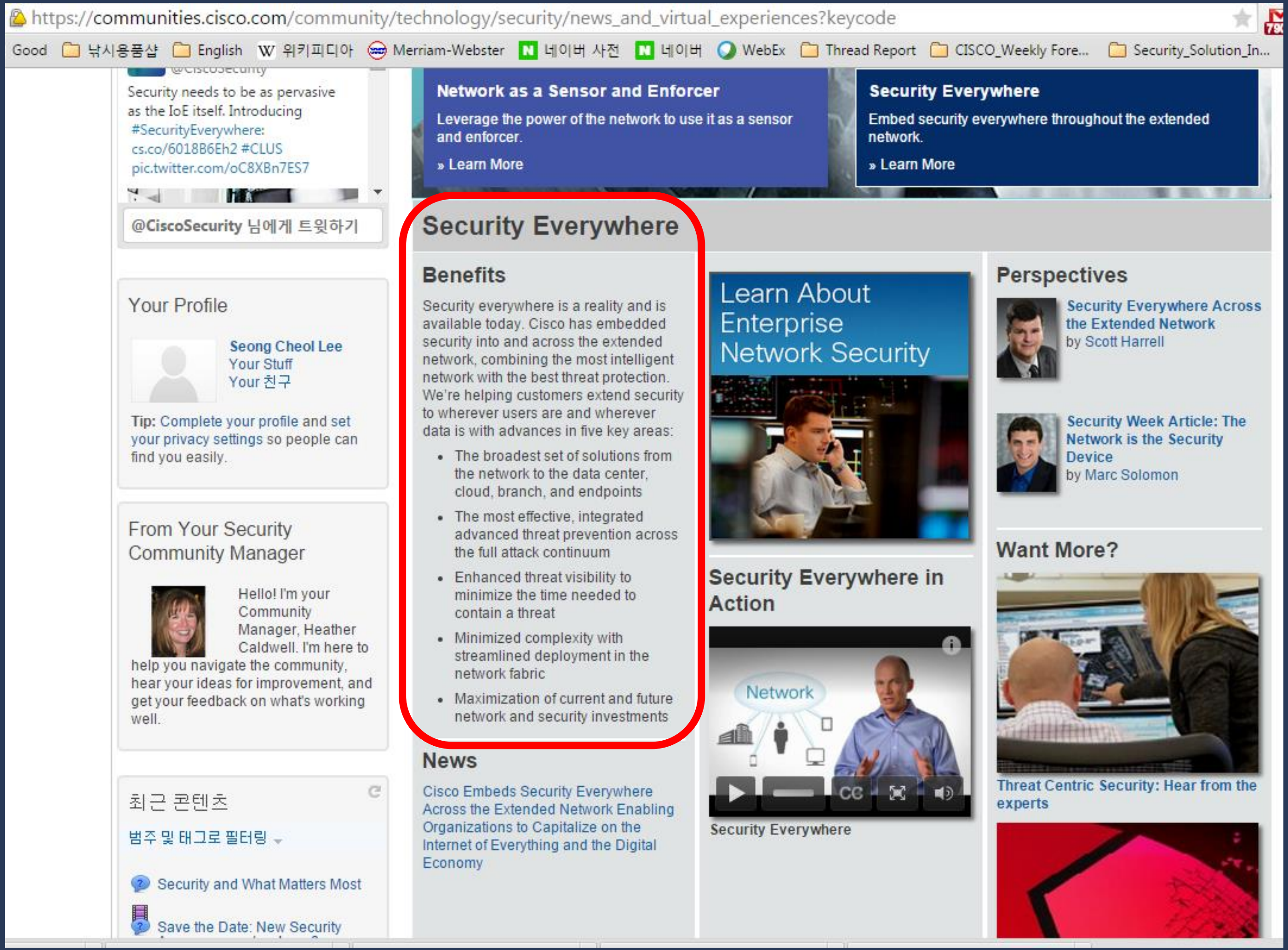
이제 지능형 위협 공격의 생각을 바꿀 때 입니다.

이성철이사
lscbruce@cisco.com
Cisco Systems Korea,GSSO

New Released



https://communities.cisco.com/community/technology/security/news_and_virtual_experiences?keycode

@CiscoSecurity

Security needs to be as pervasive as the IoE itself. Introducing #SecurityEverywhere: cs.co/6018B6Eh2 #CLUS pic.twitter.com/oC8XBn7ES7

@CiscoSecurity 님에게 트윗하기

Network as a Sensor and Enforcer

Leverage the power of the network to use it as a sensor and enforcer.

» Learn More

Security Everywhere

Embed security everywhere throughout the extended network.

» Learn More

Your Profile

Seong Cheol Lee
Your Stuff
Your 친구

Tip: Complete your profile and set your privacy settings so people can find you easily.

From Your Security Community Manager

Hello! I'm your Community Manager, Heather Caldwell. I'm here to help you navigate the community, hear your ideas for improvement, and get your feedback on what's working well.

최근 콘텐츠

범주 및 태그로 필터링

Security and What Matters Most

Save the Date: New Security

Security Everywhere

Benefits

Security everywhere is a reality and is available today. Cisco has embedded security into and across the extended network, combining the most intelligent network with the best threat protection. We're helping customers extend security to wherever users are and wherever data is with advances in five key areas:

- The broadest set of solutions from the network to the data center, cloud, branch, and endpoints
- The most effective, integrated advanced threat prevention across the full attack continuum
- Enhanced threat visibility to minimize the time needed to contain a threat
- Minimized complexity with streamlined deployment in the network fabric
- Maximization of current and future network and security investments

News

Cisco Embeds Security Everywhere Across the Extended Network Enabling Organizations to Capitalize on the Internet of Everything and the Digital Economy

Learn About Enterprise Network Security

Security Everywhere in Action

Security Everywhere

Perspectives

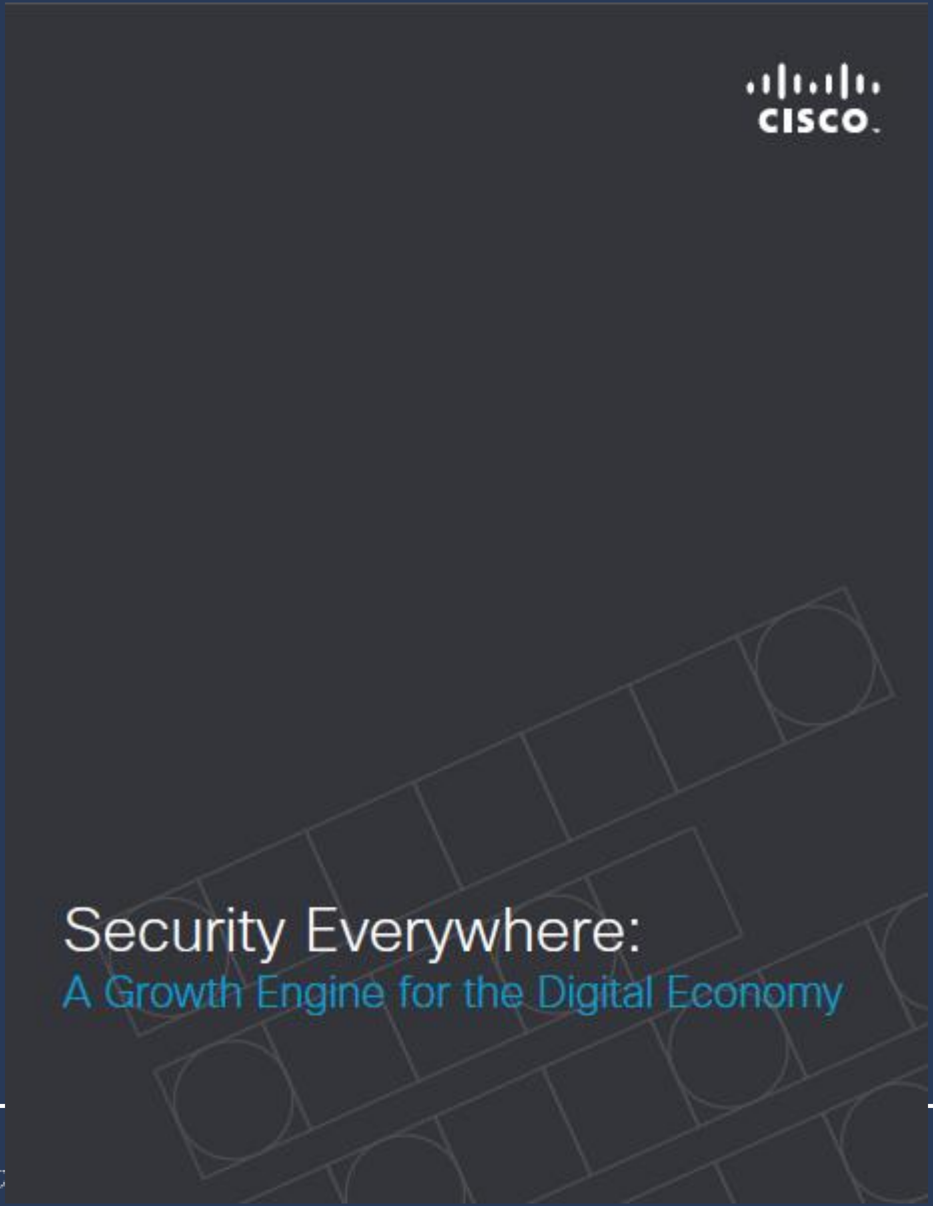
Security Everywhere Across the Extended Network
by Scott Harrell

Security Week Article: The Network is the Security Device
by Marc Solomon

Want More?

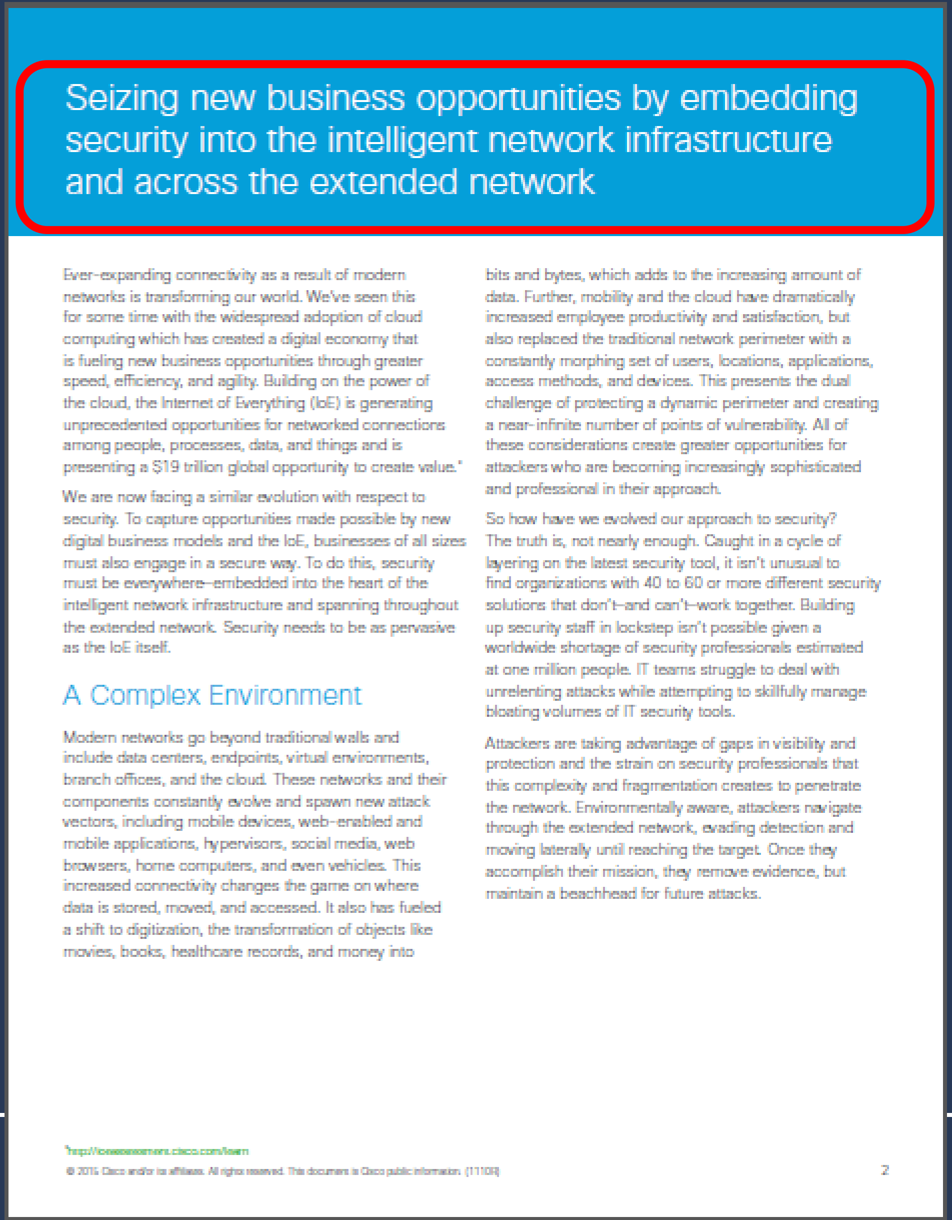
Threat Centric Security: Hear from the experts

Security Everywhere



Security Everywhere:

A Growth Engine for the Digital Economy



Seizing new business opportunities by embedding security into the intelligent network infrastructure and across the extended network

Ever-expanding connectivity as a result of modern networks is transforming our world. We've seen this for some time with the widespread adoption of cloud computing which has created a digital economy that is fueling new business opportunities through greater speed, efficiency, and agility. Building on the power of the cloud, the Internet of Everything (IoE) is generating unprecedented opportunities for networked connections among people, processes, data, and things and is presenting a $19 trillion global opportunity to create value.[1]

We are now facing a similar evolution with respect to security. To capture opportunities made possible by new digital business models and the IoE, businesses of all sizes must also engage in a secure way. To do this, security must be everywhere–embedded into the heart of the intelligent network infrastructure and spanning throughout the extended network. Security needs to be as pervasive as the IoE itself.

