intel Security

진화하는 위협대응
- 시그니처에서 플랫폼으로

McAfee Network Security Platform

™

조 현석 차장 | Enterprise SE, Intel Security

기존 IPS 한계와 차세대 IPS

전통적인 시그니처 기반의 IPS	차세대 Network Security Platform
Attacks Missed • Zero-day? • Advanced Persistent Threats? • 지능형 멀웨어?	시그니처 + 비 시그니처 기반의 다중 분석 엔진
Too Many Alerts • 수천 개에 달하는 이벤트 • 악의 적인 패턴 분석, 도출? • 어떤 것을 차단 해야 하는가?	정책 적용 판단이 가능한 실용적인 데이터 제공
No Focus • 데이터 의미 분석의 어려움 • 천차만별한 기법과 패턴 들 • unknown 공격 분석	보안 정책 개선을 위한 상황 정보 제공

VULNERABLE ← → INTELLIGENT

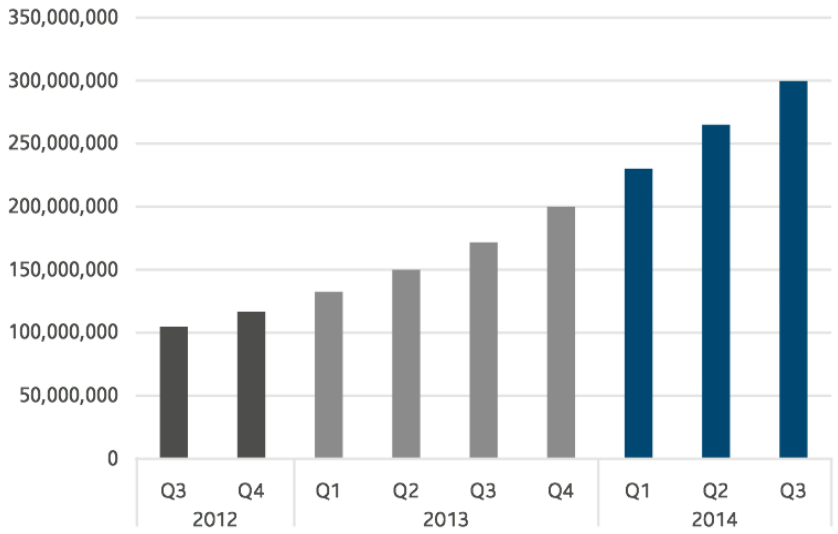
APTs, Zero-day와 지능형 멀웨어

76% 의 네트워크 보안 전문가들이 지능형 멀웨어가 오늘날 보안의 가장 주요한 관심사라고 응답

37% 의 네트워크 보안 전문가들이 주당 10시간 이상 지능형 멀웨어 대응에 소비

Survey of Network Security professionals at Black Hat USA 2013

McAfee Labs Database가 보유한 전체 멀웨어 수



McAfee Threat Reports: Third Quarter 2014

멀웨어(악성 코드)는 변함없이 꾸준한 성장을 나타내고 있으며, 이는 최근 들어 더욱 급격 한 상승세를 보이고 있음. McAfee LAB에서 확보한 멀웨어 샘플이 전년 대비 76% 증가 하였으며, 2014년 Q3에 3억 개를 돌파.

시그니처 기반의 탐지가 어렵게 되는 이유

! 발전하는 **지능형 멀웨어**

수년 동안, 시그니처 기반 보안은
알려진 공격 대부분을 빠르고 확실하게 대응

하지 만 해커들은 자신의 목적 달성을 위해
이를 회피 하기 위한 **해킹기술을 필연적인 발전**

더욱 **비밀스럽고, 파악이 어려우며, 시그니처 기반의 방어의 회피를 위해 지능적으로 상황에 적응 할 수 있는 지능형 멀웨어**로의 진화

악성 코드가(JavaScript) 내장된 PDF파일의 영향으로 의심되는 대형 마트에 대한 멀웨어의 피해로 지불 카드 정보 4000만개, 7000만 고객의 개인정보 유출. (-미국 BlackPOS)

시그니처가 심각한 공격을 탐지 못하는 이유

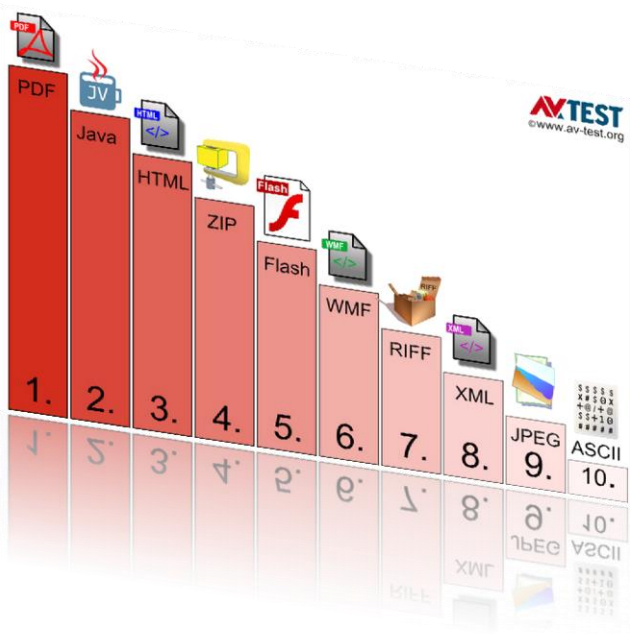
! Predatory(약탈적) **PDF**

대화형 컨텐츠를 지원 하는 문서파일 특히 **PDF는 플랫폼에 관계 없이 풍부한 콘텐츠 배포**를 위한 필수불가결한 도구.

