TREND MICRO

Security
TRENDS 2018

APT 공격 대응을 위한 Connected and Integrated 방어 전략

트렌드마이크로
최영삼 실장

Agenda

TREND MICRO | Security TRENDS 2018

최신 위협 현황

Connected Threat Defense 전략

3rd Party Integration을 통한 대응

기대 효과

고객사례

Agenda

TREND MICRO | Security TRENDS 2018

최신 위협 현황

Connected Threat Defense 전략

3rd Party Integration을 통한 대응

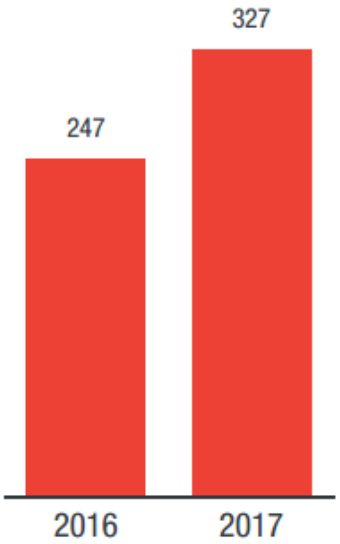
기대 효과

고객사례

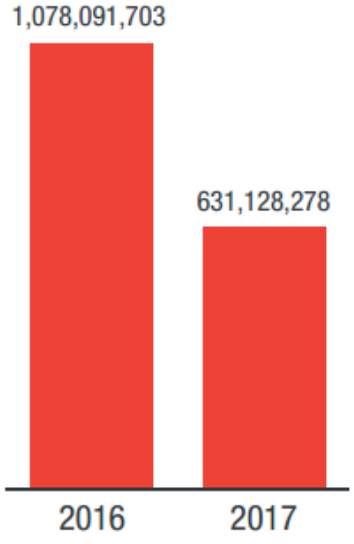
최신 위협 현황

TREND MICRO | Security TRENDS 2018

"랜섬웨어 수는 감소 했지만 패밀리 수는 증가했습니다."



2017년에 더 증가한 랜섬웨어 패밀리 수



새로운 랜섬웨어 패밀리는 증가했지만
주요 랜섬웨어의 수는 감소

Ransomware	Grand Total
LOCKY	82,805
KOVTER	50,390
NEMUCOD	46,276
CERBER	40,788
CRYPTESLA	26,172
CRYPWALL	9,875
CRYPCTB	4,773
CRYSIS	3,493
RANSOM	3,210
WALTRIX	2,998

Ransomware	Grand Total
WANNACRY/WCRY	321,814
CERBER	40,493
LOCKY	29,436
CRYSIS	10,573
SPORA	8,044
CANTIX	6,269
EXMAS	5,810
CRYPTESLA	4,608
CRYPTLOCK	3,007
ZERBER	2,691

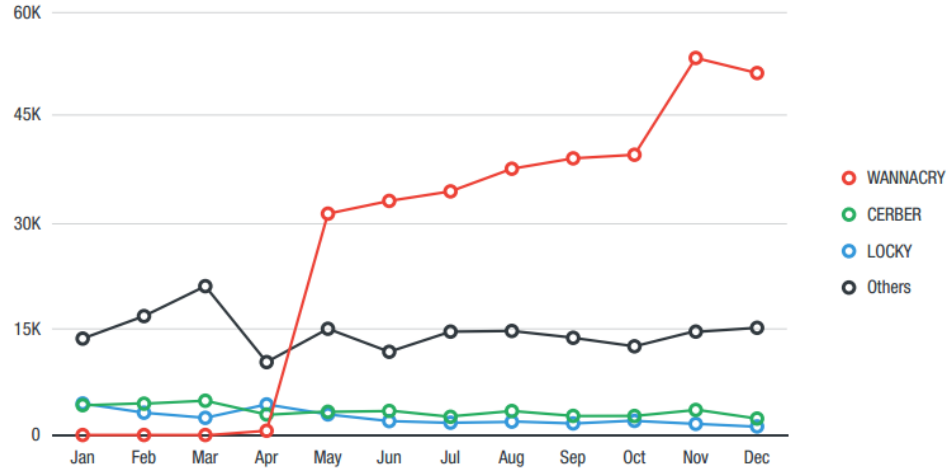
상위 랜섬웨어 패밀리

Source : TrendLabs 2017 Annual Security Roundup

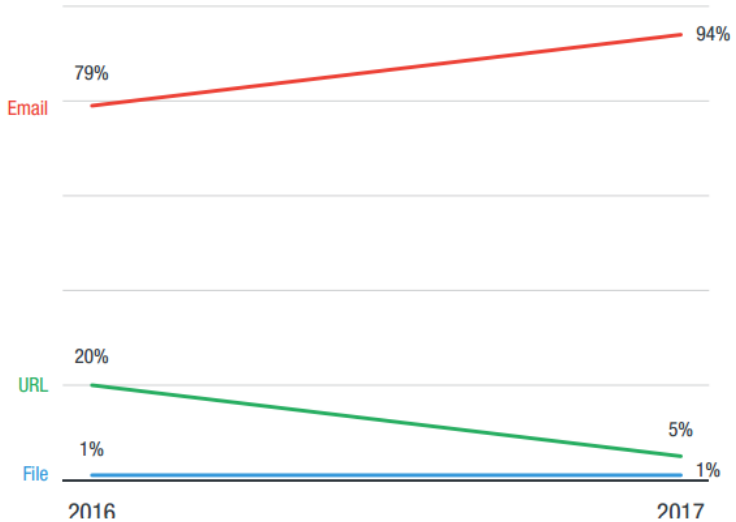
최신 위협 현황

TREND MICRO | Security TRENDS 2018

"새로운 방식의 랜섬웨어 증가, 여전히 사용되는 이메일 방식"



