# DEF-203: Protecting your Network with Scan and Block Technology

Wednesday, February 16, 2005

Moderator: Phil Schacter, VP and Service Director, Burton Group

Panelists: Scott Olson, SVP Marketing, WholeSecurity

Stacey Lum, CEO, InfoExpress

Russell Rice, Director Marketing, Cisco Systems

RSA Conference 2005

# Protecting your Network: Scan and Block

- Panel objectives
  - Give the audience an appreciation for scan and block solutions, how they work, and why they're needed
  - Communicate different perspectives on the technologies that are needed on the endpoint, policy infrastructure, and network
  - Discuss the various industry initiatives to create open architectures and develop standards for scan & block technologies to interoperate
  - Set realistic customer expectations for when scan & block solutions will be generally available and broadly supported



INFOEXPRESS ,INC. - EX2486
CISCO SYSTEMS, INC. , et al. v. INFOEXPRESS, INC. [IPR2024-00675]

# Protecting your Network: Scan and Block

- Agenda
  - Rationale for Scan and Block
  - Architecture fundamentals
  - Industry perspective
  - Scott: integrity at the endpoint
  - Stacey: policy infrastructure
  - Russ: network's role in policy enforcement
  - Panel discussion
  - Open Q&A



INFOEXPRESS ,INC. - EX2486
CISCO SYSTEMS, INC. , et al. v. INFOEXPRESS, INC. [IPR2024-00675]

# Protecting your Network: Scan and Block

- Rationale for Scan and Block
  - Individual endpoint systems, including desktop, laptop and other mobile computing devices, are vulnerable to operating system, network, Web browser, and application level attacks
  - Common vulnerabilities:
    - Configuration errors, such as file sharing enabled
    - Security patches not applied to OS, browser, or applications
    - Out-of-date virus or intrusion prevention signature files
    - Protective systems may be disabled by user
    - Use of external email or IM systems, bypassing protection
    - Potential for a “rogue” system to appear on the network
  - Escalating economic damage from rapidly propagating virus/worm



INFOEXPRESS ,INC. - EX2486
CISCO SYSTEMS, INC. , et al. v. INFOEXPRESS, INC. [IPR2024-00675]

# Protecting your Network: Scan and Block

- Architecture Fundamentals
  - Endpoint posture assessment data gathering generally requires agent software running on the endpoint system
  - Some vulnerability scanners sit on the network and probe endpoint systems to discover compromised or vulnerable systems
  - For systems that aren't managed by corporate IT, a clientless approach allows for automated download of transient assessment client code
  - Mechanism is required to "quarantine" any system that isn't running approved posture assessment software, or systems which are non-compliant to company policies for secure endpoint systems



INFOEXPRESS ,INC. - EX2486
CISCO SYSTEMS, INC. , et al. v. INFOEXPRESS, INC. [IPR2024-00675]

