보안 시장 진화 방향과 NAC

Cisco Systems Korea

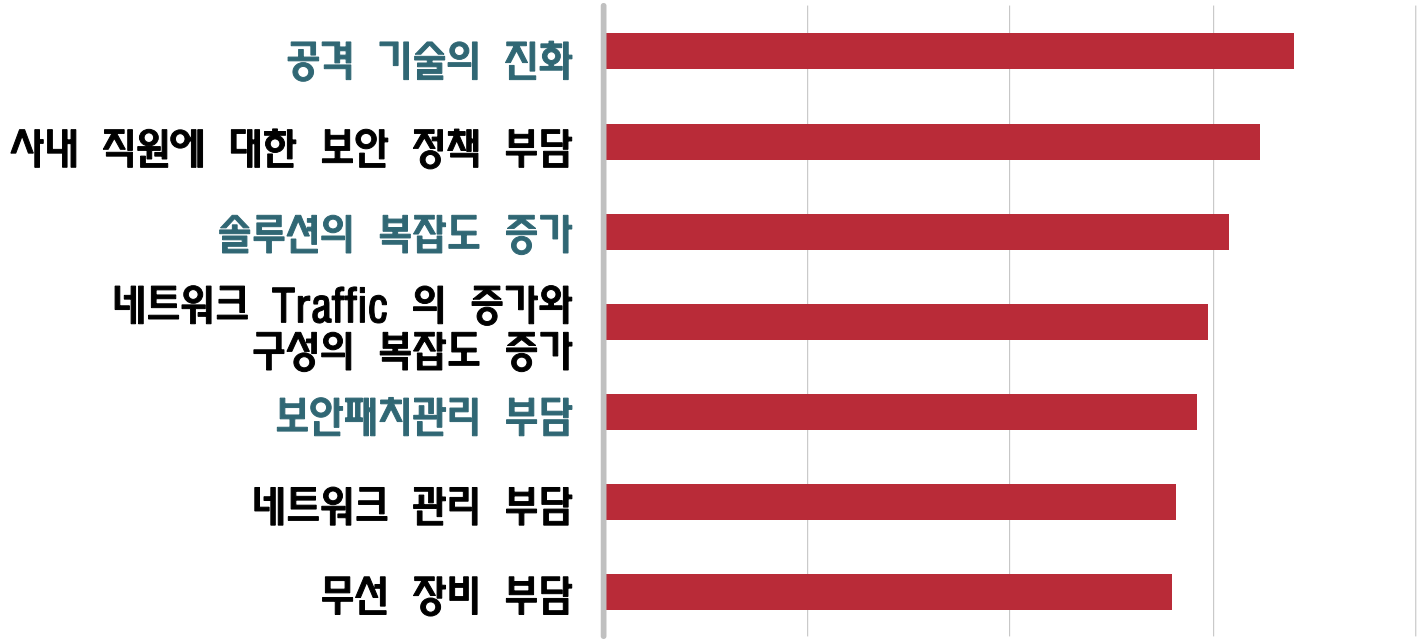
Solution S.E team

S.E 최 우 형 (whchoi@cisco.com)

Agenda

1. 보안 기술 동향
2. 사용자 보안 – Cisco NAC Overview
3. 통합보안 기술 Overview

Top Security Challenges 2005



공격 기술의 진화… 보안 관리에 대한 부담 증가

심도 깊은 지능형 보안 솔루션 필요/ 통합 보안 필요성..

