기업 네트워크 보안 디자인

서 길 영 (kiseo@cisco.com)

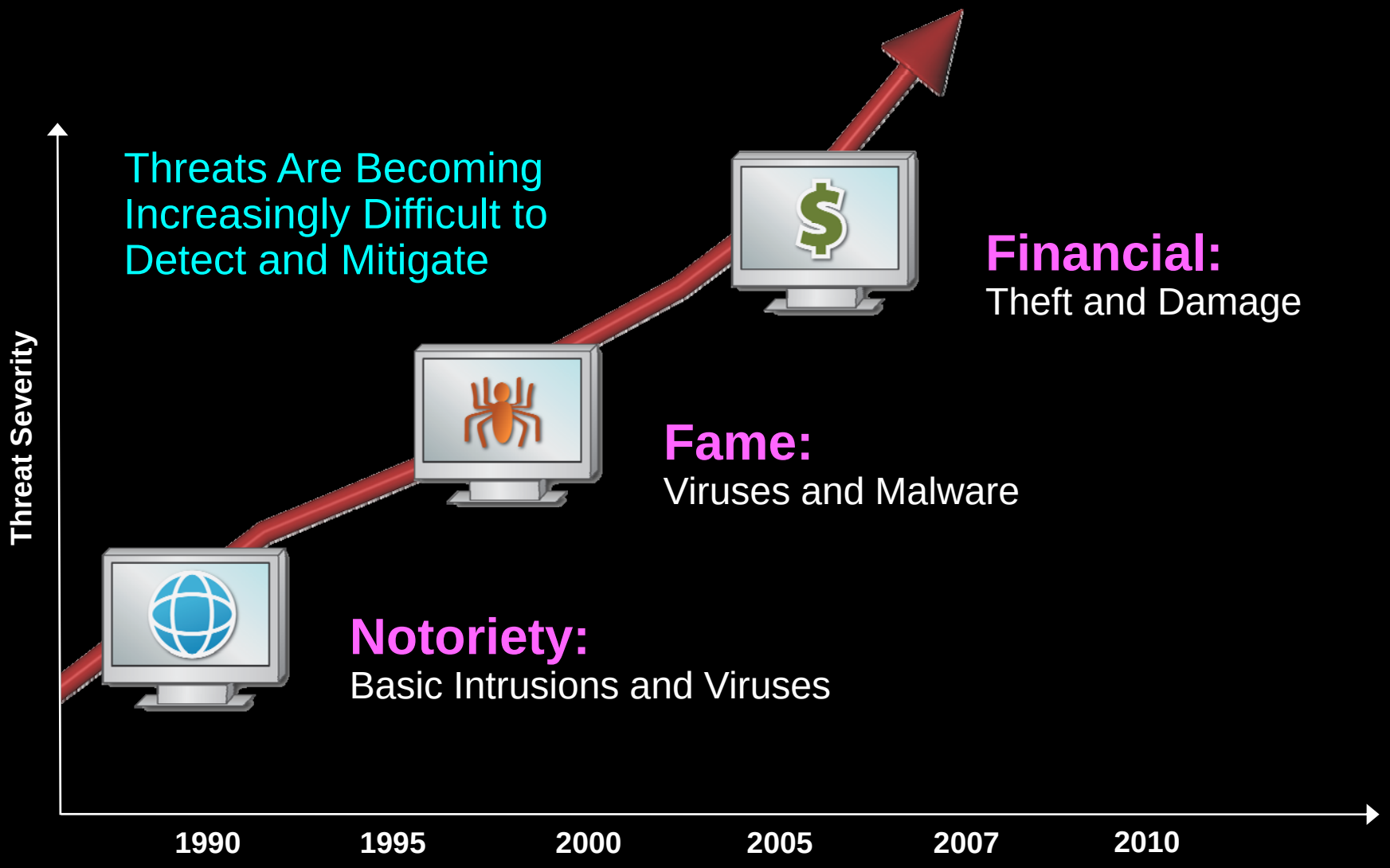
Cisco Systems Korea

Agenda