하루에도 **수천 건**에 달하는 **파일의 이동**
(E-mail 첨부와 Web Download)

동적 액션 트리거, 원격 데이터 검색, 내장형 스크립트 등의 **동적 요소 지원**

스크립트는 **악성 가능성이 거의 무제한**인 감염 백터
(Keylogger, 루트키트, Bot등의 다운로드 설치 등)



기존 IPS 알려진 위협 스크립트를 인식 할 수 있지만, 코드를 분석하거나 런타임 행위를 /예측 할 수 없음. IPS의 시그니처와 알려진 위협의 시그니처가 일치 하지 않는 한 탐지가 불가.

지능형 멀웨어의 Challenge

EVADES(회피)

Legacy-Based Defenses

- Stealthy
- Targeted
- Unknown

Typically

CRIMINAL

- 정보 유출
- 서비스 방해
- 첩보 활동

Discovered

After the Fact

Gartner

Bottom Line

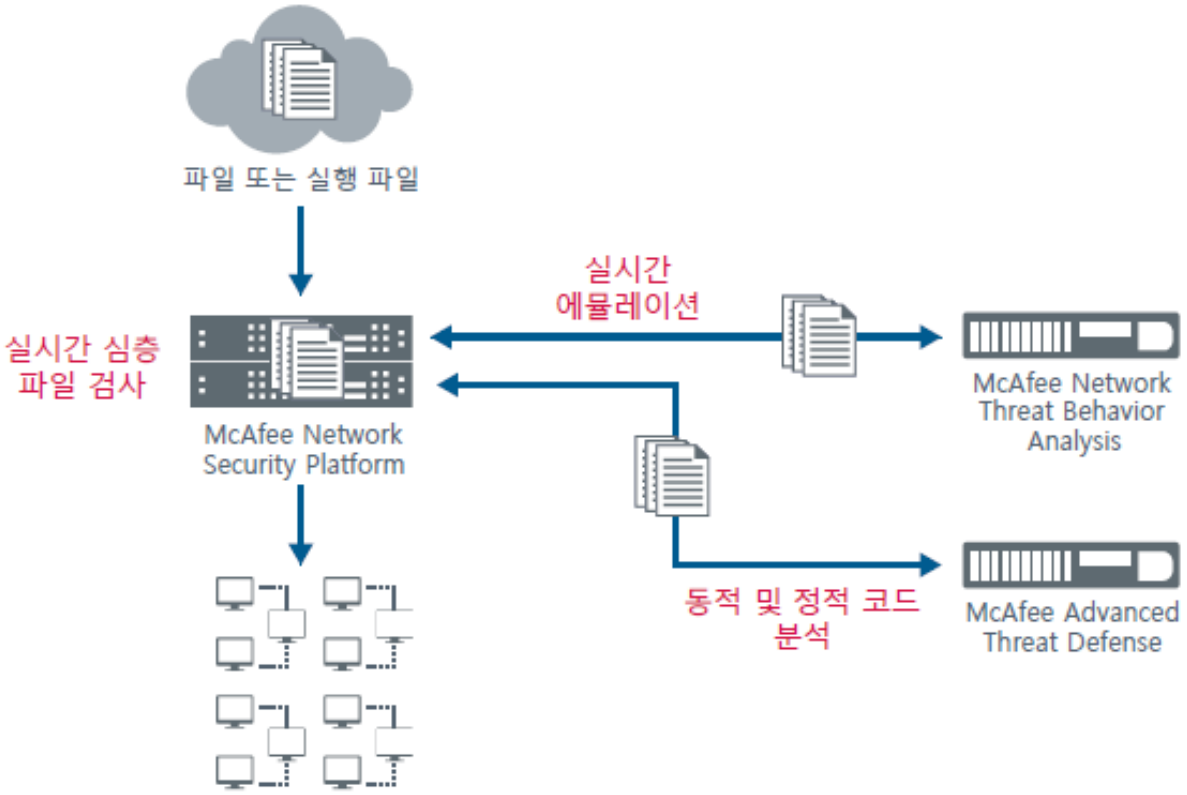
- 악성코드는 강력한 전파 체계를 구축하여 지속적인 위협을 주며 진화를 거듭하고 있다.
- 기존의 네트워크에 집중된 보안 Concept만 으로는 APT(Advanced Persistent Threat)과 같은 위협에 대해서 완벽하게 대처하기 어렵다.
- 기업들은 자신의 경계를 강화 해야 한다.

