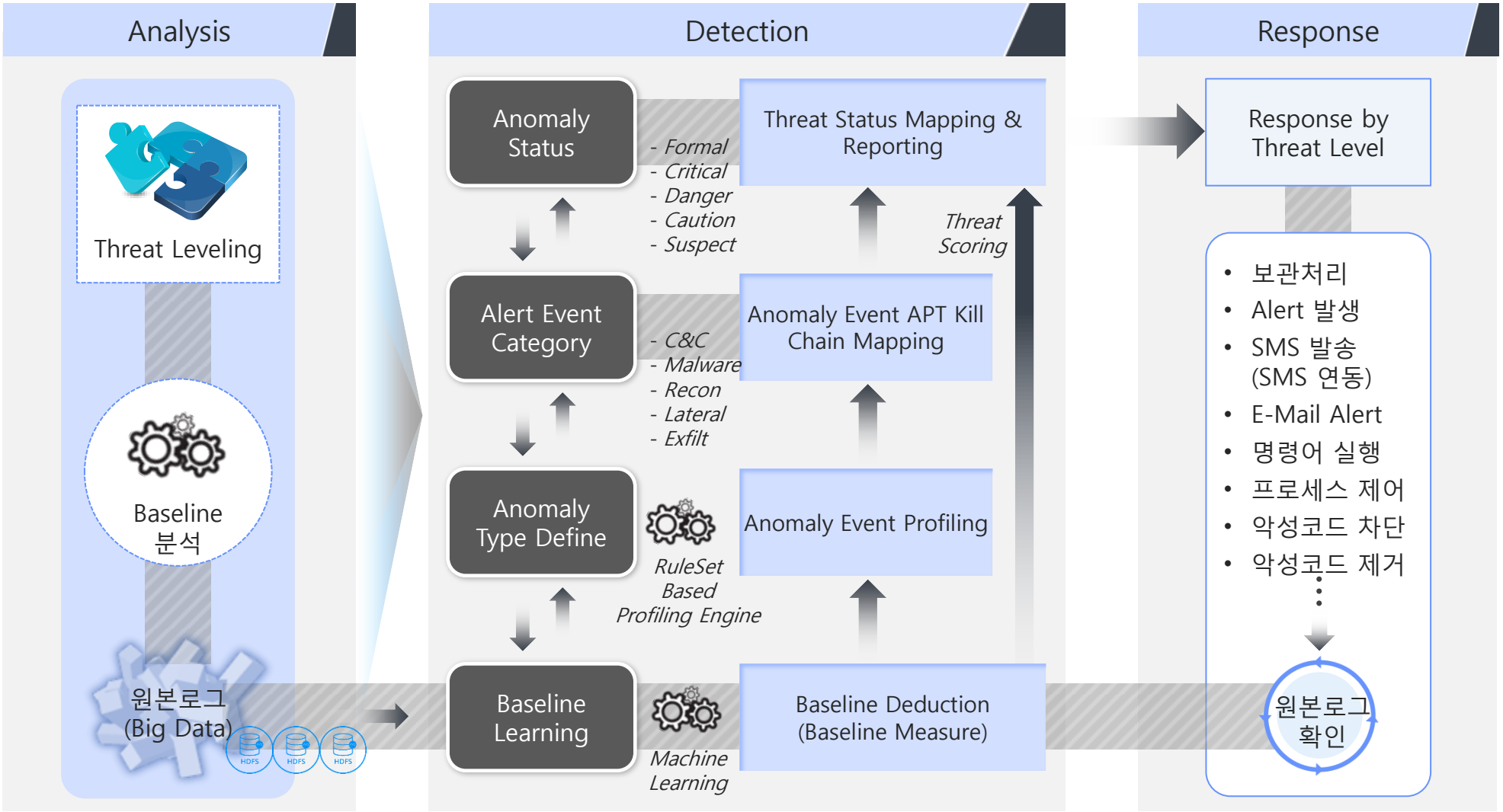
- PC 내 악성패턴 유입 탐지
- 로그 수집, 전송
- 다양한 행위의 위협 분석

엔드포인트 기반 대응방안 제공

- 에이전트 기반 대응 기능
- 바이러스, 웜, 악성코드
  - 격리, 삭제, 치료 등
- 악성 정보 데이터베이스 업데이트

2. 시스템 동작 개요

수집 로그에 대해 빅데이터, 머신러닝을 통한 지속적인 학습과 위협 탐지 및 대응으로 보안위협 차단 및 예방



3. 시스템 핵심기능 및 구성

비정상 행위에 대한 위협 프로파일링을 통해서 “[탐지]-[대응]-[분석]”의 일체화 된 위협 대응 및 처리방법 제공

탐지(Detection)

- 비정상 행위 분석 탐지
- Recon/Lateral/자료수집, 데이터 유출 등 대상 시스템 내의 내부행위 탐지
- 서비스형(ftp/telnet/ssh 등) 비정상 행위 탐지

대응(Response)

- 대상 시스템 내 이상 프로세스 실행 차단(Kill)
- 중요 파일 접근 차단
- 세션통제, 경유통제, 악성코드 격리
- 이벤트 타입별 자동/수동 대응

분석(Analysis)

