



지능형 지속 위협 공격에 대한 대안, 적응형 보안 기술

시스코 ASA with FirePOWER 서비스

김용호 부장

시스코 코리아

October 2014



기존 차세대 보안 플랫폼들의 문제점

오로지 어플리케이션 통제만 집중

결국...실제 위협은 놓치는...

A vertical list of logos with status indicators to their right. From top to bottom: Citrix logo with a red 'X' in a circle; Facebook logo with a red 'X' in a circle; Skype logo with a green checkmark in a circle; Outlook logo with a green checkmark in a circle; and an envelope icon with a red 'X' in a circle. The background features horizontal bands of binary code (0s and 1s).

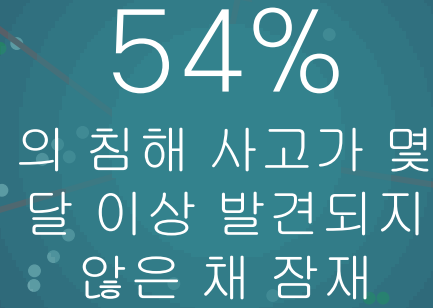


기존 차세대 보안 플랫폼들은 공격의 대상이 되는 것을 줄일 수는 있으나
더욱 지능화된 공격 및 악성코드들에 의해 쉽게 우회

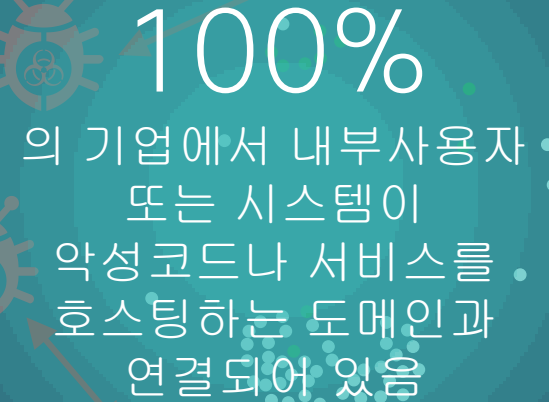
실제 위협 상황은 어플리케이션 통제 그 이상을 요구



60%
의 데이터가
단 몇시간
안에 탈취됨



54%
의 침해 사고가 몇
달 이상 발견되지
