새로운 ICT 메가트렌드를 위한 차세대 데이터센터 보안 혁신

Yong Ho Kim(yonghkim@시스코.com)


비즈니스 챌린지
비즈니스 및 기술 트렌드의 변화로 인한
데이터센터 혁신에 대한 압박
기술 트렌드

세그먼테이션

- 네트워크, 컴퓨팅 및 가상화에 대한 **경계 수립**
- 기능별, 디바이스별 및 조직별 **정책 적용**
- 네트워크, 자원 및 응용프로그램에 대한 **접근 제어**

위협 방어

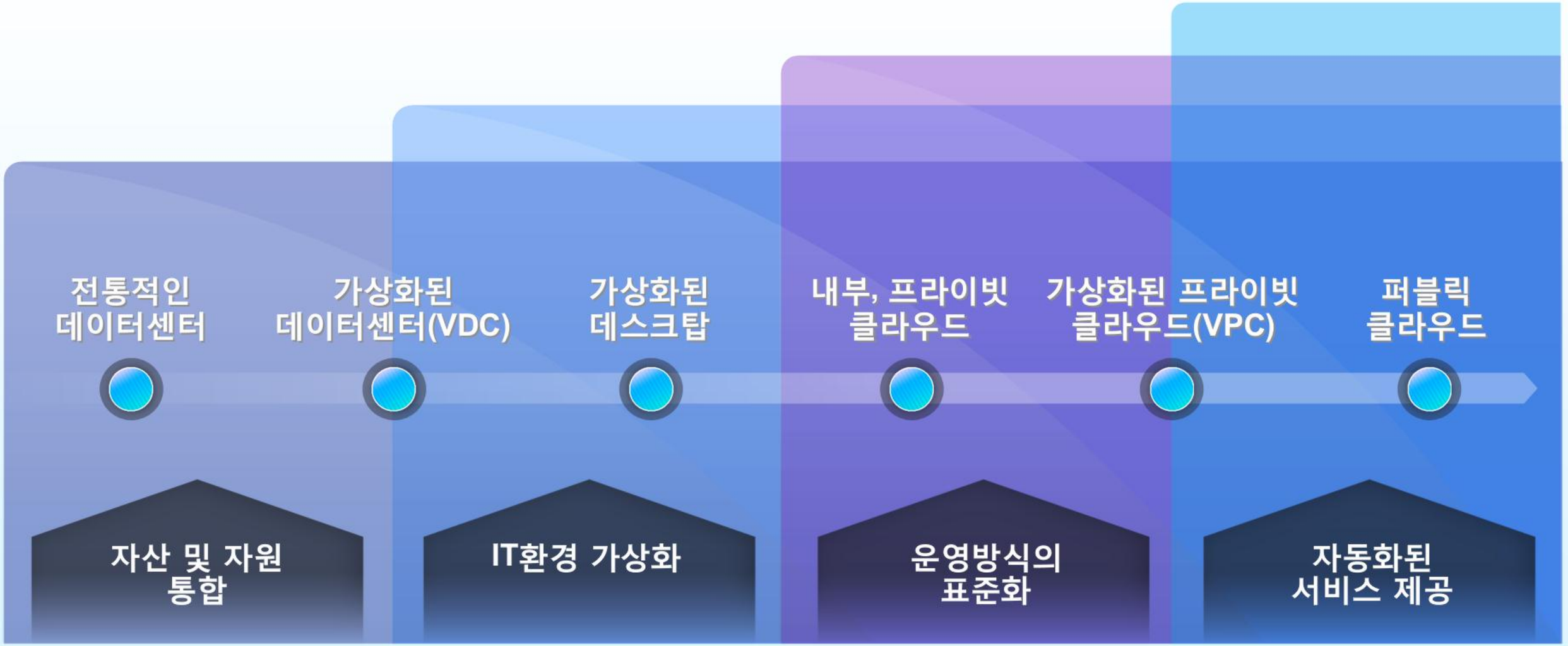
- 내외부 **공격 차단**
- **보안 감시 영역** 선정 및 에지 경계 보호
- 접근 및 사용에 대한 **정보 통제**