2017년 급성장한 WannaCry

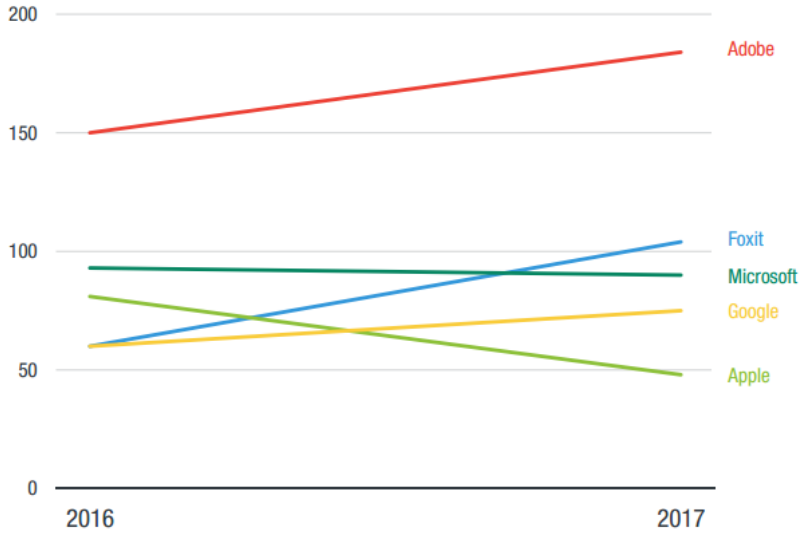


랜섬웨어의 시대에도 여전히 사용되는 이메일 방식

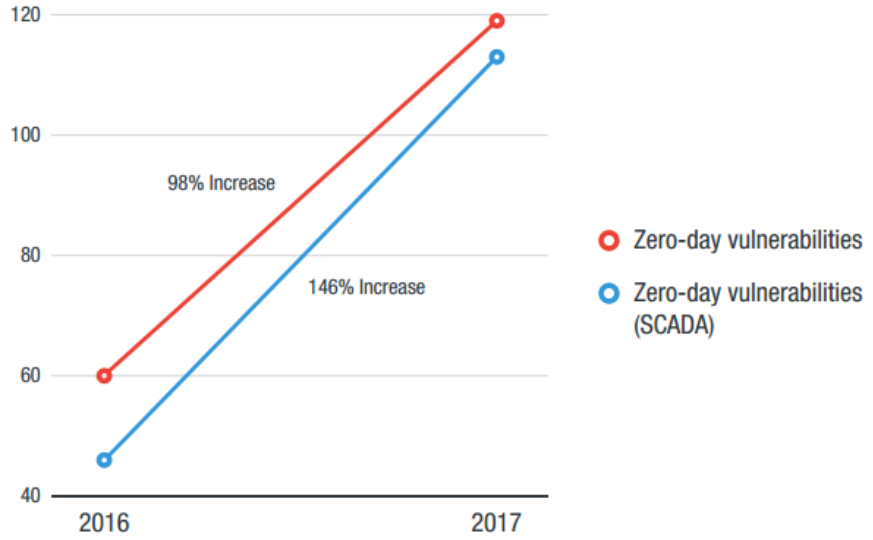
Source : TrendLabs 2017 Annual Security Roundup

최신 위협 현황

"적응형 위협들이 기존의 취약점을 새로운 방식으로 악용"



2016년과 2017년 업체 별 탐지된 취약점 수



제로데이 취약점의 급격한 증가
2016년과 2017년에 발견된 제로데이 취약점과 SCADA 관련 제로데이 취약점의 수

Source : TrendLabs 2017 Annual Security Roundup

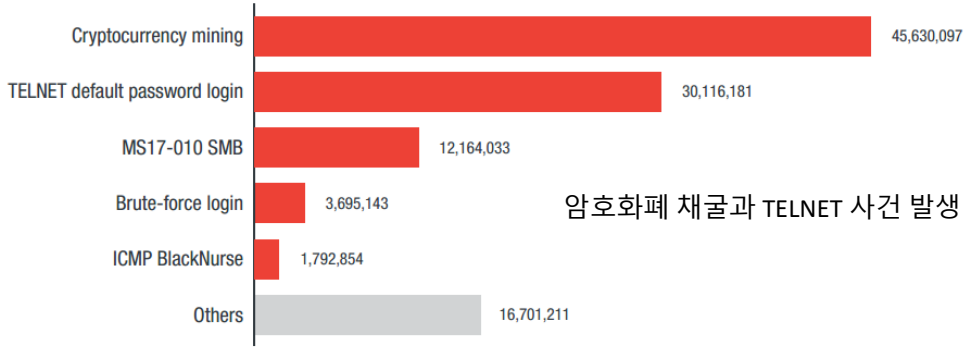
최신 위협 현황

TREND MICRO | Security TRENDS 2018

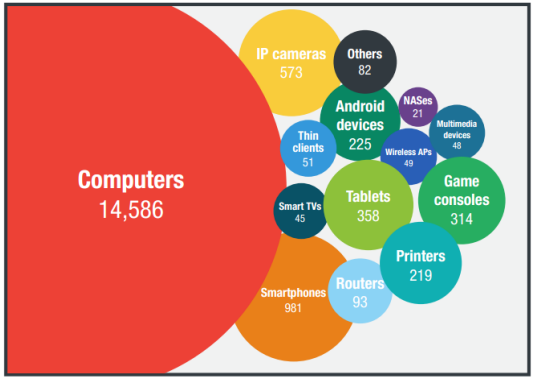
"암호화폐의 급성장으로 새로운 멀웨어와 위협들이 양산"

다양한 암호화폐 공격 방식 (2017)

"네트워크화된 IoT 기기들의 처리능력 악용"



암호화폐 채굴과 TELNET 사건 발생 횟수



암호화폐 채굴 활동이 탐지된 기기들 (2017)

Source : TrendLabs 2017 Annual Security Roundup

Agenda

TREND MICRO | Security TRENDS 2018

최신 위협 현황

Connected Threat Defense 전략

3rd Party Integration을 통한 대응

기대 효과

고객사례

APT 방어 플랫폼 - Deep Discovery

TREND MICRO | Security TRENDS 2018

Deep Discovery Inspector - DDI

APT 탐지

네트워크 미러링 방식의 악성 사이트 접속, 악성코드 다운로드, C&C 통신 및 악성 행위 탐지

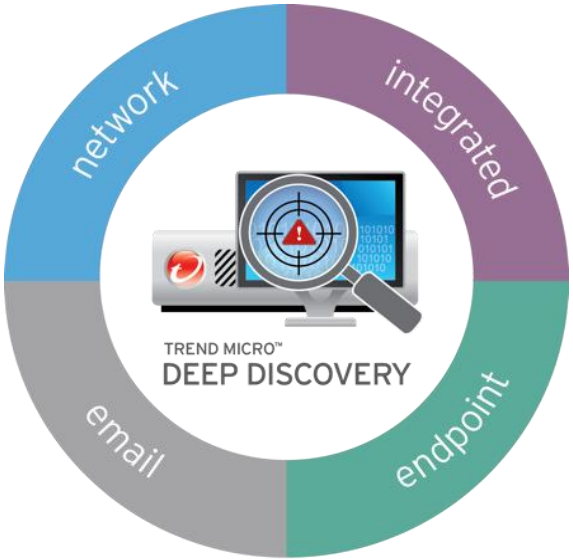
(모델 : DDI510/1100/4100)