Note: 1 = No challenge; 5 = Significant Challenge
Source: IDC's *Enterprise Security Survey*, 2005

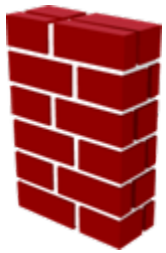
공격 기술의 진화
Application Level로의 공격 목표 변경

공격목표의 75%
이상이 상위 Application

No Signatures / Patches

다수의 다양한 웹 어플리케이션
- 비즈니스 주요 정보 포함
- 자산 주요 정보 포함
- 개인 정보 정보 포함

Deep Inspection의 필요성



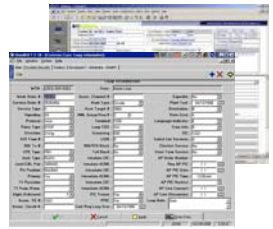
Network Firewall

IDS IPS

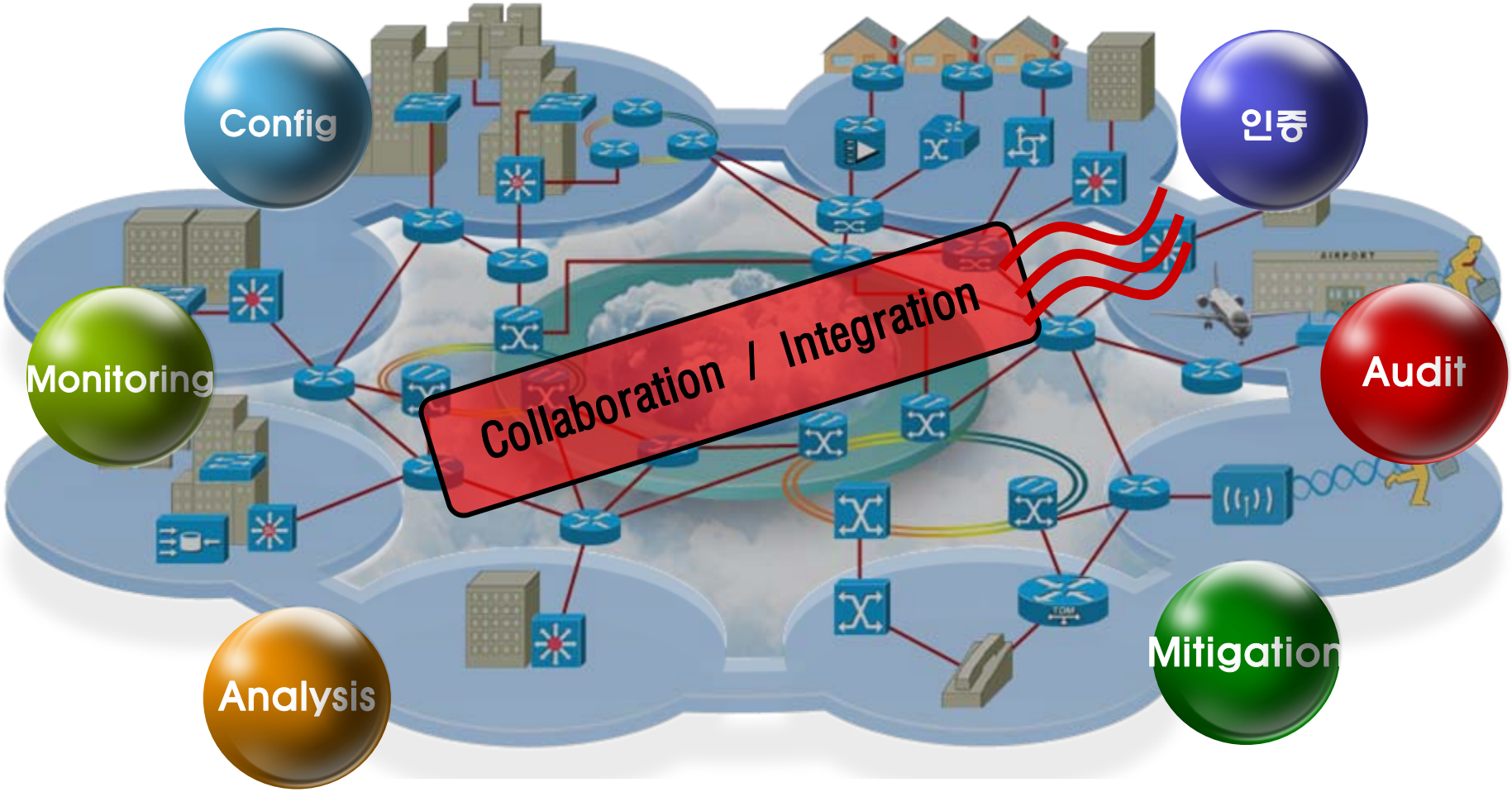
웹 서버 | 어플리케이션 서버 | DB 서버

Windows OS | Unix OS | Others OS

Network



Management Overhead



Cisco Self Defending Network

통합 보안

모든 IT 자원에 대한 보안
- IOS Security
- 802.1x
- 통합형 보안 장비

상호 협력 보안

Cisco NAC
- Cisco NAC을 통한 상호 협력 보안