# Protecting your Network: Scan and Block

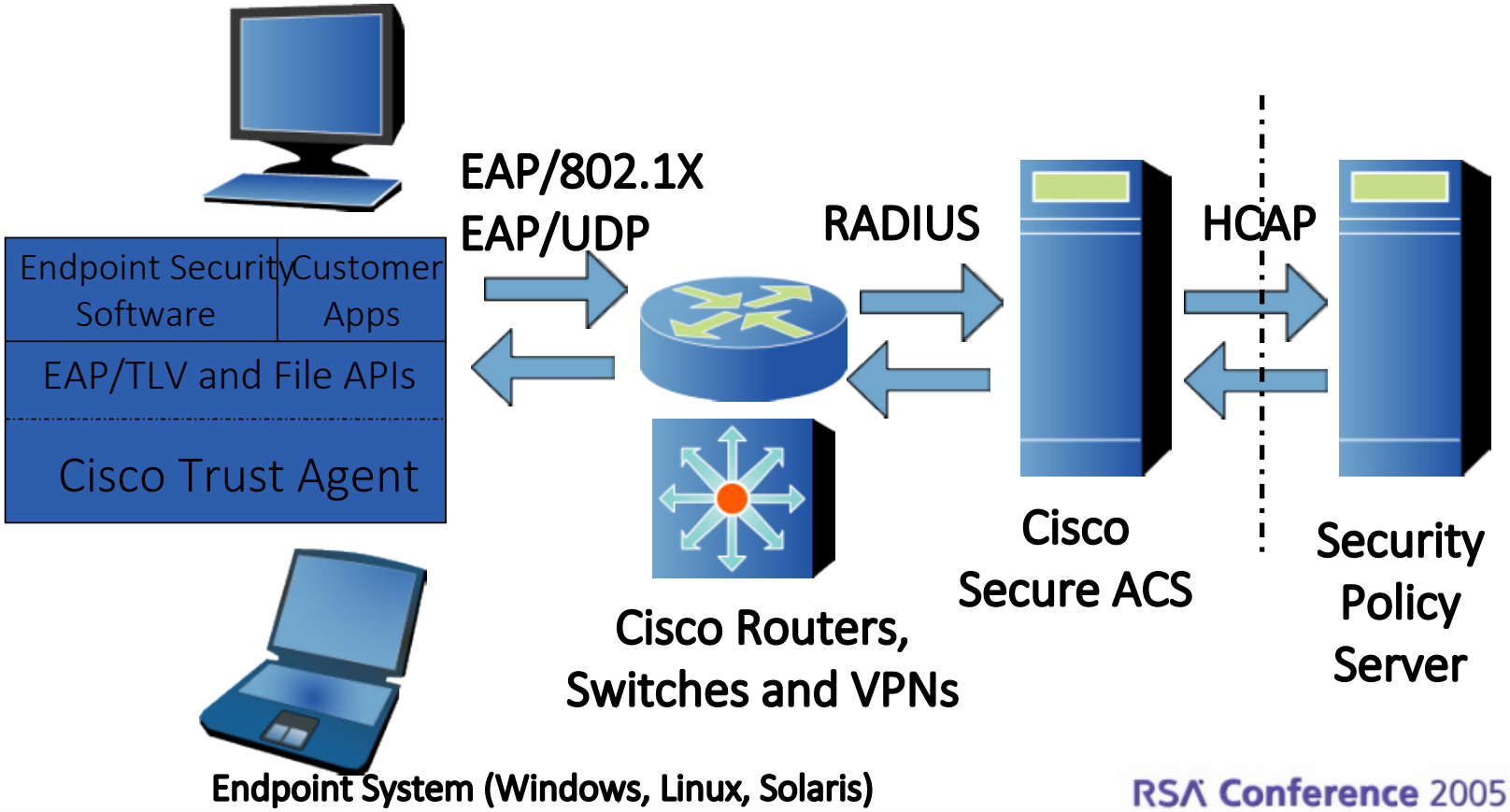
- Architecture Fundamentals (cont'd)
  - Interfaces required to enable security policy administrators to define and maintain endpoint security policies
  - Policy distribution mechanism is required to ensure most current policies are available to policy evaluation/enforcement functions
  - Policy enforcement can occur in a network switch/router, VPN gateway, DHCP server, or network access gateway/appliance
  - Quarantine mechanisms include VLANs and private subnets/DMZ areas
  - Remediation resources to bring the endpoint system back into compliance are generally made available in the quarantine zone



INFOEXPRESS ,INC. - EX2486
CISCO SYSTEMS, INC. , et al. v. INFOEXPRESS, INC. [IPR2024-00675]

