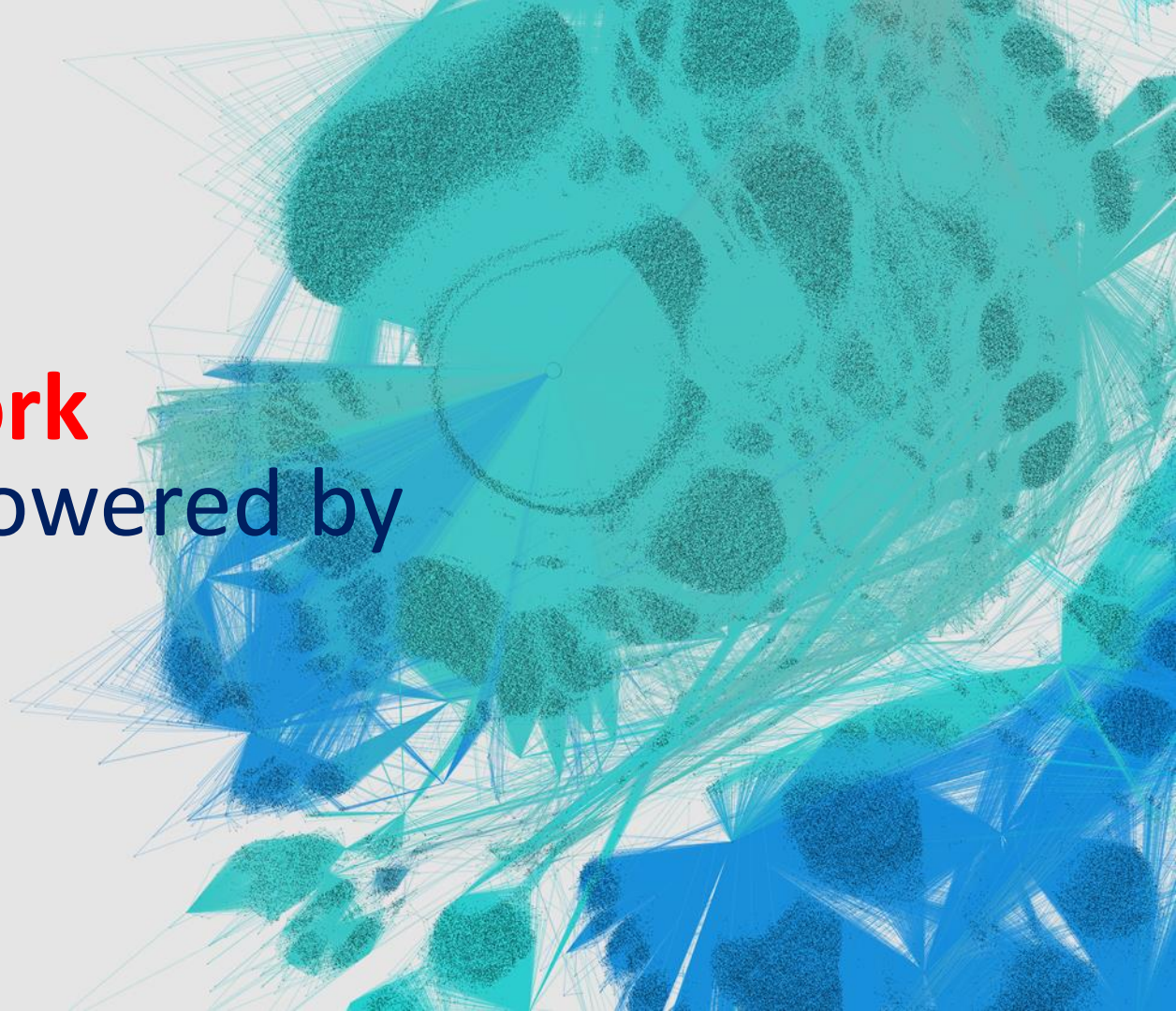
Cloud Network Protection powered by TippingPoint

TREND MICRO




Trend Micro
is extending
TippingPoint
to the cloud.

오늘날 클라우드 네트워크 보안 과제

사용자 의견 인용

"클라우드내 컴플라이언스 요건에 필요한 툴과 감사 로그 알람을 내/외부 환경에서 모니터링 방안에 대한 과제가 있다."

"Outbound 트래픽에서 '.ru domain'을 차단할 수 있을까?"

"Application에 영향을 최소화 하는 보안이 필요하다."

"기존 사용 툴들은 클라우드내 비용이나 성능면에서 적합하지가 않다."