- AV Vendor + Cisco

TREND MICRO

적응형 위협 보안

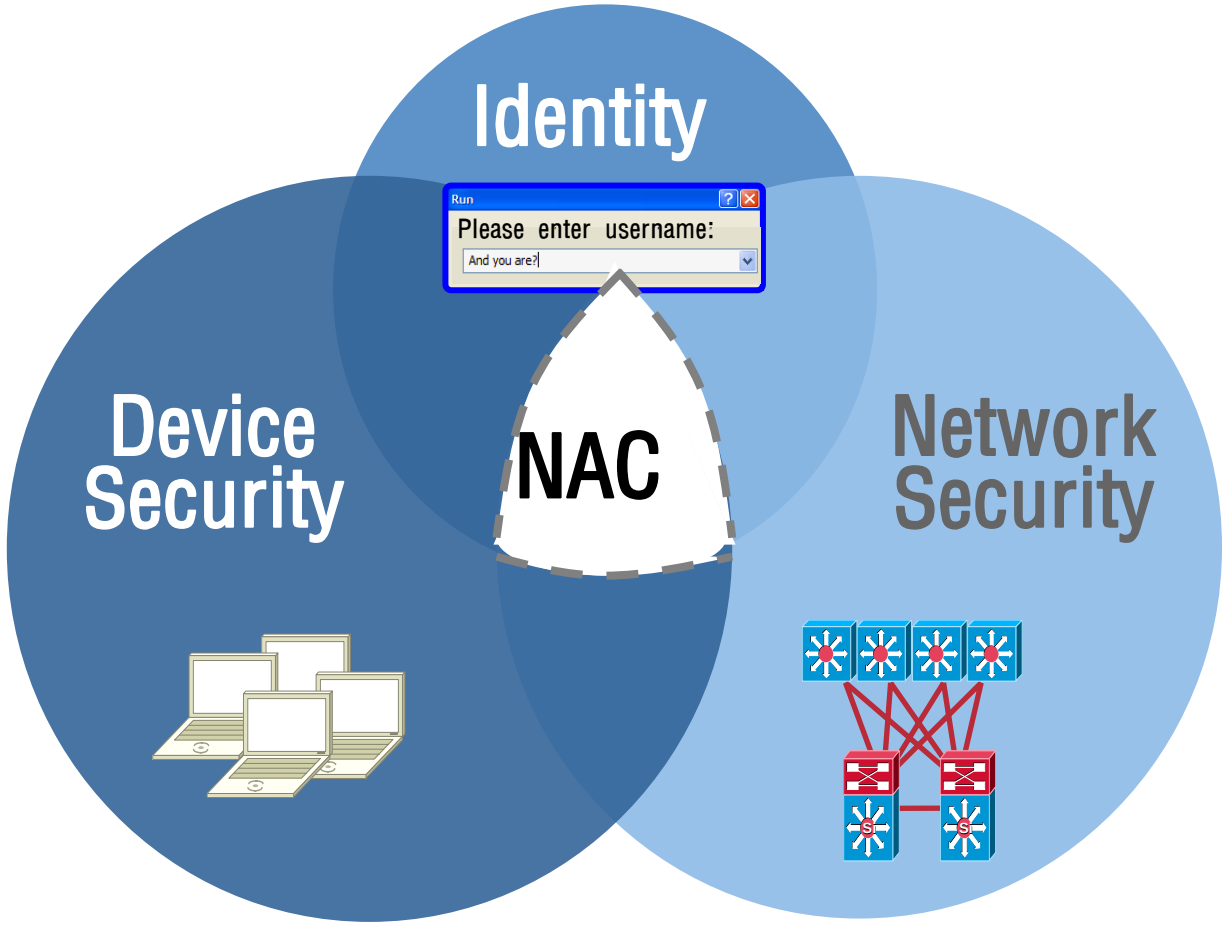
위협에 대한 적극적 대응
심도 깊은 보안
통합형 보안 장비 구성

TREND MICRO

Agenda

1. 보안 기술 동향
2. 사용자 보안 – Cisco NAC Overview
3. 통합보안 기술 Overview

Cisco NAC (Network Admission Control)이란?

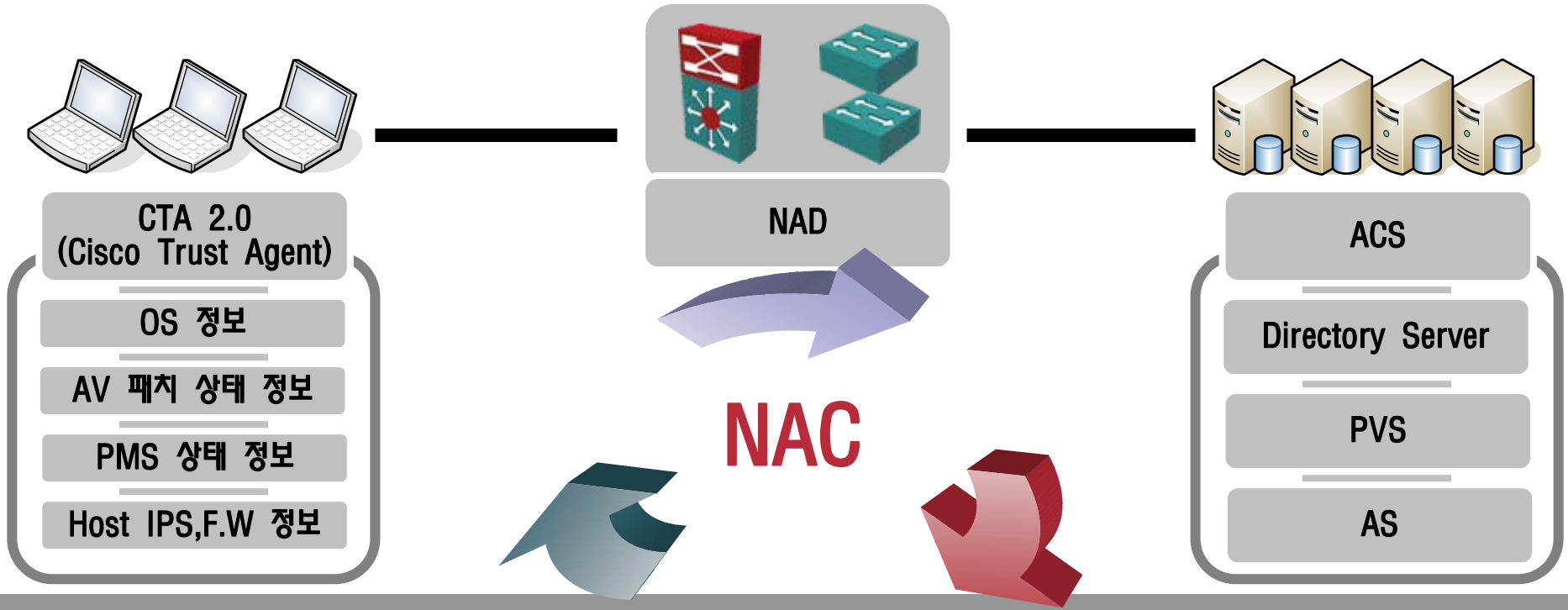


Cisco NAC(Network Admission Control)이란?

