Experience Today the Network of Tomorrow.

Cisco Expo 2009

Protecting Your Goldmine Securing the End Point

Talhah Jarad

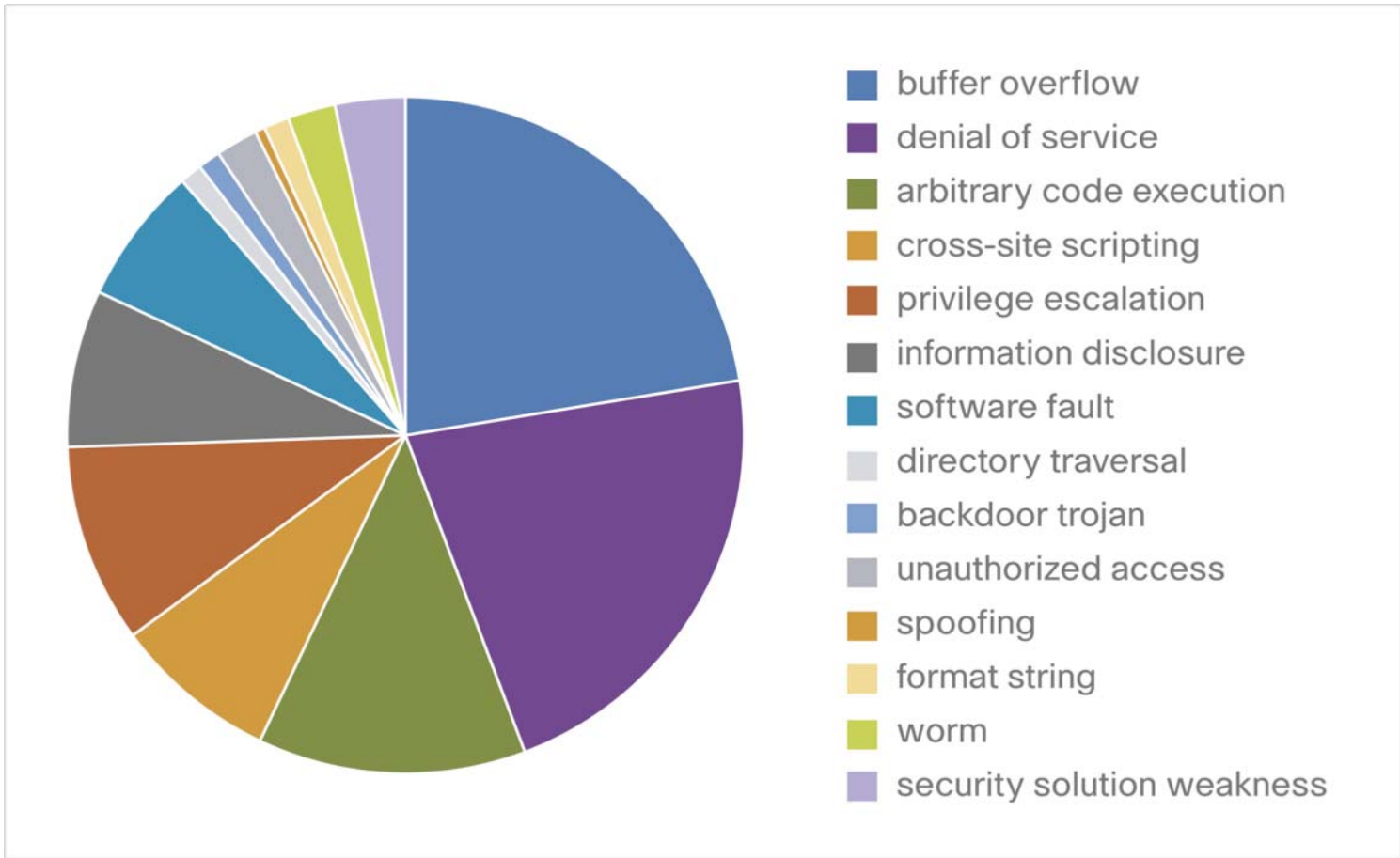
Business Development Manager

Information and Physical Security

Year in Review: 2008 Threats & Trends

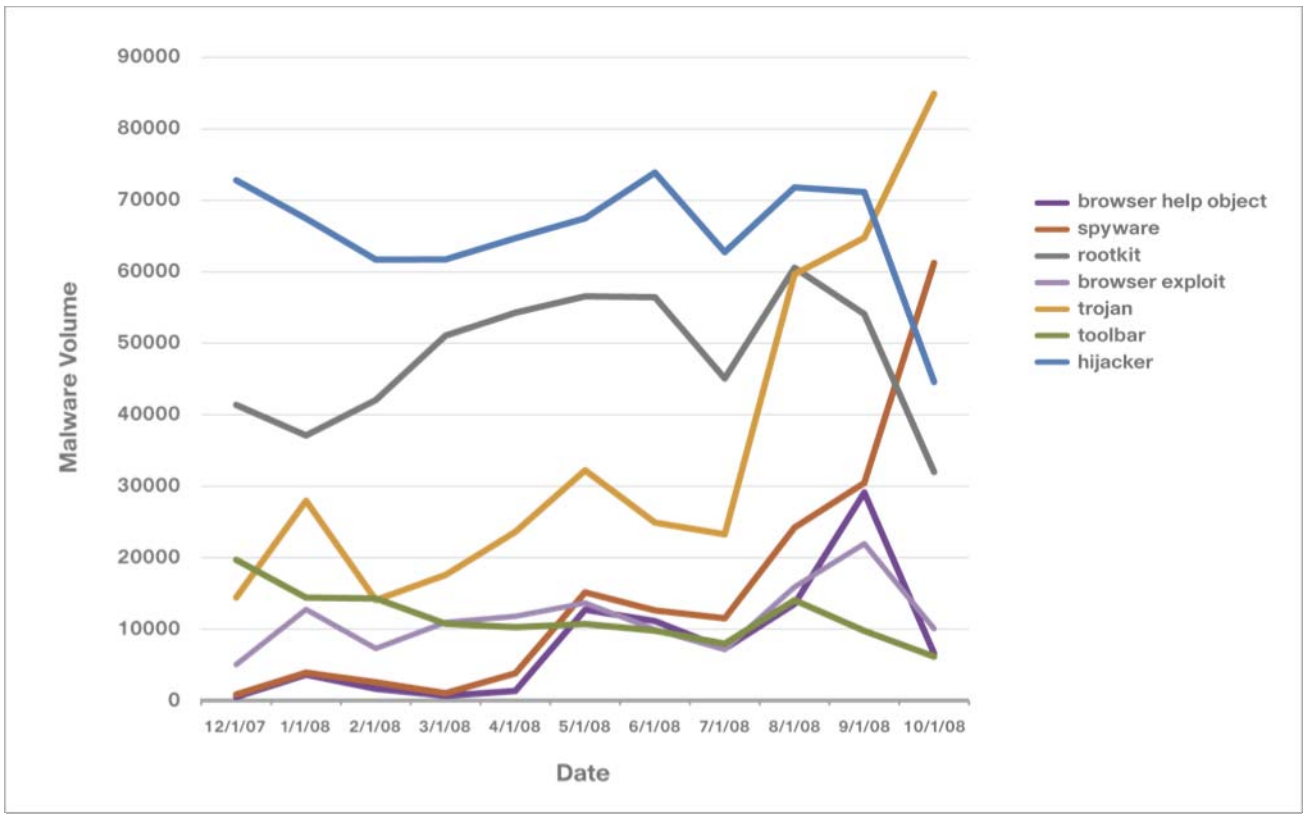
- Criminal specialization driving more sophisticated attacks
- Web ecosystem becomes number one threat vector
- Criminals exploit users trust, challenging traditional security solutions
- Loss of data and intellectual property climbing rapidly

