제로데이공격방어를 위한 향상된 위협방어 플랫폼

장 성 민 소장

April 26 2018

지연 시간이 없는
고성능의 네트워크 인프라

클라우드
데이터센터

물리/가상화
데이터센터

지방 및 해외
지점/사업장

스마트팩토리

재고 관리 시스템

의료 기기

공조설비
시스템

차량 관제
시스템

경계가 없는
기업 네트워크의 확장

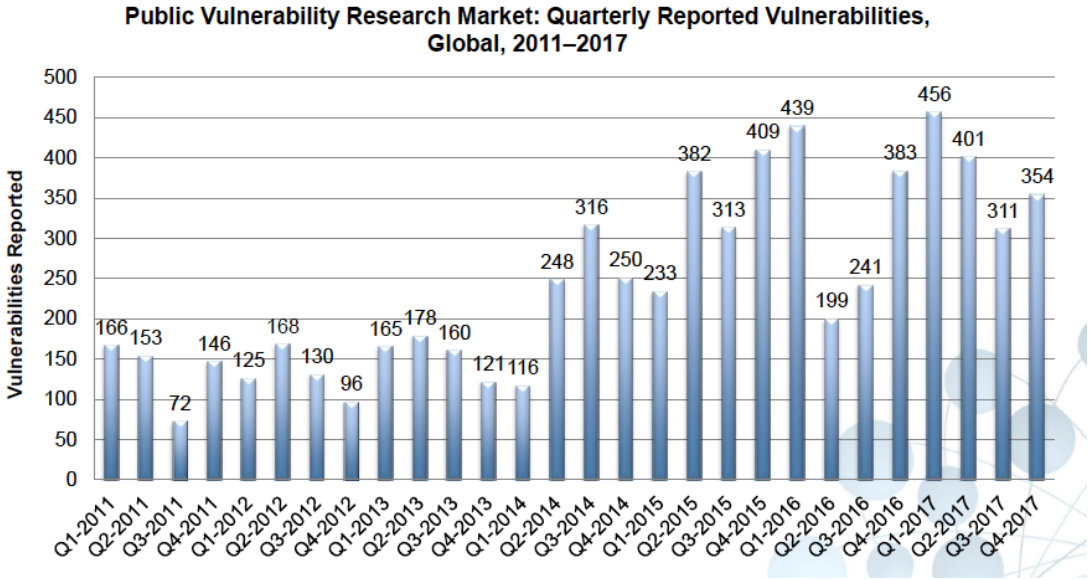
어디에서든 접속 가능한
IoT/IIoT 환경 확산

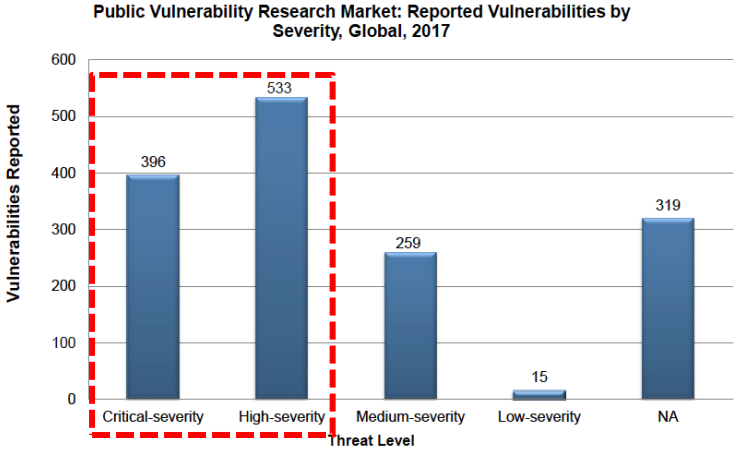
* IIoT(Industrial Internet of Thing) : 산업용 사물인터넷

TREND MICRO

제로데이 취약점은 계속되고..

* Source : Analysis of the Global Public Vulnerability Research Market (Feb 2018)





타킷 랜섬웨어 위협

110 seconds - From send to open for a spear phishing email

Under 60 seconds - Endpoints are encrypted

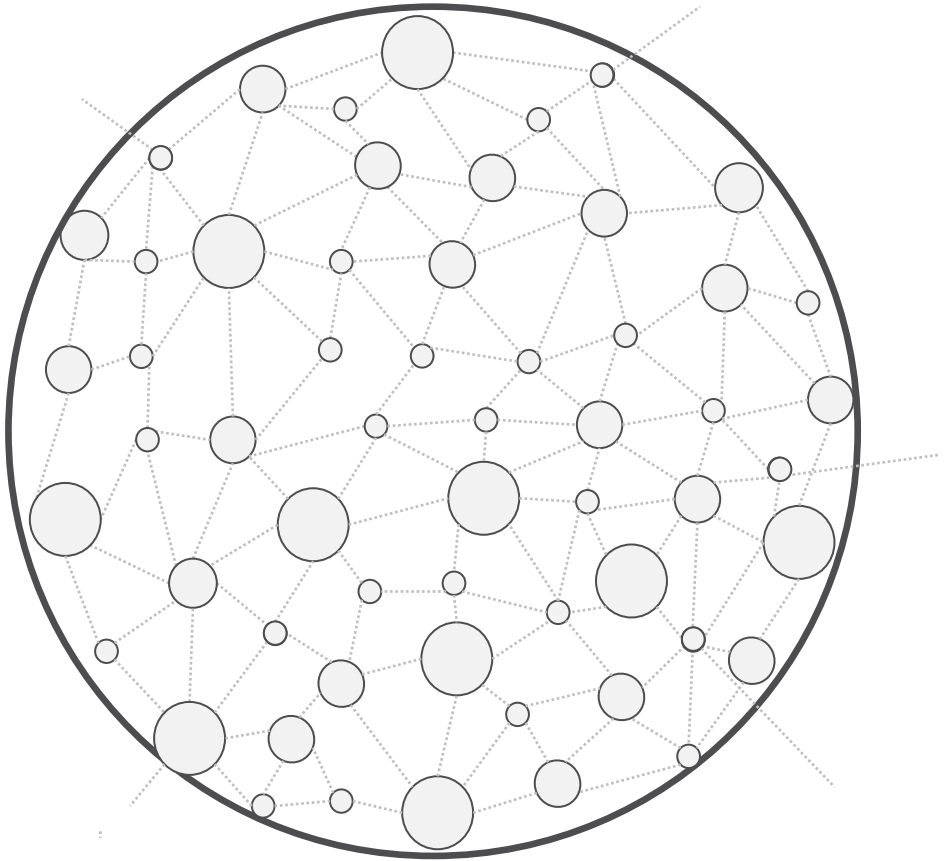
The Cost of Ransomware

- Downtime: 72% lack access for 2 days, 32% 5 or more days
- Ransom costs
- Support costs