Cisco NAC

사용자의 기본적인 보안 상태와 다양한 사용자 보안 프로그램들의 상태 정보를 파악하여, 사용자가 보안의 건강성을 충분히 가지고 있는지를 점검

사용자가 보안 건강성을 유지하고 있지 않는 상태일 경우 자동 격리, 치료



NAC Appliance Enforces Compliance

누가, 어떤 권한을 요구합니까?

정상적인 접근을 위해서 요구되는 사항은?

비정상접근시에는 어떠한 조치를 받습니까?

관리와 구성은 어떻게 되나요?

Securely Identify Device and User

사용자 인증과 권한 (local db, RADIUS, LDAP, Kerberos, AD, etc.)

모든 환경에서의 접속 (LAN, wireless, remote/VPN, WAN)

Enforce Consistent Policies

중앙 집중 관리를 통한 정책 배포

AV,개인 보안 툴을 통한 취약점 분석 및 패치 관리

Quarantine and Remediate

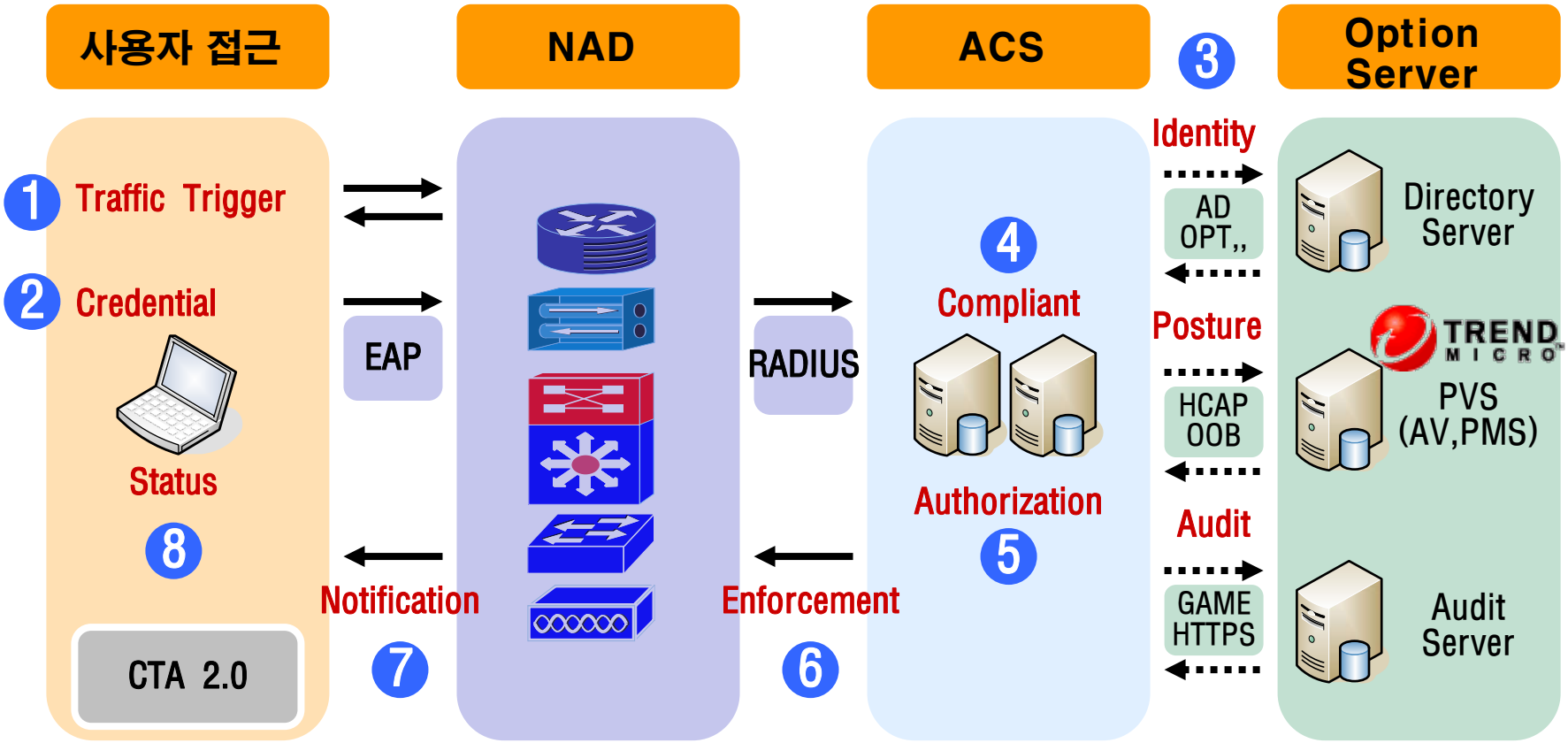
사용자 기반의 검역 및 치료 서비스 제공

Configure and Manage

사전 Config를 통한 간단한 룰 생성 및 관리

웹기반의 정책,치료 관리 서비스

NAC Architecture
NAC 기본 동작 개요

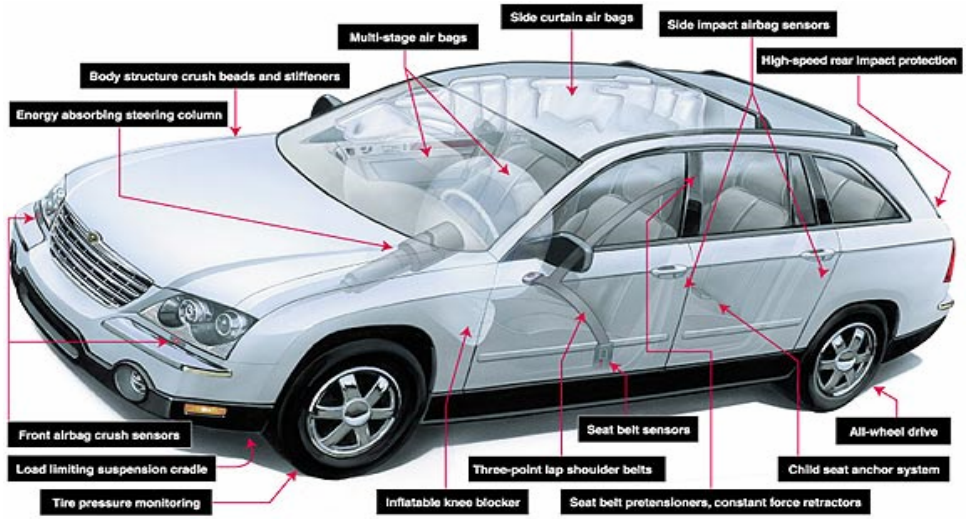


사용자의 보안 건강성 상태에 따라 네트워크 접근 허용, 접근 제어, 검역 구역 이동 등에 따른 조치를 받게 된다.

