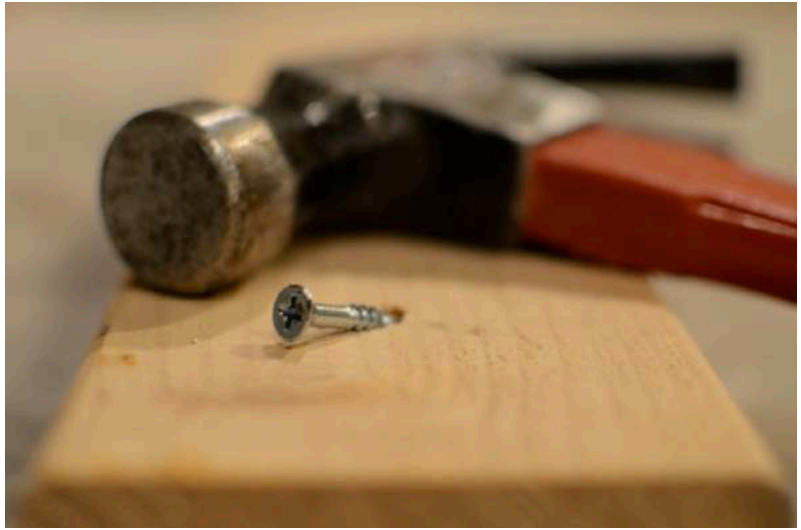
APT 공격 이제는 다른 각도로 볼수 있어야 합니다.

Seong Cheol(Bruce) Lee
May 2016

ATP(Advanced Persistent Threat)가 Cyber Security Radar에 포착



침투 … 검색 … 수집 … 유출

Preparation	Intrusion	Active Breach

1. Reconnaissance
Harvest information to create attack strategy and toolset

2. Weaponization
Coupling exploit with backdoor into deliverable payload

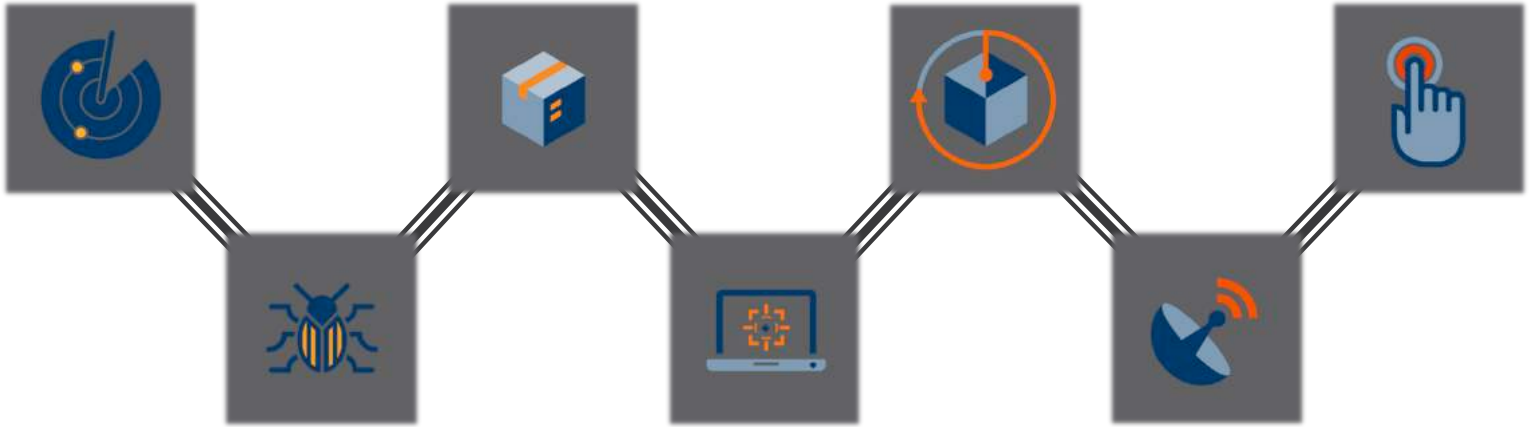
3. Delivery
Delivering weaponized bundle to the victim via email, web, USB, etc.