A Complex Environment

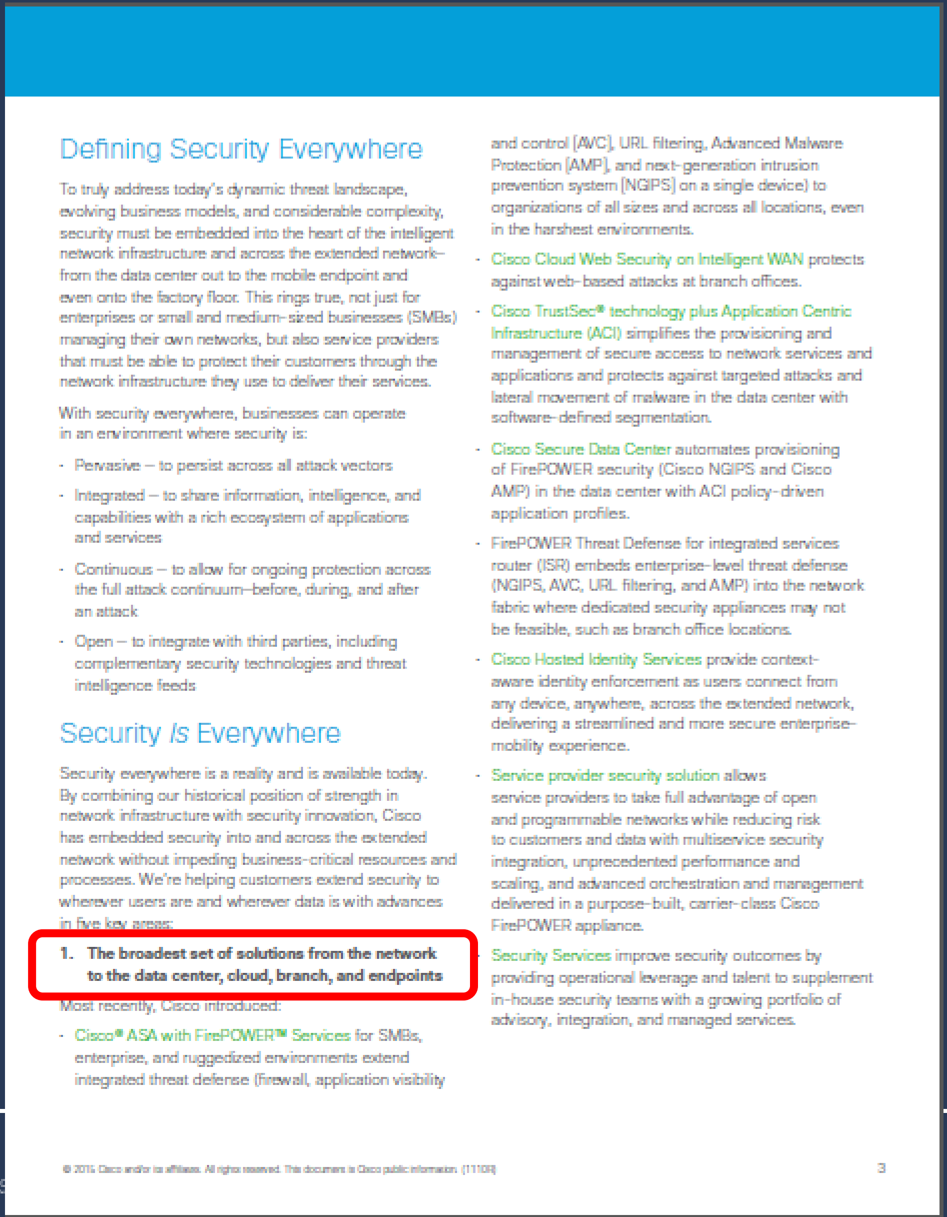
Modern networks go beyond traditional walls and include data centers, endpoints, virtual environments, branch offices, and the cloud. These networks and their components constantly evolve and spawn new attack vectors, including mobile devices, web-enabled and mobile applications, hypervisors, social media, web browsers, home computers, and even vehicles. This increased connectivity changes the game on where data is stored, moved, and accessed. It also has fueled a shift to digitization, the transformation of objects like movies, books, healthcare records, and money into bits and bytes, which adds to the increasing amount of data. Further, mobility and the cloud have dramatically increased employee productivity and satisfaction, but also replaced the traditional network perimeter with a constantly morphing set of users, locations, applications, access methods, and devices. This presents the dual challenge of protecting a dynamic perimeter and creating a near-infinite number of points of vulnerability. All of these considerations create greater opportunities for attackers who are becoming increasingly sophisticated and professional in their approach.

So how have we evolved our approach to security? The truth is, not nearly enough. Caught in a cycle of layering on the latest security tool, it isn't unusual to find organizations with 40 to 60 or more different security solutions that don't–and can't–work together. Building up security staff in lockstep isn't possible given a worldwide shortage of security professionals estimated at one million people. IT teams struggle to deal with unrelenting attacks while attempting to skillfully manage bloating volumes of IT security tools.

Attackers are taking advantage of gaps in visibility and protection and the strain on security professionals that this complexity and fragmentation creates to penetrate the network. Environmentally aware, attackers navigate through the extended network, evading detection and moving laterally until reaching the target. Once they accomplish their mission, they remove evidence, but maintain a beachhead for future attacks.

[1] http://ioeassessments.cisco.com/learn

Security Everywhere (Cont’d)



Defining Security Everywhere

To truly address today’s dynamic threat landscape, evolving business models, and considerable complexity, security must be embedded into the heart of the intelligent network infrastructure and across the extended network–from the data center out to the mobile endpoint and even onto the factory floor. This rings true, not just for enterprises or small and medium-sized businesses (SMBs) managing their own networks, but also service providers that must be able to protect their customers through the network infrastructure they use to deliver their services.

With security everywhere, businesses can operate in an environment where security is:

- Pervasive – to persist across all attack vectors
- Integrated – to share information, intelligence, and capabilities with a rich ecosystem of applications and services
- Continuous – to allow for ongoing protection across the full attack continuum–before, during, and after an attack
- Open – to integrate with third parties, including complementary security technologies and threat intelligence feeds

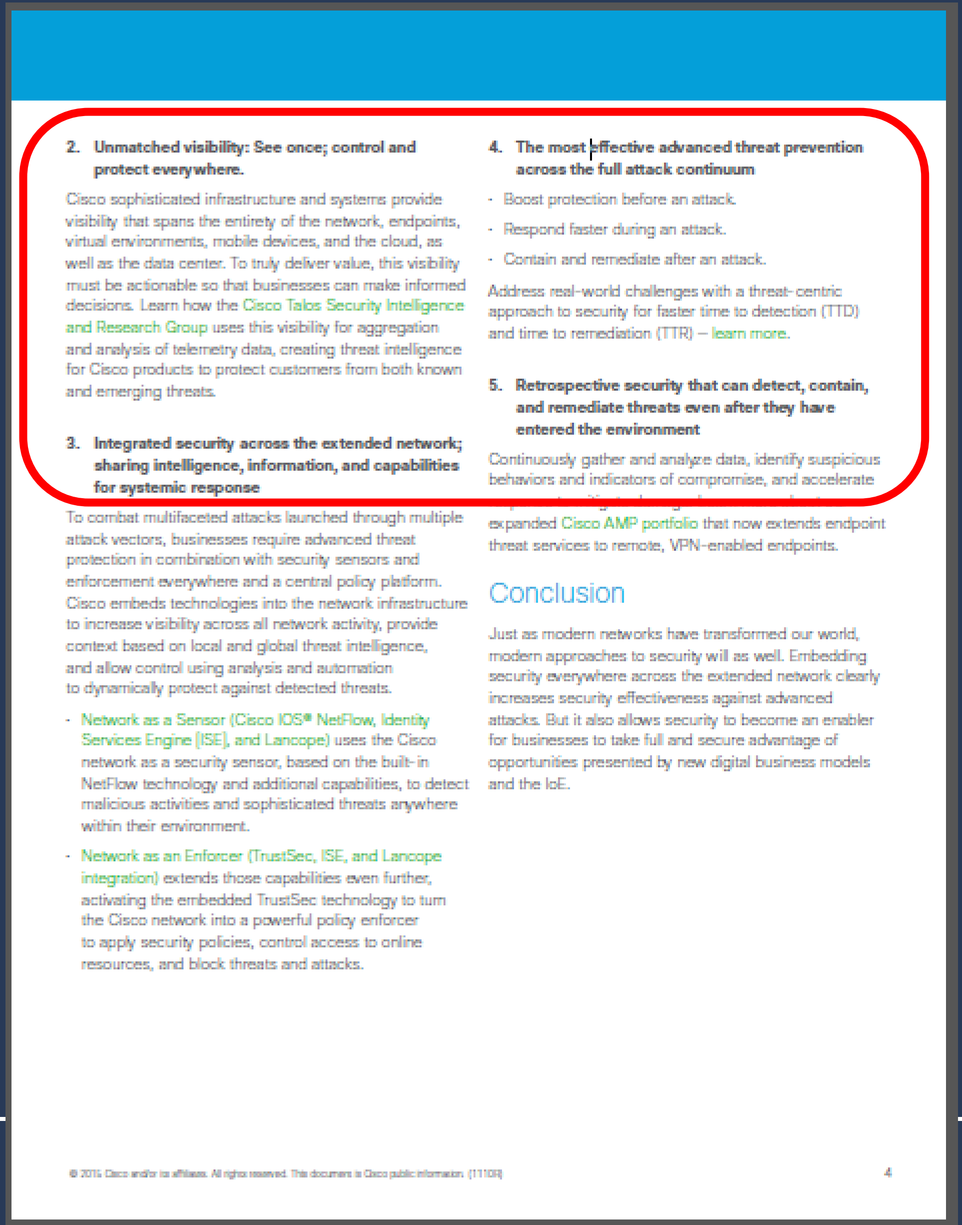
Security *Is* Everywhere

Security everywhere is a reality and is available today. By combining our historical position of strength in network infrastructure with security innovation, Cisco has embedded security into and across the extended network without impeding business-critical resources and processes. We’re helping customers extend security to wherever users are and wherever data is with advances in five key areas:

1. **The broadest set of solutions from the network to the data center, cloud, branch, and endpoints**

Most recently, Cisco introduced:

- Cisco® ASA with FirePOWER™ Services for SMBs, enterprise, and ruggedized environments extend integrated threat defense (firewall, application visibility and control [AVC], URL filtering, Advanced Malware Protection [AMP], and next-generation intrusion prevention system [NGIPS] on a single device) to organizations of all sizes and across all locations, even in the harshest environments.
- Cisco Cloud Web Security on Intelligent WAN protects against web-based attacks at branch offices.
- Cisco TrustSec® technology plus Application Centric Infrastructure (ACI) simplifies the provisioning and management of secure access to network services and applications and protects against targeted attacks and lateral movement of malware in the data center with software-defined segmentation.
- Cisco Secure Data Center automates provisioning of FirePOWER security (Cisco NGIPS and Cisco AMP) in the data center with ACI policy-driven application profiles.
- FirePOWER Threat Defense for integrated services router (ISR) embeds enterprise-level threat defense (NGIPS, AVC, URL filtering, and AMP) into the network fabric where dedicated security appliances may not be feasible, such as branch office locations.
- Cisco Hosted Identity Services provide context-aware identity enforcement as users connect from any device, anywhere, across the extended network, delivering a streamlined and more secure enterprise-mobility experience.
- Service provider security solution allows service providers to take full advantage of open and programmable networks while reducing risk to customers and data with multiservice security integration, unprecedented performance and scaling, and advanced orchestration and management delivered in a purpose-built, carrier-class Cisco FirePOWER appliance.
- Security Services improve security outcomes by providing operational leverage and talent to supplement in-house security teams with a growing portfolio of advisory, integration, and managed services.



2. **Unmatched visibility: See once; control and protect everywhere.**

Cisco sophisticated infrastructure and systems provide visibility that spans the entirety of the network, endpoints, virtual environments, mobile devices, and the cloud, as well as the data center. To truly deliver value, this visibility must be actionable so that businesses can make informed decisions. Learn how the Cisco Talos Security Intelligence and Research Group uses this visibility for aggregation and analysis of telemetry data, creating threat intelligence for Cisco products to protect customers from both known and emerging threats.

3. **Integrated security across the extended network; sharing intelligence, information, and capabilities for systemic response**

To combat multifaceted attacks launched through multiple attack vectors, businesses require advanced threat protection in combination with security sensors and enforcement everywhere and a central policy platform. Cisco embeds technologies into the network infrastructure to increase visibility across all network activity, provide context based on local and global threat intelligence, and allow control using analysis and automation to dynamically protect against detected threats.

- Network as a Sensor (Cisco IOS® NetFlow, Identity Services Engine [ISE], and Lancope) uses the Cisco network as a security sensor, based on the built-in NetFlow technology and additional capabilities, to detect malicious activities and sophisticated threats anywhere within their environment.
- Network as an Enforcer (TrustSec, ISE, and Lancope integration) extends those capabilities even further, activating the embedded TrustSec technology to turn the Cisco network into a powerful policy enforcer to apply security policies, control access to online resources, and block threats and attacks.

4. **The most effective advanced threat prevention across the full attack continuum**

- Boost protection before an attack.
- Respond faster during an attack.
- Contain and remediate after an attack.

Address real-world challenges with a threat-centric approach to security for faster time to detection (TTD) and time to remediation (TTR) – learn more.