가시화

- 사용에 대한 **투명성** 제공
- 비즈니스 상황이 반영된 네트워크 **활동 모니터링**
- 운영 **간소화** 및 규정 준수 **리포팅**

KEY DATA CENTER SECURITY PRIORITIES

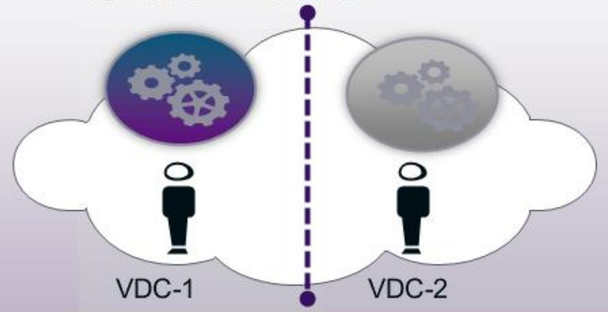
데이터센터의 발전 과정



시스코 데이터센터 및 가상화 보안 프레임워크

요구사항별 제품 맵핑

	물리적 환경	가상화 환경	클라우드 환경
	• 한대의 물리적서버에 하나의 앱 • 고정적 • 수작업 프로비저닝	• 한대의 물리적 서버에 다수의 앱 • 유동적 • 동적인 프로비저닝	• 한대의 서버를 다중소유 • 탄력적 • 자동화된 스케일링
네트워크 컴퓨팅 스토리지	시스코 Nexus 7K/5K/3K/2K 시스코 UCS for Bare Metal EMC, NetApp	시스코 Nexus® 1000V, Nexus 1010, VM-FEX 가상화된 환경을 위한 UCS NetApp, EMC	
보안	시스코 ASA5585, ASA-SM, IPS4500, WSA ……	ASA Multi-Context, ASA 1000V, Virtual WSA/ESA VSG	
검증된 디자인	Data Center Security CVD	Virtual Multi-Service Data Center (VMDC)	



* Virtual only, ** Announced

세그먼테이션

유휴 및 서비스 중인 데이터 보호를 위한 물리적 경계에서
가상화 경계까지 일관된 보안 정책 적용

세그먼테이션

위협방어

가시화

세그먼테이션

유휴 및 서비스 중인 데이터 보호를 위한 물리적 경계에서
가상화 경계까지 일관된 보안 정책 적용

방화벽 세그먼테이션
Stateful/reflective ACL
다중 가상 방화벽
VPN

패브릭 세그먼테이션
UCS 패브릭 인터커넥트

상황인식기반 세그먼테이션
보안 그룹 태그 (SGT)
Security Exchange Protocol (SXP)
보안 그룹 정책 (SGACL)

네트워크 세그먼테이션
물리적
논리적 (VLAN, VRF)
가상화 (Zones)

방화벽 세그먼테이션

물리적

시스코® ASA 5585-X

시스코 Catalyst 6500
ASA FW Module

North-south 트래픽: 데이터 센터를 기준으로 들어오고 나가는 모든 트래픽 검사

- 데이터센터의 물리적 에지 보안 어플리안스로 모든 트래픽에 대한 감시/제어
- 데이터센터에 대한 네트워크의 물리적인 내부 및 외부 경계를 구분
- 해킹등 보안 침해 사고를 막기 위한 완전한 침입방지시스템(IPS) 기능을 포함하면서도 모든 서비스에 대한 고속처리 지원

가상화 / 다중소유

시스코 ASA 1000V
Virtual Firewall

시스코 Virtual Security
Gateway (VSG)

East-west 트래픽: 데이터 센터내에 존재하는 어플리케이션 및 가상화 환경에서의 신뢰된 보안 영역 구성

가상화환경의 에지 가상방화벽 ASA 1000V

- 다중 소유 가상화 환경하에서의 소유자별 경계 구분 및 방화벽 기능 지원

가상화환경의 서비스영역별 가상 방화벽 VSG

- 가상화 환경에서의 단일 소유자 영역내에 있는 어플리케이션 또는 VM간의 방화벽 기능 지원

상황인식 기반의 세그먼테이션

트러스트섹: 비즈니스 상황별 보안 그룹 태깅을 통한 상황인식 기반의 접근제어

트러스트섹을 통해 비즈니스 상황별로
의미있고 효과적인 보안 정책을 정의

비즈니스 정책

Source \ Destination	인사부 DB	제품 CRM	스토리지
가상데스크탑 HR 직원	✓	✗	✗
VPN 사용자 HR 직원	✗	✗	✗
IT 관리자	✓	✓	✓
테스트 서버	✗	✗	✓