4. Exploitation
Exploiting a vulnerability to execute code on victim's system

5. Installation
Installing malware on the asset

6. Command & Control
Command channel for remote manipulation of victim's system

7. Actions on Objectives
With 'Hands on Keyboard' access, intruders accomplish



Based on Lockheed Martin's Cyber Kill Chain

SCADA 공격

Trans-Siberian Pipeline Explosion (1982): Trojan inserted into SCADA software that caused explosion

Sewage Dump (2000): Insider attack on sewage systems in Australia; Dumps 1 million gallons of raw sewage

Slammer (2003): Knocks nuclear monitoring system offline; Cripples airlines and 911

California Canal System (2007): Insider hacks SCADA systems

1982|...|1994|…|1999|2000|…|2003|…|2006|2007|2008|2009|2010

STUXNET

Roosevelt Dam (1994): Hacker breaks into floodgate SCADA systems

GAZPROM (2000): Hackers gain control of Russian natural gas pipeline

Stuxnet Ring Runs First SCADA operations (2009): Early proof-of-concept attacks launched and detected

1st Generation ATP 공격 방어

Harvest information to create attack strategy and toolset

- OS, AV, Applications
- Ports, Personal Information

클라이언트 통신 차단

해당 클라이언트 격리

치료(??)

멀티포트 / 멀티 프로토톨 행위 기반 활성**Botnet**
▪ Viruses Malware Spyware ▪ Bandwidth attacks ▪ Inadvertent and/or malicious data leakage ▪ Compliance regulation violations

Sandbox의 출현

위협적인 공격 방법

	Watering hole	Spear phishing	Dropper
Approach	Infect or inject a trusted site	Target users through compromised links	Deliver malware with stealth and self-deleting programs
Tactic	Conduct reconnaissance on a target	Leverage social engineering	Gain access through DLL injection and control firewalls, antivirus, ect
Impact	Deliver an exploit that will attack	Deliver an exploit that will attack	Compromises system control, personal data and authorizations
Threat vector			

2nd Generation ATP 공격 방어

악성 URL & C&C

신종 변종 악성코드 위험

제로데이 APT공격위협

모바일

Exploit

URL 분석 차단

최고 성능의 VM 성능

자체 개발 VM / 상용 VM

하루에 50개의 Suspicious Files -> Malware pattern (내가 잡고 니가 막아죠^^)

무엇을 바꾸면 될까요?

Get your head out of the sandbox …

차세대 APT 공격 방어의 고려 대상

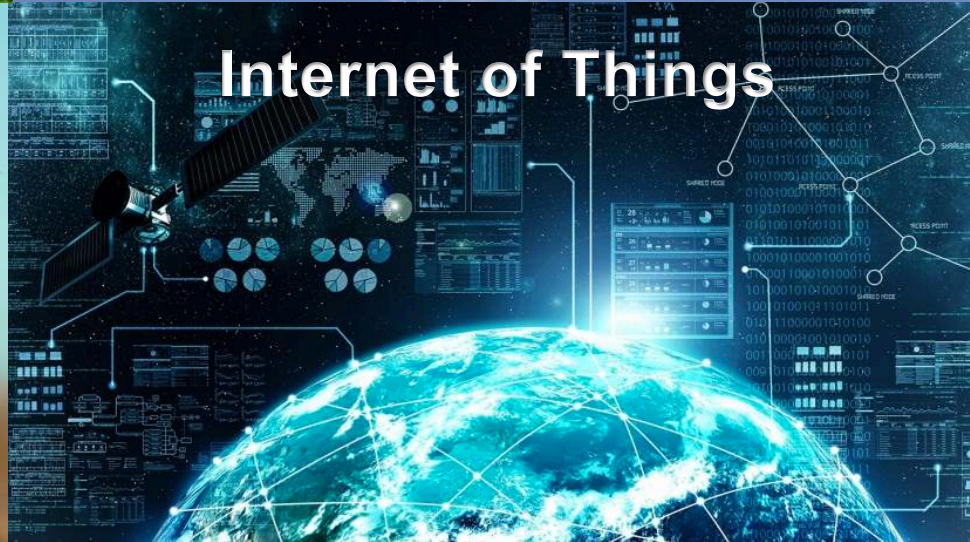
- 샌드박스는 클라우드, On-Premise를 지원
- 다양한 오픈 플랫폼 지원(기존 운영 시스템과의 연동)
- 실시간 업데이트 되는 위협 분석 시스템 지원
- 회귀적 분석 (Point-In-Time and Retrospective)