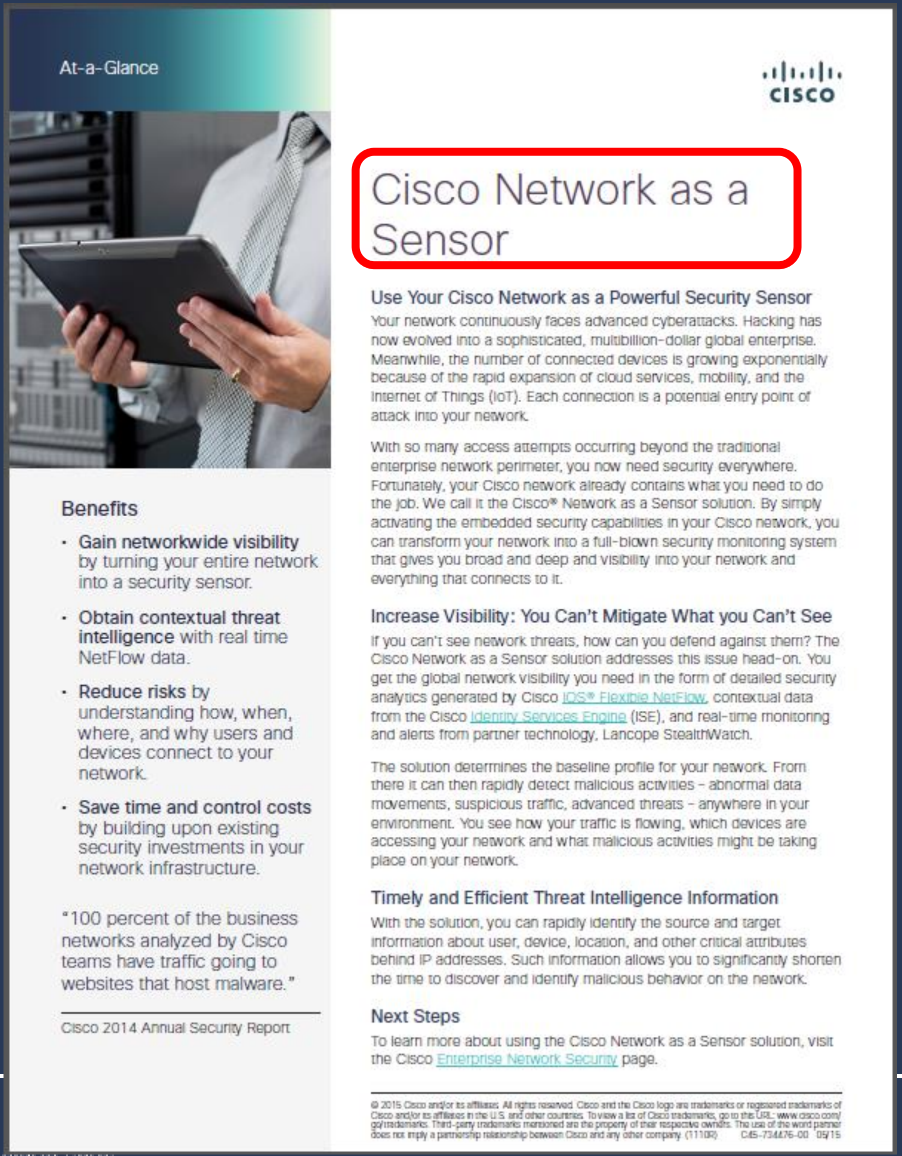
5. **Retrospective security that can detect, contain, and remediate threats even after they have entered the environment**

Continuously gather and analyze data, identify suspicious behaviors and indicators of compromise, and accelerate [illegible] expanded Cisco AMP portfolio that now extends endpoint threat services to remote, VPN-enabled endpoints.

Conclusion

Just as modern networks have transformed our world, modern approaches to security will as well. Embedding security everywhere across the extended network clearly increases security effectiveness against advanced attacks. But it also allows security to become an enabler for businesses to take full and secure advantage of opportunities presented by new digital business models and the IoE.

NaaS (Network As a Sensor), NaaE (Network As an Enforcer)



At-a-Glance

Cisco Network as a Sensor

Benefits

- **Gain networkwide visibility** by turning your entire network into a security sensor.
- **Obtain contextual threat intelligence** with real time NetFlow data.
- **Reduce risks** by understanding how, when, where, and why users and devices connect to your network.
- **Save time and control costs** by building upon existing security investments in your network infrastructure.

"100 percent of the business networks analyzed by Cisco teams have traffic going to websites that host malware."

Cisco 2014 Annual Security Report

Use Your Cisco Network as a Powerful Security Sensor

Your network continuously faces advanced cyberattacks. Hacking has now evolved into a sophisticated, multibillion-dollar global enterprise. Meanwhile, the number of connected devices is growing exponentially because of the rapid expansion of cloud services, mobility, and the Internet of Things (IoT). Each connection is a potential entry point of attack into your network.

With so many access attempts occurring beyond the traditional enterprise network perimeter, you now need security everywhere. Fortunately, your Cisco network already contains what you need to do the job. We call it the Cisco® Network as a Sensor solution. By simply activating the embedded security capabilities in your Cisco network, you can transform your network into a full-blown security monitoring system that gives you broad and deep and visibility into your network and everything that connects to it.

Increase Visibility: You Can't Mitigate What you Can't See

If you can't see network threats, how can you defend against them? The Cisco Network as a Sensor solution addresses this issue head-on. You get the global network visibility you need in the form of detailed security analytics generated by Cisco IOS® Flexible NetFlow, contextual data from the Cisco Identity Services Engine (ISE), and real-time monitoring and alerts from partner technology, Lancope StealthWatch.

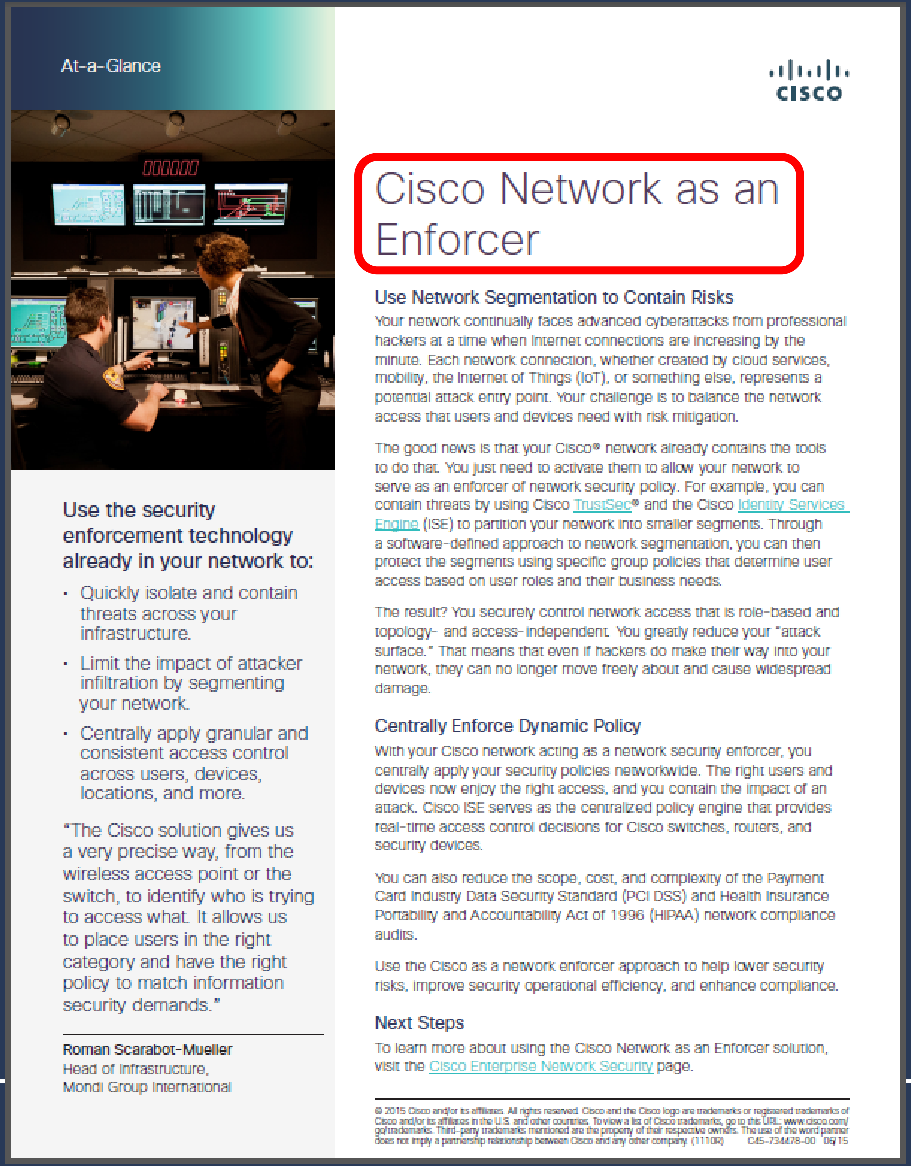
The solution determines the baseline profile for your network. From there it can then rapidly detect malicious activities – abnormal data movements, suspicious traffic, advanced threats – anywhere in your environment. You see how your traffic is flowing, which devices are accessing your network and what malicious activities might be taking place on your network.

Timely and Efficient Threat Intelligence Information

With the solution, you can rapidly identify the source and target information about user, device, location, and other critical attributes behind IP addresses. Such information allows you to significantly shorten the time to discover and identify malicious behavior on the network.

Next Steps

To learn more about using the Cisco Network as a Sensor solution, visit the Cisco Enterprise Network Security page.



At-a-Glance

Cisco Network as an Enforcer

Use the security enforcement technology already in your network to:

- Quickly isolate and contain threats across your infrastructure.
- Limit the impact of attacker infiltration by segmenting your network.
- Centrally apply granular and consistent access control across users, devices, locations, and more.

"The Cisco solution gives us a very precise way, from the wireless access point or the switch, to identify who is trying to access what. It allows us to place users in the right category and have the right policy to match information security demands."

Roman Scarabot-Mueller
Head of Infrastructure,
Mondi Group International

Use Network Segmentation to Contain Risks

Your network continually faces advanced cyberattacks from professional hackers at a time when Internet connections are increasing by the minute. Each network connection, whether created by cloud services, mobility, the Internet of Things (IoT), or something else, represents a potential attack entry point. Your challenge is to balance the network access that users and devices need with risk mitigation.

The good news is that your Cisco® network already contains the tools to do that. You just need to activate them to allow your network to serve as an enforcer of network security policy. For example, you can contain threats by using Cisco TrustSec® and the Cisco Identity Services Engine (ISE) to partition your network into smaller segments. Through a software-defined approach to network segmentation, you can then protect the segments using specific group policies that determine user access based on user roles and their business needs.

The result? You securely control network access that is role-based and topology- and access-independent. You greatly reduce your "attack surface." That means that even if hackers do make their way into your network, they can no longer move freely about and cause widespread damage.

Centrally Enforce Dynamic Policy

With your Cisco network acting as a network security enforcer, you centrally apply your security policies networkwide. The right users and devices now enjoy the right access, and you contain the impact of an attack. Cisco ISE serves as the centralized policy engine that provides real-time access control decisions for Cisco switches, routers, and security devices.

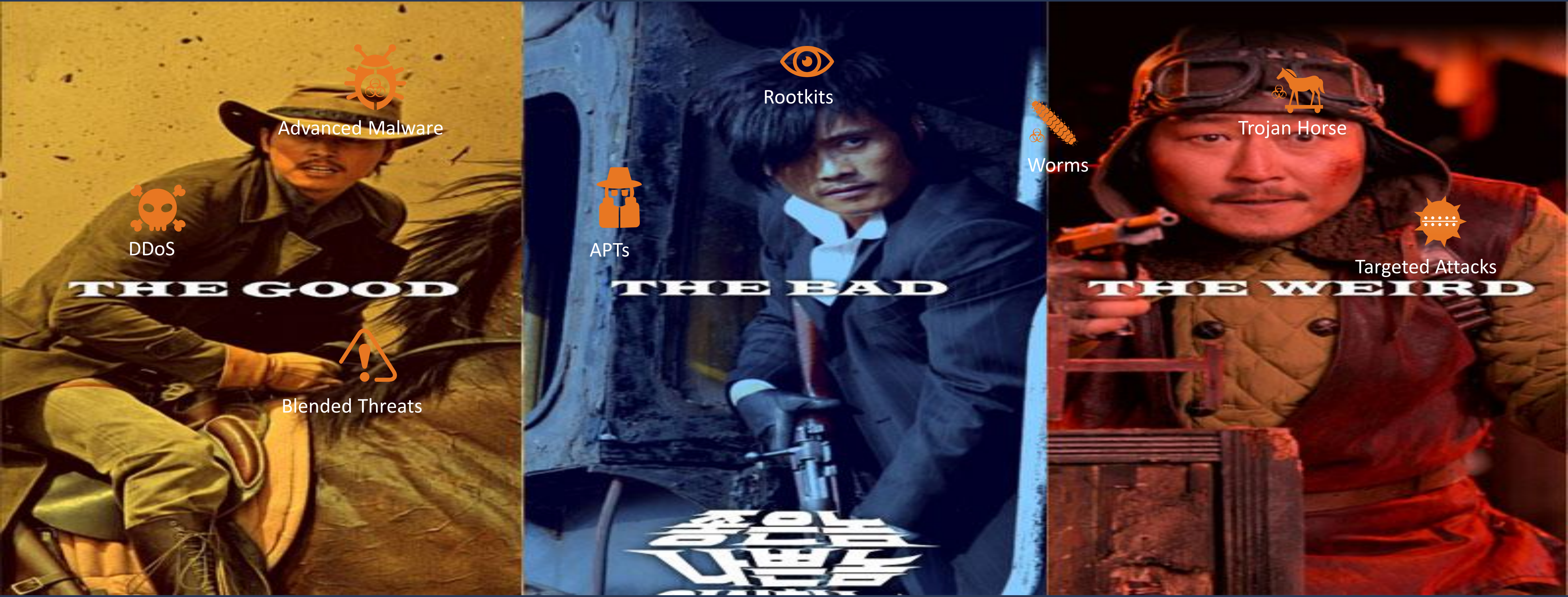
You can also reduce the scope, cost, and complexity of the Payment Card Industry Data Security Standard (PCI DSS) and Health Insurance Portability and Accountability Act of 1996 (HIPAA) network compliance audits.

Use the Cisco as a network enforcer approach to help lower security risks, improve security operational efficiency, and enhance compliance.

Next Steps

To learn more about using the Cisco Network as an Enforcer solution, visit the Cisco Enterprise Network Security page.

좋은놈, 나쁜놈, 이상한놈


Advanced Malware
DDoS
THE GOOD
Blended Threats
Rootkits
APTs
THE BAD
좋은놈
나쁜놈
Worms
Trojan Horse
Targeted Attacks
THE WEIRD

위협은 더욱 지능화 복잡화 되고 있습니다.

시스코에서 조사된 기업의 100퍼센트가 알려진 악의적인 파일 또는 서비스를 제공하는 도메인에 접속했다는 사실

(2014 CASR)

다양한 보안 위협이 우리가
자주 방문하는 사이트안에
숨어 있습니다.