# Protecting your Network: Scan and Block

- Cisco's Network Admission Control Architecture

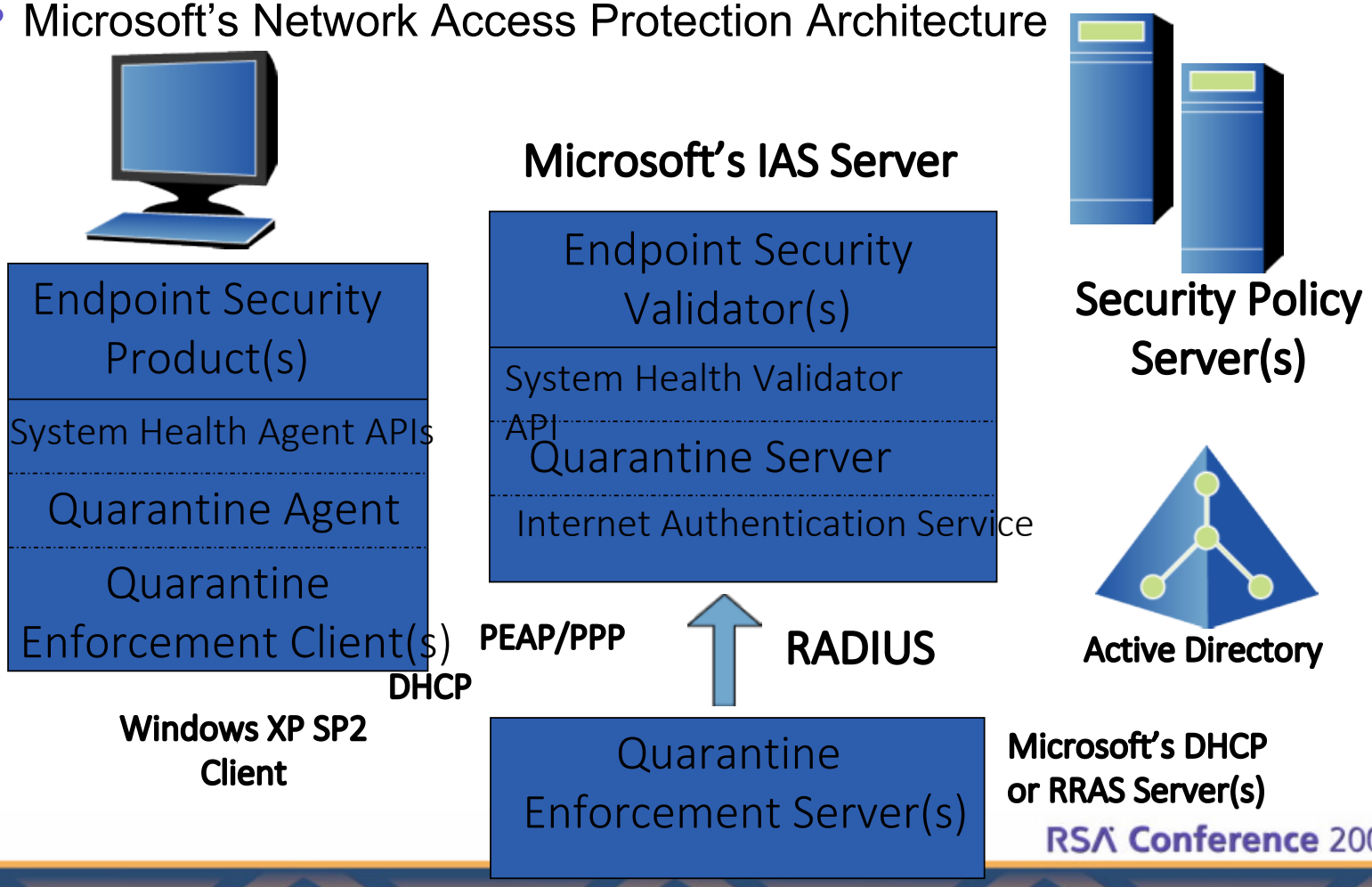





INFOEXPRESS ,INC. - EX2486
CISCO SYSTEMS, INC. , et al. v. INFOEXPRESS, INC. [IPR2024-00675]