않은 채 잠재



100%
의 기업에서 내부사용자
또는 시스템이
악성코드나 서비스를
호스팅하는 도메인과
연결되어 있음

오히려 눈에 잘 띄는 곳에
숨겨진 **Community** 가
발각되는 것을 더 신속하게
탐지하고 피할 수 있음

단독적인 '심층적인 방어' 전략의 부족성



사일로 형태의
접근 방식

복잡성증가

효율성 저하



매우 불투명한
가시성

미탐된 다양한
위협

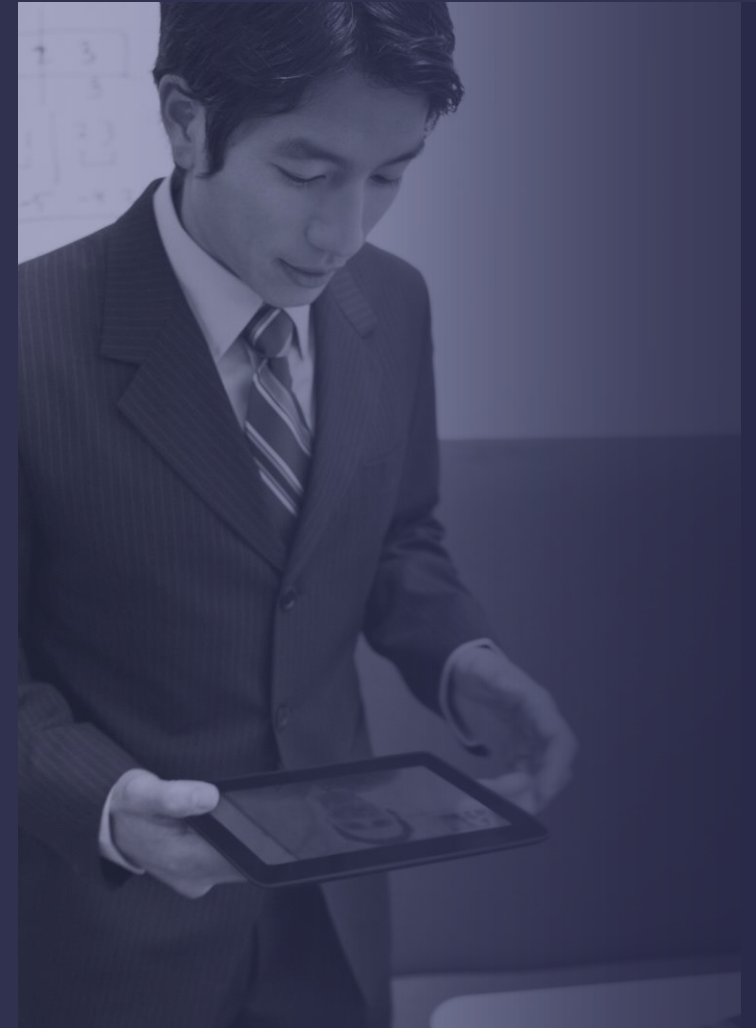
지능화된 공격



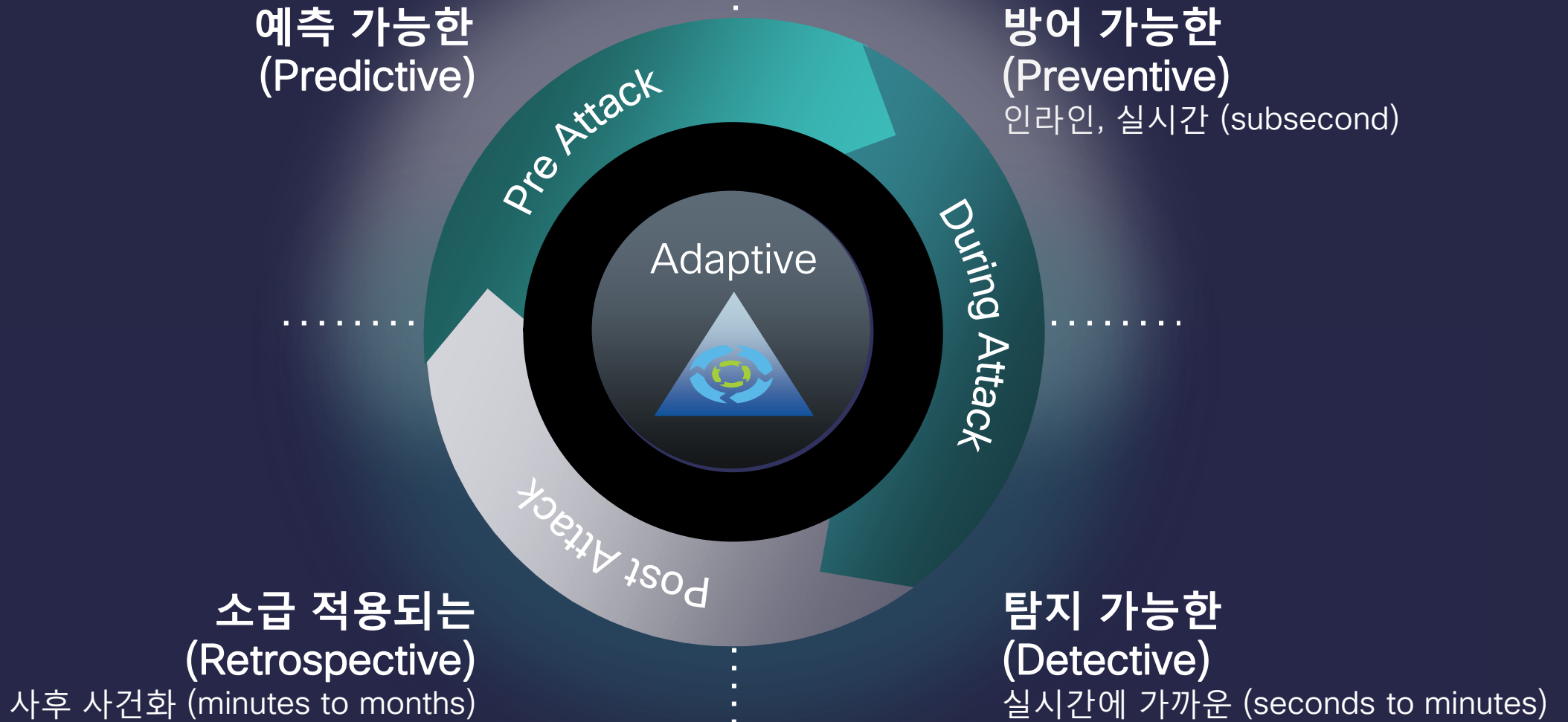
고정적이고
수작화됨

느린 대응

피해 확산

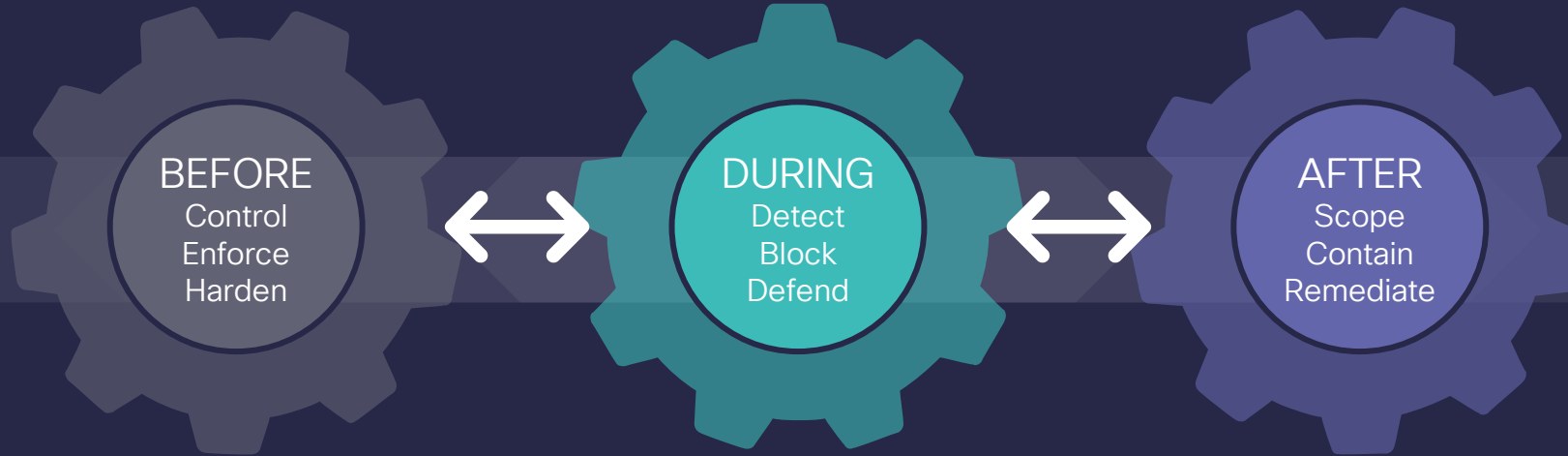


보안 요구 진화의 수렴: 적응형 보안 설계를 위한 가트너의 새로운 보안 모델



시스코의 지속적인 공격 전반에 걸친 통합 위협 방어 모델

Attack Continuum



방화벽/VPN	차세대 IPS	지능형 악성코드 차단
세밀한 어플리케이션 통제	보안 인텔리전스	회귀적 분석 및 보안
최신의 위협 통제	웹 사용 보안	침해 지표 및 사고 대응

가시성 및 자동화

현재의 네트워크 보안 플랫폼의 역할과 현실

차세대 네트워크 보안 요구 기능	방화벽/VPN	침입방지시스템	차세대방화벽
고급 네트워킹 기능 대용량, 고성능, 라우팅, 고가용성, 가상화, L2/L3 모드 및 혼합배치	부족	보통	매우부족
지능형 방화벽 기능 Application Layer Gateway, Stateful Inspection, NAT/PAT, QoS, 정책관리	보통		부족