Vulnerability and Threat Categories for 2008



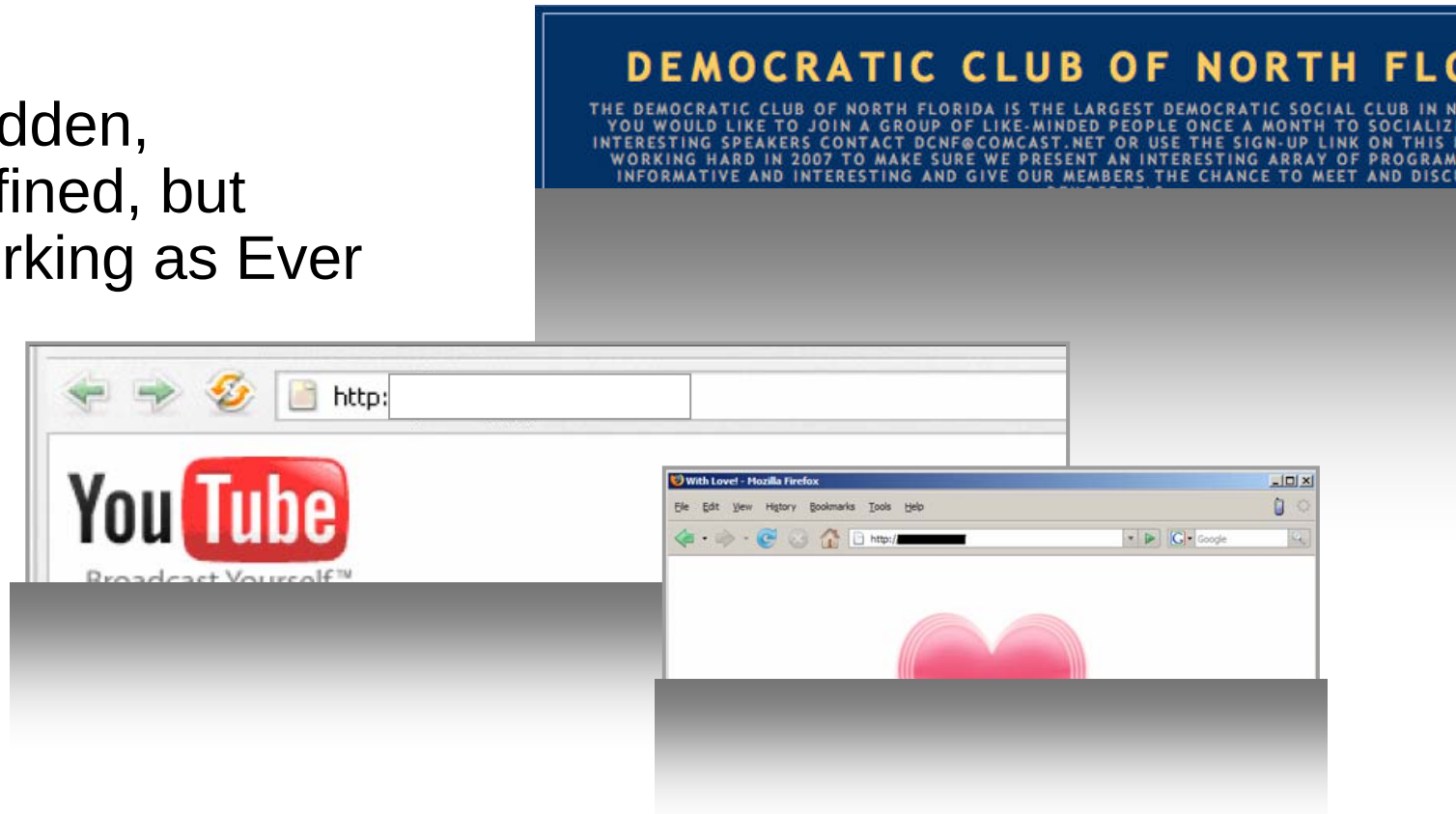
Different types of Malware Detected (by month)

- **Rise in Trojans, browser helper objects and spyware – more dangerous and increasingly clever social engineering vectors**



Botnet Trends

Better Hidden,
More Refined, but
Hard-Working as Ever



2007: Big Botnet story was Storm

2008: Storm not dead yet, now joined by Kraken/Bobax and Asprox

Employees Engage in Risky Behavior in Regards to Corporate Data

Unauthorized application use: 70% of IT say the use of unauthorized programs result in as many as **half of data loss incidents**.

Misuse of corporate computers: 44% of employees share work devices with others without supervision.

Unauthorized access: 39% of IT said they have dealt with an employee accessing unauthorized parts of a company's network or facility.

Remote worker security: 46% of employees to transfer files between work and personal computers.

Misuse of passwords: 18% of employees share passwords with co-workers. That rate jumps to 25 percent in China, India, and Italy.