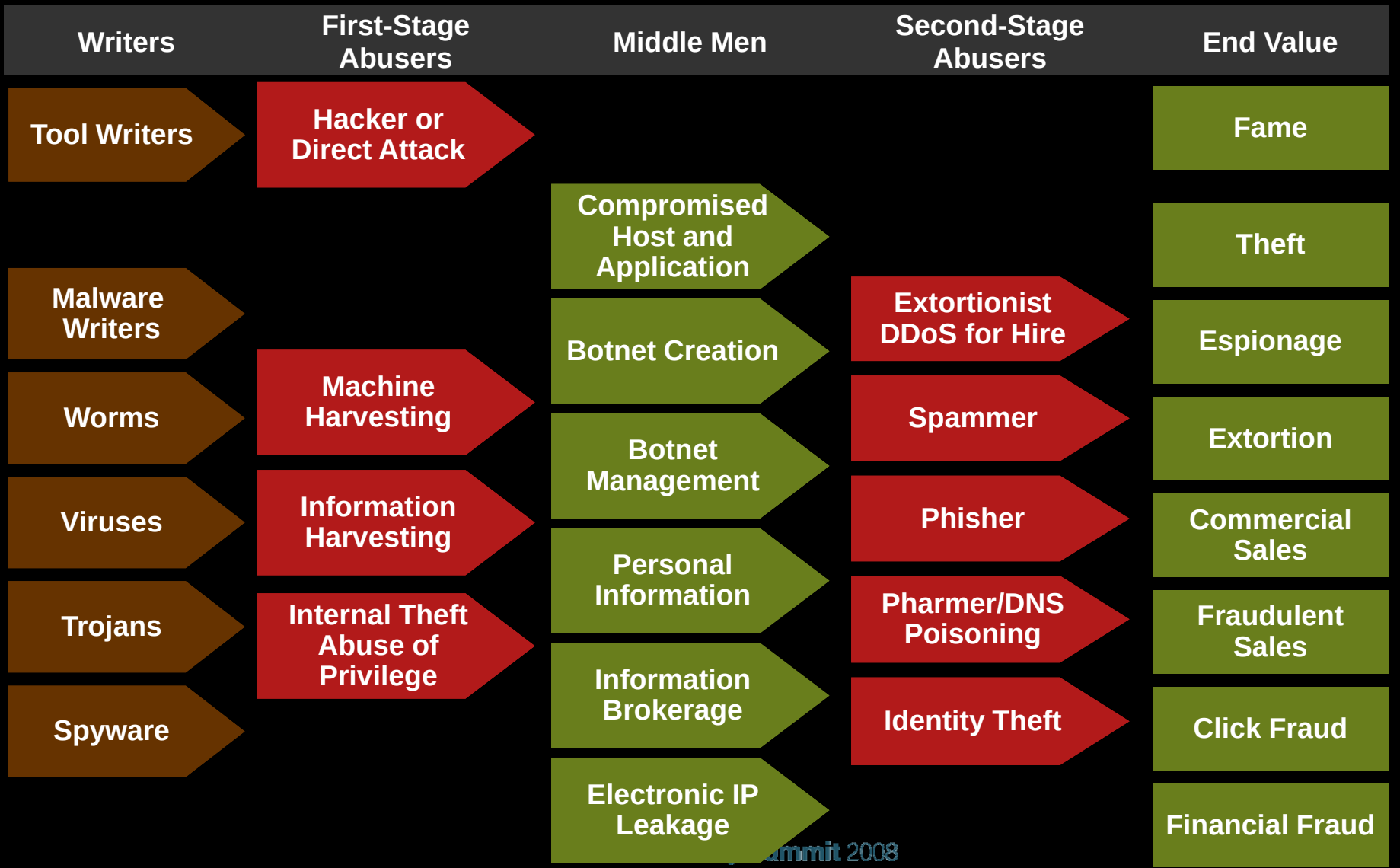
- 최근 공격 동향과 추세
- 네트워크 보안을 위한 접근 방법 및 고려사항
- 네트워크 보안 디자인 구성
- 요약

