[기조연설]

IBM Security Summit 2011

스마트 시대와 복합적 사이버 위협의 만남

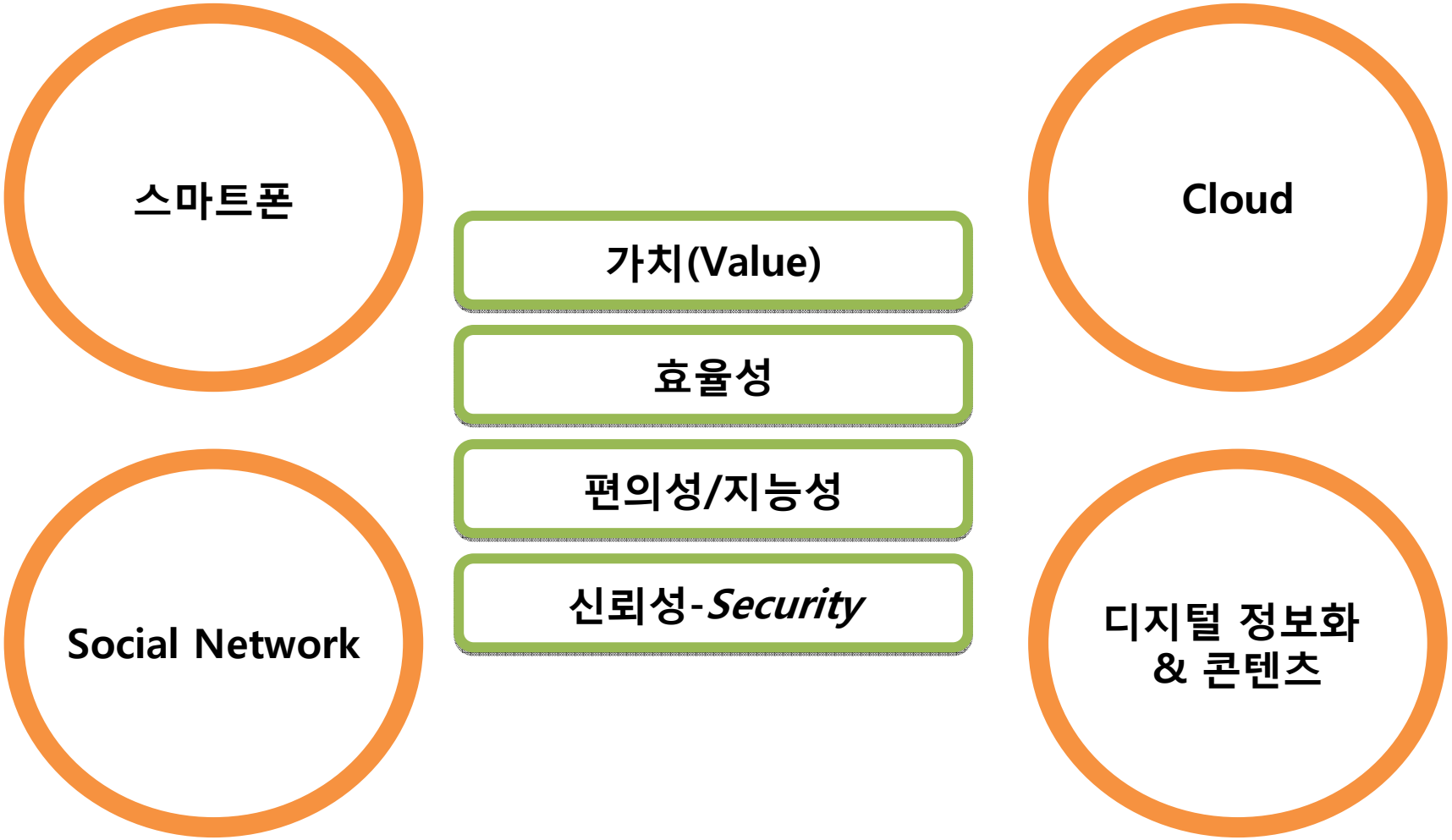
2011. 5. 18

김홍선 대표이사 (CEO, 안철수연구소)

