체크포인트 소프트웨어 테크놀로지스

Check Point®
SOFTWARE TECHNOLOGIES LTD

INDEX

체크포인트 역사

Check Point
SOFTWARE TECHNOLOGIES LTD

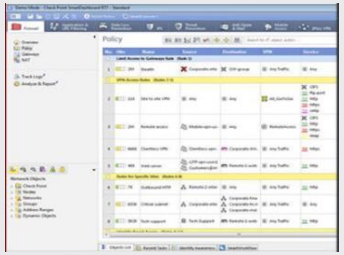
Check Point 역사

보안시장에서의 20년

Firewall-1

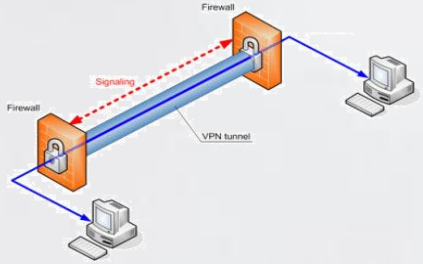
1993년

시큐리티 매니지먼트



1994년

VPN



1996년

가상화 시스템

2002년

소프트웨어 블레이드 아키텍처

2009년

2011년

차세대 방화벽

2012년

ThreatCloud

2013년

쓰렛 에뮬레이션

2015년

샌드블라스트

2016년

vSEC

Check Point 역사

보안시장에서의 20년

START

Internet Security Corporation

1994년 첫번째 공식 파트너 지정

1994년 NASDAC 첫 공모

1994년 수익 $1.41억

- 첫 1억불 이상 수익 달성

2000년 첫번째 CPX 개최

- CPX (Check Point Experience)
  - 보안 전문가들과 함께 최신 보안 트렌드 정보공유 세미나

2007년 첫 기업용 장비 UTM-1 출시

2015년 수익 $16억 달성

체크포인트 개요

Check Point
SOFTWARE TECHNOLOGIES LTD

Check Point 개요

마켓 리더십

순수 보안벤더
최대 규모

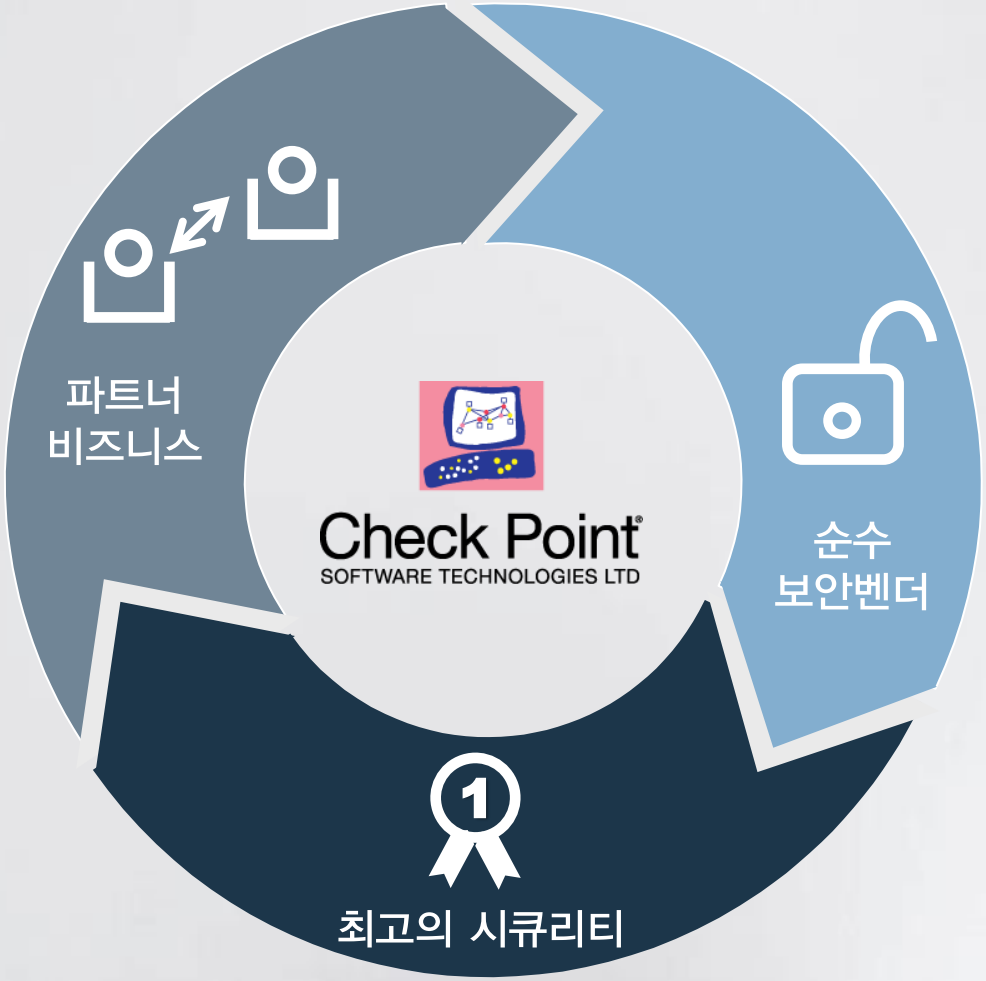
R&D 직원 수
1,300 명

고객 수
100,000명 이상

매직 쿼런트 리더 **19년 연속**	관리체계 **최고 효율**
IDC, Gartner 시장 점유율 **#1**	NSS 추천 등급 **업계 최다**
언노운 멀웨어 **최고 탐지율**	취약점 **가장 빠른 대응**

출저 : Miercom APT Industry Assessment 2014, Forrester Automated Malware Analysis Q2 2016, NSS Labs Breach Detection Systems (BDS) Test Report 2016

Check Point 개요



✓ 파트너 비즈니스

- 파트너의 성공 = 체크포인트의 성공
- 100% 파트너가 이끄는 세일즈

✓ 순수 보안 벤더

- 보안에만 집중하는 마켓 리더

✓ 최고의 시큐리티

- 공인된 기관(IDC, Gartner) 에서 높은 평가
- Fortune이 선정한 100대 기업

Check Point 개요

Gartner®

체크포인트는 2015년 4분기 방화벽 시장에서 세계적으로 21.5% 를 차지하며 세계 시장 점유율을 이끌고 있습니다.

IDC
Analyze the Future

체크포인트는 2015년 4분기 방화벽과 UTM 어플라이언스에서 글로벌 마켓 선두주자입니다.

Check Point 개요

NSS Labs가 인정한 체크포인트

NSS 그룹 테스트 – 특정 제품군 여러개 벤더 비교 테스트
추천등급 : 보안성과 가성비가 모두 뛰어난 우수 등급 (최고등급)
중립등급 : 보안성과 가성비 관점에서 중립
주의등급 : 보안성 등 사용자의 주의 필요 (최저등급)

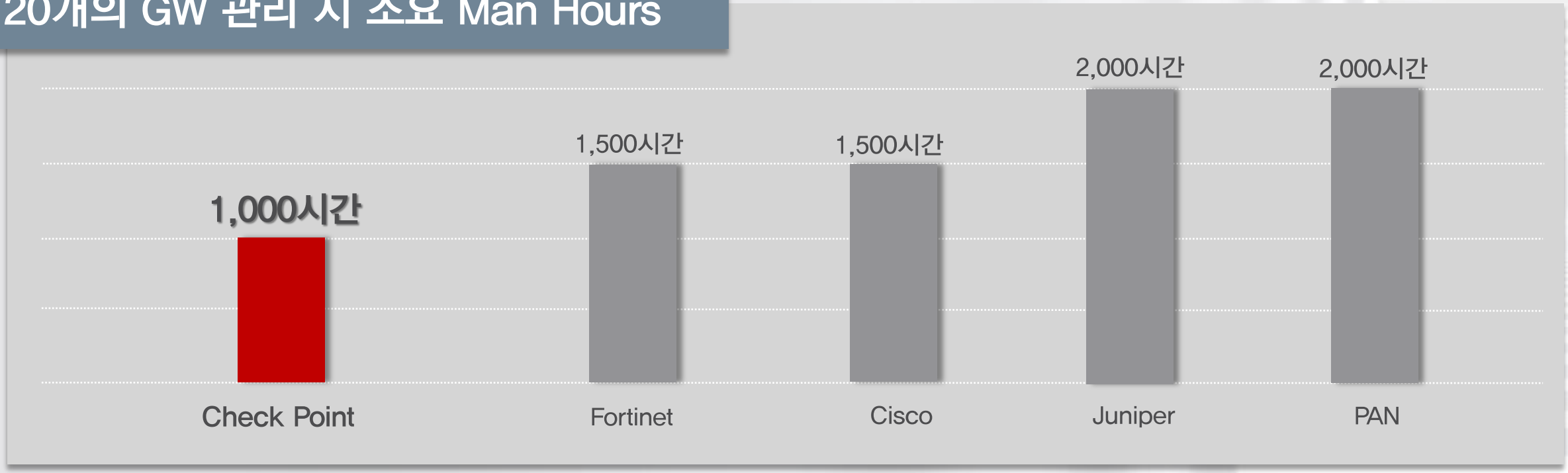
	추천 등급	중립 등급	주의 등급
체크 포인트	13	0	0
팔로 알토 네트워크	6	3	2
시스코	6	6	0
포티넷	10	4	0
주니퍼	2	3	4
파이어 아이	0	1	2

보안 벤더사 중 '주의' 및 '중립' 등급이 없는 유일한 벤더

Check Point 개요

효율적인 관리체계

20개의 GW 관리 시 소요 Man Hours



"체크포인트의 관리시스템은 다른 콘솔들에 견주면 **모범이 되는 사실상의 표준**이라 이를 만 하다. *(de facto gold standard)*"