Security for the Real World

1,000,000

JAVA

FLASH

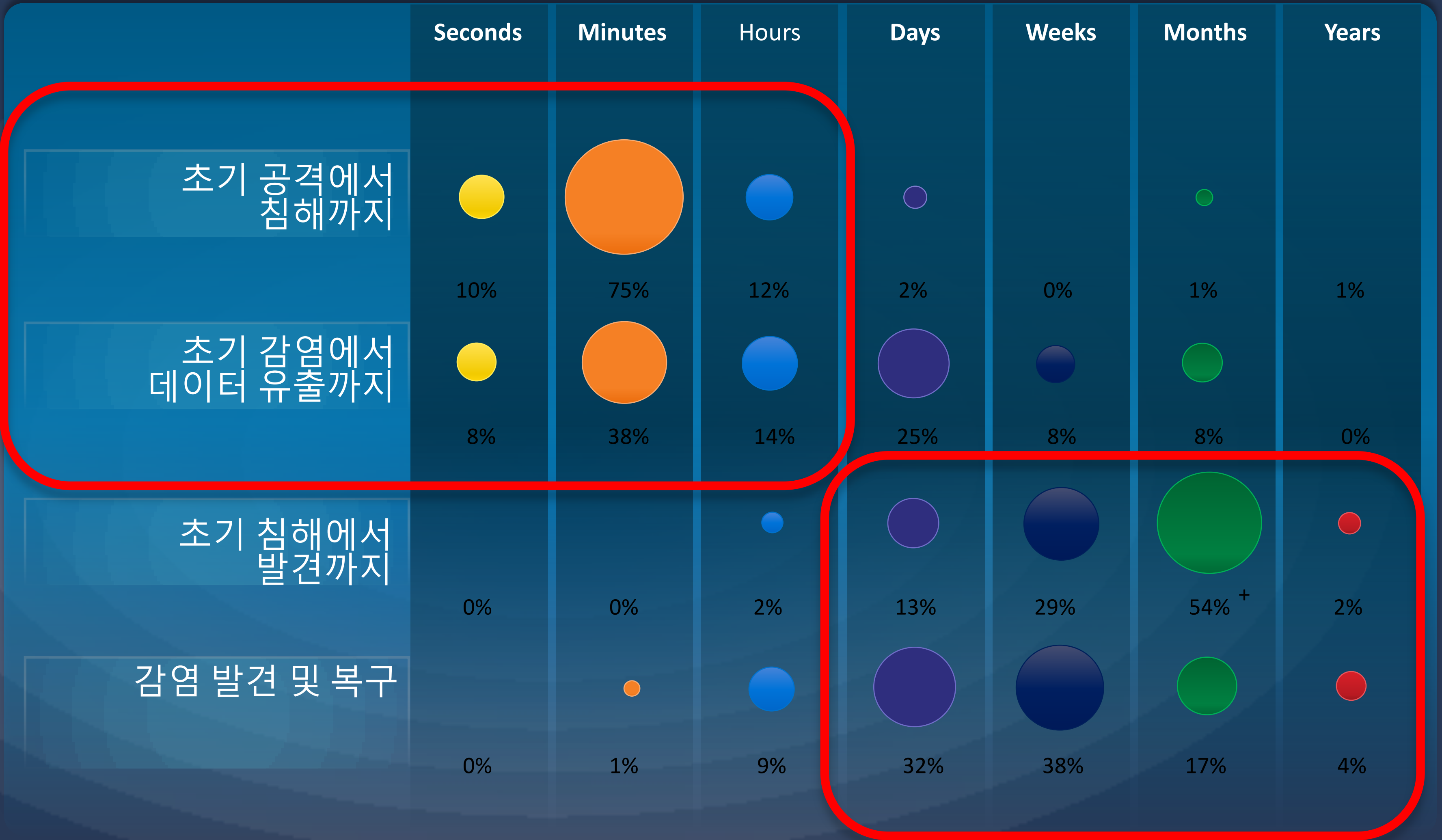
SPAM

PDF, OFFICE

지능형 위협의 진실

60% 데이터가 1시간 이내에 유출

85% 는 1주 내에 발견되지 못함



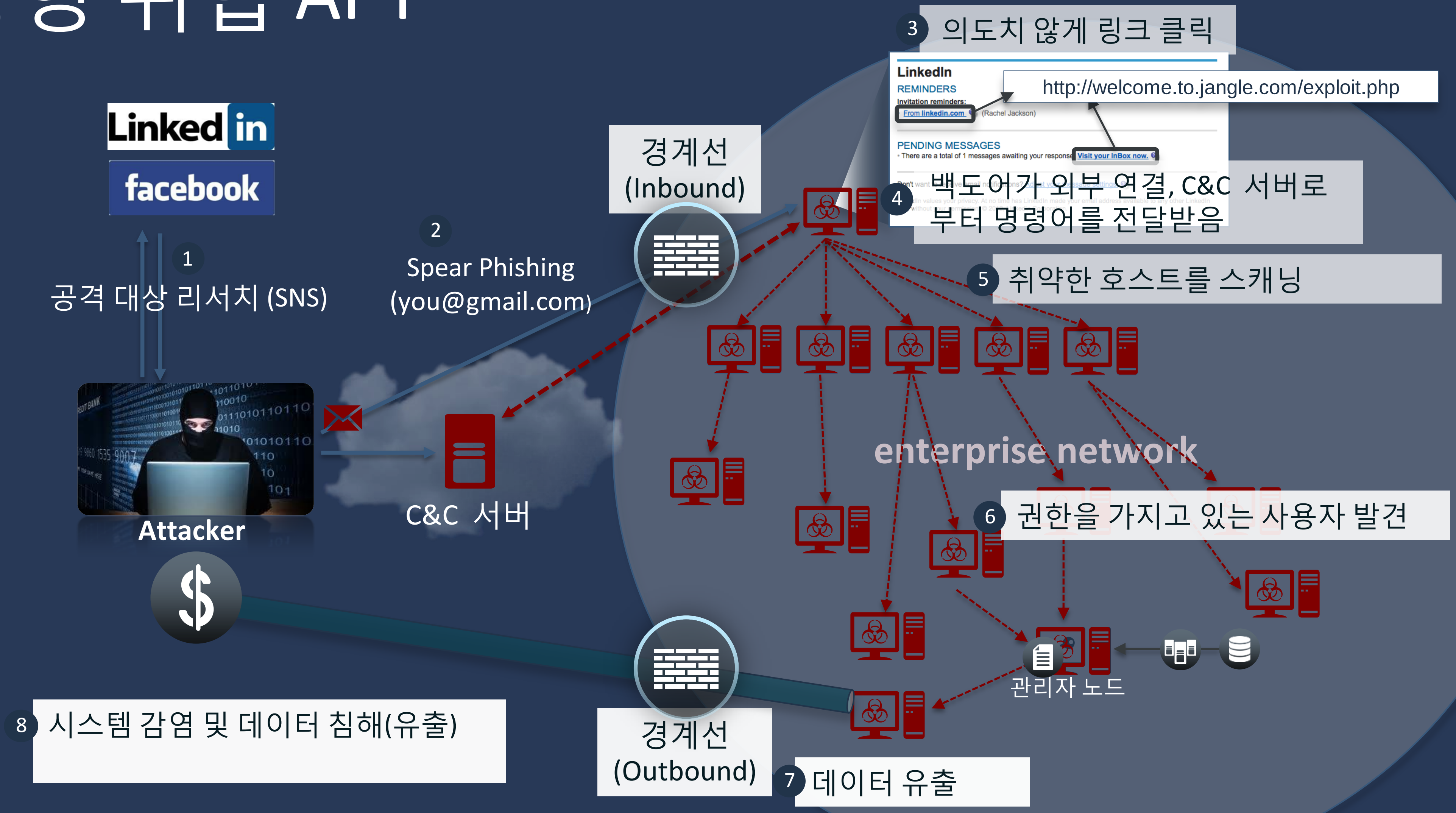
	Seconds	Minutes	Hours	Days	Weeks	Months	Years
초기 공격에서 침해까지	10%	75%	12%	2%	0%	1%	1%
초기 감염에서 데이터 유출까지	8%	38%	14%	25%	8%	8%	0%
초기 침해에서 발견까지	0%	0%	2%	13%	29%	54%+	2%
감염 발견 및 복구	0%	1%	9%	32%	38%	17%	4%

Timespan of events by percent of breaches – Source : Cisco Managed Threat Defense

만약 여러분이 침해 사실을 알았다면, 여러분의 보안은 달라졌을까요 ?

96%의 공격이 단순한 기법

지능형 위협 APT



Linked in

facebook

1 공격 대상 리서치 (SNS)

2 Spear Phishing (you@gmail.com)

Attacker

C&C 서버

경계선 (Inbound)

3 의도치 않게 링크 클릭

LinkedIn

REMINDERS

Invitation reminders:

- From linkedin.com (Rachel Jackson)

PENDING MESSAGES

- There are a total of 1 messages awaiting your response. Visit your InBox now.

http://welcome.to.jangle.com/exploit.php

4 백도어가 외부 연결, C&C 서버로부터 명령어를 전달받음

5 취약한 호스트를 스캐닝

enterprise network

6 권한을 가지고 있는 사용자 발견

관리자 노드

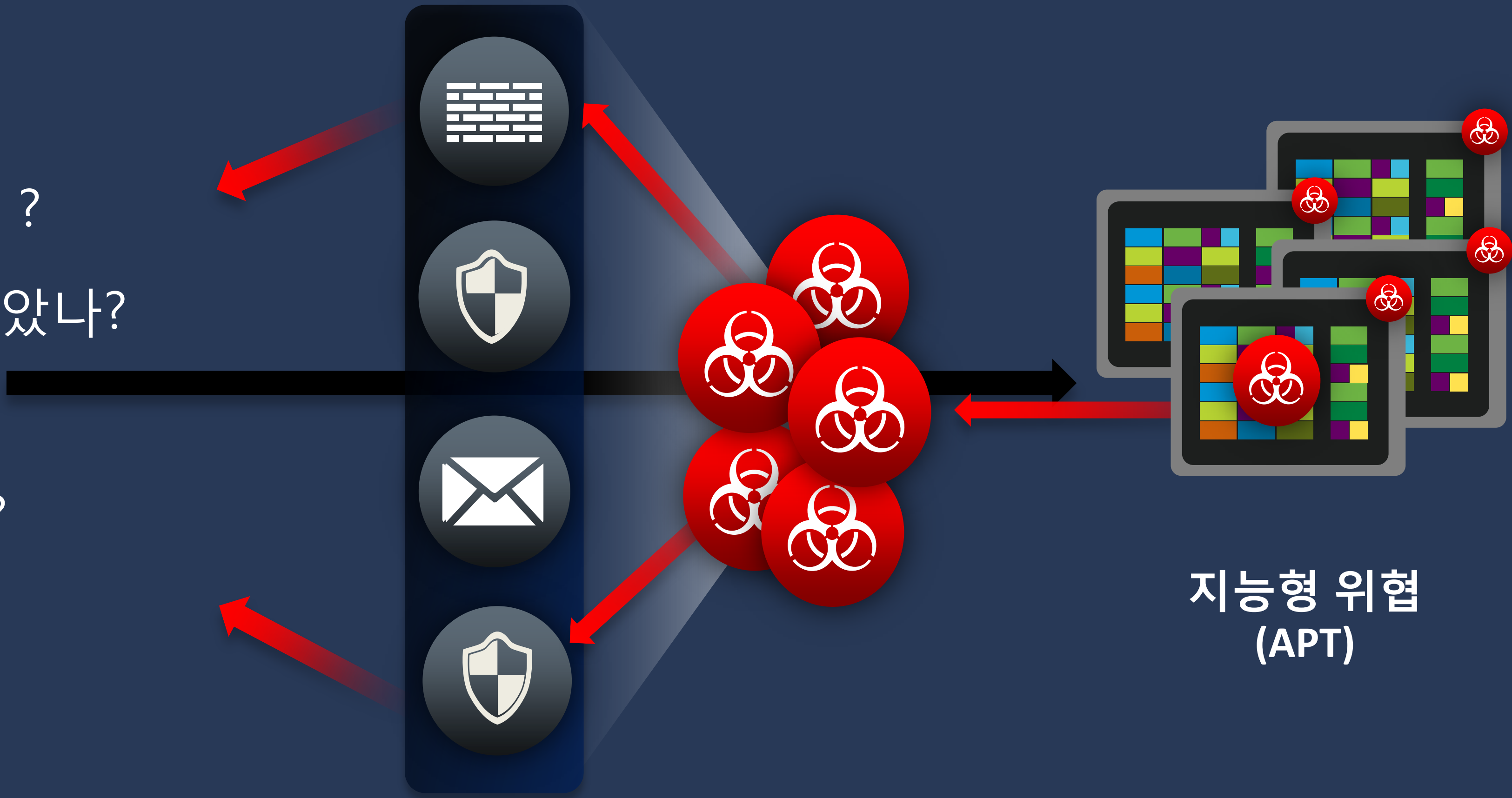
7 데이터 유출

경계선 (Outbound)

8 시스템 감염 및 데이터 침해(유출)

악성코드가 시스템에 침입하였다면 ?

- 어디서 부터 시작한 것일까 ?
- 현재 상황이 얼마나 심각한가 ?
- 시스템들이 얼마나 영향을 받았나?
- 악성코드가 무엇을 했나 ?
- 어떻게 하면 복구할 수 있나 ?
- 다시 이러한 상황이 반복되지 않으려면 ?



지능형 위협
(APT)

1

Before

공격을 사전에 방어하라

2

During

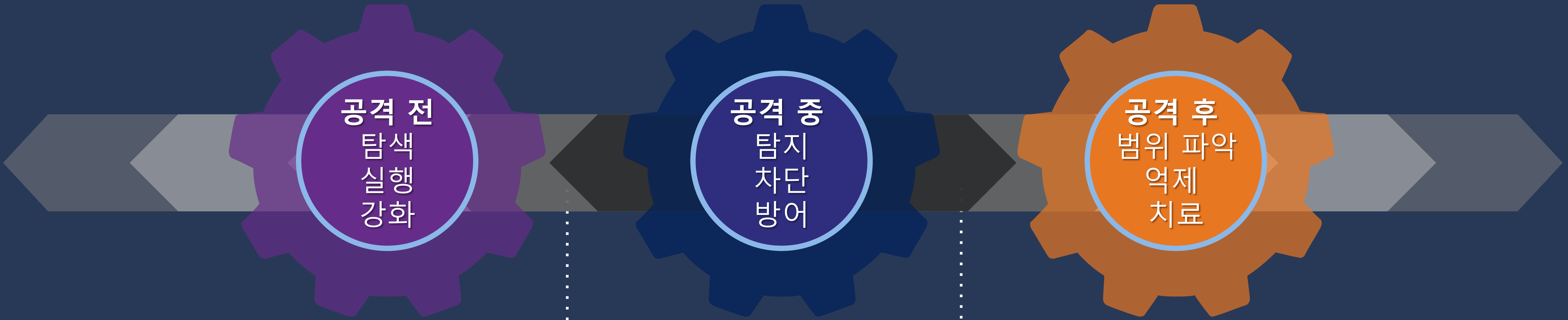
가시성 확보를 통한 감염시스템 판단과 감염원인 추적

3

After

감염시스템 추적과 지속적인 감염 차단

여기 새로운 방안을 여러분에게 소개합니다.