Deep Discovery Email Inspector - DDEI

Email APT 차단

이메일에 첨부된 악성 첨부파일과 URL을 탐지, 분석, 차단하는 Email APT 전용 솔루션

(모델 : DDEI7100/9100)



Deep Discovery Analyzer - DDAN

APT 분석

알려지지 않은 신종/변종 악성코드에 대한 행위 분석 - Sandbox 분석 전용

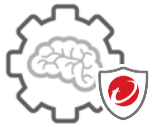
(모델 : DDAN1100)

OfficeScan Agent (Endpoint Anti-Malware)

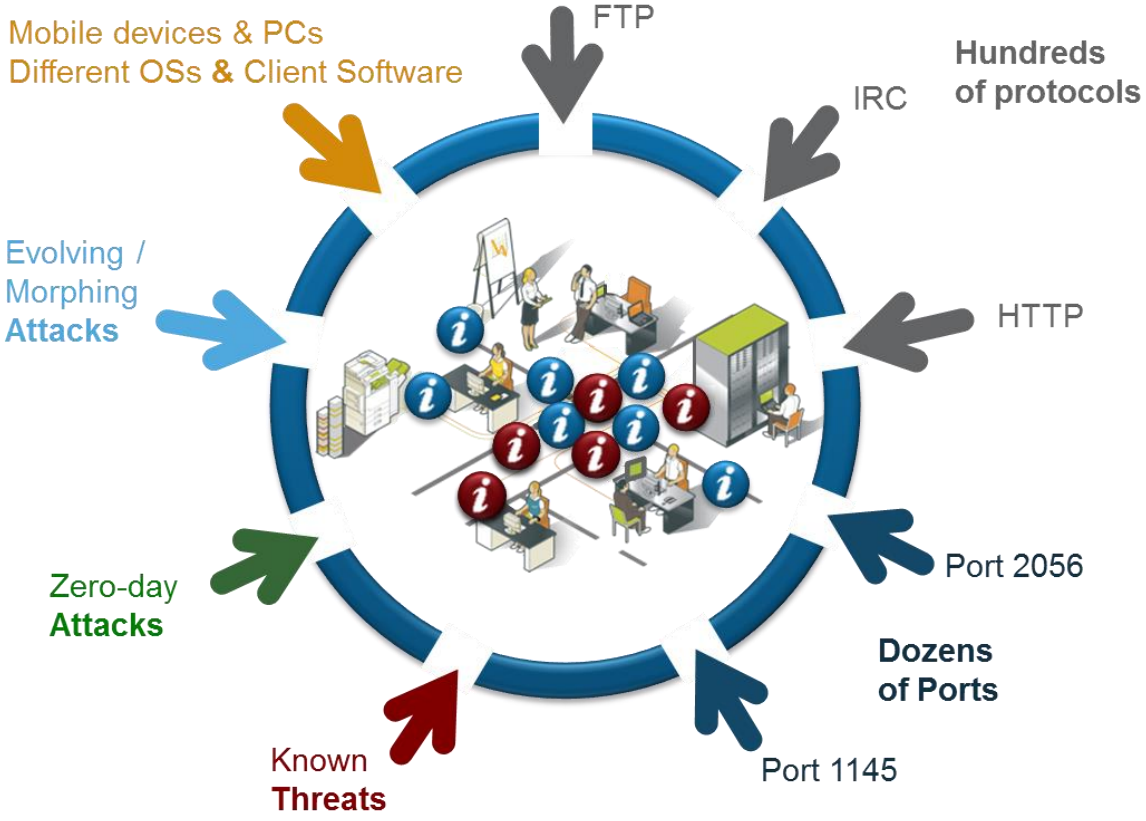
Endpoint 대응

알려진 악성코드 치료, Unknown Malware 격리 및 Endpoint Network 격리

Key Technologies - Unknown 탐지

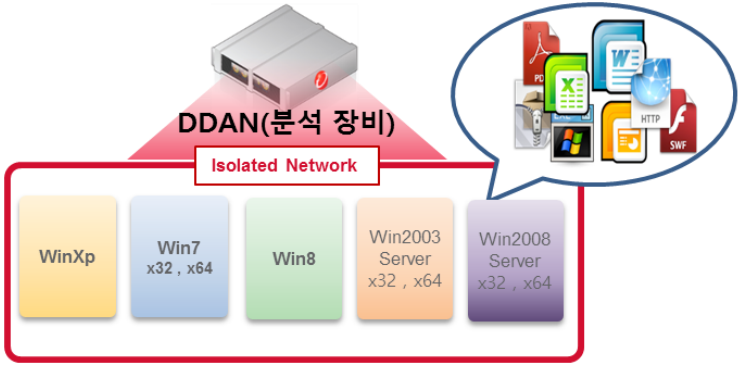
APT 특화 탐지 엔진		Document Exploit(Statistic Analysis) + Known Malware
맞춤형 샌드박스		맞춤형 샌드박스 vs. 일반 샌드박스
머신러닝		클라우드 보안센터의 학습데이터를 이용하는 머신러닝을 통해 신/변종 악성코드 탐지
글로벌 위협 인텔리전스		실시간 클라우드 인텔리전스와 리서치 파워를 활용하여 탐지 정확성 및 엔진 및 룰셋의 지속적인 업데이트
위협정보 연동		샌드박스로 부터 탐지된 IOC를 트렌드마이크로 제품 및 3rd Party 제품과 실시간 공유

100+ 프로토콜/어플리케이션 지원



"특정 프로토콜만 지원하는 제품으로는 충분하지 않습니다."