- 베이스라인 비교/분석 도출
- 머신러닝 기반 프로파일링 기법 탐지 (학습 및 임계치 조정)
- 네트워크 기반 APT 솔루션과 연계 가능

운영체제 지원

- 대부분의 기업환경에 사용되는 운영체제 지원
  - Windows Server & Desktop
  - 상용 Unix & Linux

Big Data & Machine Learning

- Big data 기반의 Machine Learing을 통한 위협정보 수집 및 학습
- PC, 서버 등의 대량의 로그를 안정적으로 분석

Threat Profiling

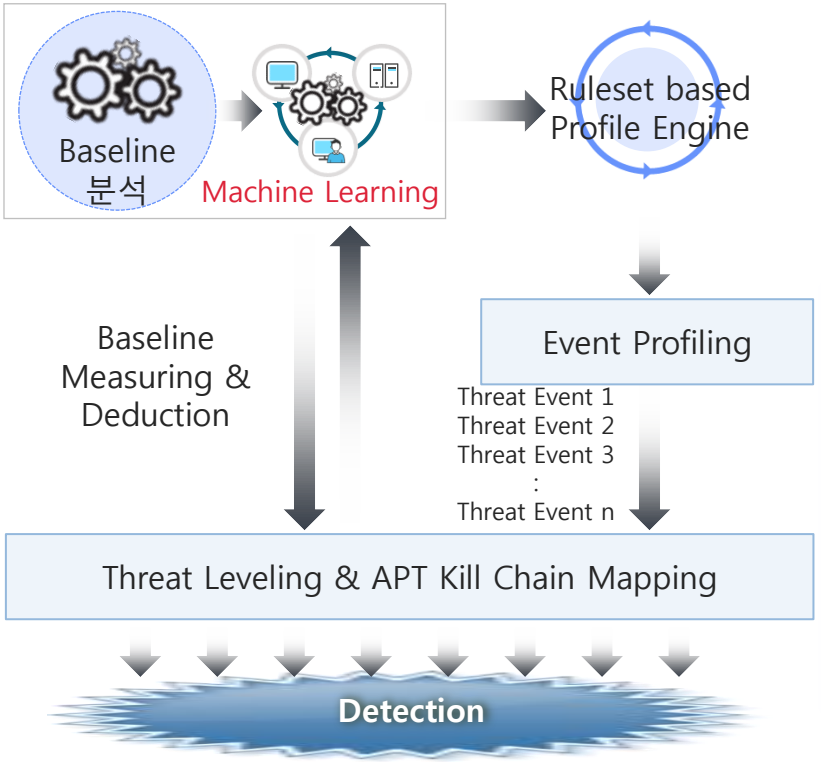
- 정형화 된 위협 프로파일 내장
- Machine Learning 학습을 통한 위협 스코어링(Threat Scoring)
- 새로운 위협 정의가 용이한 구조

Threat Visibility

- 비정상 행위에 대한 가시성 제공
  - APT Kill Chain Mapping
  - 위험도 레벨링 제공
  - TTY 모니터링
- 대응에 대한 명확한 근거 제공

4. 시스템 핵심기능 - 1) Detection Process

수집 로그에 대한 분석 및 위협 이벤트 프로파일링을 통하여 위협 수준 및 APT Kill Chain 기반의 탐지 기능을 제공



- ❖ APT Kill Chain 단계별 Threat Category 분류
  - 총 34개의 위협 유형, 지속적인 업데이트
- ❖ 위험도 레벨링 기반 위협 탐지

Baseline 분석/도출	• 축적된 대량의 데이터 분석 • Baseline Learning • 임계치 도출/정의 • Threat Profiling • Threat Event Categorizing • Threat Level Measure
APT Kill Chain Mapping	• Ruleset based APT Kill Chain Mapping - C&C - Malware - Recon - Lateral - Exfilt • APT 위협단계 기반 가시성 제공 및 분석요건 제공
Threat Leveling (위협이벤트 탐지)	• Threat Level Mapping - Level0: Suspect - Level1: Caution - Level2: Danger - Level3: Critical - Level4: Formal • 대응을 위한 판단 기준

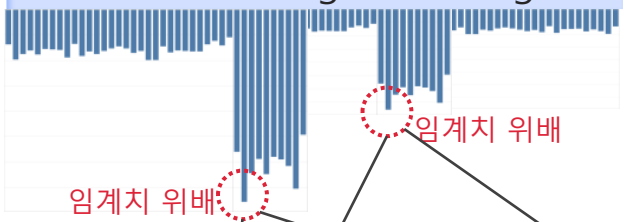
4. 시스템 핵심기능 - 2) Response Process

대상 서버 및 PC에 대해 탐지된 결과에 따라 에이전트 기반의 자동 또는 수동 대응 기능을 제공

Baseline Measure

Threat Event Profiling

Threat Scoring & Leveling



- 사전 정의된 Threat Event
- Threat Event 위험도 Leveling
- Threat Event Baseline 도출
- 임계치 위배 시 조치/대응 정의

- Process Kill
- Command Execution
- Shell Script Execution
- SMS Notification
- E-Mail Notification

- 위험도 레벨에 따른 대응 정의
- 탐지된 Threat Event 대응 조치
- Agent 기반의 대응 조치
- 자동/수동 대응 수행

Response

서버

- 상용 Unix
- Linux
- Windows Server

사용자 PC

- Windows PC (Desktop PC)