공격 전
탐색
실행
강화

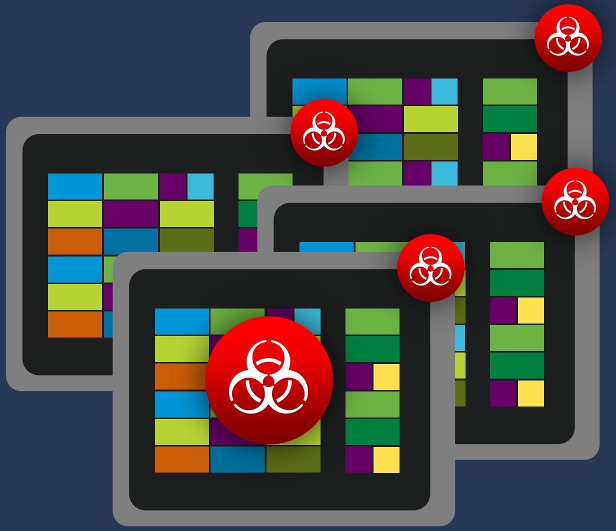
공격 중
탐지
차단
방어

공격 후
범위 파악
억제
치료

공격에 대한 전체 과정을 충분히 이해해야 합니다.

Filtering	Malware Signature	File Retrospection
Usage Controls	File Reputation	Threat Analytics
Reputation	File Behavior	Actionable Reporting

AMP 가 무엇인가요 ?

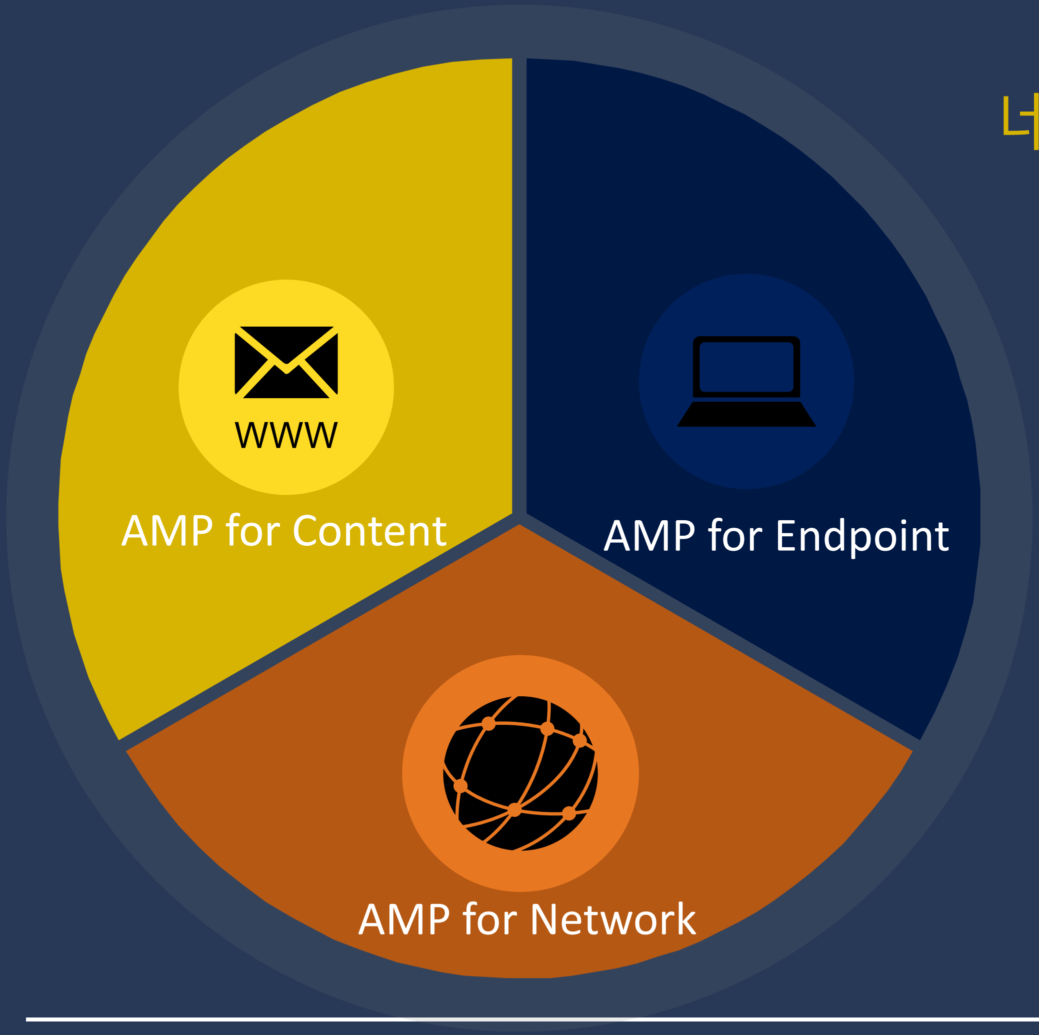


AMP(Advanced Malware Protection)

지능형 악성코드 차단 시스템으로 APT 와 같은 지속적인
위협 공격에 효과적으로 대응할 수 있는 솔루션입니다.

어떤 사용자가 무엇을 통해 어디서 언제 어떻게 위협으로부터 영향을 받았는지 알 수 있다면 어떨까요?

Better Together



네트워크와 앤드포인트단까지 통합된 AMP 전략

오늘날 지능형 위협을 차단하기 위해서는
멀티 레이어 차단 전략이 필요합니다.
AMP 기능과 NGIPS, Content Security 기능이
함께하면 더 좋은 이유가 여기에 있습니다.

AMP 주요 기능

악성코드 탐지 차단	• 디바이스 감염전 악성코드의 차단
회귀적 탐지	• 파일의 지속적 분석
파일 추적	• 문제가 되는 악성코드 영역 빠른 파악
디바이스 추적	• 감염원인의 파악 분석
위협지표, 감염원인	• 자동화된 감염시스템 분석 및 감염원인 파악
파일 상세 분석	• 샌드박스를 통한 빠르고 안전한 파일 분석
Outbreak Control	• 악성코드 전파 확산을 빠르게 차단

위협 인텔리전스 기반의 보안 (TALOS)

Threat Intelligence
I00I IIIOI IIIOOII OIIOOII IOI000
.OI000 OIIO 00 OIII000 II
OOIIIOOOIIIO IOOI IIOI IIIO
Cisco® Talos
OIIO OOOIOI IIOOIIO IIOOIII IOII IOO
II IOOOOII II IIOOIOIII OOOIIIO
IIOOIIO IIOOIII IOII IOOI OIII
Research Response

Email	Endpoints	Web	Networks	IPS	Devices

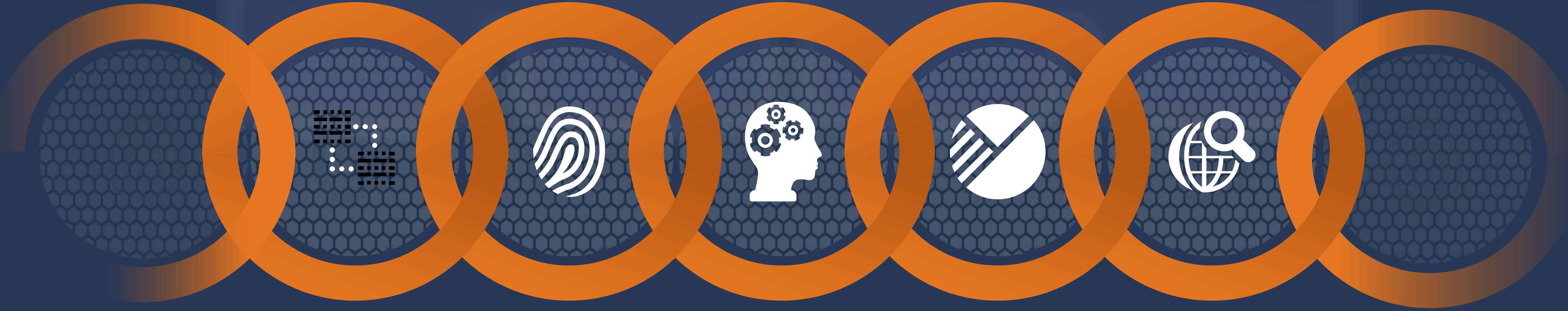
1.6 million 글로벌 센서	35% 전세계 이메일 트래픽
100 TB 매일 전달받는 데이터	13 billion 웹 요청
150 million+ 설치된 앤드포인트	24x7x365 운영
600+ 엔지니어, 기술자, 연구원	40+ 언어

AMP
Advanced Malware Protection

- 매일 180,000+ 샘플 파일
- AMP™ 커뮤니티
- Advanced Microsoft and Industry Disclosures
- Snort and ClamAV 오픈소스 커뮤니티
- 허니팟
- AMP Threat Grid 동적분석 – 1000만개/월
- Private and Public Threat Feeds
- Dynamic Analysis

지능형 악성코드 탐지를 위한 다단계 방어층

모든 탐지는 100% 미만



One-to-One Signature

Fuzzy Finger-printing

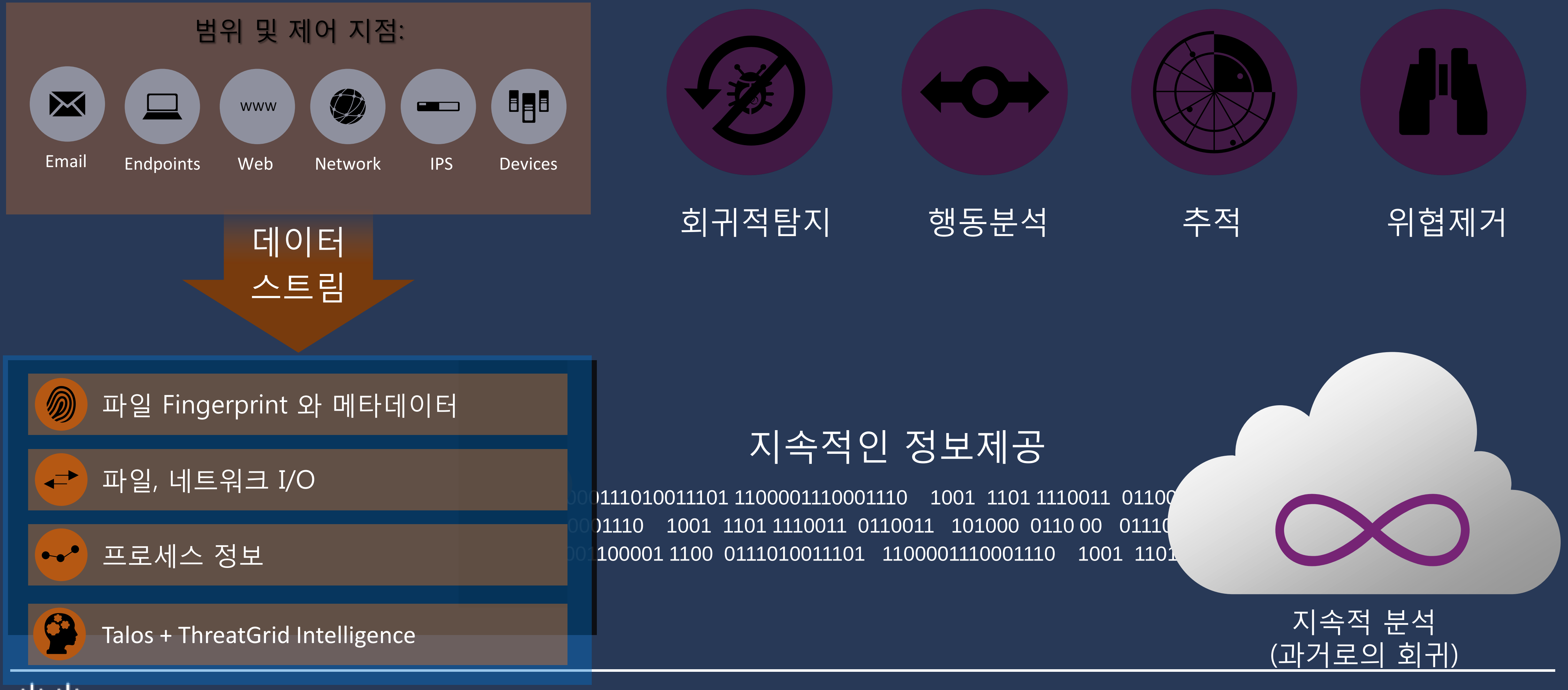
Machine Learning

Advanced Analytics

Dynamic Analysis

평판 필터링 및 파일 샌드박싱

AMP 의 전방위적인 지속적 분석



범위 및 제어 지점:

Email Endpoints Web Network IPS Devices

데이터 스트림

- 파일 Fingerprint 와 메타데이터
- 파일, 네트워크 I/O
- 프로세스 정보
- Talos + ThreatGrid Intelligence

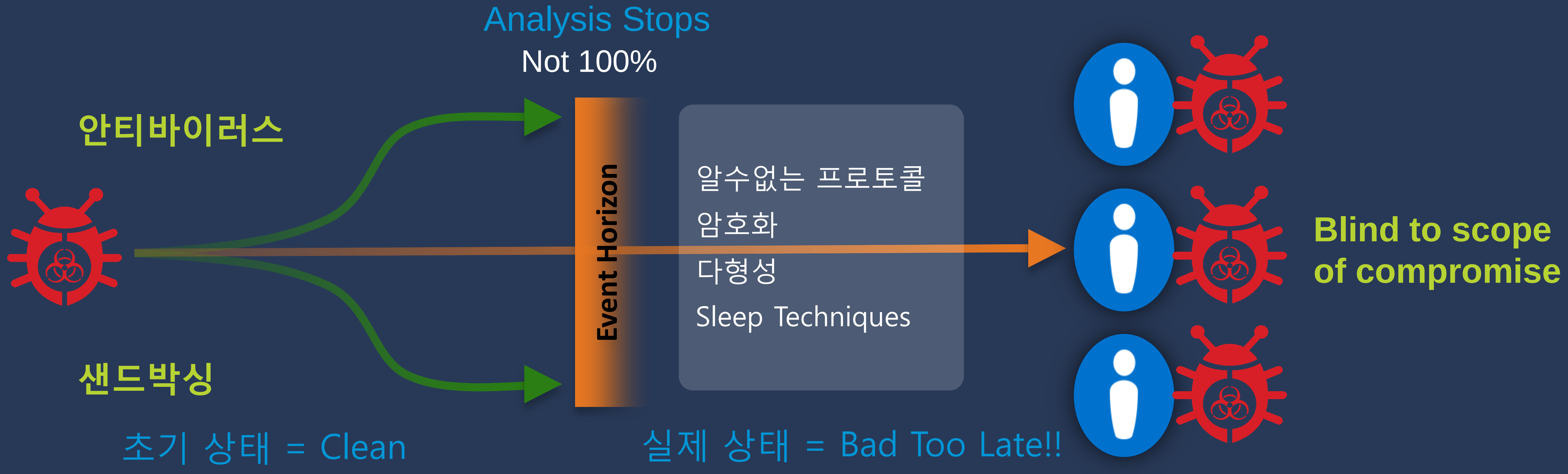
회귀적탐지 행동분석 추적 위협제거

지속적인 정보제공

0001110100111011100001110001110   1001 1101 1110011 01100
0001110   1001 1101 1110011 0110011   101000 0110 00   01110
001100001 1100 0111010011101   1100001110001110   1001 1101

지속적 분석
(과거로의 회귀)

특정 시점의 탐지



Analysis Stops
Not 100%

알수없는 프로토콜
암호화
다형성
Sleep Techniques

Blind to scope of compromise

초기 상태 = Clean

실제 상태 = Bad Too Late!!

