변화된 IT 환경을 위한 시스코의 새로운 보안 전략 소개

김용호 차장(yonghkim@cisco.com)

April 14, 2011

Agenda

1. 변화하고 있는 IT 업무 환경
2. 특명!! 모든 상황을 인식하라!!
3. 모든 상황을 반영하는 시스코의 보안 제품 업데이트

변화하고 있는 IT 업무 환경

중대한 변화


166M
향후 3년간 1억
6천만대 디바이스

200% 사용자 만족도 증가

25% 비용 절감

50% 서버 사용량 감소

30% 응용프로그램 성능 증가

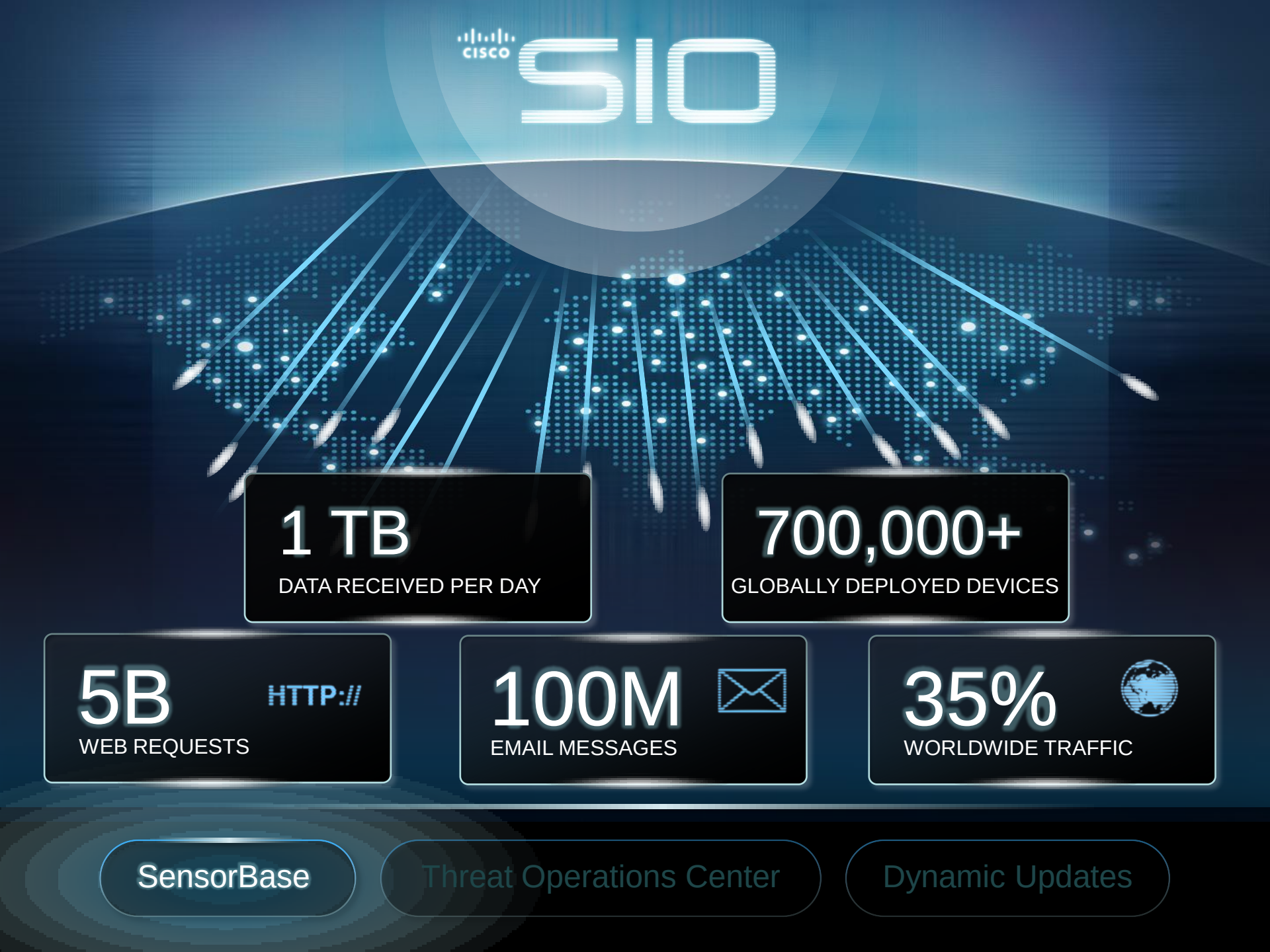
95% 구축 시간 절감

특명!! 모든 상황을 인식하라!!