VPN 기능 IPSec/SSL/L2TP 등 다양한 VPN 통합, IKEv2 및 차세대 암호 모듈 지원	부족		매우부족
L7 방화벽 기능 어플리케이션 및 사용자 인식기반 제어, 행위기반 제어, 평판기반 필터링	부족		우수
진화된 침입방지시스템 기능 실시간 자산인식, 어플리케이션인식, 글로벌 위협정보 반영, 실영향도기반		보통	매우부족
악성코드 방어 기능 안티 악성코드 월, 샌드박싱, 회귀적 분석, 전파 경로 추적			부족

지능형 지속 위협에 대한 대안! 적응형 보안 기술이 탑재된 시스코 ASA with FirePOWER Service

업계 최초의 위협 중심 차세대 방화벽



#1 Cisco Security announcement of the year!

검증된 시스코 ASA-X 방화벽



업계선도의 NGIPS 및 AMP



시스코 ASA with FirePOWER Services

- 최상의 가시성을 확보를 지원하는 방어 계층 **통합**
- 다양한 보안 위협에 대한 **적응 및 동적인 통제** 수단 제공
- 공격 전반에 걸친 지속적이고 지능화된 위협으로부터의 **전방위적 보호** 기능 제공

최고의 통합 및 멀티레이어 보안 솔루션



전세계에서 가장 많이 사용되고 있는 엔터프라이즈 급 ASA-X 지능형 방화벽

세밀한 시스코의 어플리케이션 가시화 및 통제 기능 (AVC)

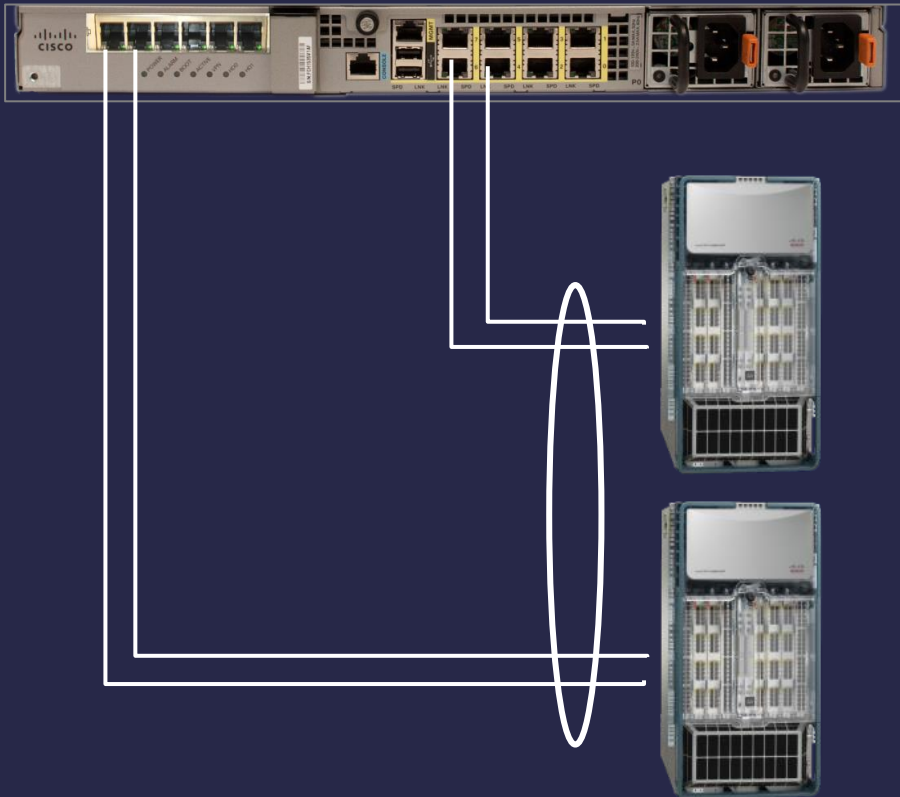
업계를 리딩하는 FirePOWER 차세대 IPS (NGIPS)

