TREND MICRO

Security
TRENDS 2018

Hidden Attack에 대한 선제적 공격대응 방안

트렌드마이크로
장 성 민

Agenda

1. What is your X?
2. Trend Micro XGen!!!
3. Connected Threat Defense!!!

The modern workplace has no boundaries

The threat landscape is evolving

Ransomware

Targeted Attacks

Fileless Malware

Cyptocurrency

Blockchain

Total Visibility

Multi-Layered, Multi-vector,

Hidden attacks!!!

Powered by XGen™

XGen™

머신 러닝

정확한 방어시점!!!
최적화된 방어기술!!!

글로벌 위협 인텔리전스

고객의 보안 x에 대한 답을 제공합니다!!

동적 환경

Increasingly sophisticated threats

Shift to the cloud

Changing user behavior

고객의 x

Recovering from high impact attacks

Existing defenses stagnant and ineffective

Complexity & lack of visibility

XGen™ Security

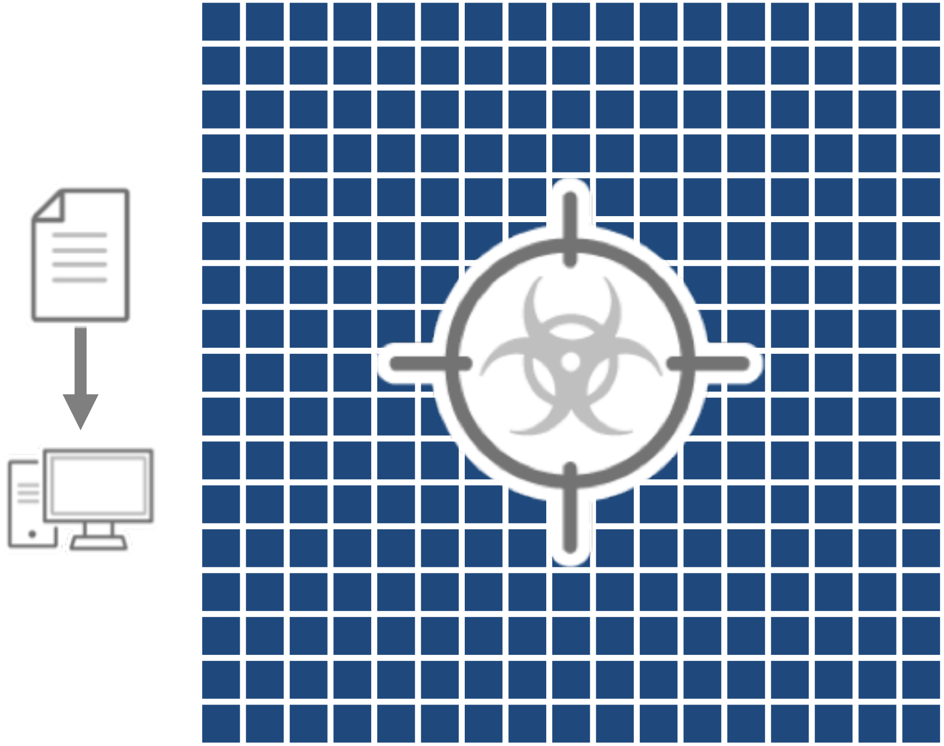
Smart

Optimized

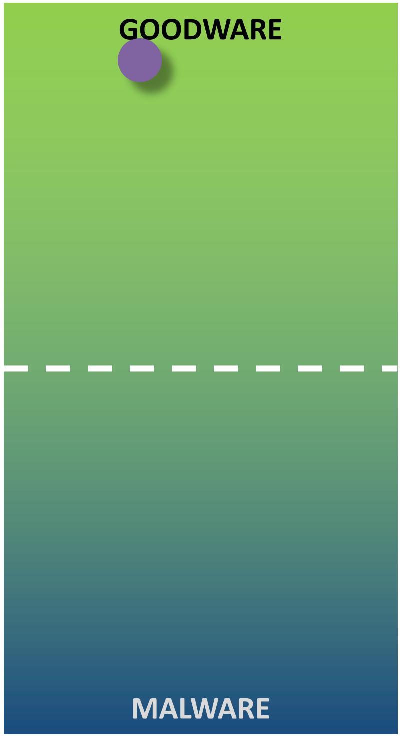
Connected

머신 러닝

머신러닝



Machine Learning Model



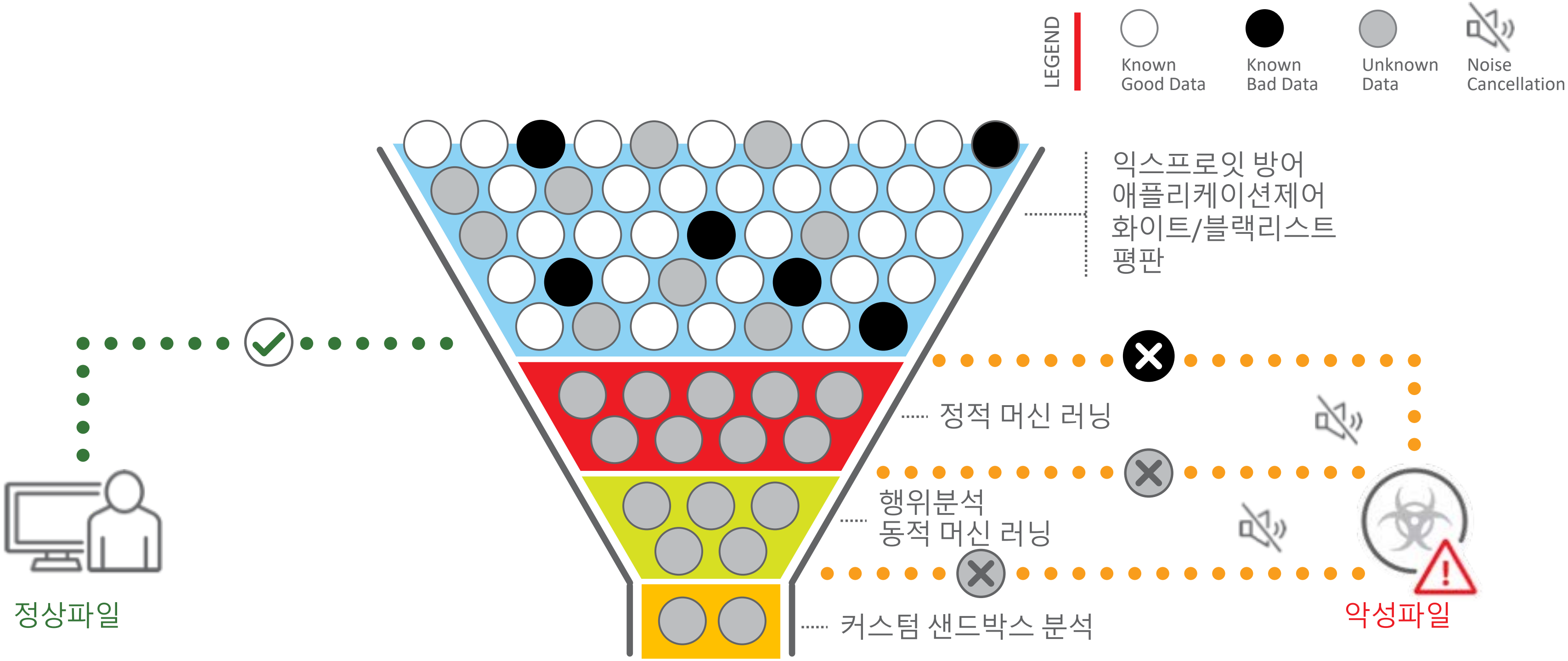
Trend Micro's ML은?

빅데이터기반 인텔리전스

정확한 특징 추출

정적(Pre-Execution) & 동적(Runtime)

정확한 방어시점!! 최적화된 방어기술적용



익스프로잇 방어
애플리케이션제어
화이트/블랙리스트
평판

정적 머신 러닝

행위분석
동적 머신 러닝

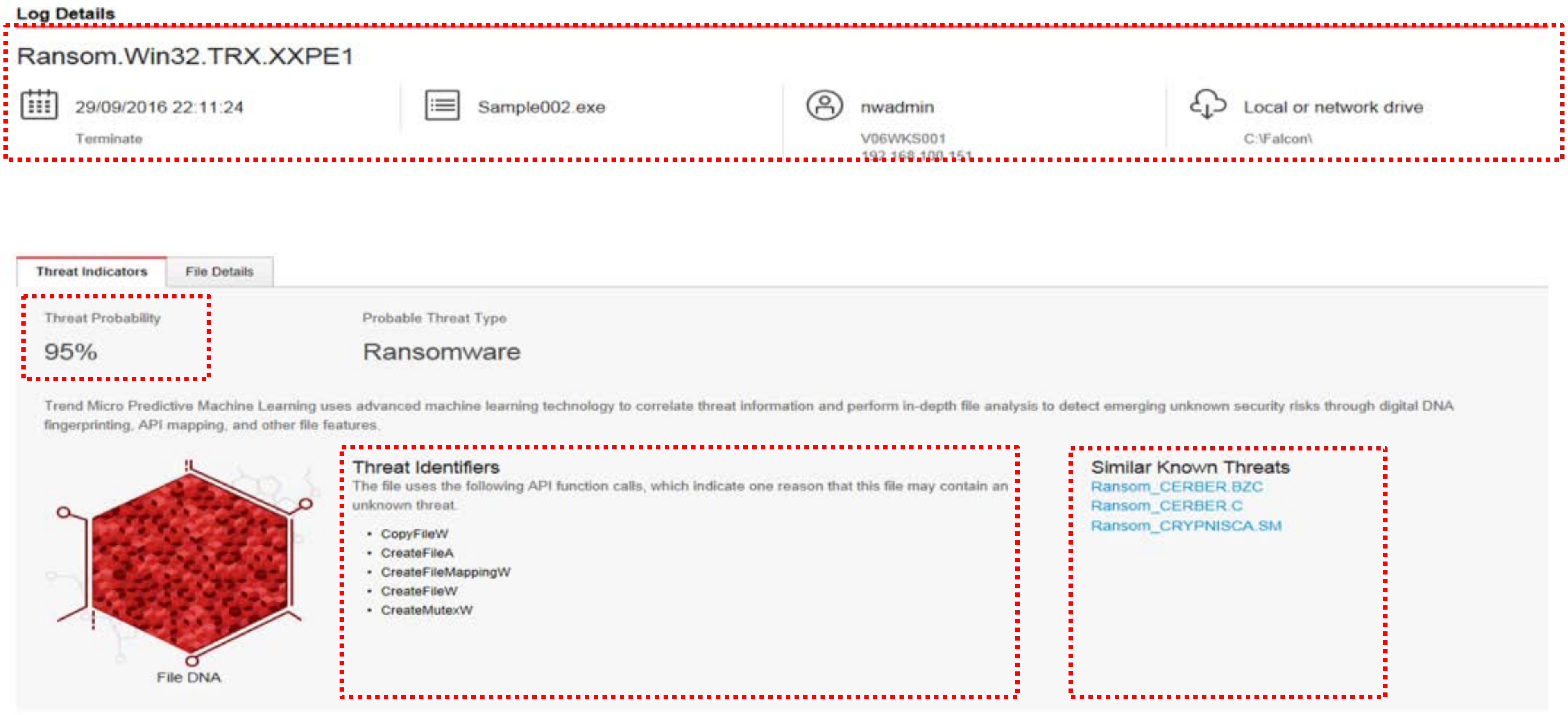
커스텀 샌드박스 분석

정상파일

악성파일

최적 방어 기술!!! 낮은 오탐!!!