CONTEXT


cisco
SIO
정확한 탐지
전방위적인 보호
지속적인 업데이트


cisco
SIO
정확한 탐지
전방위적인 보호
지속적인 업데이트

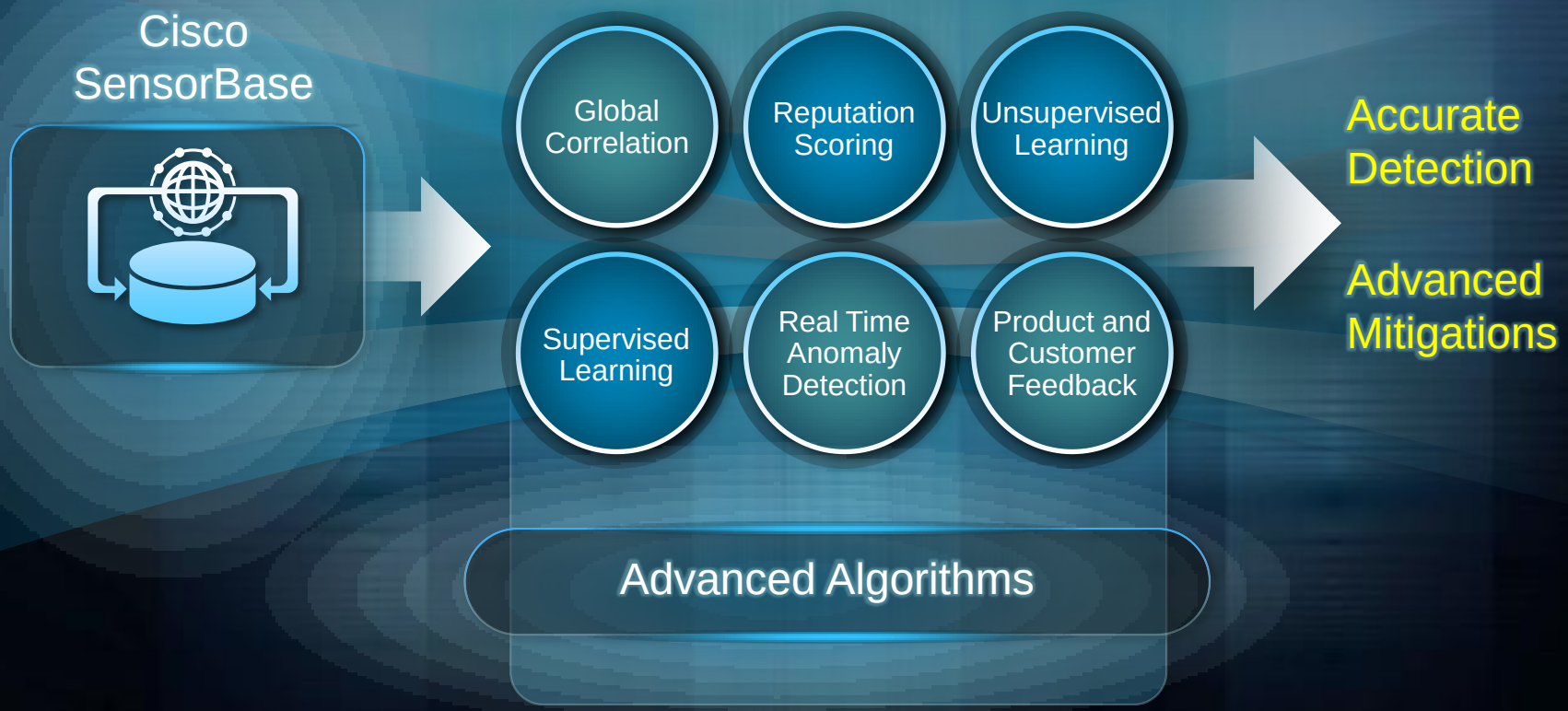

cisco
SIO
1 TB
DATA RECEIVED PER DAY
700,000+
GLOBALLY DEPLOYED DEVICES
5B
HTTP://
WEB REQUESTS
100M
EMAIL MESSAGES
35%
WORLDWIDE TRAFFIC
SensorBase
Threat Operations Center
Dynamic Updates