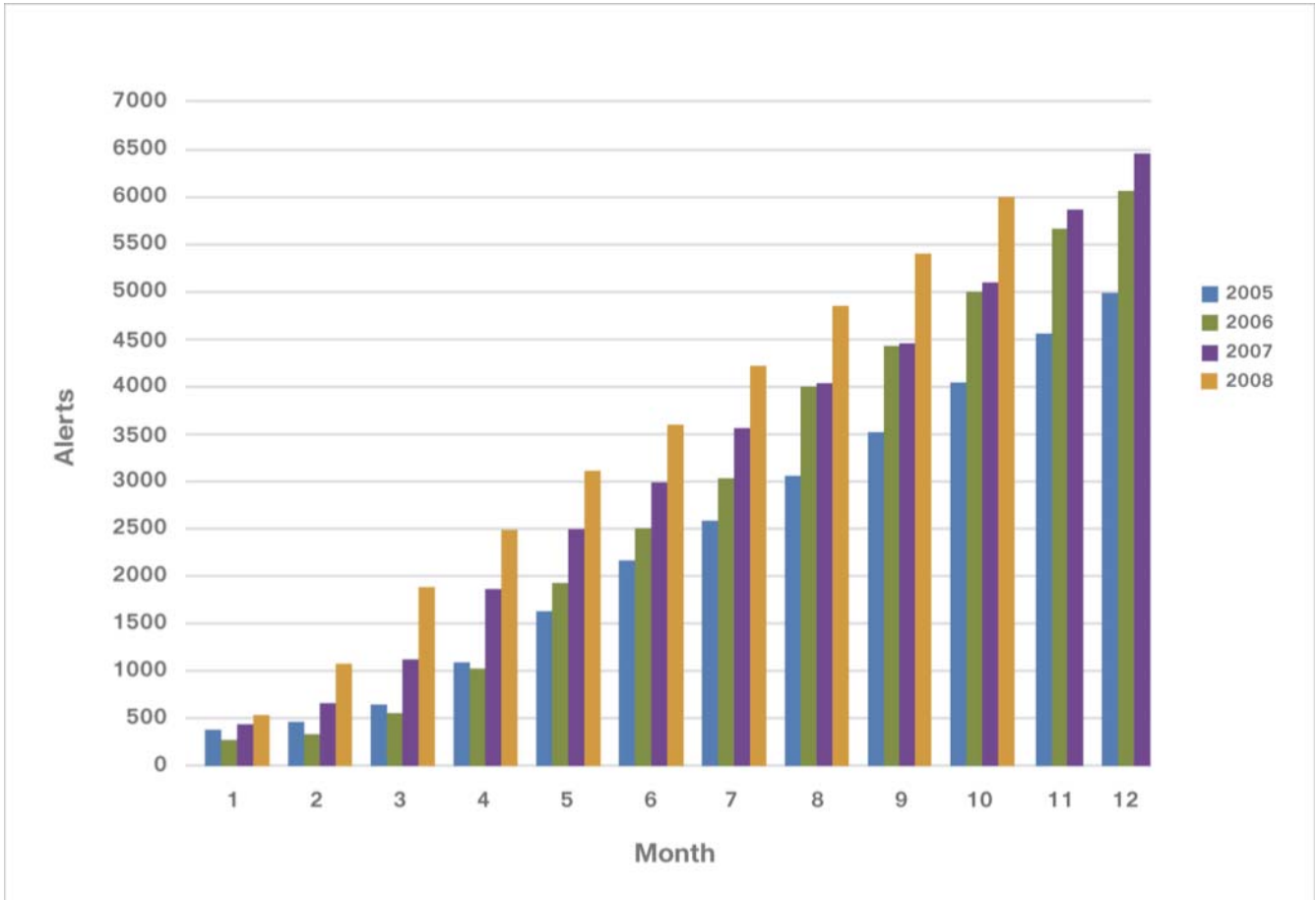
Productivity Technologies

Opportunity and Vulnerability

- Corporate network has expanded and is key platform for growth
- Also more permeable:
  - Remote access
  - Web-based tools
  - Mobile devices
- Essential to today's workforce

Cumulative Annual Alert Totals

- **The number of reported vulnerabilities in 2008 increased by 115%**



Cisco Security Agent
CSA 6.0

Cisco Expo
2009

Welcome to the Human Network.

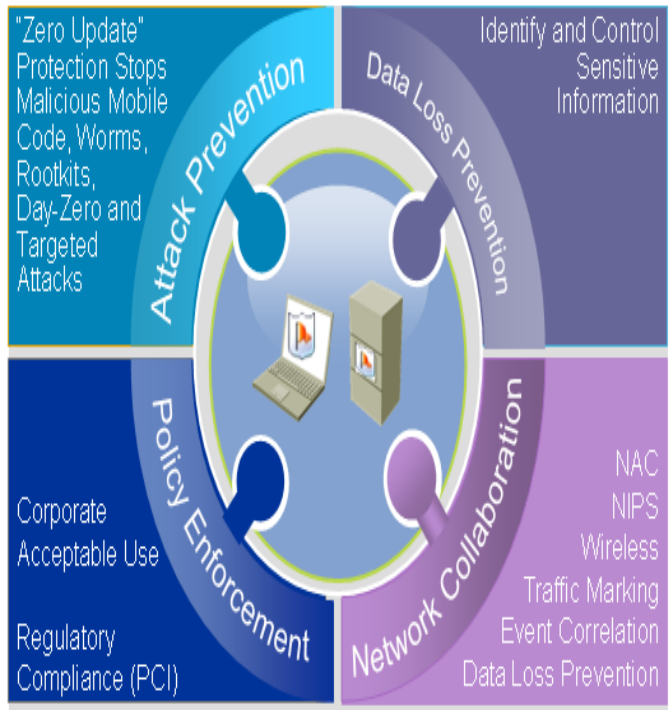
cisco

Cisco Expo 2009

End Point Security

Securing servers and Desktops with CSA 6.0

- Single Integrated Client, Simplified Management
- Protection against persistent and evolving threats
- Prevent loss of sensitive information
- Enforce appropriate use policies
- Enhance security through network collaboration
- Address corporate and regulatory compliance mandates
- Built-in Anti-Virus capabilities
- Advanced HIPS capabilities
- Anti-Spyware capabilities



Server Protection

Laptop – Desktop Protection

Welcome to the Human Network.