머신러닝을 이용한 Unknown Malware 탐지



Log Details

Ransom.Win32.TRX.XXPE1

29/09/2016 22:11:24
Terminate

Sample002.exe

nwadmin
V06WKS001
192.168.100.151

Local or network drive
C:\Falcon\

Threat Probability
95%

Probable Threat Type
Ransomware

Trend Micro Predictive Machine Learning uses advanced machine learning technology to correlate threat information and perform in-depth file analysis to detect emerging unknown security risks through digital DNA fingerprinting, API mapping, and other file features.

Threat Identifiers
The file uses the following API function calls, which indicate one reason that this file may contain an unknown threat.

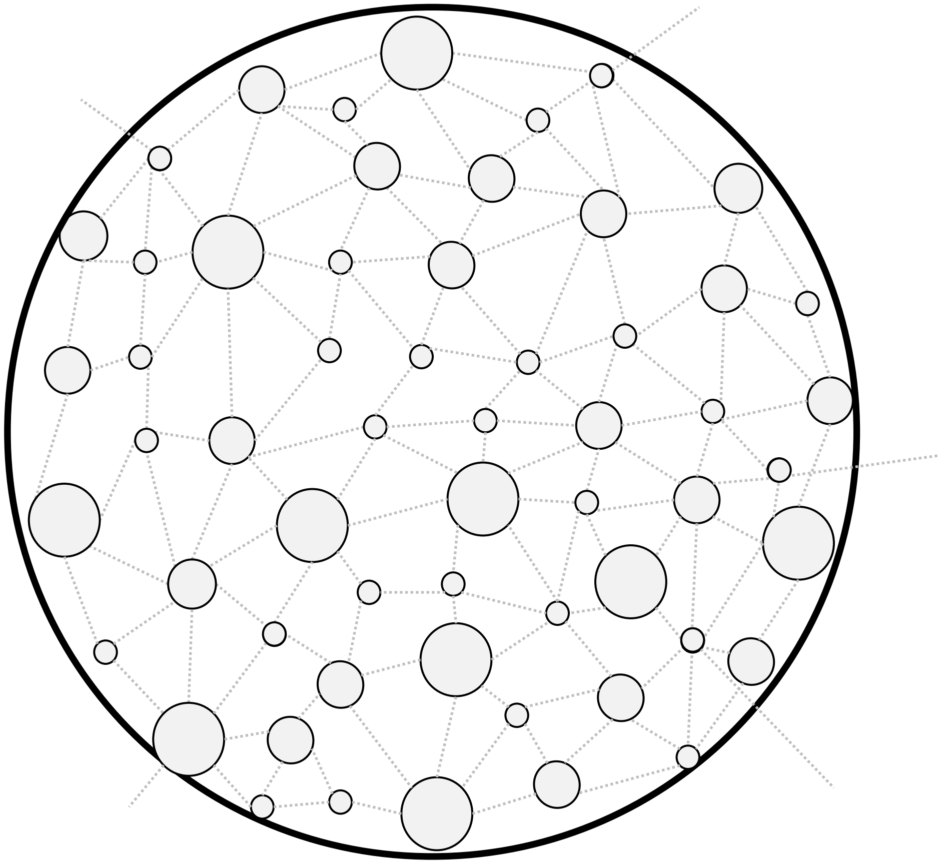
- CopyFileW
- CreateFileA
- CreateFileMappingW
- CreateFileW
- CreateMutexW