Unmatched Breadth

SensorBase | Threat Operations Center | Dynamic Updates


cisco
SIO
$100M
SPENT IN DYNAMIC RESEARCH AND DEVELOPMENT
24x7x365
OPERATIONS
500
ENGINEERS, TECHNICIANS AND RESEARCHERS
40+
LANGUAGES
80+
Ph.D.s, CCIE, CISSPs, MSCEs
SensorBase
Threat Operations Center
Dynamic Updates

수준 높은 분석 알고리즘


Cisco
SensorBase
Global Correlation
Reputation Scoring
Unsupervised Learning
Supervised Learning
Real Time Anomaly Detection
Product and Customer Feedback
Advanced Algorithms
Accurate Detection
Advanced Mitigations


cisco
SIO
40,000+
VULNERABILITIES TRACKED
3,300+
IPS SIGNATURES PRODUCED
500 GB
DATA PROCESSED per DAY
200
PARAMETERS TRACKED
8M
RULES per DAY
SensorBase
Threat Operations Center
Dynamic Updates

Powering Cisco Security Products and Services

Cisco SIO: 위협 식별, 분석 및 자동화된 방어

- 실시간 평판 점수
- 신규 또는 업데이트된 시그니처
- 검증된 룰에 대한 동적인 적용
- 매 5 분마다 자동 업데이트
- 최적화된 알람 매5분마다 자동 발생

Security Filters: Industry's Most Effective Security Features

- 제로데이 바이러스 출현 차단 필터
- 안티스팸
- 이메일 및 웹컨텐츠에 대한 평판기반 필터링
- IPS 시그니처 평판 기반 상황 상관관계 반영필터링
- 방화벽 봇넷 트래픽 필터링
- 업데이트된 모든 필터링 정보 경보

Cisco 제품과 서비스 : 사전 방어, 고성능 보장

ALERT SERVICES　SERVICE MODULES　WEB SECURITY　EMAIL SECURITY

HOSTED EMAIL SECURITY　INTRUSION PREVENTION　ADAPTIVE SECURITY

모든 상황을 반영하는 시스코의 보안 제품 업데이트

Cisco SecureX Architecture

SecureX Context Aware Enforcement

ASA 5585-X

FIREWALL

- **MultiScale™ 성능**

  ✓최대 35Gbps 방화벽 성능
  ✓최대 1,000만 동시 커넥션 수
  ✓최대 35만 초당 동시 커넥션 수

- **상황인식(Context Aware) 기반 보안 기능**

  ✓SIO에 의한 실시간 악성코드 유포지 및 봇넷 C&C 정보 반영
  ✓봇넷 트래픽 필터링 기능에 의한 자동/수동 차단

FIREWALL

ASA 5585-X

- **상황 인식 기반 방화벽 기능 로드맵**

2011

1H 2011

✓위치기반
✓사용자 및 디바이스 식별
✓TrustSec 연동

2H 2011

✓응용프로그램
✓컨텐츠
✓보안상태정보

ASA 5585-X

VPN

- **One Platform**

  ✓L2TP, IPSec 및 SSL VPN 기능 동시 지원
  ✓최대 10,000 개 세션 동시 연결
  ✓최대 5Gbps VPN 성능
  ✓Site-to-Site, Remote Access VPN

- **상황인식(Context Aware) 기반 보안 기능**

  ✓AnyConnect Telemetry 기능
  ✓AnyConnect VPN Client 에 의한 상황 정보 반영

ASA 5585-X

IPS

- **Real 10 Gbps 성능**

✓ASA 5585-X 용 모듈형 IPS
✓방화벽 기능과 IPS 기능 동시 지원
✓동시 지원시 최대 15Gbps 성능 지원

- **상황인식(Context Aware) 기반 보안 기능**

✓Global Correlation 기능
✓SIO에 의해 제공되는 실시간 상황 및 평판 정보 반영
✓실공격 및 위협도 조정

고성능 다기능 보안 어플라이언스 ASA5585-X 포트폴리오

- 4 Gbps Firewall
- 2 Gbps IPS
- 1 Gbps IPSec/SSL VPN
- 5000 IPSec/SSL VPN
- 1M F/W Concurrent
- 50,000 CPS

ASA 5585-S10P10

- 10 Gbps Firewall
- 5 Gbps IPS
- 2 Gbps IPSec/SSL VPN
- 10,000 IPSec/SSL VPN
- 2M F/W Concurrent
- 125,000 CPS

ASA 5585-S20P20

- 20 Gbps Firewall
- 10 Gbps IPS
- 3 Gbps IPSec/SSL VPN
- 10,000 IPSec/SSL VPN
- 4M F/W Concurrent
- 200,000 CPS