평판 및 카테고리 기반 URL 필터링 및 사용 통제

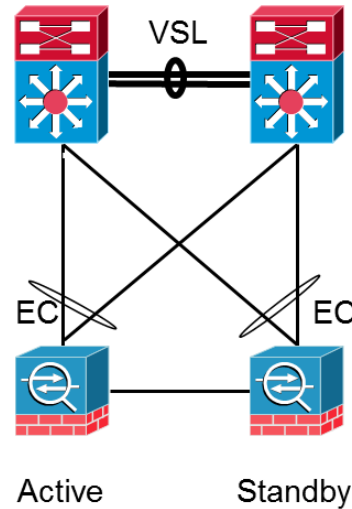
지능형 악성코드 차단(AMP)

멀티샤시 이더채널링(MEC)

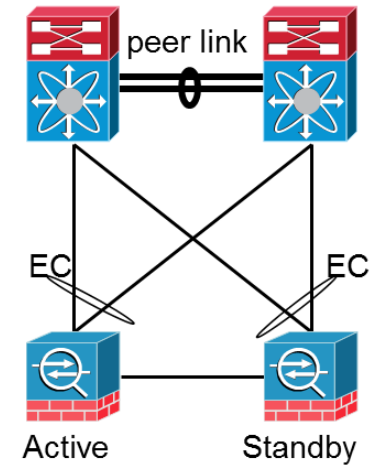
- 신속한 토폴로지 변화 수렴에 의한 안정성 제공 및 구성의 복잡성을 완벽하게 간소화



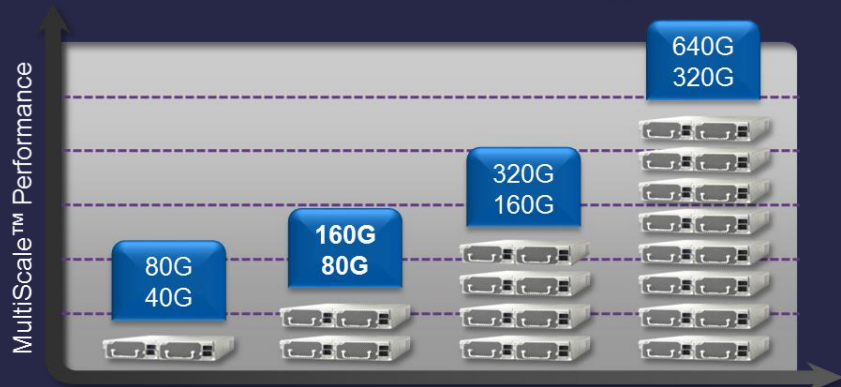
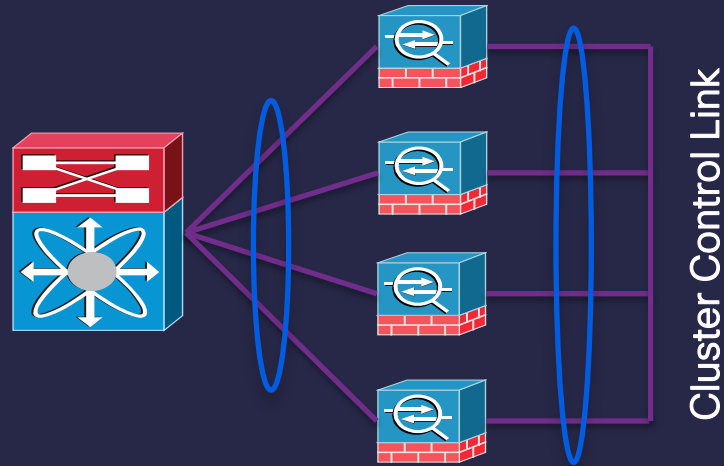
Catalyst 6500 Switch
Virtual Switching System



Nexus 7000 Switch
Virtual PortChannel



방화벽 클러스터링



Scaling Factor

- 최대 16개의 방화벽 및 FirePOWER Service 모듈 클러스터링
- 최대 방화벽 성능 640Gbps, 적응형 보안 기능 적용에 따라 성능 영향

