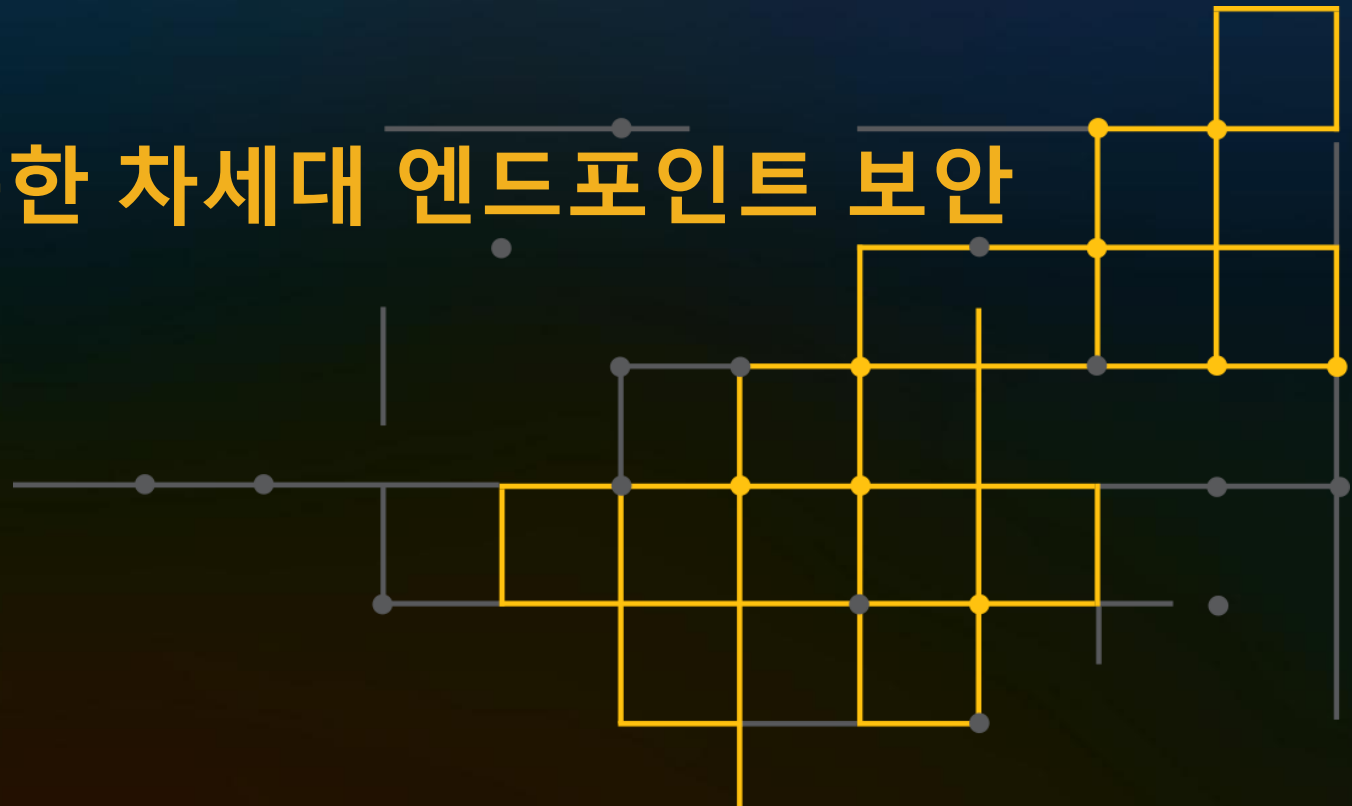


# Why Endpoint?

다차원 머신러닝을 활용한 차세대 엔드포인트 보안

최재우 / SE 팀  
시만텍코리아



# 1

## 최신 보안 위협 동향



# 갈수록 확대되는 보안 위협 환경

엔드포인트 보안 솔루션은 공격 체인 전반에서 보안 위협을 탐지하고 차단



**4억 3천만**

2015년에 발생한  
신종 악성코드



**+23%**

4억2천9백만  
개인정보 탈취



**+35%**

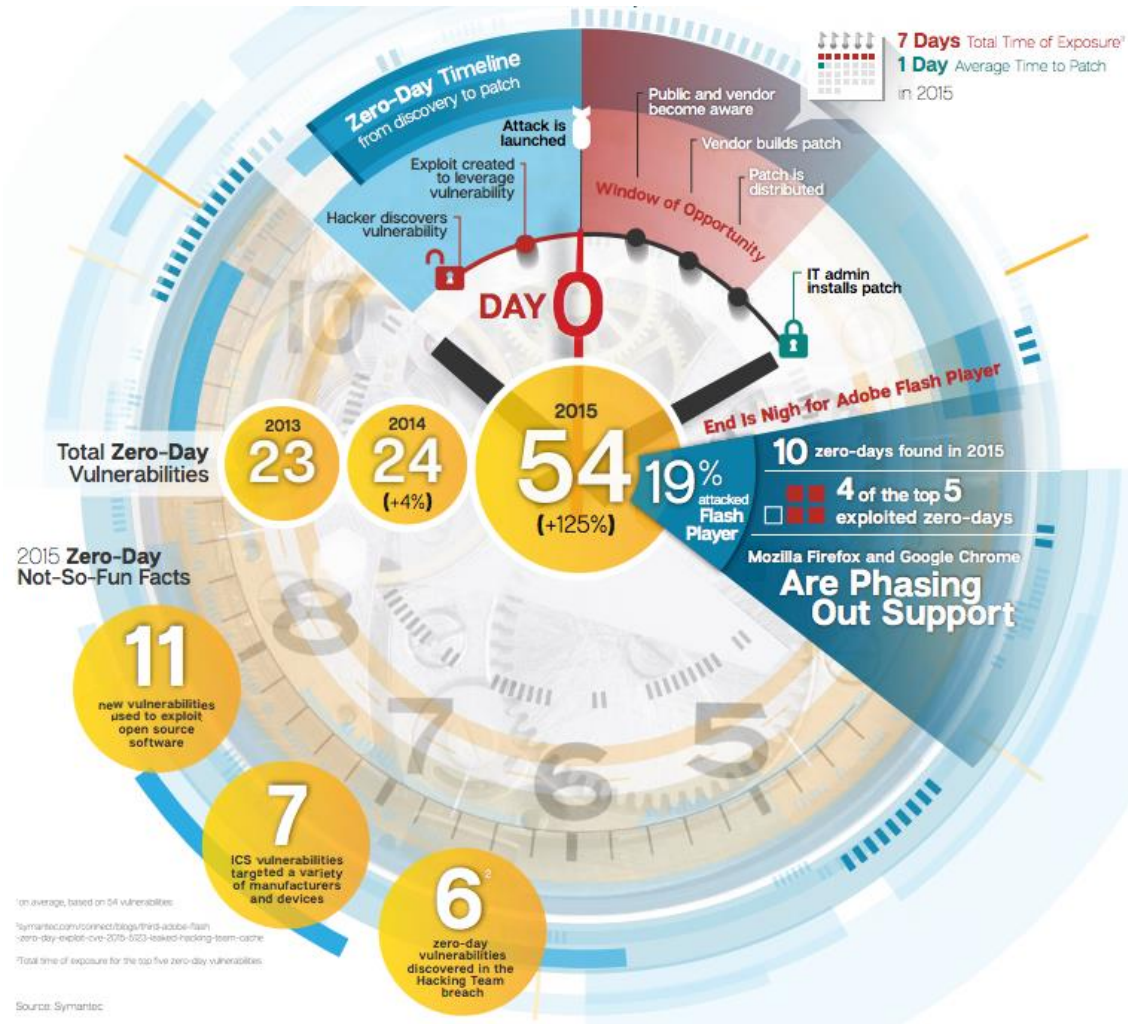
2015년 랜섬웨어  
증가



**+55%**

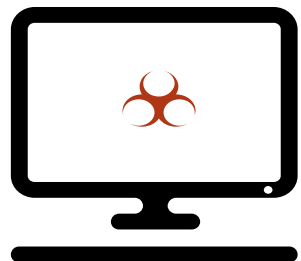
표적공격  
증가

# 새로운 제로데이 취약점 발견 매주 1건 이상의 제로데이 취약점이 발견됨



# 과거 어느 때보다도 어려워진 엔드포인트 보안

한층 심각해진 보안 위협과 부적합한 엔드포인트 보안이 비즈니스 방해



# 80%

의 보안 담당자는 엔드포인트 보안 관리가 2년 전에 비해 더욱 어려워졌다고 느낍니다.

- ESG Endpoint Security Report



## 속도를 따라잡기 어려움

31%가 신종 악성코드 위협 해결을 최우선 순위로 간주



## 생산성 저하

보안 전문가 38%가 발생한 문제를 해결하는 데 대부분의 시간 소비



## 고비용

기업의 데이터 보안 사고 평균 비용은 4백만 달러