클라우드 네트워크 보안에서의 문제점

지금까지 네트워크 보안 솔루션들은 구성이 복잡하고 비용이 많이 발생함으로써 적용하는데 있어 저항이 많이 발생

- **부적합적 설계**, 클라우드 사용 목적에 맞지 않는 디자인
- **비즈니스 효율 방해**, 클라우드 운영 및 DevOps 프로세스에 지연 발생
- **재 구성 요구,** 클라우드 이점 활용에 저해가 되고 시간 소요

TippingPoint Architecture For Cloud

TippingPoint의 클라우드로의 확장 의미

지속적인 네트워크 보안
TippingPoint 보안 정책을 클라우드로 빠르게 확장

SMS 통합 관리
SMS를 통해 Cloud & On-premise 통합 관리 및 가시성

구성 및 배포 간소화
사용자의 클라우드 네트워크 구조에 변경을 최소화하여 보안에 대한 부담을 줄임

간단한 배포 – 운영적 부담 최소화

Transparent

- Flow 기반 엔진
- 경계 없는 Deep Packet Inspection
- 서비스 중단 없이 인라인 구성 적용 및 해제

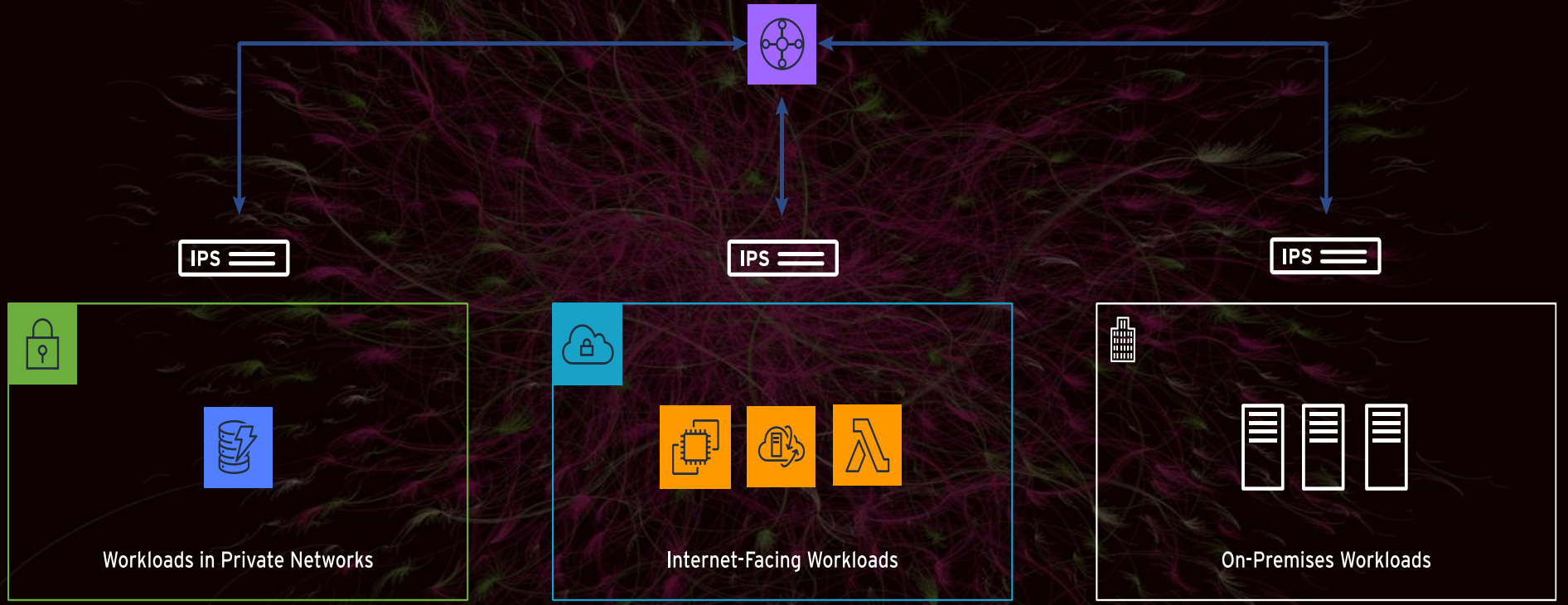
Fewer moving pieces

- 네트워크 환경에 맞게 효과적으로 In/Out 트래픽 검사
- 단일 EC2 VPC / Instance로 Load Balancer 필요 없음

Flexible

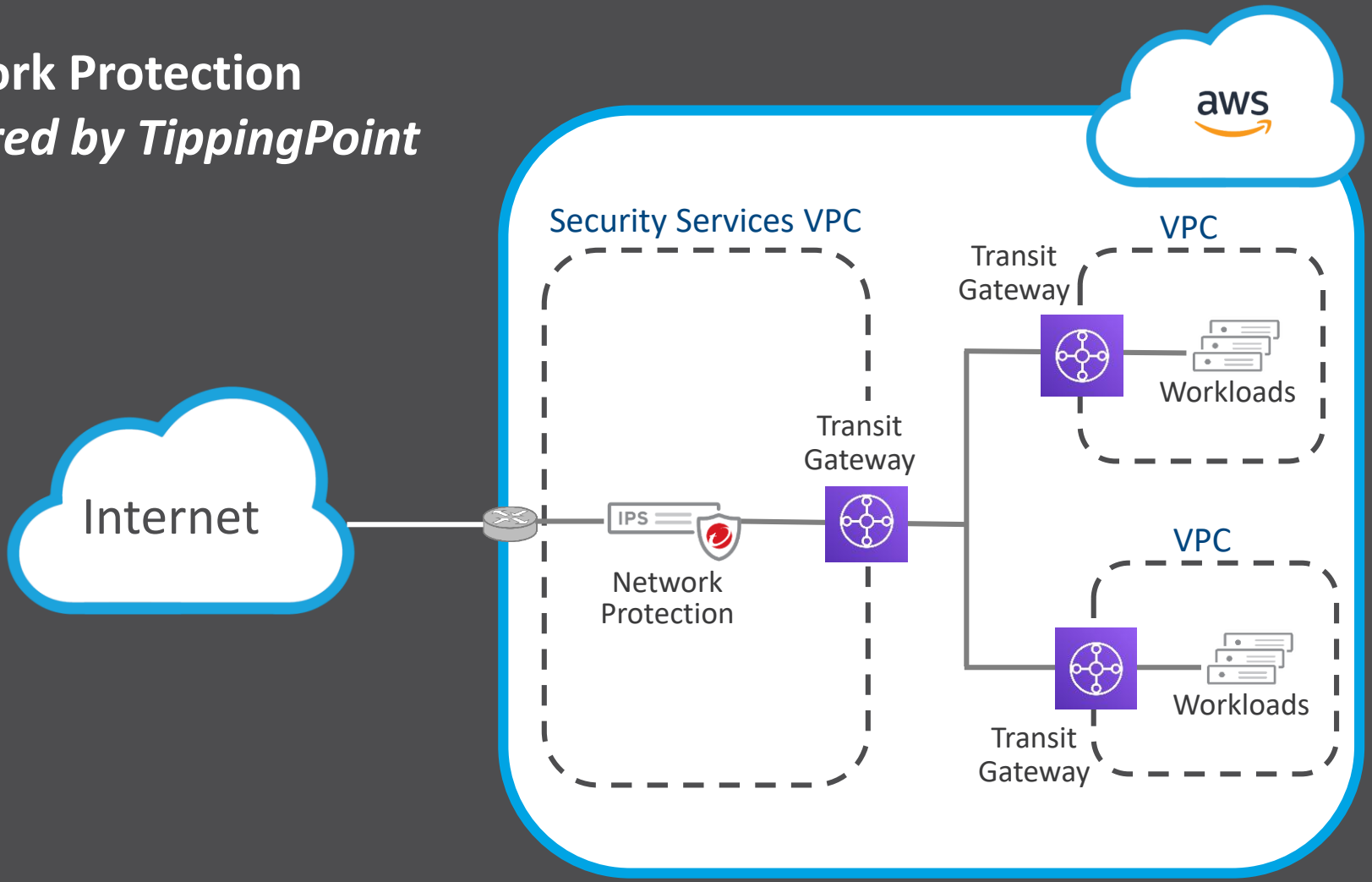
- AWS Transit-Gateway를 통해 인라인 형태로 초기 구성
- 유연한 라이선스 체계 지원