Source: Verizon Data Breach Report
Source: Barkley

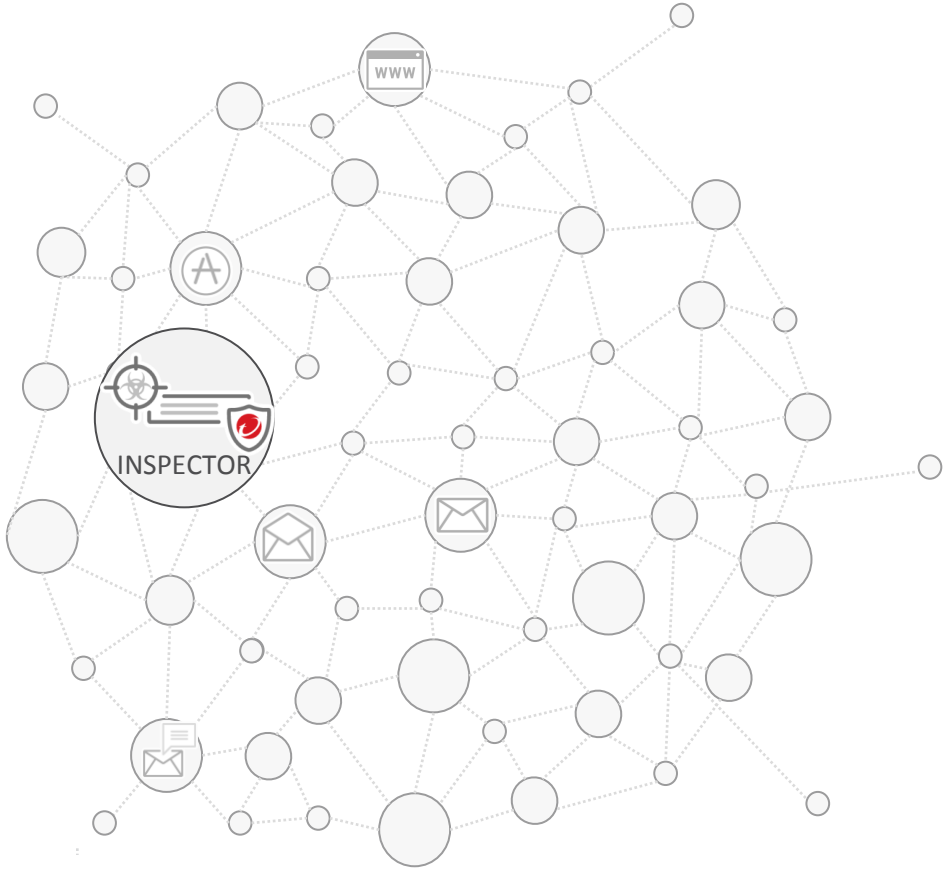
Advanced Threat Protection Platform

Network Defense



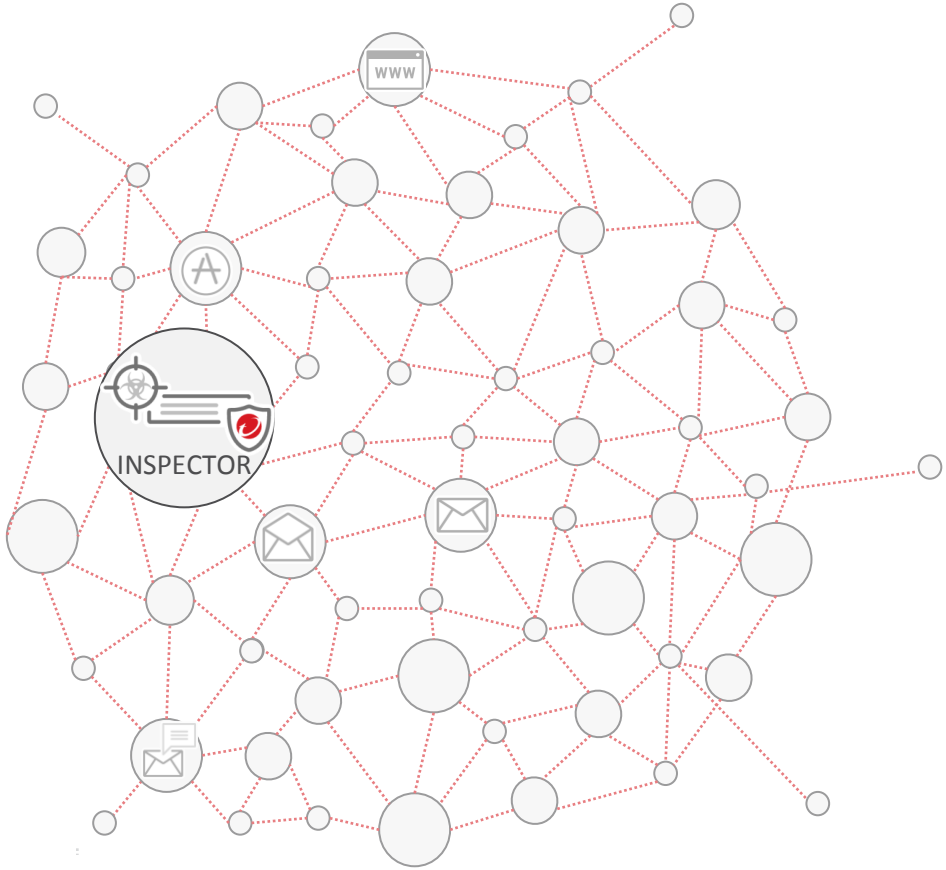
Connected & Multi-Layered Network

Deep Discovery + TippingPoint



Deep Discovery Inspector

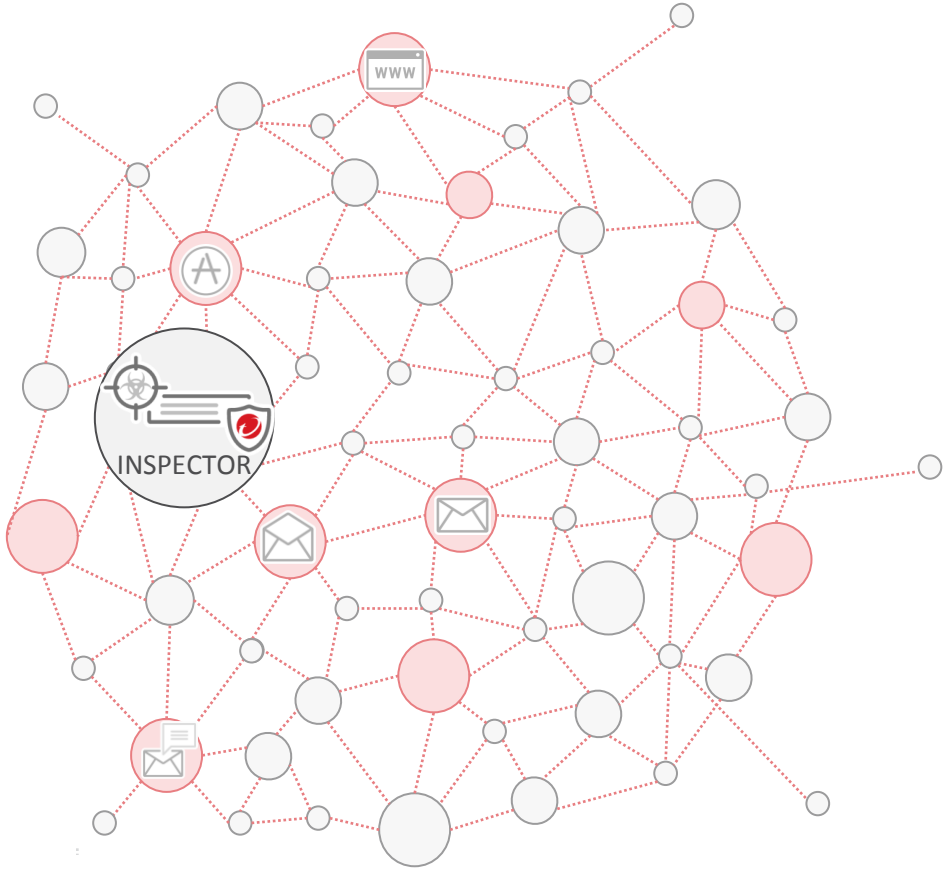
Deep Discovery + TippingPoint



Deep Discovery Inspector

- 모든 통신 포트

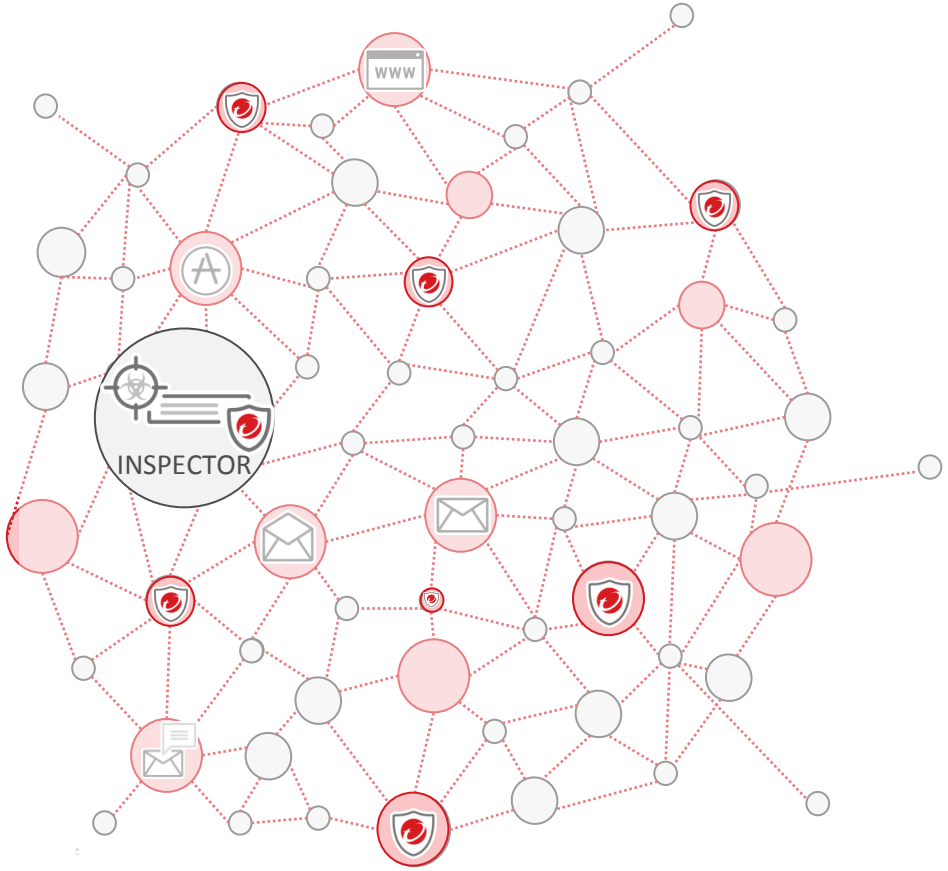
Deep Discovery + TippingPoint