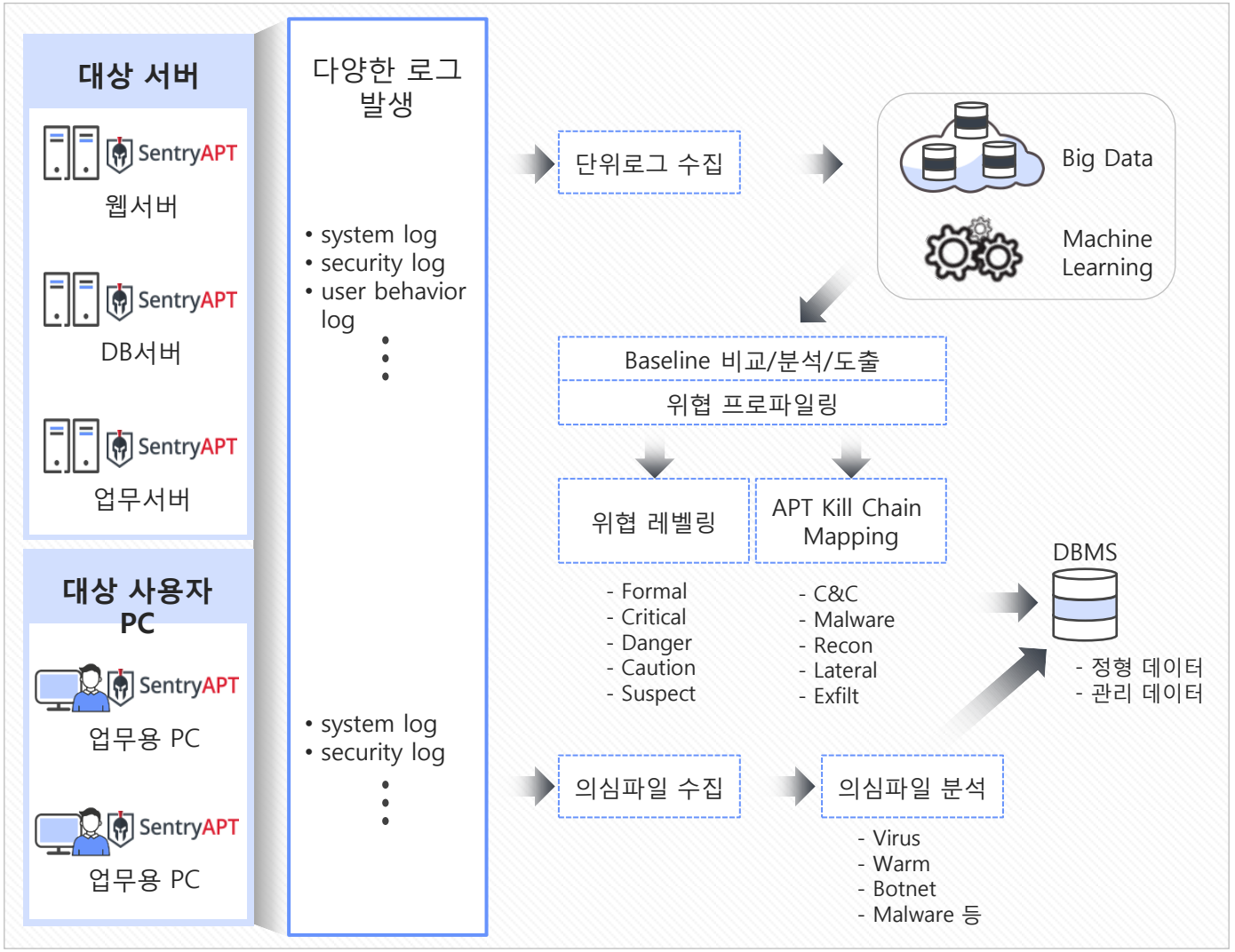
Pre-Defined Response Policy

SentryAPT Agent

- 대부분의 상용 운영체제 기반의 서버 지원
- 윈도우즈 서버 및 PC 지원

4. 시스템 핵심기능 - 3) Analysis Process

빅데이터 기반의 머신러닝을 통하여 지속적인 임계치 비교/분석 및 위협 프로파일링 결과를 제공



서버로그 수집 및 분석/탐지

- 대상서버 로그 수집 (웹서버, DB서버, 업무서버 등)
- 수집 로그 분석
- 기본 룰셋 적용
- 경로분석, 행위재연 등

사용자로그 수집 및 분석/탐지

- 사용자 PC에서 발생하는 다양한 시스템 정보 수집
- 수집된 의심파일 분석 및 탐지

빅데이터 플랫폼 적용

- 대상 서버, PC에서 수집된 로그를 빅데이터 플랫폼에 저장
- 저장된 로그를 NoSQL 방식으로 안정적 처리

4. 시스템 핵심기능 - 4) 위협 프로파일링

다양한 보안 위협들에 대해 자동화 된 위협 프로파일링(비정상 행위 등에 대한 정의)을 통한 위협 대응 기반 제공

다양한 보안장비 및 어플리케이션 서버

- 시스템 로그
- 어플리케이션 로그
- 보안 로그
- .....

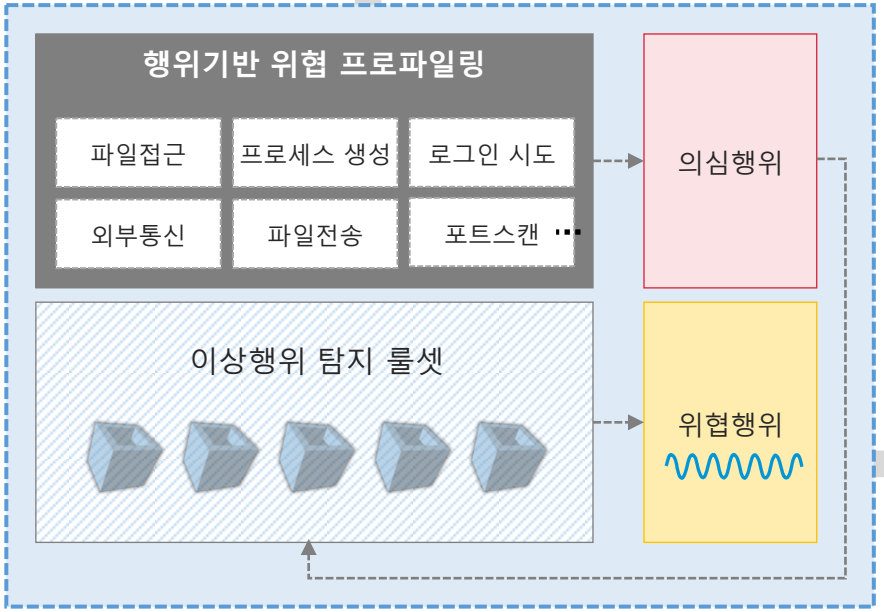
빅데이터 기반의 머신러닝 기법 적용

- Baseline 값을 기반으로 비교/분석
- 데이터 분류 및 그룹핑
- 장기적, 대량의 데이터 처리

위협 점수화를 통한 비정상행위 정의 및 대응

로그 수집 및 이벤트 축적

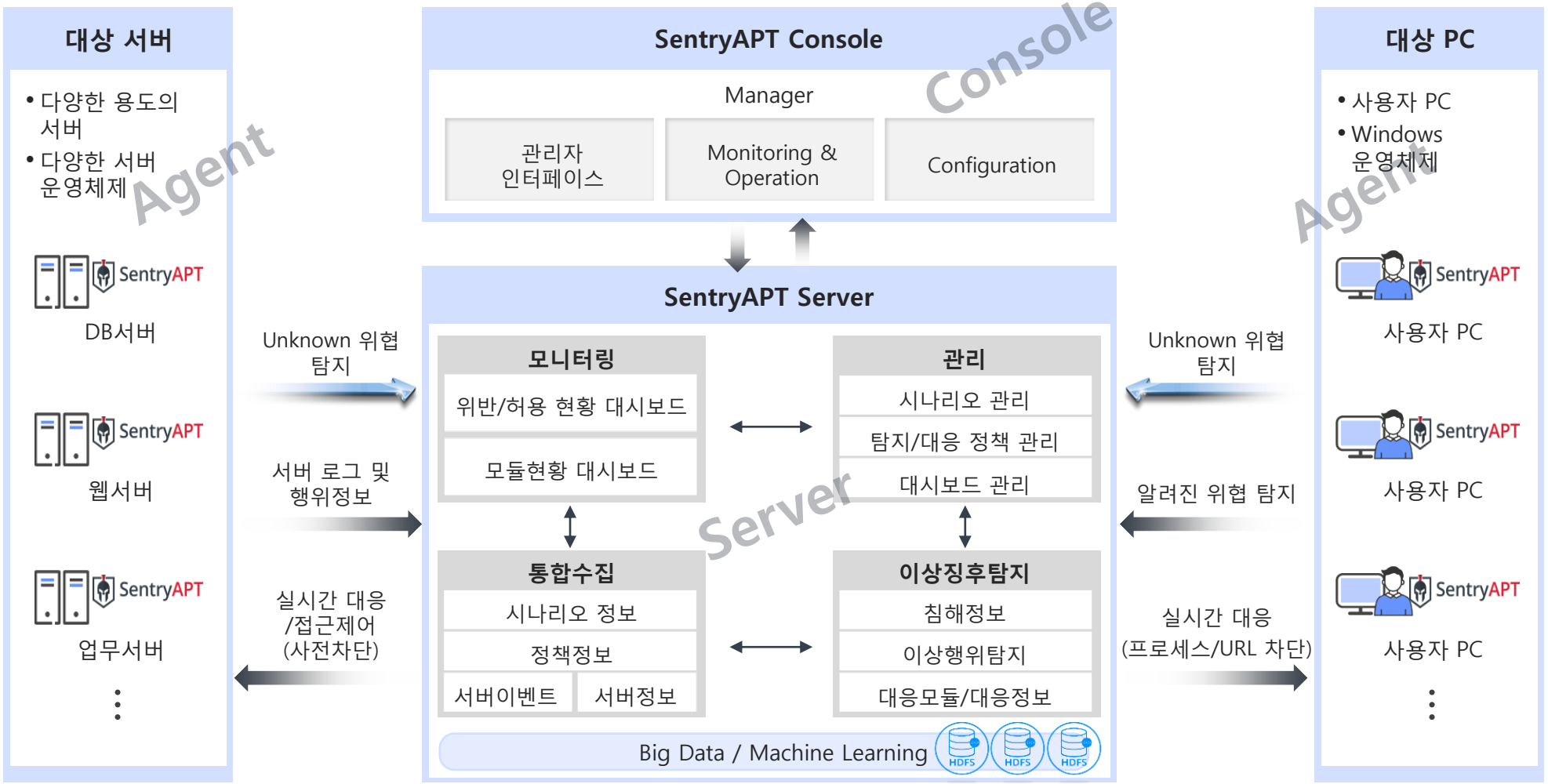
- 대량의 데이터를 안정적으로 수집·저장
- 비교/분석을 위한 원본로그 제공