Every Country, City, Government, and Business Will Become Digital


Existing Viewpoint
for Security


Public Cloud


Mobility


Internet of Things

The Industry Has You Covered…

54

특정 고객이 사용하고 있는 전체 보안 관련 제품 제조사 수

Source: Momentum Partners.

자료출처 : 시스코 2016 연례 보안 보고서

사이버보안 인프라 및 체계 확신 감소 추세

59%
최근 기술에 대한 신뢰도
-5%

51%
보안 취약점의 지능적인 탐지 능력에 대한 확신
0%

54%
방어 능력에 대한 확신
-4%

45%
공격 억제 범위의 산정 및 식별 능력에 대한 확신
-1%

54%
공격 검증 능력에 대한 확신
+0%

56%
정기적인 보안 정책에 대한 리뷰
+0%

자료출처 : 시스코 2016 연례 보안 보고서

3세대 APT 공격 방어

Pervasive
Integrated
Continuous
Intelligent
Open

Pervasive

④ Human♪

＋

② Network♪

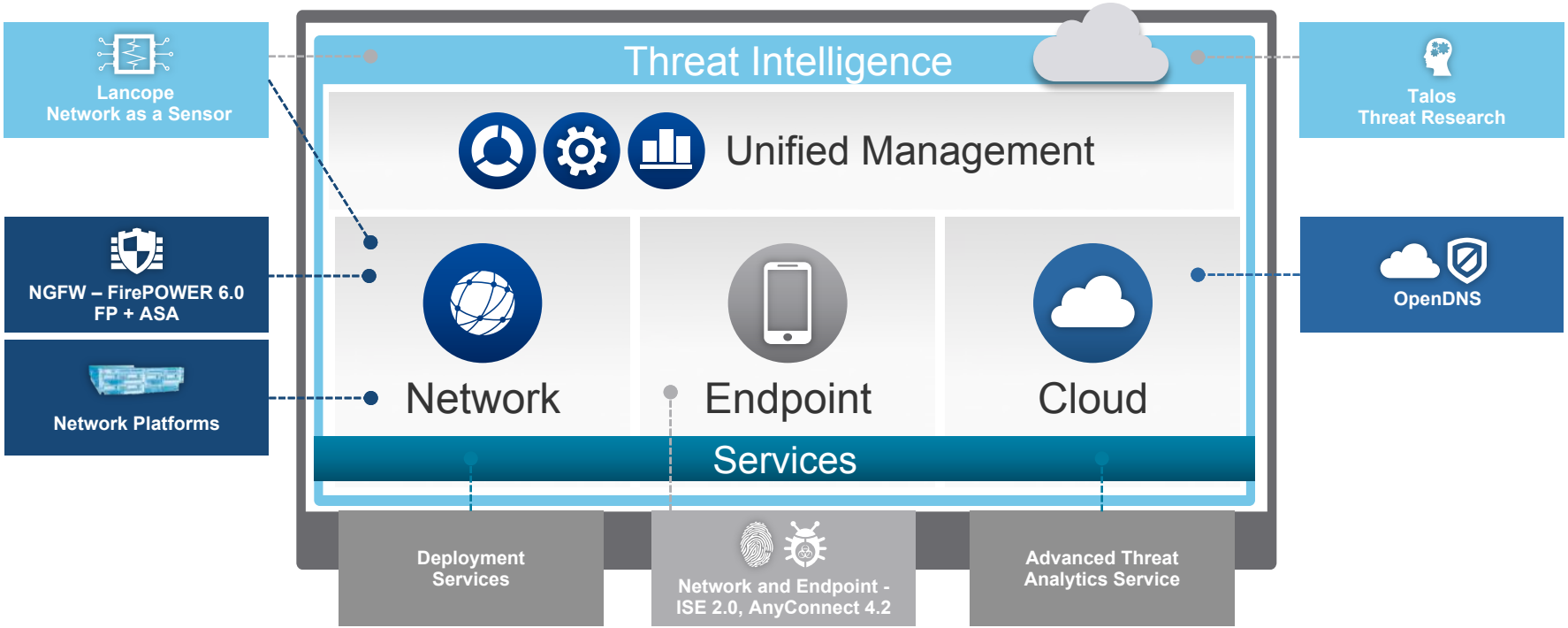
＋

① Security♪

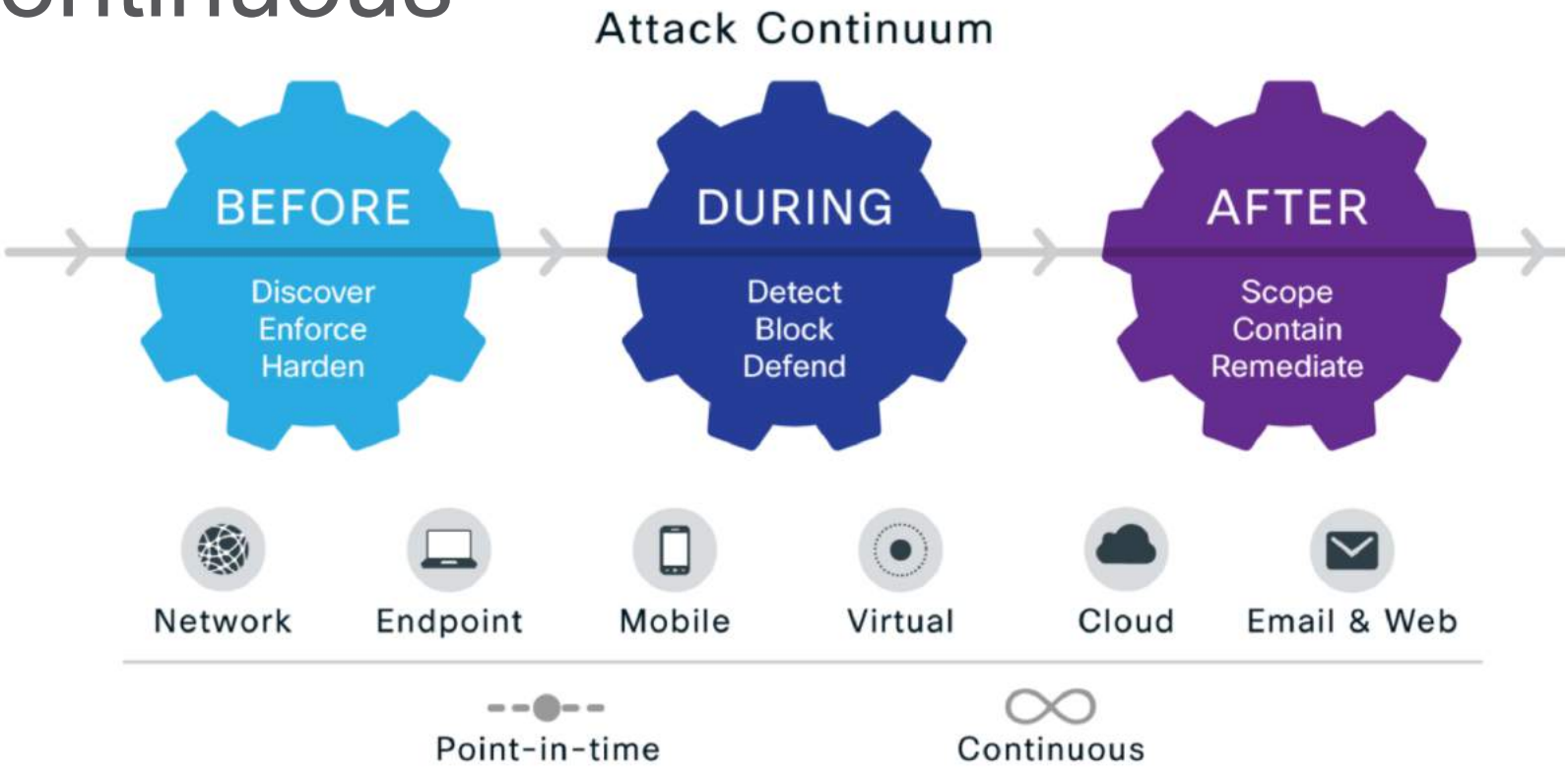
＋

③ Physical Security♪

Investment and Integration to Simplify Security



Continuous



Intelligent
Next Generation Analytics

Big Data♪

+

Real-time♪

+

Machine Learning♪

TALOS

*PayPal FDS (Fraud Detection System)

Open

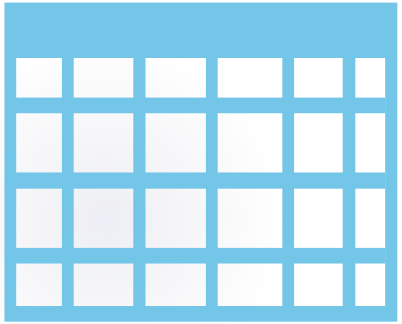
OpenDNS

SOURCEfire®

SNORT™

Game Changing Innovation

Industry
100
DAYS



VS.

Cisco
Less than
1 Day

Reduced Time to Detection

Source: Cisco Annual Security Report, 2016

Cisco의 전방위 보안 솔루션

Security Extended	OpenDNS	Cloud Access Security	Security Consulting
일반적인 네크워크보안	FW/NG-FW	NG-IPS	AMP Advanced Malware Protection
네트워크기반 보안	STEALTH WATCH By Lancope	ISE	

보안통합 & 자동화

보안 통합 & 자동화

기존 보안 투자 인프라 활용을 극대화

- ThreatGRID의 REST API는 sample 분석, 축재 및 보고를 자동화
  - 수 많은 기술을 이용하여 sample 제공 자동화 (host or network)
  - 수 많은 기술의 내부로 결과를 끌어옴

다양한 시스템과의 연동 제공(Open Platform)