Cisco Expo 2009

End Point Security

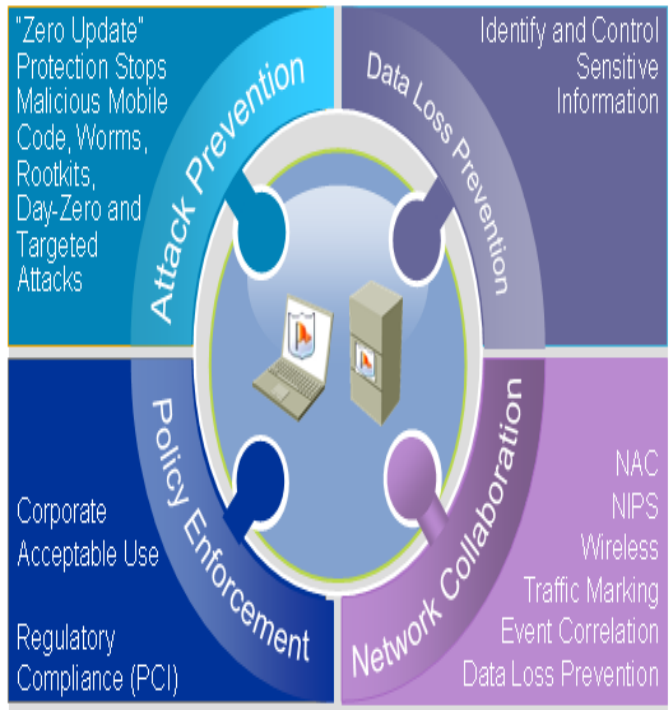
Securing servers and Desktops with CSA 6.0

Servers equipped with CSA 6.0 to protect them from

KNOWN and UNKNOWN attacks.

Cisco Security Agent immediately provides important intrusion detection and prevention features against classes of vulnerabilities such as

- Distributed Port Scans
- Buffer Overflows
- Trojan Horses
- SYN Floods
- Ping of Death and Malformed Packets
- Common IIS Vulnerabilities
- Email Worms



Server Protection

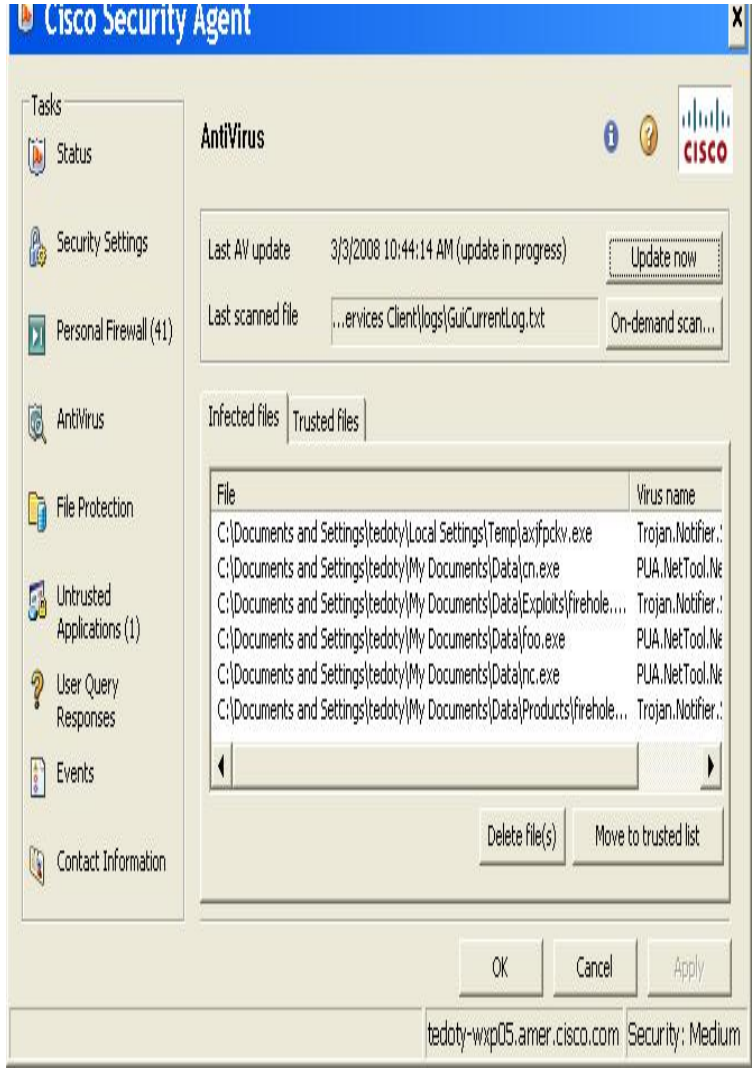
Laptop – Desktop Protection

Welcome to the Human Network.

End Point Security

Securing servers and Desktops with CSA 6.0

- Single Integrated Client, Simplified Management
- Protection against persistent and evolving threats
- Prevent loss of sensitive information
- Enforce appropriate use policies
- Enhance security through network collaboration
- Address corporate and regulatory compliance mandates
- Built-in Anti-Virus capabilities
- Advanced HIPS capabilities
- Anti-Spyware capabilities



The PCI Data Security Standard

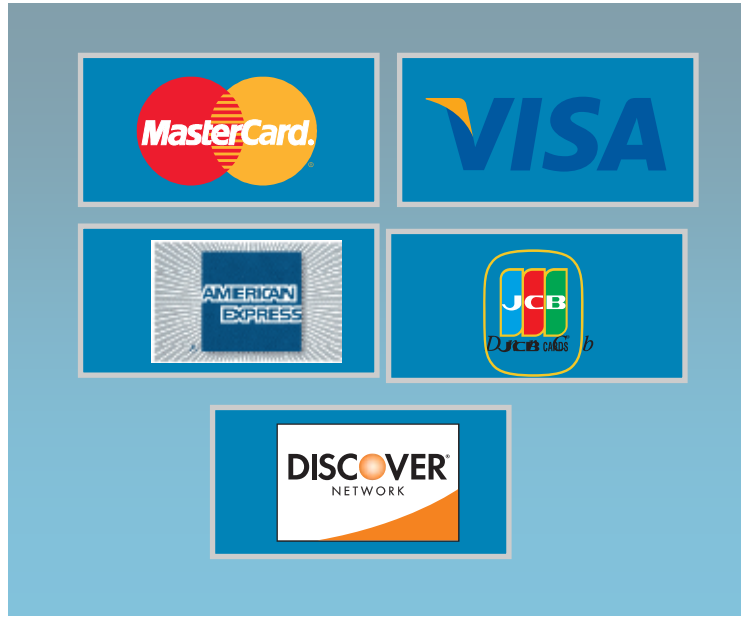
- **Impacts ALL who**

  Process,

  Transmit or

  Store cardholder data

- http://www.pcisecuritystandards.org



Requirement 3: *Protect stored data*
Requirement 4: *Encrypt transmission of cardholder data and sensitive information across public networks*
Requirement 7: *Restrict access to data by business need to know*
Requirement 10: *Track and monitor all access to network resources and cardholder data*