5. 시스템 아키텍처

[콘솔]-[서버]-[에이전트]의 3-Tier 아키텍처로서 대부분의 상용서버 및 PC 운영체제를 에이전트 대상으로 지원함

3-Tier Architecture



6. 시스템 상세 구성

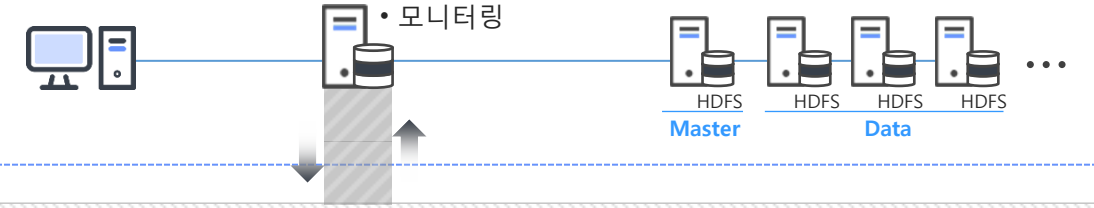
SentryAPT 서버는 기능 및 역할에 따라 관리콘솔, 관리서버, 데이터저장서버로 구분되어 구성됨

SentryAPT Server

[관리콘솔] Windows
- 관리자 인터페이스
- 대시보드 모니터링
- 시스템 설정
- 탐지/대응/분석 운영

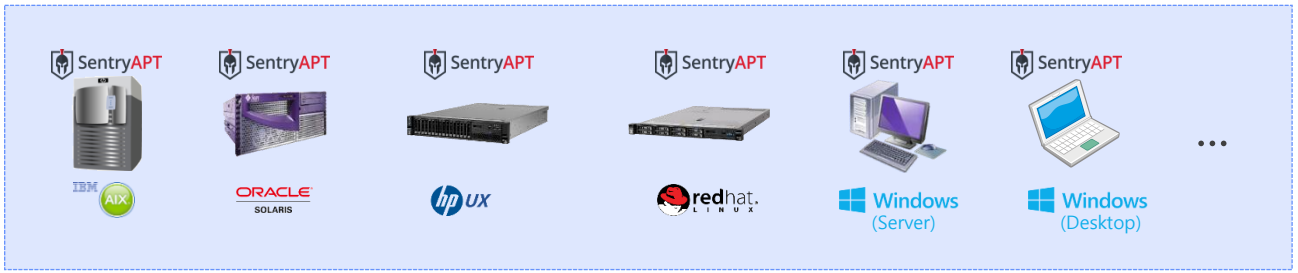
[관리서버] LiNUX
- Machine Learning
- 룰셋 프로세싱
- 정책 설정 및 시스템 운영
- 에이전트 제어(위협대응)
- 모니터링

[데이터 저장서버] LiNUX
- 원본로그 수집·저장
- Big Data 기반
- Master 서버 1대 구성
- Data 서버 3대 이상 구성 권장



구분	수량	O/S	비고
관리서버	1대	Linux (64bit)	PostgreSQL (RDBMS)
데이터 저장서버 (Master)	1대	Linux (64bit)	데이터 저장서버 관리
데이터 저장서버	3대	Linux (64bit)	기본 3대 (Big Data)
관리콘솔	1대	Windows	별도 구성 (C/S 콘솔 환경)

SentryAPT Agent

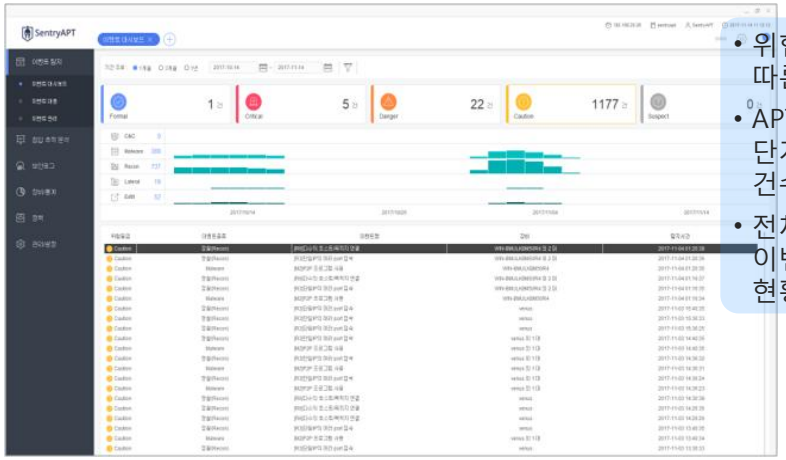


- 상용 Unix 운영체제 지원
  - HP HP-UX
  - Oracle Solaris
  - IBM AIX
- Linux 운영체제 지원
  - RedHat Linux(CentOS)
  - Oracle Linux
  - SUSE Linux
  - Asianux Linux
- MS Windows 운영체제 지원
  - Windows Server
  - Windows Desktop

- 로그 수집·전송
- 에이전트 정보 전송
- 명령어 실행, 프로세스 Kill 등 대응 수행
- 악성코드 탐지/제거/차단
- 백그라운드 실행
- User Transparent (백그라운드 동작)