Similar Known Threats
Ransom_CERBER.BZC
Ransom_CERBER.C
Ransom_CRYPNISCA.SM

Network Defense

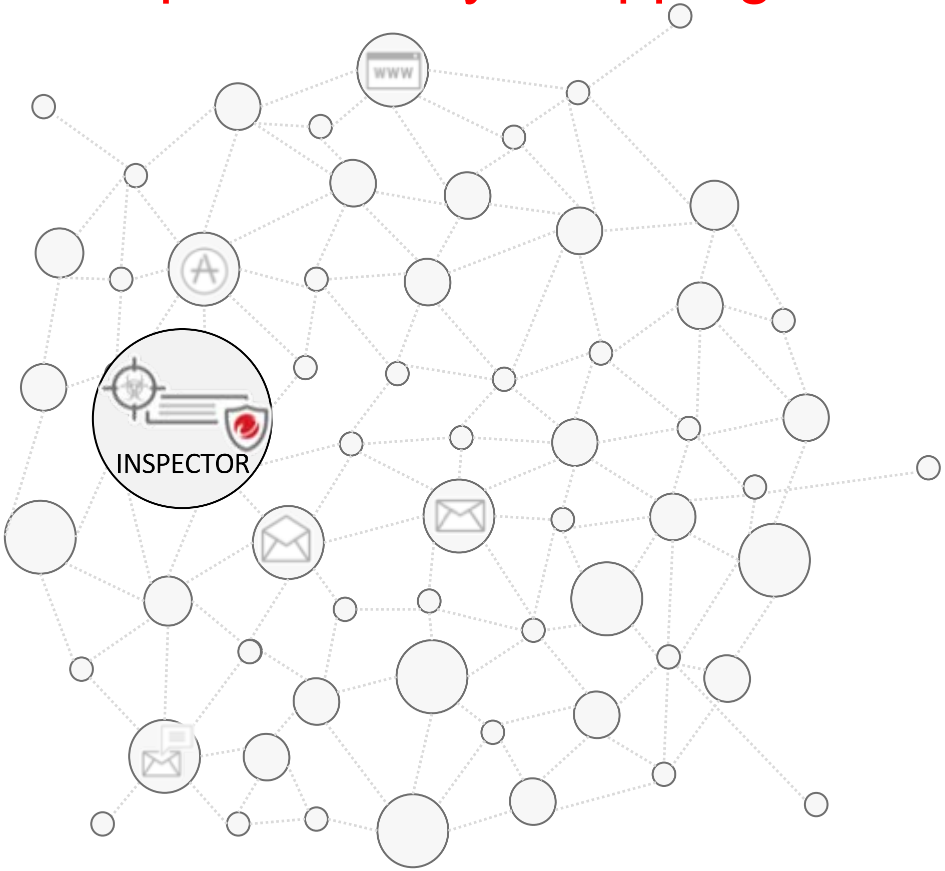
Network Defense

Connected & Multi-Layered Network

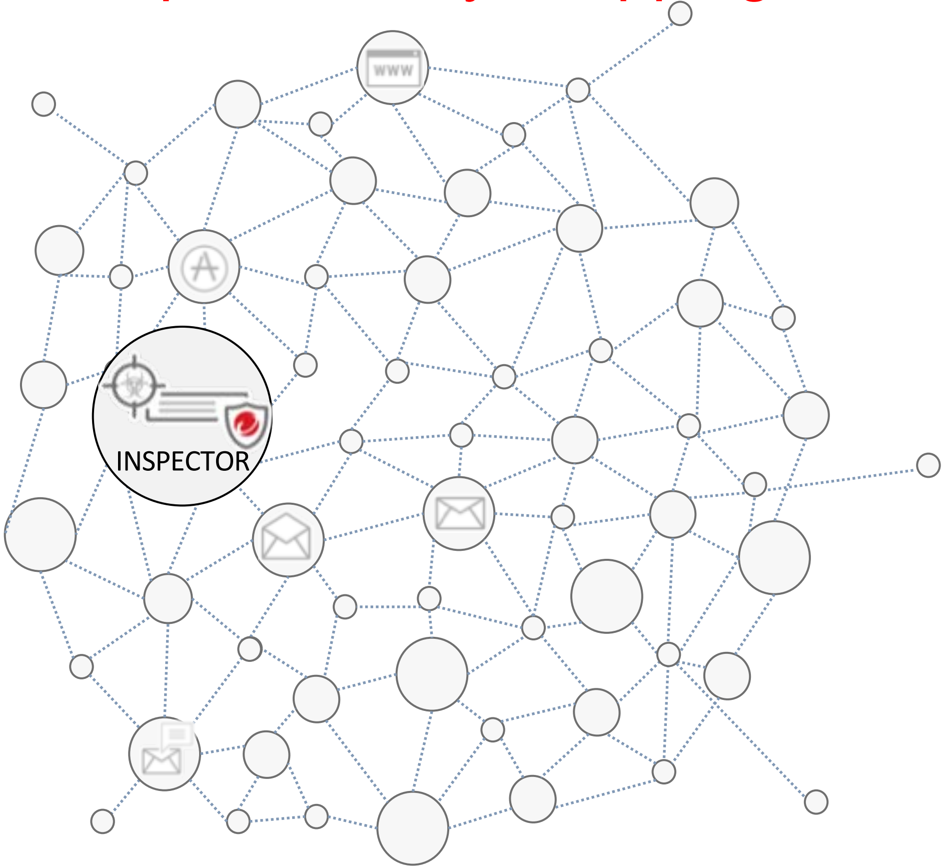


Deep Discovery + TippingPoint

Deep Discovery Inspector



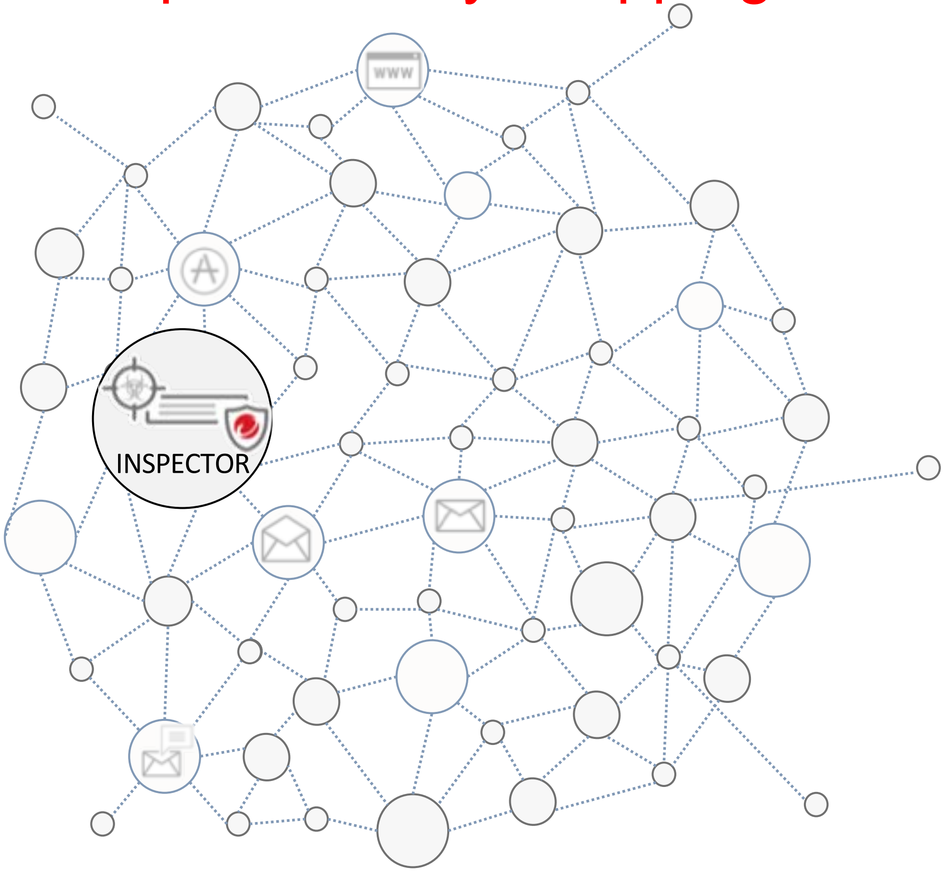
Deep Discovery + TippingPoint



Deep Discovery Inspector

- 모든 통신 포트

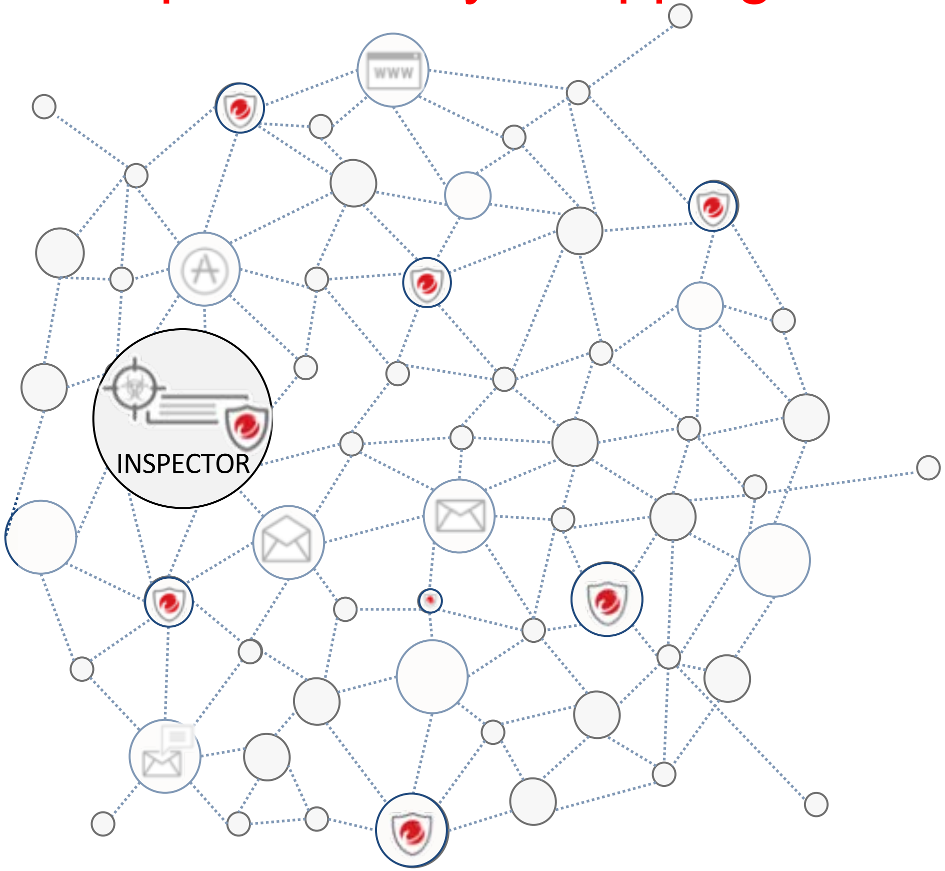
Deep Discovery + TippingPoint



Deep Discovery Inspector

- 모든 통신 포트
- 107개의 통신 프로토콜
- 측면이동(Lateral movement) 탐지

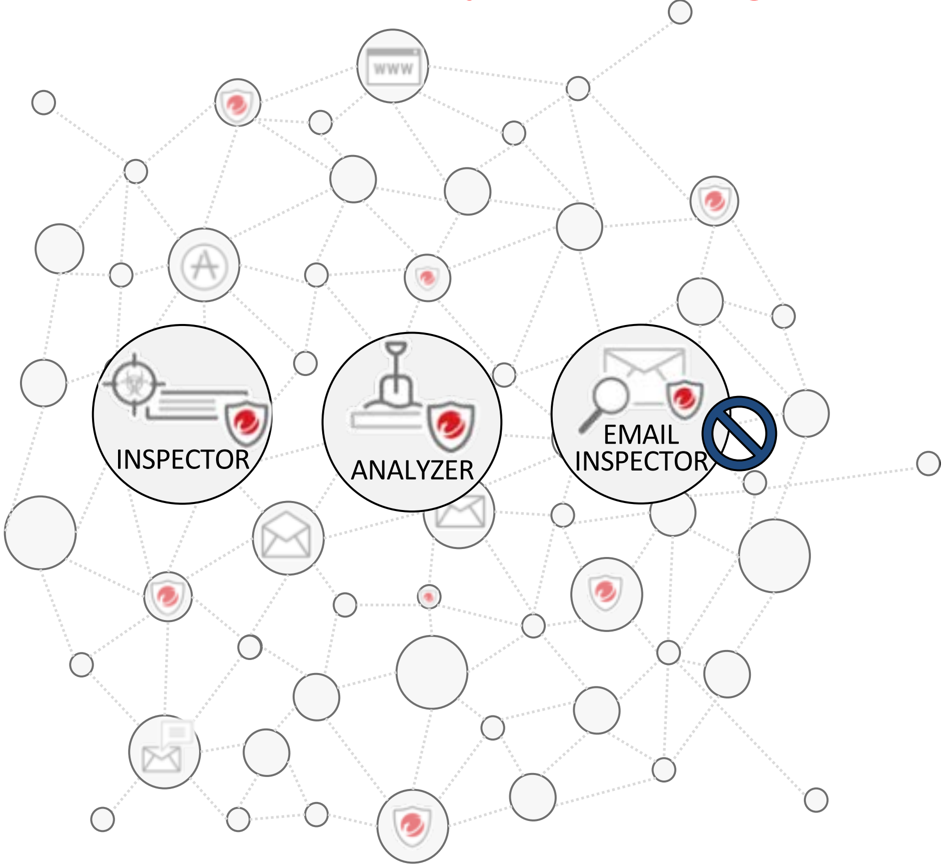
Deep Discovery + TippingPoint



Deep Discovery Inspector

- 모든 통신 포트
- 107개 통신 프로토콜
- 측면이동(Lateral movement) 탐지
- 위협정보 동기화

Deep Discovery + TippingPoint



Deep Discovery Inspector

- 모든 통신 포트
- 107개 통신 프로토콜
- 측면이동(Lateral movement) 탐지