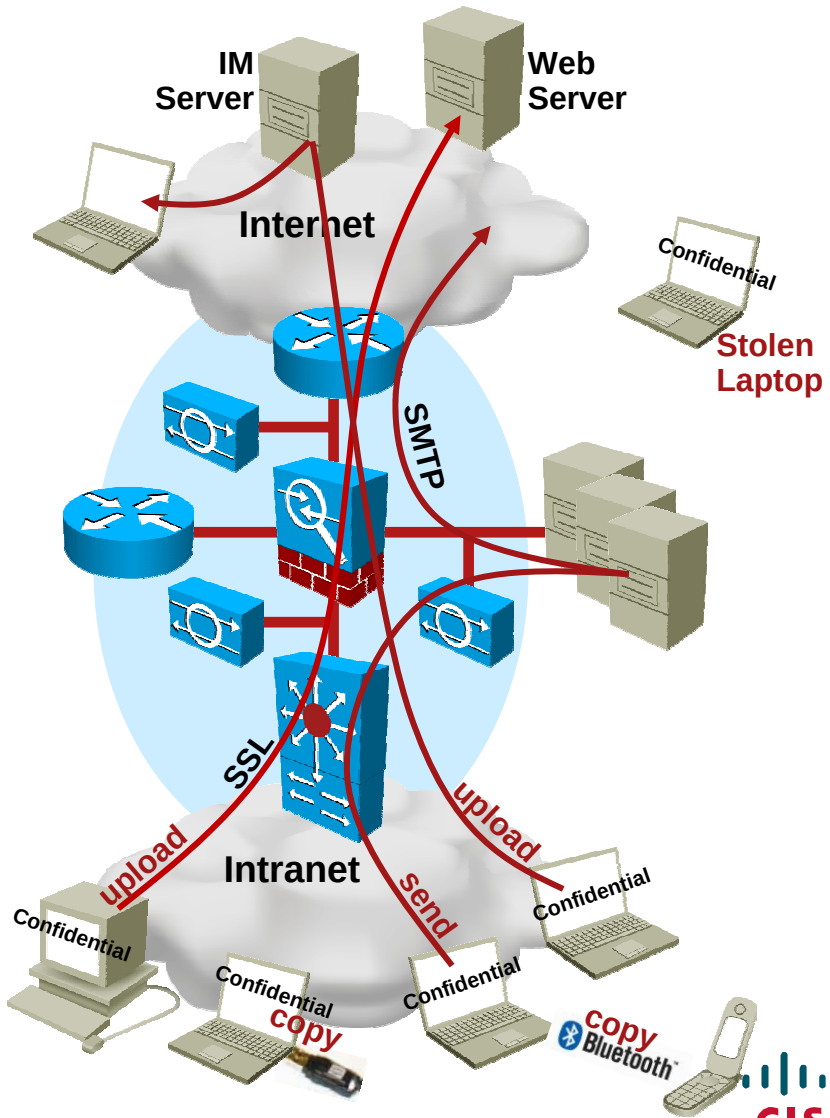
End Point DLP

Cisco Expo
2009

cisco

Endpoint Data Loss Prevention

- Storage (data at rest):
  - Local disk (laptop)
  - Removable disk (USB)
  - USB flash
  - Mobile phone
- Transport (data in motion):
  - Network (e-mail, web, IM, FTP, etc.)
  - Physical (mobile storage devices)
- Processing (data in use):
  - Creating, editing, deleting
  - Copying (e.g. clipboard)
  - Printing



Cisco Expo 2009

Cisco Endpoint DLP capabilities
Cisco Security Agent (CSA)

Discover

- Classification
  - Credit card, Social Security #s
  - Intellectual property definitions

Monitor

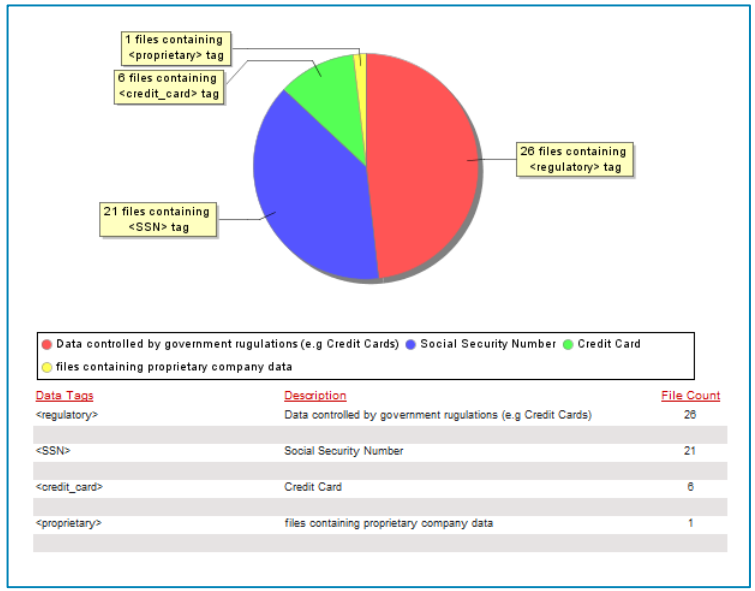
- Reporting
  - Track the location and usage of sensitive data

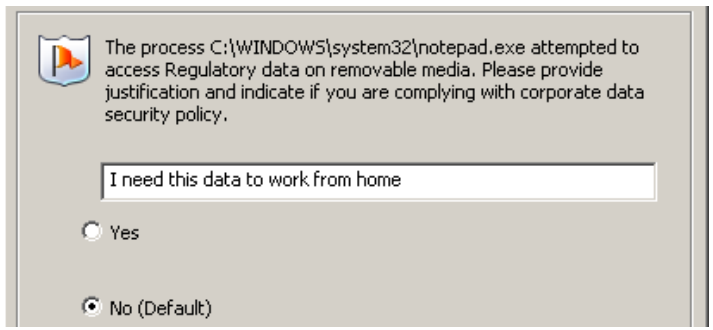
Educate

- Enhanced user education
  - Query user and audit

Enforce

- Updated enforcement controls
  - Block printing
  - Flexible clipboard control
  - NAC quarantine