맞춤형 샌드박스(Custom Sandbox)



다양한 OS Sandbox 이미지 구성 가능

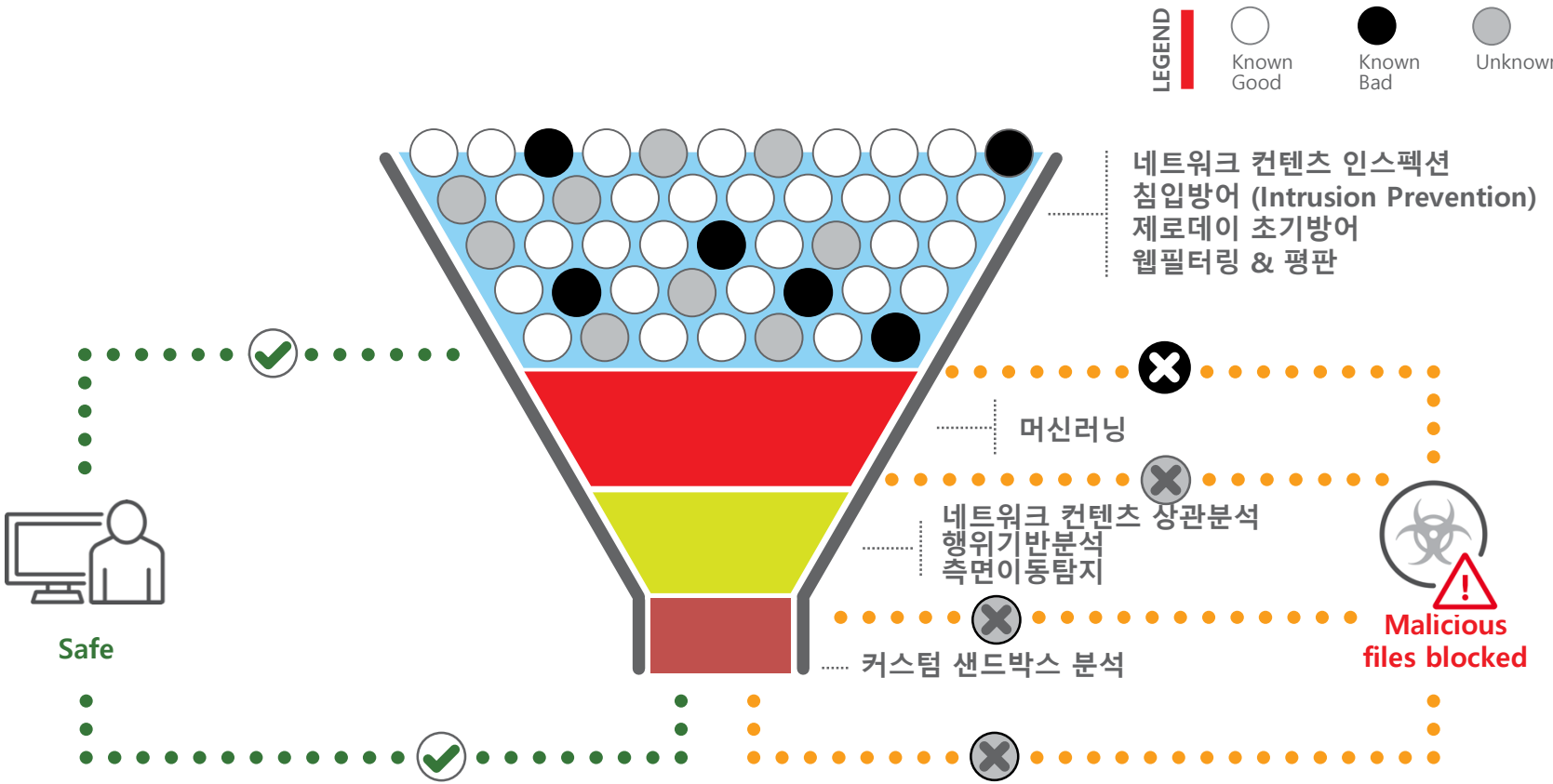
맞춤형 Sandbox

- **60개 샌드박스** 동시 분석 가능
- 사용자 정의 VM Image
- 가상분석 회피 탐지 및 대응 기술
- 코드실행, 문서파일 & URL 검증
- CloudSandbox 기능을 통해 MacOS지원
- 지원OS종류: WinXp, Win7, Win8, Win8.1, Widows10, Win2003, Win2008, Win2012 Server 지원

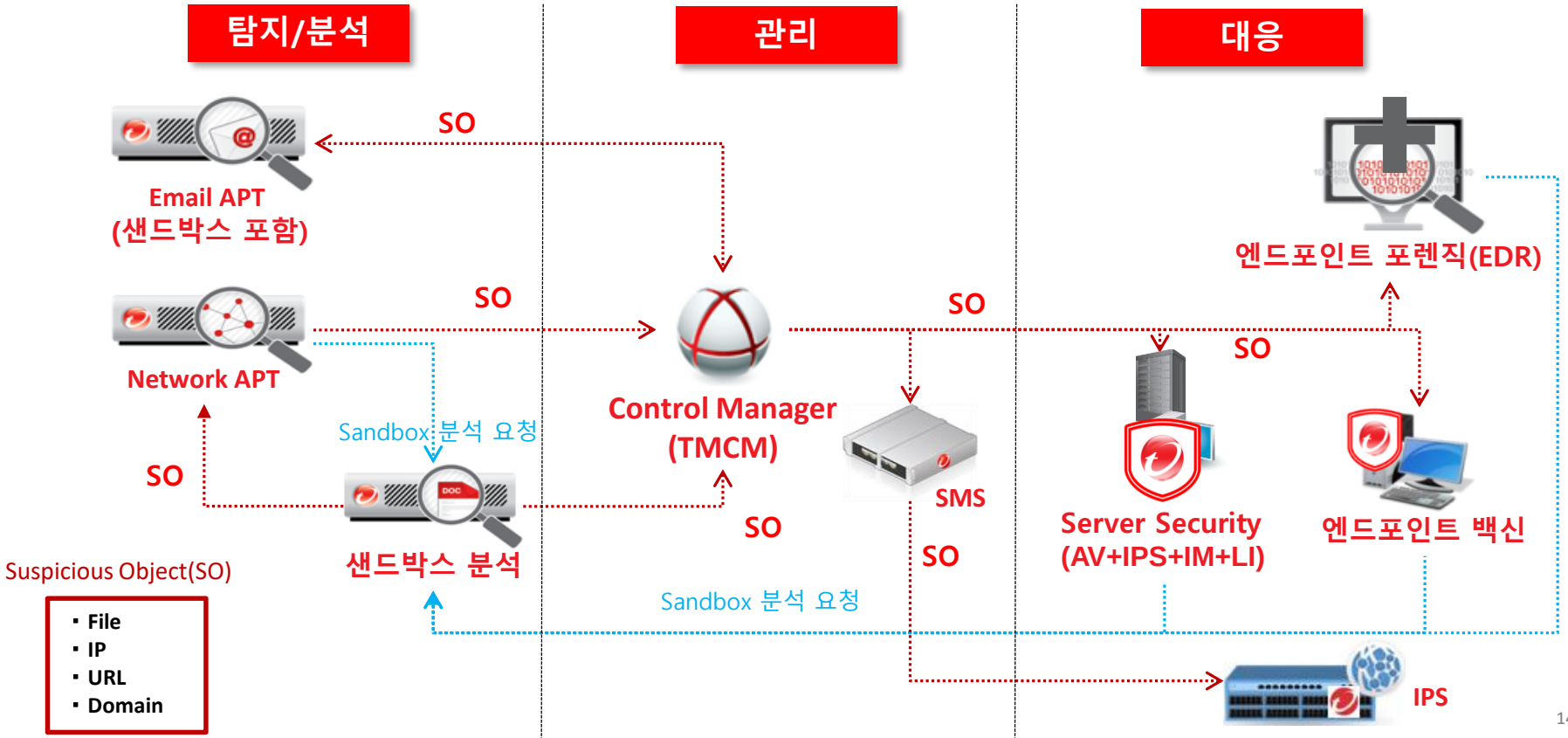
최대 3가지 타입의 Sandbox를 동시에 운영 가능

표적형 공격 대응에는 "맞춤형 샌드박스"가 효과적입니다.