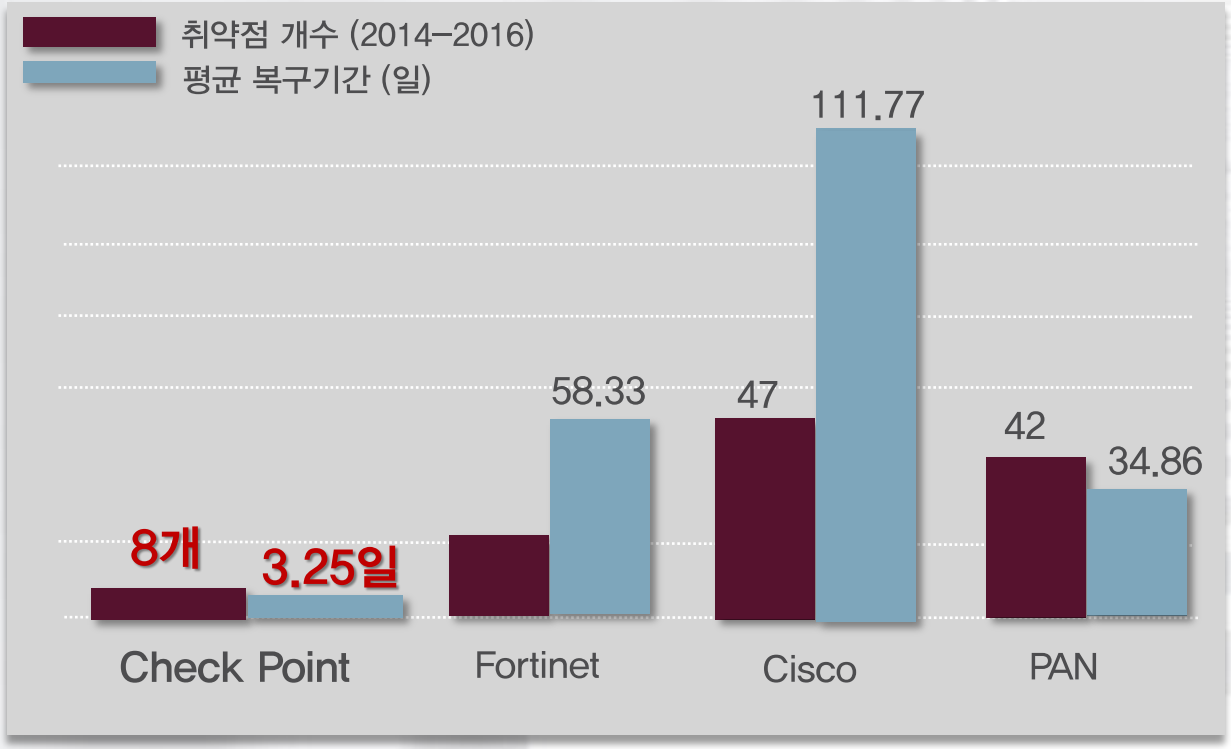
Gartner

Check Point 개요

체크포인트 보안 DNA1

체크포인트 vs 경쟁사 벤더 취약점 대응 시간

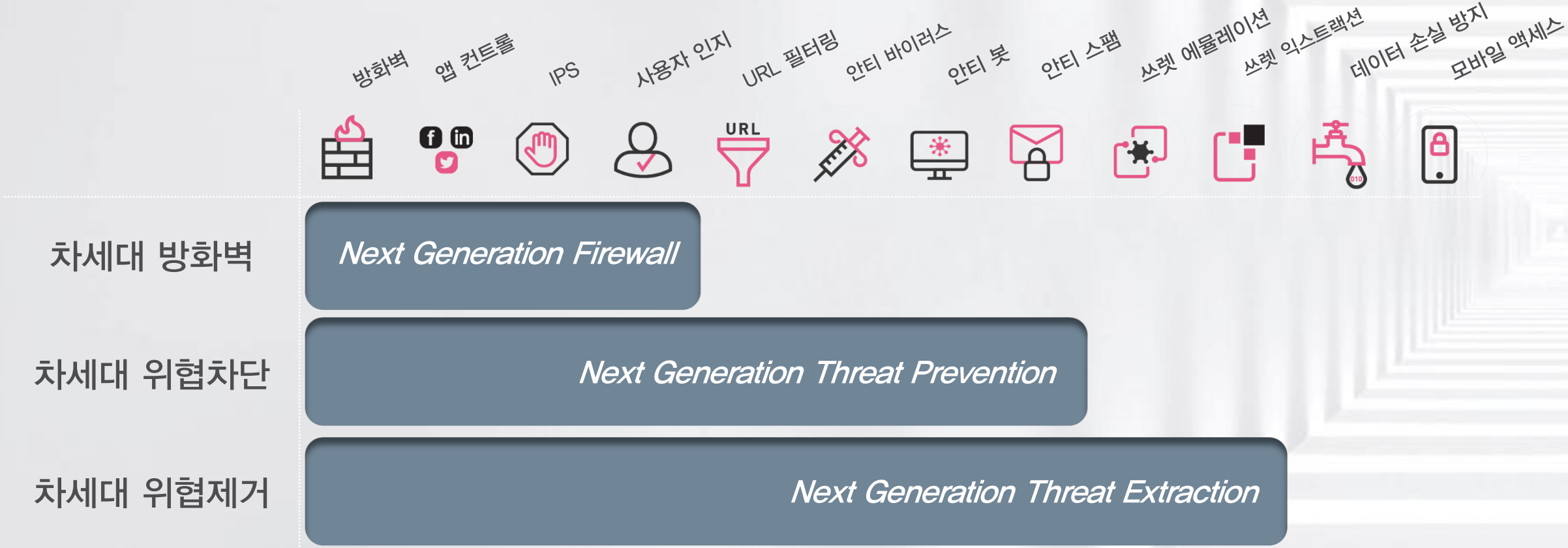
Check Point	취약점	PAN	Fortinet
9시간	Heartbleed	4일	5일
22시간	Shellshock	29일	14일
18시간	Poodle–TLS	56일	10일
30시간	Venom	10일	9일



경쟁사 대비 적은 취약점과 빠른 대응

Check Point 개요

체크포인트 보안기능 (소프트웨어)



Check Point 개요

풀 레인지에 걸친 어플라이언스 (소프트웨어 + 하드웨어)

3200 어플라이언스
1400 어플라이언스
(4 모델)

SOHO

5000 어플라이언스
(4 모델)

SMB

15000 어플라이언스
(2 모델)

엔터프라이즈

23000 어플라이언스
(2 모델)

*데이터센터,
엔터프라이즈*

41000 어플라이언스
(1 모델)

*데이터센터,
캐리어*

61000 어플라이언스
(1 모델)

*데이터센터,
캐리어*

모든 성능요구 영역에 대응 가능한 어플라이언스

체크포인트 소프트웨어 테크놀로지스

제품 소개

Check Point®
SOFTWARE TECHNOLOGIES LTD

INDEX

체크포인트
차세대 방화벽
(Next Generation Firewall)

Check Point
SOFTWARE TECHNOLOGIES LTD

차세대 방화벽 (NGFW)