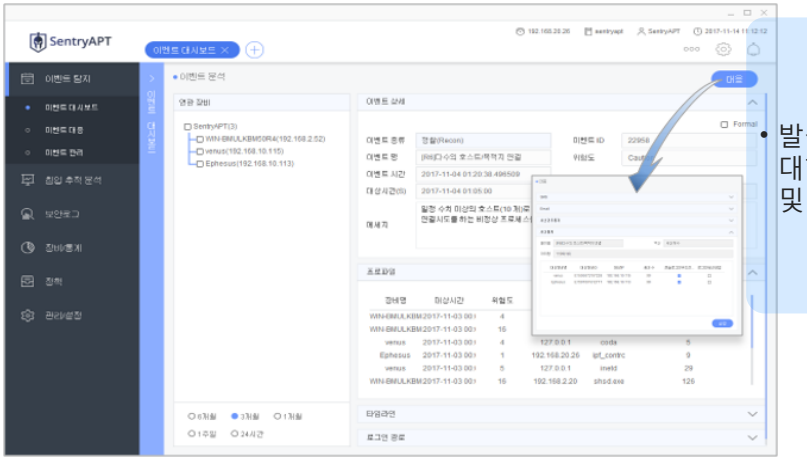
7. 주요 기능 화면

이벤트 탐지 메인 대시보드



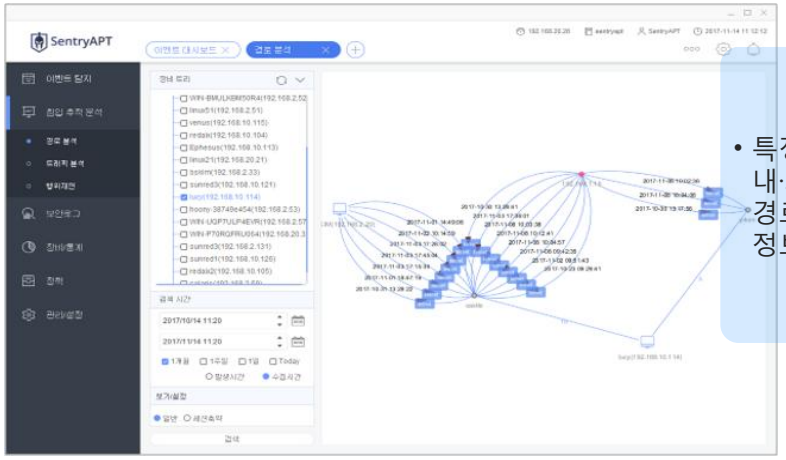
- 위협레벨에 따른 탐지 현황
- APT Kill Chain 단계별 발생 건수 및 추이
- 전체 대상별 이벤트 발생 현황 정보

탐지 이벤트 분석



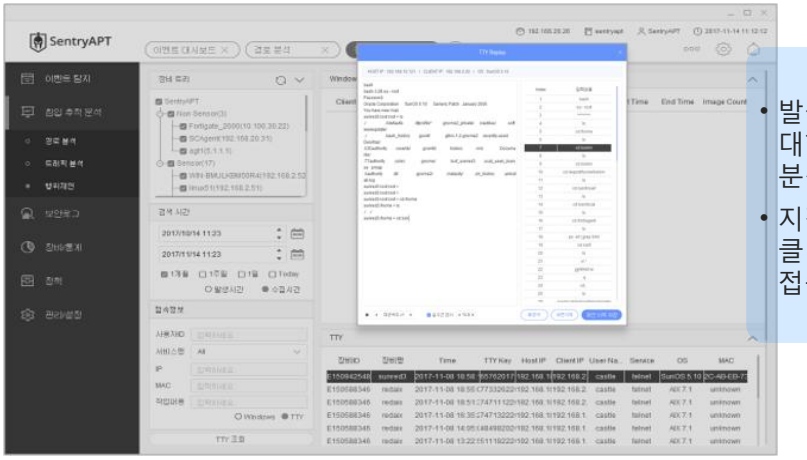
- 발생 이벤트에 대한 대응 설정 및 실행

경로 분석



- 특정 대상의 내·외부 접속 경로에 대한 정보

행위 재연



- 발생 이벤트에 대한 행위재연 분석
- 지정된 서버와 클라이언트 간 접속 재연 등

Ⅳ. 도입 효과

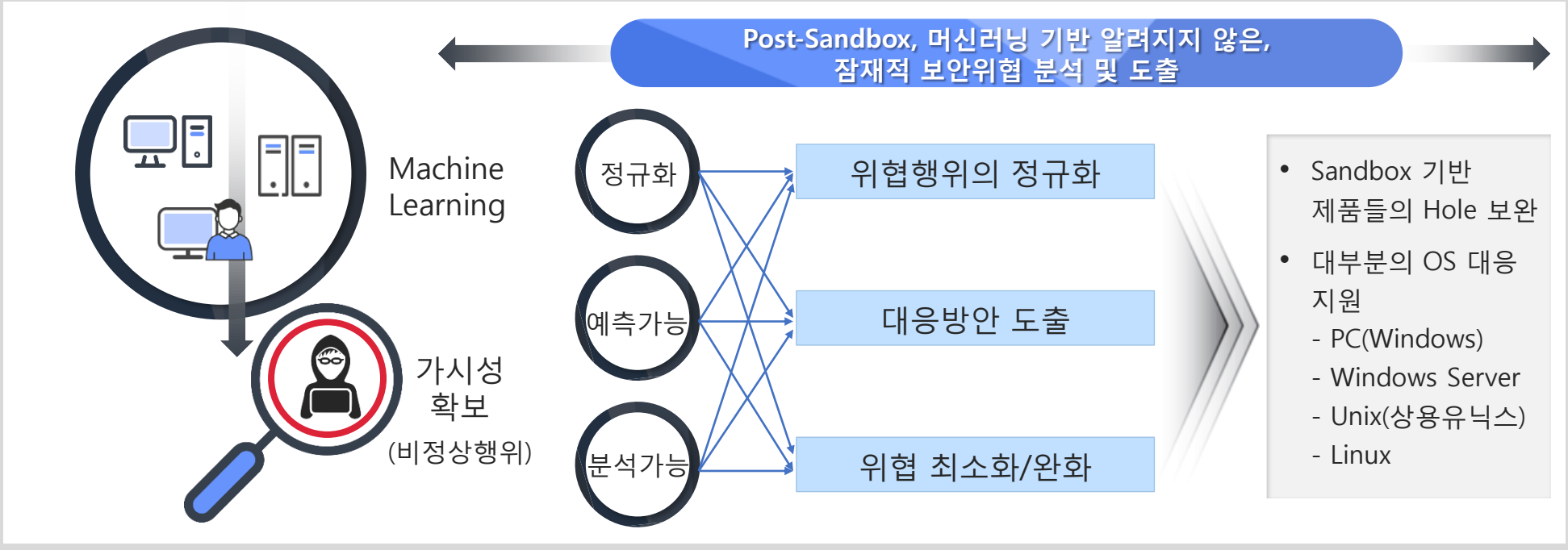
1. 최신 보안위협 대응
2. 서버 및 PC의 실질적인 위협 탐지 및 대응
3. 전통적인 관제시스템 대체