# Protecting your Network: Scan and Block

- Microsoft's Network Access Protection Architecture




RSA Conference 2005

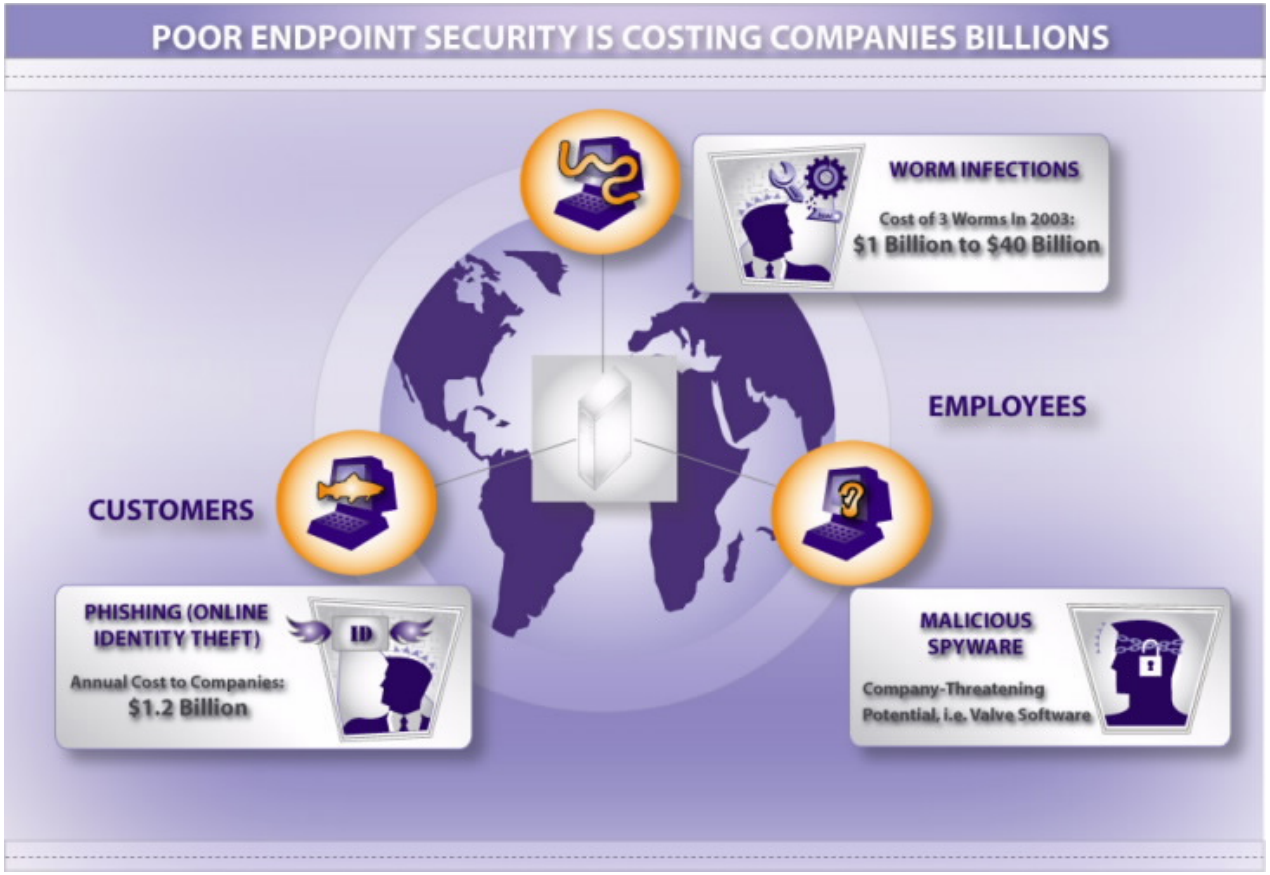
# Protecting your Network: Scan and Block