체크포인트 차세대 방화벽

어플리케이션 컨트롤

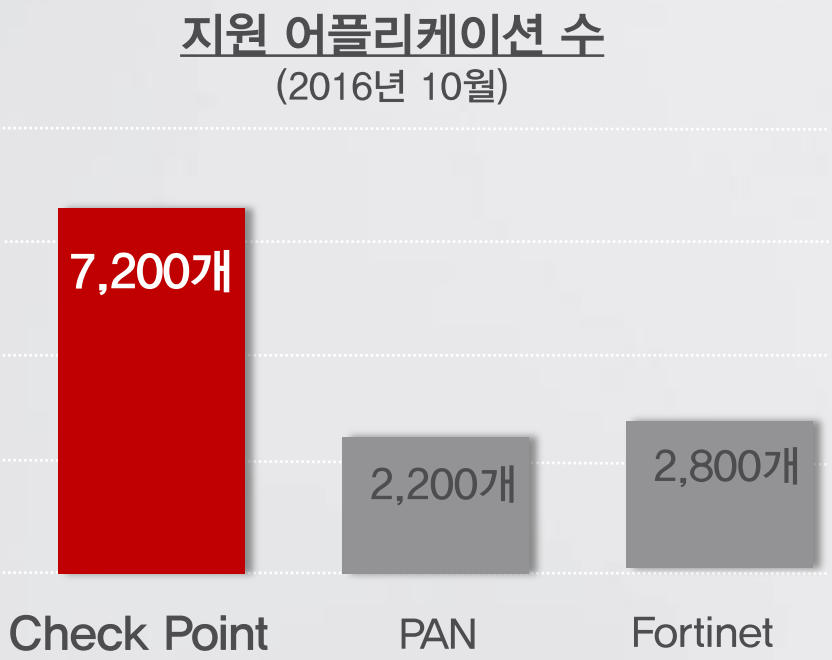
- 어플리케이션을 IP/Port 대신 고유의 시그니쳐 기반으로 통제

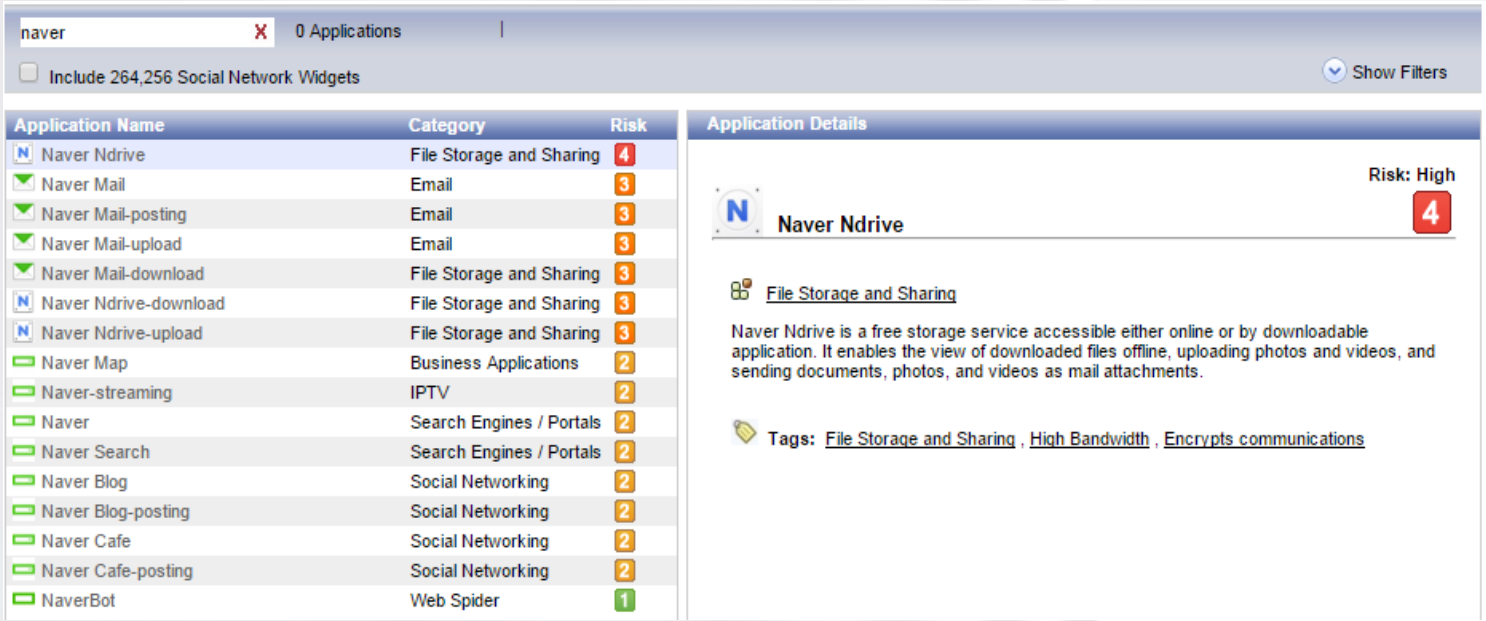
IPS

- 취약점에 대한 공격 차단 (시그니쳐 기반 & 어노말리 차단)

차세대 방화벽 (NGFW)

체크포인트 차세대 방화벽 장점_ *어플리케이션 컨트롤*





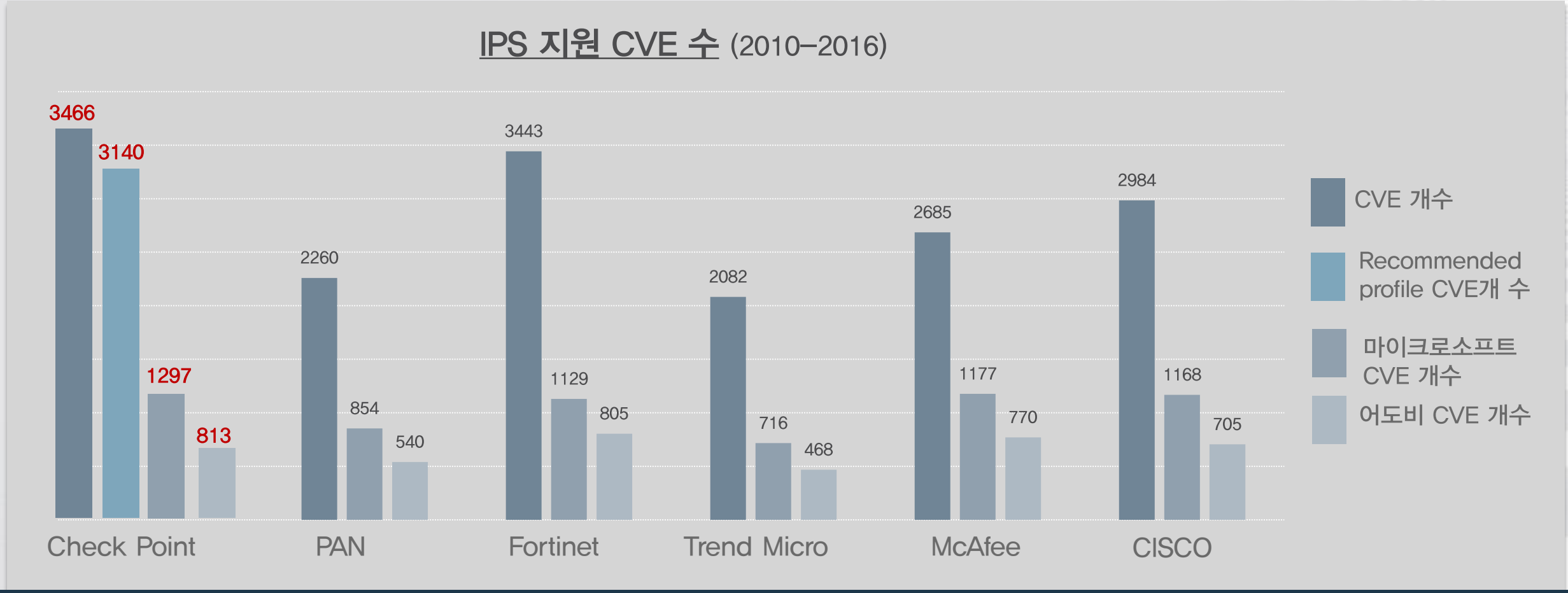
- TCP / UDP 포트 대신 어플리케이션 기반 제어
- 264,000 소셜 네트워크 위젯
- 월등한 가시성과 함께 세밀한 통제 가능

- 7200개 이상의 어플리케이션 지원 (업계 최다)
- 140개의 카테고리 지원
  (Web 2.0, IM, PWP, Voice & Video, File share)

차세대 방화벽 (NGFW)

체크포인트 차세대 방화벽 장점_ *침입 차단 시스템 (IPS)*

알려진 취약점에 대한 공격시도 차단 시그니처 검사, 프로토콜 사양 준수 검사, 어노말리 검사



체크포인트
차세대 위협 차단
(Next Generation Threat Prevention)

Check Point®
SOFTWARE TECHNOLOGIES LTD

차세대 위협 차단 (NGTP)

체크포인트 차세대 위협 차단

URL 필터링

- 카테고리 기반의 웹 페이지 접근 제어

안티 바이러스

- 멀웨어 다운로드 차단 및 멀웨어 배포 사이트 접근 차단

안티 봇

- Bot에 감염된 사용자 탐지 및 Bot과 C&C 서버간 통신 차단

안티 스팸

- 스팸 메일 차단

차세대 위협 차단 (NGTP)

체크포인트 차세대 위협 차단

ThreatCloud

- 클라우드 기반의 보안 지식 데이터 베이스
- 가장 빠르게 확장되는 세계 최대의 보안 인텔리전스
- 전 세계 체크포인트 GW와 실시간 연동
- 50만 업데이트 / Day

+ 500,000,000

악성파일 해쉬와 악성 사이트

+ 10,000

봇 시그니처

+ 10,000,000

봇 어드레스

체크포인트
차세대 위협 제거
(Next Generation Threat Extraction)
– Sandblast Family

Check Point
SOFTWARE TECHNOLOGIES LTD

차세대 위협 제거 (NGTX)

체크포인트 차세대 위협 제거

쓰렛 에뮬레이션

- 알려지지 않은 위협을 행위기반 (샌드박싱)으로 탐지
- OS 기반 샌드박스와 CPU 레벨 탐지를 함께 제공

쓰렛 익스트랙션

- 문서에서 위협이 되는 동적요소(매크로, 스크립트, 링크 등)를 지연없이 제거 한뒤 사용자에게 전달

차세대 위협 제거 (NGTX)

Detection vs Prevention

DETECTION

PREVENTION

제한적 방어

선제적 원천 방어

랜섬웨어란?

인터넷 사용자의 컴퓨터에 잠입해 내부 문서나 스프레드 시트, 그림파일 등을 암호화해 열지 못하도록 만든 후 돈을 보내주면 해독용 열쇠 프로그램을 전송해 준다며 금품을 요구하는 악성 프로그램