데이터센터내의 물리/가상화영역 보안 접근 제어

시스코 트러스섹 장점

트러스트섹을 통한 비즈니스 혜택

- **비즈니스 상황별 정책 간소화**
  - ü 기술적인 해석이 아닌 비즈니스적인 관점을 기반으로 함
  - ü 정의된 그룹 기반으로의 자원 이동 및 접근 제어
- **보안 강화 및 복잡성 감소**
  - ü 간소화된 디자인 : 트래픽 제어를 위한 운용을 감소시키고 데이터센터의 성능을 향상
  - ü 고효율의 확장성 : 트러스트섹 기능 지원 디바이스 상에서 속도 저하 없이 태깅 및 정책 적용
  - ü 네트워크 토포롤리지에 구애 받지 않는 접근 제어 구현
- **운영 비용 감소**
  - ü 자동화된 방화벽 및 접근 제어 정책 관리
  - ü ACL 관리, 복잡성 및 오버해드 감소

위협방어

기업 내외부 위협으로 부터의 비즈니스 보호

- 해커
- 조직화된 범죄
- 사이버 범죄
- 악의적인 내부직원

위협방어

기업 내외부 위협으로 부터의 비즈니스 보호

해커

조직화된 범죄

보호방안

- IPS 4500 Security Appliance
- 시스코® ASA CX Application Control

사이버 범죄

악의적인 내부직원

위협방어를 위한 보안 옵션

시스코 IPS 4500

데이터센터에서 요구되어지는 보안 위협 방어

- 빈번히 발생하는 내외부 네트워크, 서버 및 어플리케이션 공격에 대한 광범위한 보호 기능 지원
- 고밀집도의 포트 및 확장형 샤시 형태의 하드웨어 기반의 고성능
- 실시간으로 업데이트되는 보안 시그니처 및 SIO 활동을 통해 수집되는 보안 위협 및 평판 정보 반영을 통한 상황인식기반의 IPS 기능 지원

시스코 ASA CX

상황인식 기반 차세대 방화벽 모듈

- 어플리케이션 및 마이크로 어플리케이션까지 포함한 광범위한 어플리케이션 가시화 및 통제
- 어플리케이션 분류, 사용자 및 그룹등 세밀한 상황적 보안 정책
- 하드웨어 모듈 기반의 어플리케이션 인지 및 상황인식 기반 접근 제어
- SSL 암호화된 트래픽에 대한 어플리케이션 식별 및 가시화를 통한 접근 제어

가시화

보안 정책 관리 및 데이터 센터 운영 상태 가시화

- 설정 관리 및 리포팅
- 가시성
- 통합 접근제어 정책

가시화

보안 정책 관리 및 데이터 센터 운영 상태 가시화

관리 및 리포팅

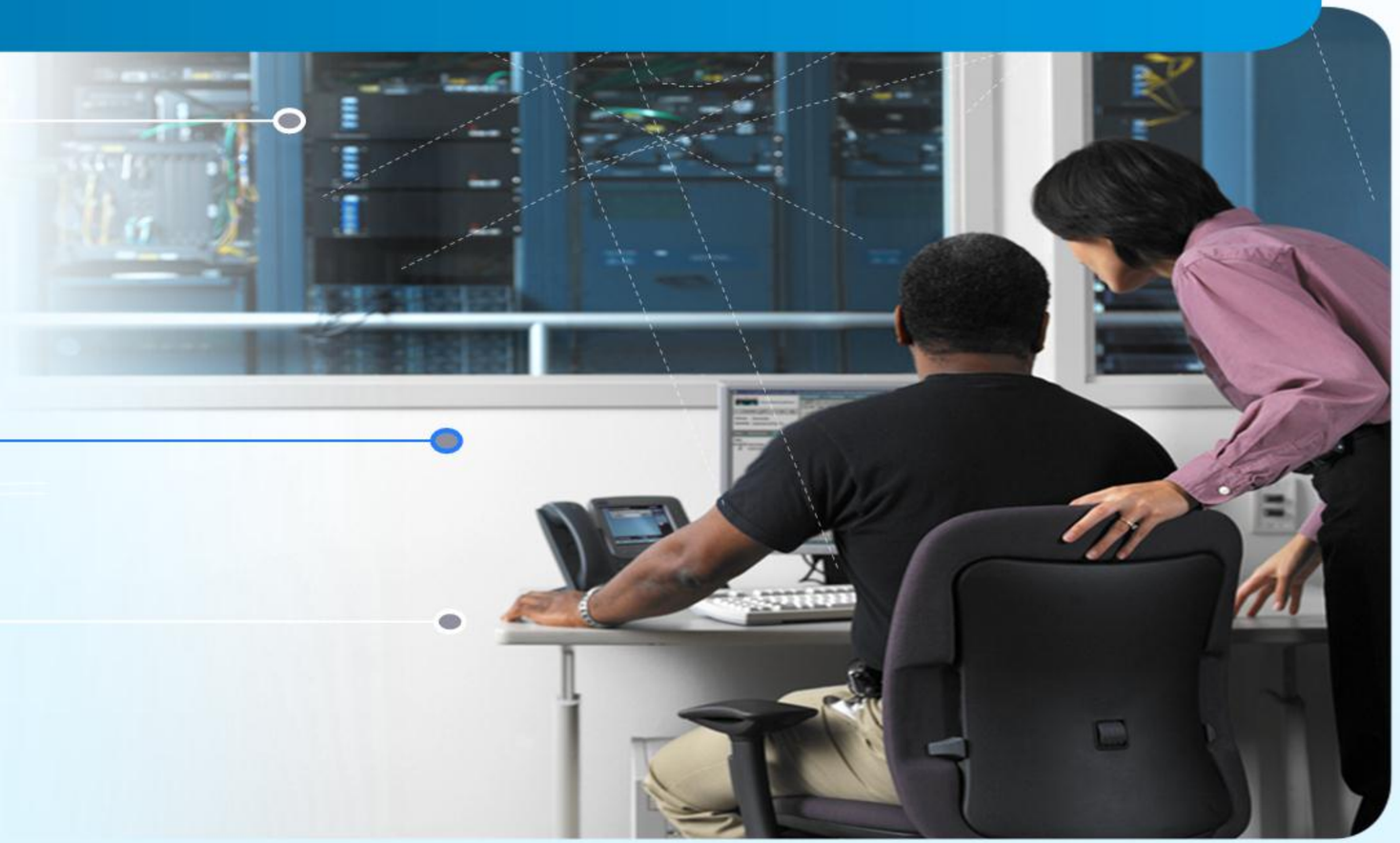
- 시스코® Security Manager (SM)
- 시스코 Virtual Network Management Center (VNMC)