- Industry Perspective
  - Comprehensive security architecture must address the reality of the distributed perimeter, and this includes endpoint system defenses
  - Large companies need tools to effectively manage security posture on thousands of connected endpoint systems
  - Industry must collaborate on interoperable security systems that cross categories – endpoint integrity, policy infrastructure, network
  - Promising early initiatives by Cisco (NAC) and Microsoft (NAP)
    - Open through partnership programs, but not industry standards
    - Promising collaboration between Cisco and Microsoft
  - Trusted Computing Group work on Trusted Network Connect (TNC)



INFOEXPRESS ,INC. - EX2486
CISCO SYSTEMS, INC. , et al. v. INFOEXPRESS, INC. [IPR2024-00675]

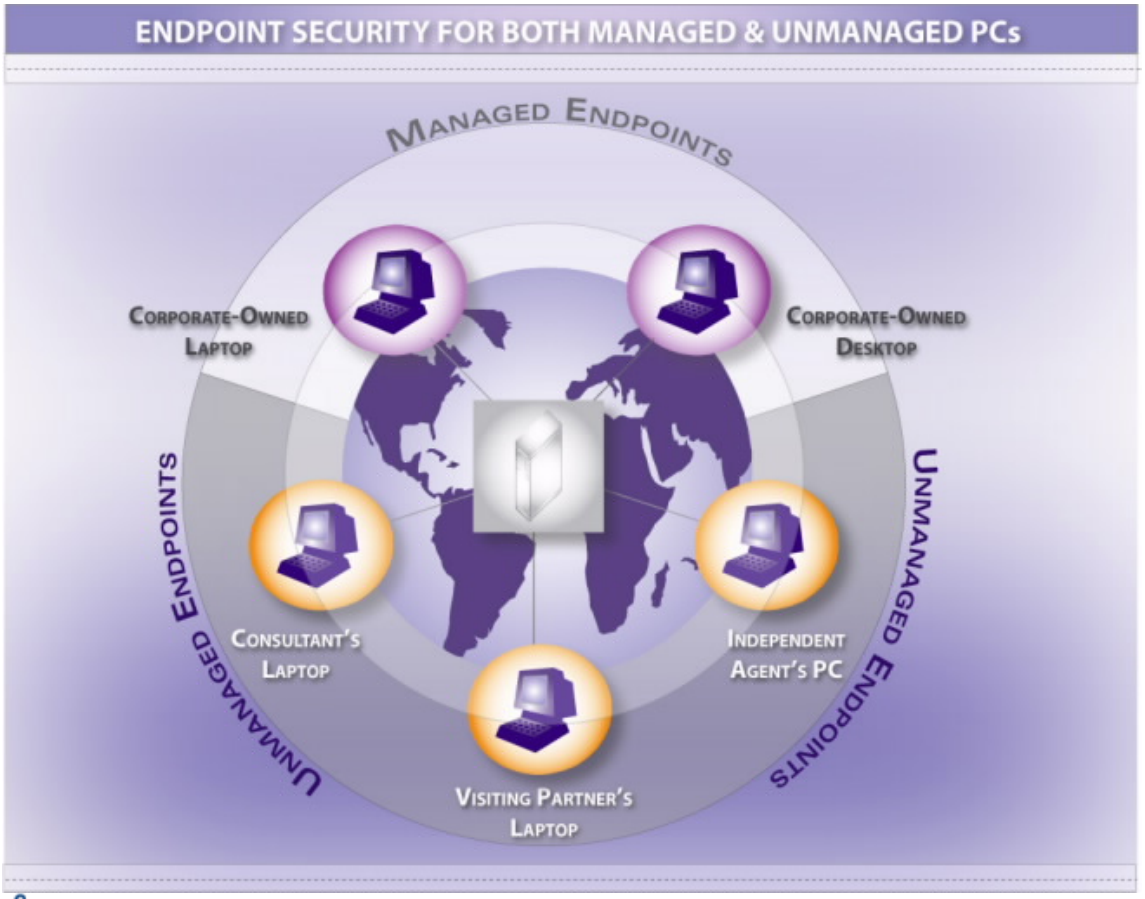
# Endpoint Security/Integrity Perspective: Whole Security