Deep Discovery Inspector

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

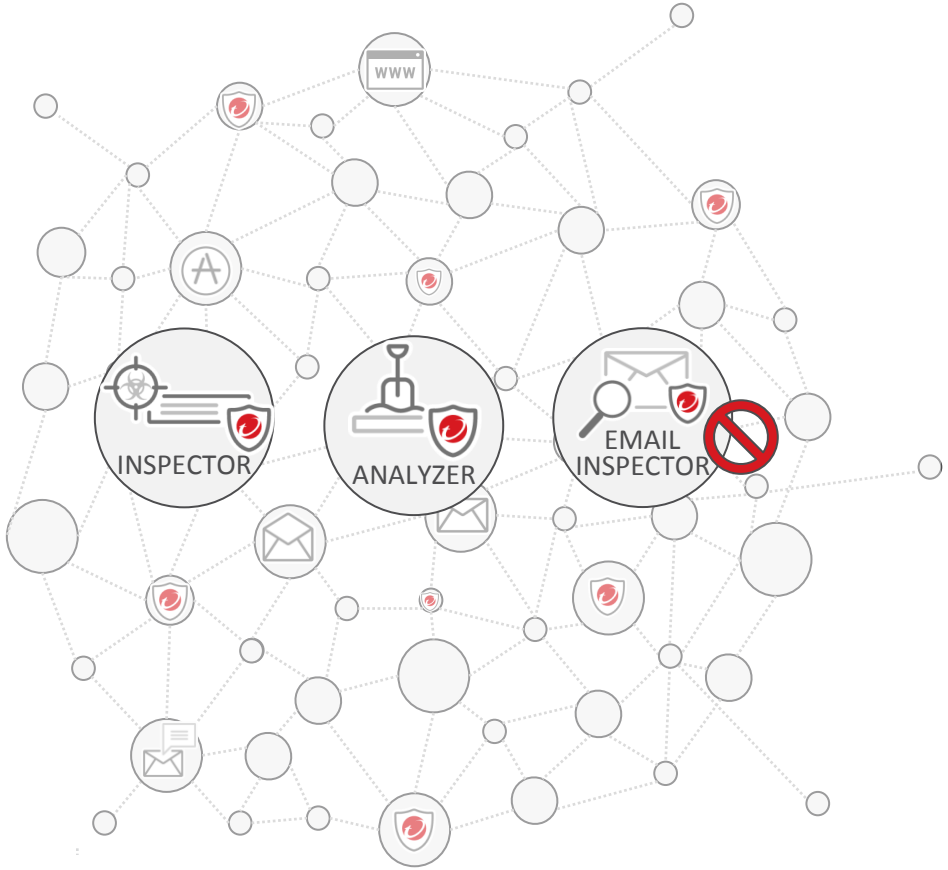
Deep Discovery + TippingPoint



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

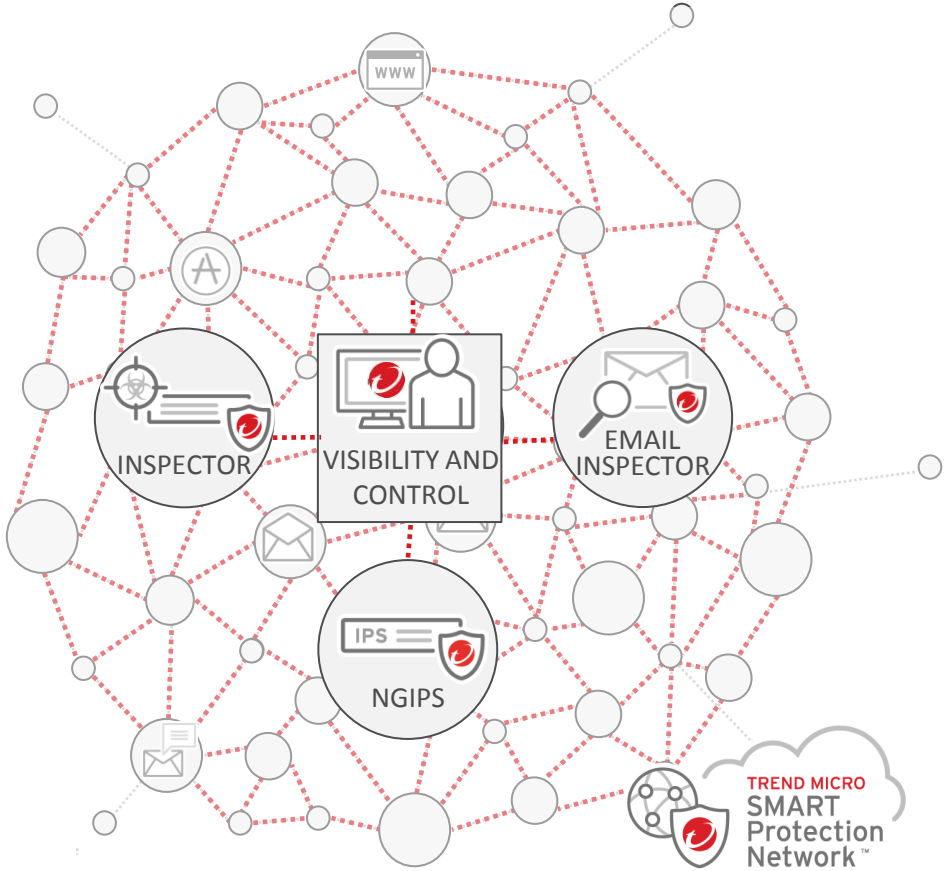
Deep Discovery Email Inspector

- 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

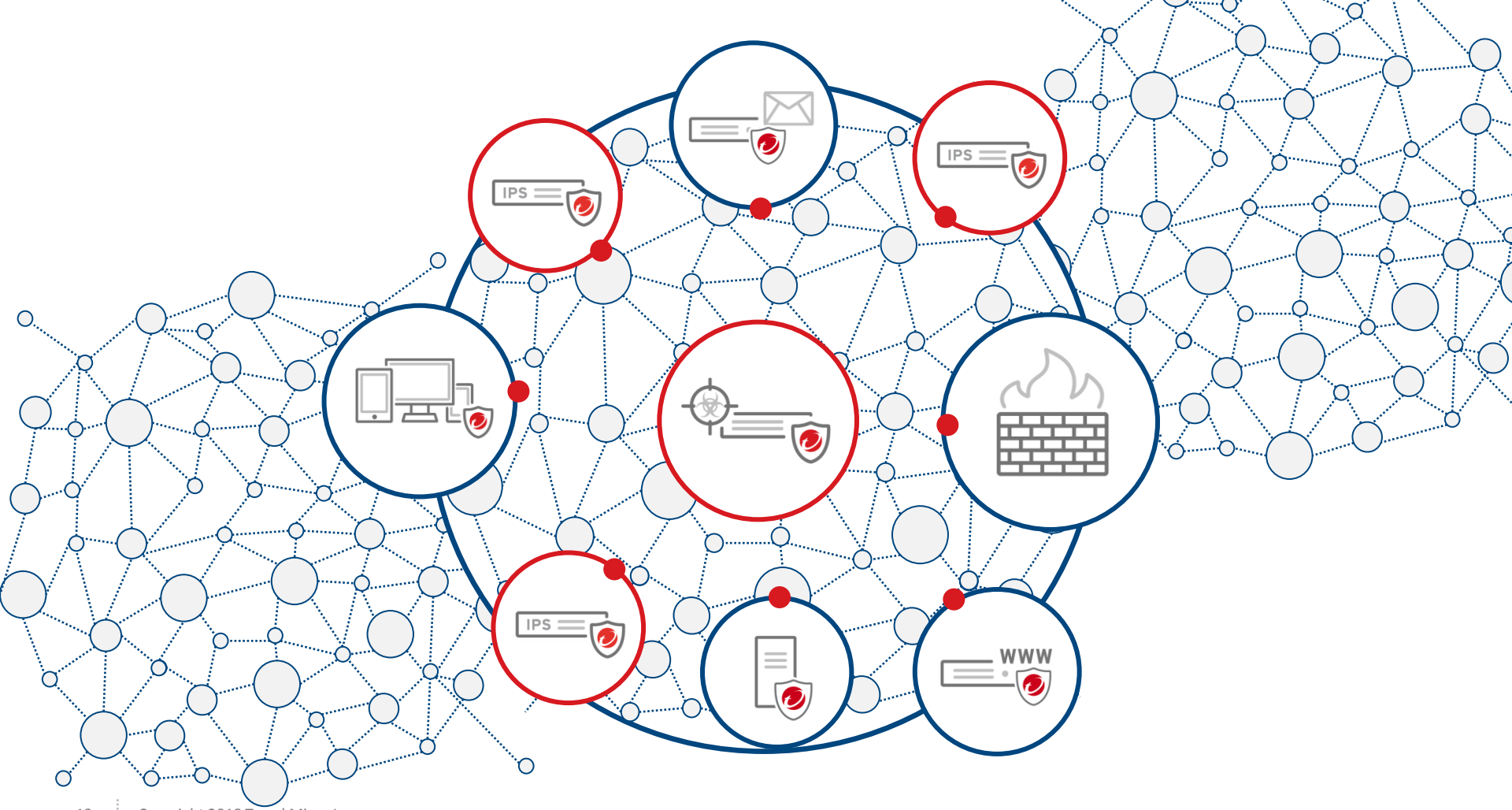
- 스피어피싱 메일 대응
- 랜섬웨어 메일 대응

Deep Discovery Analyzer

- 커스텀 샌드박스

TippingPoint Next Generation IPS