특정 시점의 악성코드 탐지 방법으로는 100% 차단할 수가 없다.

만약

99%

위협을 탐지하더라도

나머지

1%

침해사고 발생한다면

효과적인 탐지를 위해서는, 언제 어디서나

지속적

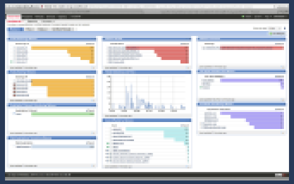
Tell the Story

악성코드의 스토리를 말하다

WHO, WHAT, WHEN, WHERE, HOW

가시성을 통해 A-Z 까지

Who



어떤 사용자가
처음 접근했나

What

어떤 애플리케이션
이 영향을 받았나

Where

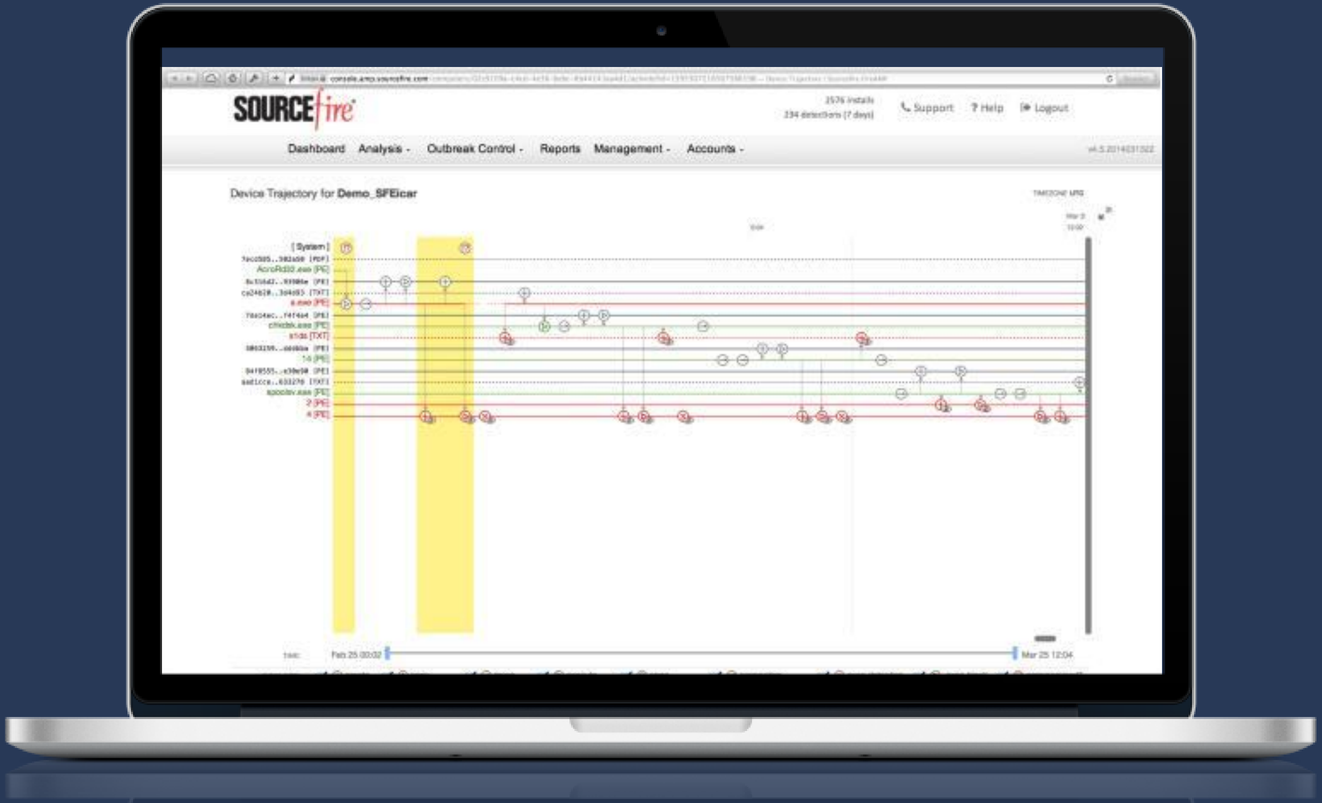
침해당한 영역 범위

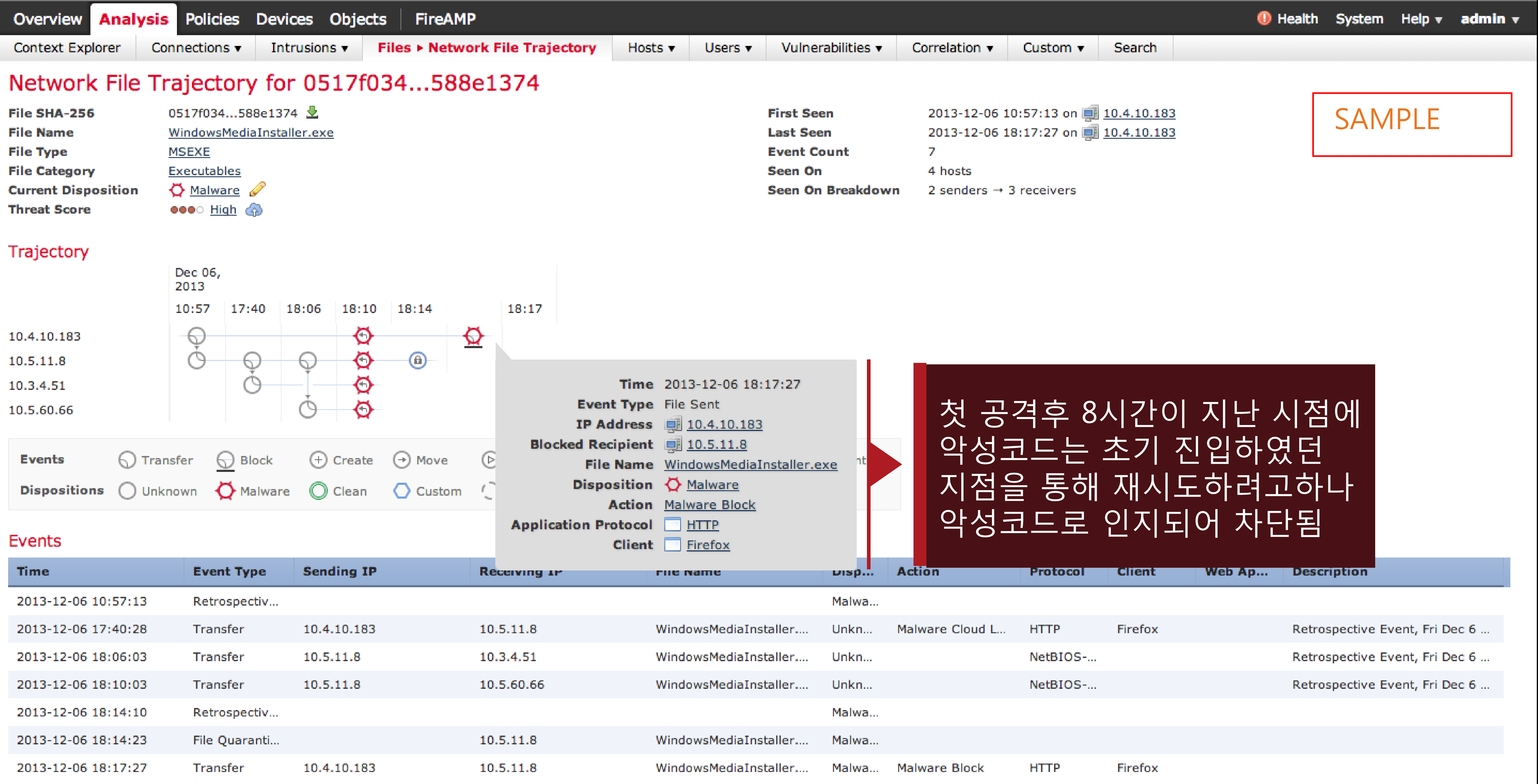
When

위협에 노출된
시간과 타임라인

How

위협의 진행상황
과 감염원인





Overview | Analysis | Policies | Devices | Objects | FireAMP | Health | System | Help ▾ | admin ▾

Context Explorer | Connections ▾ | Intrusions ▾ | Files ▸ Network File Trajectory | Hosts ▾ | Users ▾ | Vulnerabilities ▾ | Correlation ▾ | Custom ▾ | Search

Network File Trajectory for 0517f034...588e1374

SAMPLE

File SHA-256	0517f034...588e1374	**First Seen**	2013-12-06 10:57:13 on 10.4.10.183
File Name	WindowsMediaInstaller.exe	**Last Seen**	2013-12-06 18:17:27 on 10.4.10.183
File Type	MSEXE	**Event Count**	7
File Category	Executables	**Seen On**	4 hosts
Current Disposition	Malware	**Seen On Breakdown**	2 senders → 3 receivers
Threat Score	●●●○ High		

Trajectory

Dec 06, 2013

10:57 | 17:40 | 18:06 | 18:10 | 18:14 | 18:17

10.4.10.183

10.5.11.8

10.3.4.51

10.5.60.66

Events ○ Transfer ○ Block ⊕ Create ⊕ Move

Dispositions ○ Unknown ○ Malware ○ Clean ○ Custom

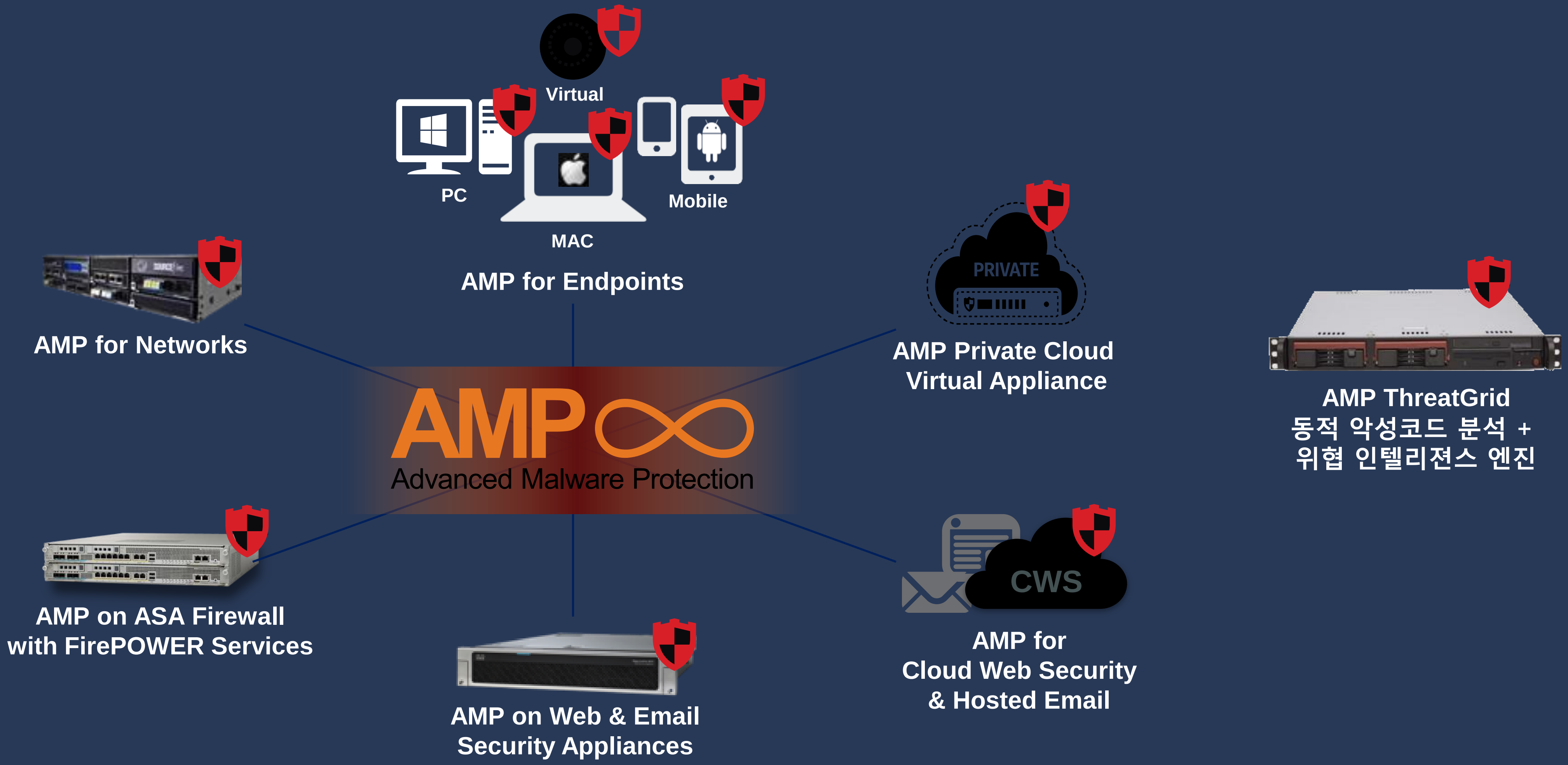
Time	2013-12-06 18:17:27
Event Type	File Sent
IP Address	10.4.10.183
Blocked Recipient	10.5.11.8
File Name	WindowsMediaInstaller.exe
Disposition	Malware
Action	Malware Block
Application Protocol	HTTP
Client	Firefox