최근 공격 동향과 추세

공격 목적의 변화



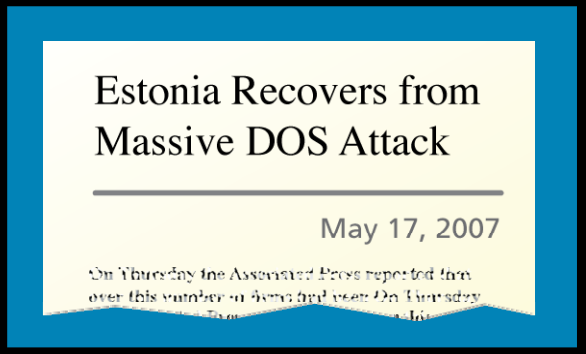
보안 위협의 진화



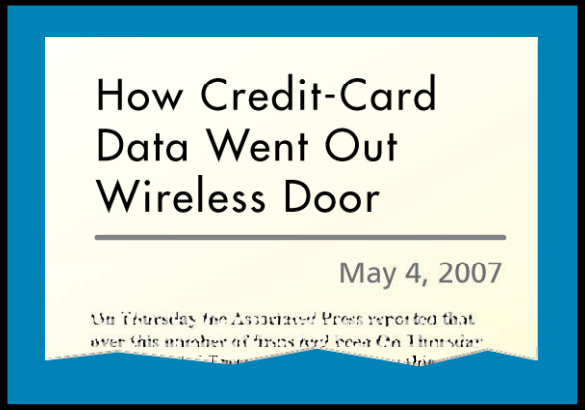
새로운 형태의 보안 위협

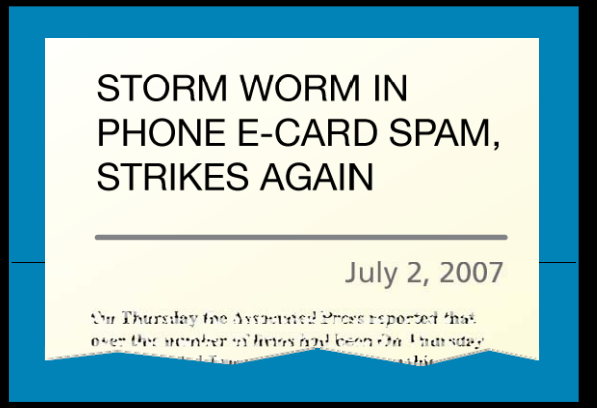
Source: 2007 CSI Survey

최근의 보안 위협 사례



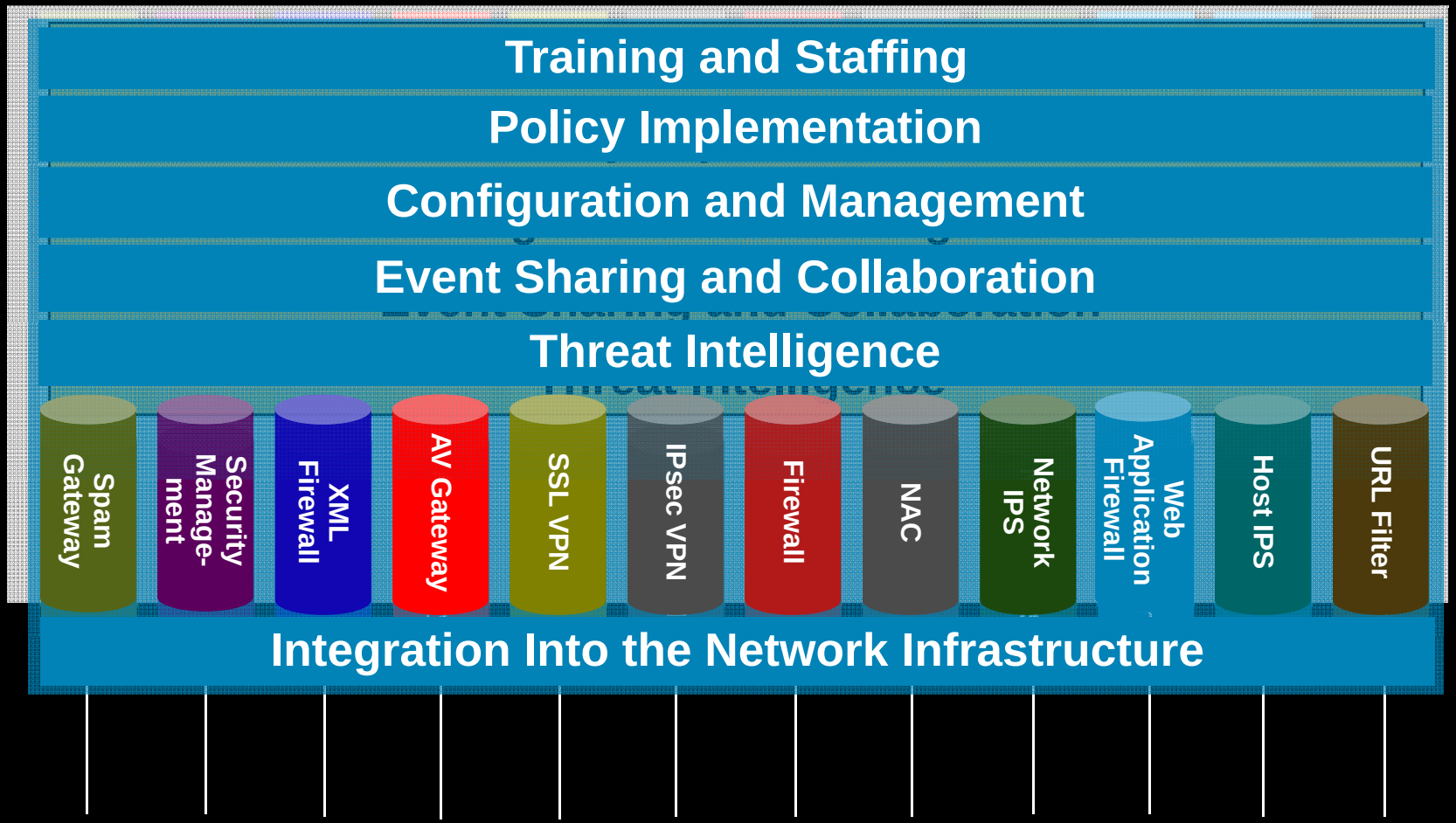
- 다운타임 발생으로 인한 서비스 중단
- 데이터 손실 및 개인정보 유출
- 기업, 국가 이미지 손상
- **DDoS** 공격의 규모 및 범위 증가