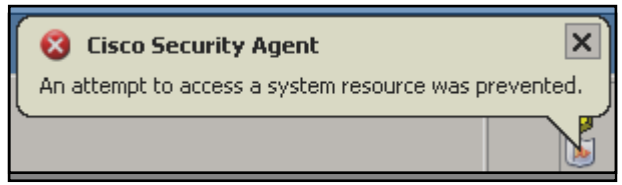


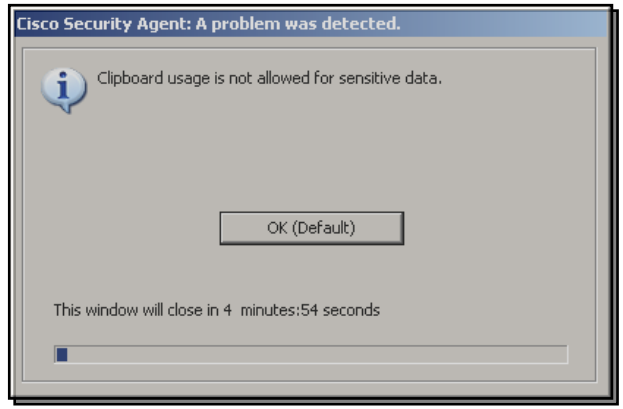


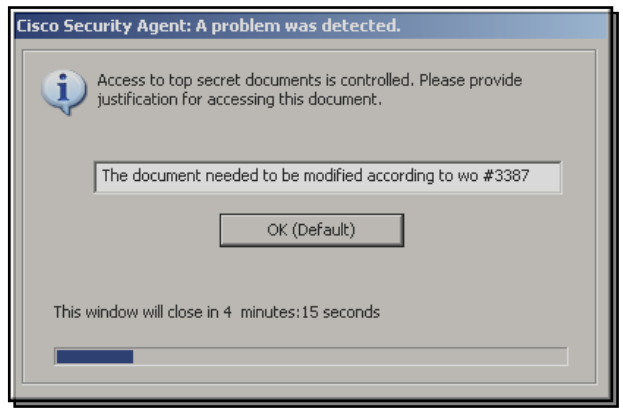
Information to the user

Reinforce Acceptable-Use Policies

- CSA can provide basic notification to users about denied actions
- CSA can provide detailed notification to users when access to a certain resource has been denied (10 languages)
- CSA can require justification from users accessing sensitive resources

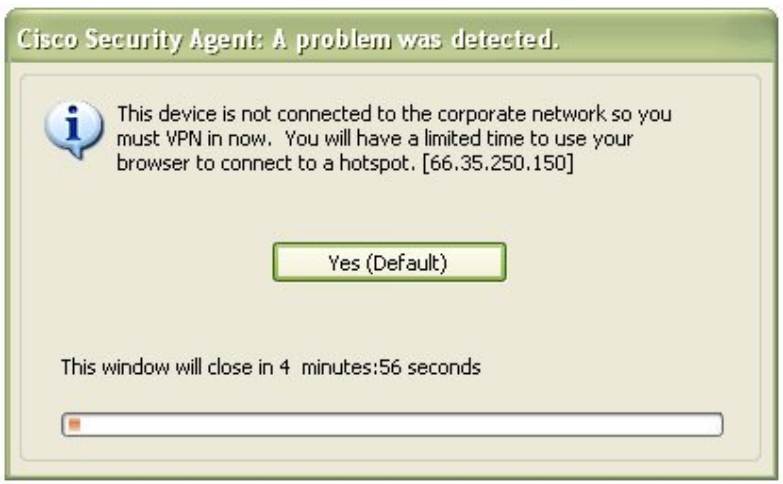


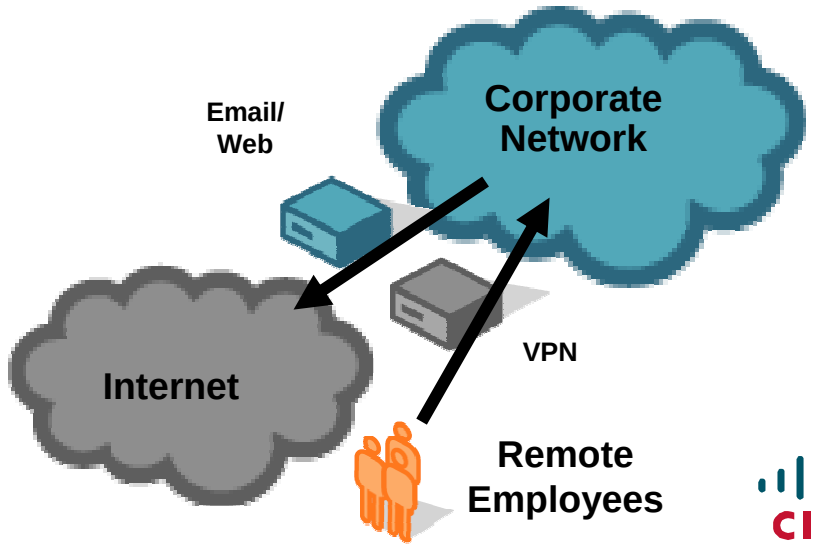




CSA Enforces Policy for Mobile Users

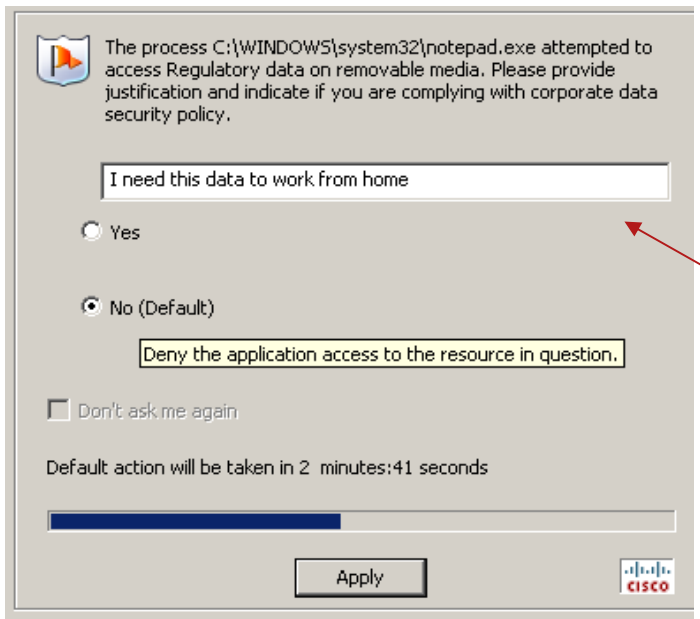
- ✓ CSA can require the use of VPN for remote users
- ✓ CSA can block SSL sessions not sent via corporate proxy
- ✓ These ensure that corporate network mail & web protections are not bypassed





Range of DLP Controls

- Controls for USB drives, CD, iPod
- Monitor usage
- Confidential file controls
- Authorised user controls
- Location-based controls