Source: Malware, APTs, and the Challenges of Defense, Gartner (updated 26 December 2012)

McAfee NSP 지능형 위협 방어

코드 행위 분석

코드 에뮬레이션: 내장형 스크립트에 대한 실시간 에뮬레이션 환경



오늘날 진보된 위협은 취약점을 공격하는 Exploit같은 특정 패턴 의 취약점 공격 형태가 아닌, 문서 파일 내의 Active Script나 HTML내 정상 서비스를 가장 한 Code형태로 작성 되는 경우가 크게 증가

맥아피 NSP는 독자적인 코드 행위 분석 Feature를 구축 코드의 악의성을 분석 하고 실시간으로 대응 가능한 **코드 행위 분석 기능을 제공**

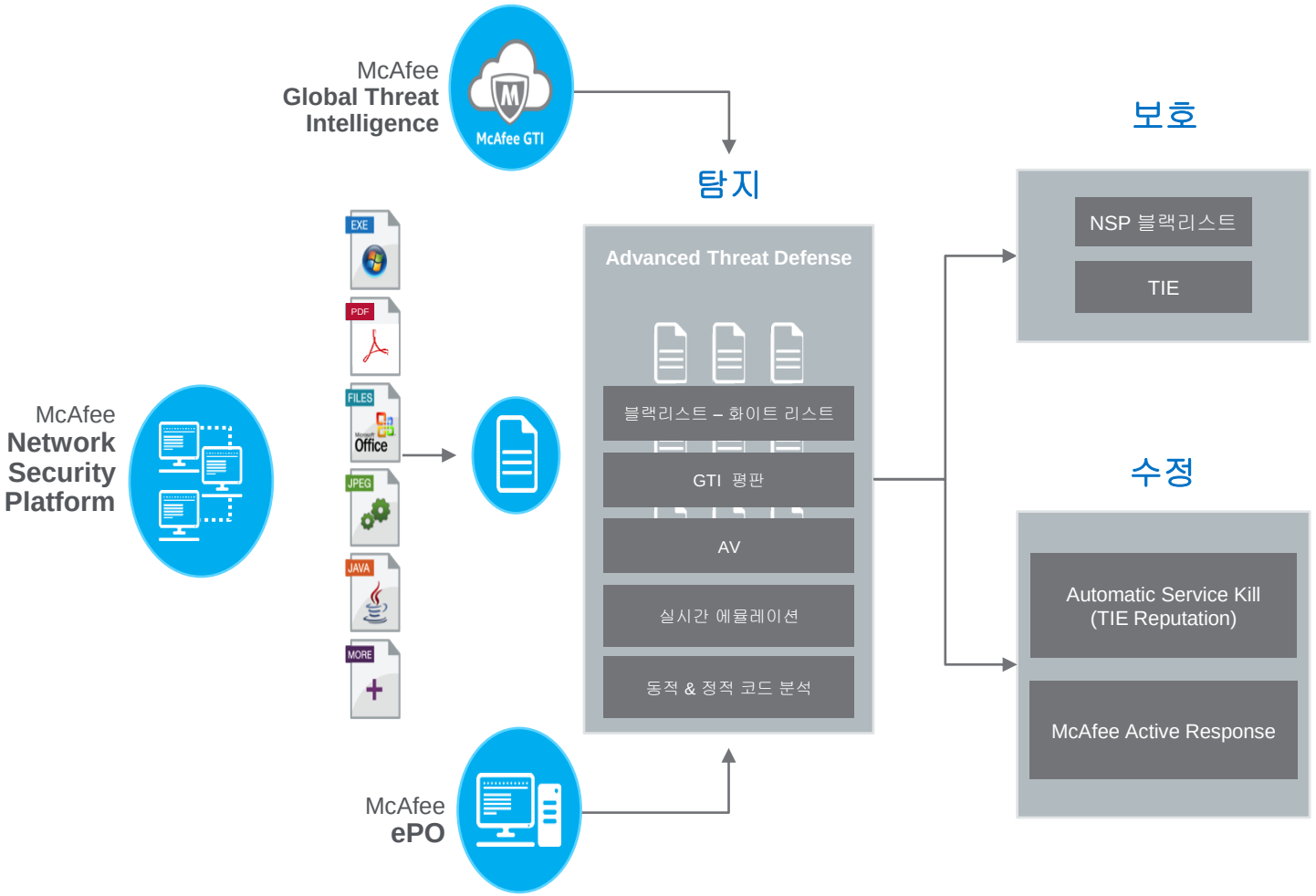
코드 에뮬레이션

- 자바스크립트 환경의 **실시간 에뮬레이션**
- 문서파일 내의 Malicious 패이로드에 대한 **지능적 탐지**
- 수 백만개의 파일에 대한 **평판 정보 기반의 탐지/차단**