- 새로운 위협정보 동기화

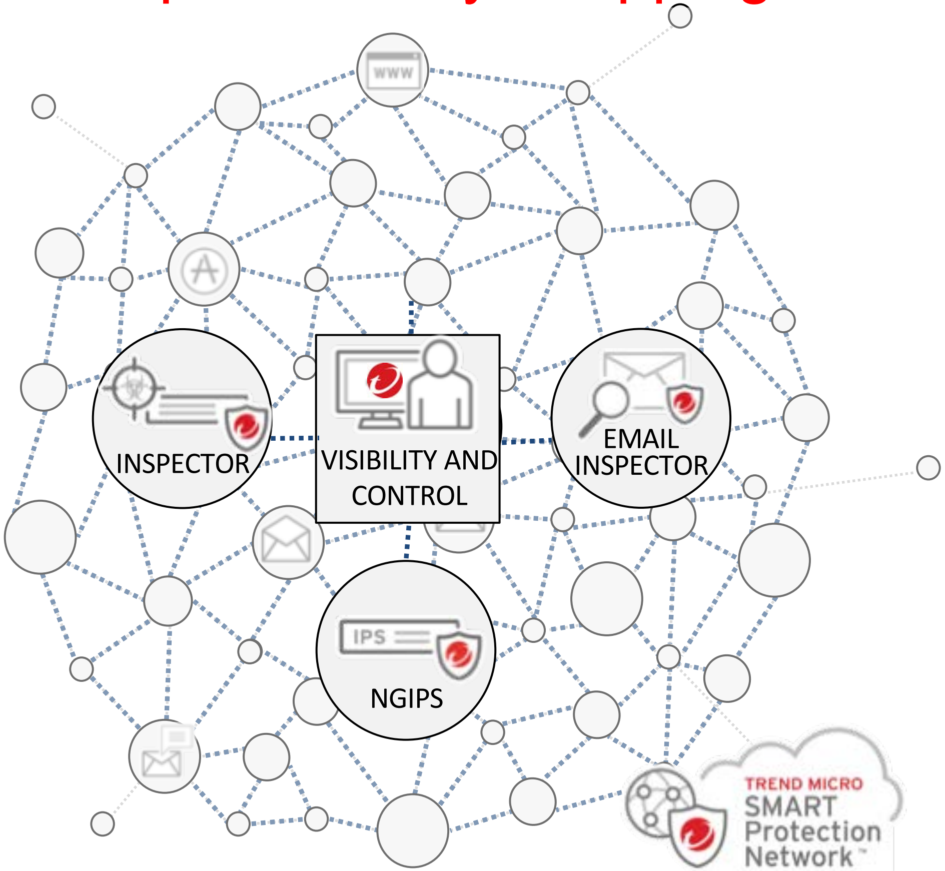
Deep Discovery Email Inspector

- 스피어피싱 메일 대응
- 랜섬웨어 메일 대응

Deep Discovery Analyzer

- 커스텀 샌드박스

Deep Discovery + TippingPoint



Deep Discovery Inspector

- 모든 통신 포트
- 107개 통신 프로토콜
- 측면이동(Lateral movement) 탐지
- 새로운 위협정보 동기화

Deep Discovery Email Inspector

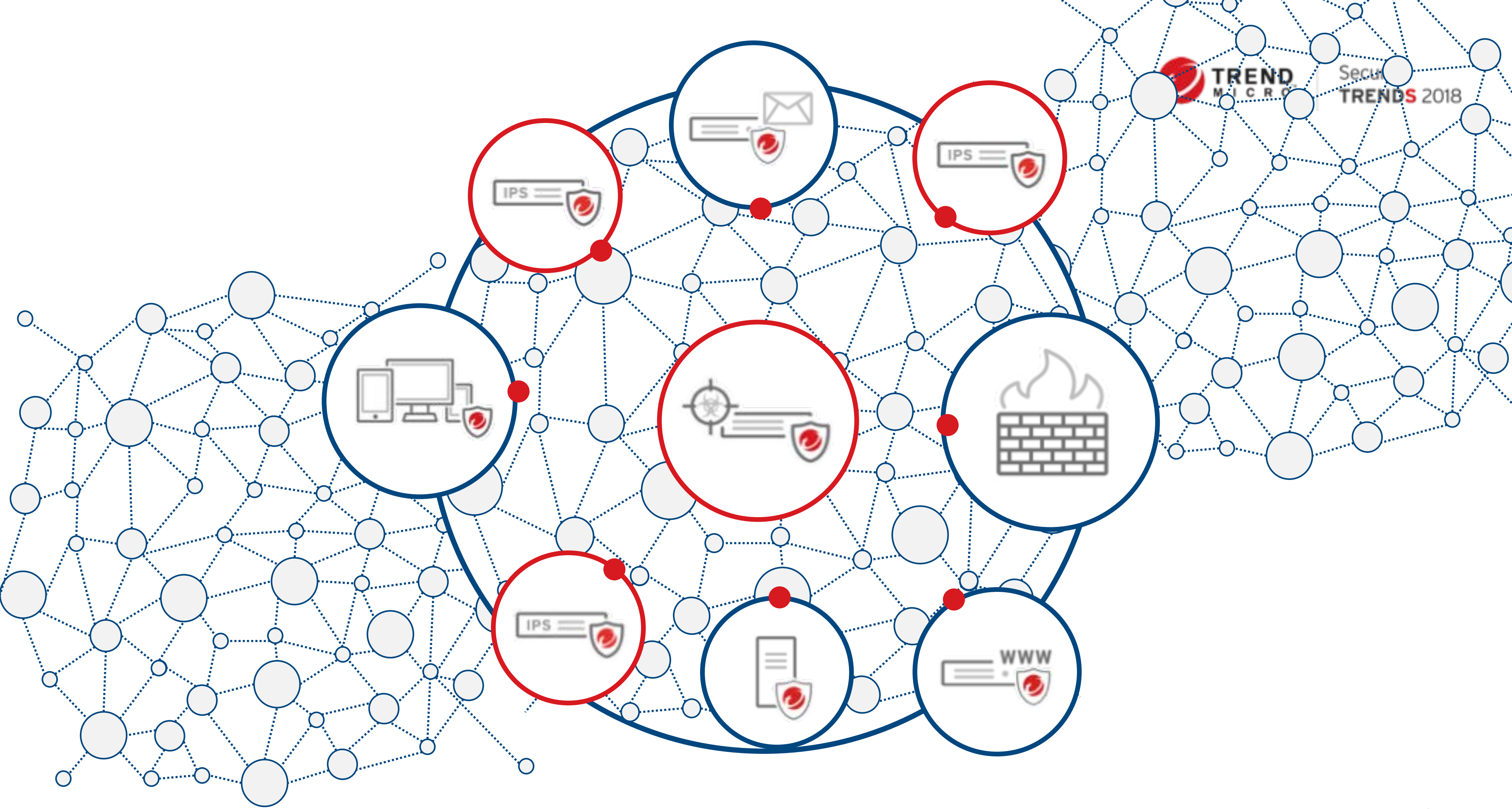
- 스피어피싱 메일 대응
- 랜섬웨어 메일 대응

Deep Discovery Analyzer

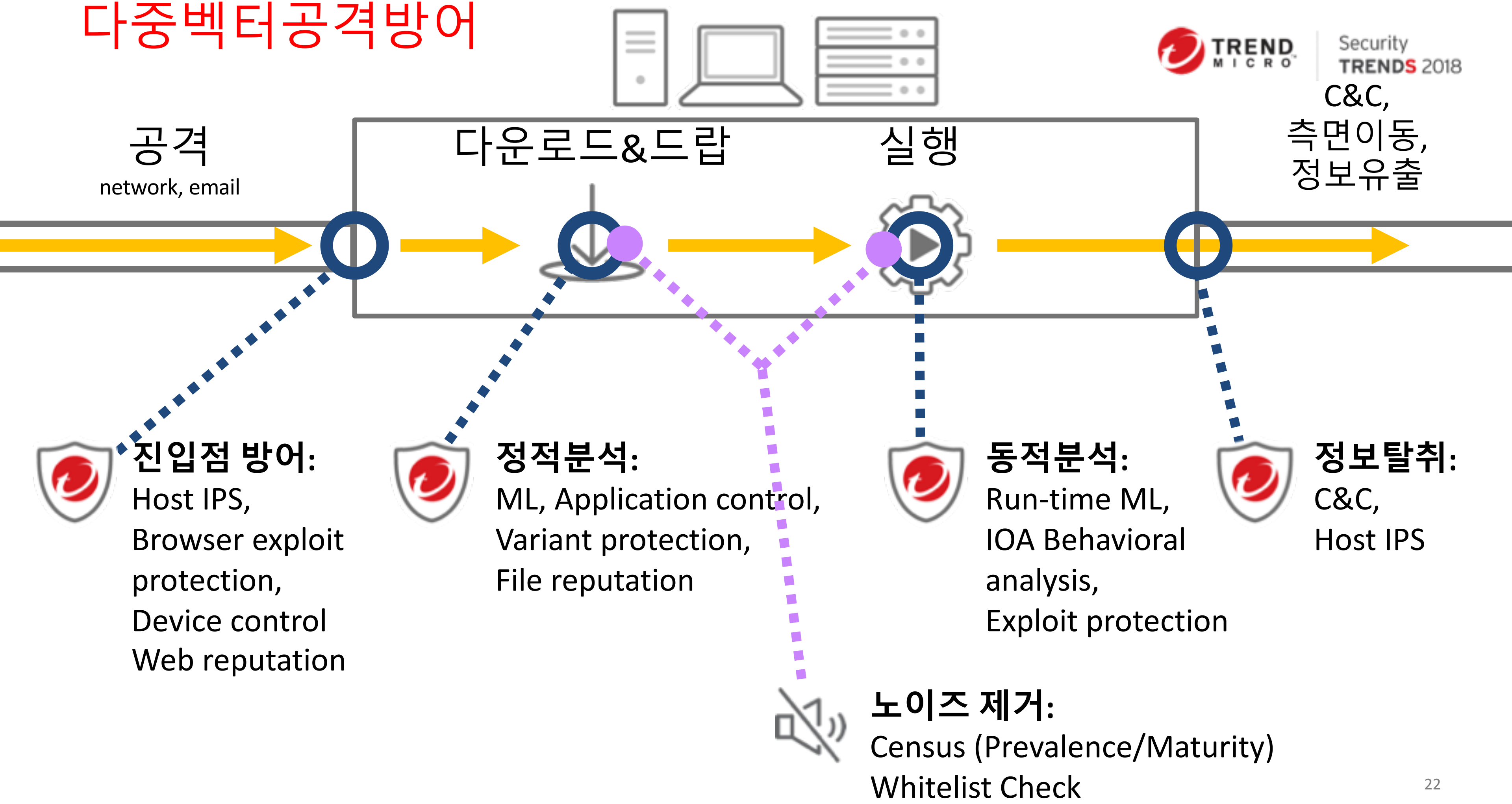
- 커스텀 샌드박스

TippingPoint Next Generation IPS

- 와이어 스피드 위협 방어
- 취약점 대응
- 다양한 네트워크 구성 지원


IPS
IPS
IPS
WWW
Security
TRENDS 2018

다중벡터공격방어



공격
network, email

다운로드&드랍

실행

C&C,
측면이동,
정보유출

진입점 방어:
Host IPS,
Browser exploit protection,
Device control
Web reputation

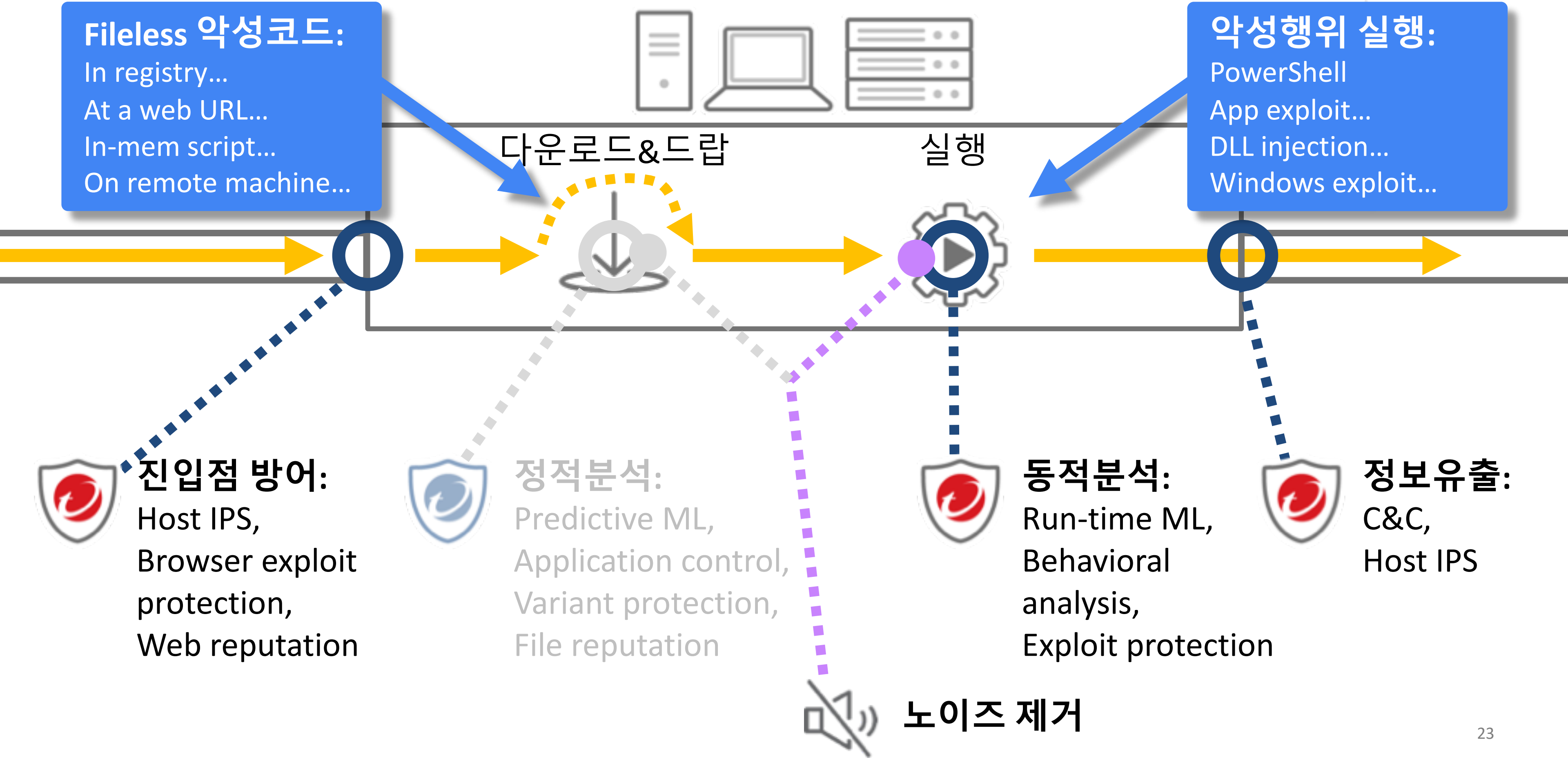
정적분석:
ML, Application control,
Variant protection,
File reputation