안철수연구소

IT 패러다임의 변화

Platforms & Business Model



통합적 소프트웨어 플랫폼

Service Platform

- Social Network
- Web Service
- Cloud

Accountability | **Security** | **Intelligence**

Device Platform

- Utilities
- Security
- Backup
- 최적화
- 가상화
- 동기화



스마트폰 시대의 키워드

"나" 중심으로 세계를 보는 스펙트럼

Convergence

- ✓ Technology + Liberal Art
- ✓ Apps + Contents + 광고
- ✓ Home + Biz + 모바일

IT 산업의 구조적 변화

- User의 접근성 요구 확대 - *Consumerization*

  Device, Platform, Browser, Contents, Service, etc.

- 플랫폼 중심의 재편 – Clous/SNS vs. Smart Devices

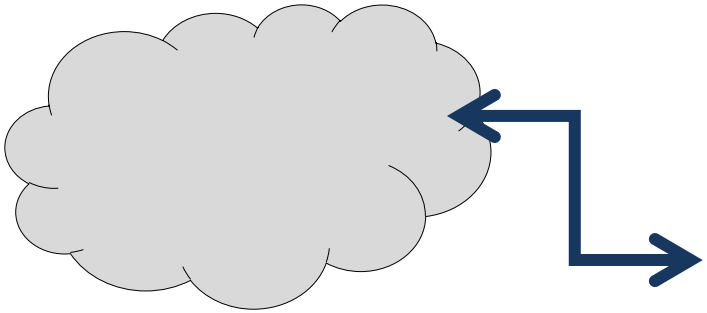
- 무너지는 사업 영역 – HW? SW? Service? Contents?