진화한 위협의 다각적 접근법

Faster Time to Advanced Threat Conviction, Containment and Remediation

- 탐지
- 보호
- 수정

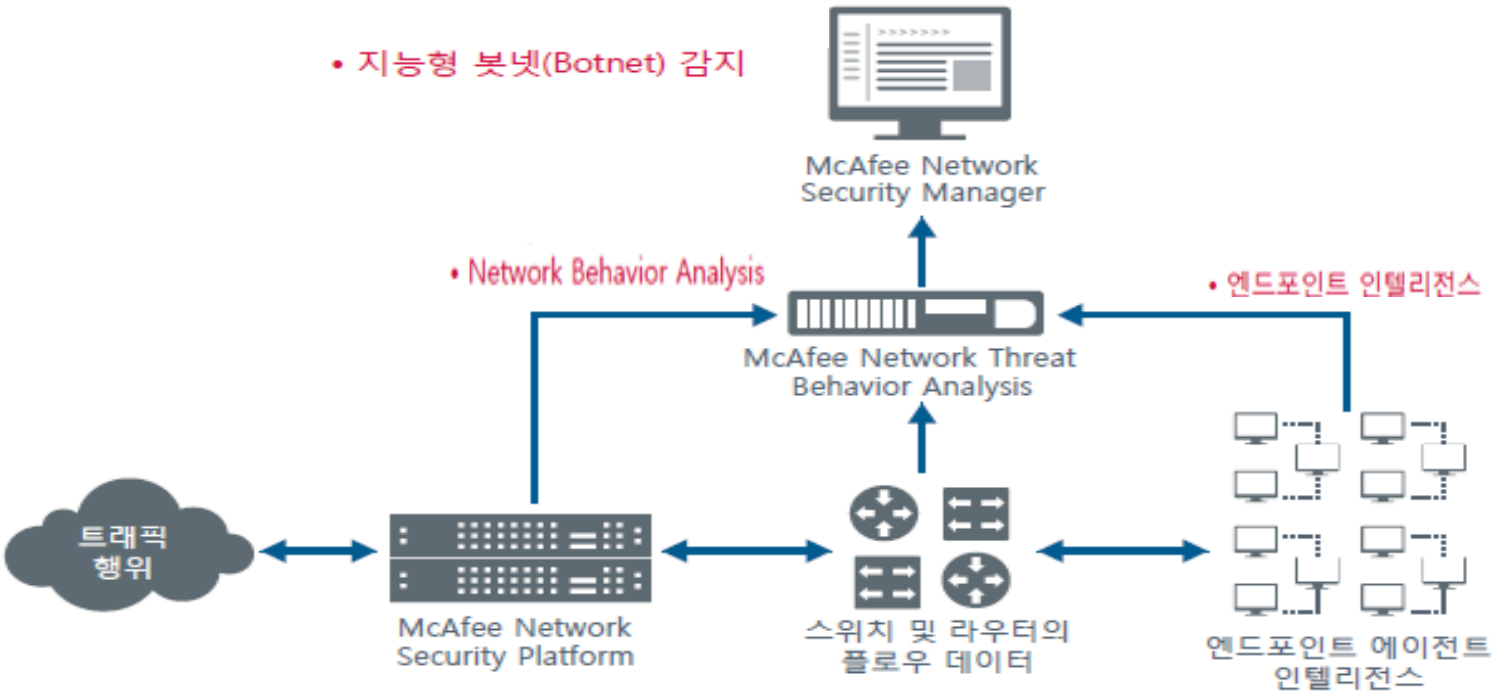


트래픽 행위 분석

엔드포인트 정보: 네트워크 엔드포인트 연동, 상태정보 컨트롤

봇네 탐지: 지능형 멀티 이벤트 상관 관계

네트워크 행위 분석: 고급 상관 관계 분석 및 가시성 제공



McAfee Endpoint Intelligence Agent

오늘날의 어플리케이션 가시성

NETWORK PERSPECTIVE	
사용자	네트워크 어플리케이션
Alice	Oracle
	SalesForce
	Twitter
Bob	Skype
	SSH
	Oracle
Carol	HTTP, SSL
	IMAP
	Oracle

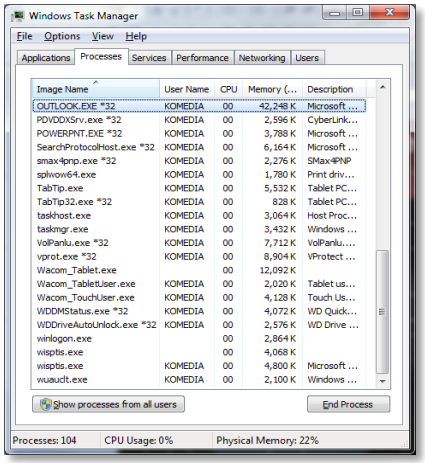
Network Security Platform

네트워크 어플리케이션이 사용하는 포트에 대한 검사만으로 오늘날의 진보된 위협 대응에는 많은 한계 성을 보이게 됨.

특히 APT의 경우는 하나의 위협도가 높은 행위가 아닌 다수의 일반적인 행위를 다수 수행 하는 형태적 특징을 가짐으로 **개별적인 기능으로 동작하는 형태의 보안 장비로는 탐지가 어려움**

McAfee NSP는 엔드포인트의 정보와 연계 하여 실제 악성코드가 행동하는 엔드포인트의 프로세스 통신 상태, 해당 프로세스의 악성 행위 여부 정보 등과 연계 되어 능동적, 입체적 대응 체계를 구축.

Endpoint Intelligence in Action



NETWORK PERSPECTIVE		ENDPOINT INTELLIGENCE	
사용자	네트워크 어플리케이션	Host Process	Anomaly
Alice	Oracle	Hyperion	No
	SalesForce	Firefox	No
	Twitter	TweetDeck	No
Bob	Skype	Skype	No
	SSH	PuTTy	No
	Oracle	Oracle CRM	No
Carol	HTTP, SSL	Safari	No
	IMAP	Thunderbird	No
	Oracle	OUTLOOK.EXE	**Yes**