네트워크 보안을 위한 접근 방법 및 고려사항

보안에 대한 시스템적 접근



SDN 사상과 적용 기술

Integrated	Adaptive	Collaborative

- Firewall
- N-IDS / IPS
- Router
- Switch

- Anti-Virus
- Anti-Spyware
- H-IPS
- Access Control

- Anti-Phising
- Content Filtering
- Email Security

- XML F/W
- Application F/W

- Traffic Control
- Worm Prevention
- ACL
- L2 Security

- Virus Prevention
- Host Protection
- Network Admission Control

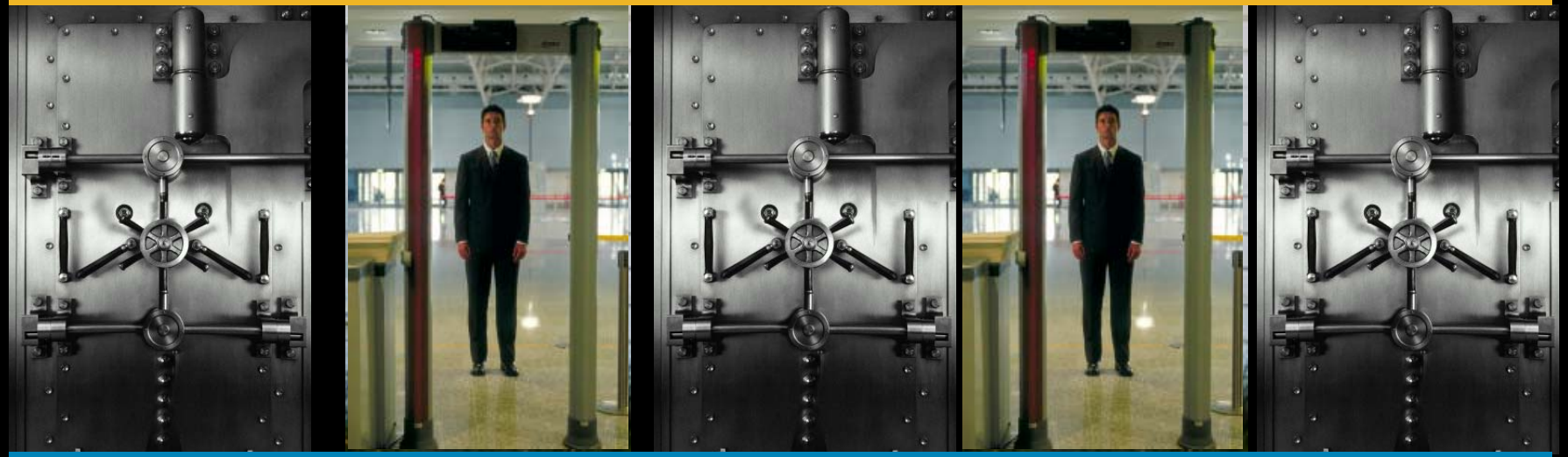
- Malware Prevention
- URL Filtering
- Anti-Spam
- Data Loss Prevention

