# Peace of Mind with Secure Network Solutions

Marlon T. Ceniza

Network Consultant

Cisco Systems, Inc.

# Agenda

- Security issues and trends
- Self Defending Network Messaging
- Key security issues/solutions for the Campus environment
- Key opportunities (PCI, DLP, Trust, etc.)

# Factors That Impact Business Security

## Collaboration and Communication

- TelePresence / Video / IM / Email
- Mobility
- Web 2.0 / Web Services / SOA

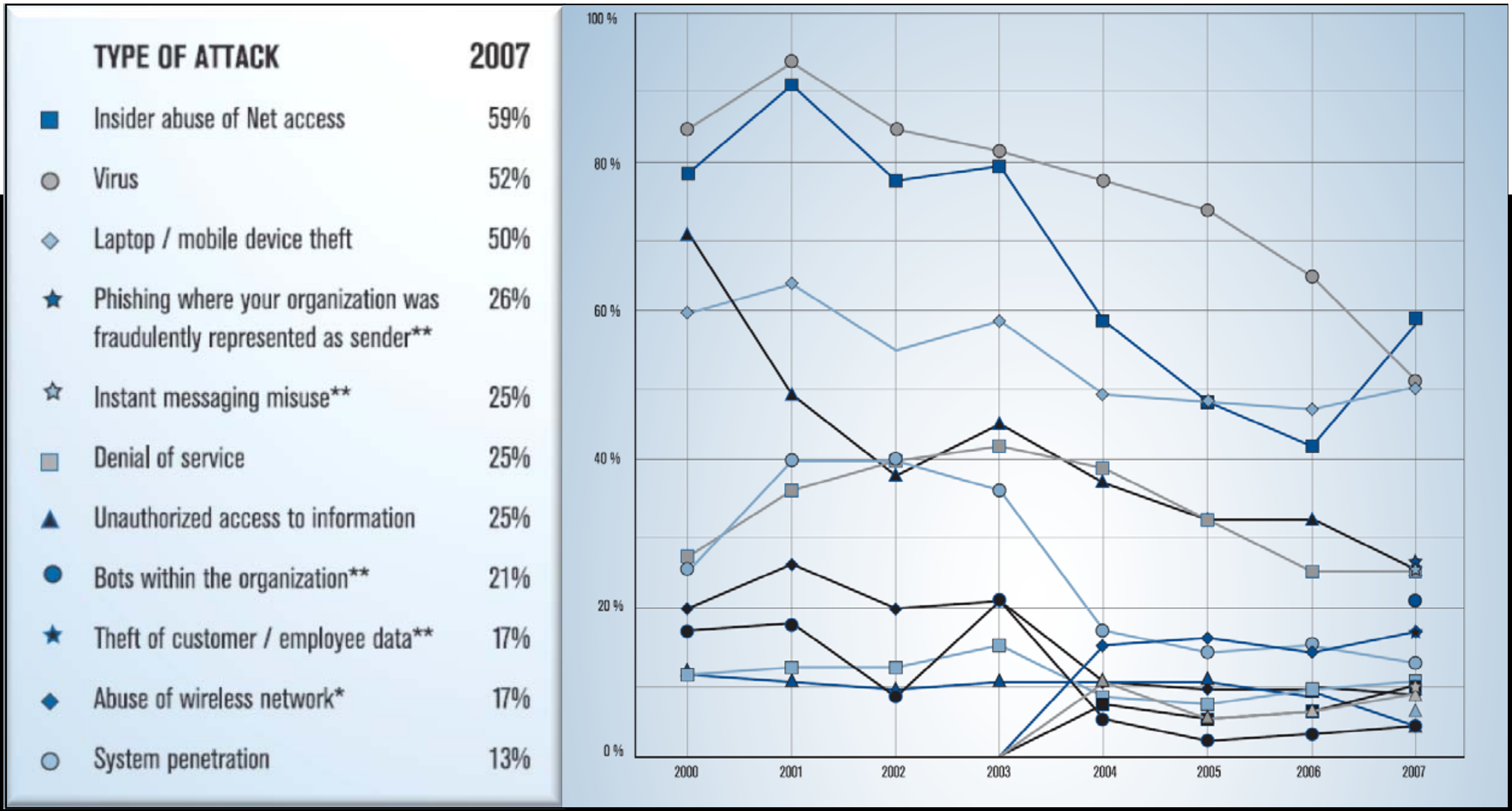
## The New Threat Environment

- The Eroding Perimeter
- Spam / Malware / Profit-Driven Hacking
- Data Loss and Theft

## The Business Impact of Security

- IT Risk Management
- Regulatory Compliance
- Security as Business Enabler

# The Evolving Security Challenge: Emergence of New Attack Types



| | TYPE OF ATTACK | 2007 |
|---|---|---|
| ■ | Insider abuse of Net access | 59% |
| ● | Virus | 52% |
| ◇ | Laptop / mobile device theft | 50% |
| ★ | Phishing where your organization was fraudulently represented as sender** | 26% |
| ☆ | Instant messaging misuse** | 25% |
| ■ | Denial of service | 25% |
| ▲ | Unauthorized access to information | 25% |
| ● | Bots within the organization** | 21% |
| ★ | Theft of customer / employee data** | 17% |
| ◆ | Abuse of wireless network* | 17% |
| ○ | System penetration | 13% |

# Vulnerability Sources

**Technical Vulnerability:**

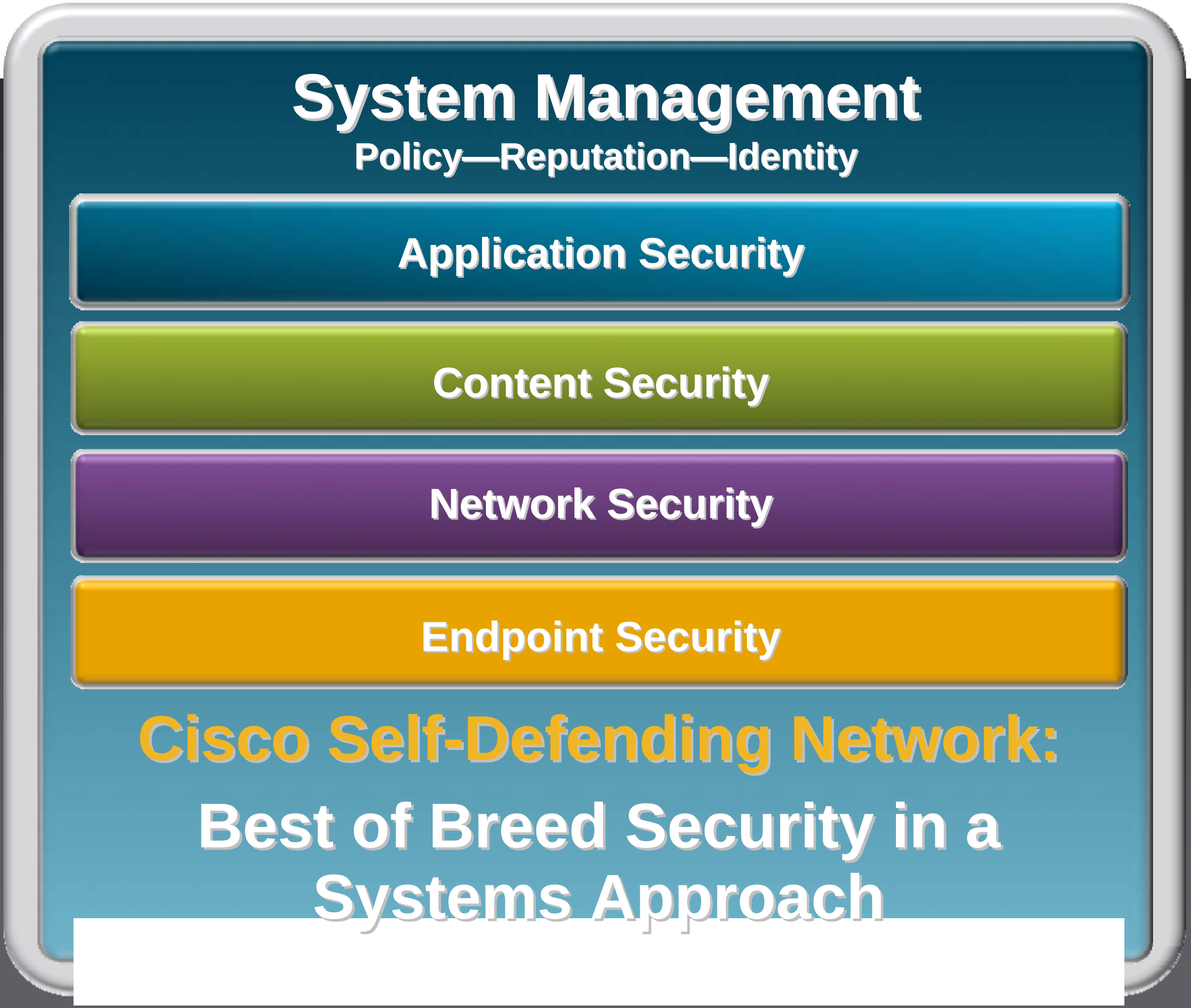
**A hardware, firmware, or software weakness or design deficiency that leaves a system open to potential exploitation, either externally or internally, resulting in the risk of compromise of information, alteration of information or denial of service**

**Administrative Vulnerability:**

**A security weakness caused by incorrect or inadequate implementation of a system's existing security features, lack of maintenance, lack of operational procedures, or failure to enforce policy and procedures.**

**Proactively Seek Out and Eliminate Administrative Vulnerabilities to Minimize Your Risk**

# Self-Defending Networks Relaunch



System Management

Policy—Reputation—Identity

Application Security

Content Security

Network Security

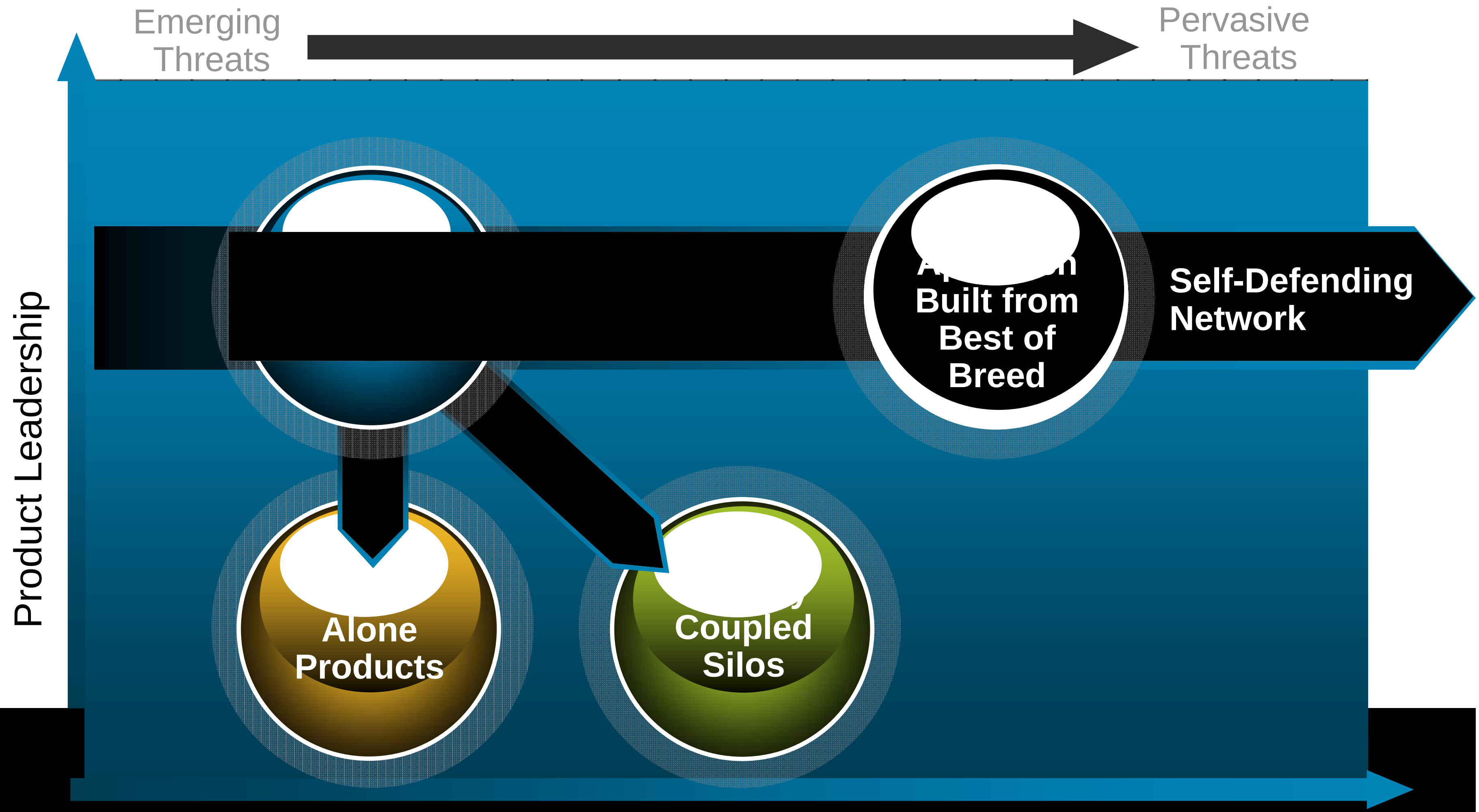
Endpoint Security

Cisco Self-Defending Network:

Best of Breed Security in a Systems Approach

- Enforce business policies and protect critical assets
- Decrease IT administrative burden and reduce TCO
- Reduce security and compliance IT risk

# Systems Approach Built from a Leadership Product Portfolio



# The Portfolio at a Glance…
## Network and Endpoint Security

### Network Security

- Integrate security pervasively into the network
- Converged services for fewer touch points
- Scale performance and services to meet any deployment needs

### Product Highlights:

- Adaptive Security Appliance
- Integrated Services Router
- Aggregation Services Router
- Cisco Switch Security Modules

### Endpoint Security

- Rich NAC and identity services
- Endpoint protection and control—host-based IPS and AV

### Product Highlights:

- CSA Desktop
- CSA Server
- NAC Appliance

# The Portfolio at a Glance…

## Content and Application Security

### Content Security

- Reputation based, zero-day defense
- Capability to address diverse attacks types and techniques
- Secure all sources of attack

### Product Highlights:

IronPort Email

IronPort Web

Intrusion Prevention Systems

### Application Security

- Layer 7 protection for application and data vulnerabilities
- XML traffic validation and inspection
- Enhanced deep packet inspection

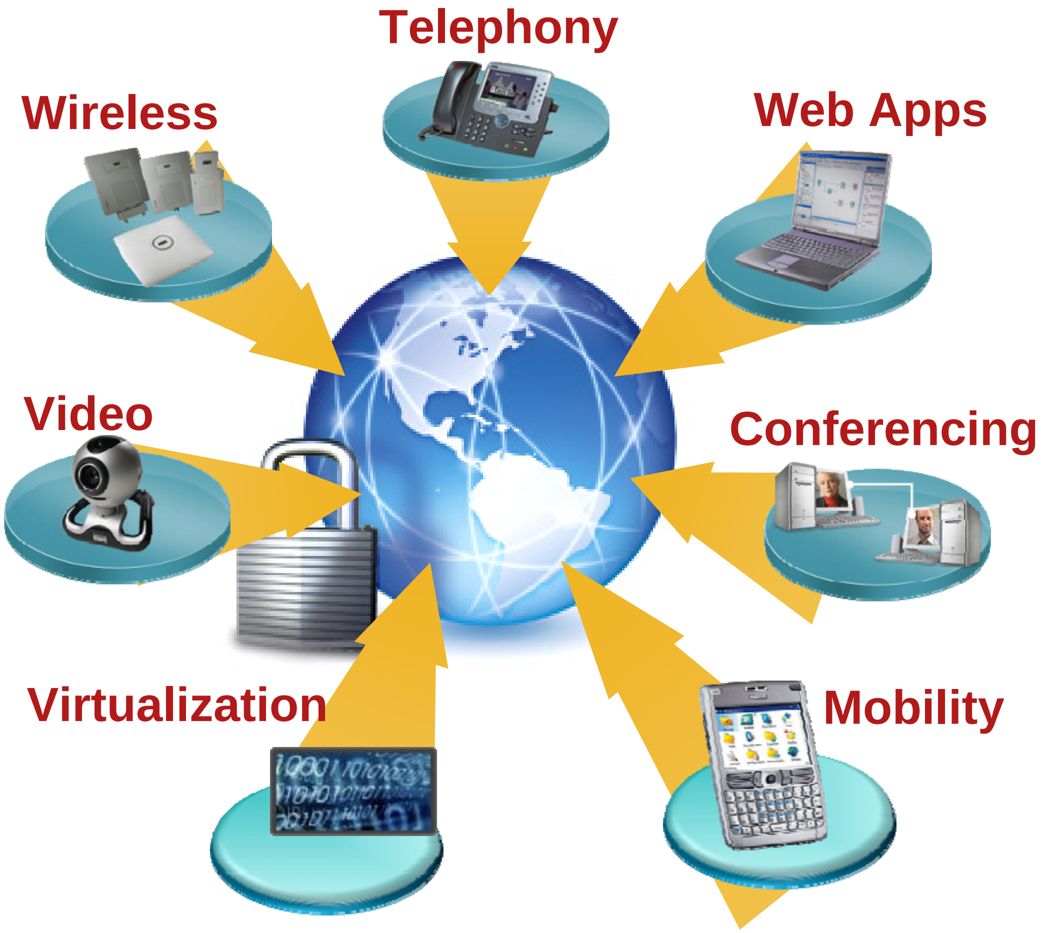
### Product Highlights:

ACE XML Gateway

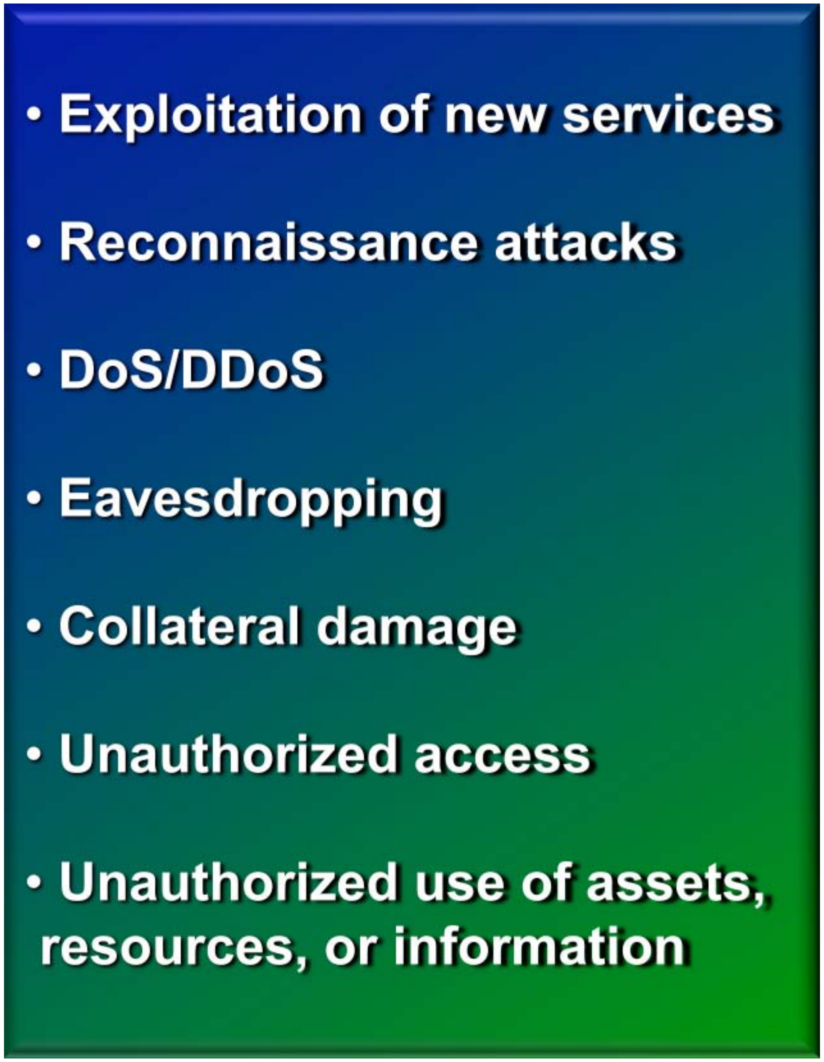
Web Application Firewall

# Campus Network Trends

- Transition to a mobile environment
- Integration of services
  - Video
  - Web Conferencing
  - Telepresence
  - Unified Communications
- Virtualization
- Operational Savings
- Compliance



# Campus Complexity Increases Risk

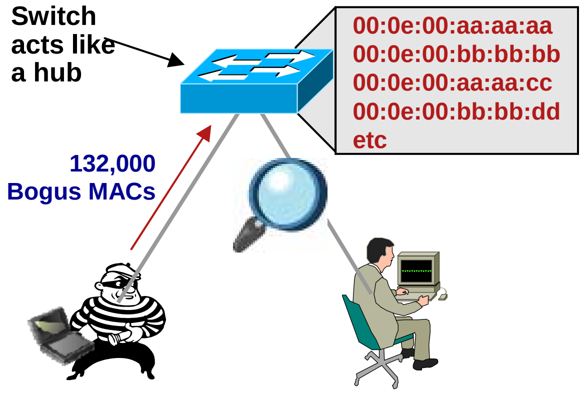


- Exploitation of new services
- Reconnaissance attacks
- DoS/DDoS
- Eavesdropping
- Collateral damage
- Unauthorized access
- Unauthorized use of assets, resources, or information

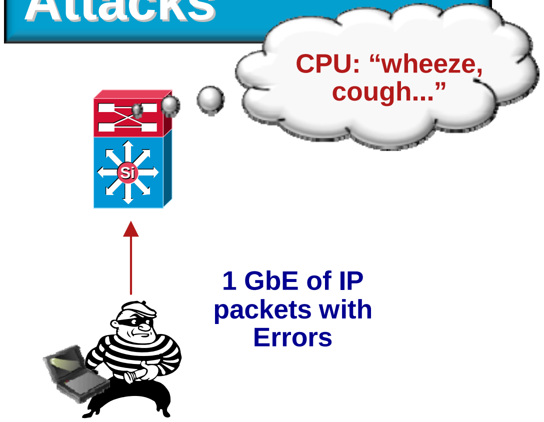
Protecting the Campus requires combining switching fabric tools with external monitoring, prevention, and intervention