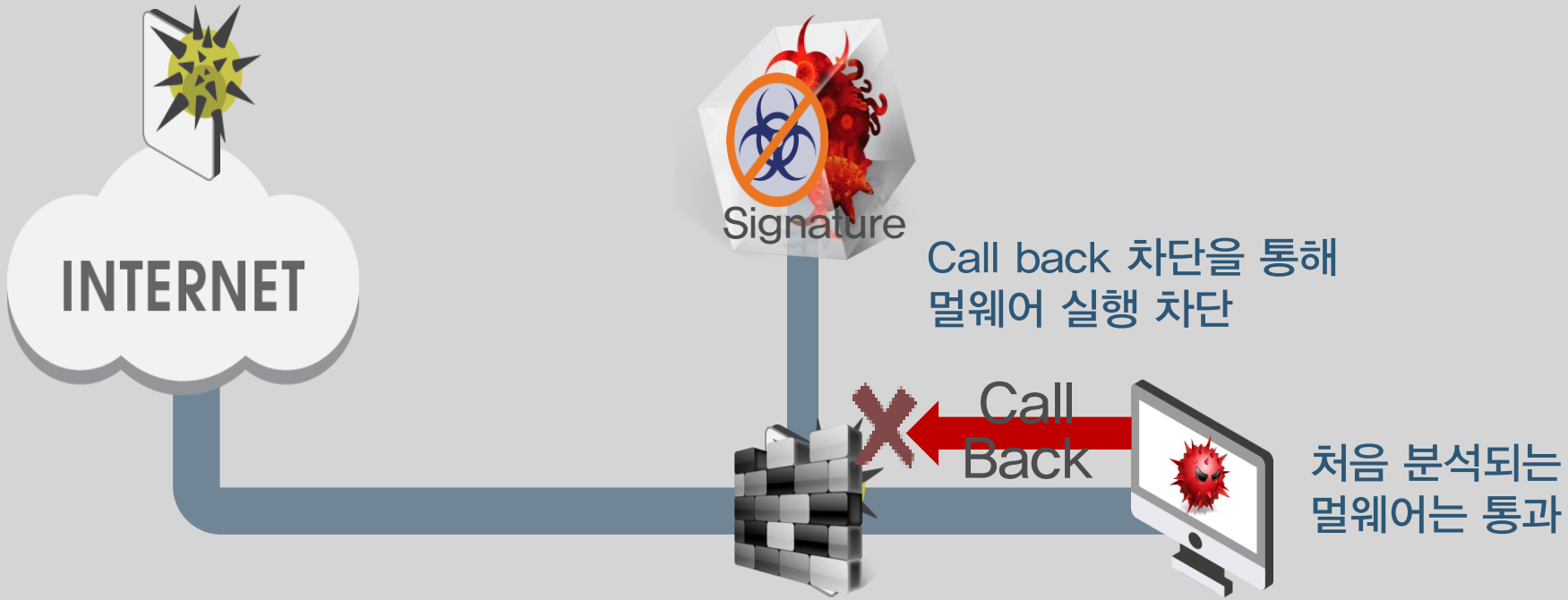
차세대 위협 제거 (NGTX)

랜섬웨어 공격

침입 → 실행 → 컨텐츠 암호화 → 사용자 알림 → 지불 → 복호화

Call back이 필요 없는 멀웨어라면?

1세대 샌드박스는 랜섬웨어에 어떻게 대응하는가?



차세대 위협 제거 (NGTX)

샌드블라스트 개요

알려지지 않은 멀웨어에 대한 선제적 보안

1 CPU 레벨 차단

- 가장 높은 탐지율
- 우회기법에 대응하는 멀웨어 탐지

2 Threat Extraction

- 문서에서 멀웨어를 제거
- 적극적인 차단방식

CHECK POINT
SandBlast™
ZERO-DAY PROTECTION

OS레벨 샌드박스와
CPU 레벨 디텍션을 조합하여
가장 높은 탐지율 제공

차세대 위협 제거 (NGTX)

샌드블라스트 선제적 멀웨어 차단_ ***체크포인트 유일***

CHECK POINT SandBlast™ ZERO-DAY PROTECTION

CPU 차단 엔진

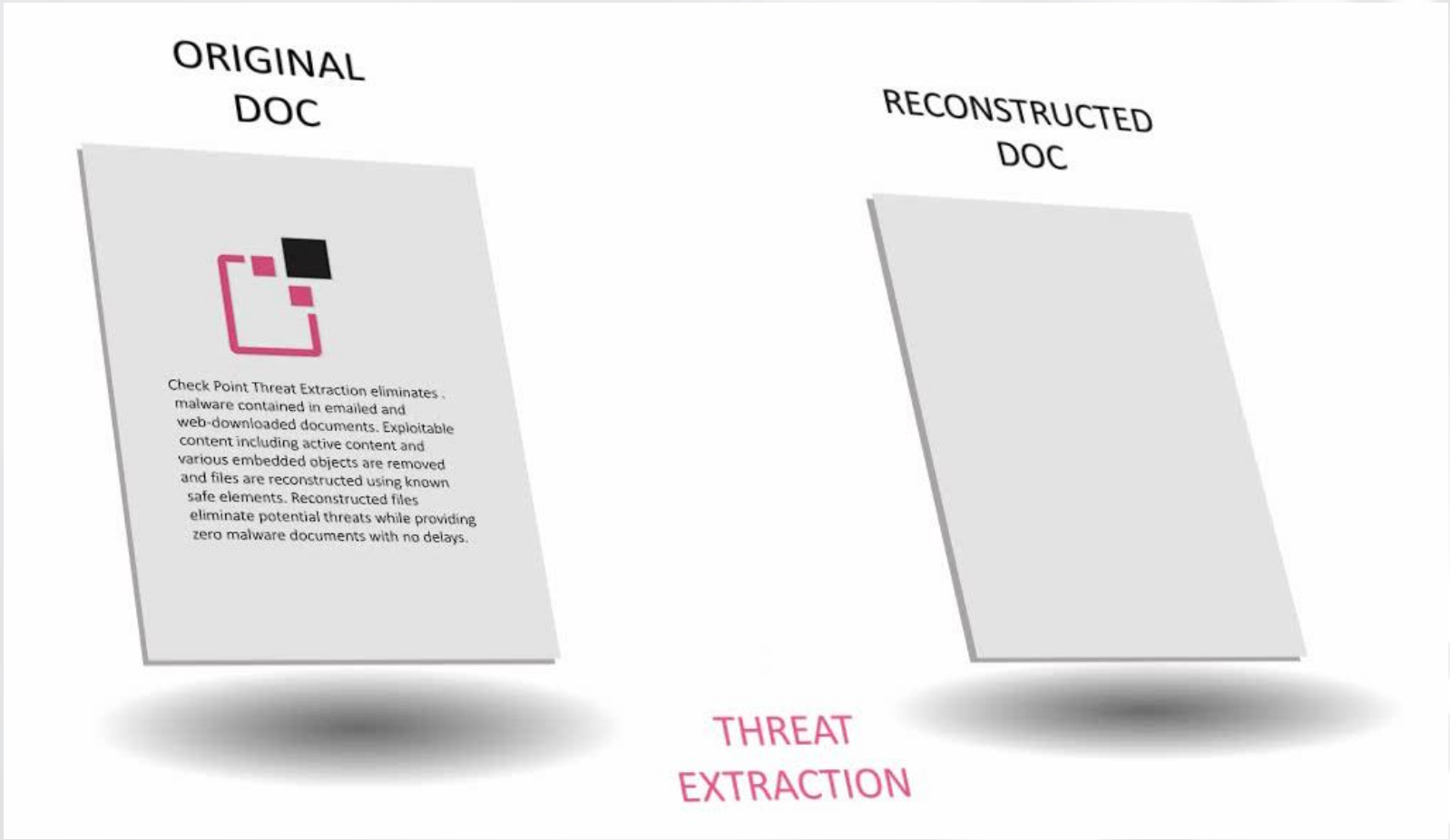
말웨어가 다운로드 되거나
보안 우회기법이 발현되기 전
CPU레벨에서 위협 차단

전통적인 샌드박스

OS 레벨 차단
(기존 타 벤더)

차세대 위협 제거 (NGTX)

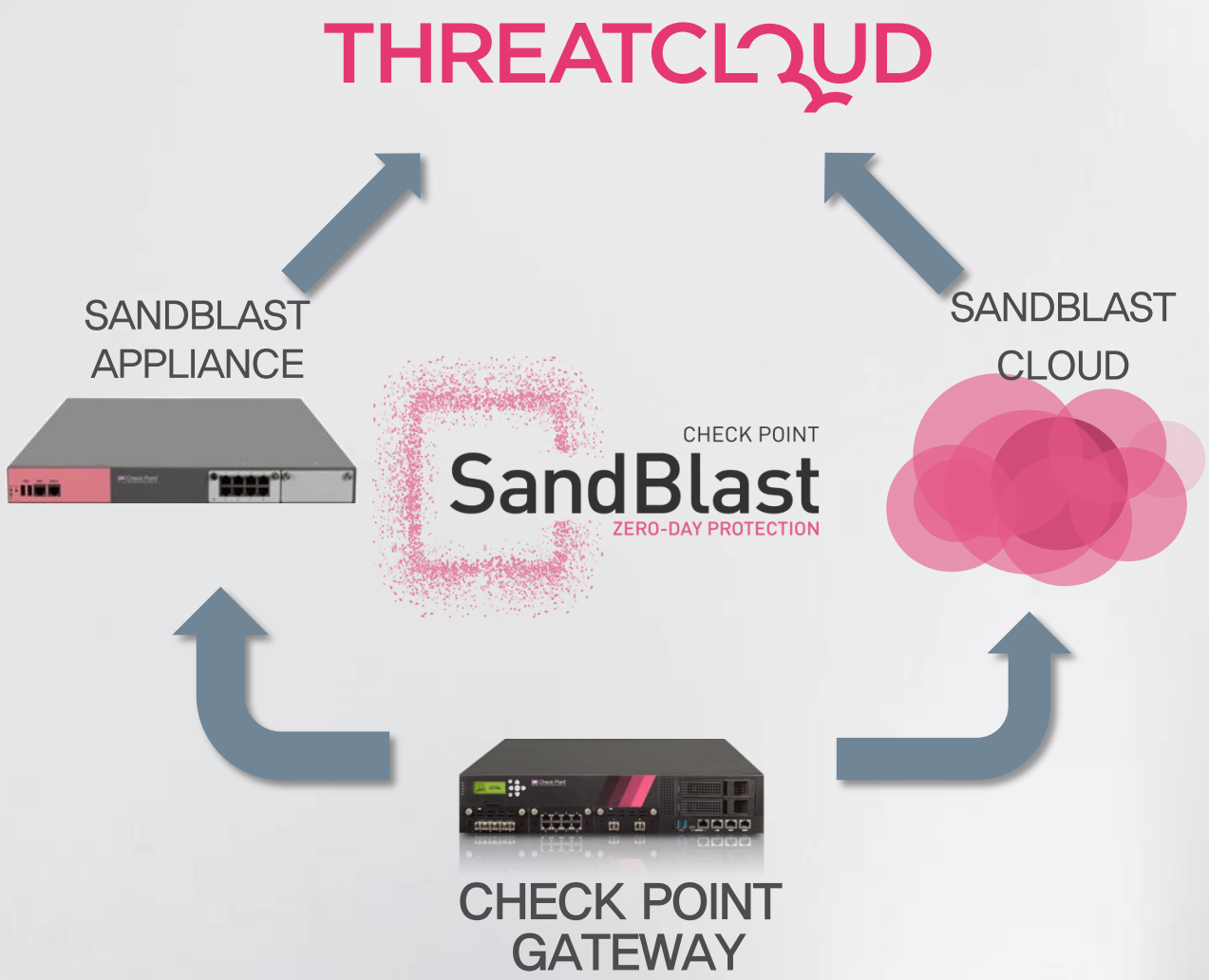
샌드블라스트 쓰렛 익스트랙션_ ***체크포인트 원천기술***



위협을 먼저 제거한 뒤 샌드박싱을 통해 지연 없이 깨끗한 파일 전송

차세대 위협 제거 (NGTX)