1. 최신 보안위협 대응

최신 보안 위협인 APT에 대응함으로써 기업의 알려진 보안위협 뿐만 아니라 잠재적인 보안위협 까지 탐지/제거

APT 보안위협	악성 C&C, Malware	Sandbox Based	Network Area
	일반적으로 알려진 위협 탐지	해킹 사실 미인지	Sandbox 기반의 APT 보안위협 탐지의 hole 존재	지속적인 정보유출 등의 해킹피해 발생	네트워크 영역 위주의 제품이 다수 출시됨

PC 뿐만 아니라 상용 서버 영역을 지원함으로써 기존 지원범위 및 방식에 따른 취약한 부분을 커버리지



2. 서버 및 PC의 실질적인 위협 탐지 및 대응

서버 및 PC에 대해서 보안위협 분석·탐지 뿐만 아니라 명확한 위협행위에 대한 차단 등의 대응이 가능함

서버 및 PC 영역의 커버리지

- 대표적인 상용 서버 운영체제 지원
- 국내에서 많이 사용되고 있는 리눅스 운영체제 지원
- Windows PC 운영체제 지원

IBM AIX, ORACLE SOLARIS, hp UX, redhat. LINUX, CentOS, ORACLE LINUX, Asianux, SUSE, Windows Server & Desktop

서버/PC 상의 분석·탐지 기능

서버 접근통제

- 서버 상의 비정상 행위 탐지
- 서버 상의 비정상 프로세스 탐지
- 룰셋 기반의 이상징후 탐지

서버 방화벽

- 서버로 비정상 접근 행위 탐지
- 룰셋 기반의 임계치 초과 행위 탐지
- 허용되지 않은 지속적인 접근 행위 탐지

PC 위협탐지

- PC 상의 악성코드, 악성 프로그램 탐지
- 바이러스, 멀웨어 탐지
- 의심파일 수집

위협 대응 제공

서버 상의 위협 탐지 결과에 따른 대응 정의 및 대응 실행

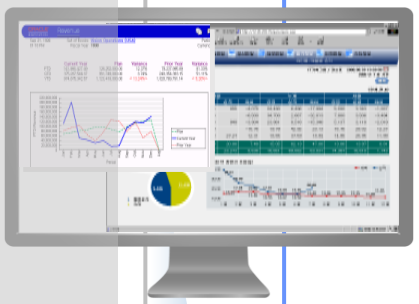
자동 / 수동

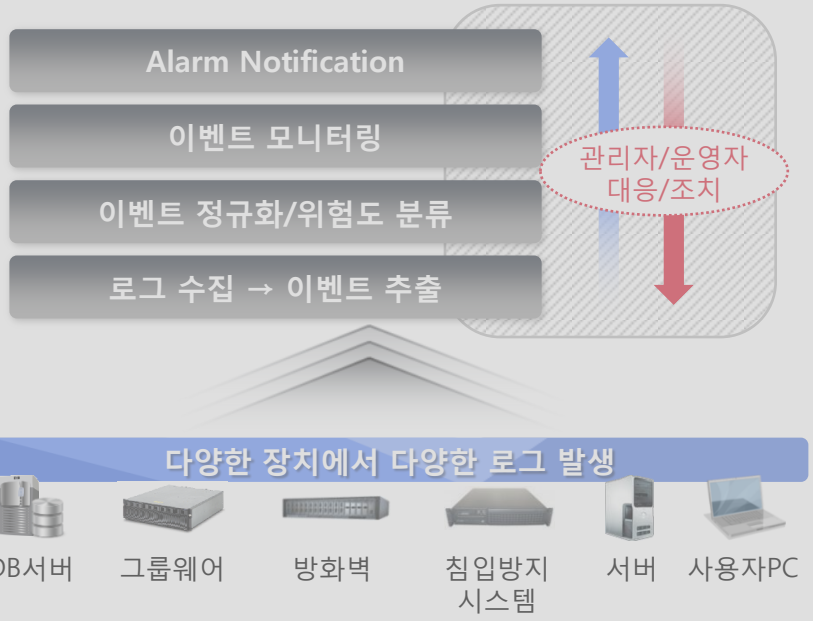
- 서버 명령어 실행
- 서버 접근제어
- 위협 프로세스 KILL
- 에이전트 명령어 실행
- 바이러스 격리/제거(윈도우즈)
- 악성코드 차단, 제거, 격리
- Alert 전송(E-Mail/SMS/팝업)
- :

3. 전통적인 관제시스템 대체

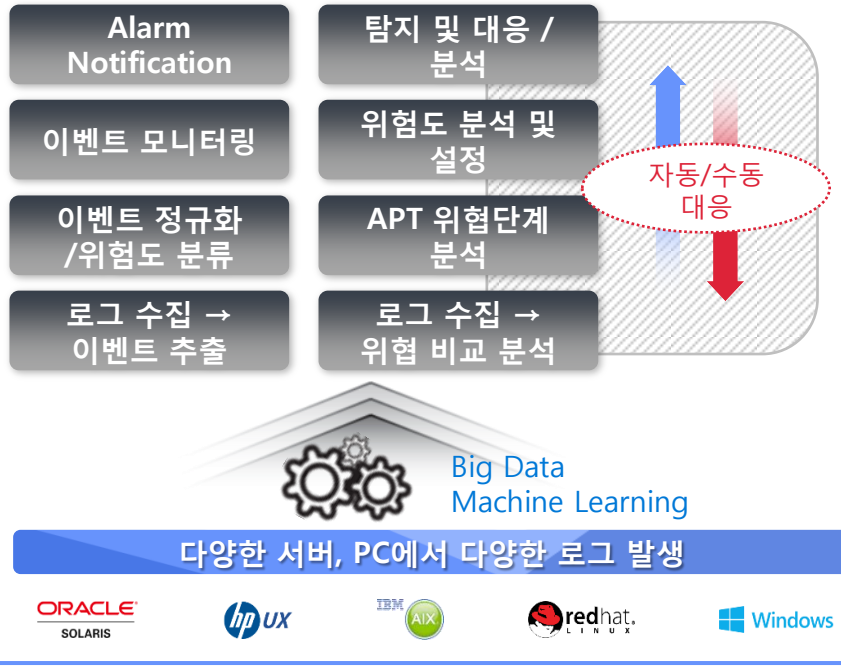
빅데이터 · 머신러닝 기반의 진보적인 기술 기반의 보안위협 탐지 및 이를 기반으로 한 분석 및 대응체계 제공