가시성

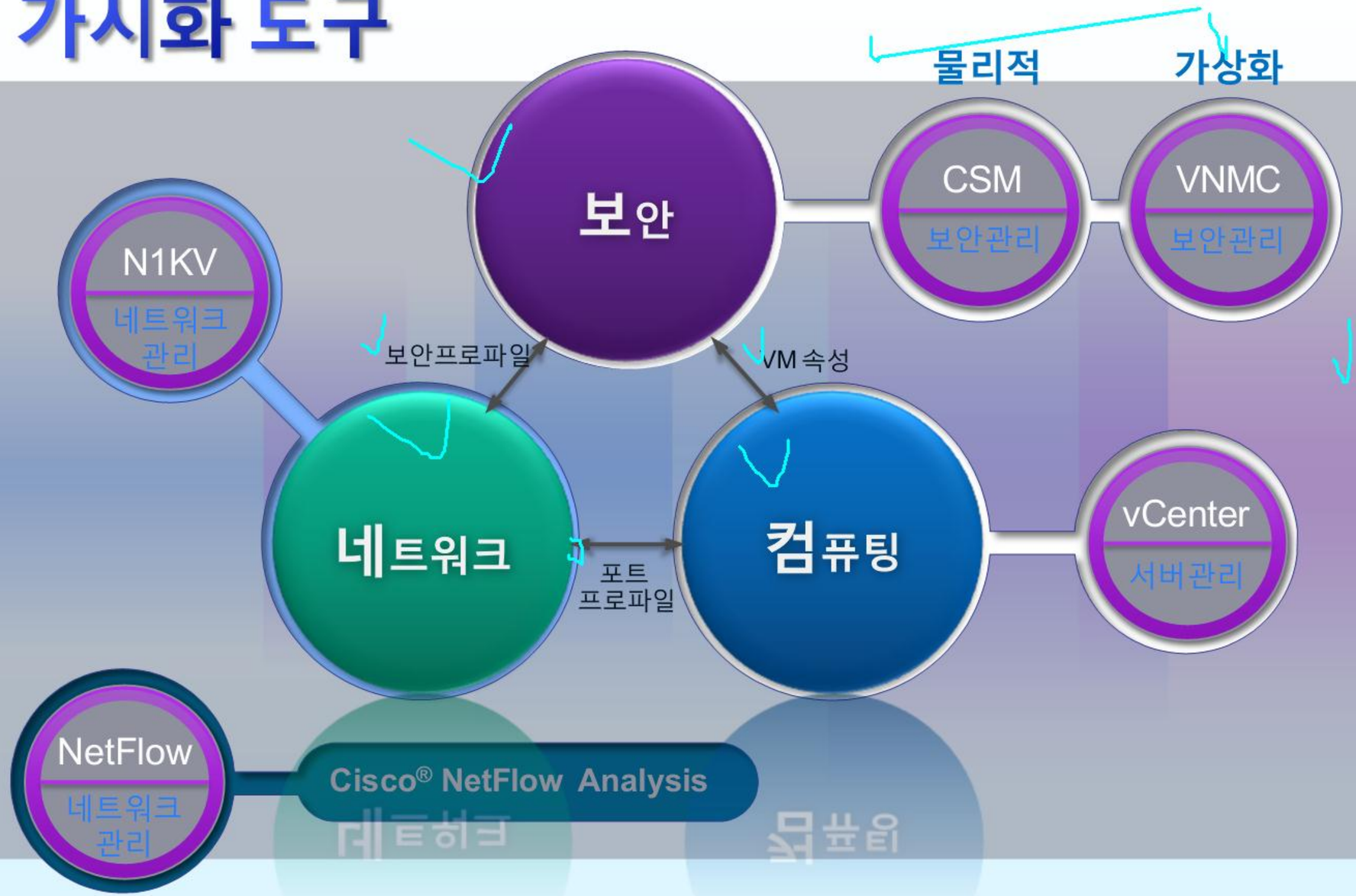
- 시스코 넷플로우 기술

통합 접근제어 정책

- 시스코 Identity Services Engine (ISE)
- 시스코 TrustSec Security Group Tagging (SGT)