샌드블라스트 구성 방식



웹과 이메일
모두 사용 가능

차세대 위협 제거 (NGTX)

샌드블라스트 에이전트

CHECK POINT SandBlast ZERO-DAY PROTECTION

엔드포인트(사용자 PC) 까지
적용범위 확장

CHECK POINT SandBlast™ AGENT

- 더 많은 멀웨어 탐지
- 사전에 예방
- 어떤 곳에서 사용하더라도 보호가능
- 완벽한 통합 보호

차세대 위협제거 (NGTX)

엔드포인트에서 제로데이 멀웨어 차단

1 다운로드한 파일을 SandBlast로 전달

2 깨끗한 버전의 문서를 즉시 전달

3 백그라운드로 원본 에뮬레이션

차세대 방화벽 (NGFW)

샌드블라스트 에이전트 감염 식별 및 격리 방법

2 ANTI-BOT
아웃바운드 트래픽 검사

1 THREAT INTELLIGENCE
보안 인텔리전스 제공

CHECK POINT THREATCLOUD™

3 C&C traffic
트래픽 차단

4 QUARANTINE
악성 프로세스 또는 전체 시스템 격리

차세대 위협제거 (NGTX)

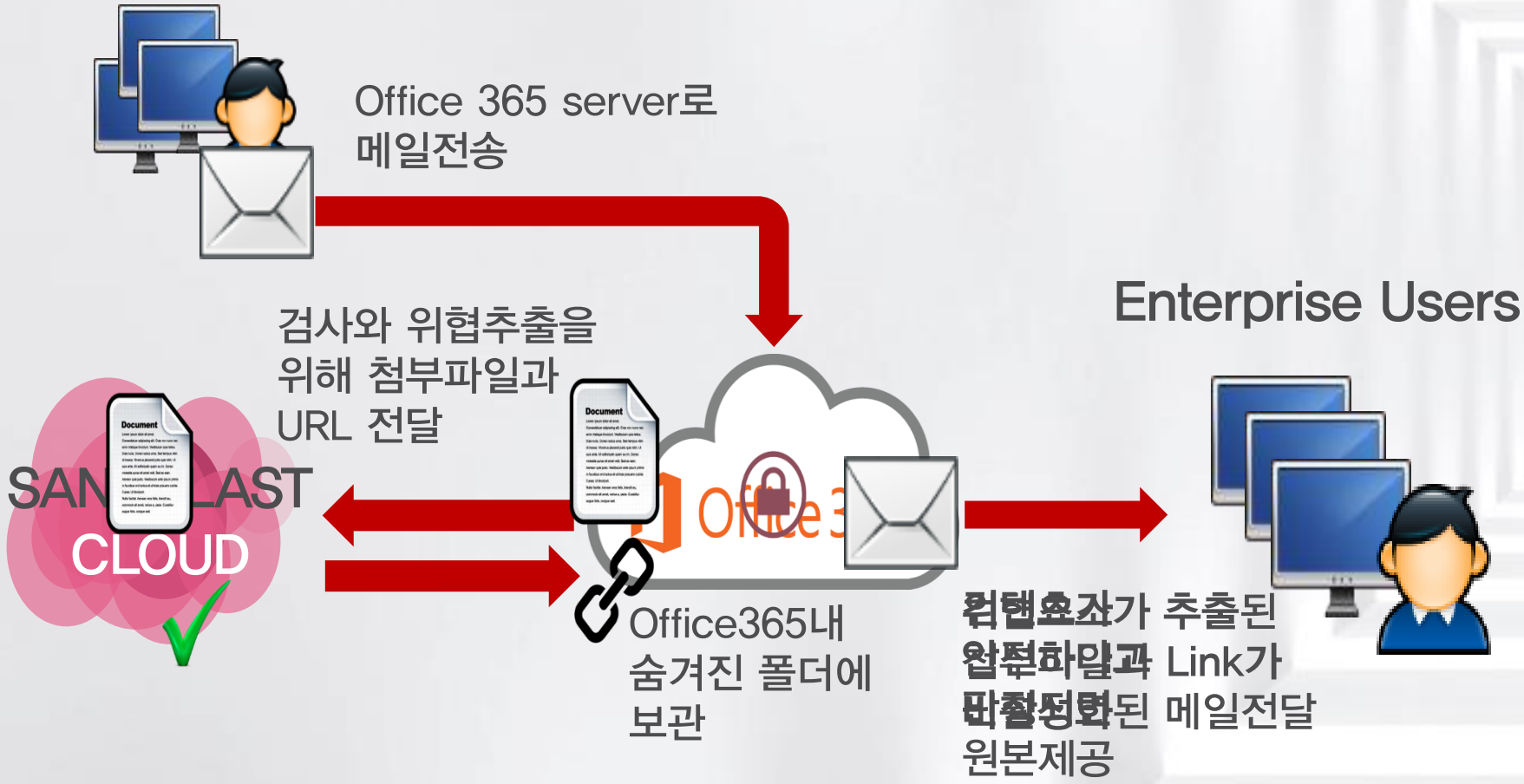
샌드블라스트 클라우드_ *클라우드 상에서 작동하는 유일한 가상 APT 솔루션*

샌드블라스트 클라우드

- Office 365에 SandBlast기능을 똑같이 적용
- 알려지지 않은 공격과 제로데이 공격 차단
- 손쉬운 구성과 관리

차세대 위협제거 (NGTX)

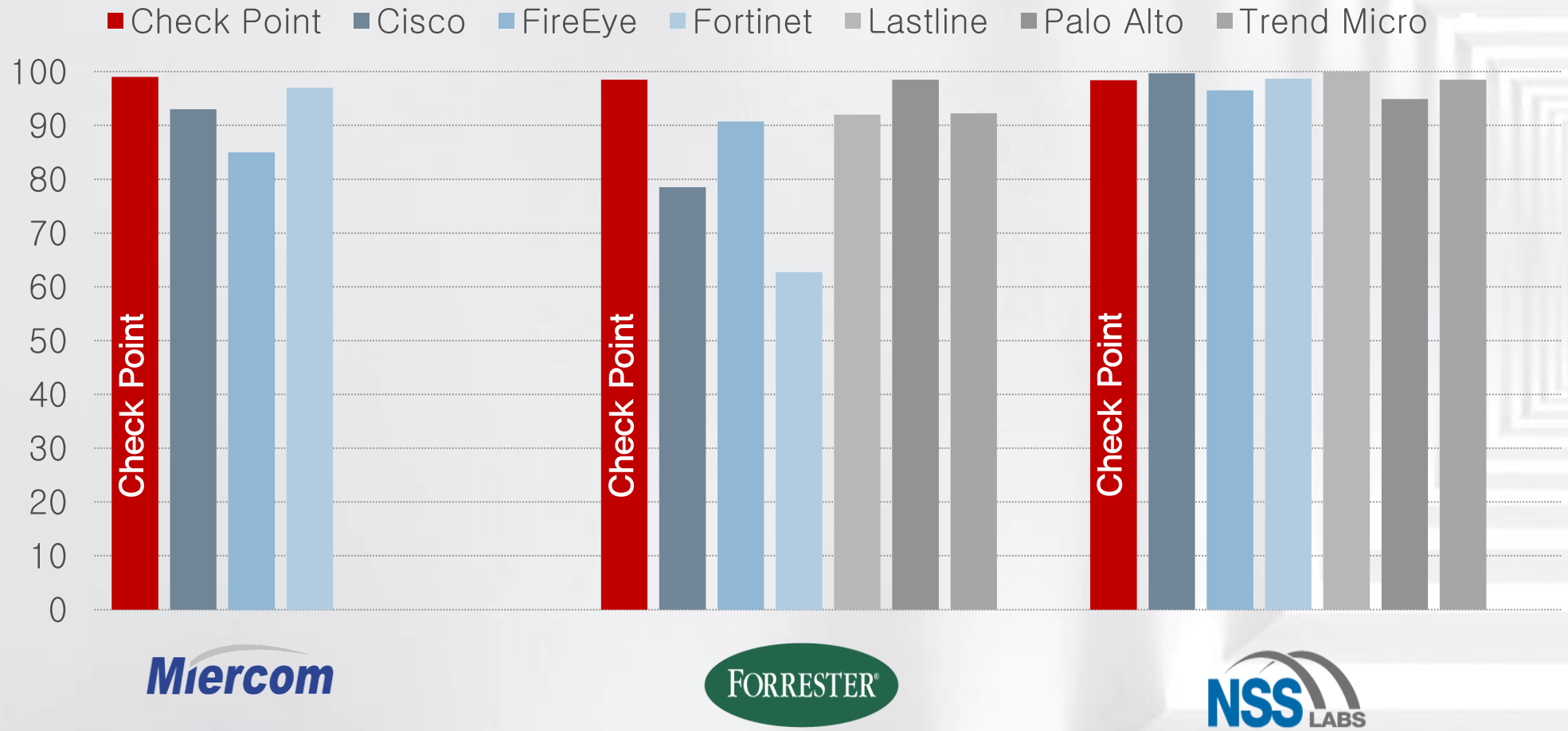
샌드블라스트 클라우드 동작방법



Content Analyzed in the Cloud

차세대 위협제거 (NGTX)