- 다양한 장비, 솔루션 등에 대한 로그수집 목적의 연동 비효율성
- 로그 및 이벤트 기반의 현황 모니터링
- 정형화 된 DBMS 데이터 기반의 고비용, 저효율성
- APT 등 지능화 된 차세대 보안위협 대응 부족





- 중요 위협에 대한 Threat Profile 기반
- Big Data 엔진기반 대량의 수집로그 처리
- 수집된 대량의 로그, 이벤트 비교 분석
- Machine Learning 기반의 학습기능을 통한 알려지지 않은 잠재적인 위협의 탐지
- 명확한 침해행위에 대한 자동/수동 대응



Ⅴ. 제품 비교

1. 국내 유사 제품과의 비교
2. 글로벌 유사 제품과의 비교

1. 국내 유사 제품과의 비교

구분	에스지에이솔루션즈	A사	B사	C사
제품명	SentryAPT	A 제품	B 제품	C 제품
시스템 레벨 탐지/대응	• 시스템 레벨 탐지 및 대응 • 호스트에 설치된 에이전트를 기반으로 강력한 위협탐지 및 대응	• 관련 기능 없음	• 관련 기능 없음	• 관련 기능 없음
시스템 레벨 분석	• 호스트에 설치된 에이전트를 기반으로 강력한 위협분석 제공 • 시스템 레벨에서의 이벤트 추적 및 위협분석 제공	• 관련 기능 없음	• 관련 기능 없음	• 관련 기능 없음
빅데이터 플랫폼 관련	• 시스템 및 각종 장비에서 발생하는 모든 로그 및 이벤트를 빅데이터화	• 빅데이터 엔진 기반 엔드포인트 위협 탐지/대응	• 관련 기능 없음	• 관련 기능 없음
머신러닝 (기계학습) 관련	• 빅데이터화 된 로그/이벤트를 머신러닝을 통해 보안위협 임계치 자동설정 및 위협대응	• 향후 머신러닝 기법 적용 예정	• 향후 머신러닝 기법 적용 예정	• 의심 파일 수집 성능 강화 및 검사 시간 단축, 과탐율 최소화
지원 OS	• Unix, Linux, Windows, Windows Server • 국내·외 유일하게 상용 Unix 지원	• 별도의 장비나 서비스의 로그 및 이벤트 수집/분석	• Windows, Windows Server	• Windows, Windows Server
엔드포인트 레벨 통제	• 보안위협 탐지 • 자사 백신기반 탐지기술 적용하여 통제	• IoC 기반의 탐지/대응	• 행위기반 엔진으로 탐지/대응	• 전용 에이전트 연계를 통해 엔드포인트 구간 대응 지원
네트워크 레벨 통제	• 보안위협 탐지 • 서버 및 PC의 네트워크 정보 수집 및 탐지, 분석 제공	• 자체 NAC 제품 연계를 통한 탐지/대응	• 가상시스템을 통한 네트워크 패킷 분석/탐지	• 네트워크 샌드박스 형태로 유출입되는 파일에 대한 악성 여부 진단

2. 글로벌 유사 제품과의 비교

구분	에스지에이솔루션즈	P사	V사	S사
제품명	**SentryAPT**	P 제품	V 제품	S 제품
시스템 레벨 탐지/대응	• 시스템 레벨 탐지 및 대응 • 호스트에 설치된 에이전트를 기반으로 강력한 위협탐지 및 대응	• 관련 기능 없음	• 관련 기능 없음	• 관련 기능 없음
시스템 레벨 분석	• 호스트에 설치된 에이전트를 기반으로 강력한 위협분석 제공 • 시스템 레벨에서의 이벤트 추적 및 위협분석 제공	• 관련 기능 없음	• 관련 기능 없음	• 관련 기능 없음
빅데이터 플랫폼 관련	• 시스템 및 각종 장비에서 발생하는 모든 로그 및 이벤트를 빅데이터화	• 관련 기능 없음	• 대량의 악성 트래픽 및 공격 트래픽 분석 방법 제공	• 관련 기능 없음
머신러닝 (기계학습) 관련	• 빅데이터화 된 로그/이벤트를 머신러닝을 통해 보안위협 임계치 자동설정 및 위협대응	• 네트워크 레벨 위협 탐지/분석	• 네트워크 레벨 위협 탐지/분석	• 머신러닝을 통한 자체 백신 기반 멀웨어 탐지/대응
지원 OS	• Unix, Linux, Windows, Windows Server • 국내·외 유일하게 상용 Unix 지원	• Windows	• Windows	• Windows, Windows Server, /Embedded, Mac, Linux
엔드포인트 레벨 통제	• 보안위협 탐지 • 자사 백신기반 탐지기술 적용하여 통제	• 관련 기능 없음	• 관련 기능 없음	• 위협 탐지 및 자체 엔진 기반 멀웨어 탐지/대응
네트워크 레벨 통제	• 보안위협 탐지 • 서버 및 PC의 네트워크 정보 수집 및 탐지, 분석 제공	• 위협 탐지만 가능 • 위협 대응 불가	• 위협 탐지만 가능 • 위협 대응 불가	• 네트워크 기반으로 탐지 및 대응

동영상 시연

1. 시연 개요

● APT 공격의 과정을 시나리오 형태로 정의

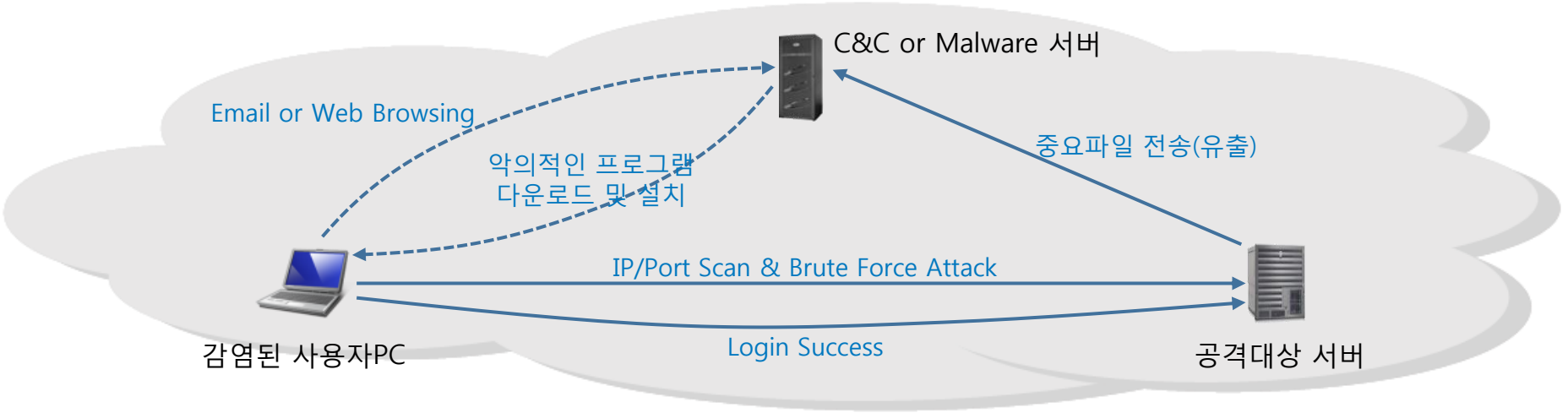
- 시나리오 기반의 단계별 APT 공격 실행
  - ✓ 공격시도 부터 성공 완료까지 실행
- APT 공격의 킬체인 단계별 행위 식별
  - ✓ 단위 룰셋 기반의 탐지 결과
- 최종 탐지결과에 따른 대응
  - ✓ 대상 서버와 PC에 대한 에이전트 기반의 대응