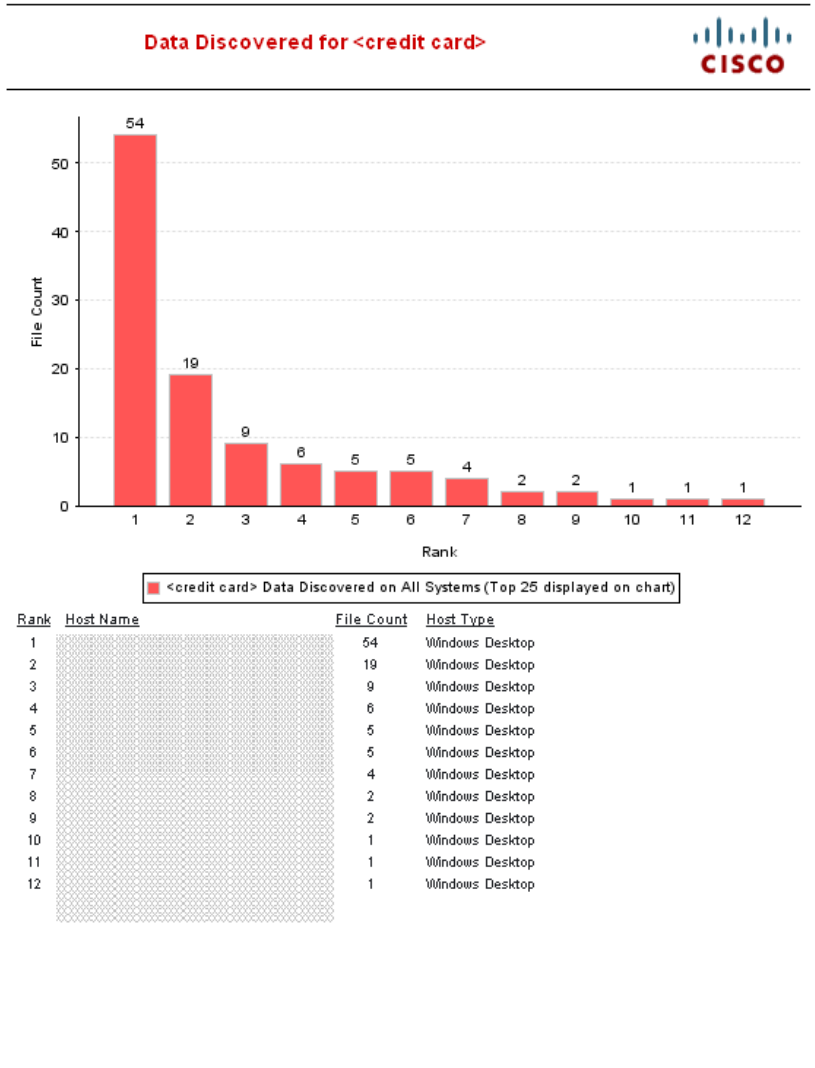


End user Business Justification for audits

Consolidated event reporting of USB usage

Data Loss Prevention Logs & Reports

- Repository of DLP events
- Audit trail and activity log
- Activity reporting



Rank	Host Name	File Count	Host Type
1		54	Windows Desktop
2		19	Windows Desktop
3		9	Windows Desktop
4		6	Windows Desktop
5		5	Windows Desktop
6		5	Windows Desktop
7		4	Windows Desktop
8		2	Windows Desktop
9		2	Windows Desktop
10		1	Windows Desktop
11		1	Windows Desktop
12		1	Windows Desktop

CSA and Network IPS
Better Together at Attack Prevention

CSA Brings…

- Protection for Local Application Attacks (e.g. half of the MS Tuesday vulnerabilities, privilege escalation)
- Inspect encrypted traffic
- Devices off the corporate network (i.e. road warriors)
- Day Zero Attack Protection through Application Behavioral

Network IPS Brings…

- Protect all devices (inc. those not running CSA)
- Stop attacks closer to source
- Defense against network application-only attacks (i.e. Javascript attacks)
- DDoS and Worm Propagation Protection
- Day Zero Attack Protection through Network Behavioral Anomaly Detection

Better Together Because…

- Every end-system sending intelligence into IPS Cloud (Sharing of CSA Watch List)
- Higher fidelity NIPS through sharing of end-system OS
- Complete picture with MARS for Incident Response and Forensics
- Two different technologies (and teams) for defense in

Network Admission Control (NAC)

Cisco Expo 2009

Welcome to the Human Network.

cisco

Cisco NAC Components

Policy Components

NAC Manager

Centralized management, configuration, reporting, and policy store

NAC Server

Posture, services and enforcement

Ruleset Updates

Scheduled automatic rulesets for AV, Microsoft hot-fixes, etc.

NAC Profiler

Profiles unmanaged devices and applies policy based on device type

NAC Guest

Full-featured guest provisioning server

Endpoint Components (Optional)

NAC Agent

No-cost client for device-based scans.

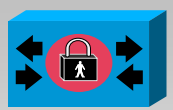
Web Agent

No-cost client for device-based scans.

802.1x Supplicant

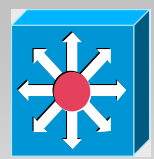
802.1x supplicant via CSSC or Vista embedded supplicant