# Symantec Endpoint Protection

“ 2016년 사이버 첩보 사고의 90%가 악성코드를 통해  
진행되었습니다. 이것이 이메일, 웹, 또는 직·간접으로 설치 등의  
배포 수단이 무엇이든지, 엔드포인트 보안이 가장 필수적입니다. ”

Verizon 2016 Data Breach Investigations Report



# 복잡한 환경 + 스마트 공격자 = 지능형 보안 위협



## 침투

- 웹
- 이메일
- 정상 애플리케이션
- 매체

다양한 공격 경로



## 감염

- 파일
- 매크로
- 메모리
- 네트워크 조사(recon)
- 암호화 악성코드
- 루트킷

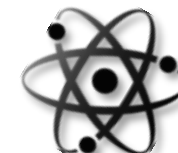
다양한 페이로드



## 침입

- 무기화 및 회피
- C&C 통신
- 측면 이동
- 비인가 실행

빠른 전염



## 예방 및 대응

- 파일 및 엔드포인트 격리
- 제거 및 사고조치
- 시스템 하드닝

공격 체인 전반에서 지능형 보안 위협 차단에 효과적인 기술이 부족한 엔드포인트 보안 벤더

# 2



## SEP 14 강력한 보호





# 공격 체인 전반에서 강력한 보호

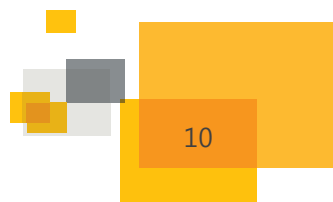
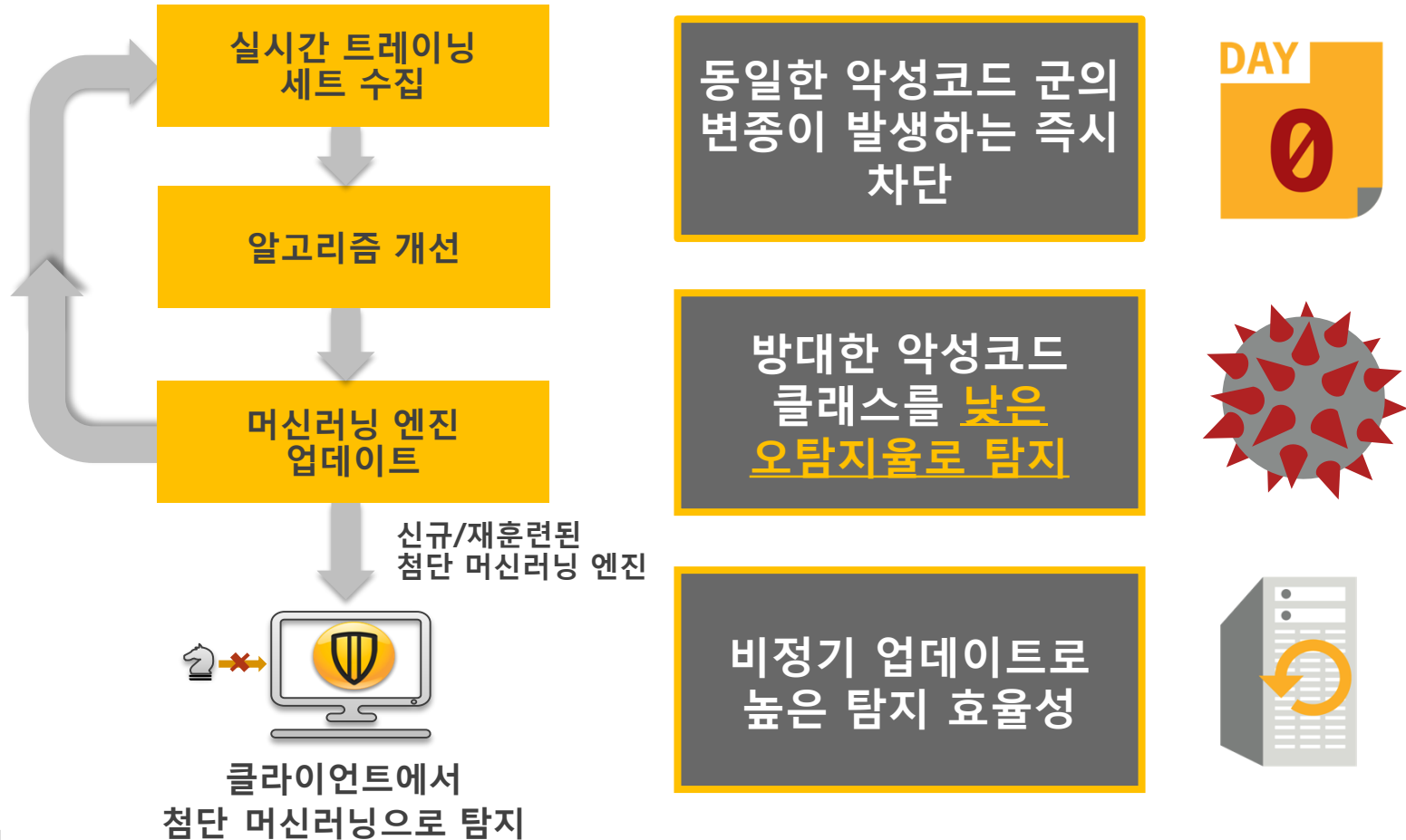
## 다계층 보호로 표적 공격 및 제로데이 보안 위협 차단