Machine Learning Powered by XGen



Connected Threat Defense 개요



Connected Threat Defense 개요

Deep Discovery에서 의심스런 파일의 정보를 취득하고,
트렌드마이크로 전 제품과의 연계를 통해 미지의 위협에 대해 검출에서 방어까지 수행하는 “원스톱 솔루션”

Goal

- Network + Email + Endpoint 구간 연계 위협 탐지 공유
- 샌드박스/머신러닝/행위기반의 Unknown 위협 탐지
- 공식 패턴 없이 자동 방어

Suspicious Object (SO)

Suspicious Object (SO : 의심스러운 객체) 란? **Sandbox분석 결과「High RISK」**로 판단된 파일로 부터 취득한 정보가 기재되어 있는 위협 데이터로서, 의심스러운 파일의 해쉬값, 접속URL, IP주소, 도메인 정보가 해당됩니다.

Sandbox Analysis

Suspicious Objects

Suspicious objects are known or potentially malicious IP addresses, domains, URLs, and SHA-1 values found during sample analysis, obtained by managed products from Virtual Analyzer. Objects in the exc considered safe and are not added to the suspicious objects list.

Virtual Analyzer Feedback | Exceptions

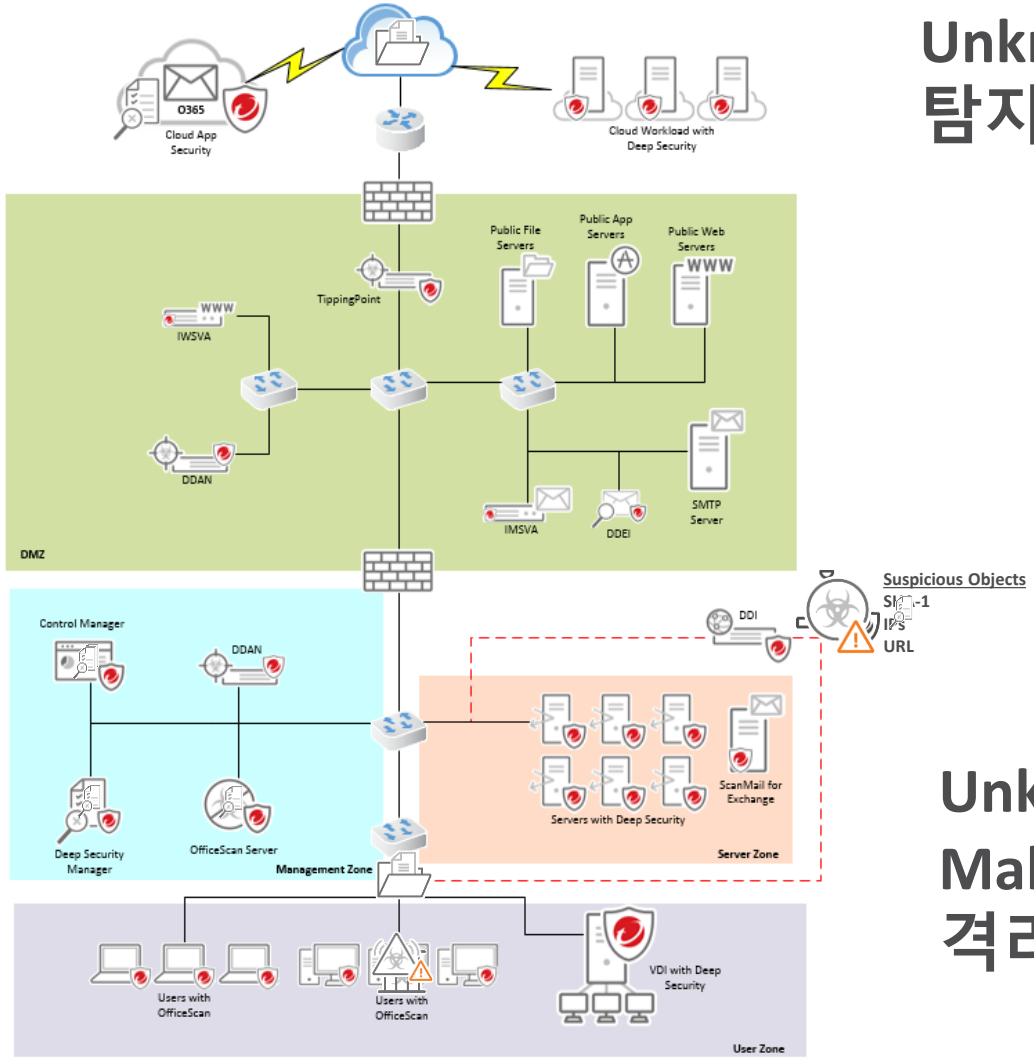
View: All

Export All | Add to Exception | Never Expire | Expire Now | Configure Scan Action | Assess Impact

Virtual Analyzer Feedback Entity	Severity	Type	Expiration	At Risk Endpoints	Scan Action
http://103.25.60.74	Medium	URL	04/22/2015 02:17:50	Not yet assessed	Log
95052B10607210C6C3CC74DE80AE867D3E6E4F65	High	File	04/22/2015 02:17:50	Not yet assessed	Log
http://103.25.60.74/%7Ezadmin/mach/DNS.bin	Medium	URL	04/22/2015 02:17:50	Not yet assessed	Log
robruprod.com	Medium	Domain	04/22/2015 02:15:44	Not yet assessed	Defined by Product
1A7902623E1399B1571D7634D60FF30833F8909C	High	File	04/22/2015 02:15:44	Not yet assessed	Log

IOC 정보는 다양한 보안 솔루션에 공유됩니다.

Unknown 멀웨어 탐지



C&C 콜백 시도 또한 차단됩니다.