Events

Time	Event Type	Sending IP	Receiving IP	File Name	Disp...	Action	Protocol	Client	Web Ap...	Description
2013-12-06 10:57:13	Retrospectiv...				Malwa...					
2013-12-06 17:40:28	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Unkn...	Malware Cloud L...	HTTP	Firefox		Retrospective Event, Fri Dec 6 ...
2013-12-06 18:06:03	Transfer	10.5.11.8	10.3.4.51	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:10:03	Transfer	10.5.11.8	10.5.60.66	WindowsMediaInstaller....	Unkn...		NetBIOS-...			Retrospective Event, Fri Dec 6 ...
2013-12-06 18:14:10	Retrospectiv...				Malwa...					
2013-12-06 18:14:23	File Quaranti...		10.5.11.8	WindowsMediaInstaller....	Malwa...					
2013-12-06 18:17:27	Transfer	10.4.10.183	10.5.11.8	WindowsMediaInstaller....	Malwa...	Malware Block	HTTP	Firefox		

첫 공격후 8시간이 지난 시점에 악성코드는 초기 진입하였던 지점을 통해 재시도하려고하나 악성코드로 인지되어 차단됨

시스코 AMP Everywhere 전략



Virtual

PC

MAC

Mobile

AMP for Endpoints

AMP for Networks

PRIVATE

AMP Private Cloud
Virtual Appliance

AMP ThreatGrid
동적 악성코드 분석 +
위협 인텔리전스 엔진

AMP
Advanced Malware Protection

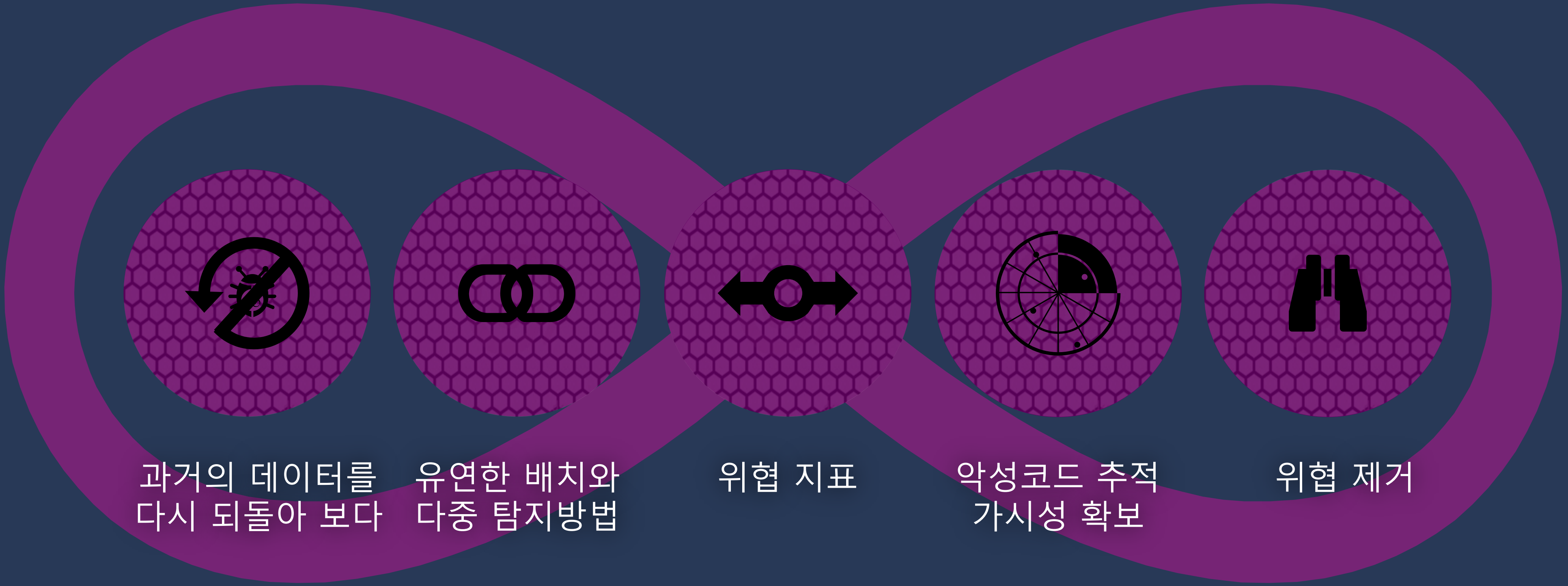
AMP on ASA Firewall
with FirePOWER Services

AMP on Web & Email
Security Appliances

CWS

AMP for
Cloud Web Security
& Hosted Email

AMP의 차별화 포인트



과거의 데이터를 다시 되돌아 보다
유연한 배치와 다중 탐지방법
위협 지표
악성코드 추적 가시성 확보
위협 제거

네트워크부터 엔드포인트까지 전방위 위협 대응
Not point in Time

Summary

가시성

여러분들의 네트워크를 알고,
위협을 인지하라

회귀적 분석

과거로의 회귀 그리고
지속적인 분석

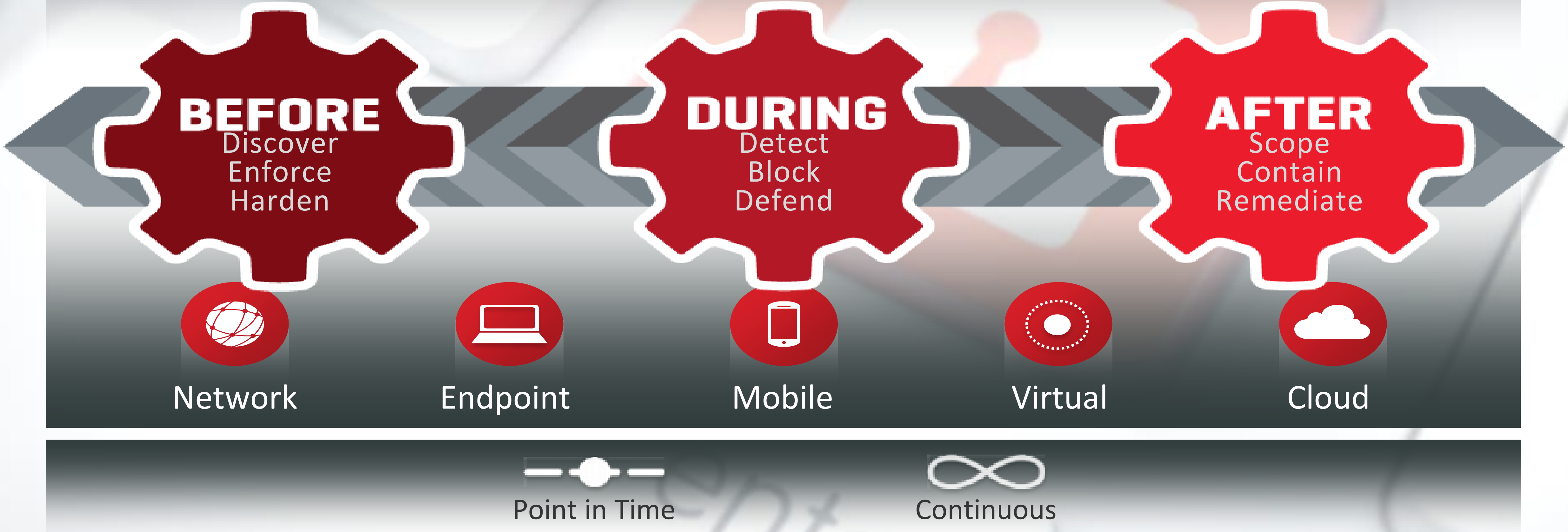
긴급상황 제어

통합된 대응환경

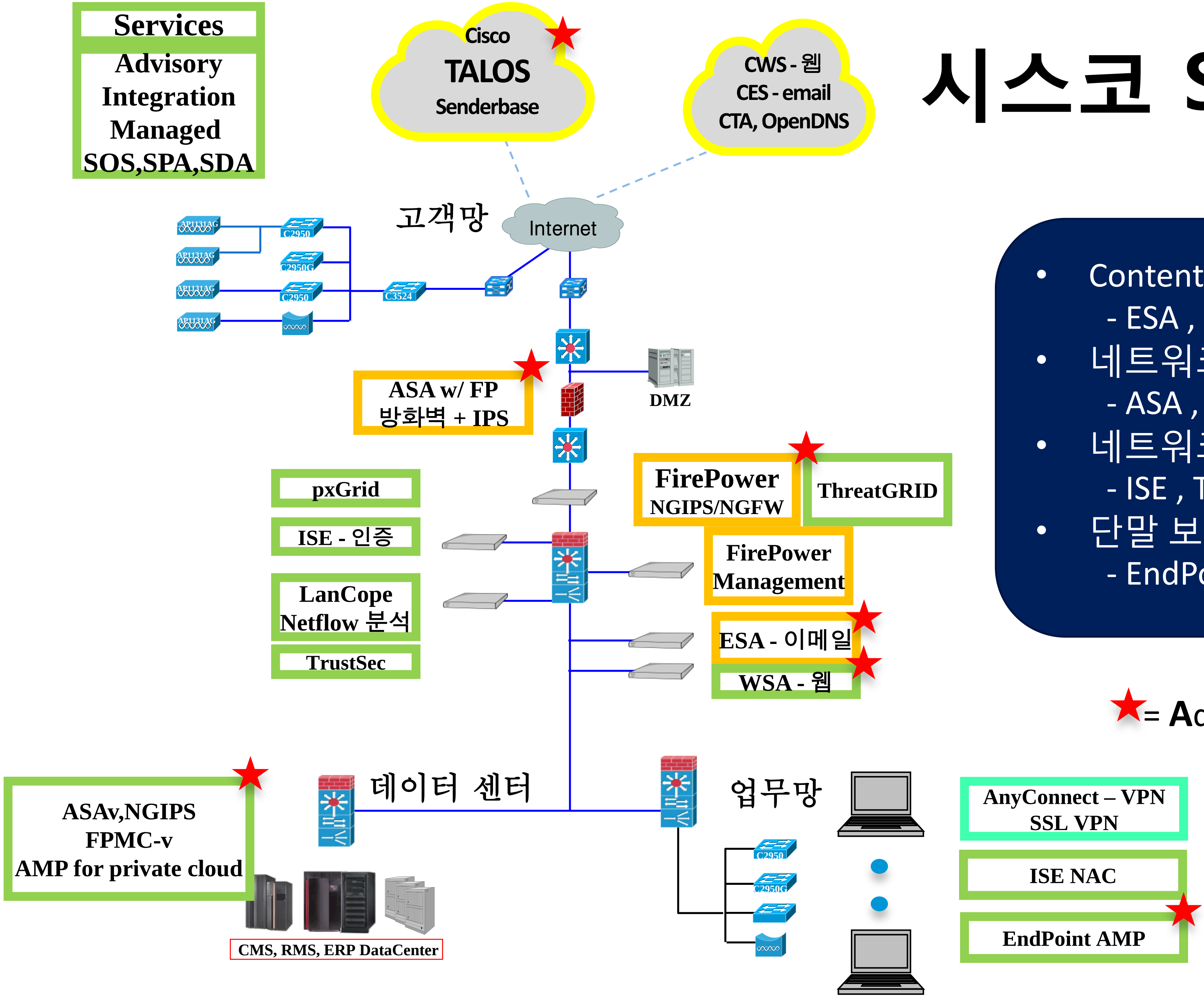
다 단계 방어층을 이용한 전방위적인 차단
Better Together

그럼 어떤 것이 필요할까요 ...

A New Threat Centric Security Approach which Offers Pervasive Protection Across the Full Attack Continuum



시스코 Security 제품군



- Content 보안
  - ESA , WSA , CES ,CWS
- 네트워크 보안
  - ASA , FirePower, FireSight, AMP
- 네트워크 장비 보안
  - ISE , TrustSec, StealthWatch
- 단말 보안
  - EndPoint AMP, NAC, AnyConnect

★= **A**dvanced **M**alware **P**rotection

시스코 차세대 방화벽 (Next Generation)

- 방화벽 ASA 플랫폼에 소스파이어 차세대 위협 차단 솔루션을 서비스 모듈 형태로 통합
- 새로운 지능적인 보안위협에 대응하는 **통합 보안 플랫폼**