- 와이어 스피드 위협 방어(단일장비 40G)
- Zero day Initiative 취약점 대응



Network Security
Deep Discovery

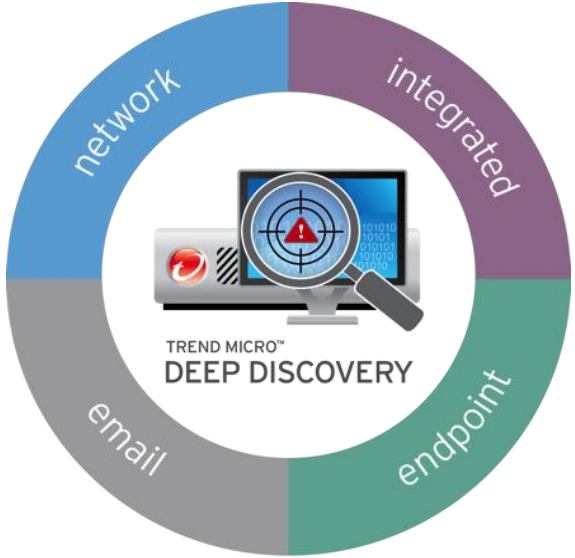
Deep Discovery

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 Analyzer - DDAN

APT 분석

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

(모델 : DDAN1100)

Deep Discovery Email Inspector - DDEI

Email APT 차단

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

(모델 : DDEI7100/9100)

OfficeScan Agent (Endpoint Anti-Malware)