동적분석:
Run-time ML,
IOA Behavioral analysis,
Exploit protection

정보탈취:
C&C,
Host IPS

노이즈 제거:
Census (Prevalence/Maturity)
Whitelist Check

다중벡터공격 어(Fileless 악성코드)



Fileless 악성코드:
In registry…
At a web URL…
In-mem script…
On remote machine…

악성행위 실행:
PowerShell
App exploit…
DLL injection…
Windows exploit…

진입점 방어:
Host IPS,
Browser exploit protection,
Web reputation

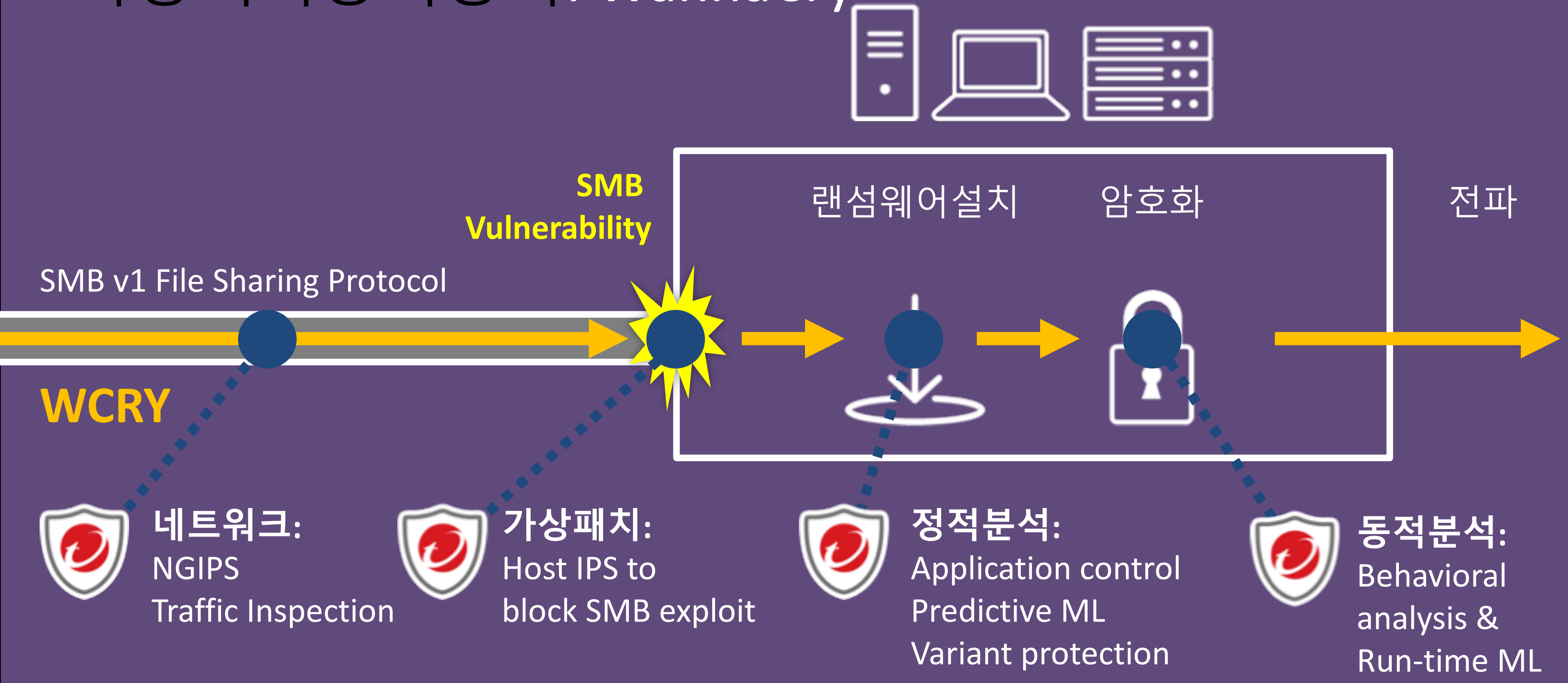
정적분석:
Predictive ML,
Application control,
Variant protection,
File reputation

동적분석:
Run-time ML,
Behavioral analysis,
Exploit protection

정보유출:
C&C,
Host IPS

노이즈 제거

다중벡터공격방어: WannaCry



SMB v1 File Sharing Protocol

SMB Vulnerability

WCRY

랜섬웨어설치

암호화

전파

네트워크:
NGIPS
Traffic Inspection

가상패치:
Host IPS to
block SMB exploit

정적분석:
Application control
Predictive ML
Variant protection

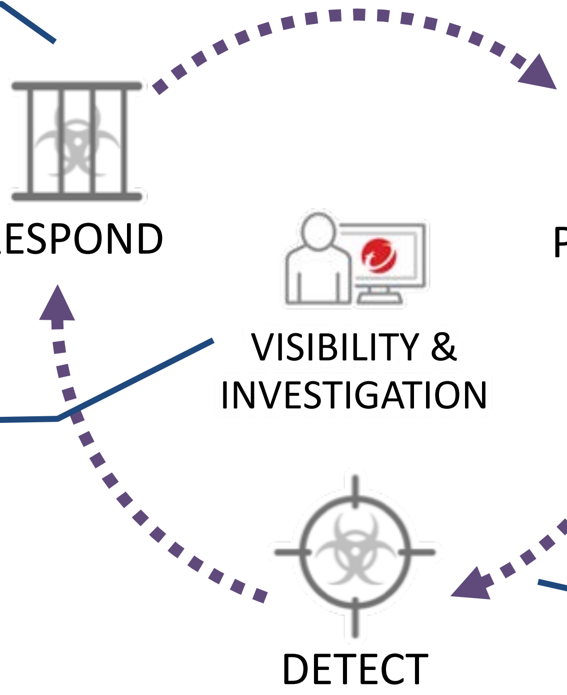
동적분석:
Behavioral
analysis &
Run-time ML

“Connected Threat Defense”

Connected Threat Defense

위협 인텔리전스 공유
실시간 보안 업데이트
를 통한 신속한
공격대응

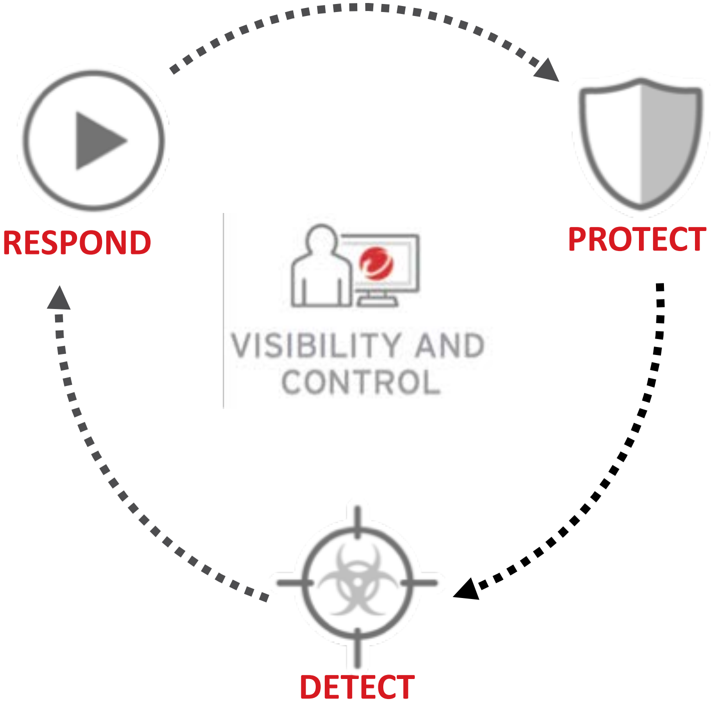
잠재적 취약성 검사,
엔드 포인트, 서버 및
애플리케이션 사전
예방 보호



시스템 전반에 걸친 **중앙**
집중형 가시성 확보 및
위협도 영향 분석 및 평가

기존 대응방법으로
탐지할 수 없는 **숨겨진**
공격(Hidden Attack) 탐지

Connected Threat Defense



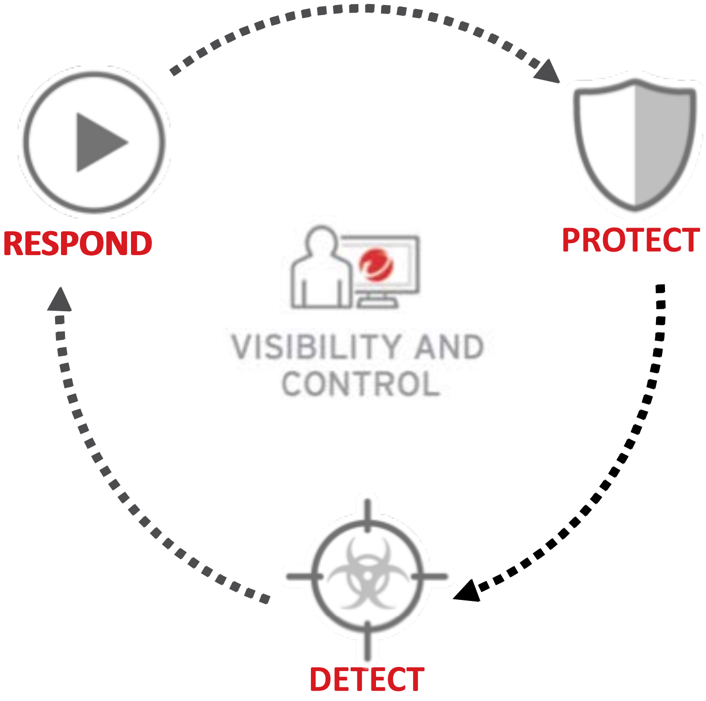
Connected Threat Defense

PROTECT

- Anti-Malware and Content Filtering
- App Control
- Intrusion Prevention
- Integrity Monitoring