- 보안 위협의 사업화, 브랜드화, 글로벌화

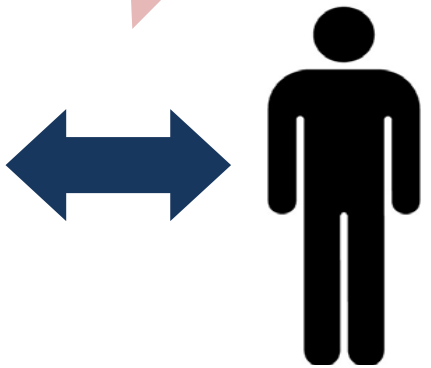
→ **Mobile, Social, Large, Secure**

소프트웨어/보안의 범위

✓ 지능성



Social

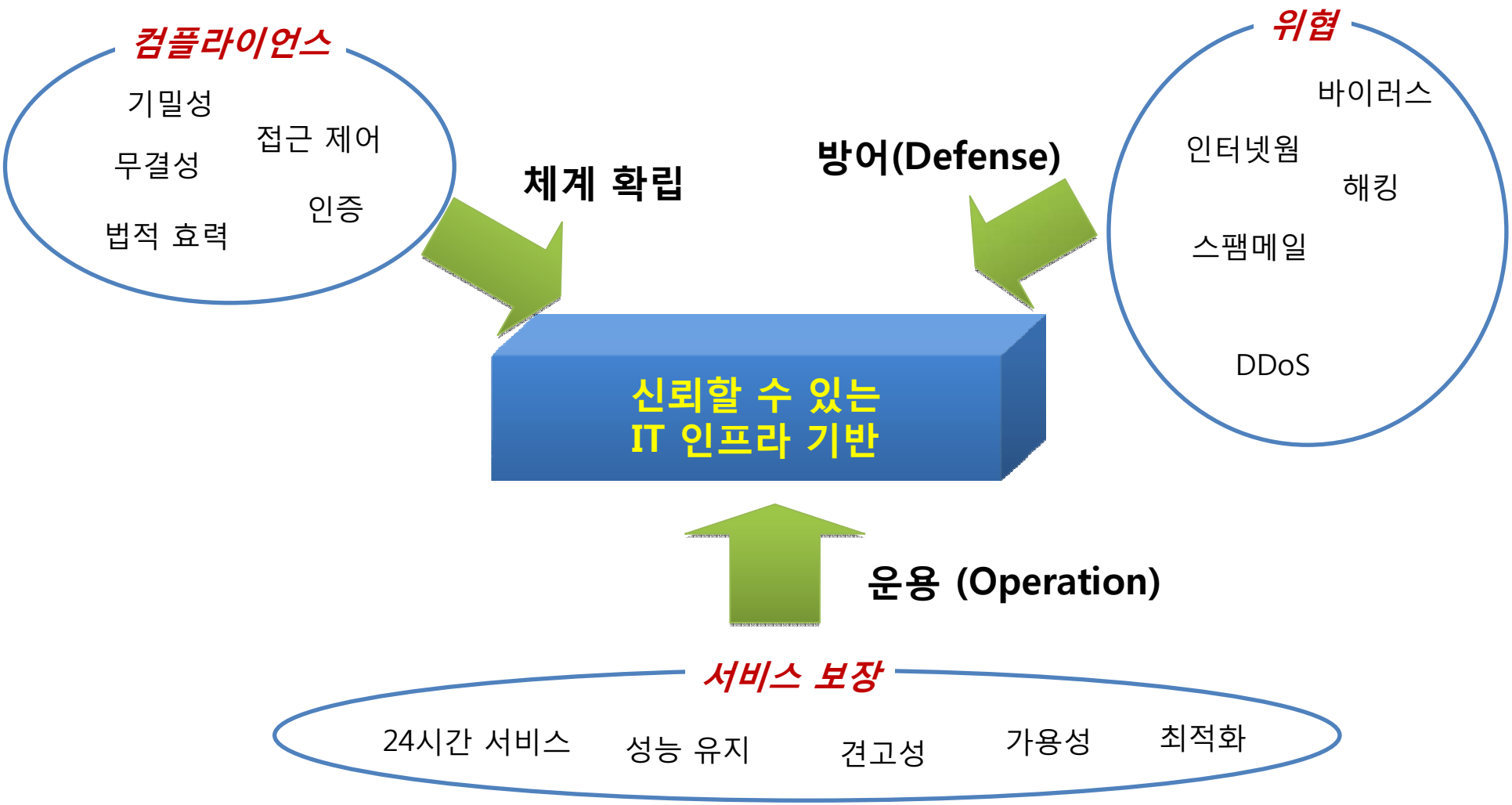


✓ 사용친화성

✓ Accountability

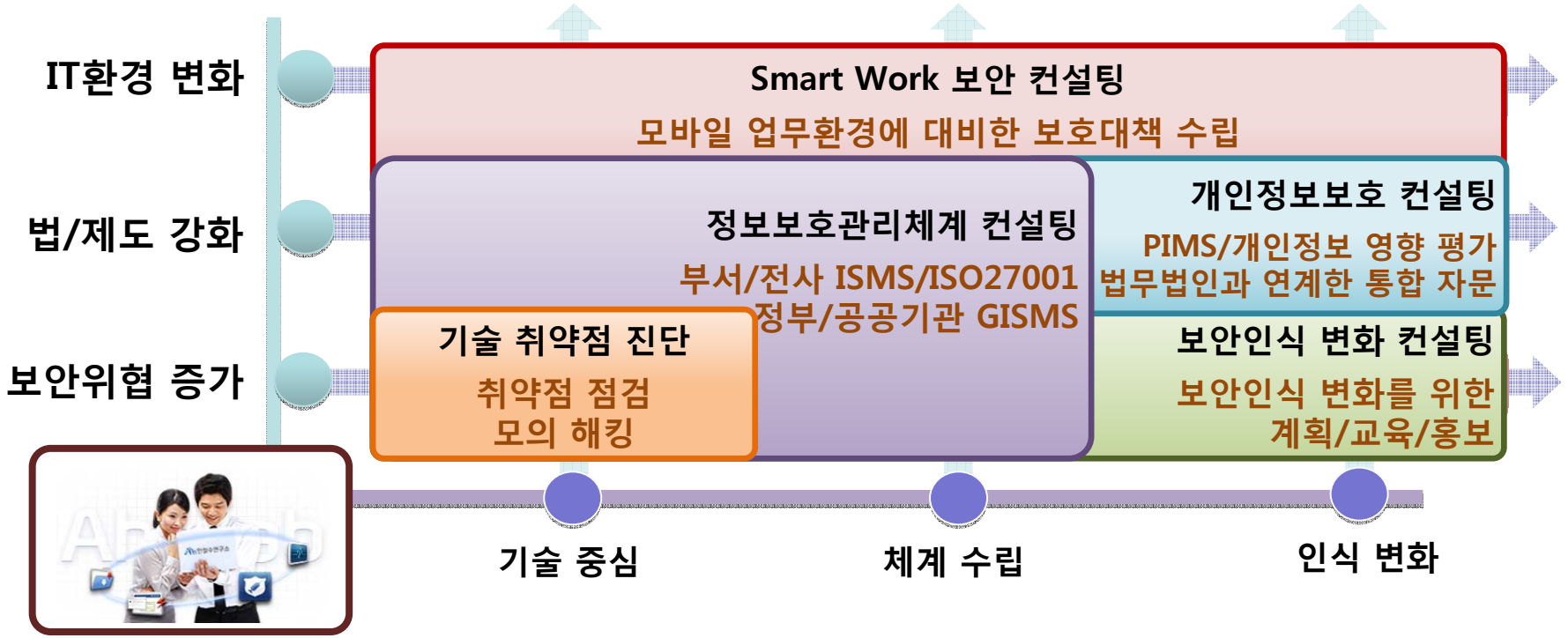
정보 보안의 범위와 역할

정보 보안의 기본 역할



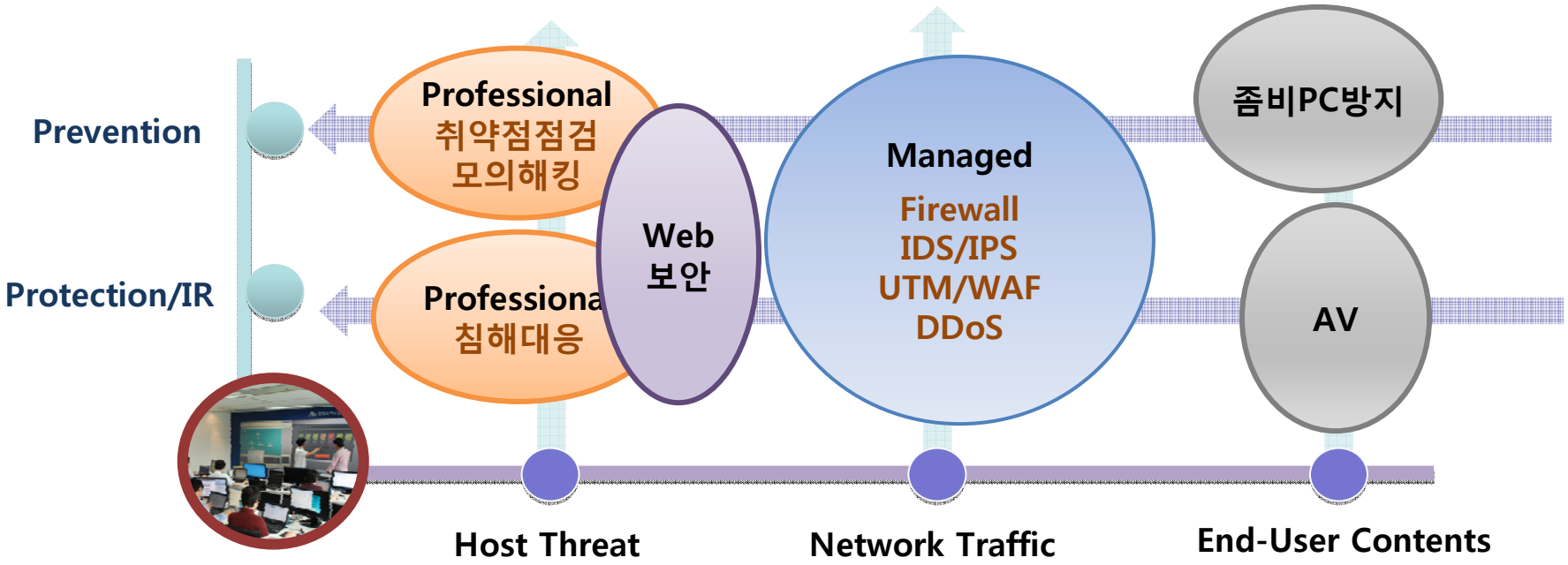
Regulation Vs. 실행 – 실효적 컴플라이언스