# Campus Security Threats

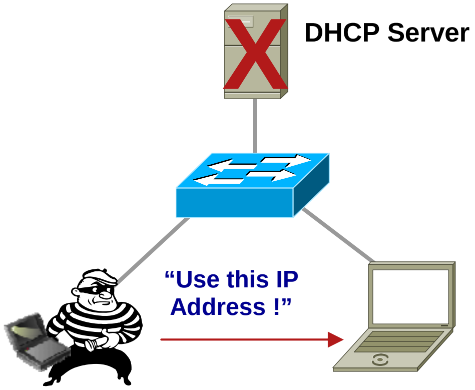
## MAC Flooding Attacks



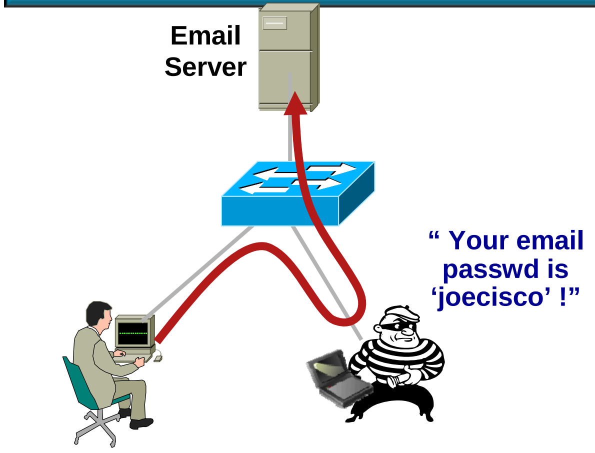
## Network Element Attacks



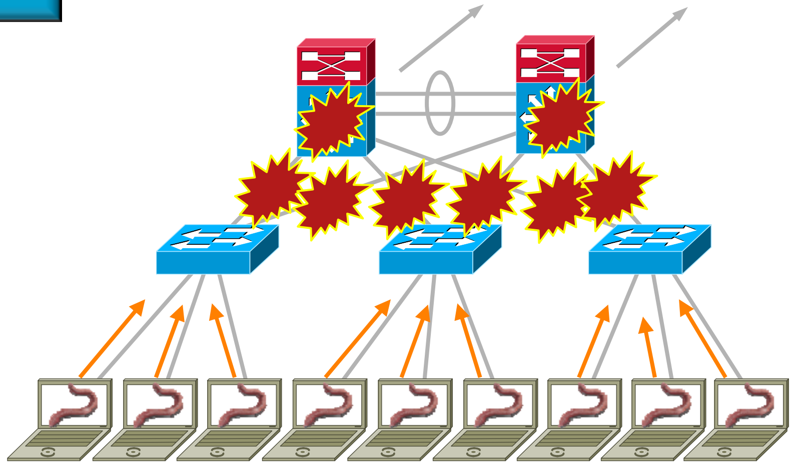
## DHCP Vulnerabilities



## Man-in-the-Middle Attacks

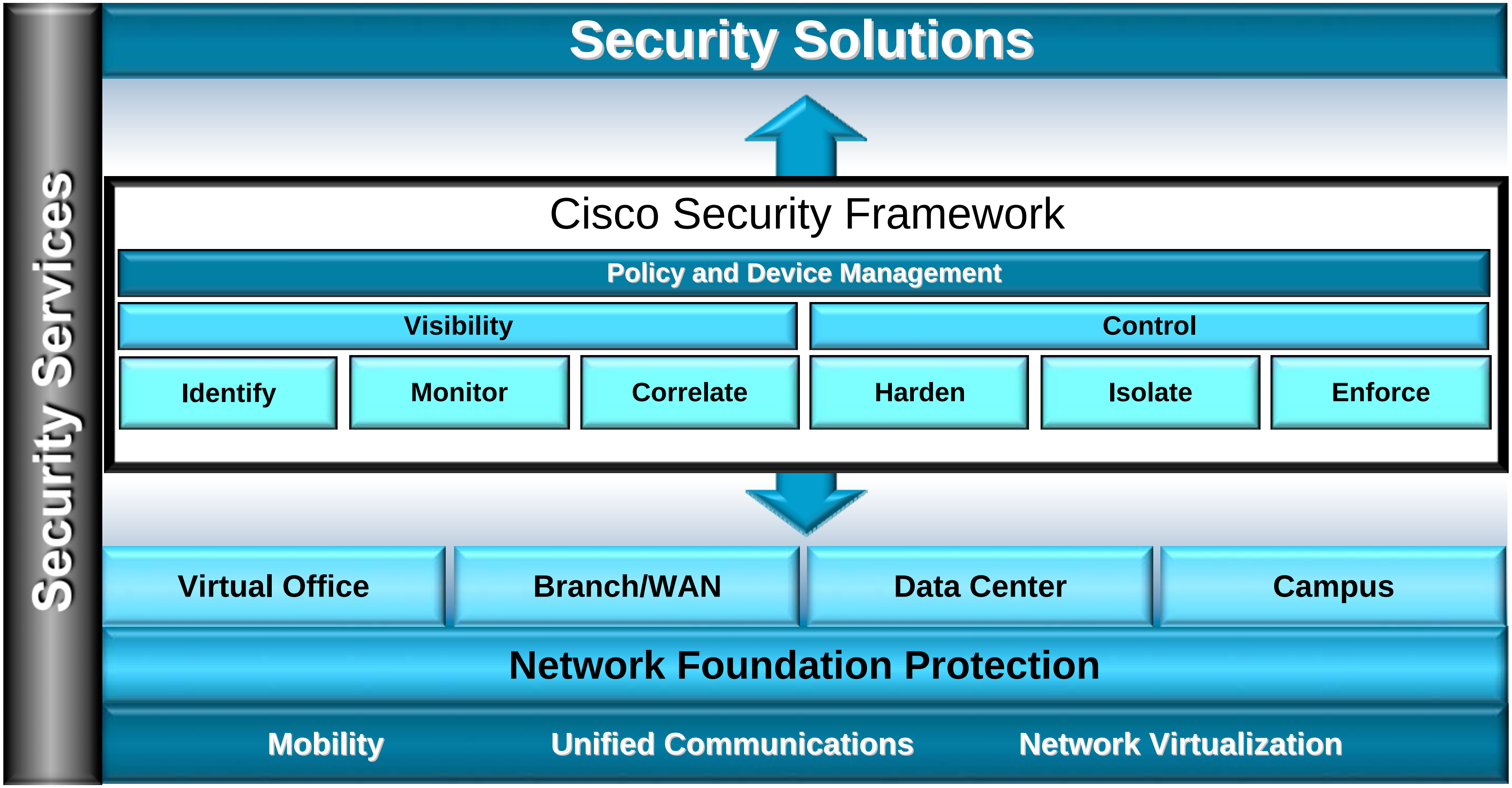


## Worms and Viruses



High volume of Worm-generated traffic can block links and overrun switch CPUs

# Common Cisco Security Framework



Security Services

Security Solutions

Cisco Security Framework

Policy and Device Management

Visibility

Control

Identify

Monitor

Correlate

Harden

Isolate

Enforce

Virtual Office

Branch/WAN

Data Center

Campus

Network Foundation Protection

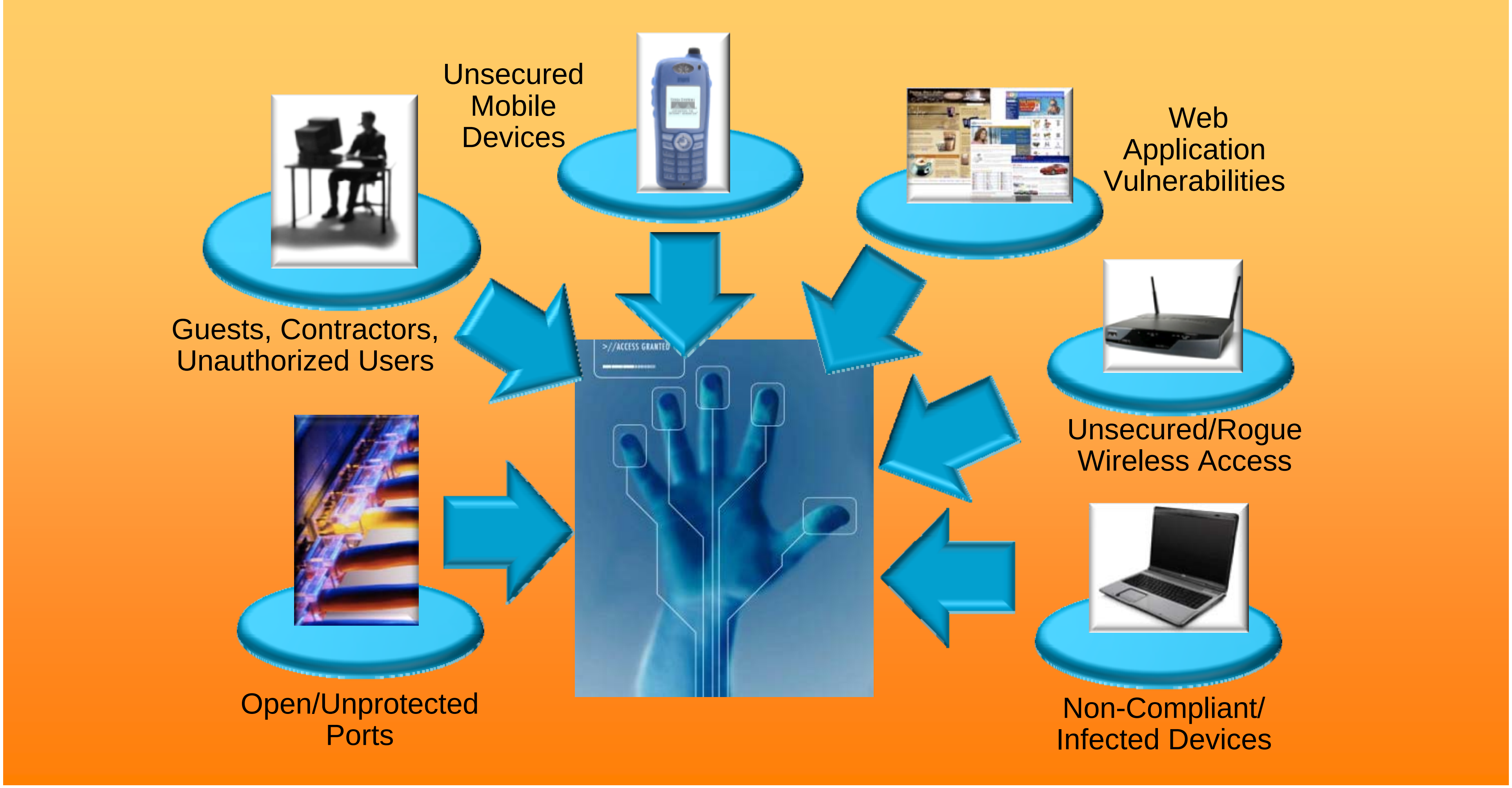
Mobility

Unified Communications

Network Virtualization

# Controlling Campus Access

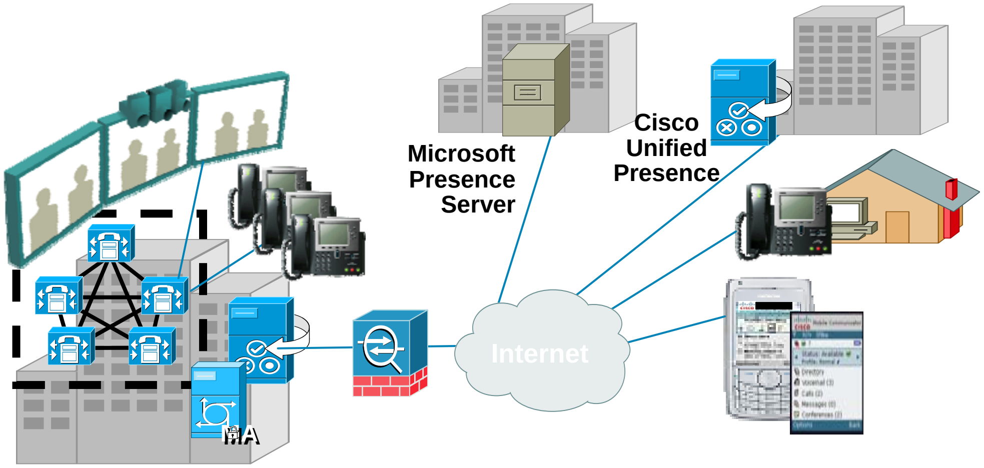
Security enables new work and collaboration solutions by controlling and protecting endpoints and access to the Campus network


Unsecured Mobile Devices
Web Application Vulnerabilities
Guests, Contractors, Unauthorized Users
>//ACCESS GRANTED
Unsecured/Rogue Wireless Access
Open/Unprotected Ports
Non-Compliant/ Infected Devices

# Cisco ASA Enhances Campus UC Security

**Cisco Adaptive Security Appliance (ASA) 8.0(4) provides a single support architecture for simplifying and securing the deployment of softphones, remote phones, clients, and presence architectures**

- Secures communications between Cisco and Microsoft presence servers for efficient collaboration between organizations
- Secures Softphone connections between data and phone networks
- Simplifies and secures deployment of remote IP phones without additional VPN devices, negotiates between encrypted and unencrypted phone connections
- Secures traffic between Cisco Unified Mobile Communicator software and Cisco Unified Mobility Advantage server
- New IPS signatures inspect inbound traffic to stop known attacks against UC call-control and application servers



# Botnets - The #1 Online Security Threat

Wikipedia on Botnets: . . . a collection of compromised computers (called zombies or bots) running programs, usually referred to as worms, Trojan horses, or backdoors, under a common command and control infrastructure

**Botnets are the prime enablers of:**

- DDoS
- Extortion
- Advertising click-through fraud
- Fraudulent sales
- Identity theft and financial fraud (phishing, stealing info from PCs, etc.)
- Theft of goods/services
- Espionage/theft of information
- Spam-based stock-market manipulation

# Campus Endpoint Security

- Campus security architecture should include endpoints
- Implement Cisco Security Agent (CSA) on corporate controlled assets
- Deploy NAC and IBNS client software on the endpoints that participate with the rest of the integrated network security elements.