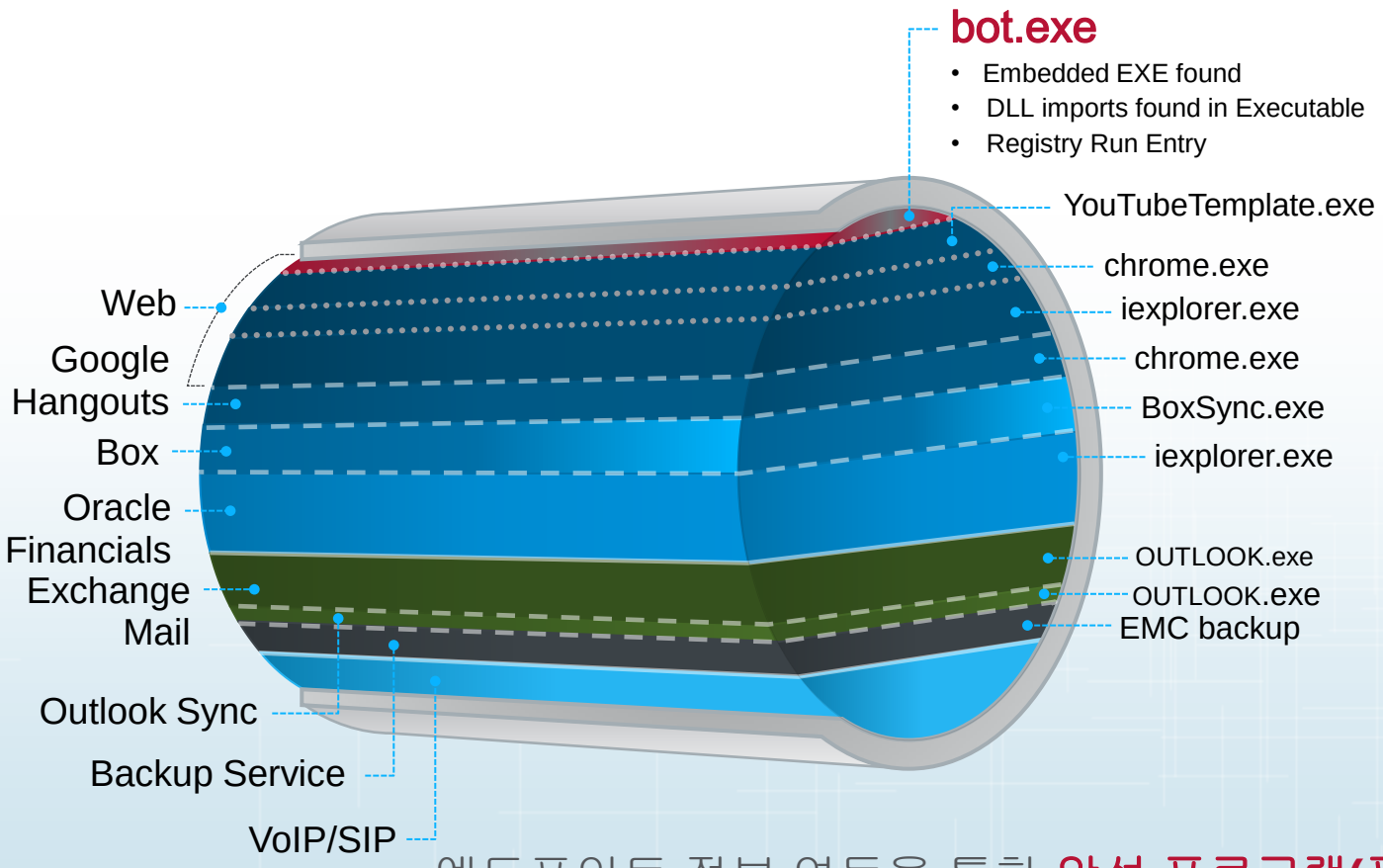
싱글 패킷 시그널

Endpoint Intelligence Agent

Network Security Platform

McAfee Endpoint Intelligence Agent

Beyond Layer 7 Visibility with McAfee Endpoint Intelligence Agent

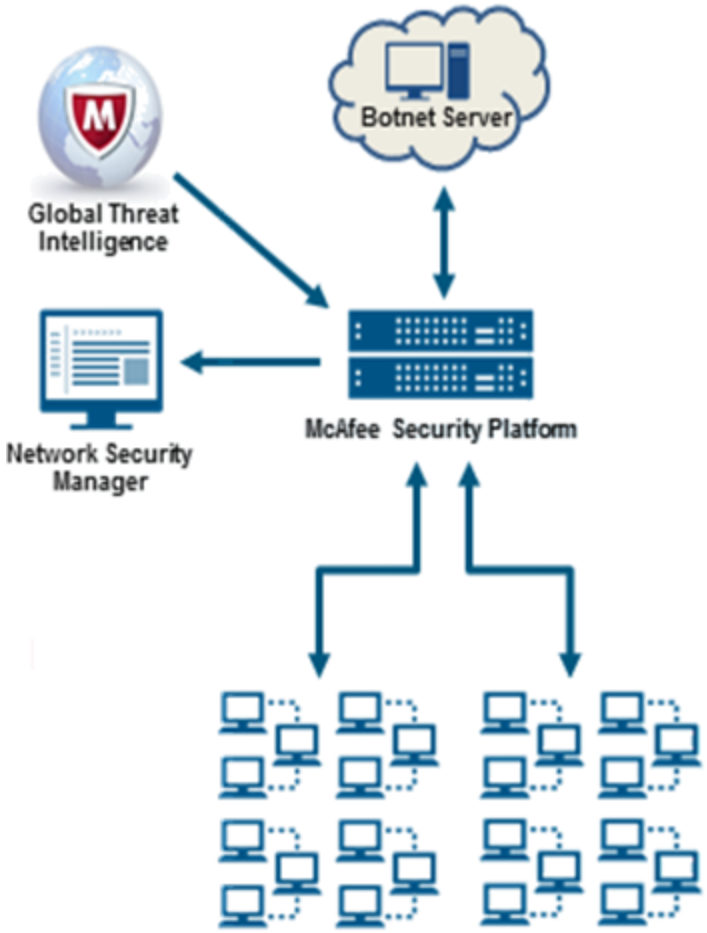


- Intelligent
- Exfiltration protection
- Combines endpoint and network perspective