기존 Cloud IPS 구성

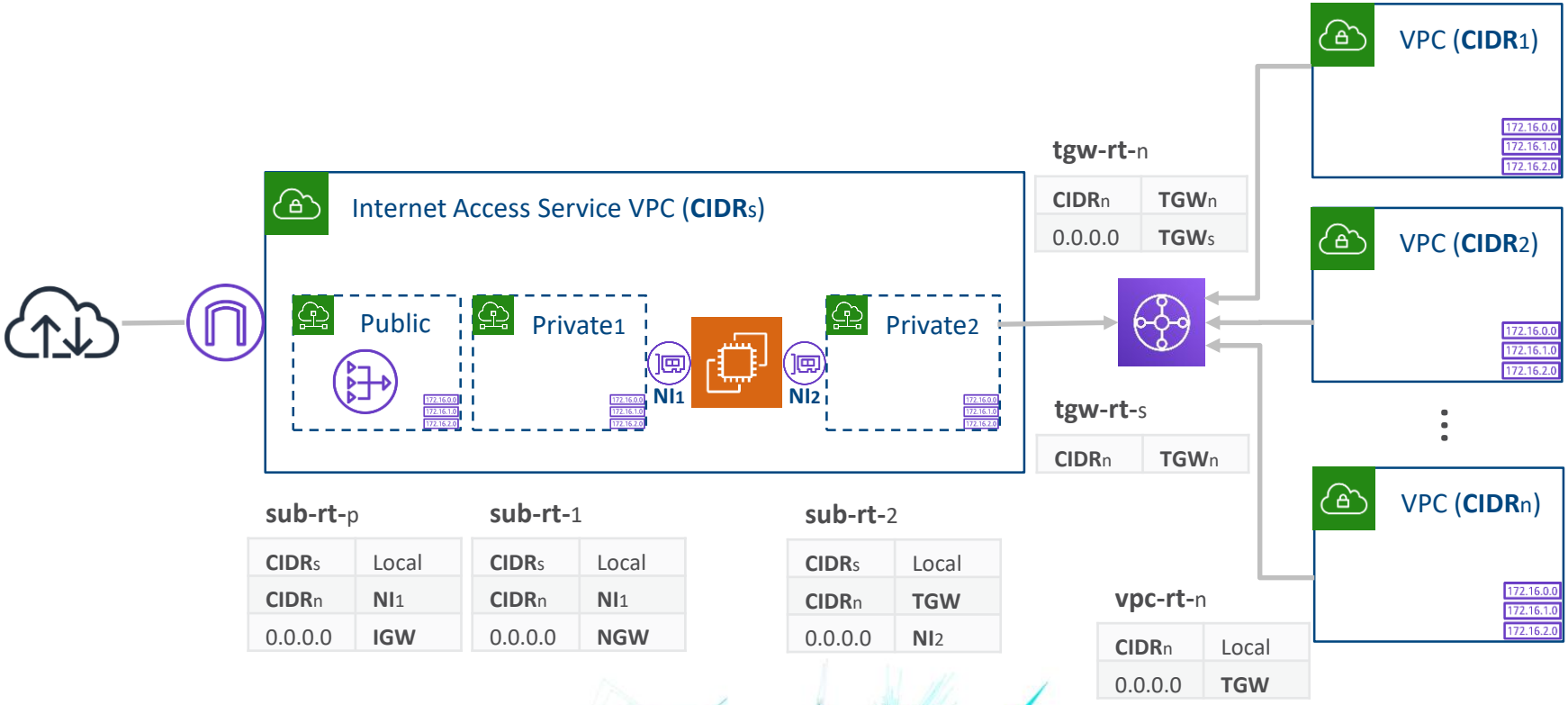


TippingPoint Cloud IPS 구성

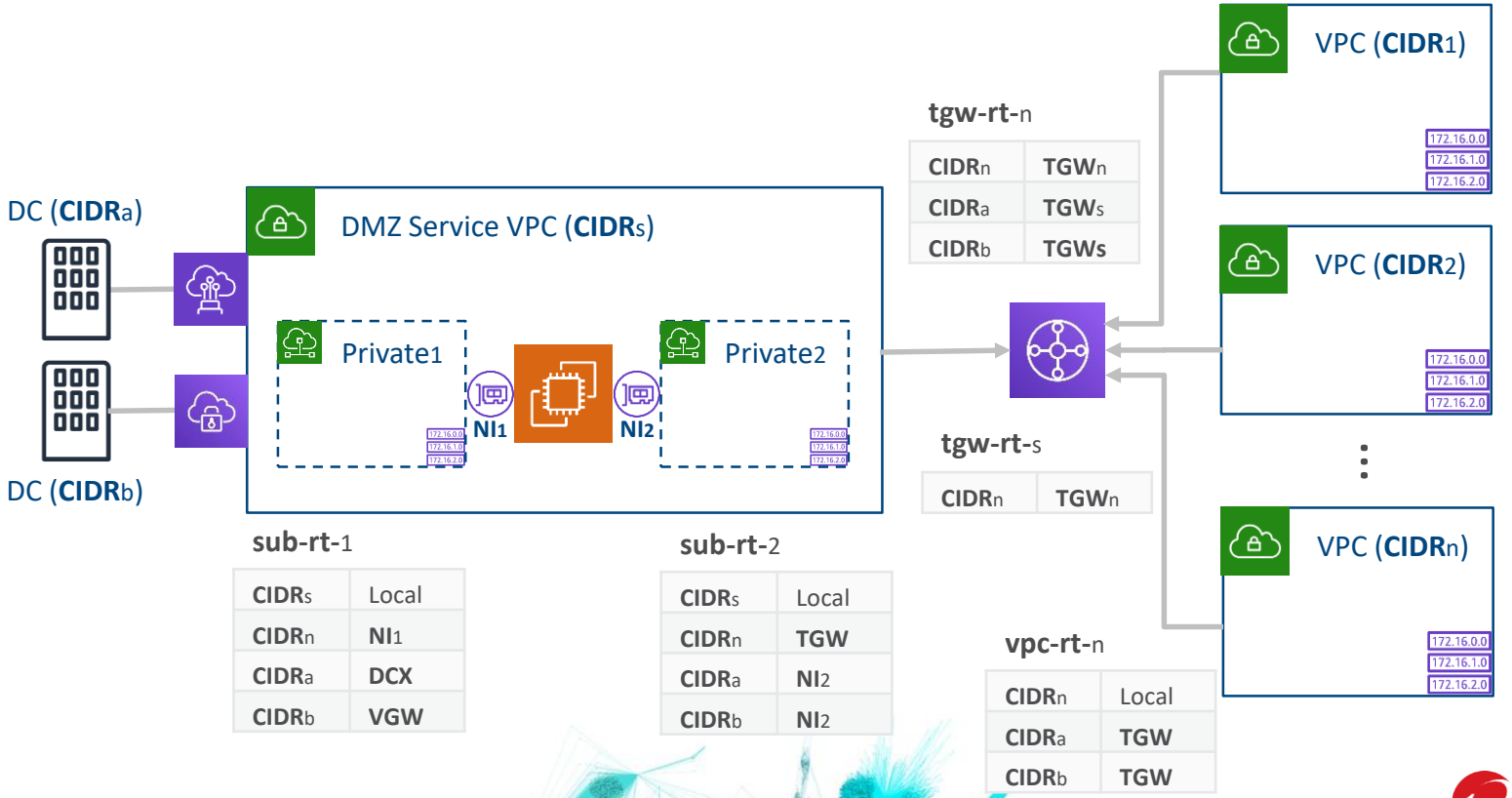
Network Protection
powered by TippingPoint