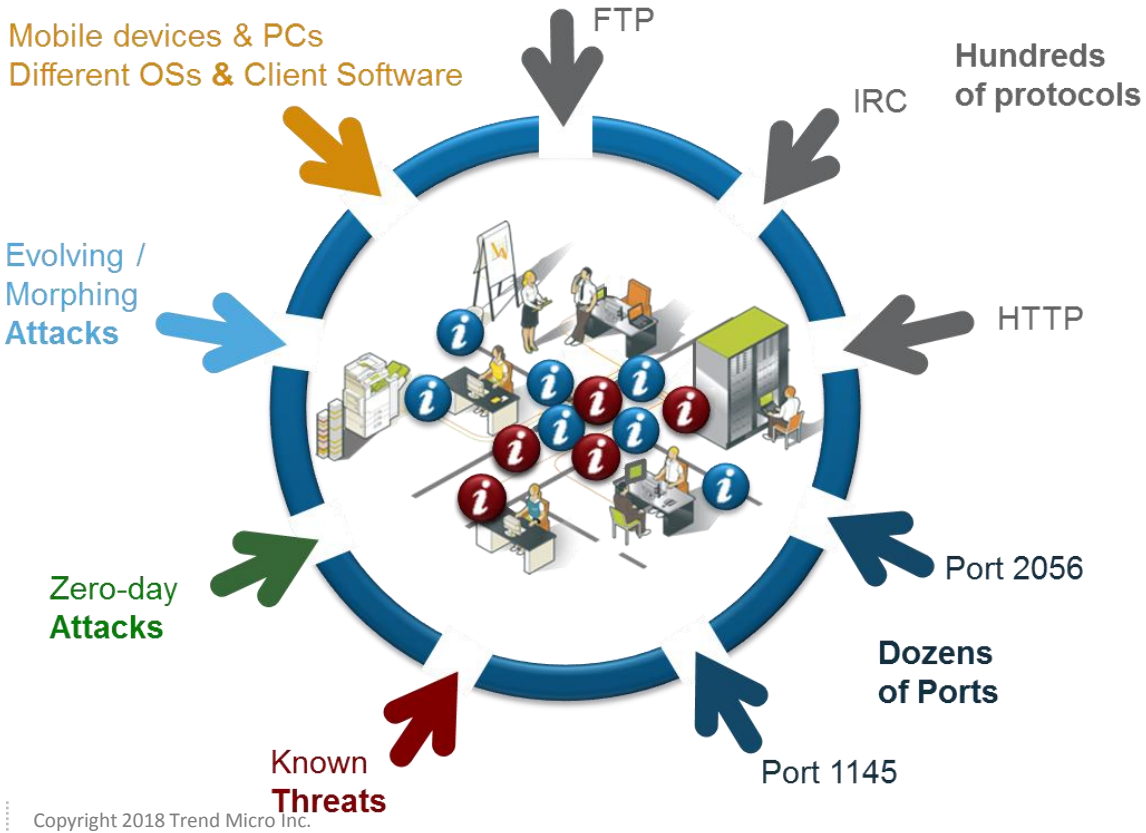
Endpoint 대응

알려진 악성코드 치료, Unknown Malware 격리 및 Endpoint Network 격리

Key Technologies

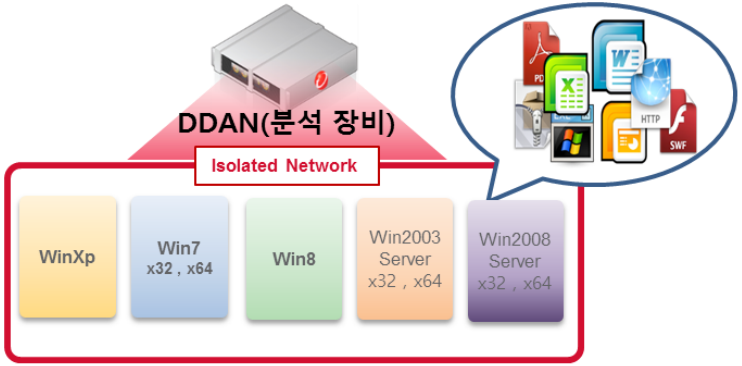
APT 특화 탐지 엔진		Document Exploit(Statistic Analysis) + Known Malware
맞춤형 샌드박스		맞춤형 샌드박스
머신러닝		클라우드 보안센터의 학습데이터를 이용하는 머신러닝을 통해 신/변종 악성코드 탐지
글로벌 위협 인텔리전스		실시간 클라우드 인텔리전스와 리서치 파워를 활용하여 탐지 정확성 및 엔진 및 룰셋의 지속적인 업데이트
위협정보 연동		샌드박스로 부터 탐지된 IoC를 트렌드마이크로 제품 및 3rd Party 제품과 실시간 공유

100+ 프로토콜 탐지 지원



"특정 프로토콜만 지원하는 제품으로는 충분하지 않습니다."