# Cisco Security Agent 6.0
## Enhanced Endpoint Protection

CSA
Data Loss Prevention
Attack Prevention
Policy
ation
Network

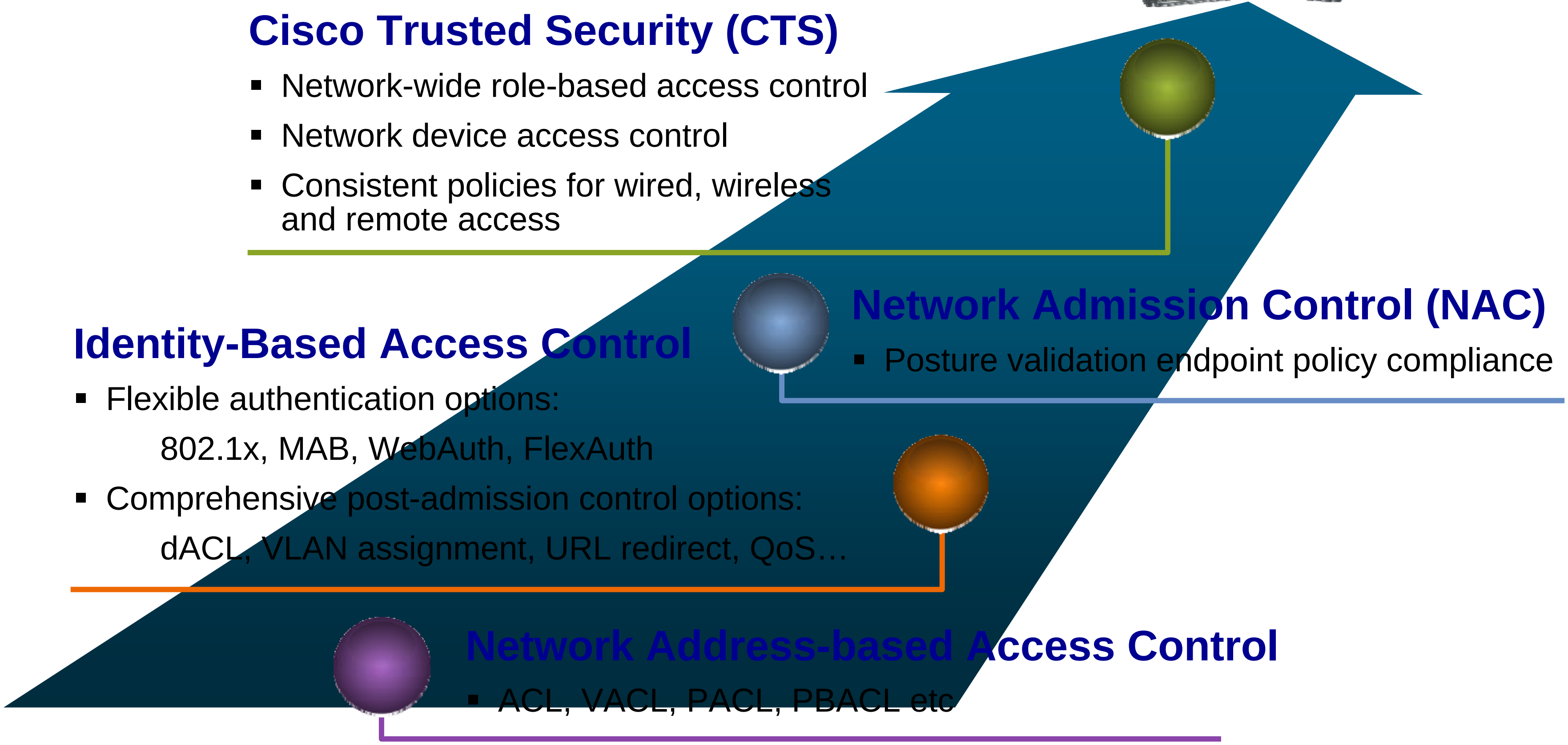
**Innovation:**

- Data-loss prevention protects against customer private data and intellectual property being improperly accessed or removed from laptops and desktops.
- Improved usability allows for seamless protection with minimal end-user involvement
- Integrated antivirus with no yearly subscription cost

> "The new CSA 6.0 solution is brilliant."
>
> –*Andreas Antonoupolos, Nemertes Research.*

# Evolution of Network Access Control

## Topology Aware to Role Aware



### Cisco Trusted Security (CTS)

- Network-wide role-based access control
- Network device access control
- Consistent policies for wired, wireless and remote access

### Network Admission Control (NAC)

- Posture validation endpoint policy compliance

### Identity-Based Access Control

- Flexible authentication options:

  802.1x, MAB, WebAuth, FlexAuth
- Comprehensive post-admission control options:

  dACL, VLAN assignment, URL redirect, QoS…

### Network Address-based Access Control

- ACL, VACL, PACL, PBACL etc

# Securing the Campus Infrastructure

Securing the Campus Network is critical to maintaining the resiliency and performance of the network and business-critical applications and services

## Focused Attacks

- Intercept data
- Disrupt business critical applications
- Impact availability and productivity

## Denial of Service

- Overwhelm bandwidth
- Impact operations and productivity

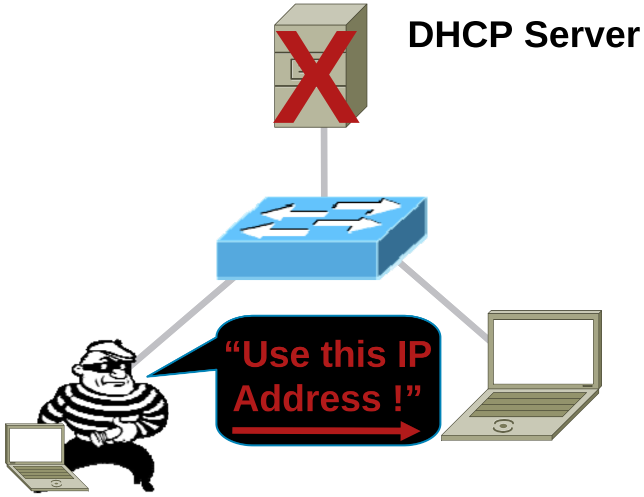
## Malware

- Impact performance
- Collateral damage
- Recovery costs and downtime

# Protect Campus Network Devices

- Implement security policy and audit
- Cisco IOS AutoSecure
- Authenticate network devices
  - MAC/IP addresses, CTS Secure Group Tags
- Manage bandwidth consumption
- Monitor network traffic
- Enable port security
  - MAC flooding, DHCP starvation, and Spanning Tree Loop Attacks
- Enable DHCP snooping
  - Rogue DHCP server attacks
- Enable IP Spoof Guard
  - Prevent IP/MAC Spoofing, TCP/UDP splicing, and DoS attacks
- Segment traffic with VLANs
  - Segment traffic based on type, user, group, etc.

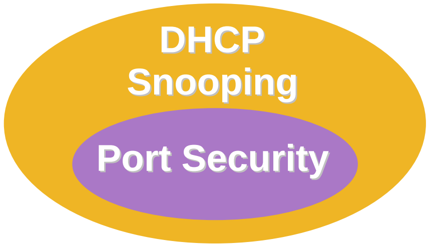
# Implement Cat6K Integrated Security



Port Security

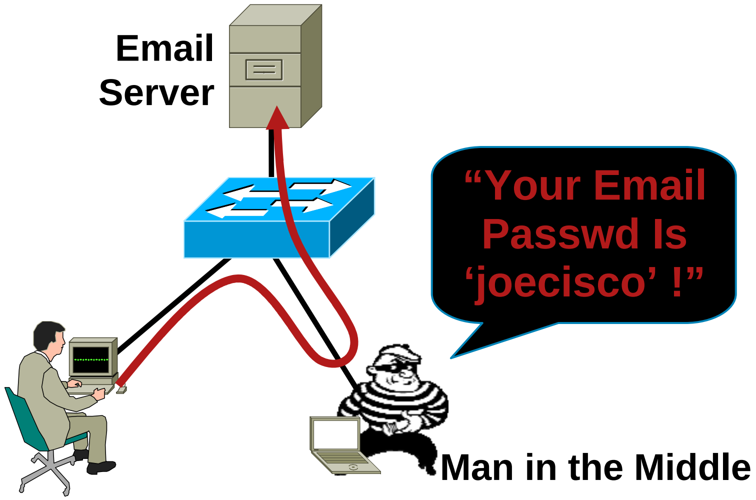
- **Port Security** prevents MAC flooding attacks, DHCP Starvation
  attacks and spanning tree loop mitigation

# Implement Cat6K Integrated Security



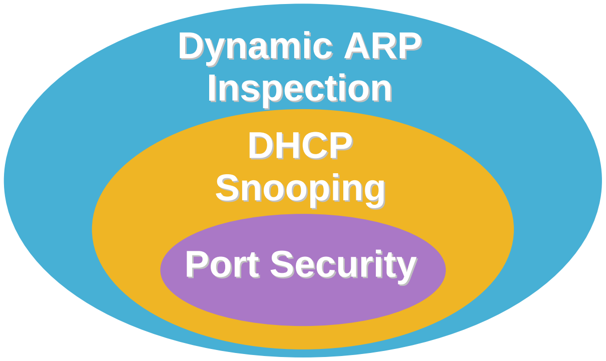
DHCP Snooping

Port Security



- **Port Security** prevents MAC flooding attacks, DHCP Starvation
  attacks and spanning tree loop mitigation
- **DHCP Snooping** prevents Rogue DHCP Server attacks