Technology Partnerships

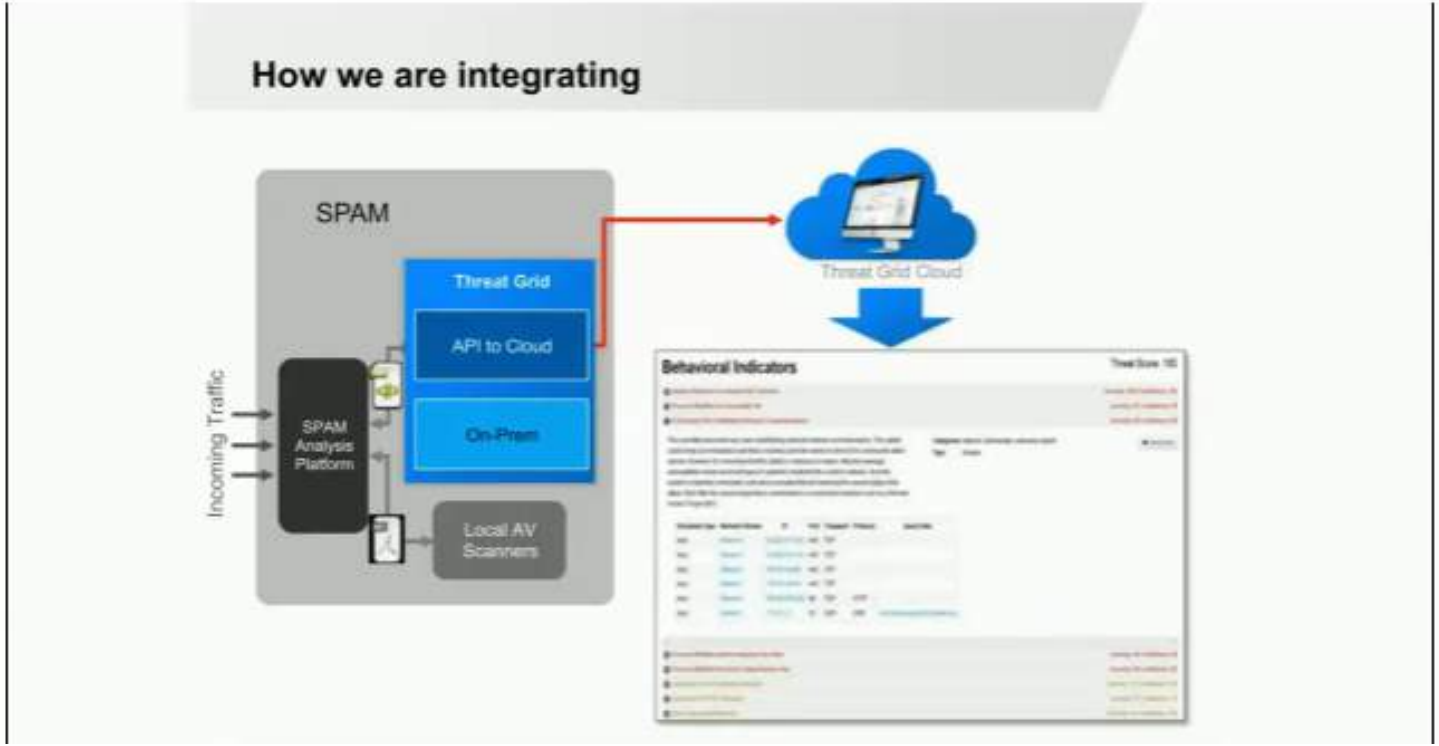
ThreatGRID 와 통합하거나 파트너가 되어 있는 조직

RSA
Guidance SOFTWARE
IBM Radar
tenable network security
GENERAL DYNAMICS Fidelis Cybersecurity Solutions
MALFORMITYLABS
splunk>
AccessData
BlueCoat
REVERSING LABS
invincea
McAfee
SOURCEfire
Palantir
hp ArcSight

현재 50% 정도에서 2016년 경에는 전체 보안제안의 85%가 조직화, 상황인식 기반으로 이루어 지고 보안 인텔리전스 피드가 표준기능으로 포함될 것이다.

Source: Gartner, "Predicts 2014: Security Solutions," November 2013

스팸메일시스템의 APT고도화



Cisco Security Integration with Threat Intelligence

Built on Unmatched Collective Security Analytics

Threat Intelligence

Email | Endpoints | Web | Networks | IPS | Devices

1.6 million global sensors	**35%** worldwide email traffic
100 TB of data received per day	**13 billion** web requests
150 million+ deployed endpoints	**24x7x365** operations
600+ engineers, technicians, and researchers	**40+** languages