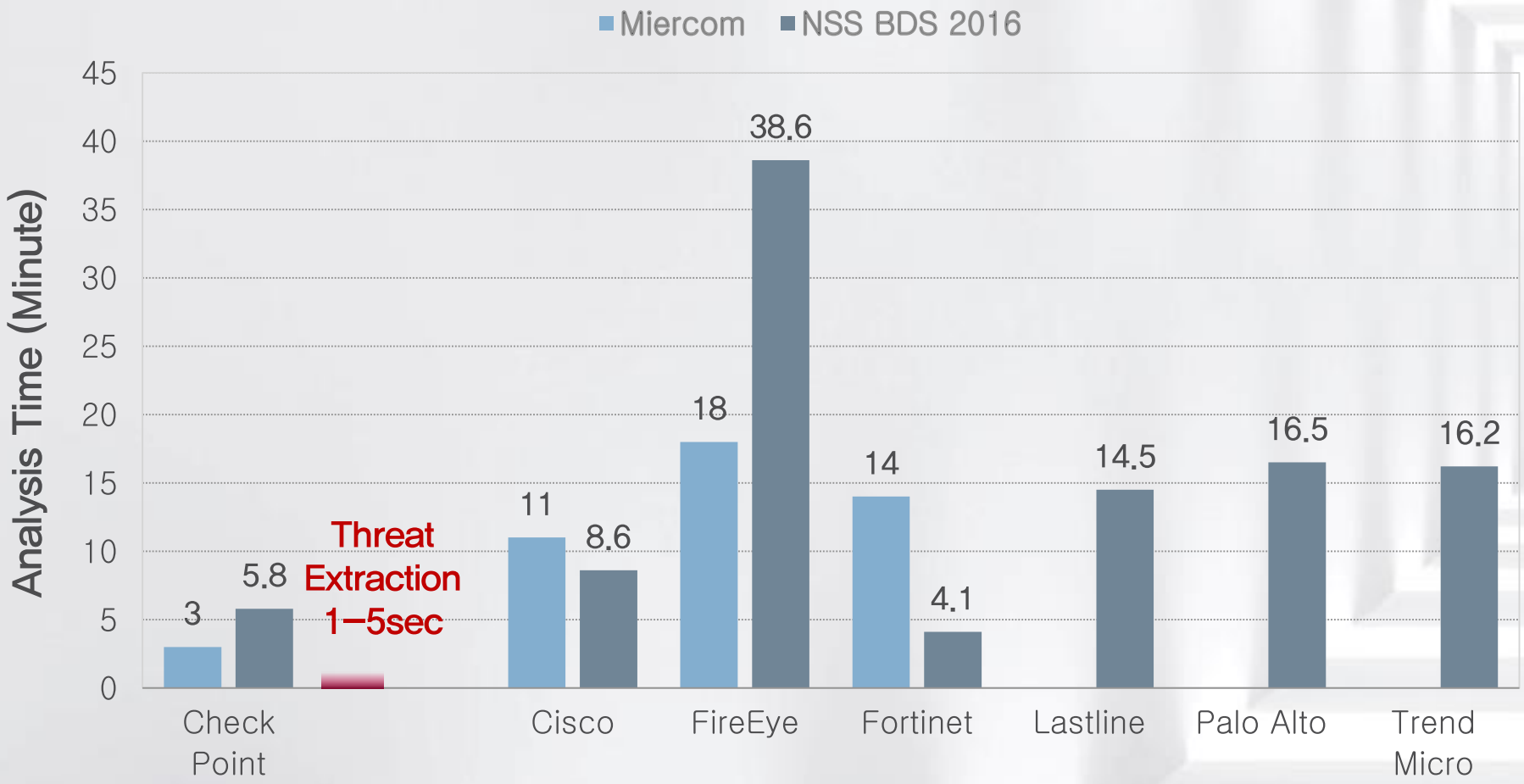
장점 _ 업계최고 탐지율



Source: Miercom APT Industry Assessment 2014
Source: Forrester Automated Malware Analysis Q2 2016
Source: NSS Labs Breach Detection Systems (BDS) Test Report 2016

차세대 위협제거 (NGTX)

장점 _ 가장 빠른 탐지



Source: Miercom APT Industry Assessment 2014

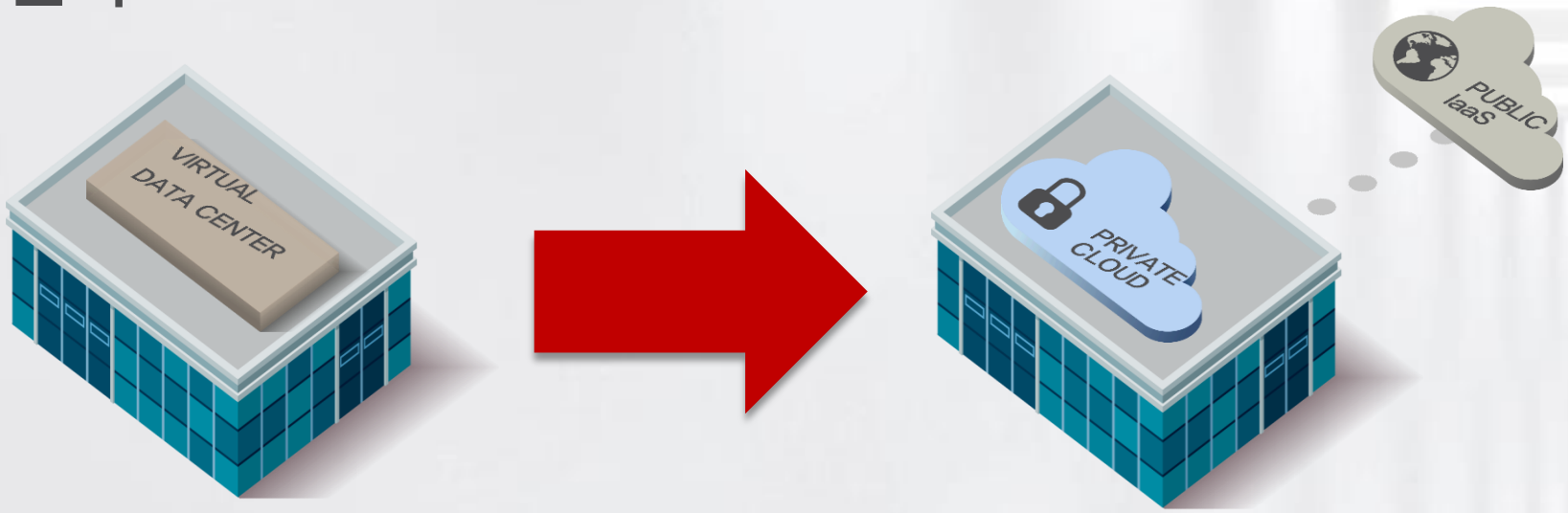
Source: NSS Labs Breach Detection Systems (BDS) Test Report 2016