특허 받은 실시간 클라우드 조희 기술로  의심스러운 파일 검사 

								
네트워크 방화벽 및 침입 차단	애플리케이션 및 매체 제어	메모리 익스플로잇 공격 차단	평판 분석	첨단 머신러닝	에뮬레이션	안티바이러스	행동 모니터링	네트워크 방화벽 및 침입 차단
악성코드가 시스템에 감염되기 전 차단하고 네트워크를 통제함	파일, 레지스트리, 디바이스 액세스 및 행동 제어, 화이트리스트, 블랙리스트 등	인기 소프트웨어의 취약점을 공격하는 제로데이 익스플로잇 차단	커뮤니티의 집단지성을 활용하여 파일 및 웹 사이트의 안전성 확인	악성코드가 실행되기 전에 신종 및 진화하는 악성코드 탐지	커스텀 패커를 사용하여 탐지우회기능 악성코드를 가상머신에서 탐지	시스템에 침투한 악성코드 검사 및 제거	의심스러운 행동을 나타내는 프로세스 모니터링 및 차단	악성코드가 시스템에 감염되기 전 차단하고 네트워크를 통제함
침투				감염			침입 및 유출	

# 첨단 머신러닝

## 알려지지 않은 보안 위협 및 변종 악성코드 차단



# 첨단 머신러닝

## 알려지지 않은 보안 위협 및 변종 악성코드 차단

### 다차원 머신러닝 기법을 사용한 공격 분석

시만텍은 머신러닝을 위한  
실시간 분류기법 사용



위협 연관관계



악성코드 속성



웹도메인



프로세스 행동분석



IP 주소



디지털 서명



기타 분석 요소

속성, URL, 행동 또는 상호연관정보에 의한 학습이 가능한 다차원 머신러닝 기술을 사용해  
알려지지 않은 악성코드 차단

# 세계 최대 규모의 글로벌 보안 위협 인텔리전스 네트워크

다양한 데이터, 고급 알고리즘, 뛰어난 기술력을 갖춘 보안 위협 전문가

**1억 7천5백만**

보호 대상 개인 사용자 및  