Unknown Malware는 격리됩니다.

Deep Discovery + TippingPoint

Unknown & Undisclosed & Known

Deep Discovery: APT 대응 솔루션	**TippingPoint:** 차세대 위협 차단 시스템	
UNKNOWN	**KNOWN**	**UNDISCLOSED**
		

Agenda

TREND MICRO | Security TRENDS 2018

최신 위협 현황

Connected Threat Defense 전략

3rd Party Integration을 통한 대응

기대 효과

고객사례

Ecosystem

Deep Discovery

Analysis

Network Capture

SMTP Relay

WEB API

Log Correlation

3rd party SIEM (CEF/LEEF)

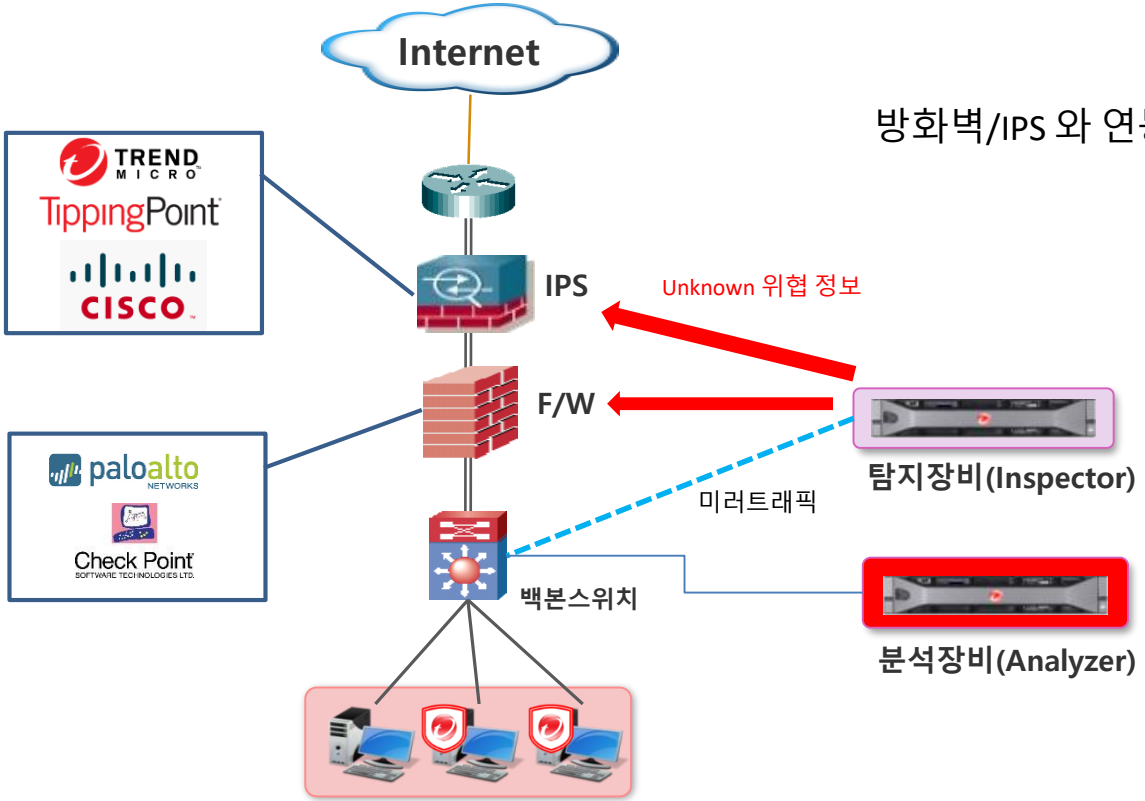
3rd Party Blocking

Threat Profiles

Notable Characteristics

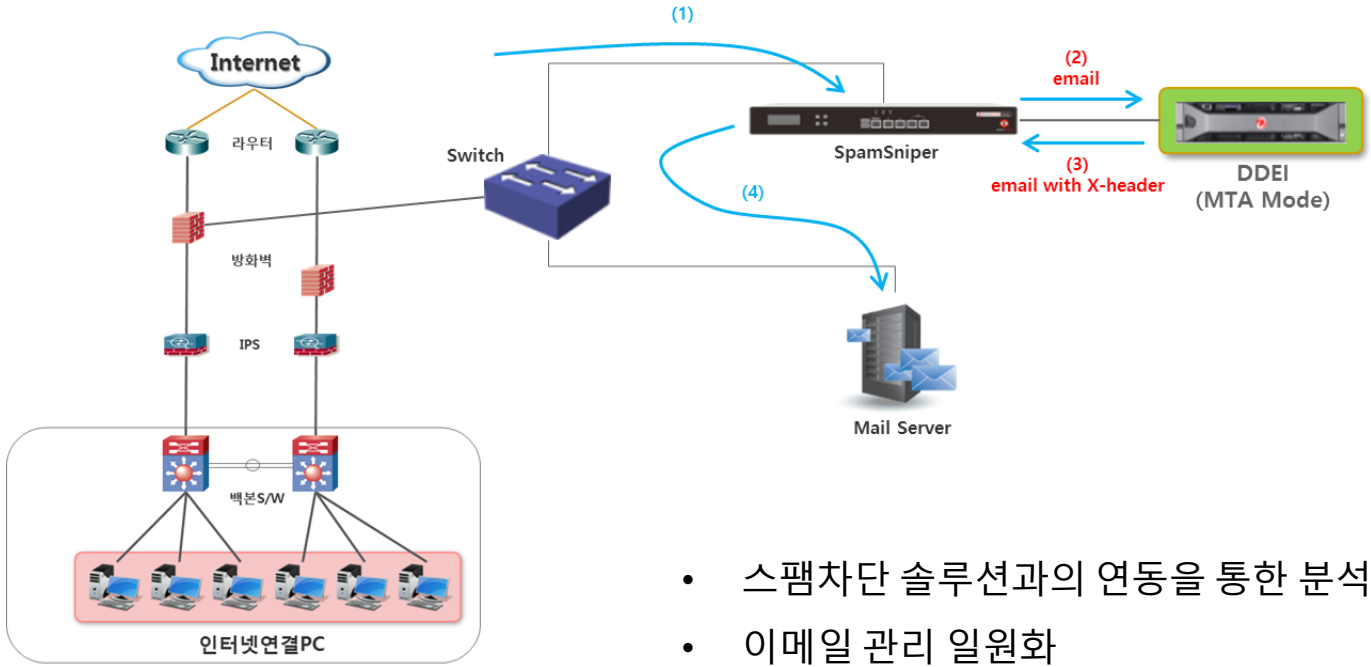
Network packet

Deep Discovery + FW/IPS



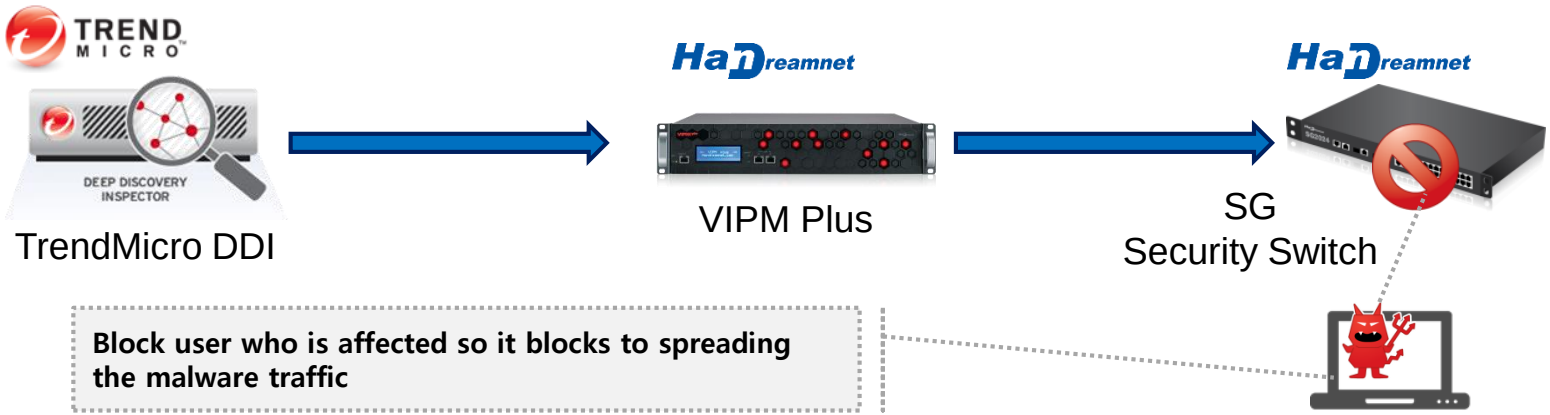
방화벽/IPS 와 연동하여 차단 대상 위협 정보 제공

Deep Discovery + Anti-Spam



- 스팸차단 솔루션과의 연동을 통한 분석 결과 제공