Connected Threat Defense

PROTECT



RESPOND

PROTECT

VISIBILITY AND CONTROL

DETECT

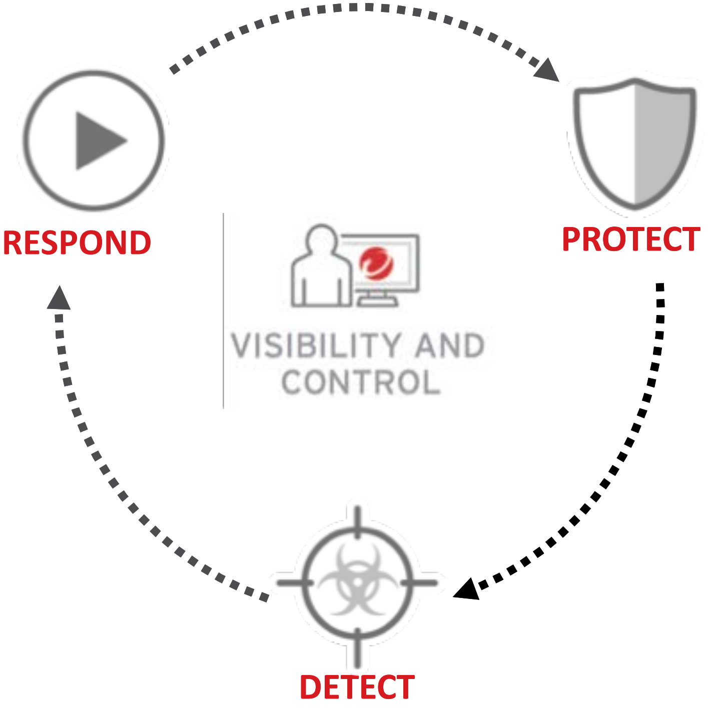
Connected Threat Defense

DETECT

"기존의 심층 방어(defense-in-depth)구성 요소는 필수지만 지능형 표적 공격 및 고급 멀웨어에 대응에는 충분하지 않다!!!"

- Network Content Inspection
- Custom Sandbox Analysis
- Lateral Movement Detection
- Machine Learning
- Behavioral Analysis

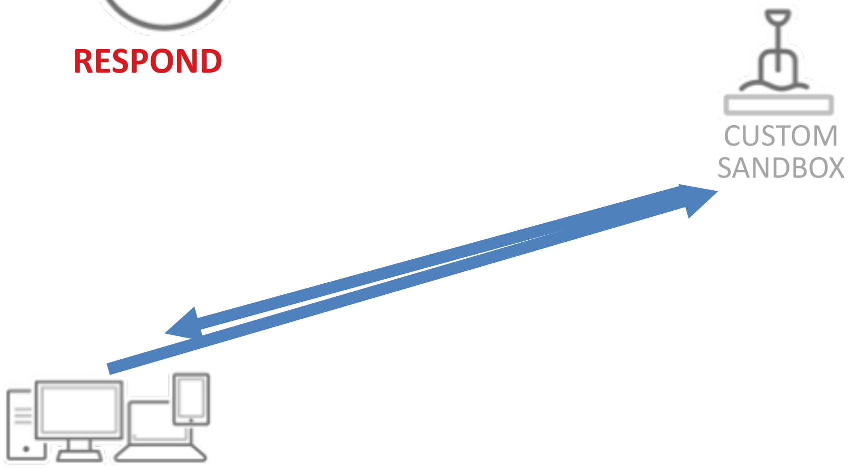
Connected Threat Defense



Connected Threat Defense

위협정보공유 및 가시성 제공

RESPOND



CUSTOM SANDBOX

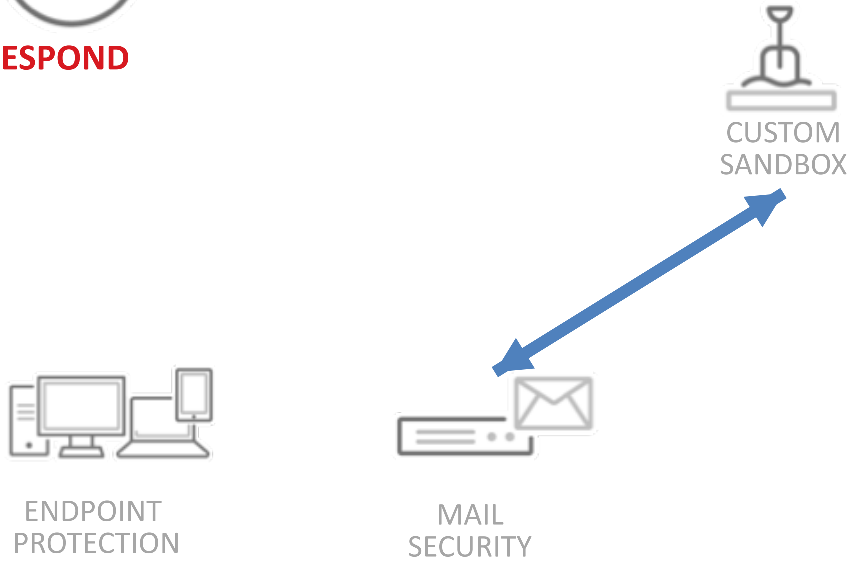
ENDPOINT PROTECTION

OfficeScan	URL, File, IP Action
Endpoint Sensor	IOC, SHA, IP, Domain

Connected Threat Defense

RESPOND

위협정보공유 및 가시성 제공



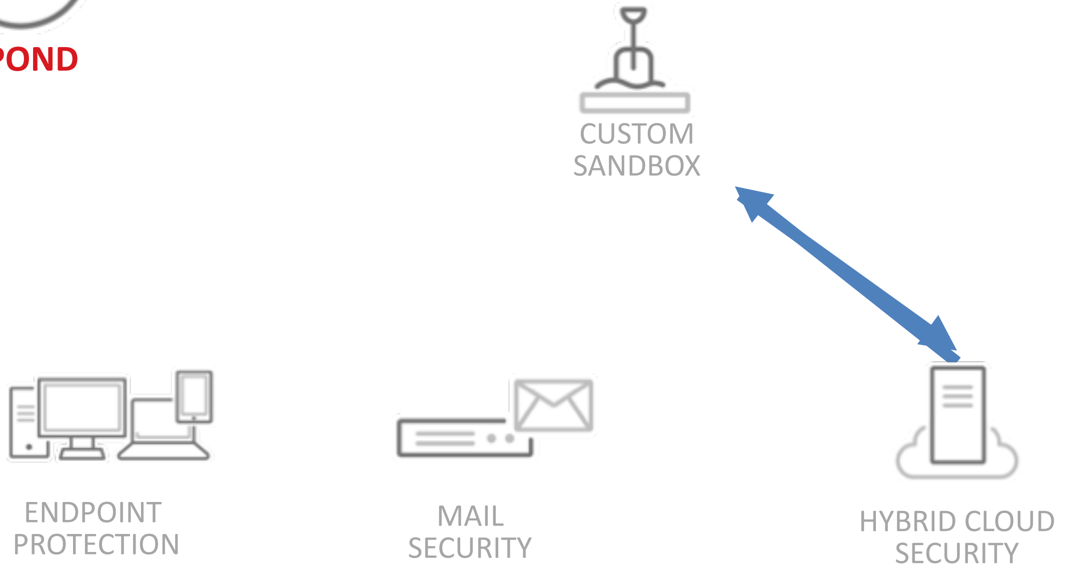
ScanMail for Exchange	SHA-1 Risk-Level
InterScan Mail Security	SHA, IP, Domain Risk-Level