기업 소유 엔드포인트

**4억 3천만**

지난해 발견한  
새로운 고유 악성코드

**수십억**

매일 검사하는  
이메일 트래픽



**9개** 보안 위협 대응 센터

**5,700만** 공격 센서-  
**157개국**

**12,000**

클라우드  
애플리케이션 보호

**1억 8천2백만**  
지난해 차단된 웹 공격

**10억**

매일 검사하는 웹 요청

최대 규모의 사이버 인텔리전스 네트워크 중 하나  
3조 7천억 행의 보안 관련 데이터

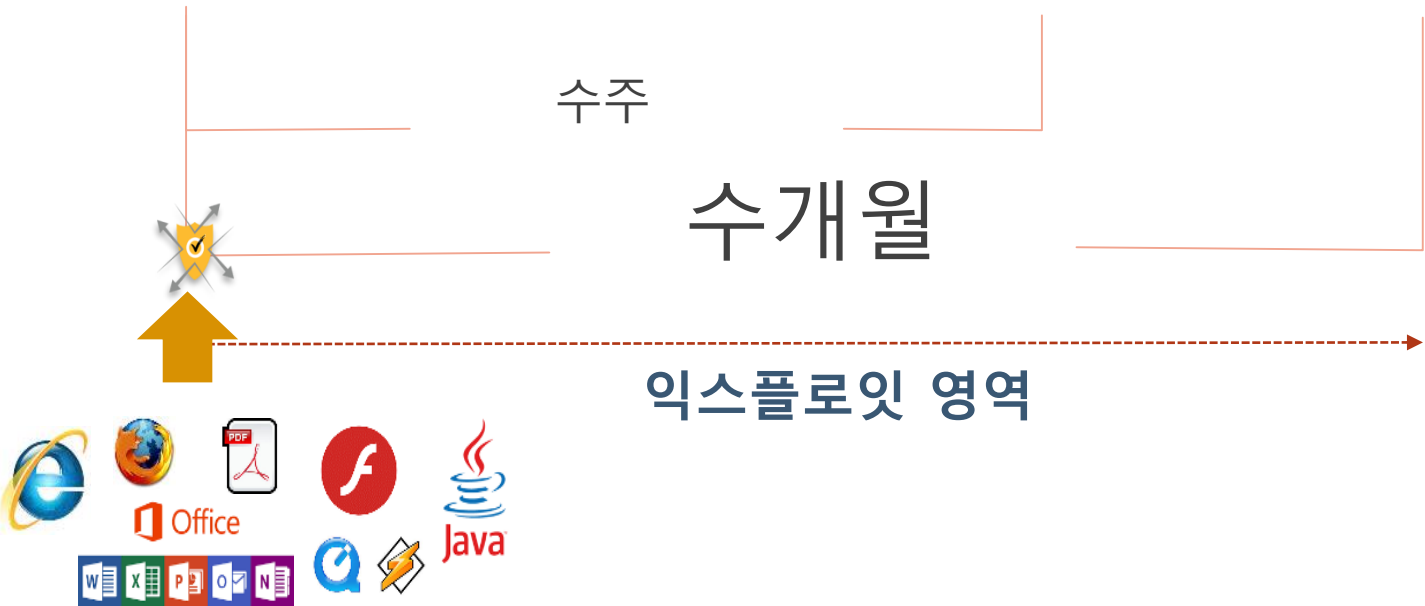
# 메모리 익스플로잇 공격 차단

## 널리 사용되는 소프트웨어에 대한 제로데이 메모리 공격 차단



사전 예방적으로 익스플로잇 기법을 차단하여 공격자의 시스템 장악 시도 차단

시그니처에 의존하지 않으며 어떤 결함/버그/취약점에도 효과적

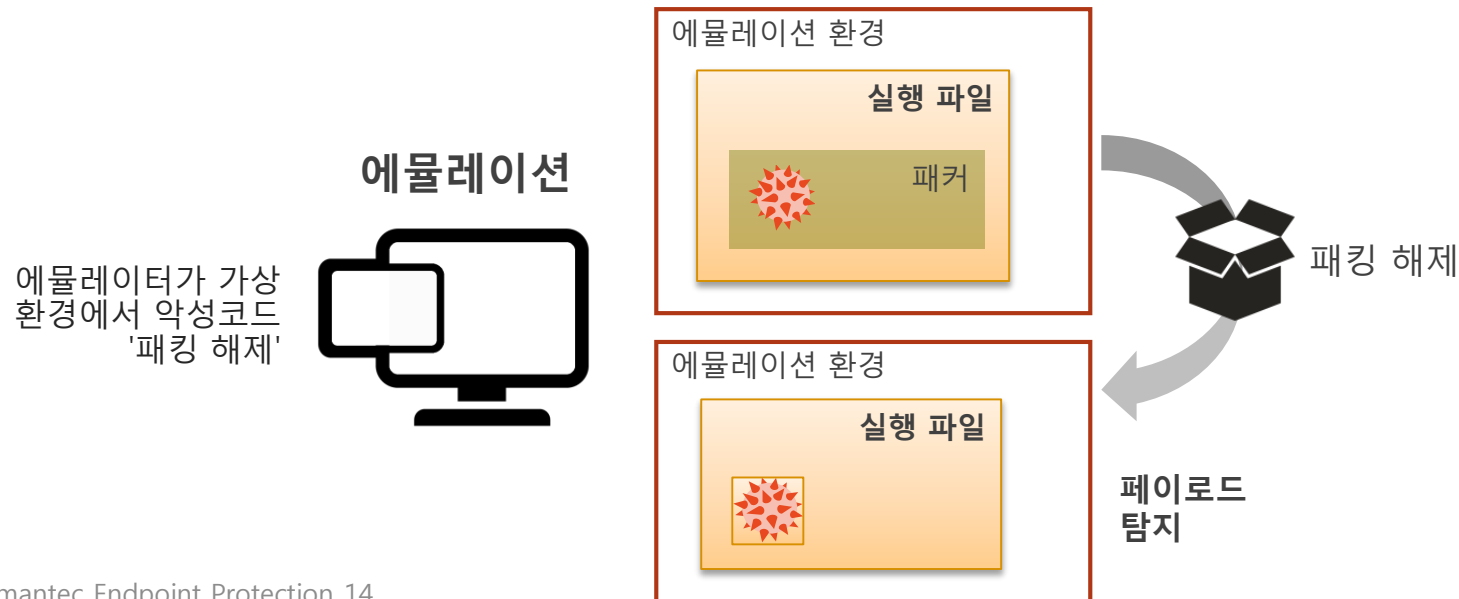


# 에뮬레이션 기능

## 신속하고 정확하게 숨어 있는 악성코드 탐지



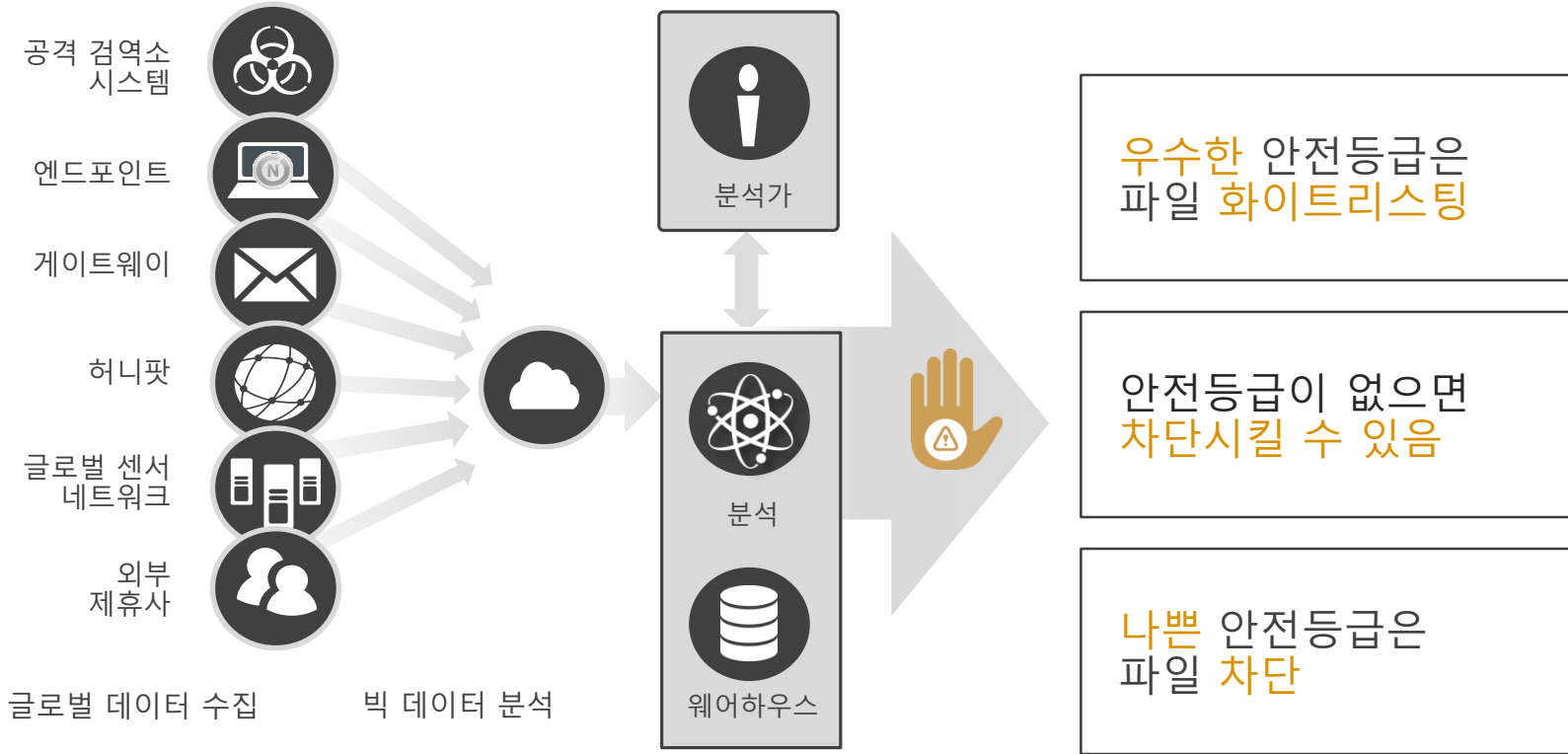
파일 실행을 에뮬레이션하여 악성코드 자체를 드러내어 악성코드 탐지



밀리초 단위로 실행되는 고효율 경량화 솔루션

# 파일 평판 분석

출현시기, 사용빈도, 위치를 사용하여 알려지지 않은 보안 위협 탐지



시만텍 보안 위협 인텔리전스 네트워크



# 행동 모니터링

행동 모니터링을 통해 제로데이 및 알려지지 않은 보안 위협 차단

인공 지능 기반  
분류 엔진



보안전문가가 작성한  
행동 시그니처



행동 정책 락다운



약 **1,400+**가지의 파일 행동을 모니터링하여 탐지:

무엇을 했는가?