- App. Attack Prevention
- XML Packet Inspection

컨텐츠 보안의 필요성

Port 25 **Port 80**

Content Security

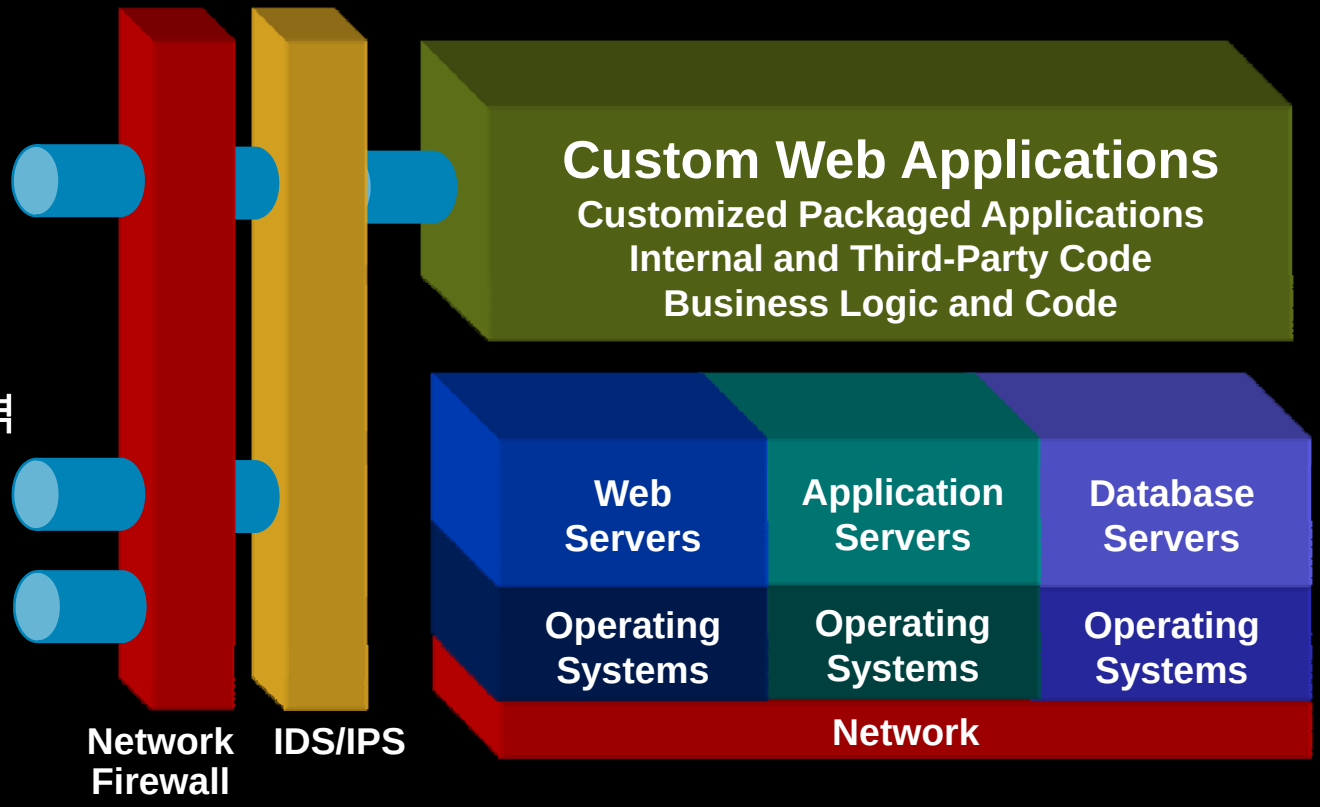


Network Security

Locked the Network Doors, but E-Mail and Web Stayed Open

어플리케이션 보안의 필요성

새로운 어플리케이션 공격의 **75%** 이상이 커스터마이즈된 어플리케이션 대상의 공격



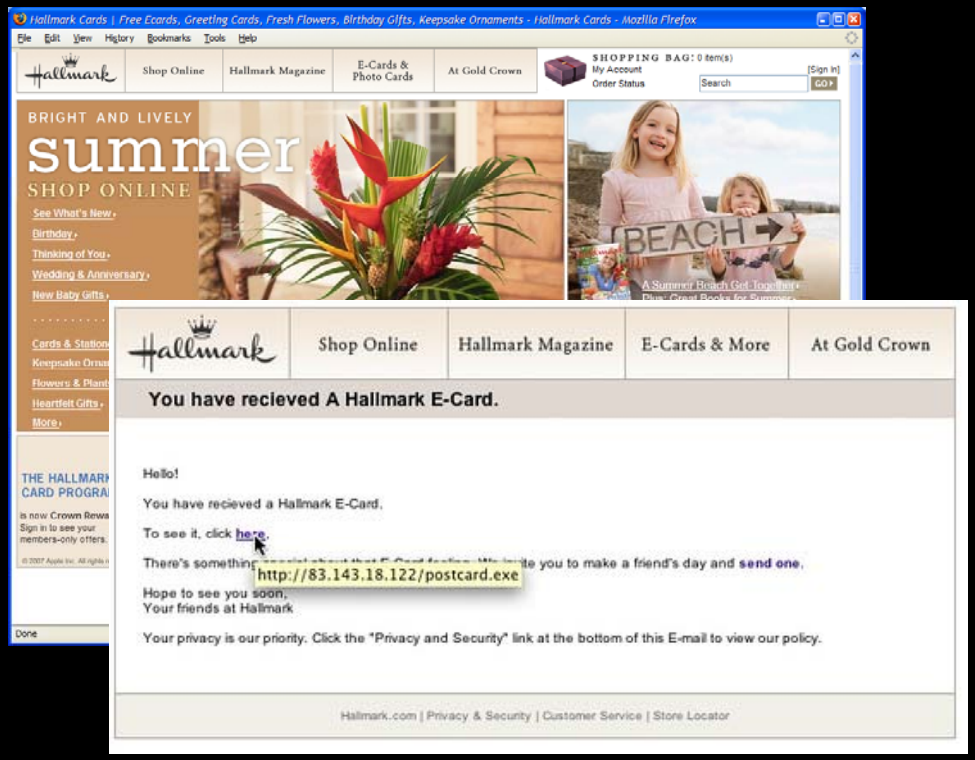
"50% of enterprises and government agencies are using XML, Web services or SOA."