체크포인트
가상화 솔루션
vSEC

Check Point
SOFTWARE TECHNOLOGIES LTD

가상화 솔루션

데이터 센터의 진화



가상화된 데이터센터

- 수동적 운영
- 영구적 라이센스 기반

하이브리드 클라우드

- 오토메이션 & 오케스트레이션
- ‘PAYG’ 라이센스 기반

시간, 비용이 최적화된 상태로
안전한 서비스 딜리버리를 위해 클라우드로 이동

가상화 솔루션

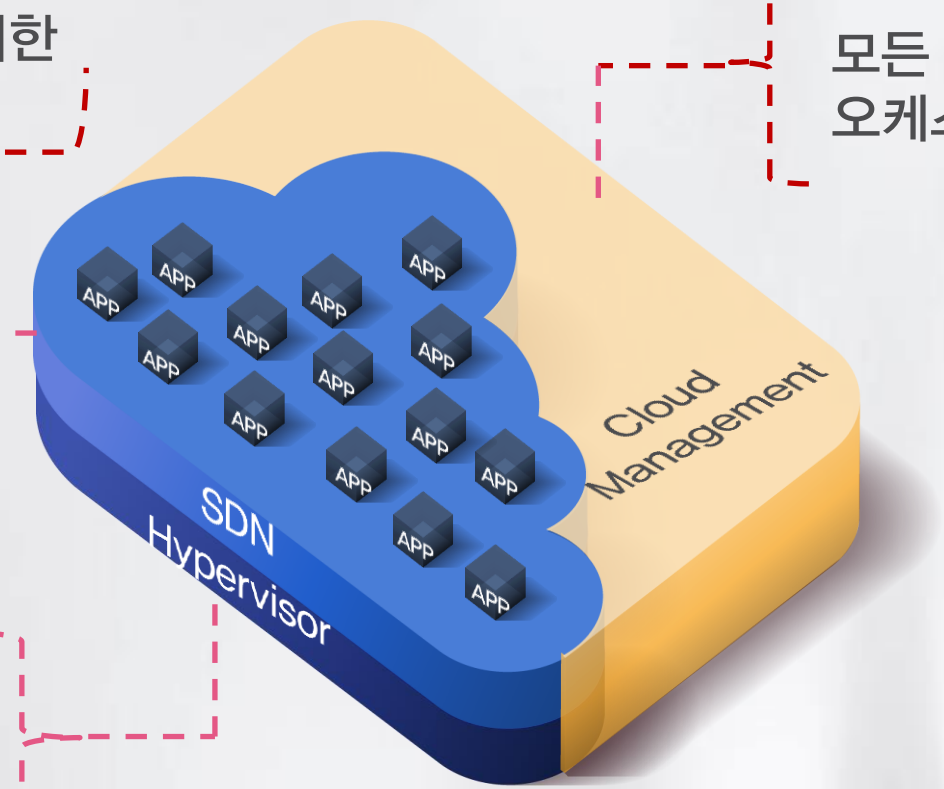
새로운 클라우드 환경

SDN

전체 네트워크에 대한
중앙관리 제공

Cloud Management

모든 어플리케이션에 대한
오케스트레이션과 오토메이션 제공

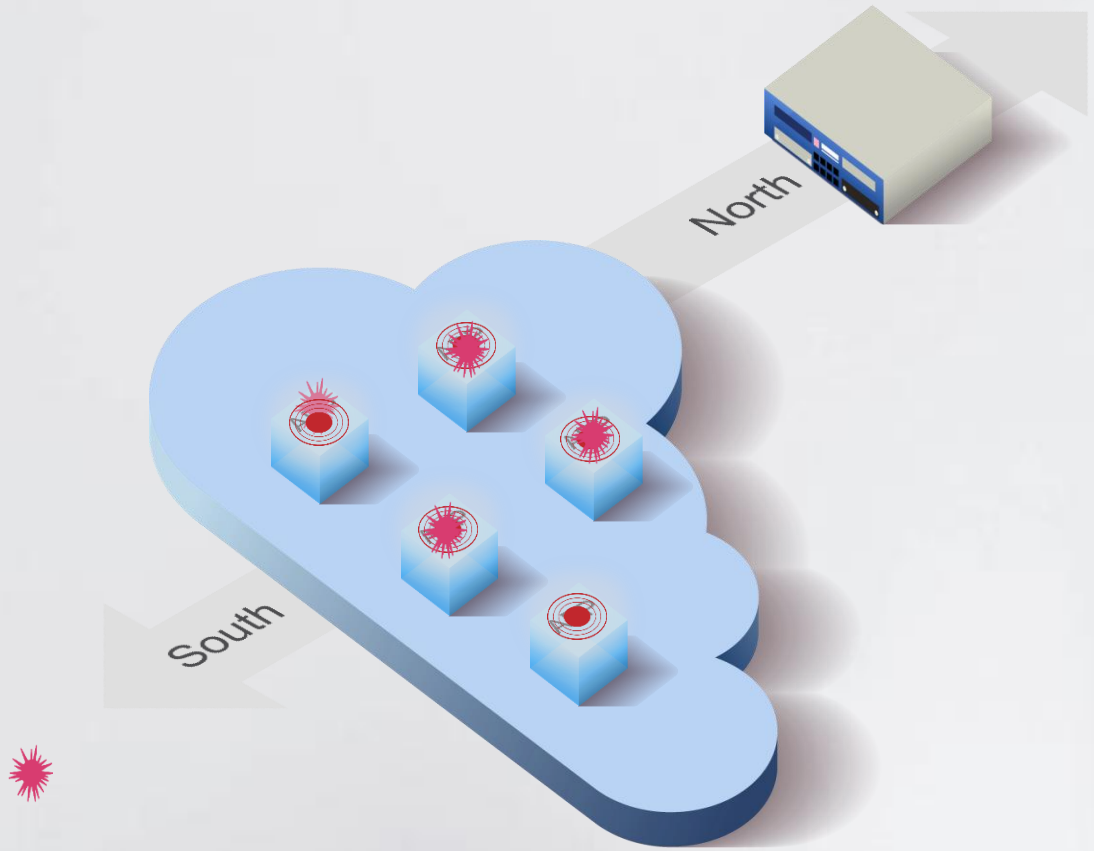


Hypervisor

가상화된 컴퓨팅 환경

가상화 솔루션

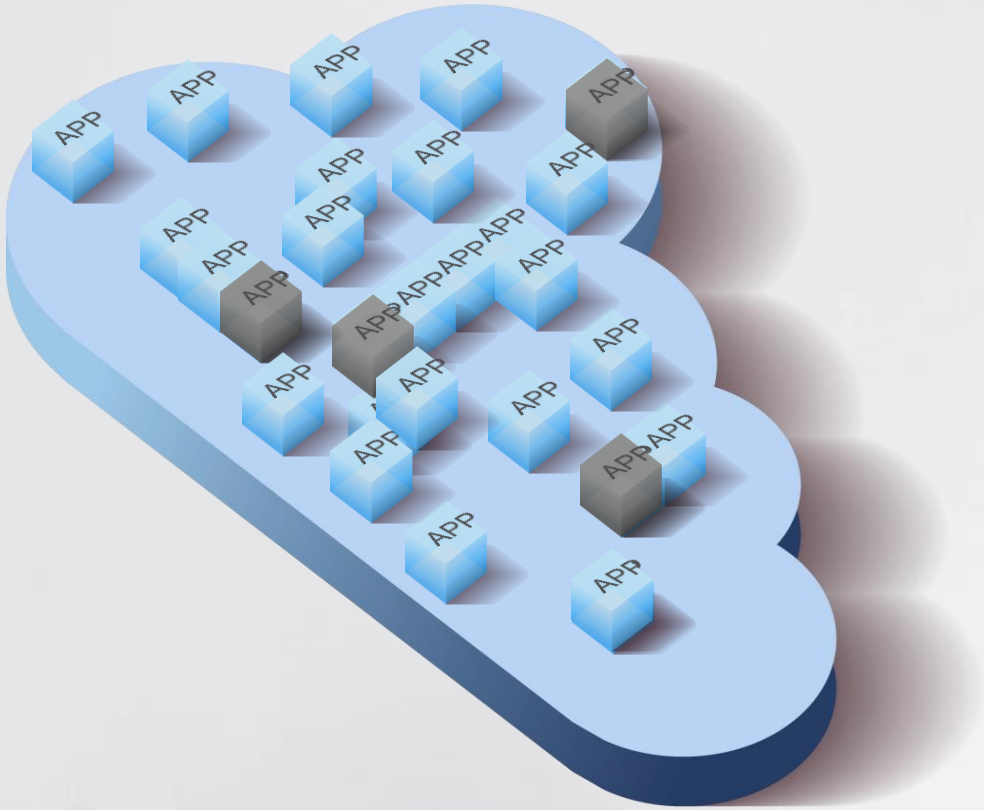
클라우드 한계_ *데이터 센터 내부에서 옆으로 전파되는 위협*



- 경계선 게이트웨이는 데이터 센터 내부의 트래픽을 보호하지 못함
- 어플리케이션간 보안통제 부족

가상화 솔루션

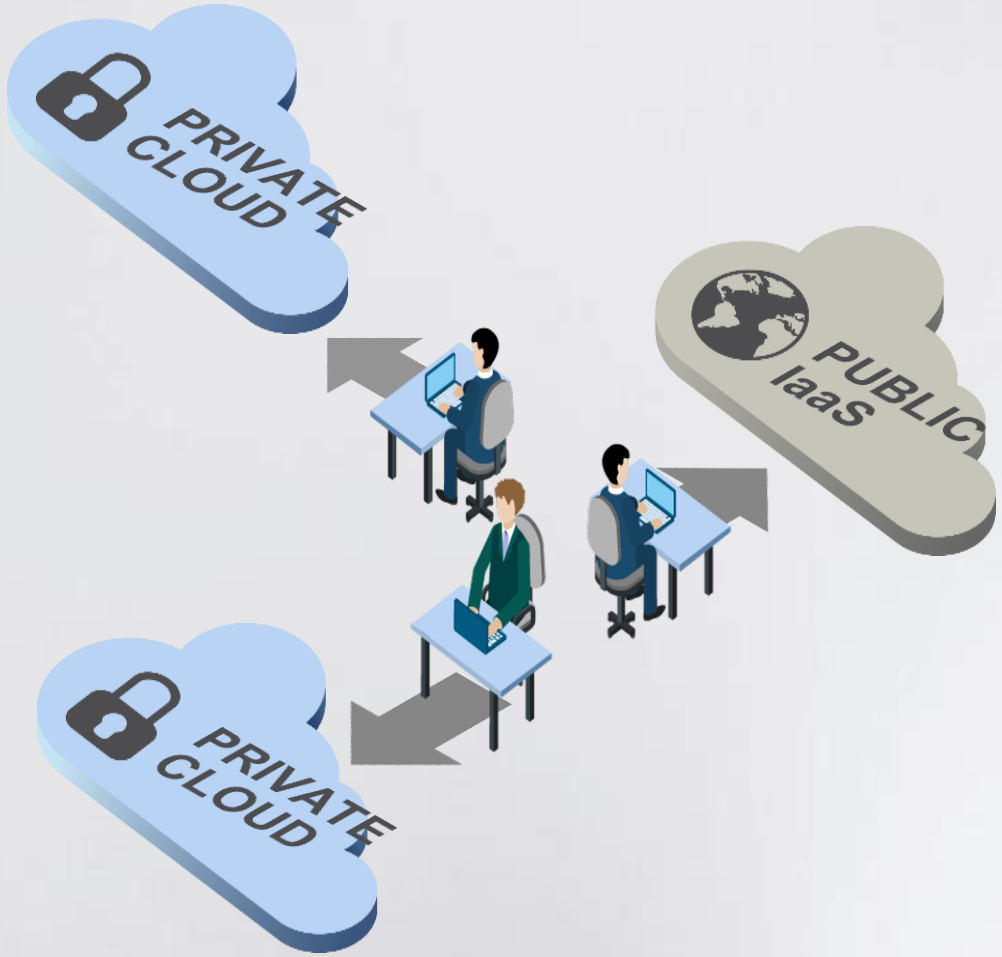
클라우드 한계_ *동적으로 변하는 데이터 센터 보호 불가능*



- 새로운 어플리케이션들의 빠른 프로비저닝
- Virtual-app의 이동
- IP 어드레스의 변경
- 패치되지 않은 휴면 VM의 재 기동

가상화 솔루션

클라우드 한계_ *멀티 클라우드 환경에서 복잡한 보안 관리*



- 다양한 형태의 클라우드 사용으로 통합 보안관리가 어려움

가상화 솔루션

체크포인트 vSEC

클라우드
사용의 편리함

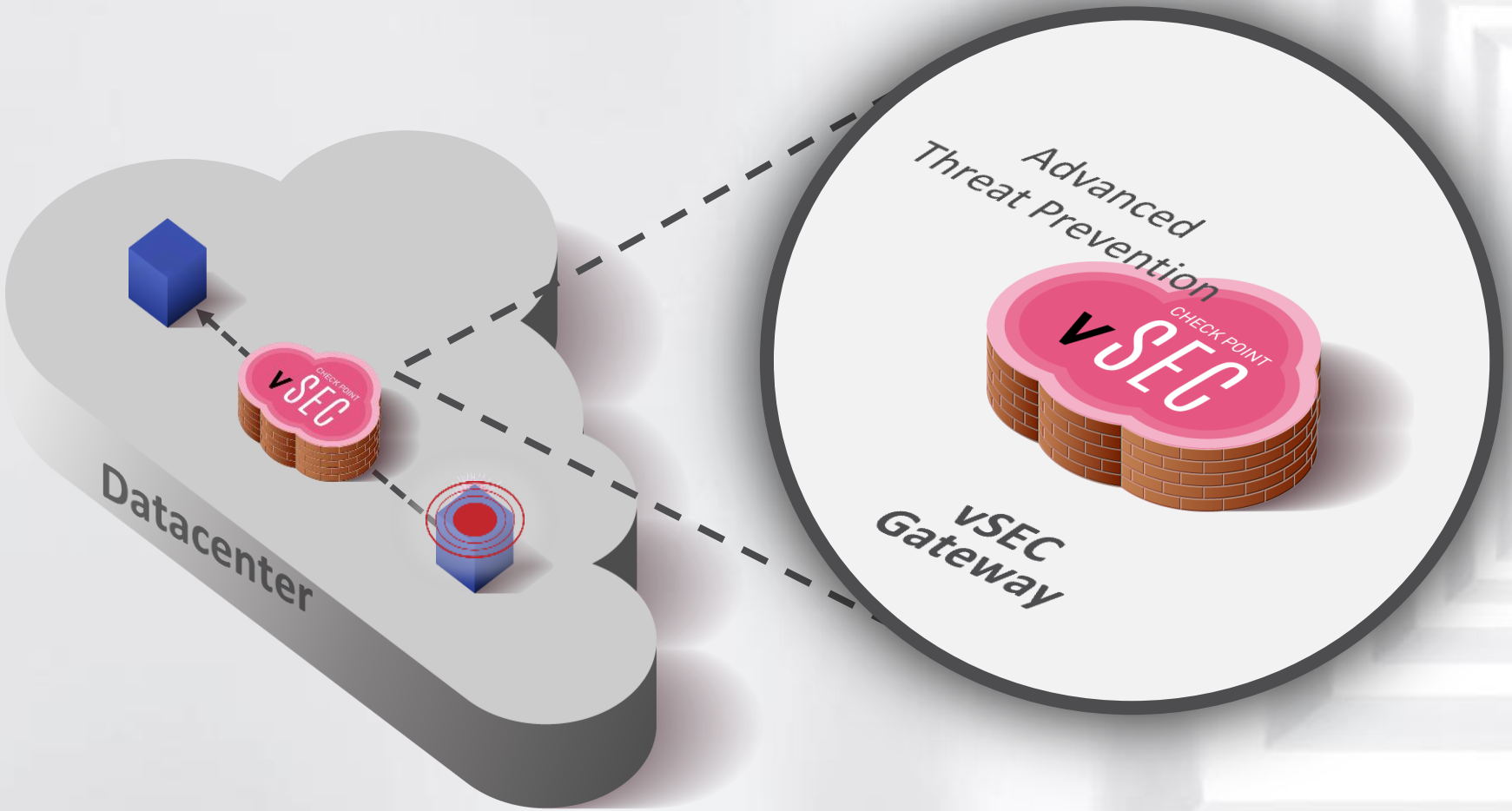
+

클라우드 보안