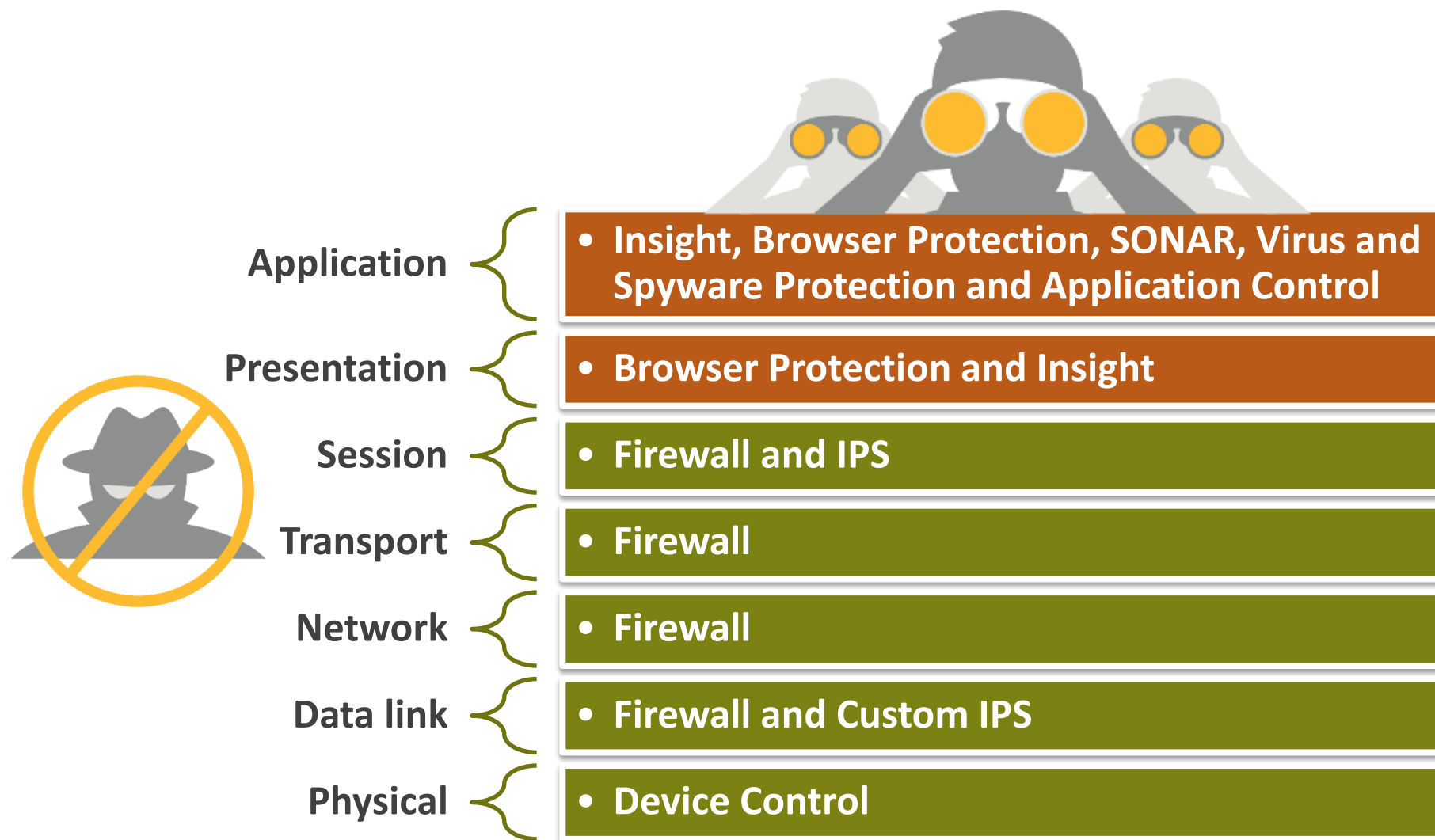
출처는 어디인가?

무엇이  
포함되었는가?

누가 관련되었는가?