엔드포인트 정보 연동을 통한 **악성 프로그램(프로세스)가 사용한 통신 Port,** 해당 파일의 악성 여부 등의 정보와 연계 하여 대응

정교한 봇넷 탐지

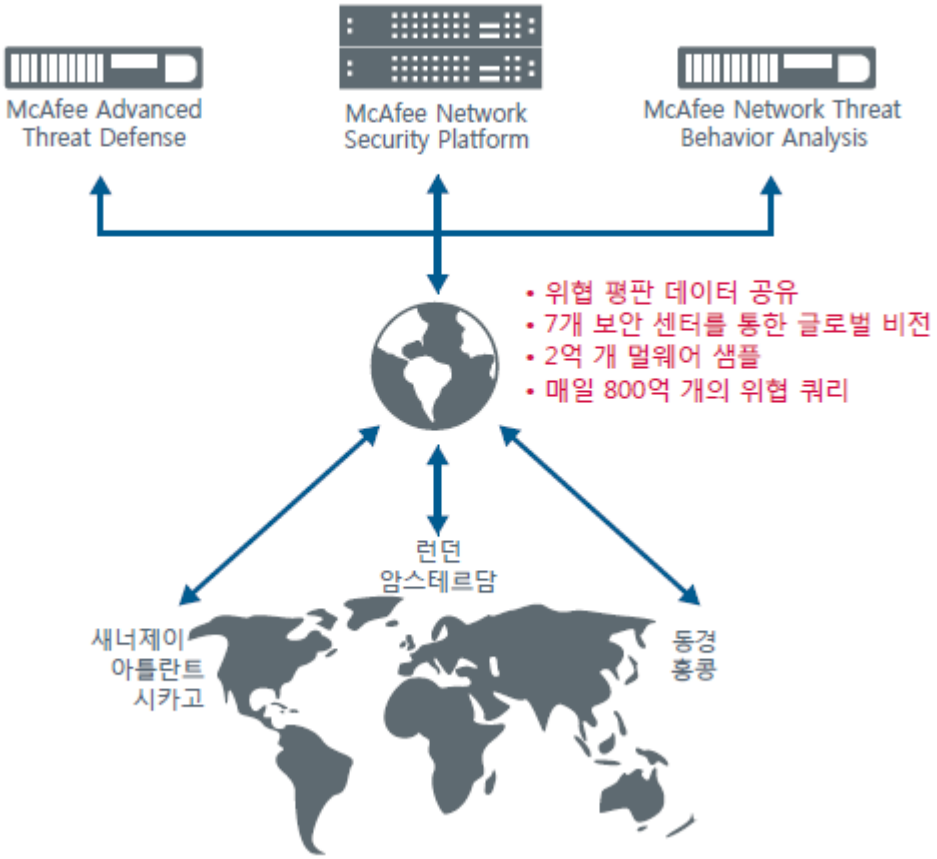
- 봇넷 활동 분석을 위한 멀티 이벤트 상관 분석
- **McAfee 글로벌 평판 정보와 Heuristic 기반의 봇넷 탐지**
- 클라이언트와 서버 플로우 기반의 분석
- 네트워크 위협 행동 분석을 통한 확장된 개념의 봇넷 탐지