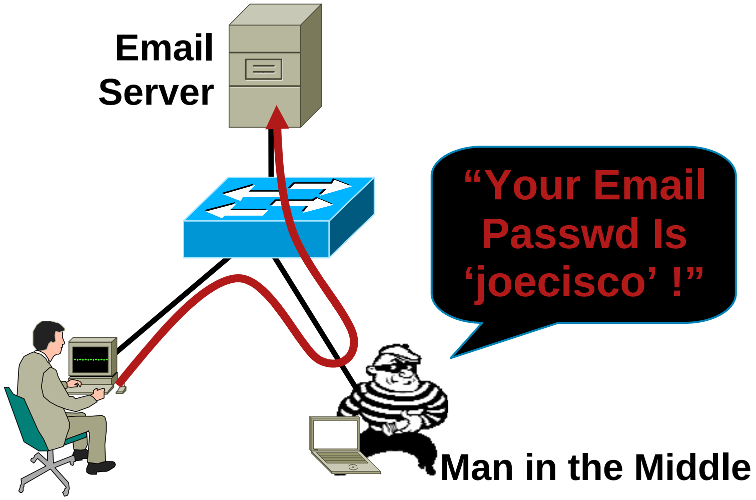
# Implement Cat6K Integrated Security



Dynamic ARP Inspection

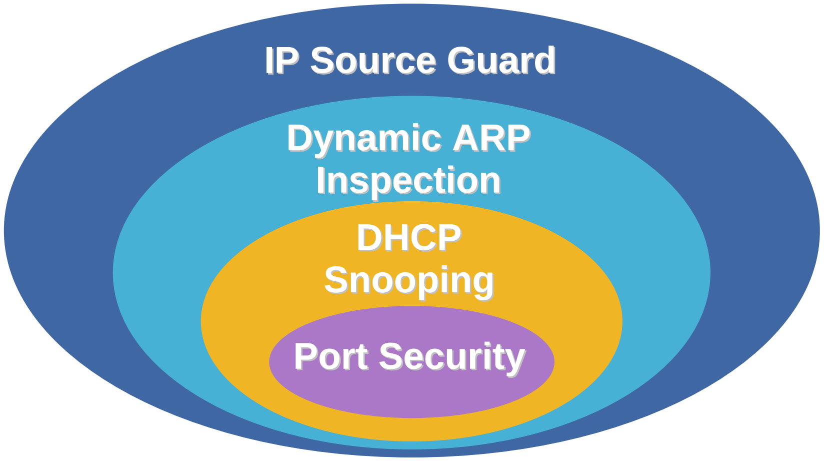
DHCP Snooping

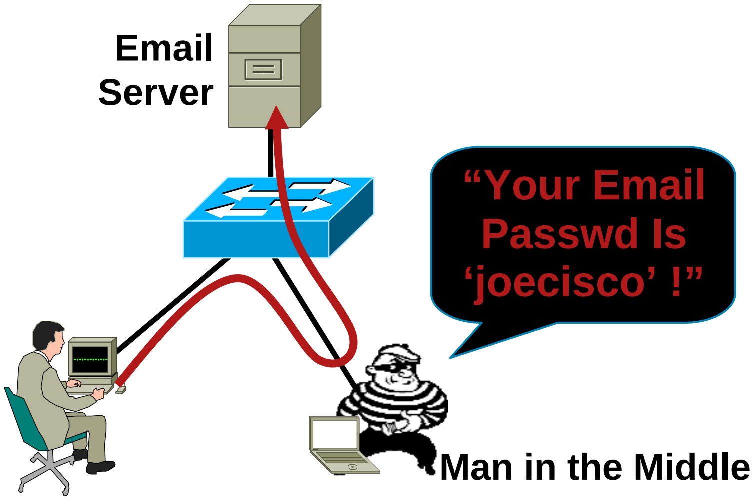
Port Security



- **Port Security** prevents MAC flooding attacks, DHCP Starvation
  attacks and spanning tree loop mitigation
- **DHCP Snooping** prevents Rogue DHCP Server attacks
- **Dynamic ARP Inspection** prevents current ARP attacks

# Implement Cat6K Integrated Security

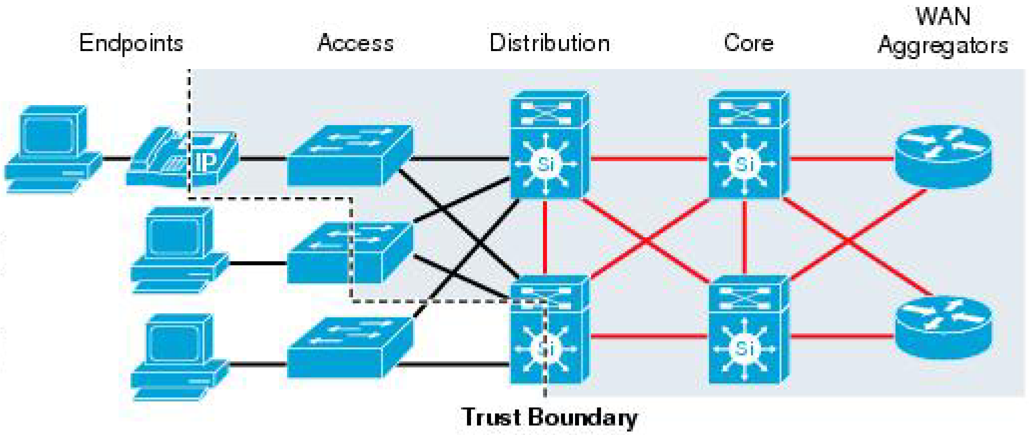




- **Port Security** prevents MAC flooding attacks, DHCP Starvation attacks and spanning tree loop mitigation
- **DHCP Snooping** prevents Rogue DHCP Server attacks
- **Dynamic ARP Inspection** prevents current ARP attacks
- **IP Source Guard** prevents IP/MAC Spoofing and a wide variety of TCP/UDP splicing and DoS attacks

# Establish a QoS Trust Boundary

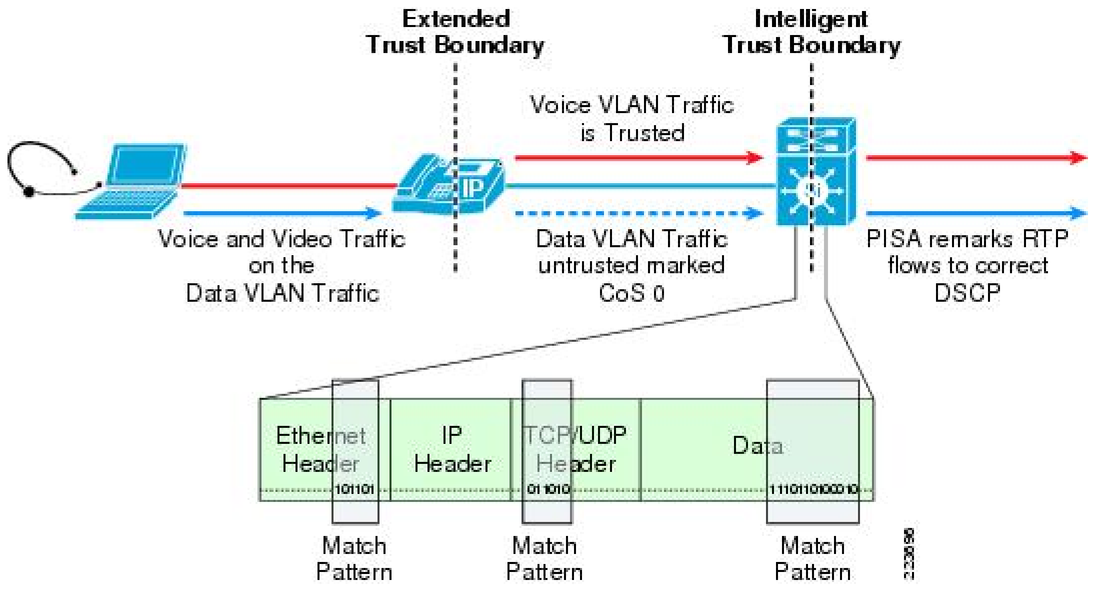
1. **Classify and mark applications as close to their sources as technically and administratively feasible.**
2. **Police unwanted traffic flows as close to their sources as possible. Especially important for DoS or worm attacks.**
3. **Where possible, perform QoS in hardware rather than software**



Areas outside of the QoS trust boundary will require additional mechanisms, such as the Cisco DDoS Guard, to be deployed to address the problems of link saturation by malicious attacks.

# Trust Boundary for Complex Applications

- **Complex applications using the same port**
- **Detecting applications hijacking other applications**
  - **Use Deep Packet Inspection (DPI) to determine what type of traffic the packet contains**
  - **Use NBAR to examine the RTP header to determine if a UDP flow is truly an RTP stream or some other application-based stream**



# Protect the Control Plane

- Implement MD5-based authentication
- Disable any control protocol not specifically required
- Implement modular design:
  - Limit baseline control plane and CPU load
  - Provide control plane isolation between modules in event of failure
- Reduce the probability of flooding
  - Reduce the scope of the Layer-2 topology
  - Harden spanning tree design with spanning tree toolkit
- Leverage CPU protection mechanisms and Control Plane Protection (CoPP):
  - Limit and prioritize traffic forwarded to each switch CPU

# Infrastructure Telemetry and Monitoring

*NetFlow* — Provides the ability to track each data flow that appears in the network

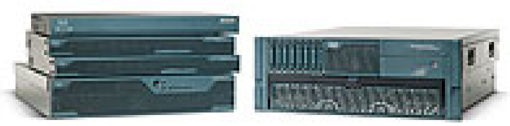
*Hardware DPI (NBAR)* — Provides the ability to detect undesirable application traffic flows at the network access layer and allow for selected control (drop or police) of undesirable traffic

*Syslog* — Provides the ability to track system events

*IPS* — Insertion at key choke points provides an additional level of observation and mitigation capability

*Cisco MARS* — Provides a consolidated view of gathered data to allow for a more accurate overall view of any security outbreaks

# Cisco Intrusion Prevention Systems 6.1
## Tailored to the needs of SMBs



**Innovation:**

- Dramatically simplified IPS management on ASA
- IPS Manager Express (IME): new, all-in-one application for IPS provisioning, monitoring, and reporting
- New ASA 5500 IPS Module delivers up to 650 Mbps
- Comprehensive Unified Communications protection

> "The Cisco IPS 4200 Series appliances and modules are threatening to competitors, because the product is positioned as a key component of the Cisco Self-Defending Network, offered in the form of appliances and devices as well as service modules for routers and switches…..Perhaps more threatening to competitors is the fact that Cisco makes IPS available on many levels."
>
> *–Current Analysis IPS 6.0 Product Assessment, April 2, 2008, Analyst Charlotte Dunlap*

# Cisco Security MARS 6.0

## Real-time security operations visibility

**Innovation:**

- Standard code base for all platforms
- Wireless controller support
- Expanded device support
- Open schema for accelerated device support
- Integration with Trend Damage Cleanup Service

> “The Cisco Security MARS solution connects the dots and provides us with an easy-to-read dashboard that allows us to streamline the management of our entire security system. This helps ensure operational efficiency and business continuity."
>
> *–Phil Swift, CIO, Esurance*