# 네트워크 위협 차단(OSI Model)



# 공격 체인 전반에서 보호

엔드포인트를 공격하는 방식에 관계없이 보호



# 3

## SEP 14 탐지 및 대응(EDR)



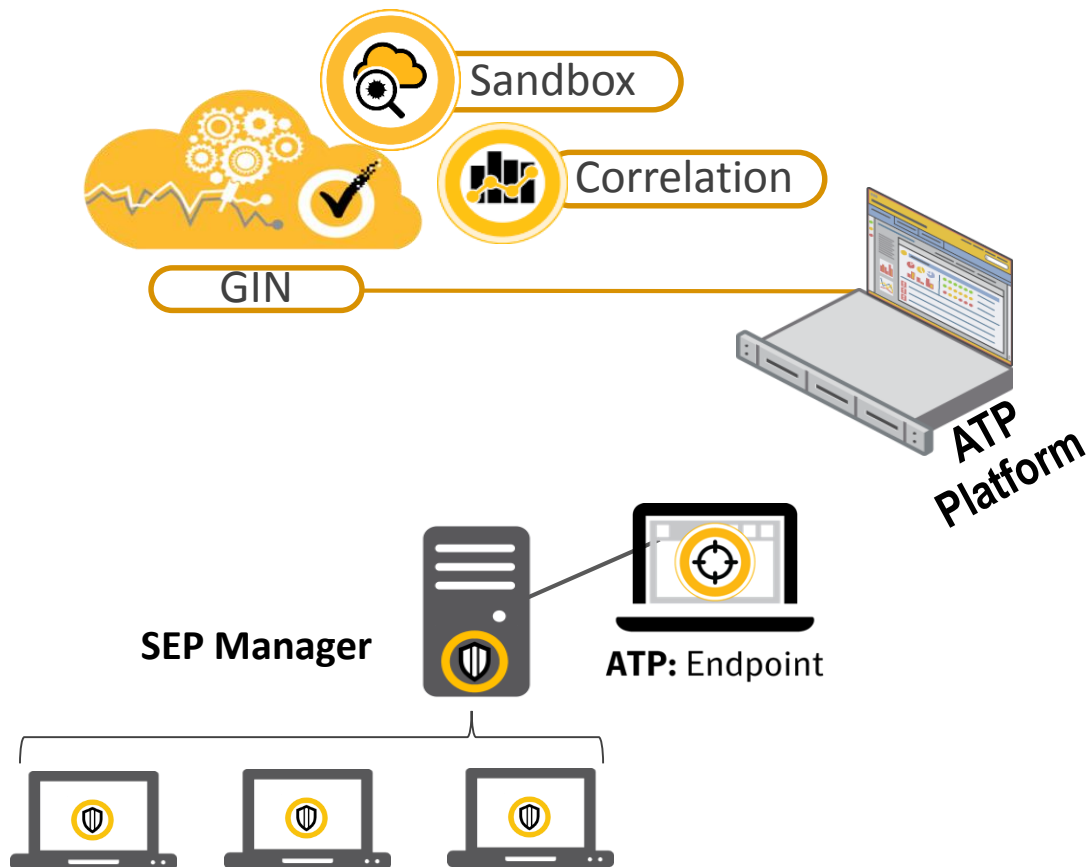
# 지능형 공격에 대처

신속하게 감염 확산을 방지하여 피해 최소화

			 <span style="color: red; font-weight: bold;">NEW</span>	
<p><b>POWER ERASER</b></p>	<p><b>호스트 무결성</b></p>	<p><b>시스템 락다운</b></p>	<p><b>시큐어 웹 게이트웨이 통합</b></p>	<p><b>EDR 콘솔(ATP: ENDPOINT)</b></p>
<p>제거하기 어려운 감염도 확실하게 해결</p>	<p>격리, 비인가 변경 탐지, 손상 정도 평가, 컴플라이언스 보장</p>	<p>애플리케이션 제어 기능 - 화이트리스트 및 블랙리스트로 강화된 엔드포인트 보안</p>	<p>API를 통해 '시큐어 웹 게이트웨이'에서 조직적으로 대응</p>	<p>Symantec EDR 콘솔의 조직적인 대응, EDR 기능은 SEP 에이전트에 내장되어 있음</p>
<p><b>예방 및 대응</b></p>				

# 엔드포인트 탐지 & 대응 (ATP: Endpoint)

새로운 엔드포인트 에이전트없이 EDR (Endpoint Detection and Response) 기능 제공



의심스러운 이벤트를 **조사하고** 완벽한 엔드포인트 **가시성** 확보

모든 공격 징후에 대한 **즉각적인 검색** 및 침해지표(IoC)에 따른 엔드포인트 조치

모든 위협 요소를 단 한번의 클릭으로 수분안에 **치료**

# 엔드포인트 탐지 & 대응 (ATP: Endpoint)

## 우선순위에 따른 대응 및 가시성 확보

### < Incident: 100008 >

Multiple attacks have been detected targeting C2011-703.

RECOMMENDED ACTIONS:

Remove any software that attempts the malicious activity. Also, consider contacting the computer's user about browsing activity that can result in malicious downloads.

**Low**  
PRIORITY

**False**  
TARGETED ATTACK

**1**  
INCIDENTS

--  
NETWORK SCANNER

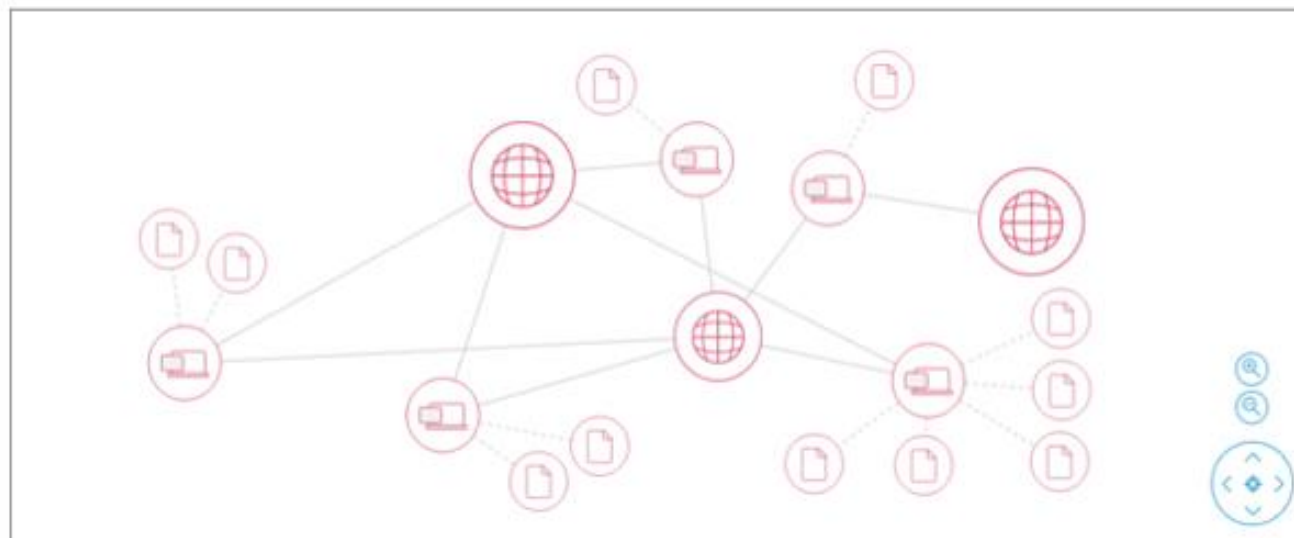
**10**  
EVENT COUNT

**Open**  
INCIDENT STATUS

2016-10-21 03:50:15 UTC  
FIRST SEEN

2016-10-26 15:00:20 UTC  
LAST SEEN

2016-10-26 15:05:06 UTC  
LAST UPDATED



# 엔드포인트 탐지 & 대응 (ATP: Endpoint)


내부 시스템들의 검색 기능을 통해 악성 파일 유입 확인

The screenshot displays the Symantec Advanced Threat Protection (ATP) search results page. At the top, there is a search bar containing the MD5 hash `b9bc3f1b2aace824482c10ffa422f78b` and a 'Search' button. To the right of the search bar is an 'Endpoint Sweep' toggle switch, which is currently turned off. A callout box points to this toggle with the text 'DB검색 Endpoint검색'. Below the search bar, the search results are displayed in a table format. The table has three columns: 'Type', 'Results', and 'Found Results'. The 'Found Results' column is further divided into 'FILE', 'ENDPOINTS', and 'DOMAINS'. The search results table shows one result: a file named `rad485ed.tmp.exe` located at the path `...CSIDL_SYSTEM/bad_folder/rad485ed.tmp.exe`. The file was first seen on 2015-04-27 at 12:55:50 UTC. The search results also show 12 related endpoints and 2 related domains. The interface includes a 'Delete Search' button and a 'Re-Initiate' button at the bottom right of the search results section.