Connected Threat Defense

Security TRENDS 2018

RESPOND

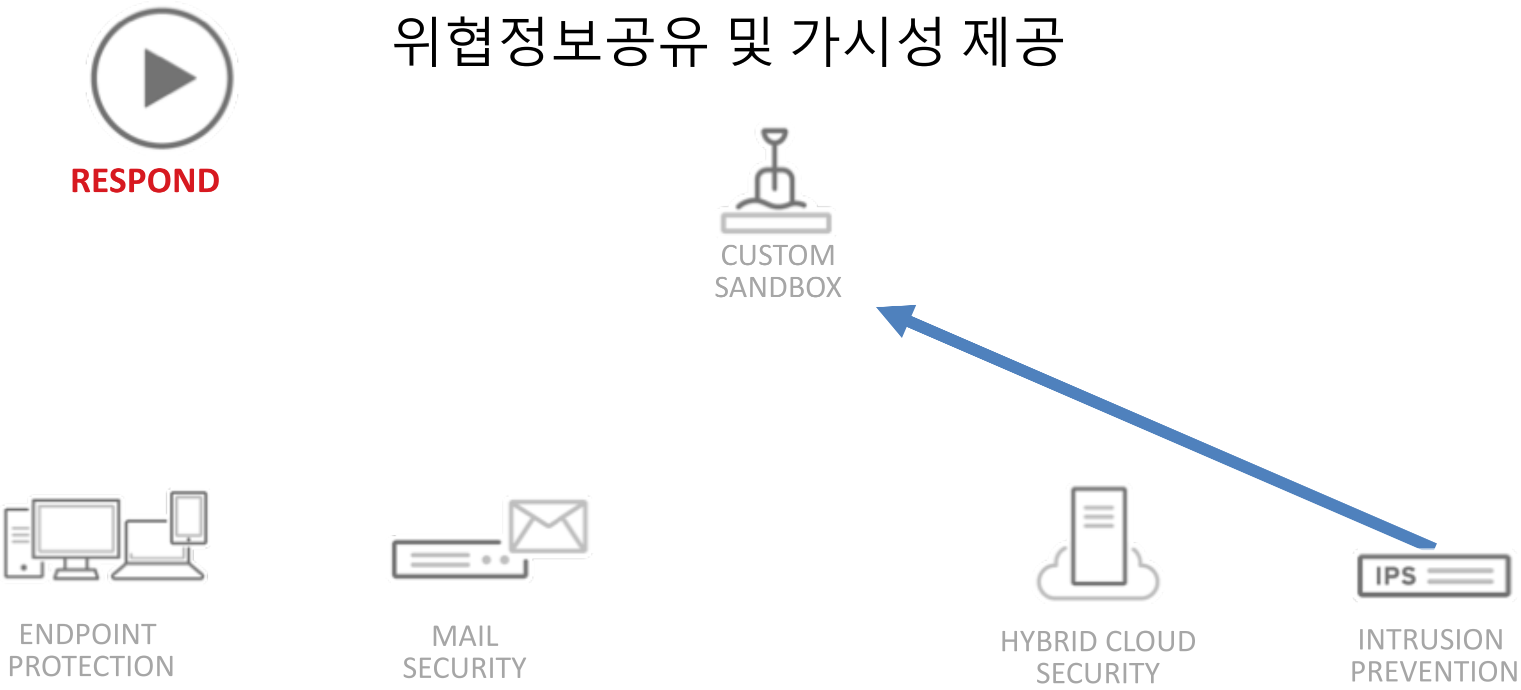
위협정보공유 및 가시성 제공



Deep Security	Action	URL, File	

Connected Threat Defense

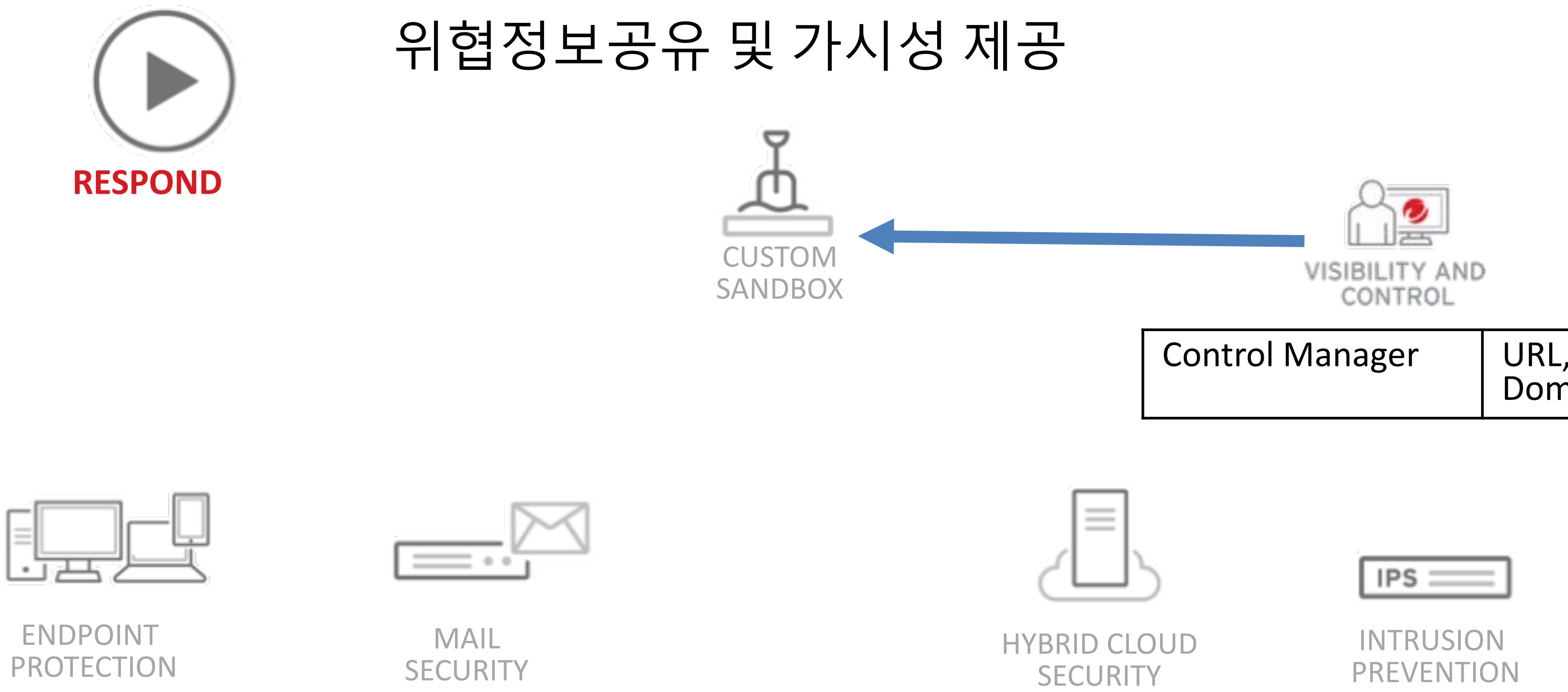
위협정보공유 및 가시성 제공



TippingPoint IPS	URL, File, IP, Domain

Connected Threat Defense

위협정보공유 및 가시성 제공

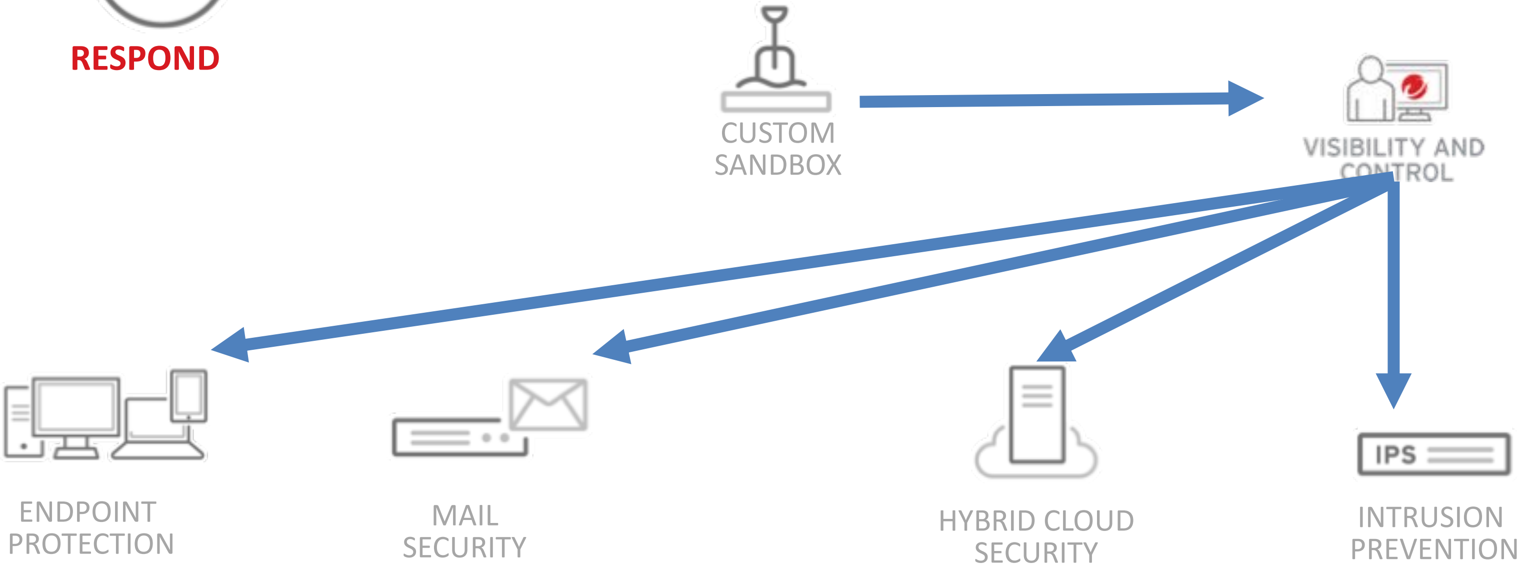


Control Manager	URL, File, IP, Domain, SHA

Connected Threat Defense

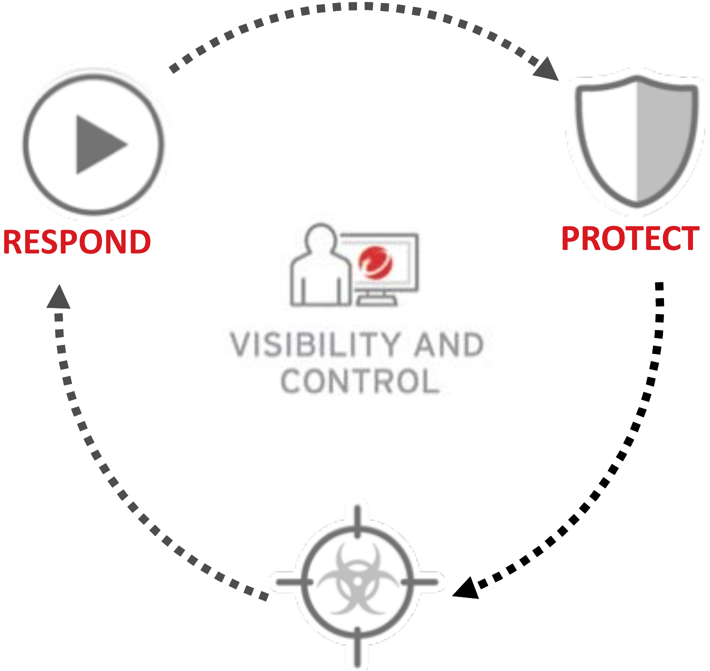
RESPOND

위협정보공유 및 가시성 제공



Connected Threat Defense

RESPOND

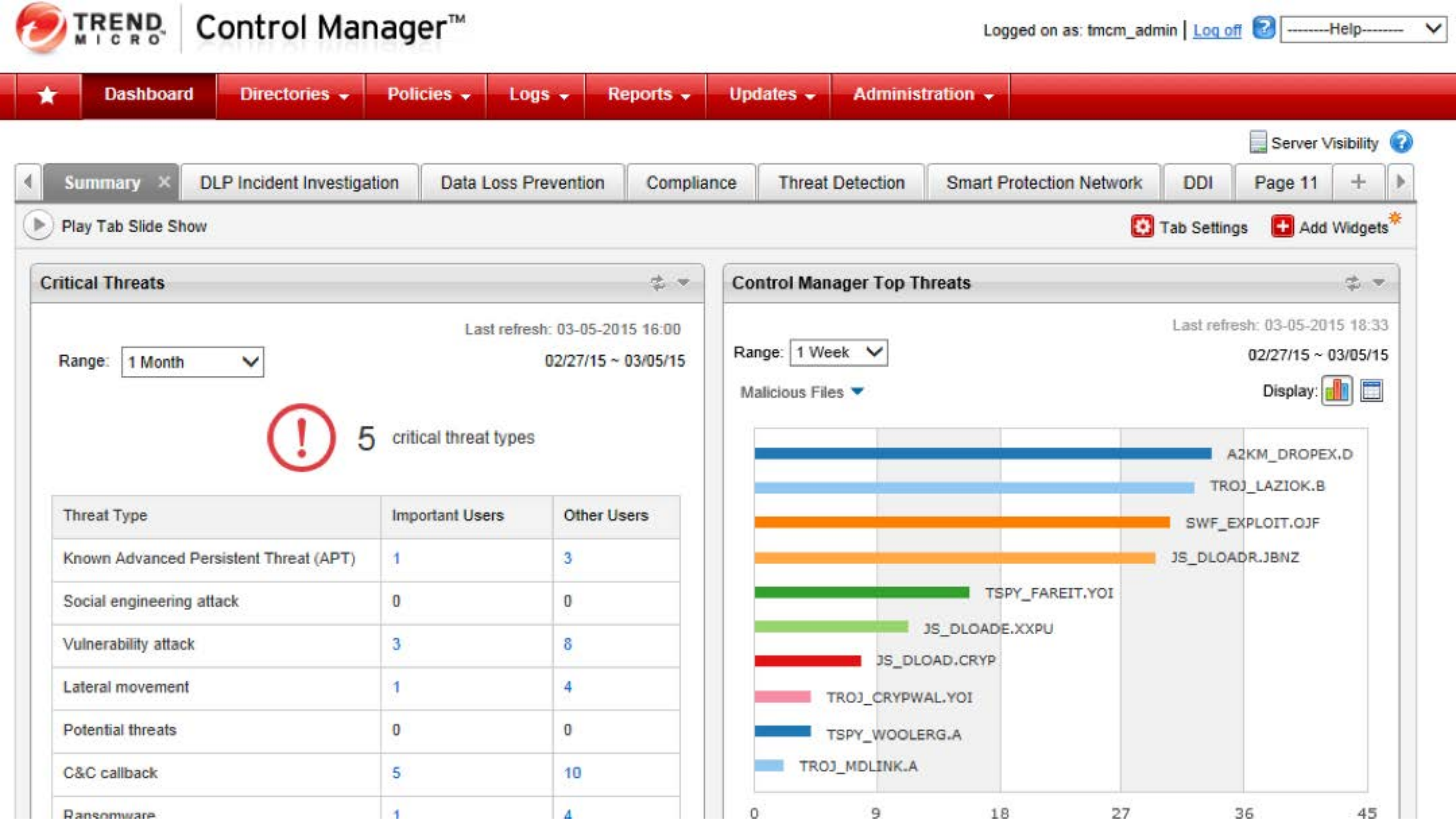


RESPOND

PROTECT

VISIBILITY AND CONTROL

DETECT



Critical Threats

Last refresh: 03-05-2015 16:00

Range: 1 Month

02/27/15 ~ 03/05/15

5 critical threat types

Threat Type	Important Users	Other Users
Known Advanced Persistent Threat (APT)	1	3
Social engineering attack	0	0
Vulnerability attack	3	8