N-to-N HA

- 모든 유닛은 Active로 운영, 무중단 업그레이드
- 노드 장애시에도 트래픽에 영향없이 서비스 가능

Redundancy

- 유닛별 그리고 전체 트래픽 플로우는 클러스터 내에서 모두 백업됨

Flexibility

- 모든 ASA mode 지원함
- Transparent, Routed, Mixed

Manageability

- 단일 설정, 클러스터내에서 자동 sync, 원격에서 명령어 실행 가능
- 클러스터 차원의 자원 사용량 통계 제공

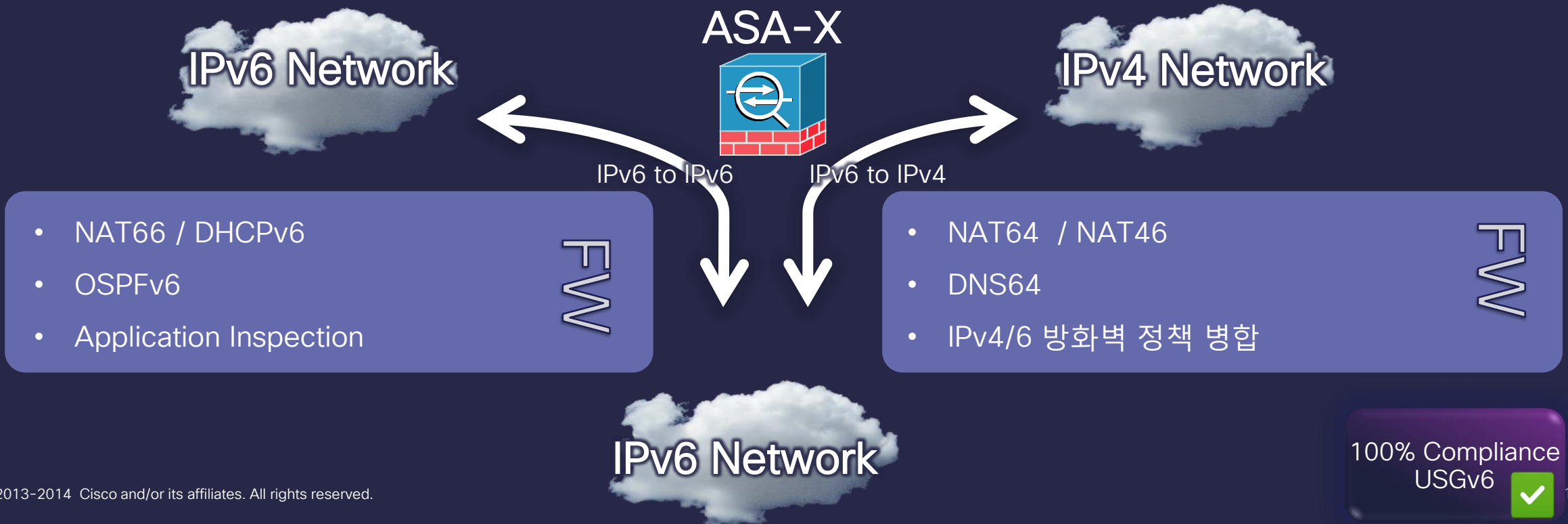
Troubleshooting

- 패킷 캡처 기능