Type	Results	Found Results
FILE	<code>rad485ed.tmp.exe</code> Name <code>b9bc3f1b2aace824482c10ffa422f78b</code> MDS	<code>...CSIDL_SYSTEM/bad_folder/rad485ed.tmp.exe</code> PATH 2015-04-27 12:55:50 UTC FIRST SEEN
ENDPOINTS		12 RELATED ENDPOINTS
DOMAINS		2 RELATED DOMAINS

# 엔드포인트 탐지 & 대응 (ATP: Endpoint) 상세내역 확인 및 대응

File: com.swotsoft.applet.spi.jar



**Bad**  
DISPOSITION

Cynic  
REASON

No  
TARGETED ATTACK

6ff86acea81a3126442a5e0349e31fa21862adcba8cb10cd05a1ae...  
SHA256

a8b27548a4466a4c06c0b7198959c5b2  
MD5

Not Signed  
CERTIFICATE

application/java-archive  
FILE TYPE

### File Overview

<b>5</b> RELATED EVENTS	<b>0</b> RELATED INCIDENTS	<b>0</b> EMAIL DETECTIONS
<b>188</b> CYNIC MODIFICATIONS	<b>1</b> EXTERNAL DOMAINS ACCESSED	

### Global Reputation

Not Available FIRST SEEN	Fewer than 5 users PREVALENCE
-----------------------------	----------------------------------

### Local Reputation

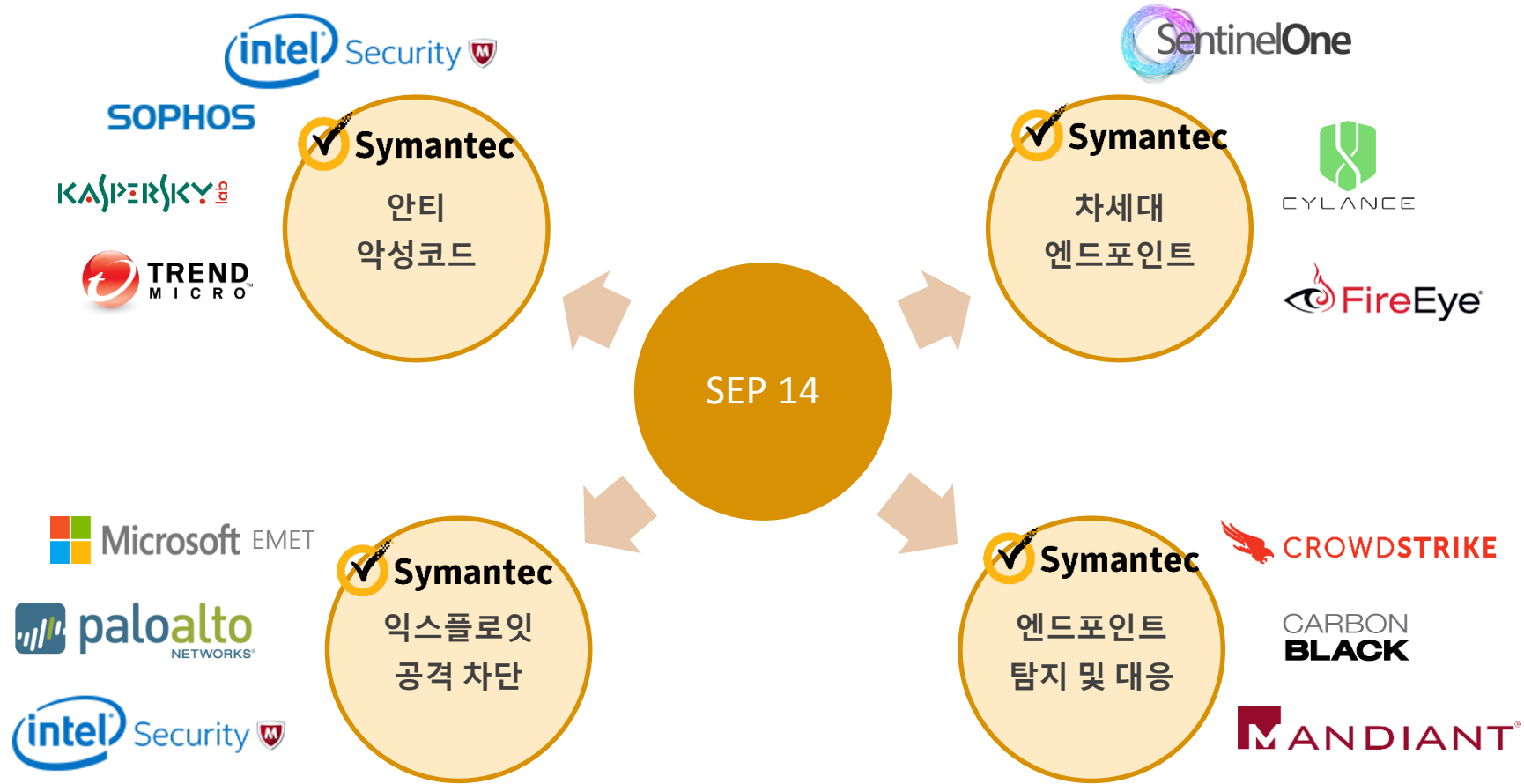
Weeks ago FIRST SEEN	5 internal endpoints PREVALENCE
-------------------------	------------------------------------

Add to Blacklist Add to Whitelist Submit to Cynic Submit to VirusTotal Download from file store Delete File