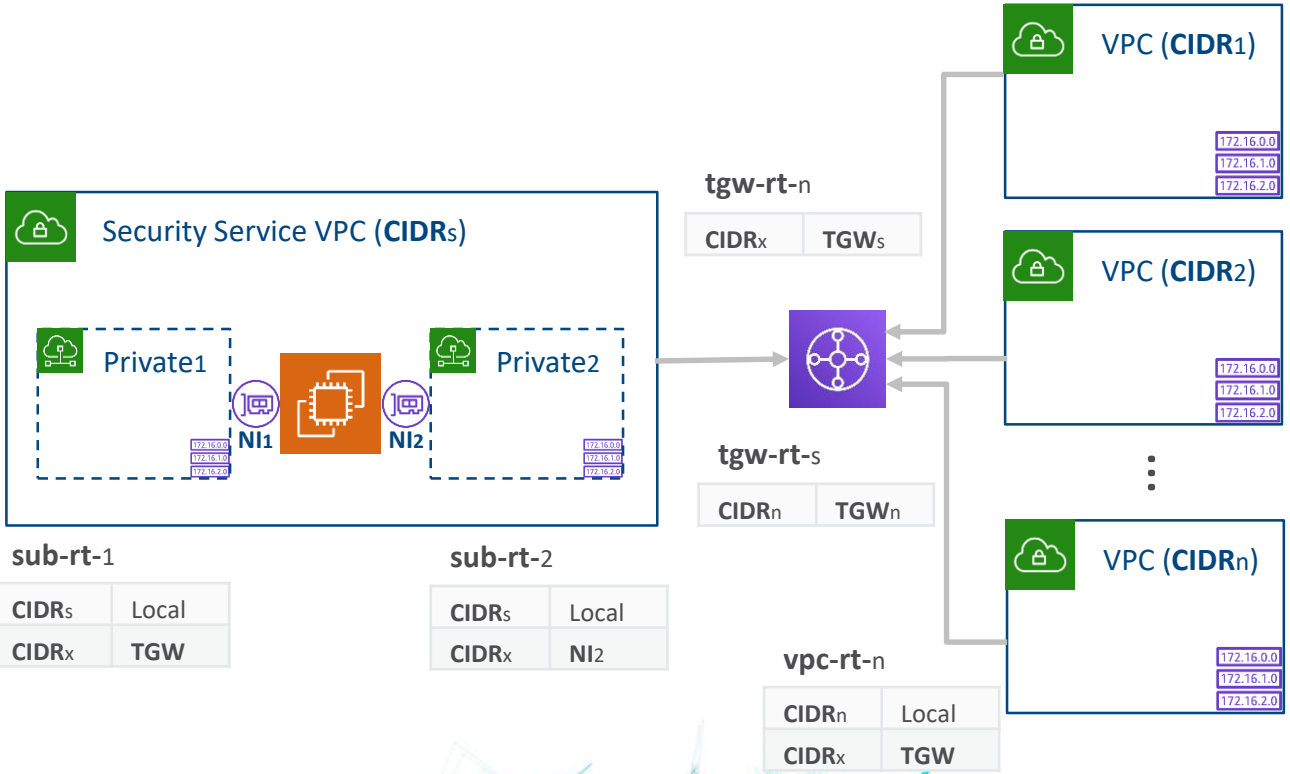
Internet Access IPS Solution Architecture



Hybrid Cloud DMZ IPS Solution Architecture



Inter-VPC IPS Solution Architecture



Trend Micro Threat Intelligence

TippingPoint Key Technologies

- **Pro-active Threat Defense:**
  DVLabs 및 Zero Day Initiative를 통하여 최신 보안취약점(Zero-day Vulnerability)으로부터 네트워크 및 중요 자산 보호
- **평판기반의 Threat Defense:**
  Score 기반으로 악성 IP & DNS에 대한 통신 제어
- **멀웨어 Threat Defense:**
  멀웨어, 랜섬웨어, C&C 통신 방어 및 Machine Learning 필터 탐지
- **Enterprise Vulnerability Remediation(eVR):**
  취약점들을 DV위협 인텔리전스에 매핑시켜, 즉각적인 조치를 취함으로써 보안 범위를 극대화하고 가상 네트워크 패치로 치료
- **위치 기반 / User ID 기반 제어**
  인텔리전스 방어 기법인 위치 정보, User ID 기반의 접근 제어
- **사용자 정의 필터**
  손쉬운 사용자 정의 필터 제작 방식 제공, Snort Rule Convertor를 이용한 보안 필터 제작 및 보안성 향상
- **TippingPoint 및 Deep Discovery 통합 기능**
  TippingPoint와 TrendMicro의 ATP 솔루션인 Deep Discovery의 연동으로 보안성 극대화