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

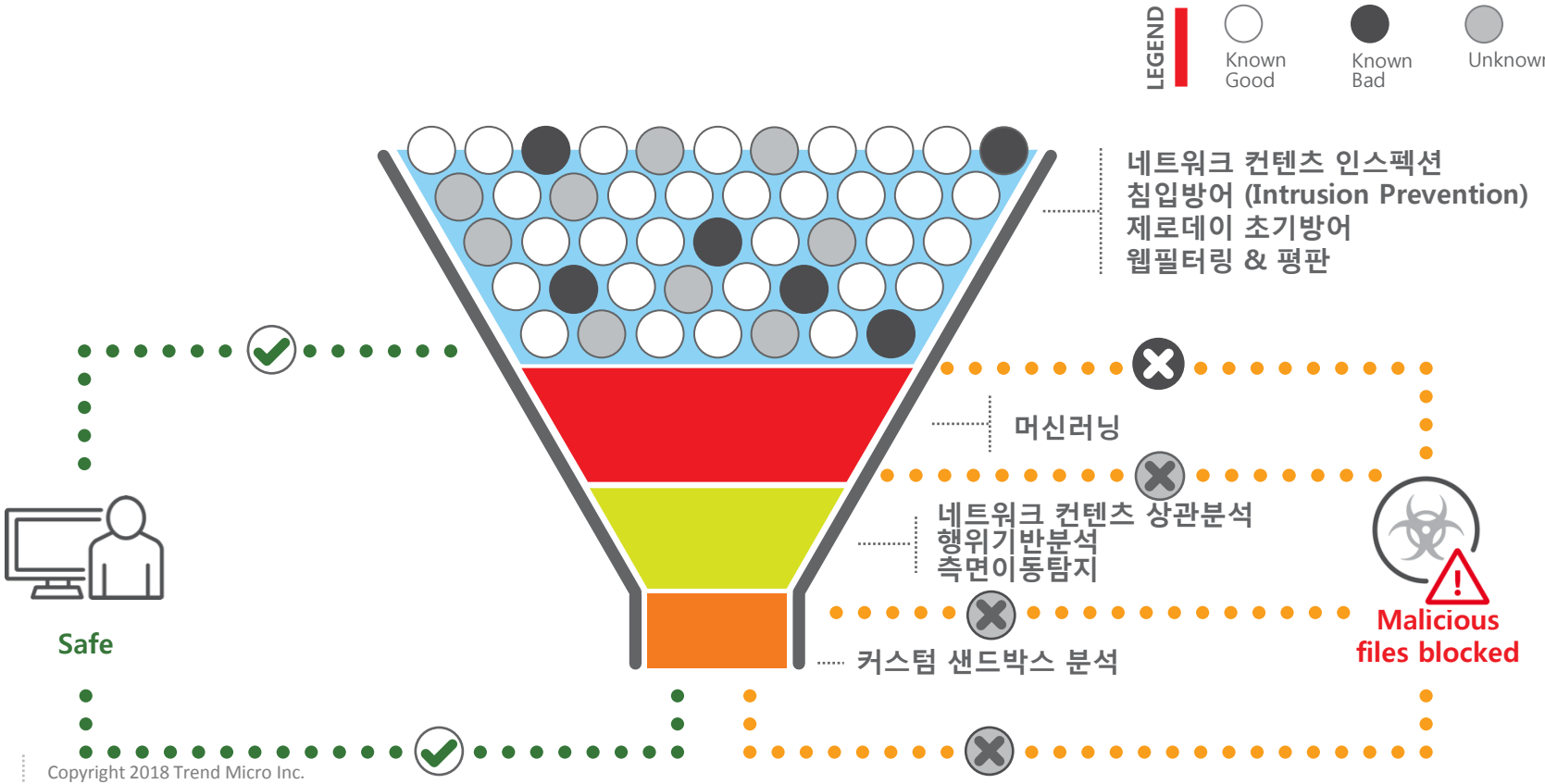
최대 3가지 타입의 Sandbox를 동시에 운영 가능

표적형 공격 대응에는

"맞춤형 샌드박스"가

효과적입니다.

Machine Learning Powered by XGen




TippingPoi
nt
is Back !!!

Industry Proven

TippingPoint 8200TX

TippingPoint 8400TX

Industry-first 40Gbps inspection on a 1U appliance!

- High performance security for high-capacity networks and data center consolidation
- Up to 40 Gbps in 1U form factor
- Up to 120 Gbps in 3U form factor
- Low latency of <40 microseconds