글로벌 평판 정보

Global Vision: 위협 평판 데이터 공유

글로벌 인텔리전스: **일 평균 800억 건의 쿼리, 3억 개의 멀웨어 셈플**



새로운 패러다임, Actionable Events

기존의 방식

탐지된 **Alerts**을 추적

Actionable **Events**

Event를 이해하는 방식

지능적인 멀웨어 정책 워크 플로우

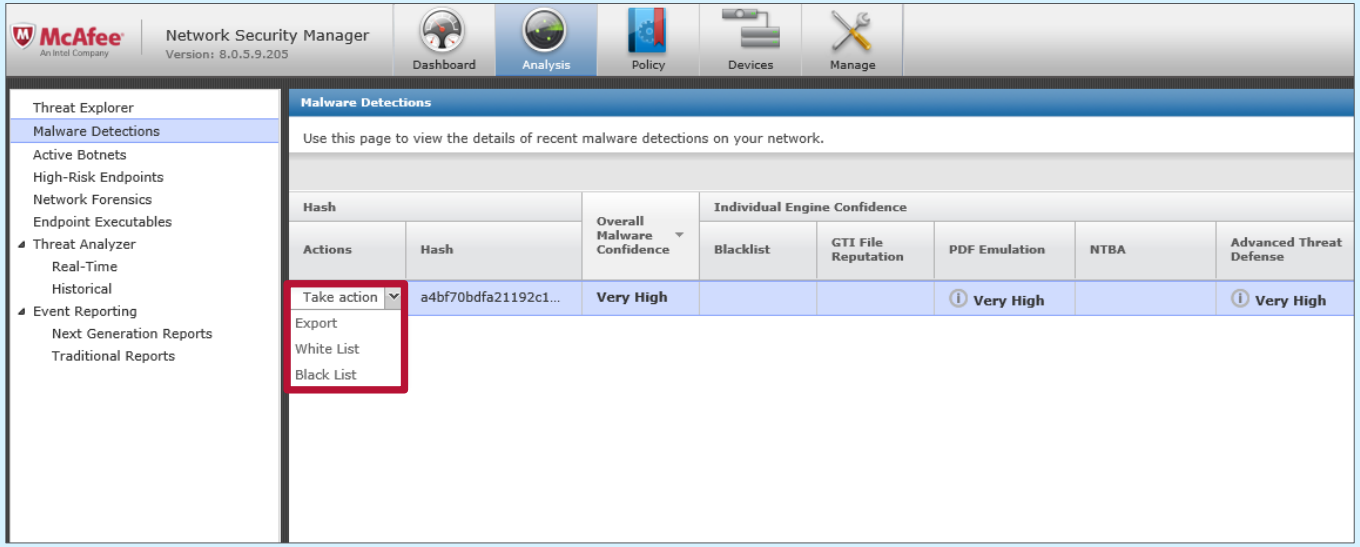
Alerts을 추적 하는 방식에서 events를 이해(분석)하는 방식으로 진화

Dashboard
Synopsis of risks and threats

Malware
Top threats, threat relevancy

ATD
Connections, behavior, files, users

Action
IPS, app control, ACLs, custom



지능적인 멀웨어 정책 워크 플로우

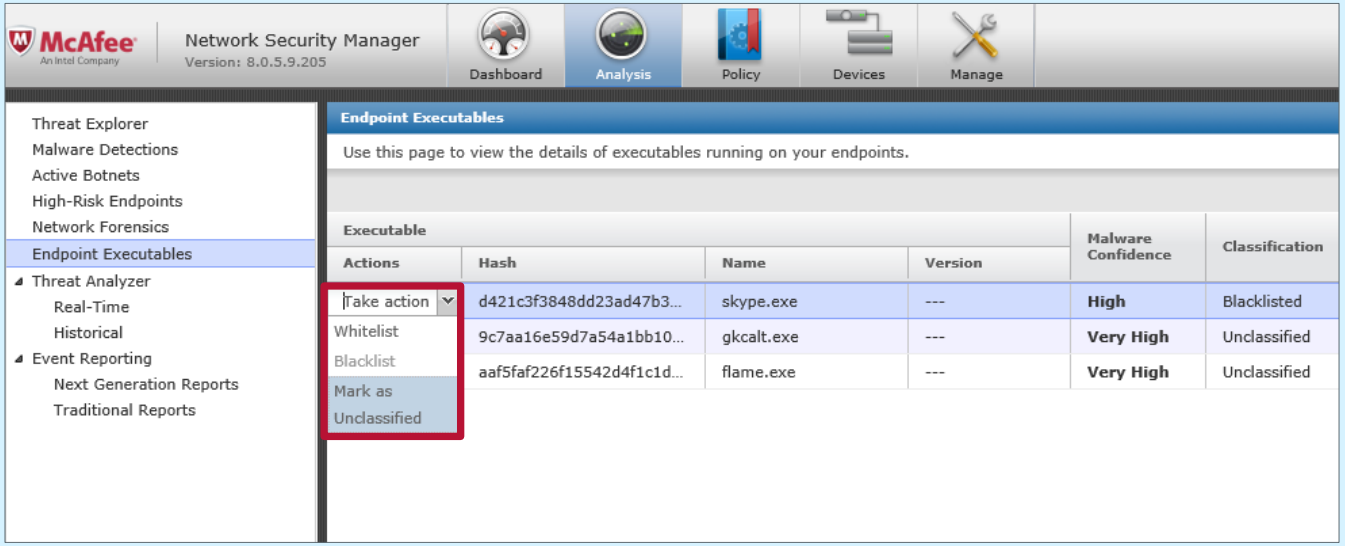
고 위험군을 추적 하는 방식에서 events를 이해(분석)하는 방식으로 진화