- 이메일 관리 일원화

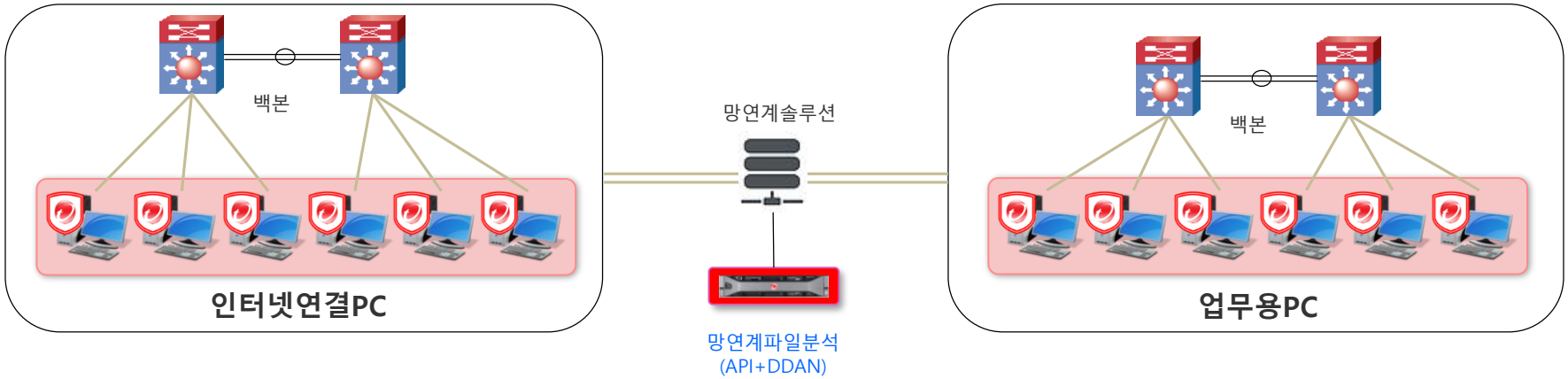
Deep Discovery + 보안스위치



감염된 엔드포인트 격리를 통한 위협 확산 방지

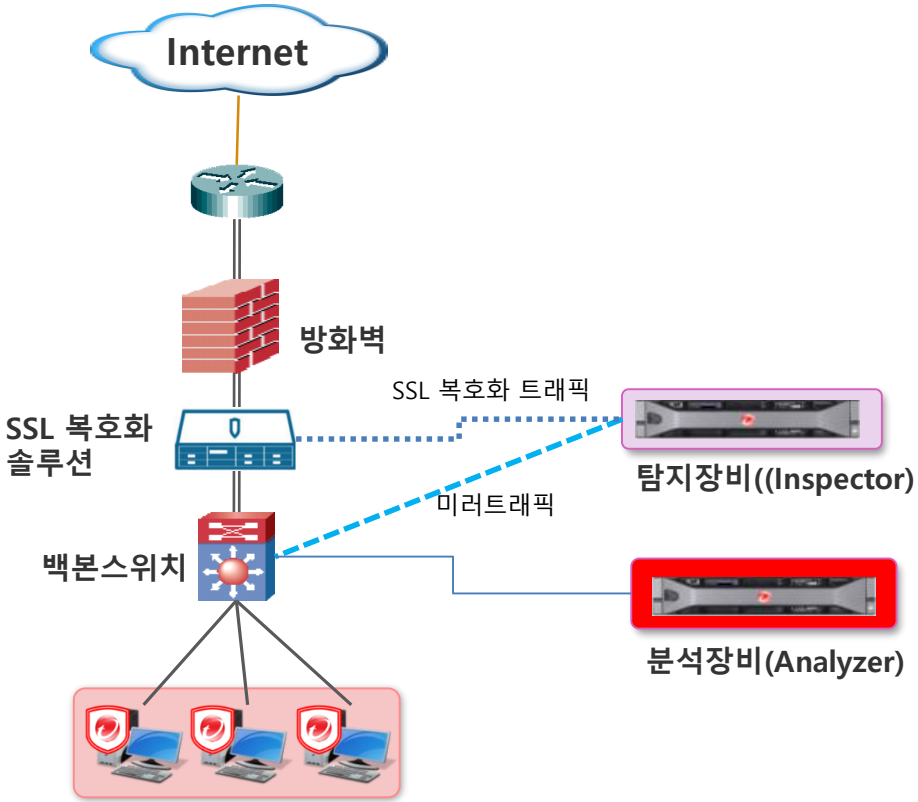
Deep Discovery + 망연계솔루션

망연계 솔루션 연동을 통한 Unknown 멀웨어 내부 유입 차단



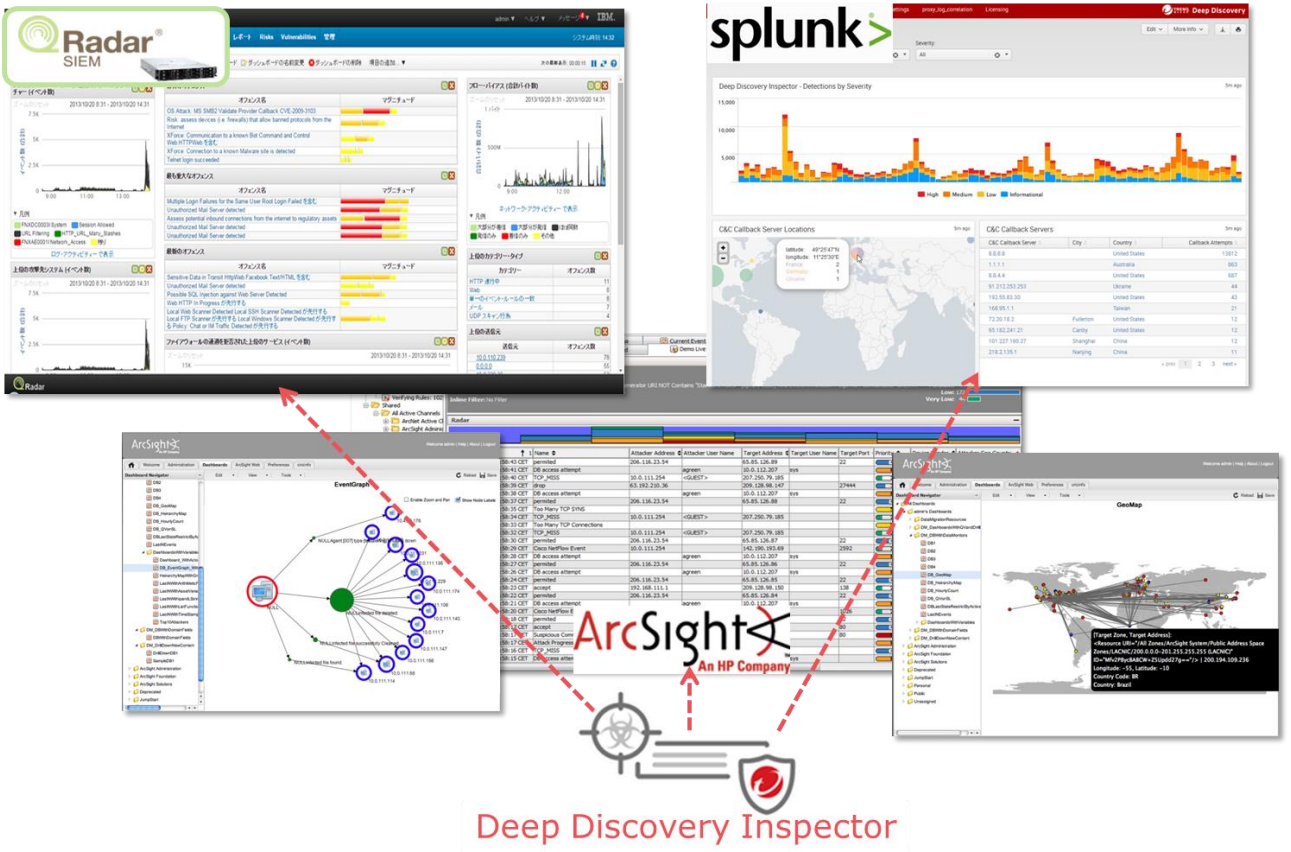
- 외부망 -> 내부망 파일 전송 시 샌드박스 분석
- 공유폴더 방식 지원
- APT 분석장비(샌드박스) API 연동

Deep Discovery + SSL Decryptor



- SSL 트래픽에 대한 가시성 확보
- SSL 트래픽으로 부터 파일 추출
- TippingPoint TX (Inbound SSL 지원)
- TippingPoint TX(Outboud SSL 예정)

Deep Discovery + SIEM



IOC 공유

Agenda

Security TRENDS 2018

최신 위협 현황

Connected Threat Defense 전략

3rd Party Integration을 통한 대응

기대 효과

고객사례

차세대 Security 운용 과제

- 멀웨어 검출 시 이를 위한 **분석 인력 운용** 필요
- **포인트솔루션**으로 모든 위협에 대응하기 어려움
- 차세대 Security는 **과탐지**가 발생하기 때문에, 완전한 자동화가 어려움
- **사람 의존 요소**가 강하며, 표준적인 운용이 어려움