보안컨설팅 + 지속적인 점검 + 교육 + Business Development



변화하는 각종 위협, 법/제도, IT 패러다임의 변화에 대응한 방안

복합적 사이버 위협 : End Point, 웹, 네트워크



사전 위협부터 사후 대응에 이르기까지 종합적인 대응 필요

사회 발전과 보안의 관계

✓ 인터넷은 사회의 기반 인프라다

✓ 인터넷은 신뢰할 수 없는 글로벌 공간이다

IT 현황

모든 PC는 네트워크로 연결되어 있다

인터넷 서비스는 비약적으로 생성된다

공격과 위협

범죄화

조직적

입체적

글로벌

정보 보안은 지식 기반 사회의 핵심이다

History of Wars

✓글로벌 테러✓공격 Vs. 수비
✓민간 분야에✓Walls
✓안전지역

IT 환경 변화와 위협 패러다임의 변화

IT 사용 환경의 변화

- 사용자 접근성 확대

  단말기, 플랫폼, SNS, 브라우저, 웹

- 상시 연결성(Always-on) - 브로드밴드

- IT플랫폼의 개방화 / 개인화

  클라우드 / SNS vs. 스마트 디바이스

위협 패러다임의 변화

- 입체적 공격

  PC, 스마트폰, NW, 웹, SNS, 사회공학

- <악성코드> 중심의 사이버 공격

- 해킹 도구의 상품화, 브랜드화, 글로벌화

- 다양한 침해 시나리오