한계 극복

현존하는 최고의
클라우드 보안 솔루션

가상화 솔루션

vSEC 장점_ *데이터 센터 내부에서 옆으로 전파되는 위협 차단*



어플리케이션간 옆으로 이동하는 위협에 대한 차단 가능

가상화 솔루션

vSEC 장점_ *통합된 관리와 가시성*

공공 및 사설 클라우드와 물리적인 GW까지 함께 관리

가상화 솔루션

vSEC 장점_ *SDN과 통합된 GW*

Check Point Access Policy

Rule	From	To	Application	Action
3	Finance_App1 (vCenter Object)	Database_Group (NSX SecGroup)	MSSQL	Allow
4	HR_App2 (Open StackObject)	Finance_Group (ACI EndPoint Group)	CRM	Allow
5	User_ID	SAP_App (AWS Object)	SAP	Allow

SDN과 가장 완벽한 통합

가상화 솔루션

vSEC 솔루션 및 제품

vSEC for Private Cloud with SDN

- vSEC for NSX
- vSEC for ACI

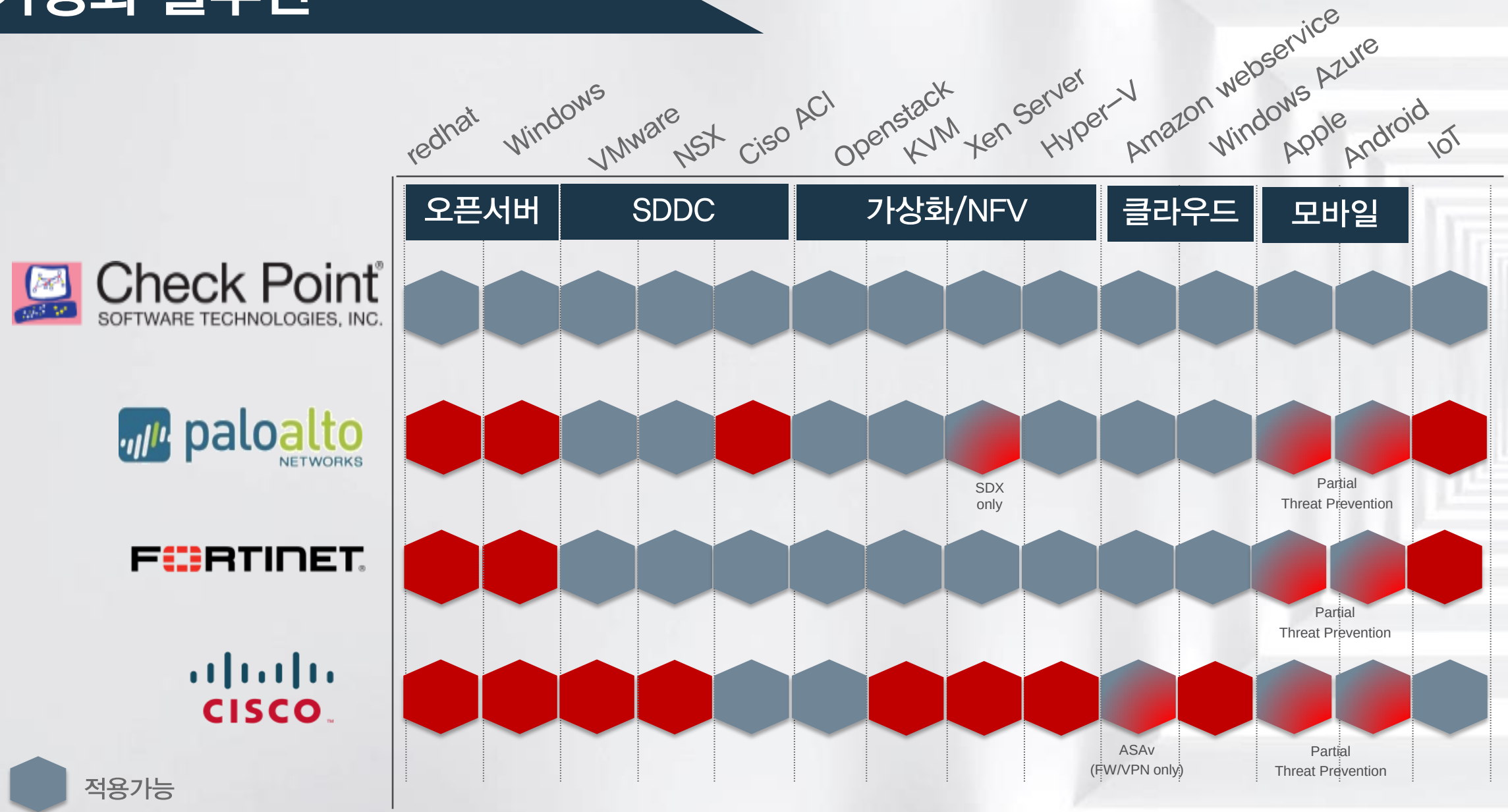
vSEC for Virtual-Datacenter

- vSEC Virtual Edition
  (also known as VE)
- vSEC for OpenStack

vSEC for Public IaaS

- vSEC for AWS
- vSEC for AZURE
- vSEC for vCloud Air

가상화 솔루션



전 세계 보안벤더 유일 모든 플랫폼에 적용 가능한 가상화 솔루션

WE SECURE THE FUTURE

Thank you

Check Point®
SOFTWARE TECHNOLOGIES LTD