Agenda

1. 보안 기술 동향
2. 사용자 보안 – Cisco NAC Overview
3. 통합보안 기술 Overview

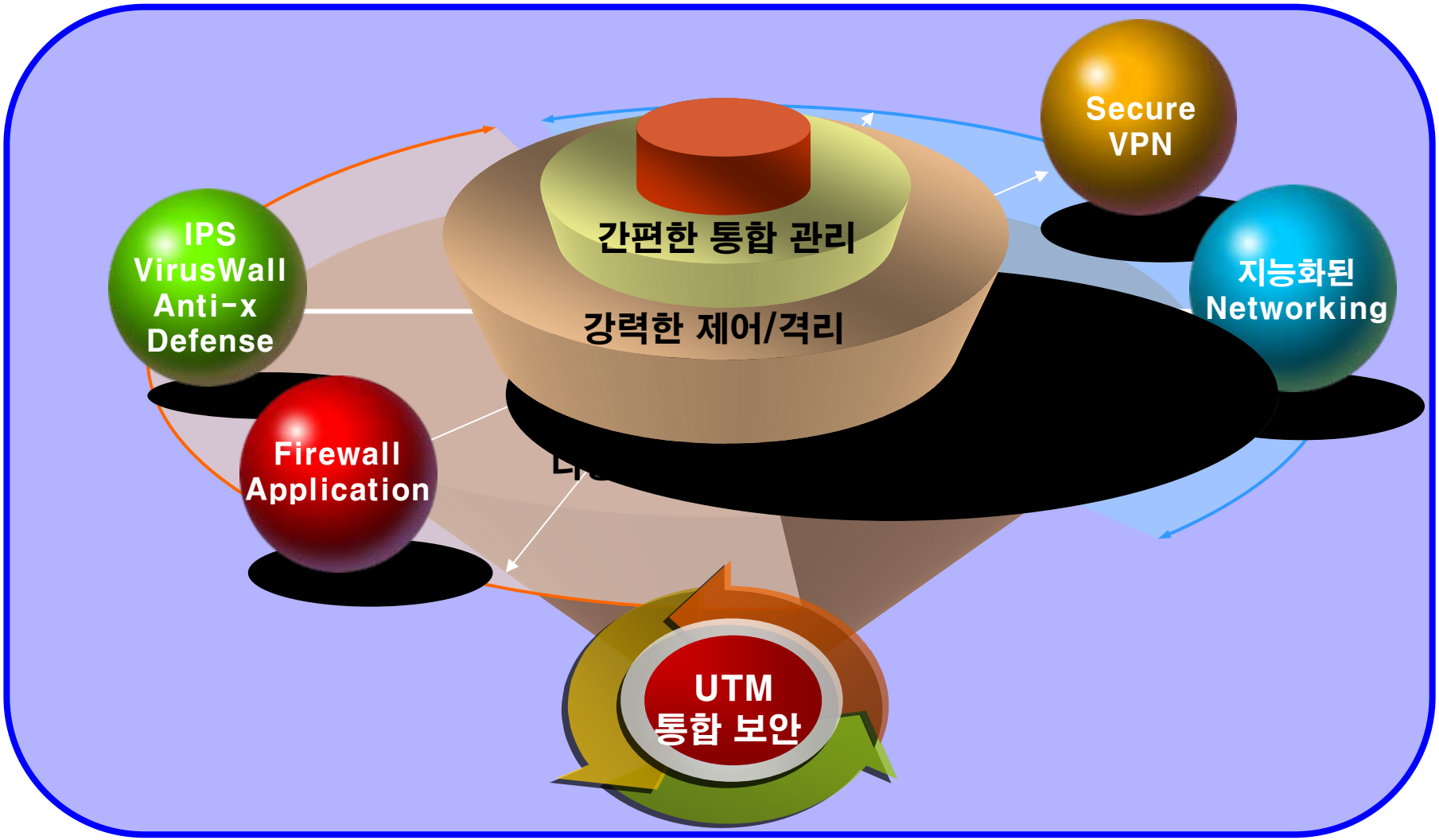
왜 통합보안이 대세인가?



- 복잡한 보안/운영환경
- 상호 운영성에 대한 모순
- Lower Visibility
- 복잡한 설치와 관리
- Higher TCO

- 간편한 보안/운영환경
- Tighter Integration = Tighter Security
- Greater Visibility
- 손쉬운 설치와 관리
- Lower TCO

통합 네트워크 보안이란 ?
UTM (Unified Threat Management)



통합 네트워크 보안
Cisco UTM Solution - ASA 5500 + CSC (Trend Micro)

Integrated / Convergence … D / V / V / M
Requires Integrated, Pervasive Security

감사합니다.