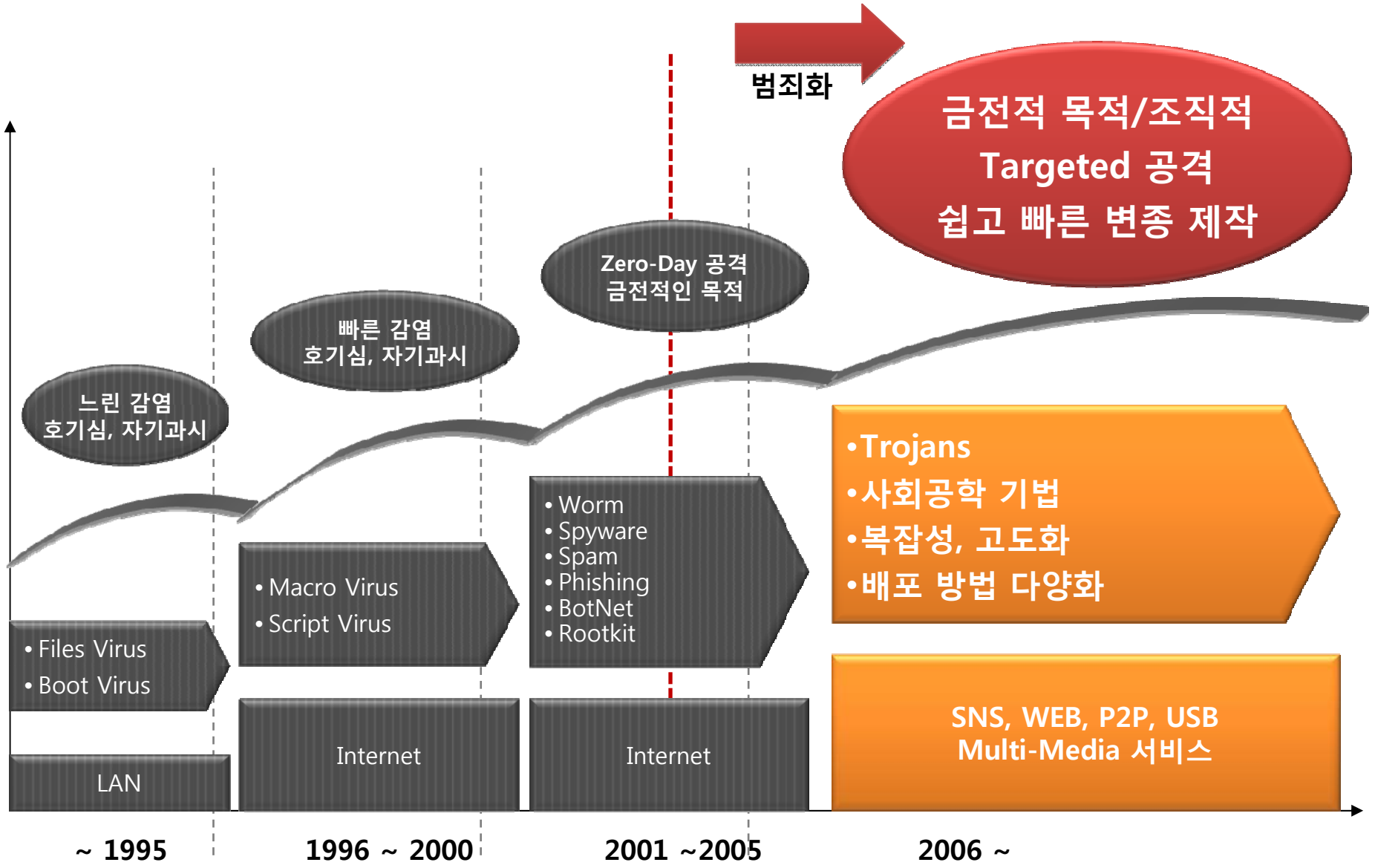
Cross Platform 전문성

원천 기술 & 실전 경험

신속한 악성코드 분석

입체적인 실시간 대응체계

악성코드의 트렌드 변화



사이버 위협 동향

Multi-Location

- End Point
- Network
- Web
- Transaction
- Resource

Multi-Directional

- Outbound
- DDoS
- 컨피커 웜
- ARP 스푸핑

Timeline

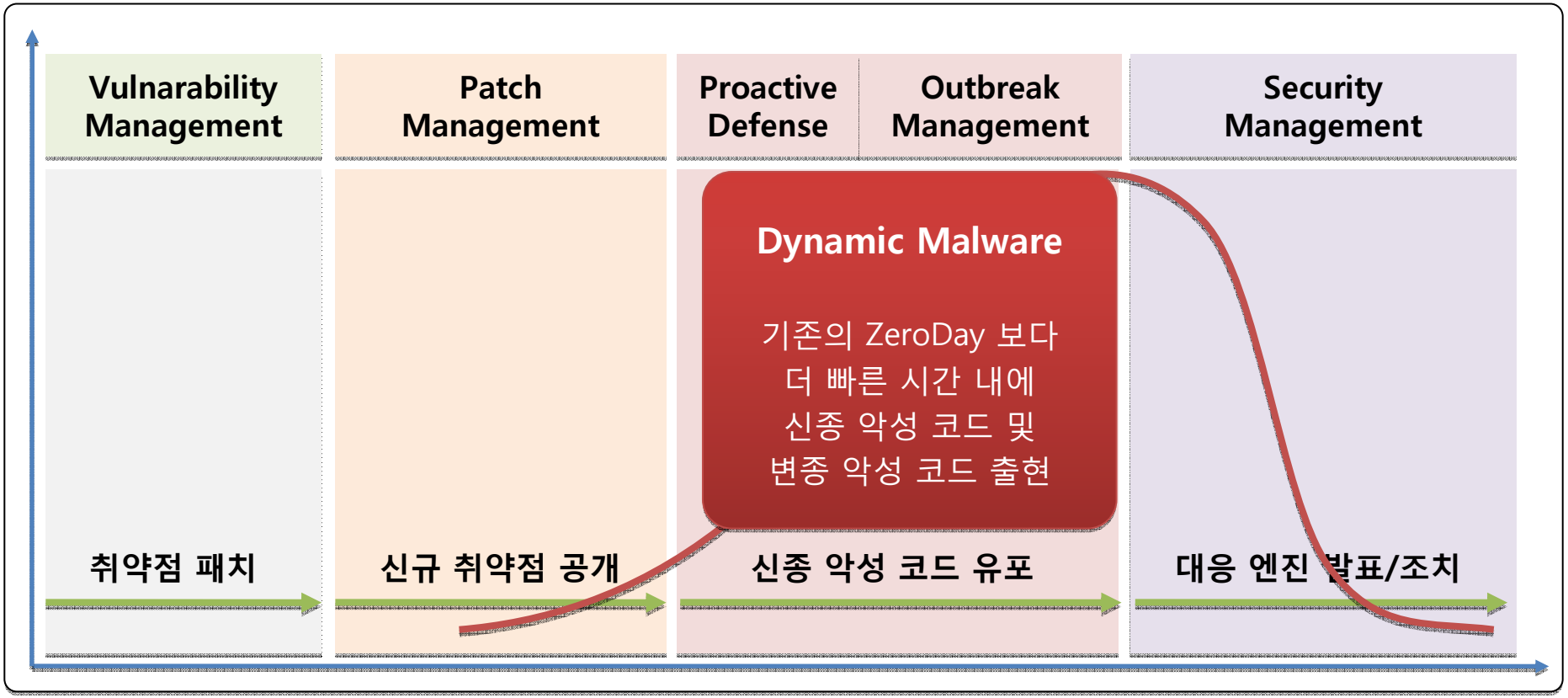
- Timing control
- 제로 데이 공격
- 순차적 잠입
- C&C