ASA 5585-S40P40

- **35 Gbps Firewall**
- **15 Gbps IPS**
- **5 Gbps IPSec/SSL VPN**
- **10,000 IPSec/SSL VPN**
- **10M F/W Concurrent**
- **350,000 CPS**

ASA 5585-S60P60

Securing Internet-Edge and Campus Networks

Scalable Data Center Solutions

Branch Office

Campus

Data Center

Performance, Scalability, Adaptivity

Enhancing the Customer Experience

IronPort C-Series

- **인바운드 이메일 보안 기능**
  - ✓평판 기반 이메일 필터링
  - ✓안티스팸 및 안티바이러스
  - ✓제로데이 바이러스 및 스팸 차단(VOF)
- **아웃바운드 이메일 보안 기능**
  - ✓암호화
  - ✓정보유출 방지 및 컨텐츠 필터링
- **상황인식 기반 보안 기능**
  - ✓SIO 에 의한 실시간 평판 점수 반영
  - ✓갑작스럽게 출현한 바이러스 및 스팸성 메일 볼륨 근원지 업데이트 및 차단

Email Security

IronPort S-Seires

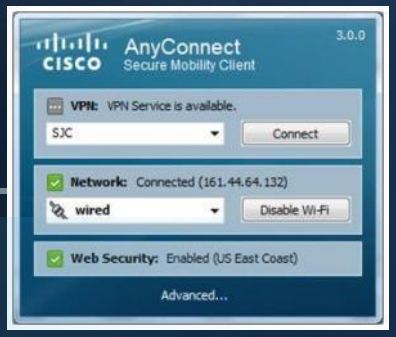
WWW

Web Security

- **웹 컨텐츠 보안 기능 for 사용자**
  - ✓카테고리 기반 URL 필터링
  - ✓웹컨텐츠 동적 분석을 통한 접근 통제(WUC)
  - ✓평판 기반 악성코드 유포사이트 접근 차단
  - ✓웹기반 어플리케이션 사용 통제
  - ✓정보 유출 방지

- **상황 인식 기반 보안 기능**
  - ✓SIO 에 의한 유해 사이트 평판 점수 실시간 업데이트
  - ✓악성코드 진화에 대한 정보 반영

AnyConnect Secure Mobility Client



- **AnyConnect 3.0 for PC**
  - ✓지원 운영체계
    - 윈도우즈 XP SP2 ,7, 비스타 (x86, x64)
    - 윈도우즈 모바일 5.0, 6.x (VPN 용)
    - 맥 OS X 10.5, 10.6.x
    - 리눅스 인텔 (2.6.x 커널)
  - ✓지원 기능
    - VPN Module : IPSec(IKE2포함)/SSL VPN
    - NAM Module : 802.1x, MACSec(802.1ae)
    - Web Module : WSA, ScanSafe
- **AnyConnect 2.4 for Mobile Device**
  - ✓지원 운영체계 :
    - iPhone 및 iPad 용 iOS 3.x/4.x 지원
    - Galaxy-S 및 S2 용 Android OS 2.3 지원
  - ✓지원 기능 : SSL VPN Client 기능 지원

Unified Secure Client

IronPort M-Seires

- **IronPort 제품군 중앙 관리 기능**
  - ✓다수의 IronPort C-Series 설정 및 정책 관리
  - ✓다수의 IronPort S-Series 리포팅 및 트랙킹 설정 관리

- **IronPort 제품군 중앙 모니터링 및 리포팅 기능**
  - ✓IronPort C,S-Series 보안 이벤트 모니터링
  - ✓사용량 통계
  - ✓사용패턴에 대한 분석 및 리포팅
  - ✓유사시 포렌식을 위한 상세 분석 및 추적기능

Management

Cisco Security Manager 4.1

Management

- **Cisco Network Security 제품군 중앙관리 기능**
  - ✓ISR, Switch, ASA 에 대한 설정 및 보안 정책 통합관리
  - ✓Work Flow 에 따른 역할별 권한 통제
  - ✓설정 변경 관리 및 감사 기능
  - ✓정책에 대한 유효성 및 중복 정책 분석

- **Cisco Network Security 제품군 중앙 모니터링 및 리포팅 기능**
  - ✓방화벽 및 IPS, VPN 로그 중앙 관리
  - ✓실시간 모니터링 및 정책연계 One-Stop-Prevention 기능
  - ✓다양한 통계 데이터에 대한 리포팅 기능
  - ✓실시간 통계 그래프 in-depth 분석 기능

Thank you.