Source: Gartner

"XML accounted for 15% of internet traffic in 2005. By 2008, it is expected to account for 50%."

Source: 451 Group

이메일과 웹 보안 위협

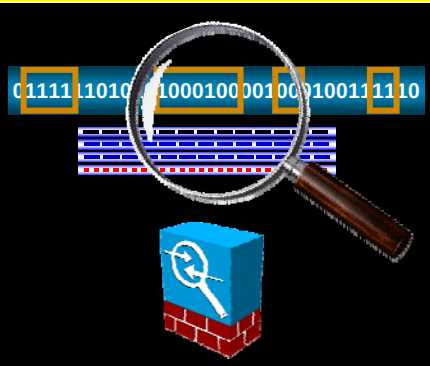


- 봇넷에 의해 전송되는 스팸 메일
- 악성코드가 존재하는 웹 서버로의 링크
- 홈페이지 방문시 사용자 시스템이 악성 코드에 의해 감염
- 스피어 피싱

영역별 적용 보안 기술

- ACL
- Firewall
- RFC2827
- uRPF
- CoPP
- Netflow
- L2 Security

- N-IDS / IPS



- Application Recognition (NBAR)
- Flexible Packet Matching (FPM)
- F/W w/ App. Engine
- Content Security

- XML F/W
- App. F/W

- DDoS Solution
- H-IPS
- Email Security
- DNS Safeguard

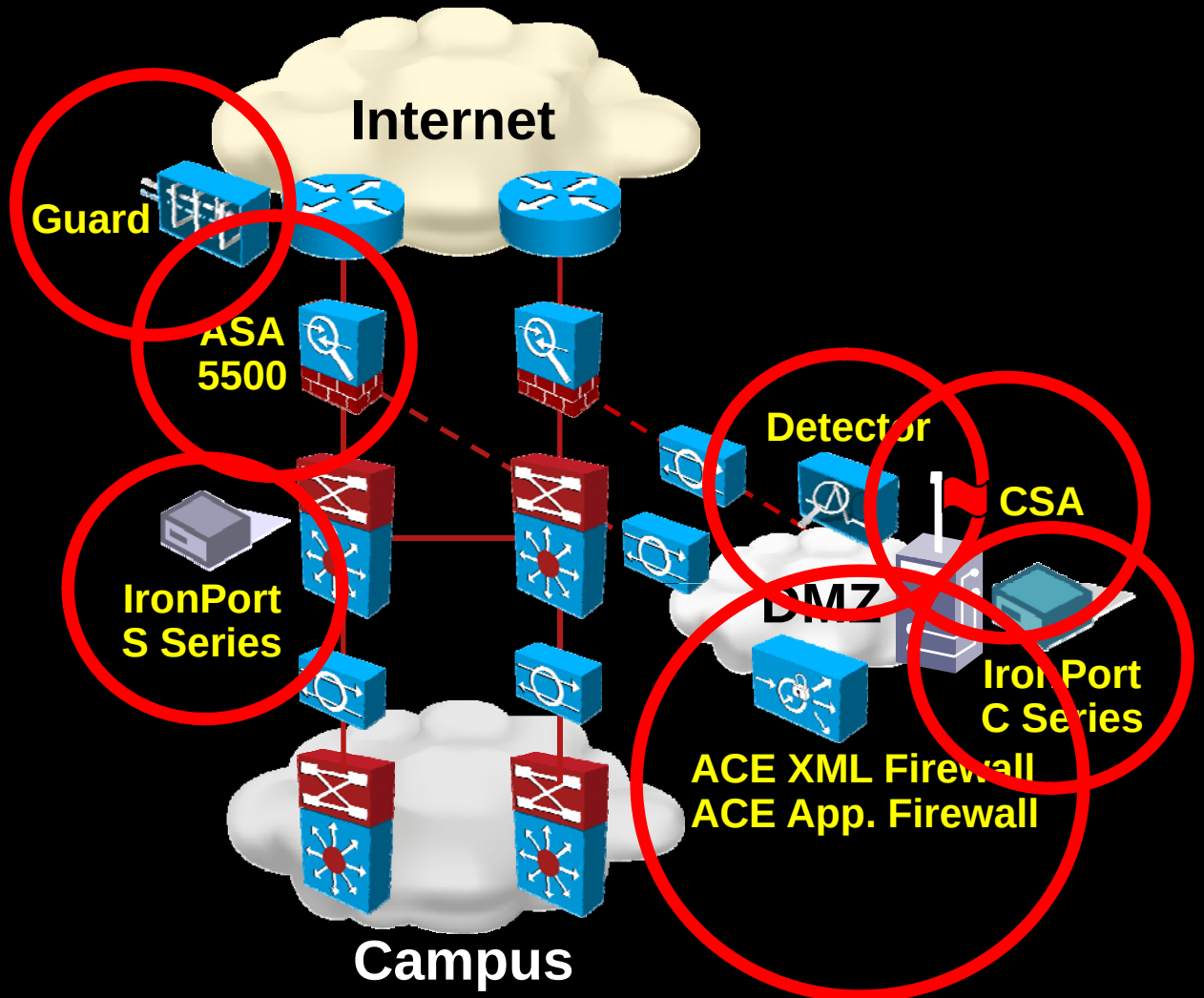
▪IP ▪TCP/UDP	▪Worm Prevention	▪Packet Inspection ▪Malformed App.	▪App. Attack Protection	▪DDoS Protection ▪Data Loss Prevention