- 상시 이벤트 추적 로그 제공

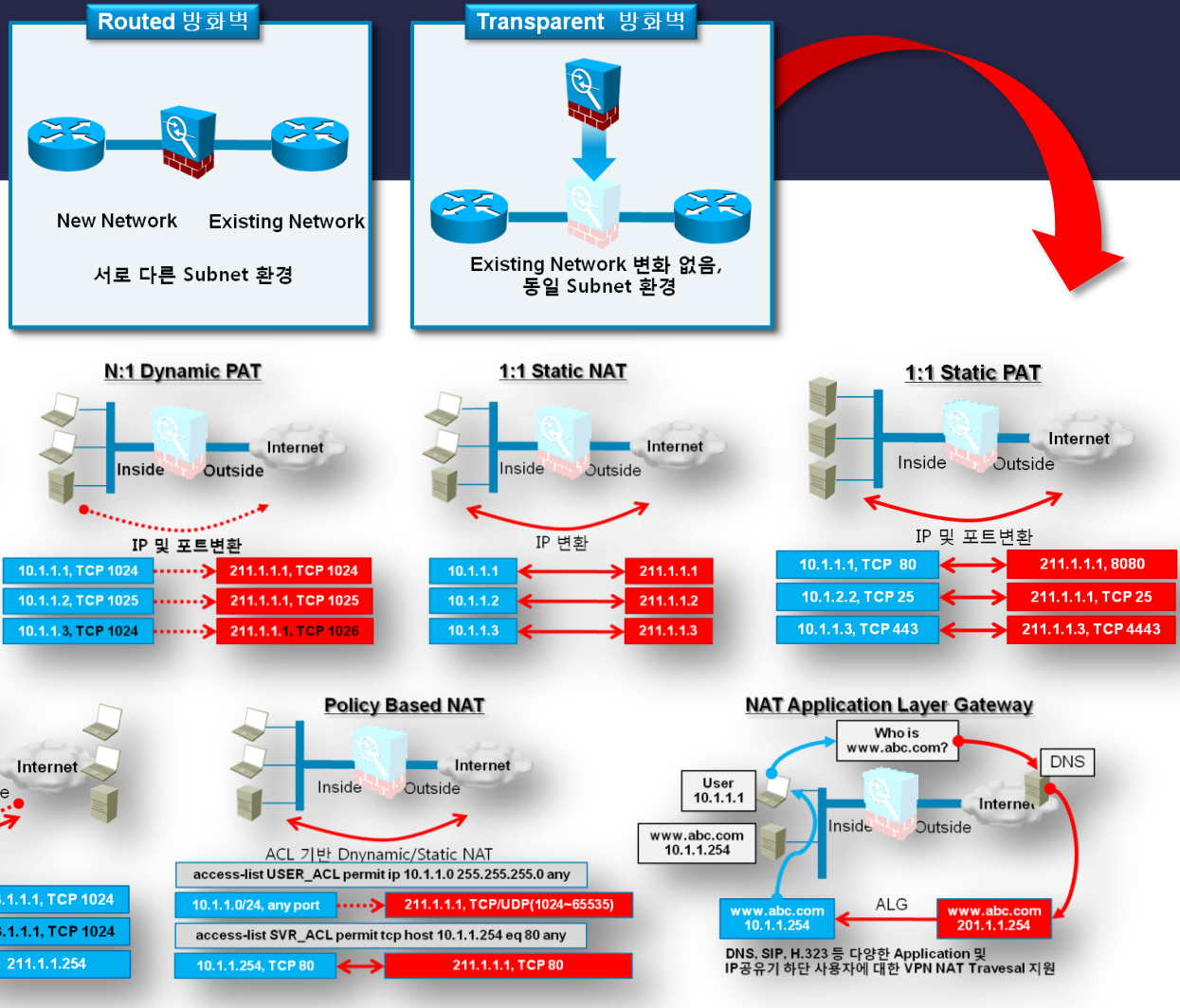
성능감소 없는 IPv6 기반 네트워킹 및 보안 기능

- IPv6, IPv4 듀얼스택 클라이언트 및 헤드엔드 지원
- AnyConnect 및 Clientless SSL VPN 지원
- 모든 주요 모바일 및 PC 운영체제와 브라우저 지원
- Site-to-Site VPN 지원
- 시스코 가상데스크탑 지원
- 보안 상태 점검 기능 지원

VPN



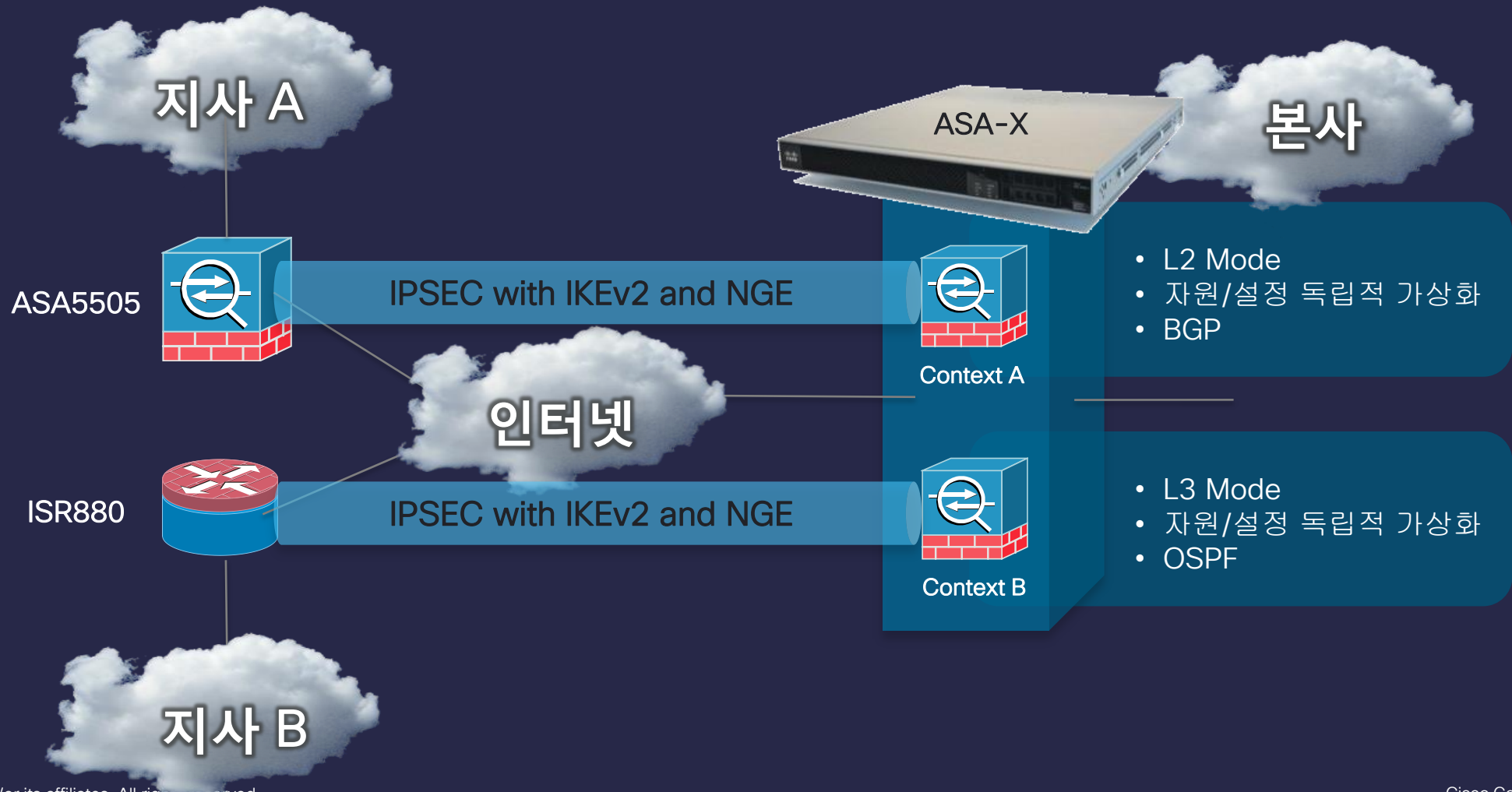
다양한 NAT/PAT 및 보안 기능



추가된 기능(v8.4 이상)