입체적

- 사회공학적 기법
- 자원 관리의 허점
- 신규 사업 모델의 취약점
- Social, Mobile, Commerce

악성코드의 라이프사이클

악성코드 대응의 시간축 (Time Dimension) 에 대한 고려



Static Malware
Zero-Day Attack
Internet

Malware → **Malware 2.0**

Dynamic Malware
Targeted Attack
Web/SNS/Multi-Media

최근 정보보안의 키워드

정보보안 산업의 특성

Technology	Product	Service
✓ 악성코드	✓ AV/PC 보안	✓ CERT
✓ 해킹도구	✓ Firewall/UTM	✓ 컨설팅
✓ 클라우드	✓ VPN	✓ 취약점 분석
✓ End Point	✓ IPS/IDS	✓ 모의 해킹
✓ 네트워크	✓ 디도스 방어	✓ Forensic
✓ 웹 프로그래밍	✓ PKI	✓ 관제서비스
✓ 암호화	✓ ESM	✓ 보안 SI
✓ 로그 분석	✓ 문서 보안	✓ 교육
✓ 인증	✓ WAF	✓ 개인정보보호
✓ 가상화	✓ DB 보안	✓ 보안 정보
✓…..	✓ …….	✓ …..

Tightly-Coupled

입체적, 지능화 공격

Office

내부정보 탈취

모바일 공격

네트워크 공격

PC 시스템 공격

WEB 공격

기업 정보
고객 정보

INTERNET
정보 유입/유출

- ✓ 웹서핑
- ✓ E-mail, 메신저
- ✓ SNS

IDC / Server Farm

서버 시스템 공격

업무 서버

서비스 공격
(DDoS attack)

웹 서버

복합적
입체적

MITM
(트랜잭션 공격)

INTERNET
서비스 제공

서비스 이용
고객 공격

- ✓ 웹서비스
- ✓ 금융서비스
- ✓ 게임서비스

Production Line

생산시설 공격

정보 보안 업무의 특성

Mission Critical	✓ 절대적 안정성, 신뢰성, 내구성 ✓ 축적된 환경 경험
전문 서비스	✓ Hands-on, Integration
다양한 Segment	✓ 신뢰와 소통 ✓ 사업 모델과의 조화
Dynamic	✓ Sensitive to IT trends ✓ Legacy와의 충돌

→ **통합적 관리 & Accountability**

Suggestions

- **Multi-Dimensional 방어 체계**
  - ✓ '예방-방어-추적'의 Lifecycle
  - ✓ Time 축의 고려 - 역동적으로 진행하는 위협 대응
- **Multi-Layered 방비**
  - ✓ IT Architecture
  - ✓ 정보의 흐름
  - ✓ 정보의 Context 분석 – 지능적, 복합적 시스템
- **명확한 가이드라인 – 편의성 Vs. Compliance**
- **최고 경영층의 책임 의식**
  - ✓ 정보 자원의 생성, 소멸, 활용의 책임자

감사합니다.

Blog: http://ceo.ahnlab.com
Twitter: @hongsunkim