시스코 컨텐츠, 어플리케이션 보안 제품

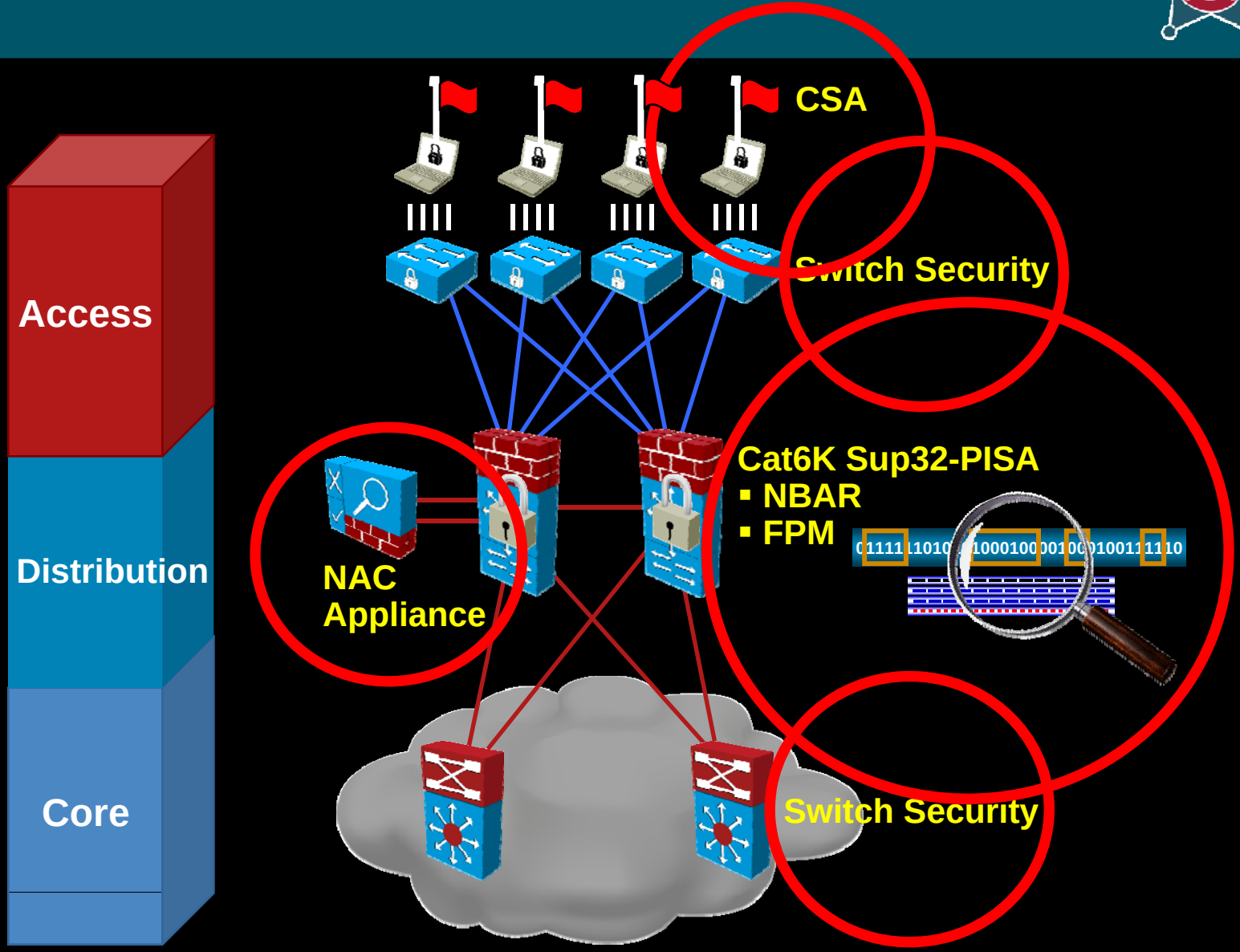
Application Inspection	▪ ASA 5500 Series ▪ Cat6K Sup32-PISA ▪ ACE XML Firewall ▪ ACE Application Firewall
Content Security	▪ IronPort S Series (Web Security) ▪ IronPort C Series (Email Security)
Endpoint Security	▪ NAC Appliance ▪ Cisco Security Agent (CSA)
DDoS Attack Prevention	▪ Guard and Detector