Cisco® Talos

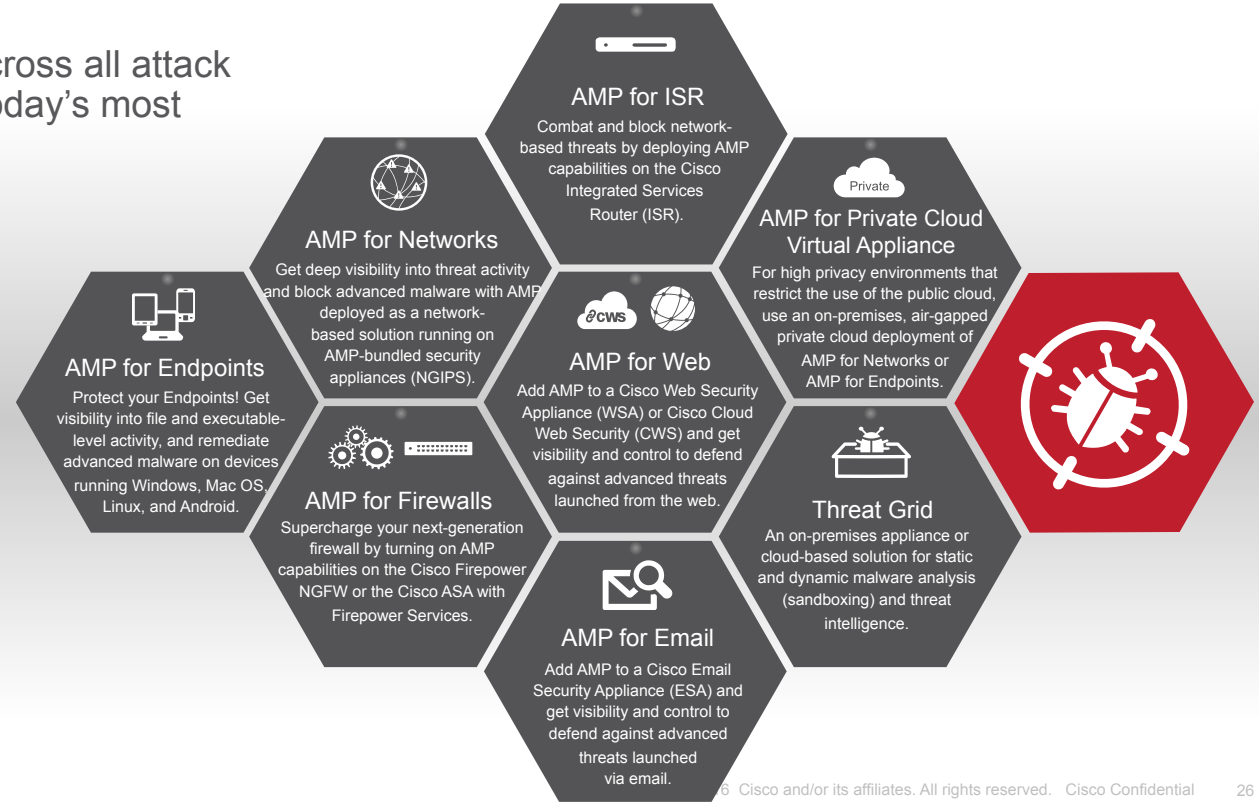
+ AMP ∞ Advanced Malware Protection

Research Response

- 180,000+ file samples per day
- FireAMP™ community
- Advanced Microsoft and industry disclosures
- Snort and ClamAV open source communities
- Honeypots
- Sourcefire AEGIS™ program
- Private and public threat feeds
- Dynamic analysis

Cisco Advanced Malware Protection (AMP)

Get Visibility and Control across all attack vectors to defend against today's most advanced threats.