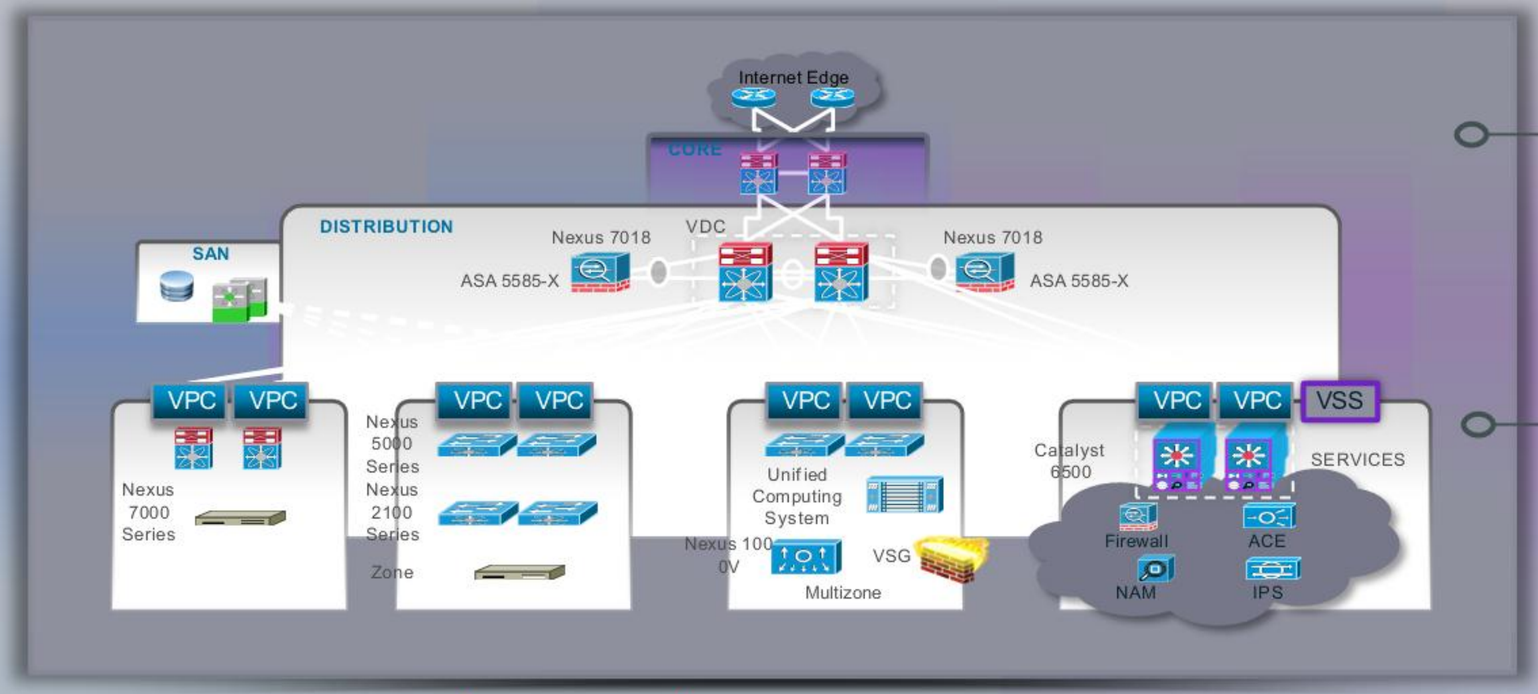
가시화 도구



- 각 영역별 중점 관리 속성에 대한 정보 연계
- 데이터 센터 운영 전반에 걸치 투명성 제공

검증된 디자인

랩테스트 및 아키텍터 검증 완료



물리적인 데이터 센터

Security, Validated Designs (CVDs)