네트워크 보안 디자인 구성

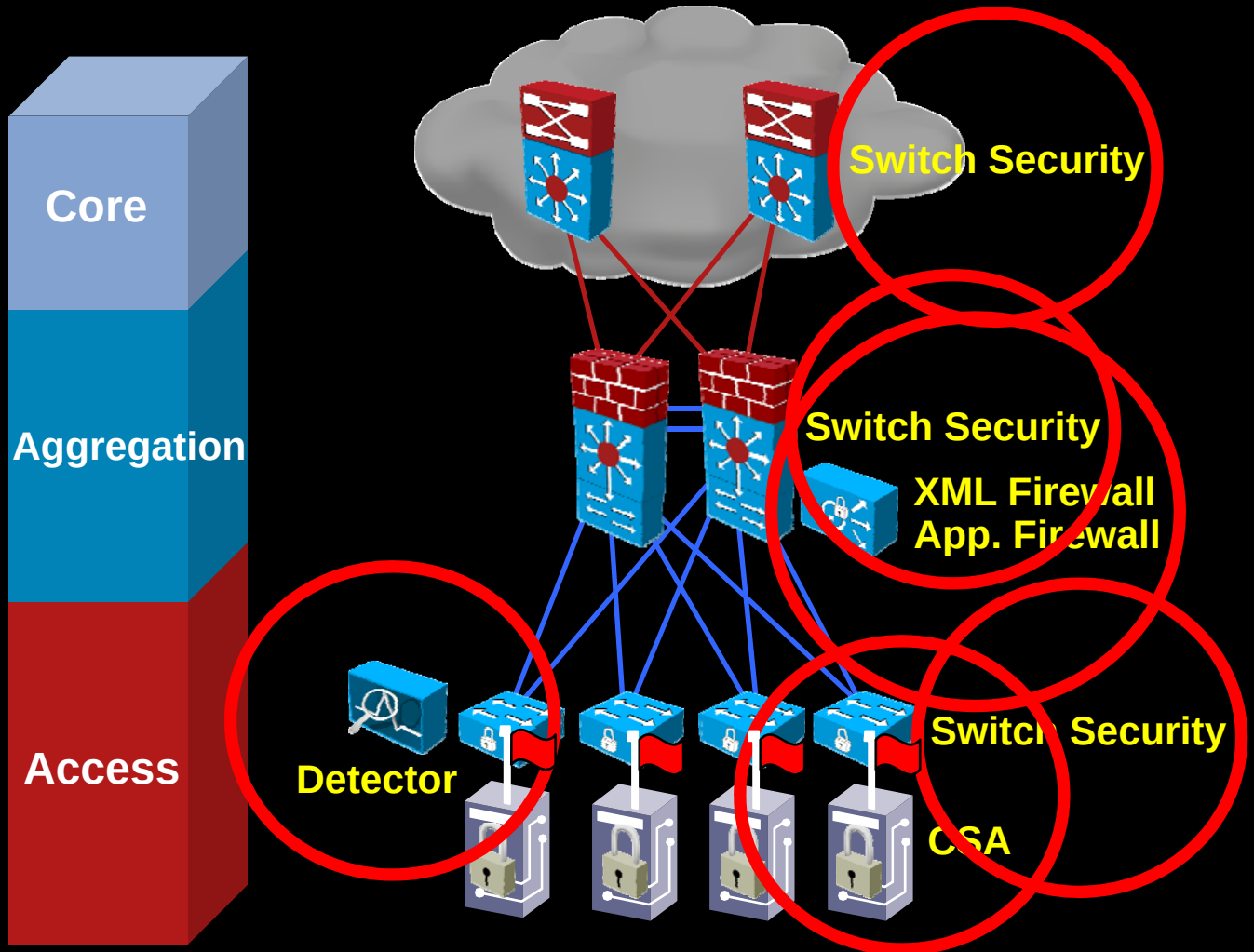
네트워크 디자인 구성: 인터넷 에지



네트워크 디자인 구성: 캠퍼스 네트워크



네트워크 디자인 구성: 데이터센터



요약

요약

- 새로운 형태의 보안 위협에 대응할 수 있는 시스템적 접근 방법 필요
- 지능적이고 복잡한 보안 위협을 고려한 심층적 보안 시스템 요구
- 기업의 네트워크 영역별로 특화된 보안 디자인 적용

CISCO