Zero Day Initiative

ZERO DAY INITIATIVE

Global Vulnerabilities Research Result

- Total Vulnerabilities by Disclosing

ZERO DAY INITIATIVE

***+ 42% YoY**: busiest year ever!*

*Over **1400** advisories in 2018, over 5500 to date*

- 전 세계 80개국 이상에서 3,000명 이상의 Zero-day 취약점 전문 연구 인력 활동
- 전반적 산업 분야의 가장 많은 신규 취약점을 발견하고 TippingPoint를 통해 가장 신속한 대응을 제공
- ZDI 주최의 Pwn2Own 해킹 대회 운영 및 참여 규모 확대

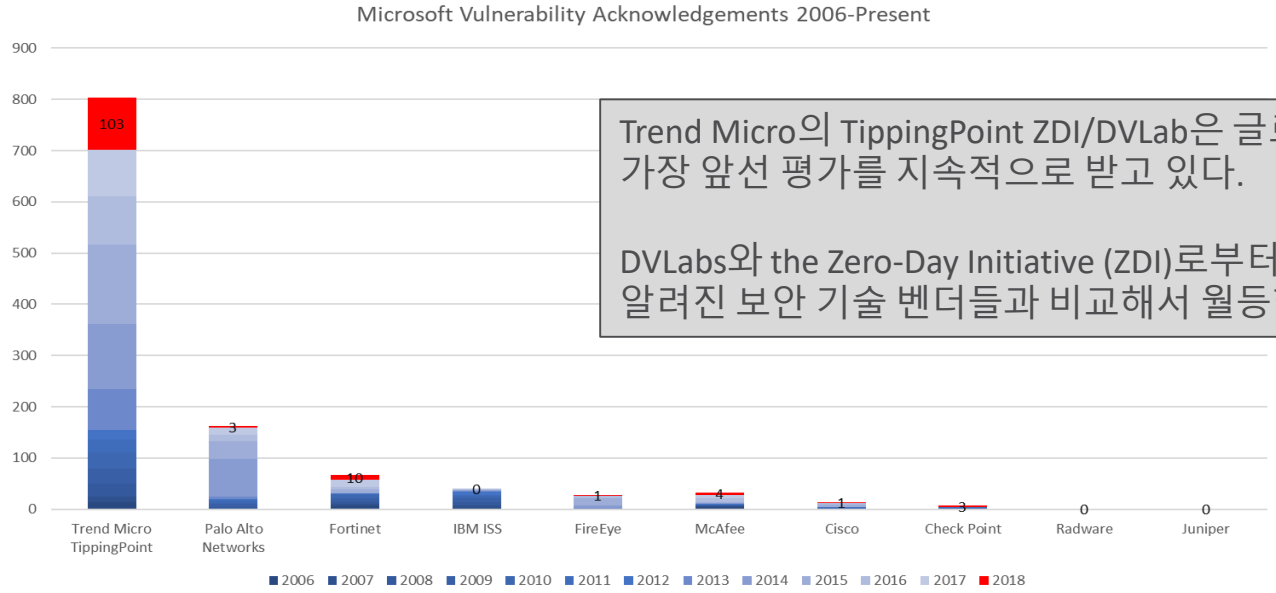
TREND MICRO

Zero Day Initiative

ZERO DAY INITIATIVE

Global Vulnerabilities Research Result

*- Microsoft Vulnerability Acknowledgments Since 2006**



Trend Micro의 TippingPoint ZDI/DVLab은 글로벌 취약점 리서치 기관 중 가장 앞선 평가를 지속적으로 받고 있다.

DVLabs와 the Zero-Day Initiative (ZDI)로부터 발견된 Microsoft 취약점은 알려진 보안 기술 벤더들과 비교해서 월등한 수치를 보여주고 있다.