# Systems Approach to Stop Malware: Visibility and Control

## Firewall and VPN

- Traffic access control
- Encryption

## Intrusion Prevention

- Detection
- Precision response

## Content Security

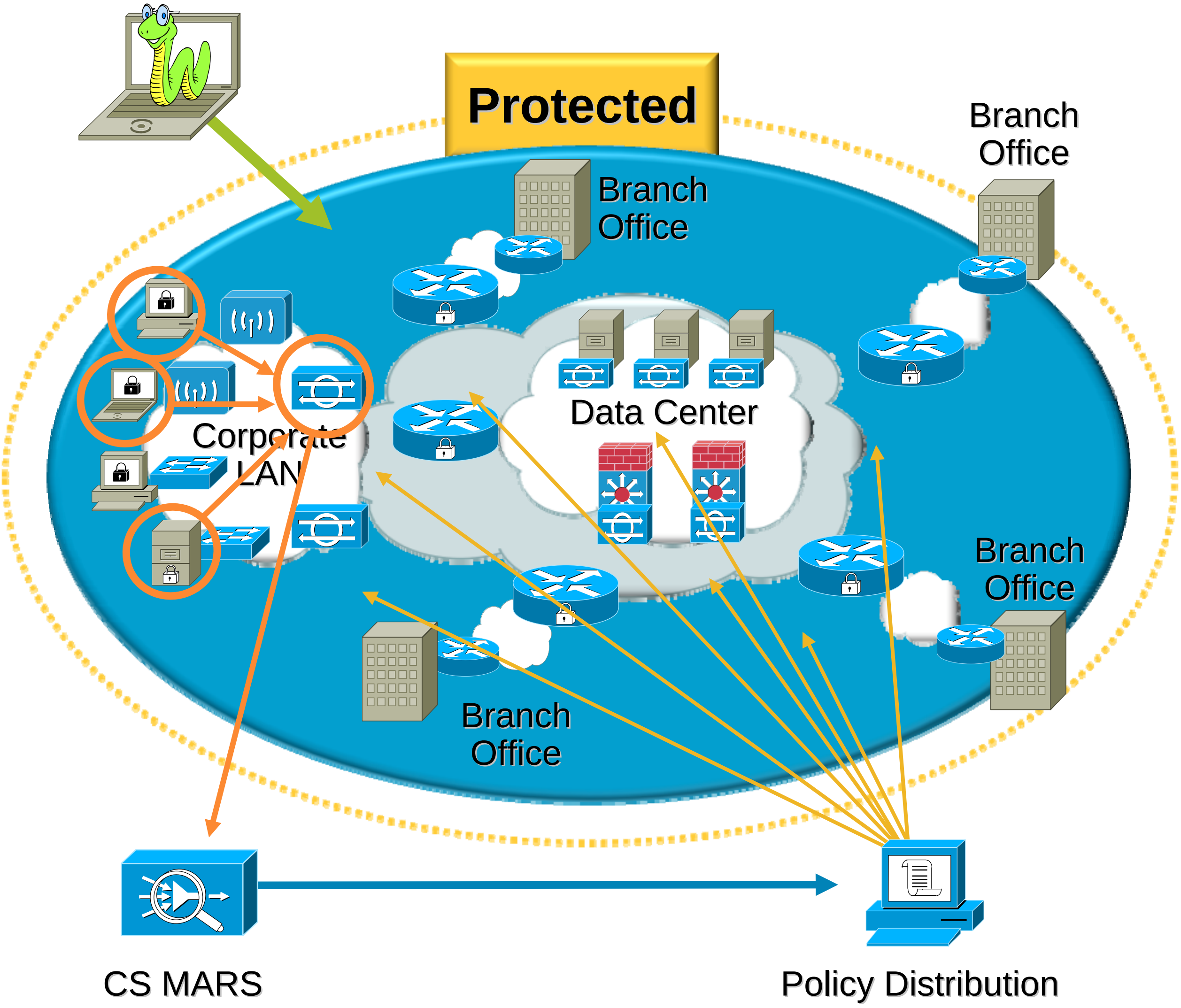
- Email Spam
- Web filtering

## Endpoint Security

- Host IPS
- AV solutions

**Centralized Policy Management and Monitoring**

# An Integrated Solution to Stop Malware:
## IPS, CSA, MARS, and CSM



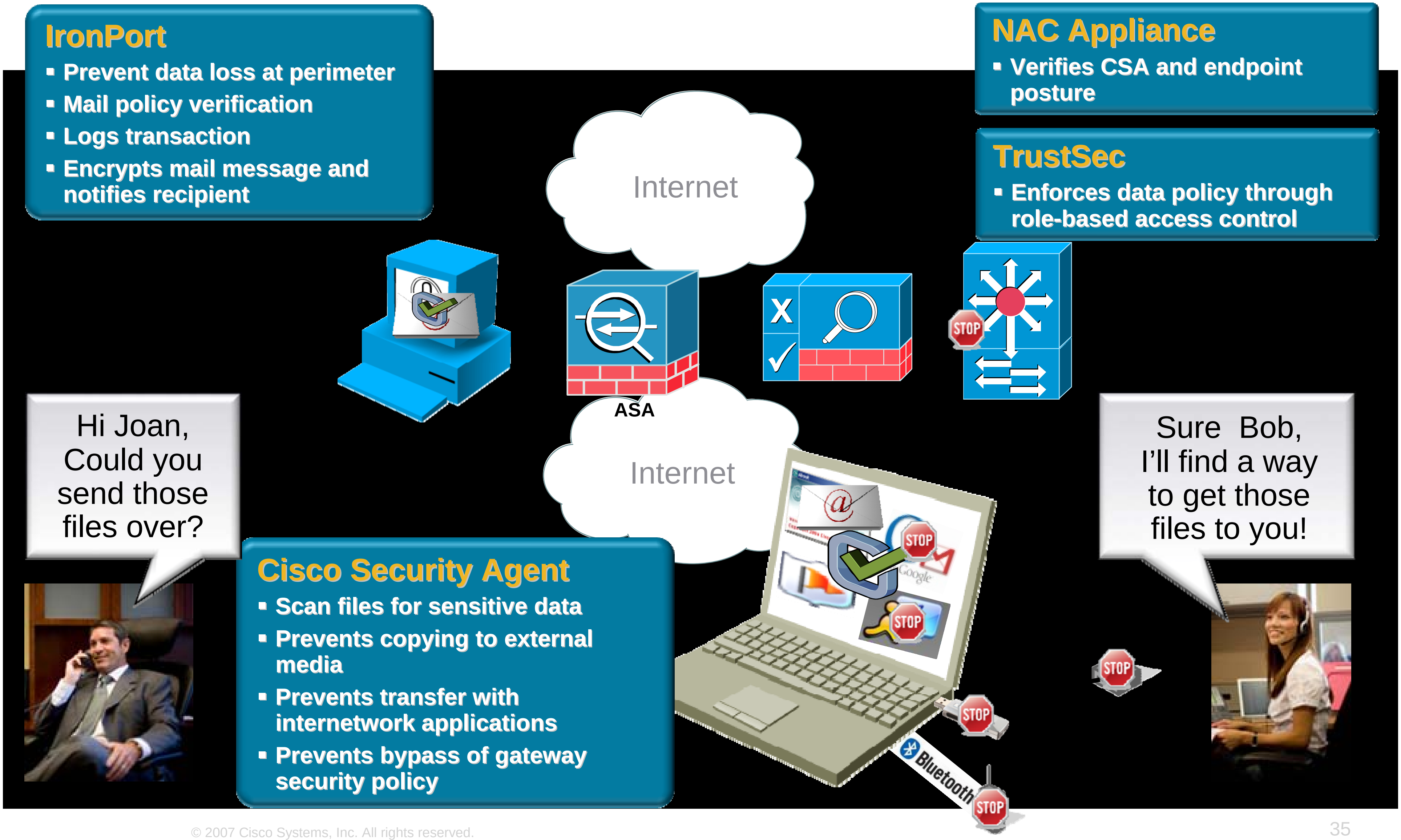
- Attacker attempts to gain access
- IPS detects the event with data inputs from CSA
- MARS receives the information and correlates the incident
- IPS signature policy is updated in one place
- Single deployment for consistent network protection

# Data Loss Prevention (DLP)
## Bypassing Traditional Security Measures

- DLP: Security measures to protect company’s data-in-use, data-in-motion and data-at-rest
- Data loss through “approved” ports (email and web)
- Computing resource theft
  - Laptops
  - Portable connected equipment
  - Data Center resources

# Cisco Data Loss Prevention Solution

## NAC, CSA, IronPort, and TrustSec



### IronPort

- Prevent data loss at perimeter
- Mail policy verification
- Logs transaction
- Encrypts mail message and notifies recipient

### NAC Appliance

- Verifies CSA and endpoint posture

### TrustSec

- Enforces data policy through role-based access control

Hi Joan, Could you send those files over?

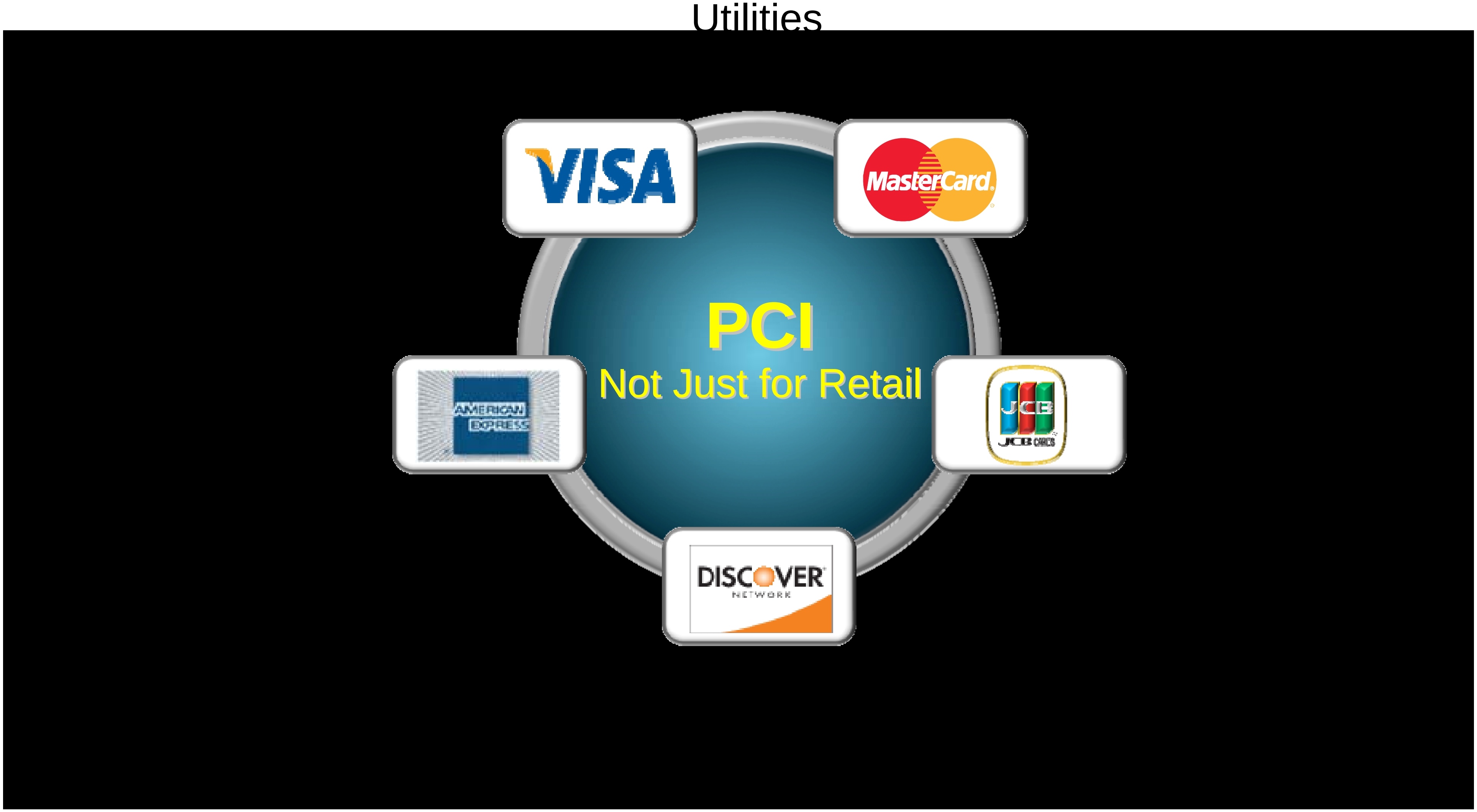
Sure Bob, I'll find a way to get those files to you!

### Cisco Security Agent

- Scan files for sensitive data
- Prevents copying to external media
- Prevents transfer with internetwork applications
- Prevents bypass of gateway security policy