Dashboard
Synopsis of risks and threats

EIA
OS, vulnerabilities, host events

System
Malware indicators, Invoked libraries

Action
IPS, app control, ACLs, custom



탁월한 위협 방지

다중 **차세대** 방어

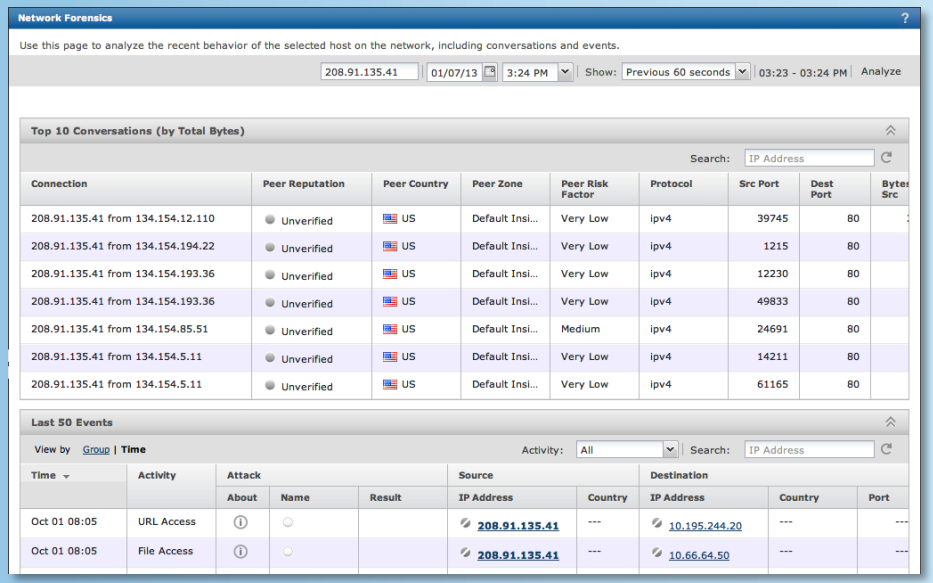
위협 익스플로러
Vulnerability-based engine requires less signatures

악성코드 다운로드
Comprehensive malware protection

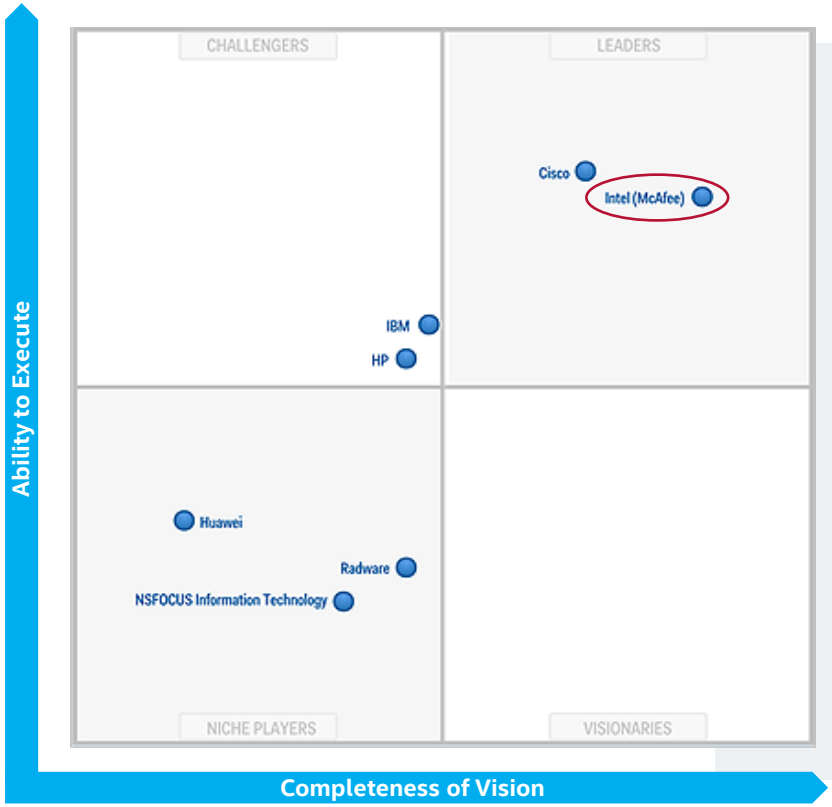
액티브 봇넷
Multi-attack heuristic identification

고 위험 호스트
Holistic host assessment

네트워크 포렌직
Detailed behavior analysis



Consistent Leadership and Vision



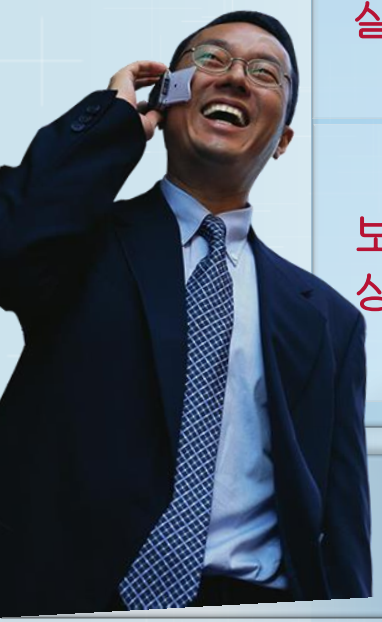
8 회 연속
쿼드런트 리더 그룹 선정
선정 이유:

1. **"다중 시그니처리스 검사 테크닉"**은 일반 시그니처 기반의 IPS비해 탁월한 강점을 제공
2. 온박스(On-box) **SSL 성능**
3. 타사에서 **우위 경쟁사(Top competitor)로 고려함**

Gartner 2014 IPS Magic Quadrant

McAfee NSP의 차별성

Network Security Platform	Value
시그니처 + 시그니처 기반의 탐지 한계를 극복 하는 다중 분석 엔진	탐지의 정확성 향상에 의한 악성 코드로부터의 손실 감소
정책 적용 판단이 가능한 실용적인 데이터 제공	분석의 신뢰성과 소비 시간 감소 운용 비용을 절감
보안 정책 개선을 위한 상황 정보 제공	숨겨진 위협들에 대한 도출과 정책 적용을 위한 오버 헤드를 절감



네트워크 보안 구현에 대한 지능적인 접근 방식


intel
Security