Pay as you grow

120 Gbps

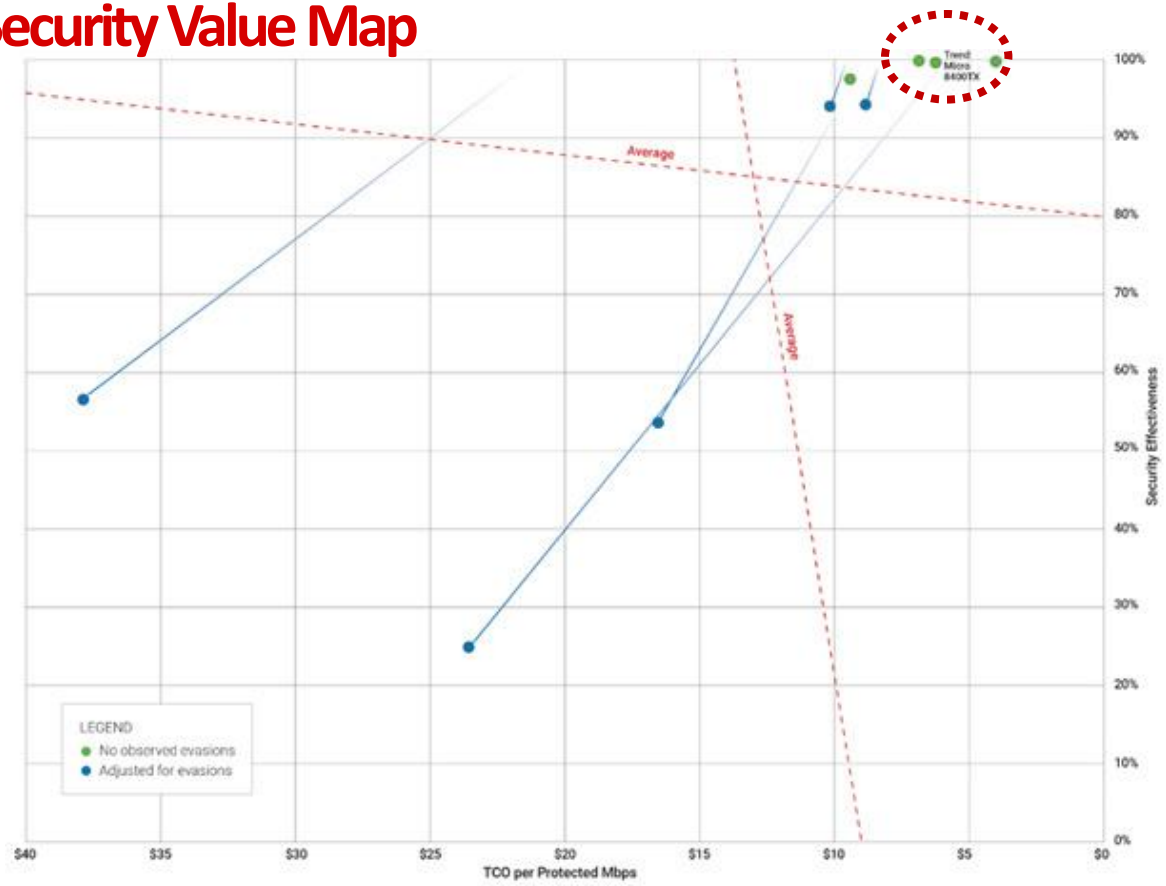
80 Gbps

40 Gbps

SSL Throughput also can be scalable from 2Gbps to 10Gbps

2017 NSS Labs : NGIPS Group Test Results

Security Value Map



NSS LABS RECOMMENDED

Trend Micro™ TippingPoint®

RECOMMENDED

99.6% Security Effectiveness

NSS Labs 2017 NGIPS Group Test

TREND MICRO TIPPINGPOINT RECOMMENDED DATA CENTER IPS

NSS LABS RECOMMENDED

NSS LABS 2018 DCIPS GROUP TEST

TREND MICRO

2017 NSS Labs : NGIPS Group Test Results

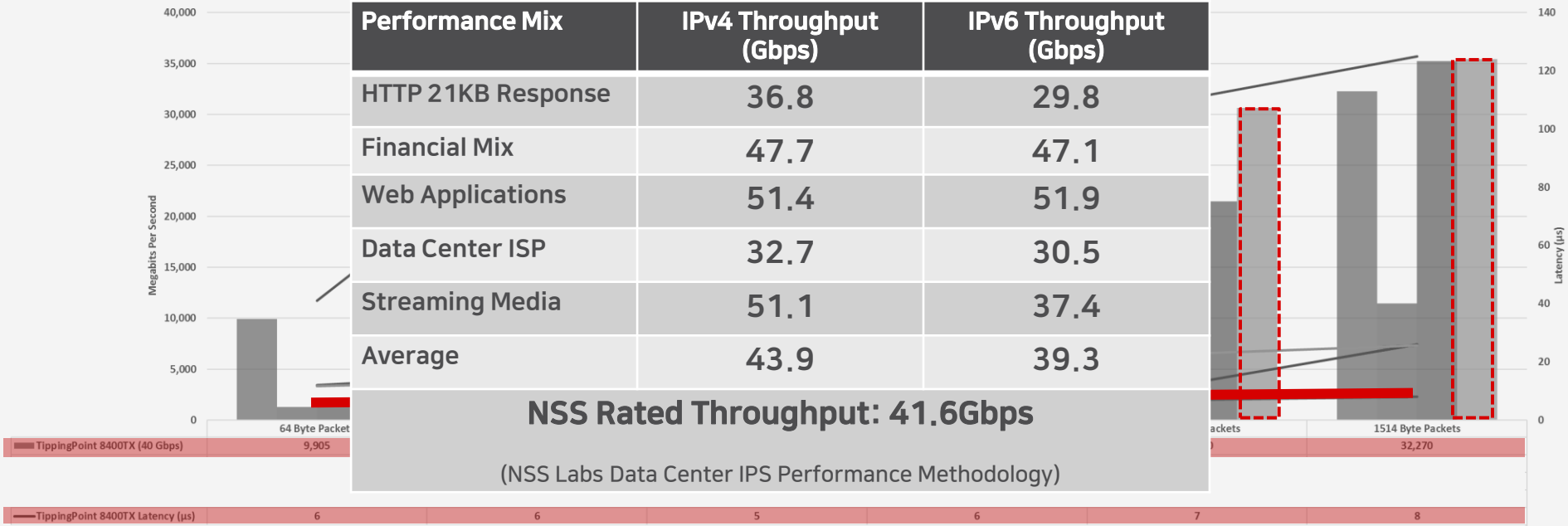
Latency & Performance

2017 NSS Labs Performance Comparison - UDP Throughput and Network Latency (Stand-alone NGIPS Only)

Performance Mix	IPv4 Throughput (Gbps)	IPv6 Throughput (Gbps)
HTTP 21KB Response	36.8	29.8
Financial Mix	47.7	47.1
Web Applications	51.4	51.9
Data Center ISP	32.7	30.5
Streaming Media	51.1	37.4
Average	43.9	39.3

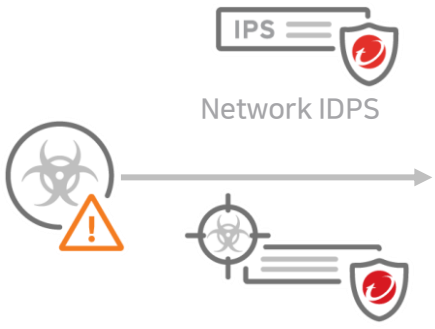
NSS Rated Throughput: 41.6Gbps

(NSS Labs Data Center IPS Performance Methodology)



2017 NSS Labs : NGIPS Group Test Results에 따르면 NG IPS 업계에서 성능 대비 최소의 지연시간(Latency) 지원 !!
네트워크 In-Line상에서 고성능/대용량 트래픽을 처리

* Source : 2017 NSS Labs : NGIPS Group Test Results, Latency & Performance



Next-Gen IDPS

- Detection of Known & Unknown Vulnerabilities
- Context-aware Traffic Inspection
- IP/DNS & URL Reputation
- Encrypted Traffic Inspection
- Geo/Location Filtering
- Active Directory Integration
- Comprehensive Network Traffic Visualization
- Third Party Integration

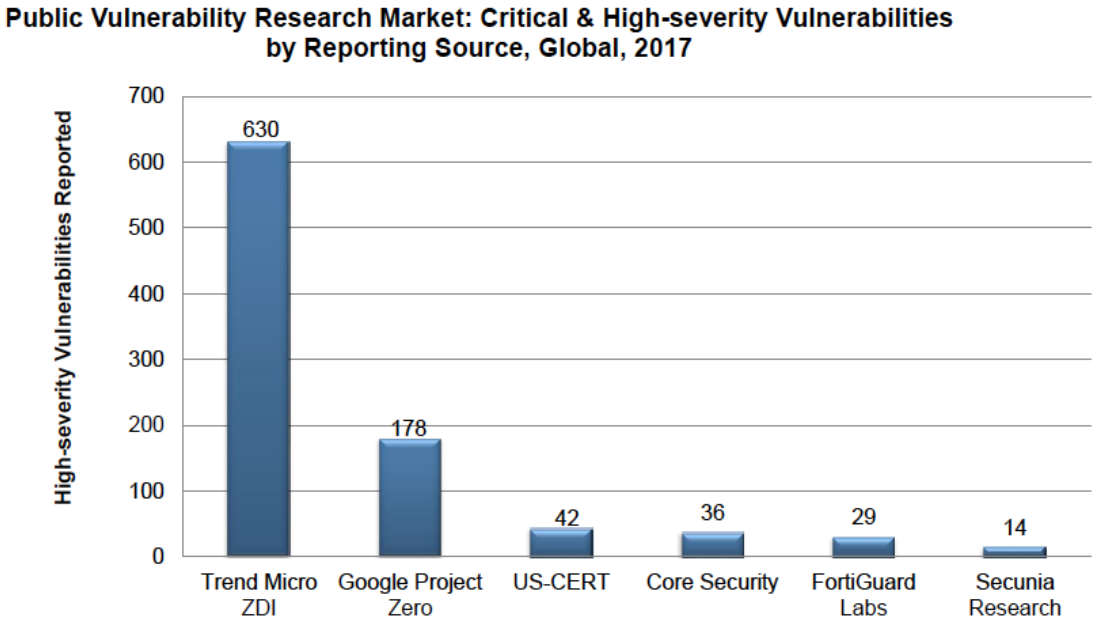
TippingPoint XGen IDPS

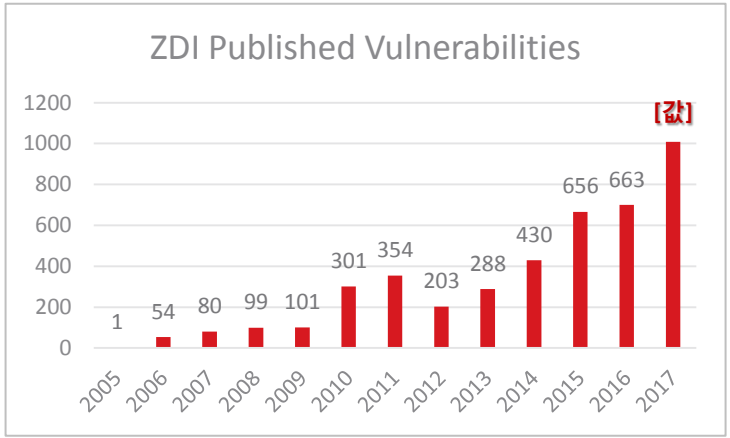
- Machine Learning
- DGA(Domain Generation Algorithms) Defense
- High-Performance Malware Filter Package
  - Bot Activity
  - Data Exfiltration
  - Ransomware
  - Mobile
  - Command & Control
  - Phone Home
- Detection/Remediation of UNDISCLOSED Vulnerabilities
- Automated Sandbox Analysis
- Lateral Movement Detection

Trend Micro ZDI(Zero Day Initiative)