- 세션 기반 PAT Idle Timeout 설정
- PAT Sticky Option 기본 설정
- PAT 대표 IP 할당 알고리즘 추가
 - Sequence 방식
 - Round Robin 방식

고급화된 가상화 기능



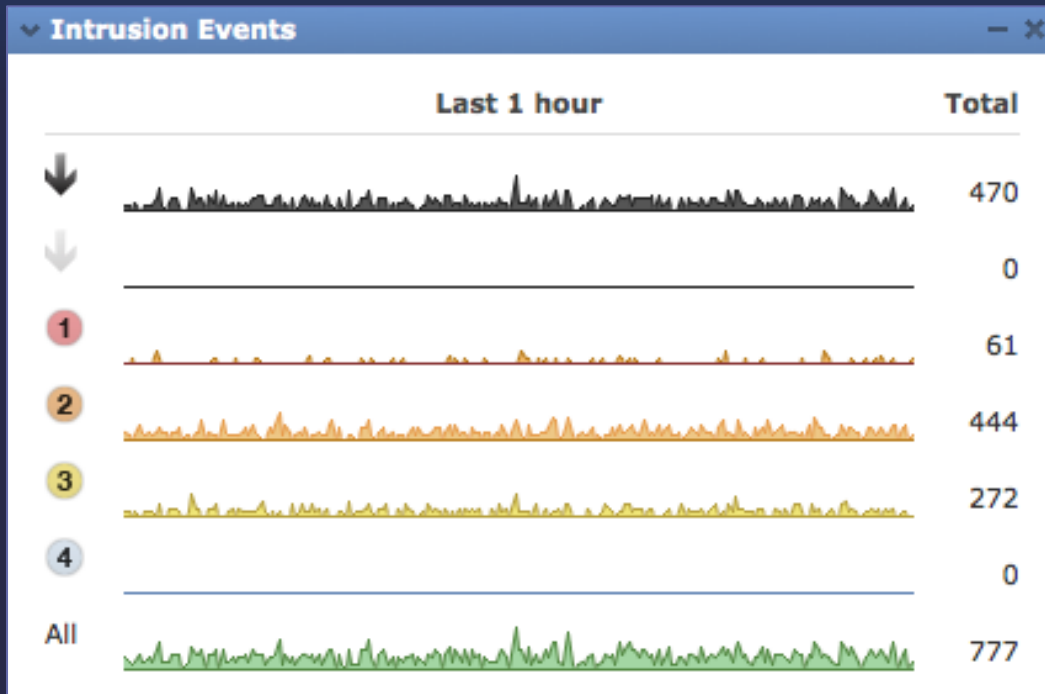
지능형 지속 위협 공격에 대한 핵심은 “가시화”

FirePOWER Brings Unprecedented Network Visibility

	Threats	Users	Web Applications	Application Protocols	File Transfers	Malware	Command & Control Servers	Client Applications	Network Servers	Operating Systems	Routers & Switches	Mobile Devices	Printers	VoIP Phones	Virtual Machines
FirePOWER Services	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Typical IPS	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Typical NGFW	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗

실질적인 공격 영향도 기반의 효과적인 대응

Correlates all intrusion events to an impact of the attack against the target



영향도	보안관리자 대응	이유
1 (Red Flag)	즉각적인 대응, 취약한	취약점이 있는 대상으로의 유효한 공격
2 (Yellow Flag)	조사 필요, 취약할 가능성이 있는	수집된 취약성이 없는 OS 또는 실제 서비스중인 대상 공격
3 (Yellow Flag)	확인만, 현재는 취약하지 않는	해당공격 대상 서비스가 없음
4 (Blue Flag)	확인, 모르는 대상	해당공격 대상 이 존재 하지 않음
0 (White Flag)	확인, 모르는 네트워크	Unmonitored network

자동화, 통합된 위협 방어

지속적인 공격 전반에 걸친 완벽한 보호



Context
and Threat
Correlation



Dynamic
Security Control



Multi-vector
Correlation



Retrospective
Security

자동화, 통합된 위협 방어

지속적인 공격 전반에 걸친 완벽한 보호



Context
and Threat
Correlation



Dynamic
Security Control



Multi-vector
Correlation



Retrospective
Security

자동화, 통합된 위협 방어

지속적인 공격 전반에 걸친 완벽한 보호



Context
and Threat
Correlation



Dynamic
Security Control



Multi-vector
Correlation



Retrospective
Security

자동화, 통합된 위협 방어

지속적인 공격 전반에 걸친 완벽한 보호



Context
and Threat
Correlation



Dynamic
Security Control



Multi-vector
Correlation



Retrospective
Security

침해 지표 (IoC : Indications of Compromise)