# PCI Applies to Nearly Every Industry

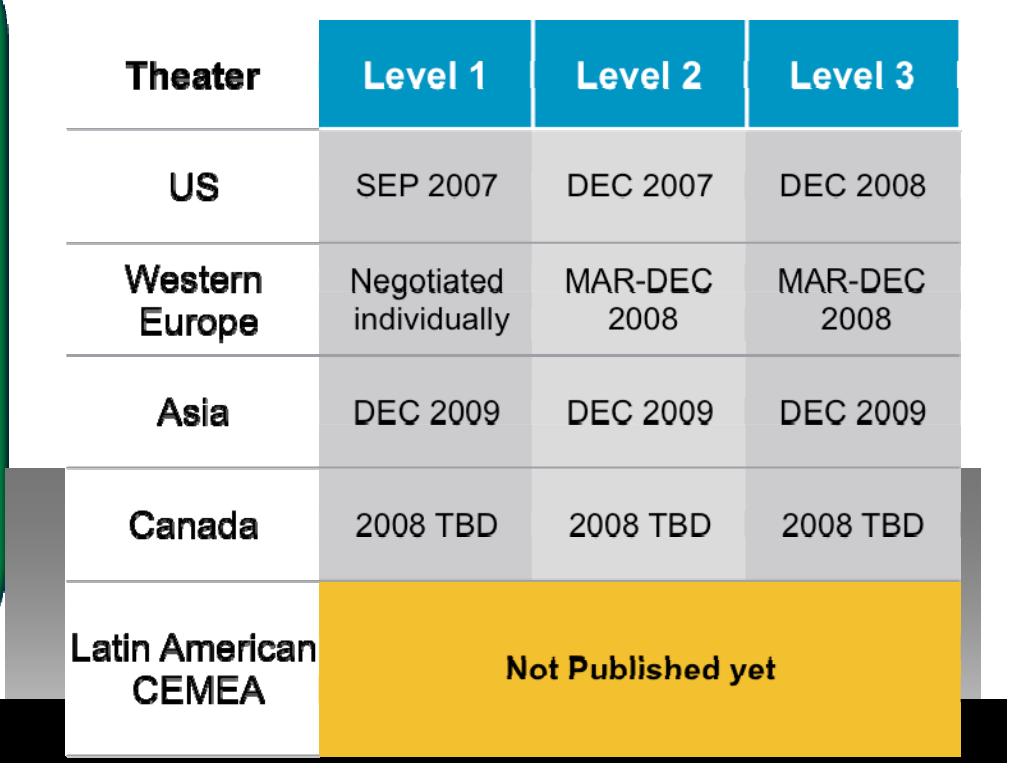
Utilities



# The Payment Card Industry (PCI)

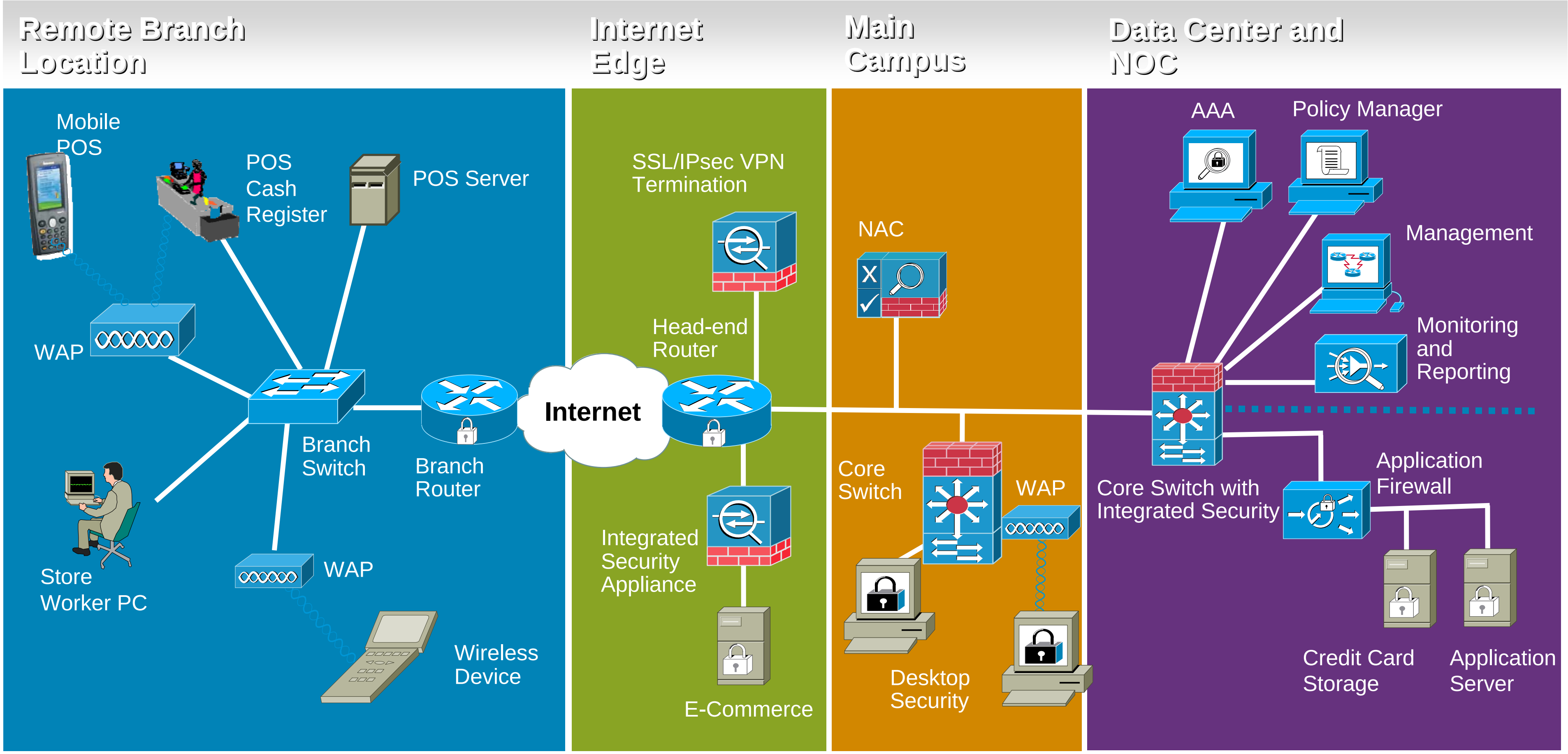
## Data Security Standard

- Published January 2005
- Impacts ALL who process, transmit, or store cardholder data
- Also applies to 3rd-party hosting companies, information storage companies, etc.
- Monthly fines ranging from $5,000 to $50,000 for missed deadlines
- Has global reach



| Theater | Level 1 | Level 2 | Level 3 |
|---|---|---|---|
| US | SEP 2007 | DEC 2007 | DEC 2008 |
| Western Europe | Negotiated individually | MAR-DEC 2008 | MAR-DEC 2008 |
| Asia | DEC 2009 | DEC 2009 | DEC 2009 |
| Canada | 2008 TBD | 2008 TBD | 2008 TBD |
| Latin American CEMEA | Not Published yet | | |

# Cisco Security Portfolio—Offers End-to-End Compliance with PCI Requirements



**Confidentiality, Data Integrity, Availability, Auditing, and Reporting**

# The Business Case for Identity Networking

- **Rich and pervasive identity services**

  Policy, protection, management, reporting

  Guest access, device profiling, flex authentication, enforcement

- **End-to-end policy framework**

  Tightly integrated with authentication and authorization

- **Service mobility**

  Policy decision implemented at resource point

  Access is based on user identity,

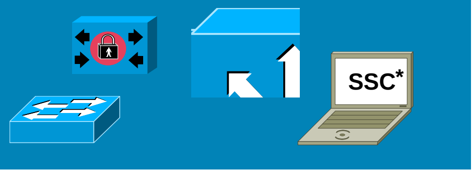
[redacted]

# Identity + NAC + TrustSec

## Pre and Post Admission Network Services

### Identity Infrastructure

- User and device authentication
- Control network access (L2 and L3)
- Device mobility in the network



* Cisco Secure Services Client

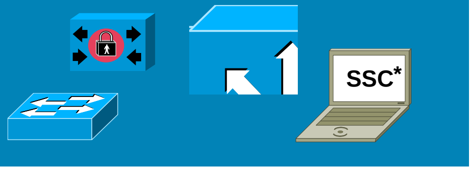
+ NAC + TrustSec

# Identity + NAC + TrustSec

## Pre and Post Admission Network Services

### Identity Infrastructure

- User and device authentication
- Control network access (L2 and L3)
- Device mobility in the network



* Cisco Secure Services Client

+

### Profiling Services

- Device profiling
- Behavioral monitoring
- Device reporting

### Guest Services

- Guest and sponsor portals
- Role-based AUP
- Provisioning and reporting

### Posture Services

- Managed device posture
- Unmanaged device scanning
- Remediation

+

## TrustSec

# Identity + NAC + TrustSec

## Pre and Post Admission Network Services

### Identity Infrastructure

- User and device authentication
- Control network access (L2 and L3)
- Device mobility in the network

SSC*

* Cisco Secure Services Client

+

### Profiling Services

NAC

- Device profiling
- Behavioral monitoring
- Device reporting

### Guest Services

- Guest and sponsor portals
- Role-based AUP
- Provisioning and reporting

### Posture Services

Clean Access Agent

- Managed device posture
- Unmanaged device scanning
- Remediation

+

### Role-Based Access Control

- Network topology-independent
- Scalability via tagging

### Data Integrity and Confidentiality

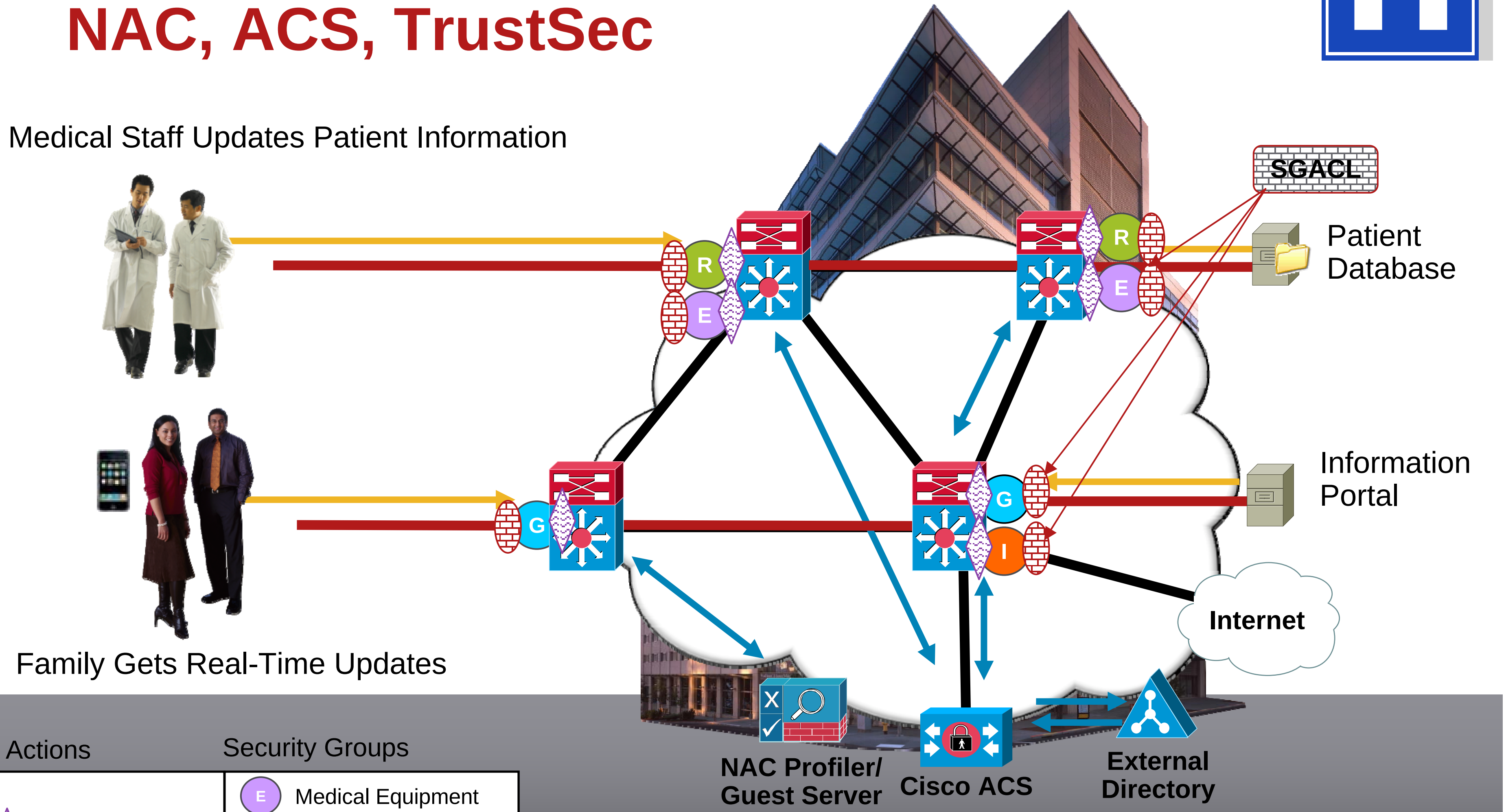
- Hop-to-hop data protection
- Preserves network L4–L7 service value

### Admission Control of Network Device

- Network device (routers, switches...) authentication
- Secure network domain

# Identity Networking in Healthcare

## NAC, ACS, TrustSec


Medical Staff Updates Patient Information
Family Gets Real-Time Updates
SGACL
R
E
G
I
Patient Database
Information Portal
Internet
NAC Profiler/ Guest Server
Cisco ACS
External Directory