 # 2006년 이후로 Microsoft 취약점 발견 수에 대한 보안 인텔리전스 기관별 비교

*From publicly available data at https://portal.msrc.microsoft.com/en-us/security-guidance/acknowledgments as of October 1, 2018

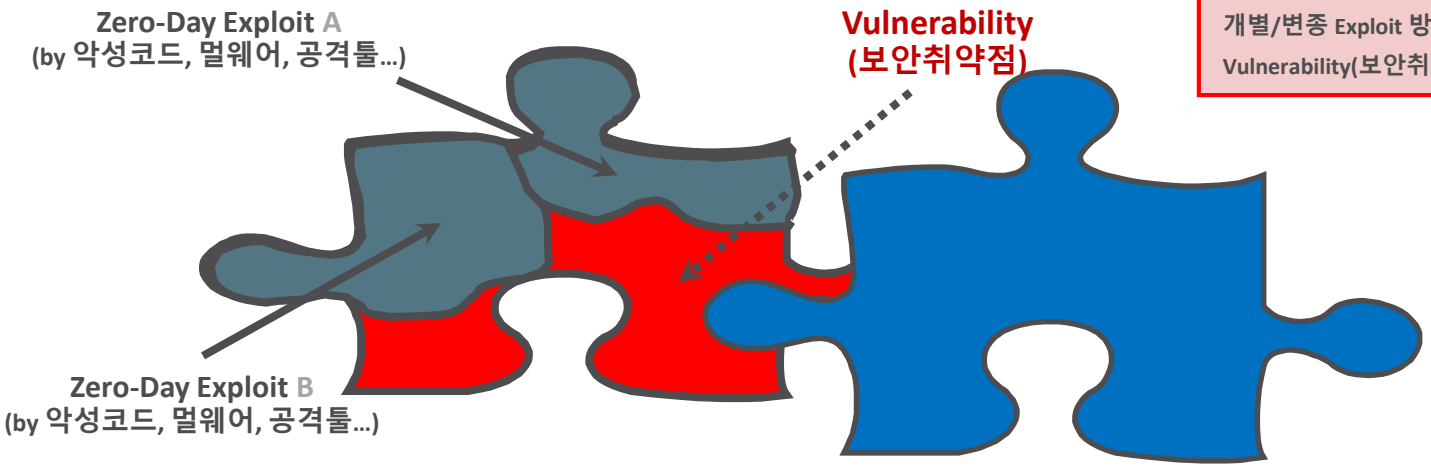
TREND MICRO

TippingPoint 특장점

Vulnerability-generic(보안취약점 방어) 기반의 Signatures

- Smart 한 대응 방안 -

개별/변종 Exploit 방어보다 원천적인 Vulnerability(보안취약점) 방어가 중요!



타사 IDS/IPS의 보안 필터/시그니처:

- 특정한 Exploit만 처리하도록 작성됨.
- 성능의 이유로 최대한 "일반적인" 보안 필터/시그니처 제작 및 배포

TippingPoint의 보안 필터/시그니처:

- 보안취약점 방어 기반의 보안 필터/시그니처를 통한 원천적인 보안취약점을 정확하게 방어함으로써 미탐/과탐 또는 오탐율 최소화 및 성능 극대화

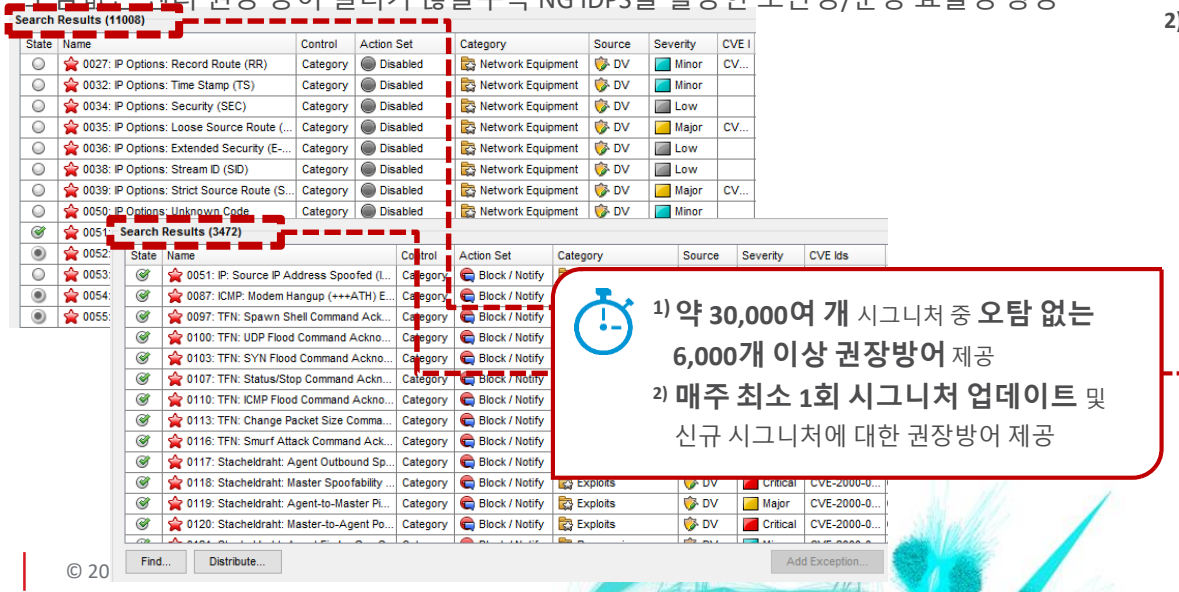
TippingPoint 특장점

Standard first-generation signature

새로운 위협에 대한 신속한 대응 및 설치 지원, Zero-Day 공격 방어, 네트워크 성능에 저하가 없는 공격 탐지/방어

- TippingPoint 보안취약점 발견/연구 성과에 의해 실시간 제로데이 공격 방어
  → NG IDPS 기술검토시, **제조사별로 알려지지 않은 보안취약점 발견/연구 성과 및 실적 검증 필요**
- **매주 최소 1회씩 보안업데이트** 제공을 통한 보안성 극대화,
- 주간 **시그니처 업데이트시 오탐없이 즉시 방어 가능한 벤더 권장 방어정책 제공 여부 검증 필요**
  오탐없는 벤더 권장 방어 필터가 많을수록 NG IDPS를 활용한 보안성/운용 효율성 향상

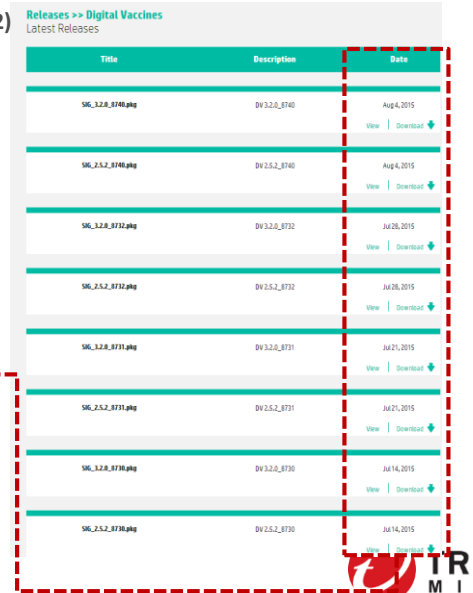
1)



1) **약 30,000여 개** 시그니처 중 **오탐 없는 6,000개 이상 권장방어** 제공

2) **매주 최소 1회 시그니처 업데이트** 및 신규 시그니처에 대한 권장방어 제공

2)



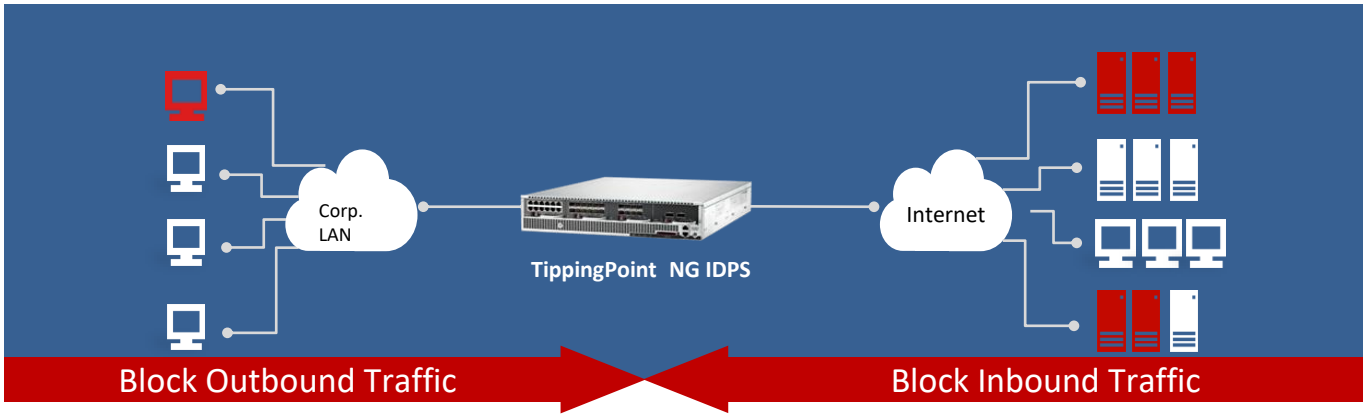
TippingPoint 특장점

Context awareness, Threat intelligence service

보안 인텔리전스(위치 정보, User ID, **평판 정보** 등)를 활용한 네트워크 접근 제어 및 탐지/차단

평판 보안 인텔리전스 활용을 통한 보안 위협 식별 및 방어 결정 능력 향상

- 전 세계에 설치된 수천 개의 센서로 인터넷 상의 봇넷 및 악성 공격자 추적
- DVLabs, ZDI를 통한 취약점 분석 및 위협 사전 대응 필터 개발 & "악성 IP/도메인"에 대한 평판 DB 업데이트
- 외부 기관과의 공조(Malware Domain List, Emerging Threats, Sunbelt, Esoft, SANS..) 를 통한 Reputation Data 추가 확보



- Botnet, Trojan 다운로드 차단
- Malware, Spyware, & Worm, 악성코드 다운로드 차단
- Botnet 명령 제어 사이트로의 접근 차단
- Phishing 사이트로의 접근 차단

- 스팸 / 피싱 이메일 차단
- 좀비 PC 감염 예방
- 웹 어플리케이션 대상 공격 방어

감사합니다