Indications of Compromise (3) Edit Rule States Mark All Resolved

Category	Event Type	Description	First Seen	Last Seen
Exploit Kit	Intrusion Event - exploit-kit	The host may have encountered an exploit kit	2013-09-17 16:46:28	2013-09-20 06:35:31
CnC Connected	Security Intelligence Event - CnC	The host may be under remote control	2013-09-17 16:52:11	2013-09-20 03:55:45
CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2013-09-17 20:09:23	2013-09-19 17:32:49

Exploit Kits
Web App Attacks
CnC Connections
Admin Privilege Escalations

Connections to Known CnC IPs

Office/PDF/Java Compromises
Malware Executions
Dropper Infections

AMP에 의한 지속적인 보호 기능 적용 및 회귀적인 보안 대응

Breadth of Control Points



Email



Endpoints



Web



Network



IPS



Devices

Telemetry Stream



File Fingerprint and Metadata



File and Network I/O



Process Information

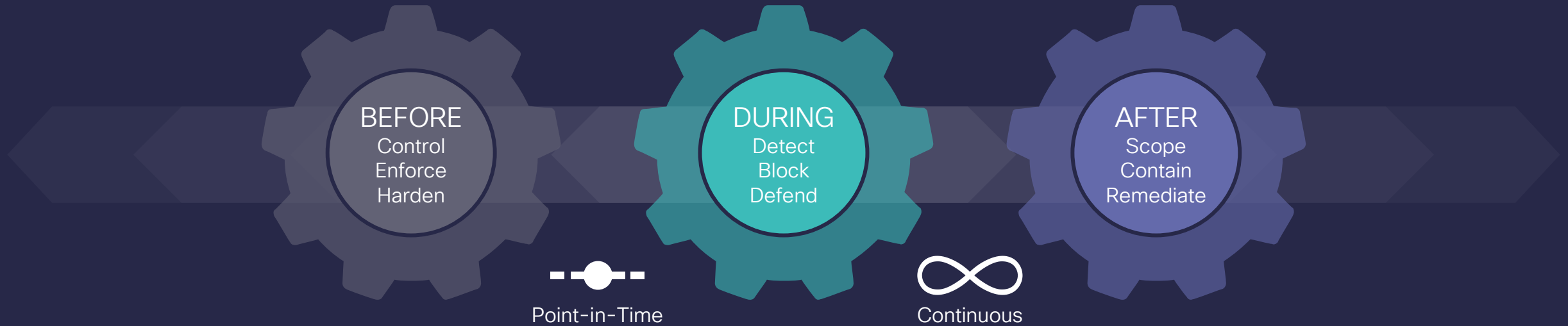
Continuous Feed

111010011101 1100001110001110 1001 1101 1110011 0110011 10
1110 1001 1101 1110011 0110011 101000 0110 00 0111000
00001 1100 0111010011101 1100001110001110 1001 1101 11

Continuous Analysis



악성코드의 Before, During, 그리고 After 전반에 걸친 보호



With Unmatched Visibility, Control, and Advanced Threat Remediation Functionality



Retrospection



Retrospective
Detection



Behavioral Indications
of Compromise



Trajectory



Threat Hunting

시스코 ASA with FirePOWER Services

기본 하드웨어



- New ASA 5585-X Bundle SKUs with FirePOWER Services Module
- New ASA 5500-X SKUs running FirePOWER Services Software
- FirePOWER Services Spare Module/Blade for ASA 5585-X Series
- FirePOWER Services Software
- Hardware includes Application Visibility and Control (AVC)



Security
Subscription
Services

- IPS, URL, Advanced Malware Protection (AMP) Subscription Services
- One- and Three-Year Term Options



Management

- FireSIGHT Management Center (HW Appliance or Virtual)
- Cisco Security Manager (CSM) or ASDM



Support

- SmartNET
- Software Application Support plus Upgrades

Additional Professional and Technical Services



SMARTnet Technical Support

Keep security solutions available by providing access to broad Cisco support tools and expertise



Migration Services

Move more quickly to new capabilities and with minimal disruption



Managed Services

Provide full-time, proactive, systematic threat monitoring and management

Cisco ASA with FirePOWER Services

A New, Adaptive, Threat-Focused NGFW



Integrated Threat Defense

Best-in-class, multilayered protection in a single device



Superior Visibility

Full contextual awareness to eliminate gaps



Automation

Simplified operations and dynamic response and remediation

시스코 ASA with FirePOWER Services

업계 최초의 적응형, 위협 중심의 차세대 방화벽



→ 기능

- 시스코의 ASA 지능형 방화벽과 소스파이어의 차세대 IPS의 통합
- 지능형악성코드에 의한 지속적인 공격 전반에 걸친 위협 방어
- 최상의 보안 인텔리전스
- 패시브 방식의 실시간 자산 인식
- 어플리케이션 가시화 및 통제
- 무분별한 웹사용 통제 및 평판기반 URL 필터링

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

→ 기대효과

- 기존 네트워크 보안 체계와 1:1 맞교체가 가능한 차세대 보안 설계
- 우수한 다계층적인 위협 보호
- 최상의 네트워크 가시화 제공
- 지능형 지속 공격 방어 및 대응
- 복잡성 및 비효 절감 효과

Thank you.