가상화된 데이터 센터

Virtualized Multi-Service Data Center (VMDC)

검증된. 호환성 | 확장성 | 신뢰성

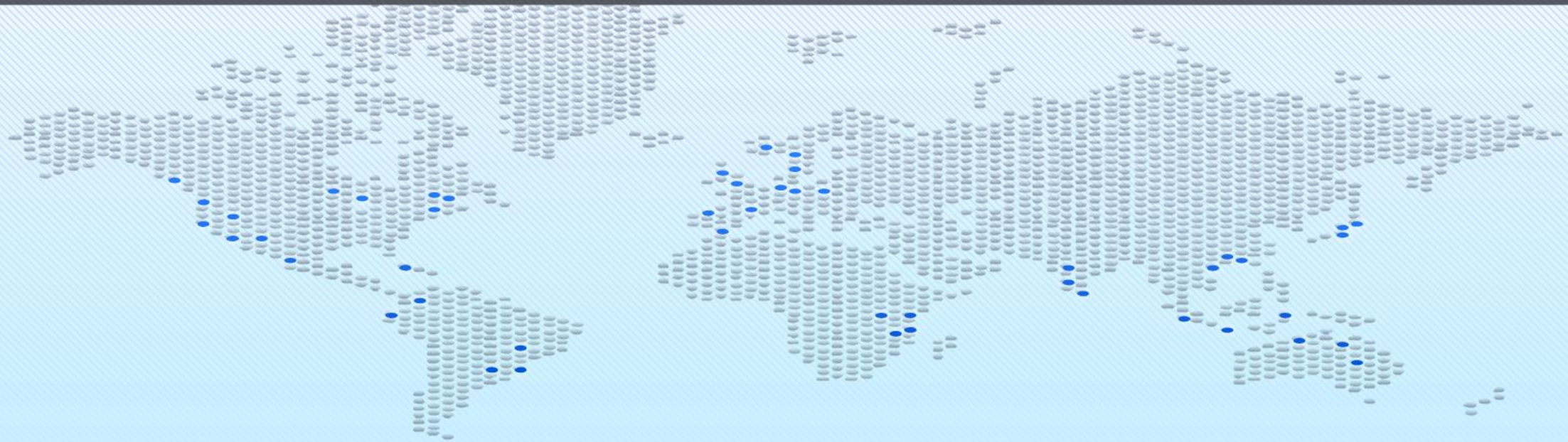
시스코 시큐리티 인텔리전스 오퍼레이션(CSIO)

3.6B
DAILY REQUE STS

71M
BLOCKS PER DAY

75TB
DAILY DATA TRANSFER

3200
SCANNING SERV ERS



2300
CUSTOMERS

140,000 USERS

Standard Chartered
120,000 USERS

IKEA
100,000 USERS

2.2M
END USERS

제품 업데이트


Cisco ASA 1000V
Cisco AnyConnect

시스코 ASA 1000V

Nexus 1000V 가상 스위치환경에서 제공하는 유연성 및 확장성, 고속 스위칭 기능 연동

- 가상화 및 클라우 환경에 대한 보안 기반 확보
- 물리 및 가상화 그리고 클라우드까지 엔드 투 엔드의 일관성있는 보안 세그먼트 지원
- 다양한 환경에서의 확장성 확보 및 구성에 대한 복잡성 감소

IPS 4500 시리즈

- 타깃된 공격과 정교한 악성 코드로부터 크리티컬한 데이터센터 자원 보호
- 인라인 IPS로써 해커, 공격대상, 그리고 공격 정보등 광범위한 정보에 대한 가시성 제공
- 로컬 보안 시그니처와 실시간으로 제공되는 글로벌 보안 위협 정보에 대한 상관관계 분석을 통해 탐지의 정확성 및 알려지지 않은 공격에 대한 신속한 대응
- 고밀집 포트지원, 작은 크기, 멀티기가빗 성능 지원 등 데이터센터 요구사항 특화된 시리즈

시스코 보안 관리 4.3 (CSM 4.3)