OpenDNS
Leveraging a Single Global Recursive DNS Service

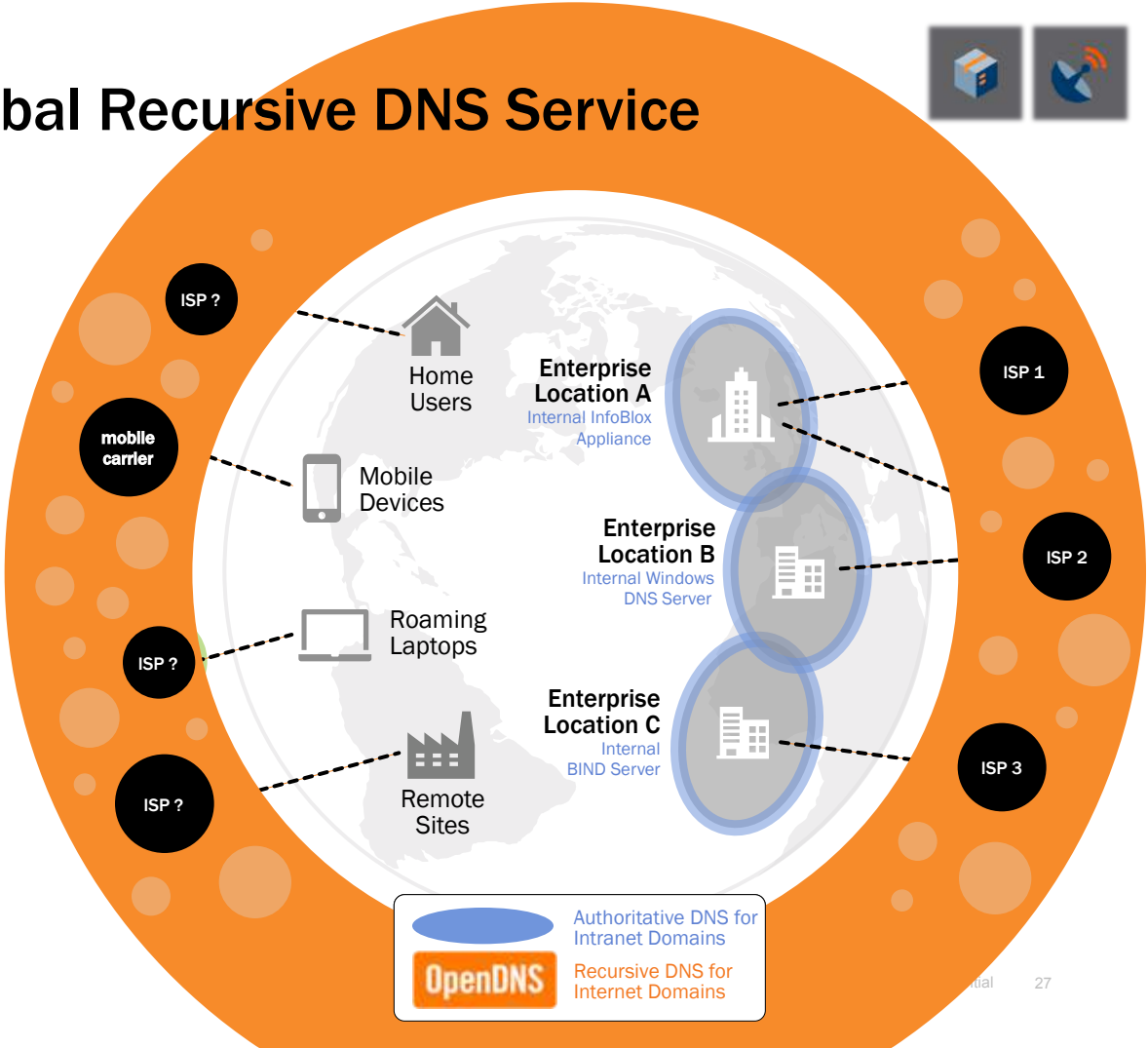
BENEFITS

Global Internet Activity Visibility

Network Security w/o Adding Latency

Consistent Policy Enforcement

Internet-Wide Cloud App Visibility



CISCO