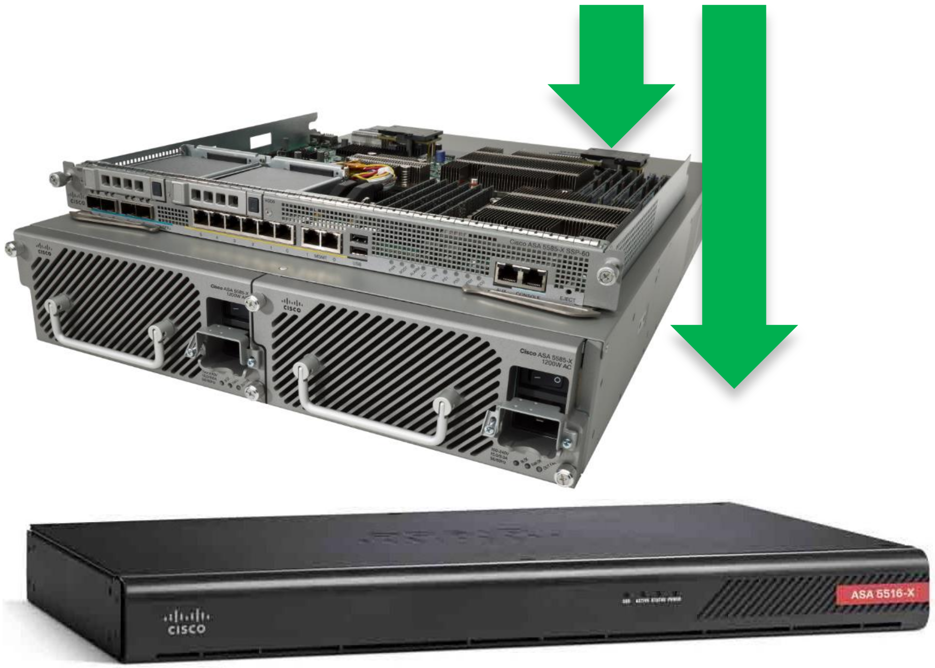
firePOWER™

“Threat-Focused” Next-Generation Firewall

▶ **통합된 멀티 차단 레이어** : 가시성의 확보로 시작

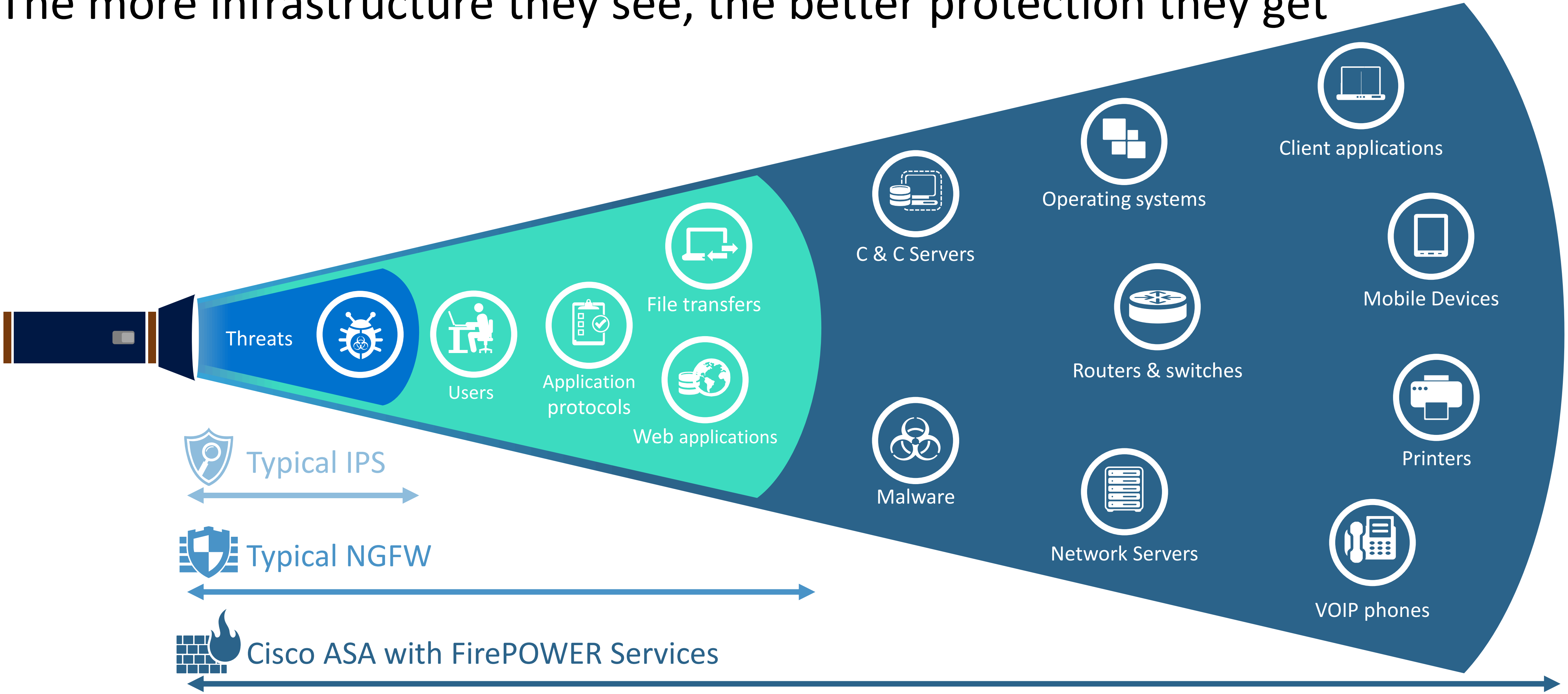
▶ 동적제어를 통한 자동화된 제어

▶ 진화된 위협에 대한 적응형 방어
(Before – During – After)



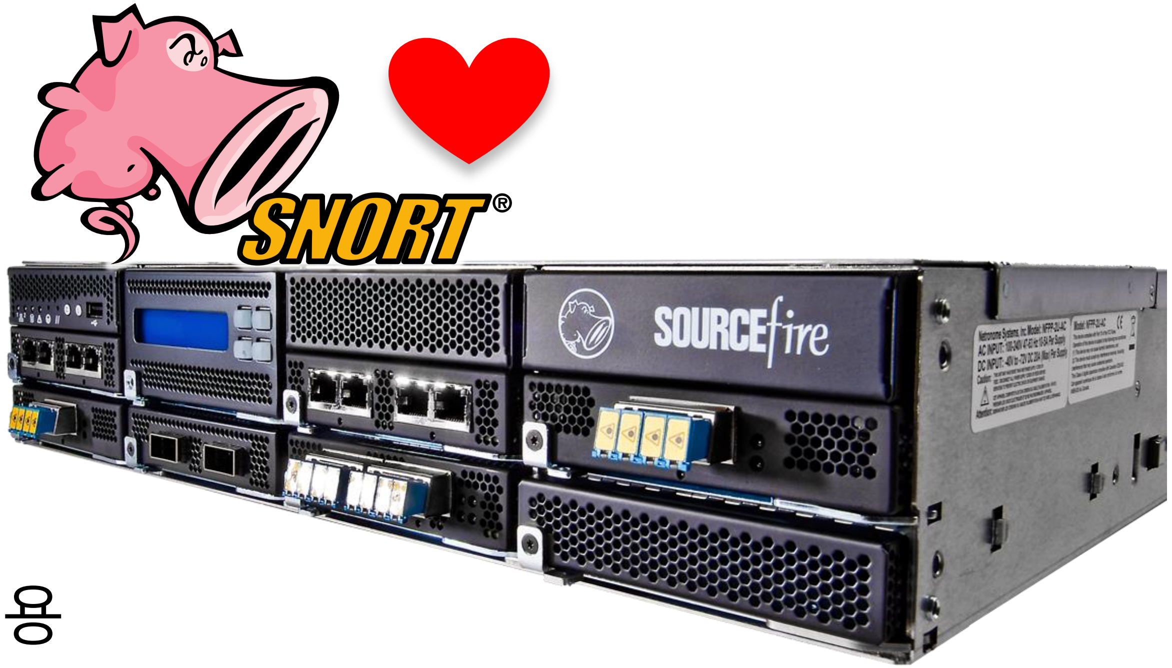
시스코NGFW 이 제공하는 가시성

The more infrastructure they see, the better protection they get



네트워크 시큐리티 플랫폼의 새로운 기준

- 업계 최고의 침입탐지 시스템
- 실시간 상황인식
- 네트워크 전체 가시성 확보
- FireSIGHT 를 통한 인텔리전트 시큐리티
- High Performance 그리고 확장성
- 애플리케이션 제어, URL 필터링 그리고 AMP 기능을 손쉽게 라이센스 추가로 사용



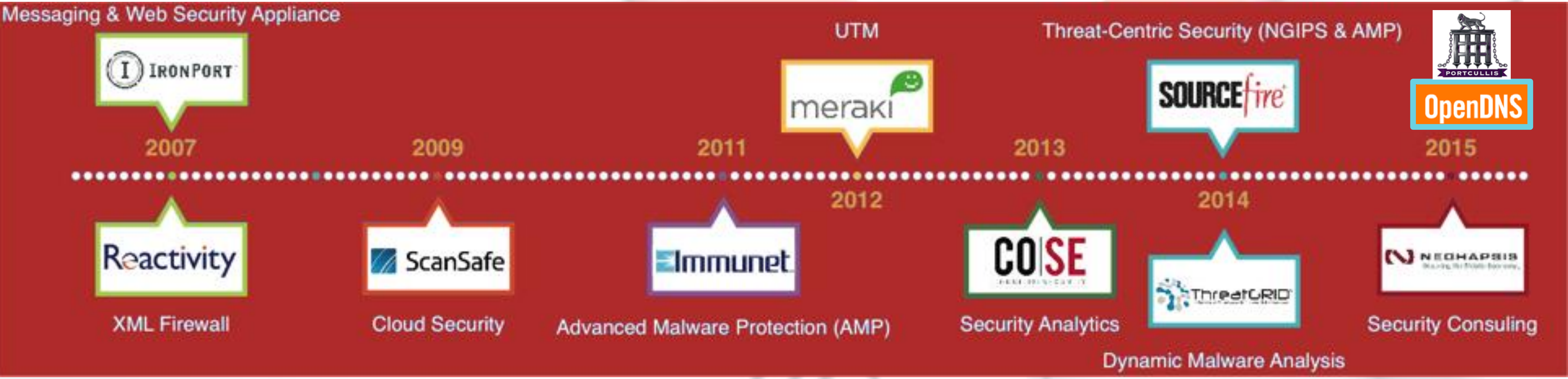
시스코 FirePower에서 제공하는 자산인식 및 가시성

APP	레거시 위협	사용자	웹 애플리케이션	애플리케이션 프로토콜	파일 전송	멀웨어	커맨드 & 컨트롤 서버	클라이언트 애플리케이션	네트워크 서버	오퍼레이팅 시스템	라우터 & 스위치	모바일 디바이스	프린터	VoIP 전화기	가상 머신 (VM)
FirePower NGIPS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
기존의 IPS	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
기존의 NGFW	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗

Threat Centric Security

왜 시스코일까요? …
#1 We are Serious About Security

We are transforming to create the industry’s broadest security solution portfolio via
보안솔루션의 이노베이션을 통하여 고객분들에게 #1 사이버시큐리티 회사가 될 것을 약속하고 지속적으로 실천해 가고 있습니다.



Messaging & Web Security Appliance

UTM

Threat-Centric Security (NGIPS & AMP)

2007

2009

2011

2012

2013

2014

2015

XML Firewall

Cloud Security

Advanced Malware Protection (AMP)

Security Analytics

Dynamic Malware Analysis

Security Consulting

왜 시스코일까요? … #2 Cisco Talos가 굉장한 규모의 인텔리젼스 디펜스를 제공합니다.

100TB Security Intelligence	**150,000** Micro-applications	**5,500** IPS Signatures	**5B** Daily Email Connections
1.6M Deployed Devices	**93B** Daily Email Messages	**150M** Deployed Endpoints	**1,000** Applications
13B Web Requests	**35%** Enterprise Email	**3-5 min** Updates	**4.5B** Daily Email Blocks
120K Sandbox Reports	**75,000** FireAMP Updates	**6,000** New Clam AV Sigs	**14M** Deployed Access Gateway

Cisco Talos represents the **Industry's largest collection of real-time threat intelligence!**

[illegible]

[illegible]

Daily Web Requests

Sandbox Reports

왜 시스코일까요…#3 리딩 시큐리티 회사

ESG

… do any network security vendors understand data center and what's needed to accommodate network security? Cisco certainly does

FROST & SULLIVAN

Market Share Leader
Cisco excels as leaders in F&S's Industry Quotient with a leading 21.9% market share in Asia Pacific

Gartner

Magic Quadrant Leader

- Network Access Control
- Intrusion Prevention Systems
- Security Email Gateway

NSS LABS

Security Value Map Leader

- Breach Detection
- Next-Gen Firewall
- Intrusion Prevention System

IDC

… no qualms in stating that Cisco is serious about security serv ices and competitors should duly t ake note

Infonetics RESEARCH

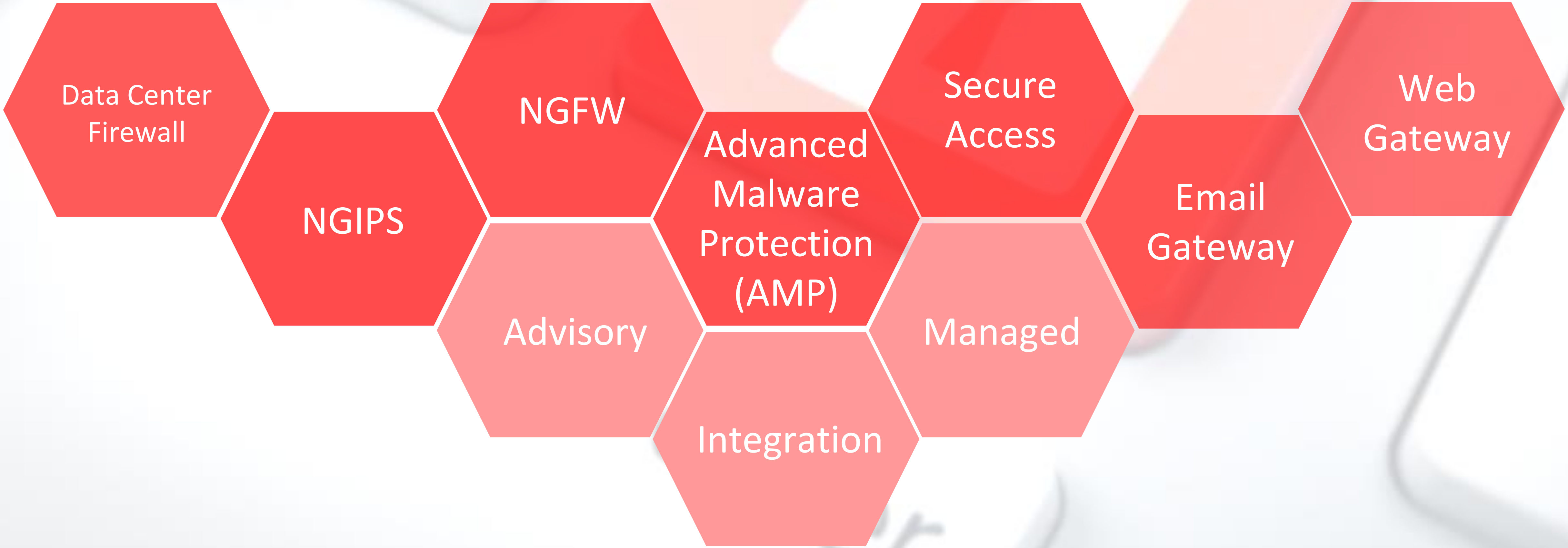
#1 Market Share

- Network Security
- Email (Appliances & SW)
- Web (SaaS)

왜 시스코일까요…
#4 완벽한 시큐리티 솔루션을 제공합니다

Cisco Threat Centric Security Model

Offers protection through the entire attack continuum …



보안제품과 서비스를 함께 제공함으로서 차별화를 추구합니다.

Security Products
Security Services

CISCO™

Thank You