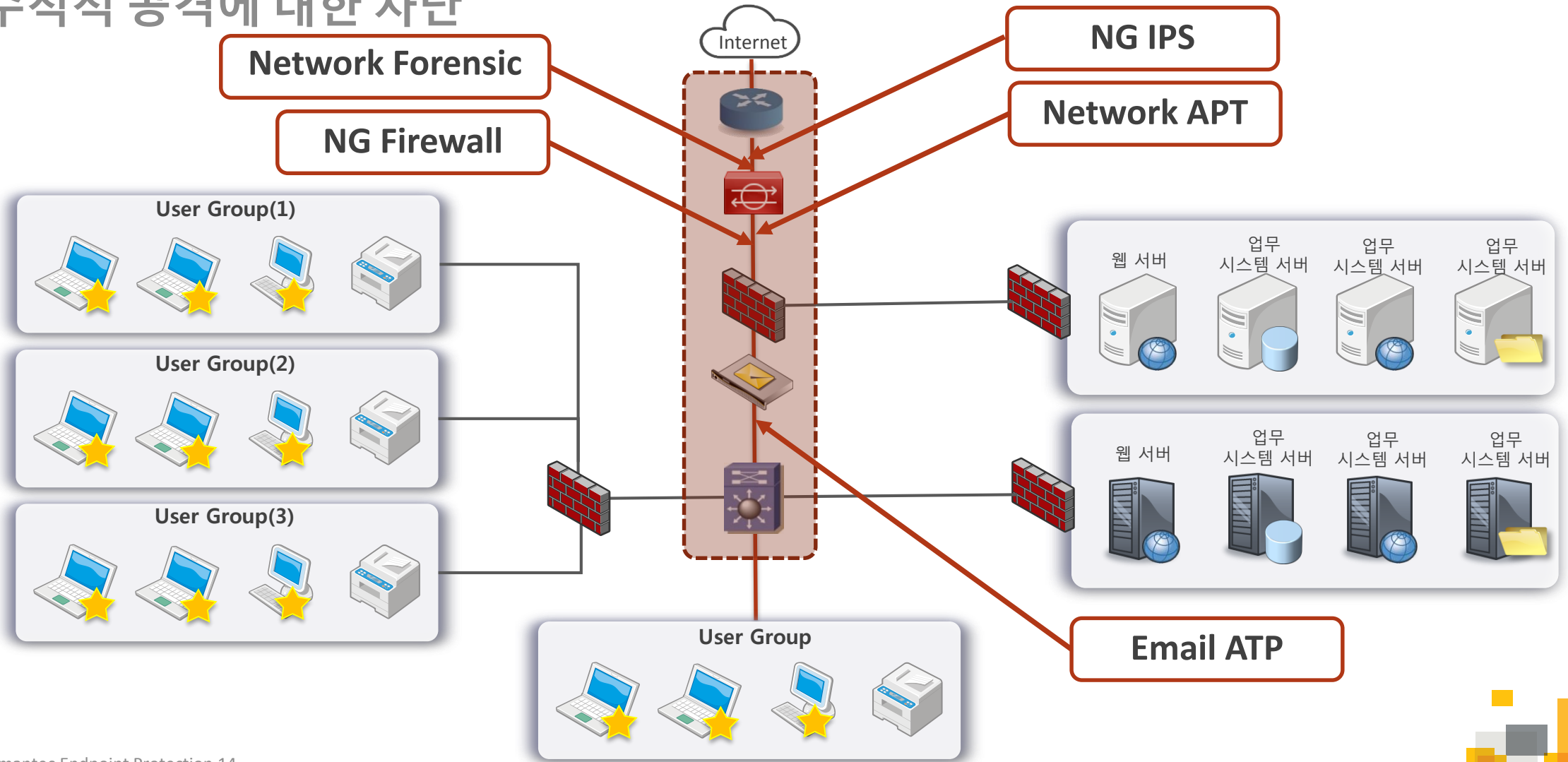
# 복잡한 엔드포인트 환경에 대한 변화 필요

단일 에이전트에서 다수의 기술 통합



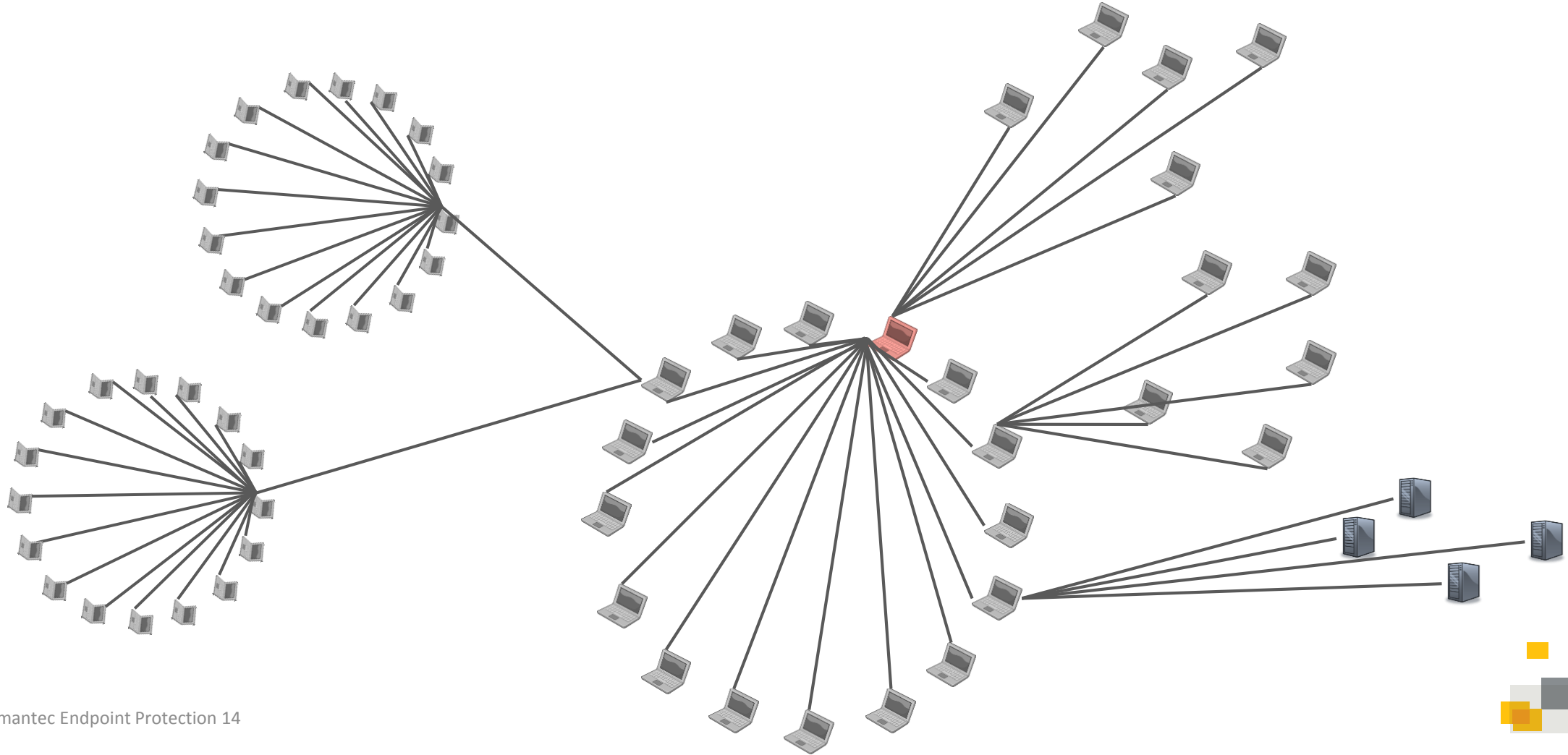
# 공격형태의 변화

## 수직적 공격에 대한 차단



# 공격형태의 변화

## 수평 공격 차단 방어로의 변화 필요





# Thank you!

**Copyright © 2016 Symantec Corporation. All rights reserved.** Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.