Communications Components



ACS

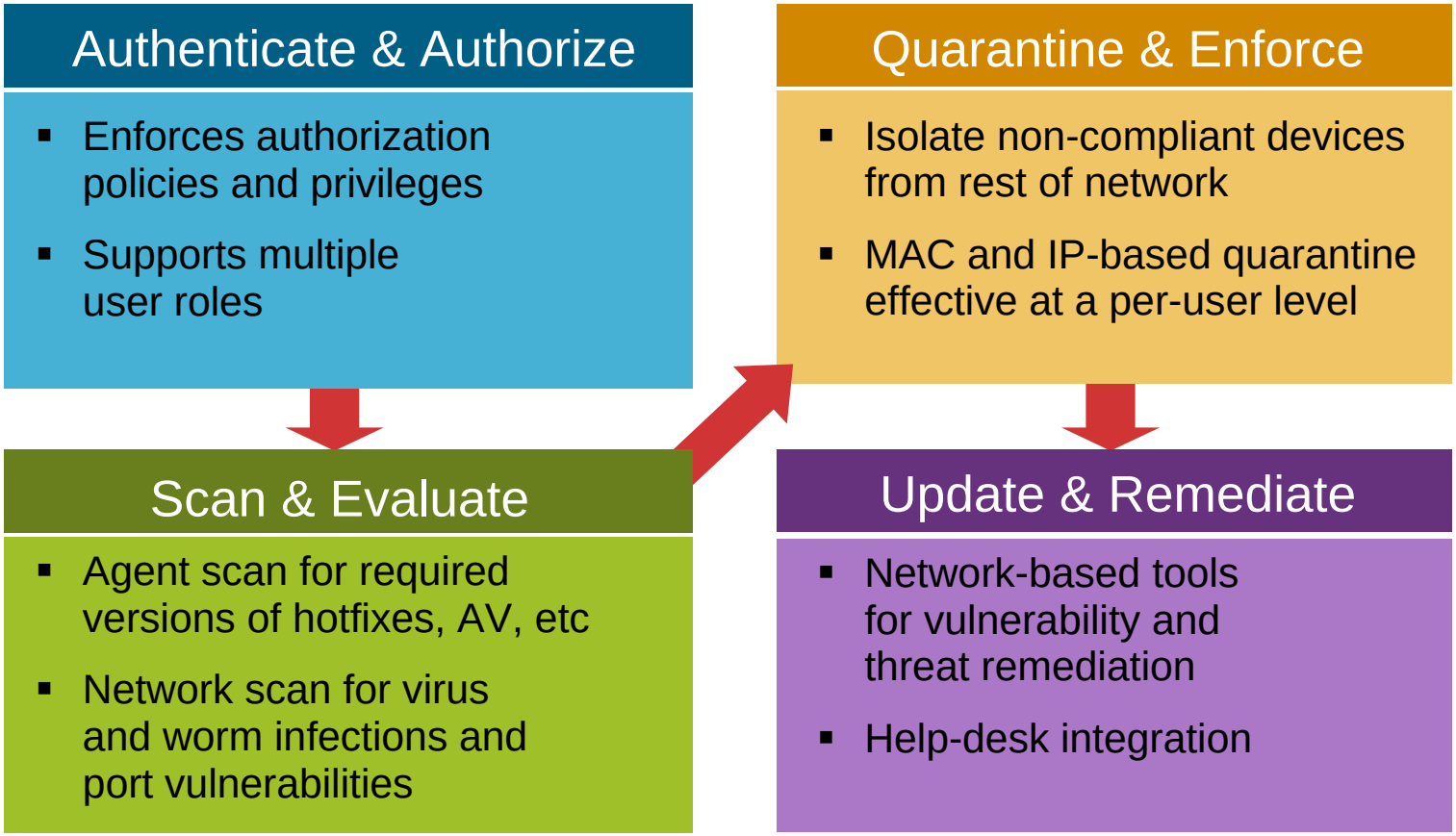
Access policy system for 802.1x termination and identity based access control



Routing and Switching Infrastructure

Make Access Contingent on Compliance

First, Establish Access Polices. Then:



NO COMPLIANCE = NO NETWORK ACCESS

Cisco NAC Profiler: Automation

Cisco NAC Profiler

PCs	Non-PCs			
	UPS	Phone	Printer	AP
				

Discovery

Endpoint Profiling

Discover all network endpoints by type and location

Maintain real time and historical contextual data for all endpoints

Monitoring

Behavior Monitoring

Monitor the state of the network endpoints

Detect events such as MAC spoofing, port swapping, etc.

Automated process populates devices into the NAC Manager; and subsequently, into appropriate NAC policy

Wireless Out of Band

Infrastructure pre-requisites

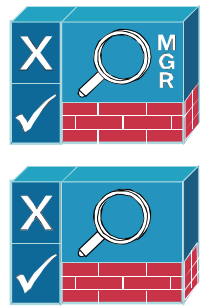
- **802.1x Supplicant** – supplicant agnostic – supports XP, Vista, CSSC etc

Client compatibility

- **NAC 4.5** – Available
- **WLC 5.1** – Available

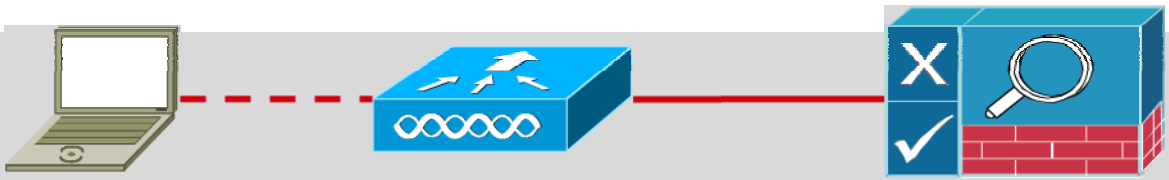
Deployment

- Compatible with Wired OOB deployments
- Supports L2 Virtual Gateway only
- No role based VLAN assignment



Wireless OOB – how it works

1. Client authenticates with WLC via 802.1x
2. WLC assigns clients traffic to quarantine vlan



3. Client is inband with NAC Server
4. Client goes through NAC process with NAC Server

5. NAC Manager tells WLC to put client in access vlan
6. Client gets direct access to the network

MAC Posture

OS Support

MAC OS 10.4 and above
NAC 4.5 Agent required

Applications

Antivirus
Antispyware

Remediation

AV Definition Update (ClamAV)
AS Definition Update (ClamAV)
Link Distribution
Local Check

Role of Identity & Access Management

- Preventing unauthorised network access
- Capabilities for differentiated network access
- Identity-based and role-based network access controls

  802.1X and NAC can provide user or machine authentication,

  VLAN/ACL assignments in access layer to avoid unauthorised access

- Checking endpoint posture – Network Admission Control

  Distinguish between managed and unmanaged assets

  Ensure protection mechanisms are present and running
  - Endpoint DLP
    - Disk or folder encryption software on clients
  - Other security or asset management tools

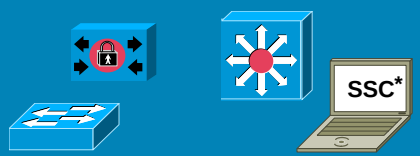
Role of Identity & Access Management

- Future: Role-based network access using Cisco TrustSec
  - TrustSec tagging scheme will extend traffic separation controls across capable network components
  - Access Policies based upon resource groups (not IP address etc)
  - Security Access Policies are decoupled from network topology
  - Identity, posture, location and time-based controls
  - Transparent to the user/system
- Future: Entitlement Management (Cisco Enterprise Policy Manager)
  - Extending controls into databases (e.g. Oracle), collaboration portals (e.g. Sharepoint, Webex) and application servers.

Controlling network access

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
- Behavioural monitoring
- Device reporting

Guest Services

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

Posture Services

- 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

Q & A

Cisco Expo 2009

Please fill in the evaluation form

Welcome to the Human Network.