Lateral movement	1	4
Potential threats	0	0
C&C callback	5	10
Ransomware	1	4

Control Manager Top Threats

Last refresh: 03-05-2015 18:33

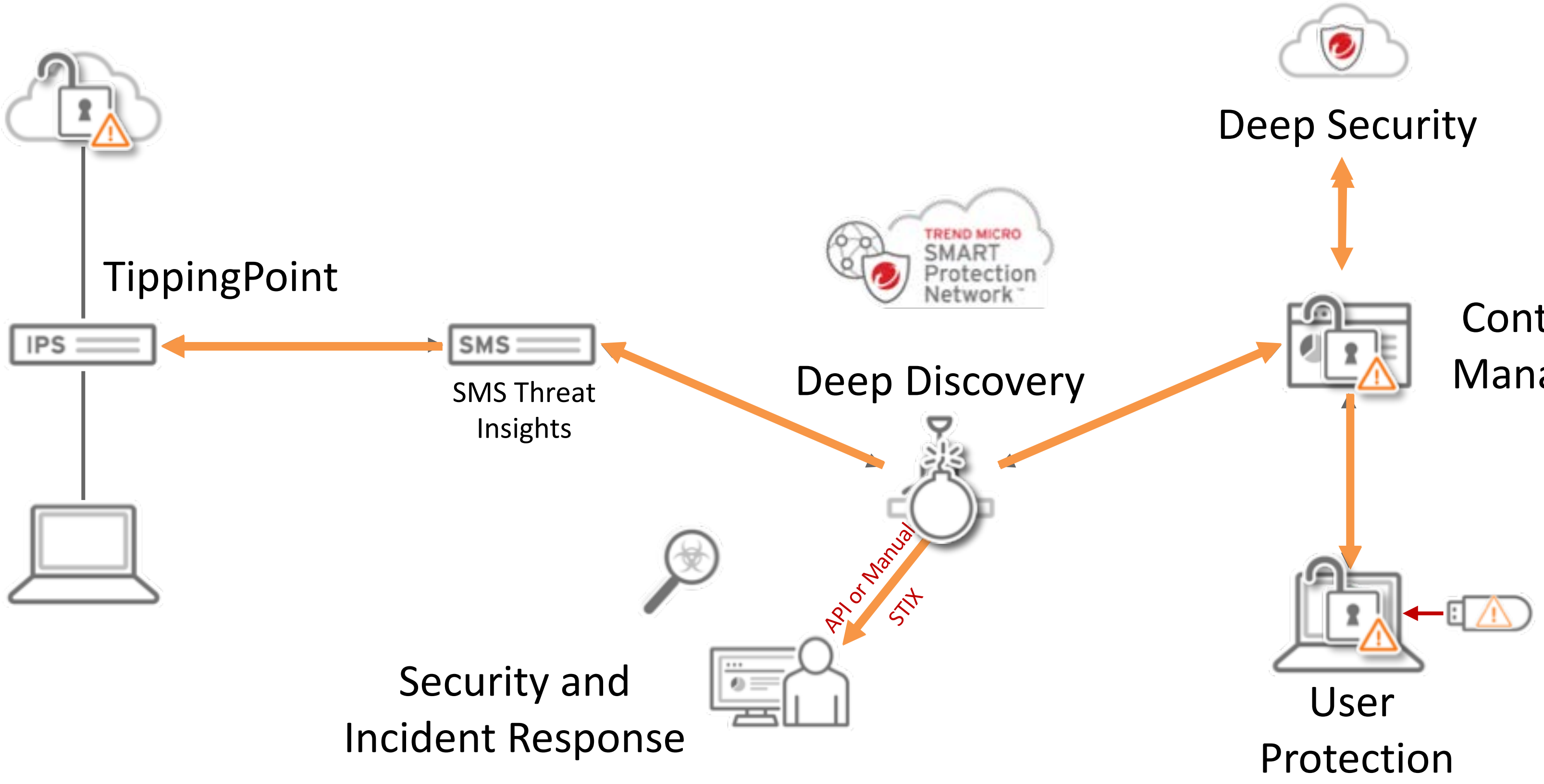
Range: 1 Week

02/27/15 ~ 03/05/15

Malicious Files

Display:

Connected Threat Defense



글로벌 위협 인텔리전스:
Smart Protection Network™

2017 글로벌 위협 인텔리전스 통계

... received 3T
Reputation queries

... blocked 65B
total threats

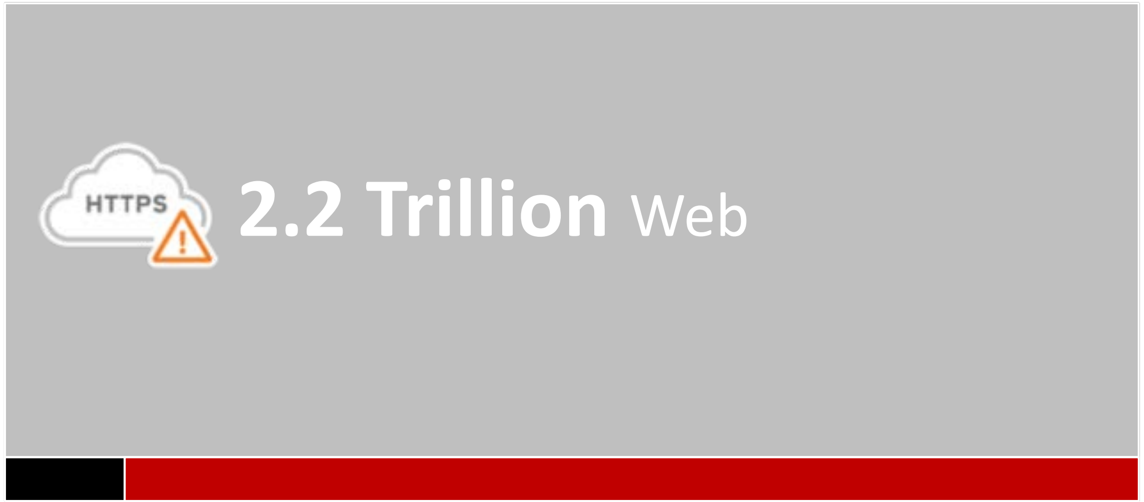
... identified 6.6B new
unique threats

... Blocked 600M+
ransomware threats

TREND MICRO SMART Protection Network™

글로벌 위협 인텔리전스

Threat Queries to Trend Micro



28 Billion
모바일 앱

105 Billion
이메일

631 Billion 파일

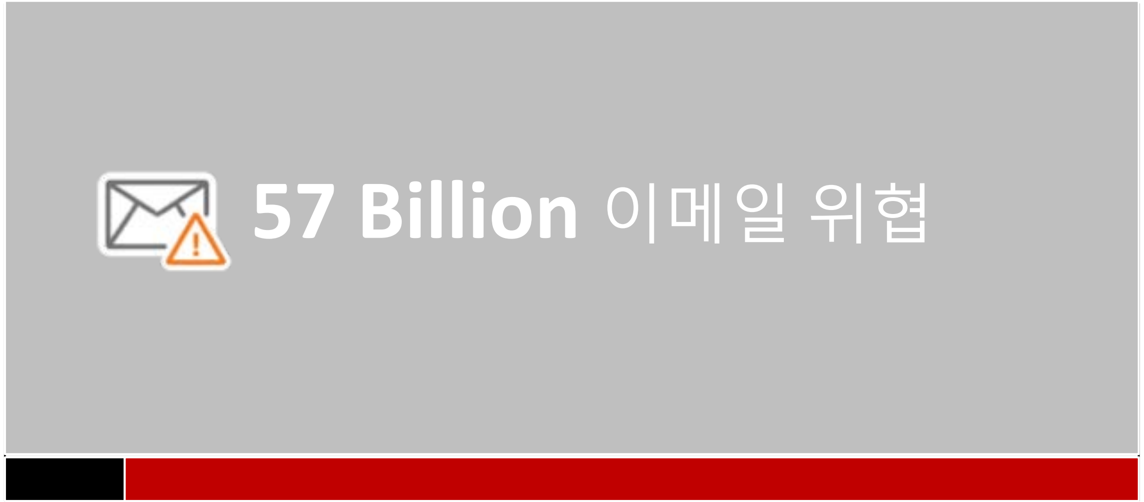
TREND MICRO SMART Protection Network™

글로벌 위협 인텔리전스

Threats Blocked by SPN

75 Million
악성 앱

1 Billion
악성 URLs



7 Billion 악성 파일

TREND MICRO

Security
TRENDS 2018

감사합니다!!!

트렌드마이크로
장 성 민