- 시스코 보안 제품에 대한 고급화된 관리 기능 및 빠른 트러블 슈팅 기능
- 자동화된 소프트웨어 및 시그니처 업데이트 중앙관리
- 시스템 상태 및 성능 모니터링 및 사전정의된 임계값 도달시 즉각적인 경보
- 시스코 시큐리 인텔리전스 오퍼레이션 기능 연동

ASA 9 Software

- 클러스터링 기술을 통한 업계 유일의 최대 320Gbps 방화벽 성능 지원
- 어플리케이션 인지는 물론 사용자 및 그룹등의 정보 종합분석을 통한 상황인식 기반의 어플리케이션 가시화 및 통제 기능
- 다중 보안 기능 통합 지원, 가상방화벽 내에서의 동적라우팅 및 Site-to-Site IPSec VPN 지원

시스코 AnyConnect

- IPv6 환경 지원
- BYOD 에 대한 회사 및 개인 기기에 대한 차별화된 보안 정책 적용rk
- 차세대 암호화 방식인 미 NSA Suite B 암호화 지원

시스코의 보안 솔루션을 통해 기업 IT 보안 가속화!!

요약

세그먼테이션

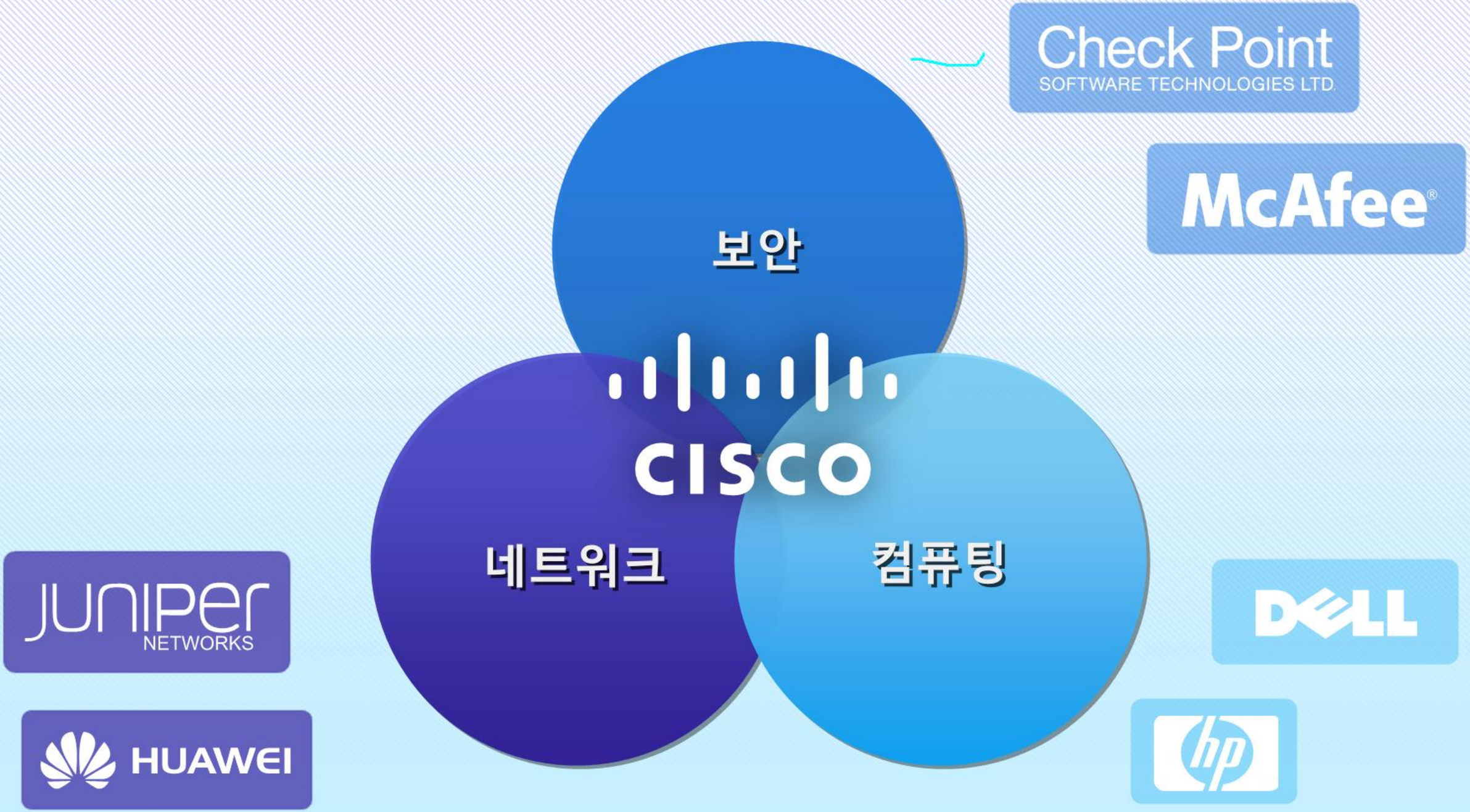
ASA 5585-X
ASA 1000V
VSG
Nexus 1000V
TrustSec