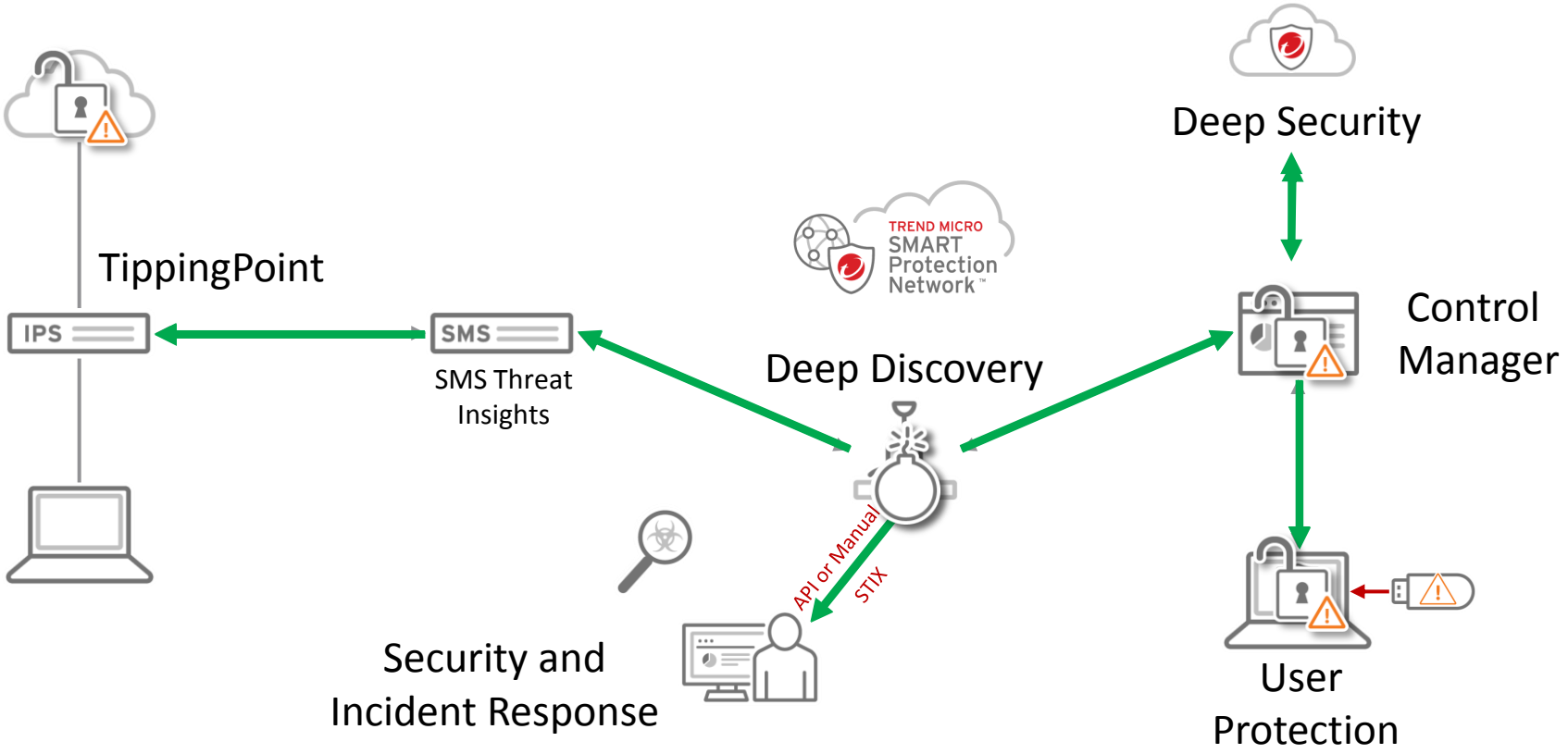
- Total Vulnerabilities by Disclosing

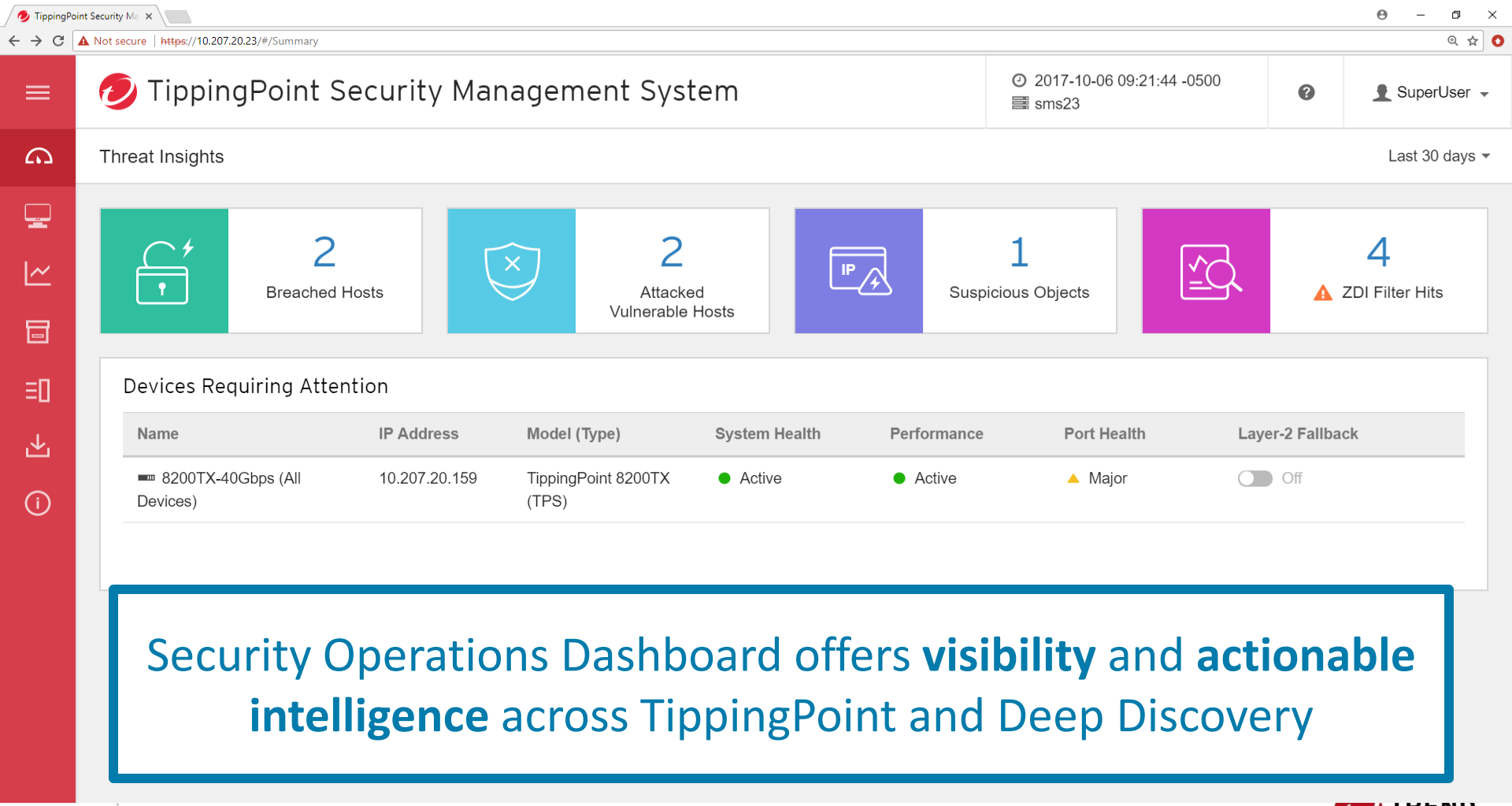
* Source : Analysis of the Global Public Vulnerability Research Market (Feb 2018)





Connected Threat Defense





Security Operations Dashboard offers **visibility** and **actionable intelligence** across TippingPoint and Deep Discovery

감사합니다.