- 사태의 종식은 Security 벤더의 **패턴 파일 작성**에 의존 할 수 밖에 없음
- 최종적으로 패턴 파일에 적용까지 **시간**, **인력**, **비용**이 필요

이 모든 운용 과제를 “제품 간 연계"로 해결

연계를 통한 새로운 대응

TREND MICRO | Security TRENDS 2018

당면 과제		해결 포인트	트렌드마이크로 제품	새로운 대응 절차	종래의 대응
미지의 위협에 대한 파악이 어려움	가시화	미지의 위협 검출	Deep Discovery Inspector/ Analyzer/ Email Inspector	발견	미지의 위협 검출
위협의 특정/분석과 대처에 시간이 소요	자동화	커스텀시그니처의 자동 제작과 엔드포인트까지 자동 배포		분석 및 작성	Trend Labs 파일분석
보안 관리자의 대응 시간이 필요 (업무부하의 원인)	자동화		Trend Micro Control Manager	배포	패턴파일 작성 및 배포
시간이 걸려 피해 확산의 원인	최소화	미지의 위협에 신속히 탐지, 차단, 격리 처리	Office Scan / Deep Security / TippingPoint	대응	패턴파일 적용

Agenda

최신 위협 현황

Connected Threat Defense 전략

3rd Party Integration을 통한 대응

기대 효과

고객사례

Security TRENDS 2018

THANK YOU

트렌드마이크로
최영삼 (sam_choi@trendmicro.co.kr)