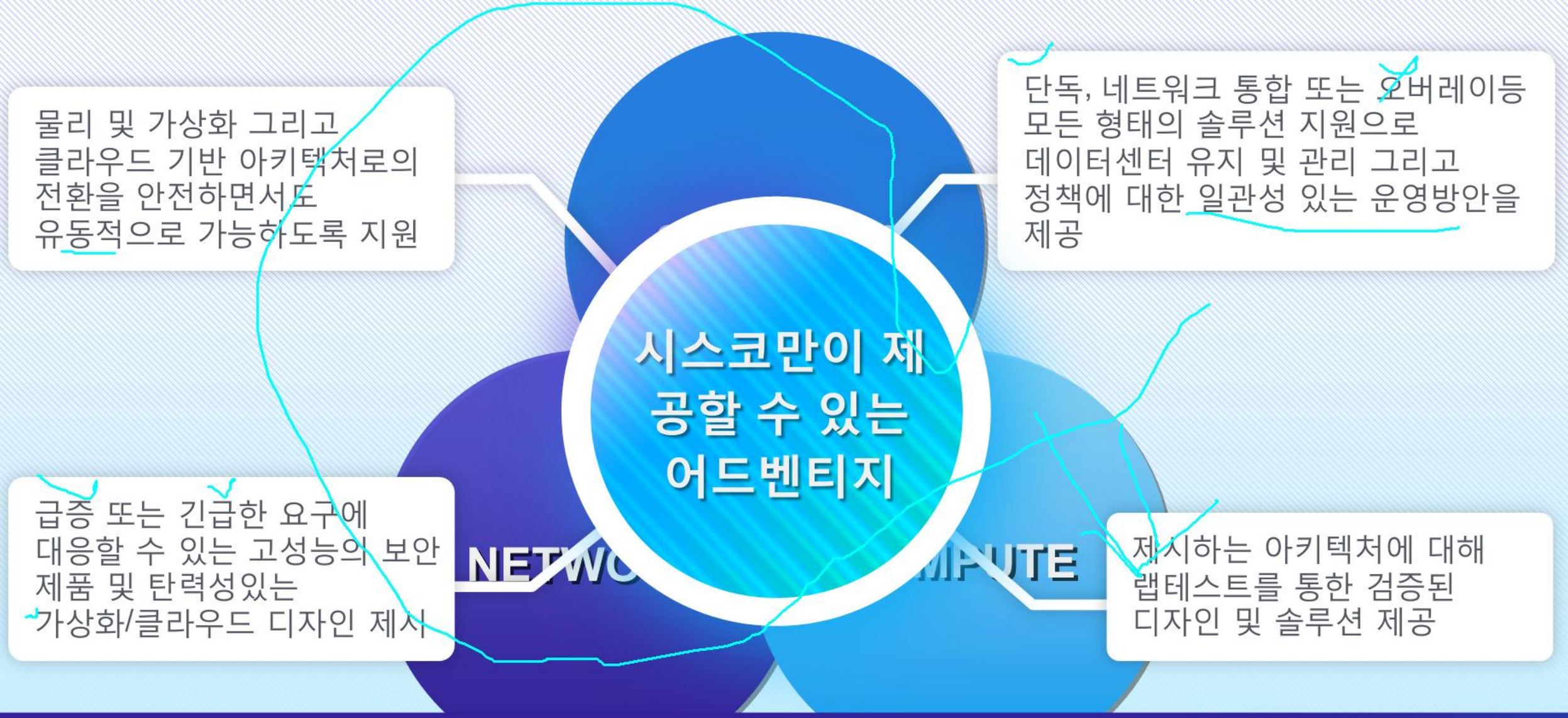
위협 방어

IPS 4500
ASA CX
SIO

가시성

CSM
NetFlow
ISE
VNMC


Check Point
SOFTWARE TECHNOLOGIES LTD.
McAfee
보안
CISCO
네트워크
컴퓨팅
JUNIPER
NETWORKS
HUAWEI
DELL
hp



Cisco Seamlessly Integrates Security Into Fabric Of The Network


CISCO