Actions

- ◇ Ingress Tagging
- ▨ Egress Filtering

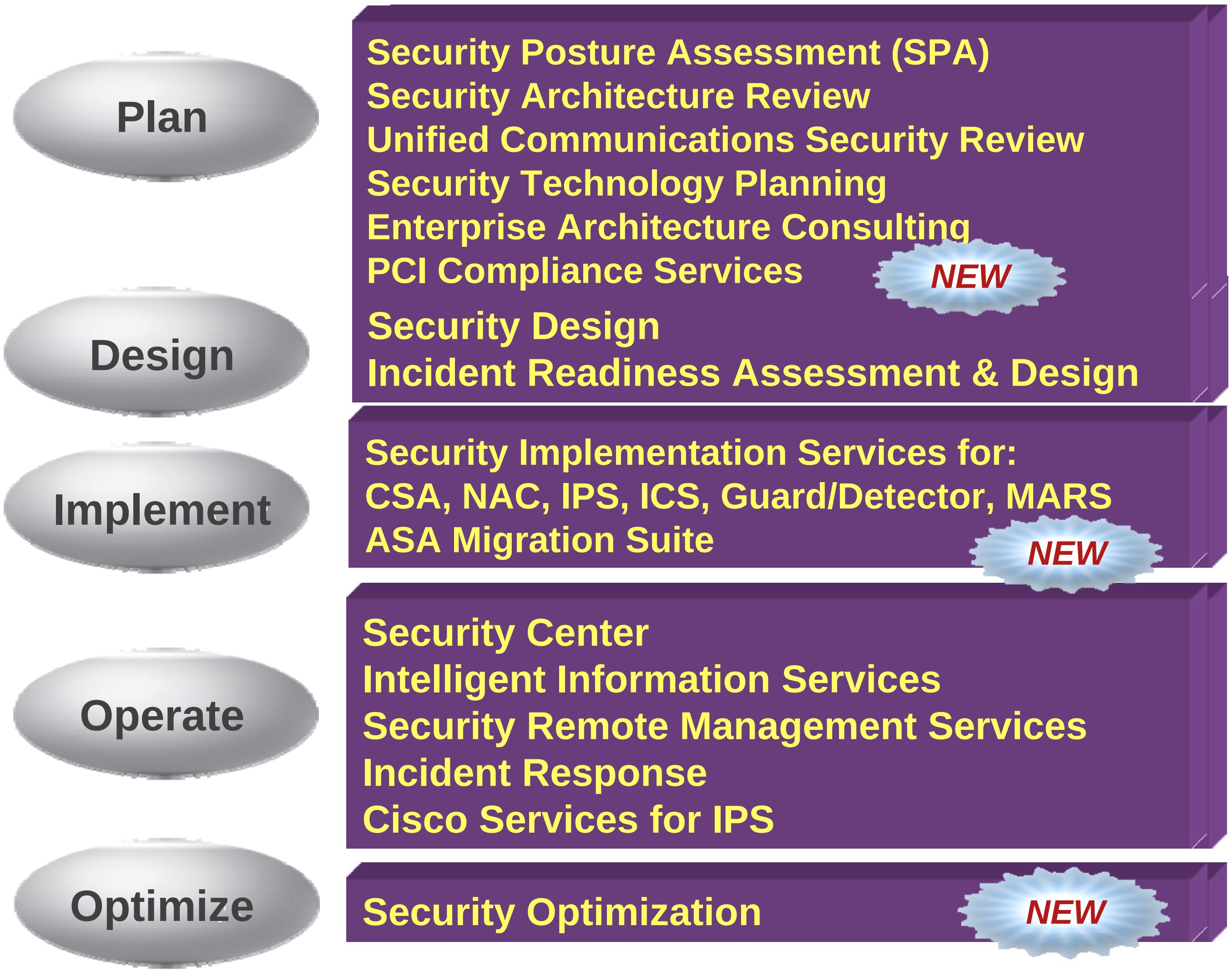
Security Groups

- E Medical Equipment
- R Medical Group
- G Guest Group
- I Internet Group

NAC/Identity verifies users and endpoints.
TrustSec enforces access control to patient information.

# Cisco Security Services Portfolio

## Delivered by Cisco and Its Partners



**Plan**

- Security Posture Assessment (SPA)
- Security Architecture Review
- Unified Communications Security Review
- Security Technology Planning
- Enterprise Architecture Consulting
- PCI Compliance Services NEW

**Design**

- Security Design
- Incident Readiness Assessment & Design

**Implement**

- Security Implementation Services for:
- CSA, NAC, IPS, ICS, Guard/Detector, MARS
- ASA Migration Suite NEW

**Operate**

- Security Center
- Intelligent Information Services
- Security Remote Management Services
- Incident Response
- Cisco Services for IPS

**Optimize**

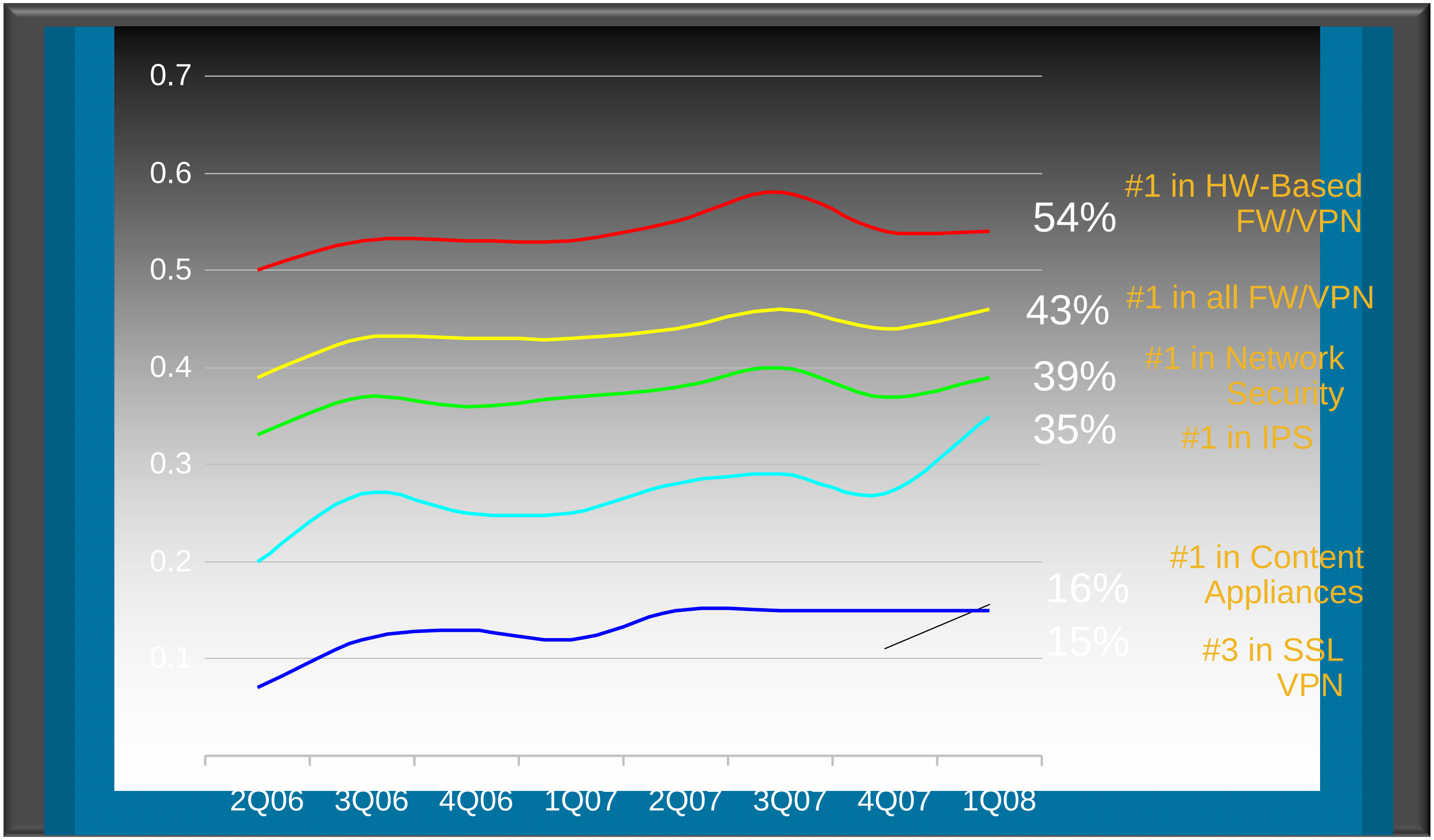
- Security Optimization NEW

### Services Benefits

- Ensures that technology supports business objectives and sound financial decisions
- Aligns network and security investments to business requirements
- Helps ensure high availability of network resources
- Helps maintain network health, keeps threat management position strong, current, proactive
- The network stays ahead of changing user demands and supports corporate policies

# Leadership Across Security Segments

## 1Q CY’08 Market Share



Source: Synergy, Infonetics

# Campus Security Solutions Summary

- **Authentication and Posture Assessment** to enforce compliance and access

  *IBNS, NAC, AAA, TrustSec*

- **Access Control** to monitor, filter and block attacks

  *ASA, IPS, WAF, FWSM, ISR, Cisco Guard*

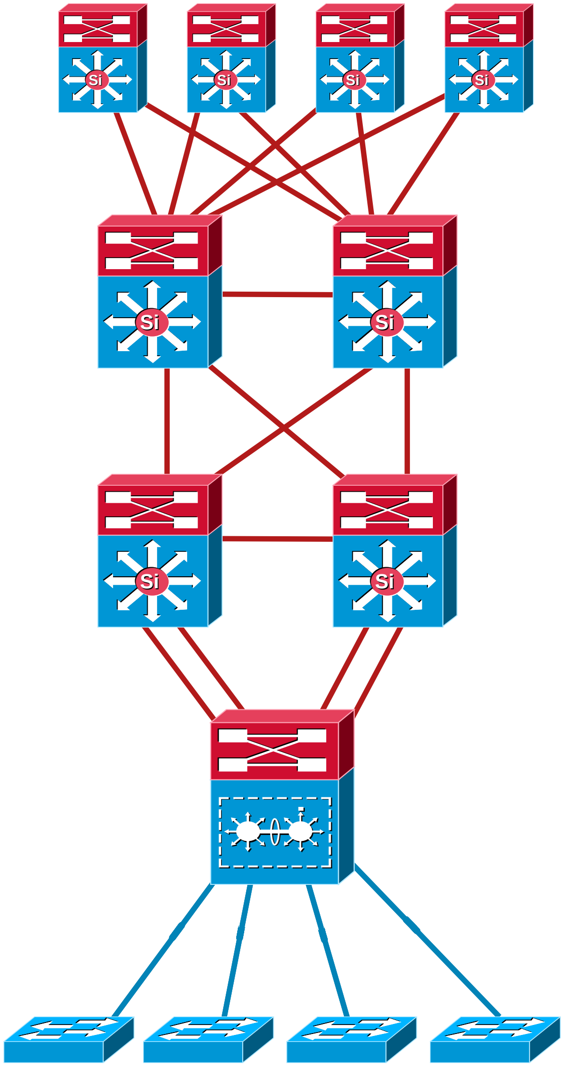
- **Policy Enforcement** via traffic monitoring and analysis

  *ASA, NAC, MARS, IPS, ACE, IronPort, WAF, NetFlow, CSM*

- **Network Foundation Security** for uniform network device policy

  *802.1x, PISA, IBNS, VLANs, ACLs, NetFlow, QoS, NBAR*

- **Security Services** to identify and resolve threats



# Making the Journey from Point Solutions to Self-Defending Networks

- Self-Defending Network: best of breed products, systems-based approach
- Helps provide solutions for business security
- Risk gaps are reduced; complexity is reduced; total cost of ownership is lower
- Protect, optimize, and grow your business

**cisco.com/go/security**

# External Cisco Security Resources

- Cisco Security Solutions

  http://www.cisco.com/go/security

- Cisco Security Management Solutions

  www.cisco.com/go/security_management

- Cisco Self-Defending Networks

  www.cisco.com/go/selfdefend

- Security Partners and Resellers Resources

  www.cisco.com/go/channelsecurity

- Cisco Security Training and Certification

  www.cisco.com/go/ccsp