❖ *Unknown Attack에 대한 가시성 확보*

❖ *APT 공격의 생명주기 전체에 걸친 통제*

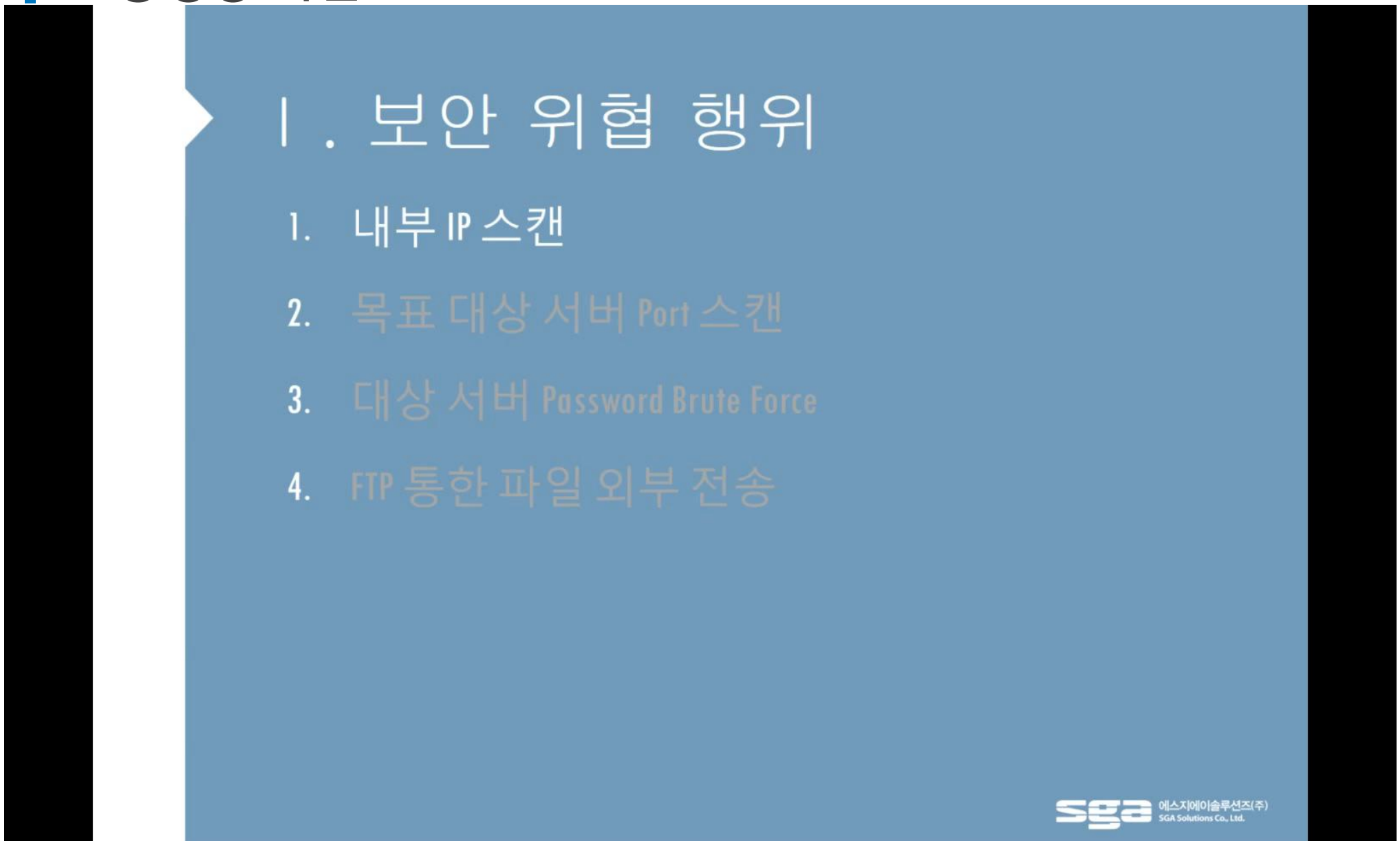
❖ *실질적인 대응*

2. 시연 시나리오



C&C/Malware	정찰(Recon)	침투(Lateral)	유출(Exfilt)	대응(Response)
Nmap Hydra • 악의적인 목적의 프로그램 다운로드 및 설치	보안이 취약한 서버 목표 • 포트 스캔을 통한 취약서버 타겟팅 • 무차별 패스워드 대입으로 취약한 계정정보 탈취	로그인 성공 및 권한 획득 • 탈취한 계정정보를 이용한 로그인 시도 및 성공 • 서버 점유 성공	중요 파일 유출 • 중요 파일을 외부로 전송 • ftp 클라이언트 프로그램 사용	탐지결과에 따른 대응 • SentryAPT Agent 명령어 실행 기능으로 ftp 프로그램 강제 삭제 • Email Notification

3. 동영상 시연



4. Value of SentryAPT

공격이 이루어지는 위협행위를 알아내야 한다.

- 행위가 이루어지는 과정을 식별
- 가시성(알아야 막는다)

APT 킬체인 공격단계를 알아내야 한다.

- 공격에 대한 위협수준의 단계를 제공
- 공격 진행단계를 식별

PC 뿐만 아니라 상용 서버도 지원해야 한다.

- 상용 Unix, Linux, Windows Server
- 강력한 대응기능을 제공

분석-탐지-대응이 일체화된 통합 솔루션이어야 한다.

- 분석, 탐지는 일반적으로 지원
- PC 및 상용서버에 대한 대응이 가능한 제품

시나리오 기반 탐지 능력을 제공해야 한다.

- 고객의 상황에 맞는 탐지 시나리오 정의
- 룰셋의 조합을 통한 강력한 APT 위협 대응

Thank You!