WholeSecurity

RSA Conference 2005

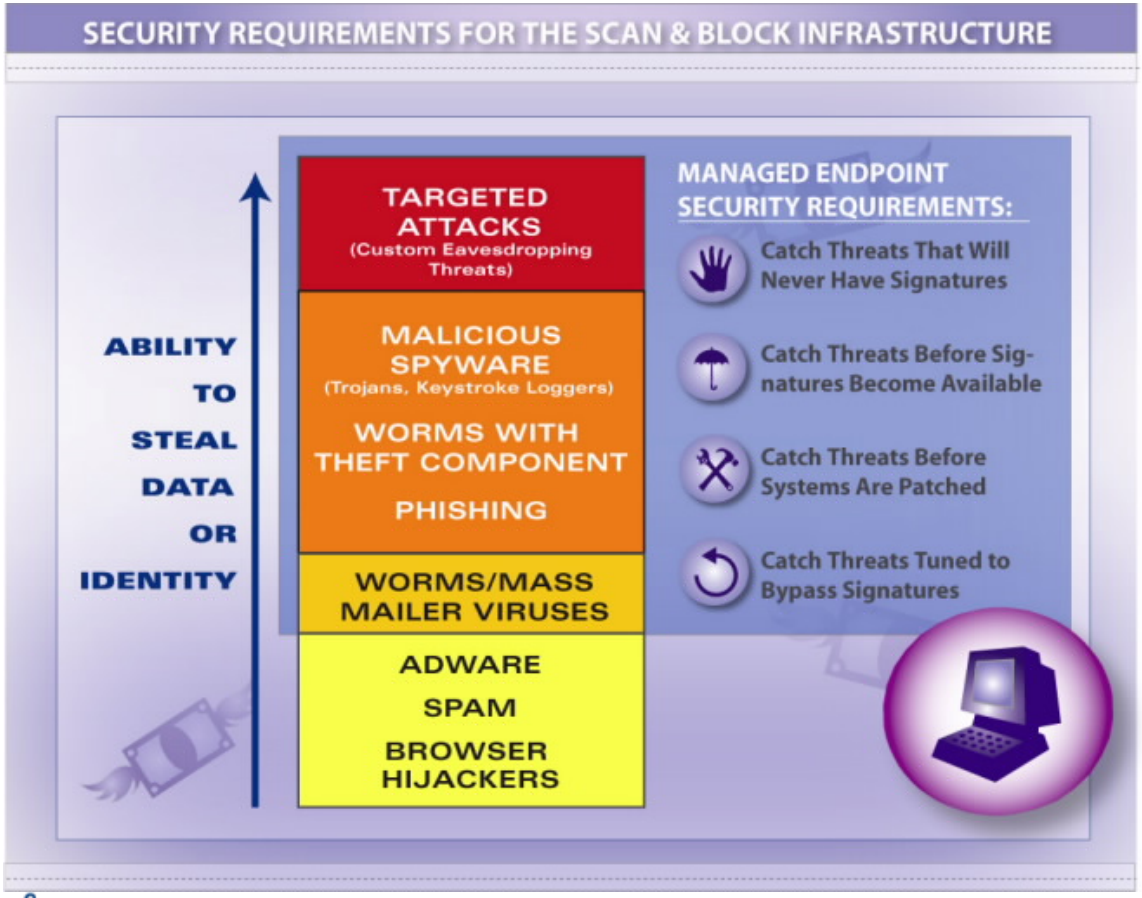
# Endpoint Security Is Required For Both Managed & Unmanaged PCs Entering the Network




WHOLESECURITY

RSA Conference 2005

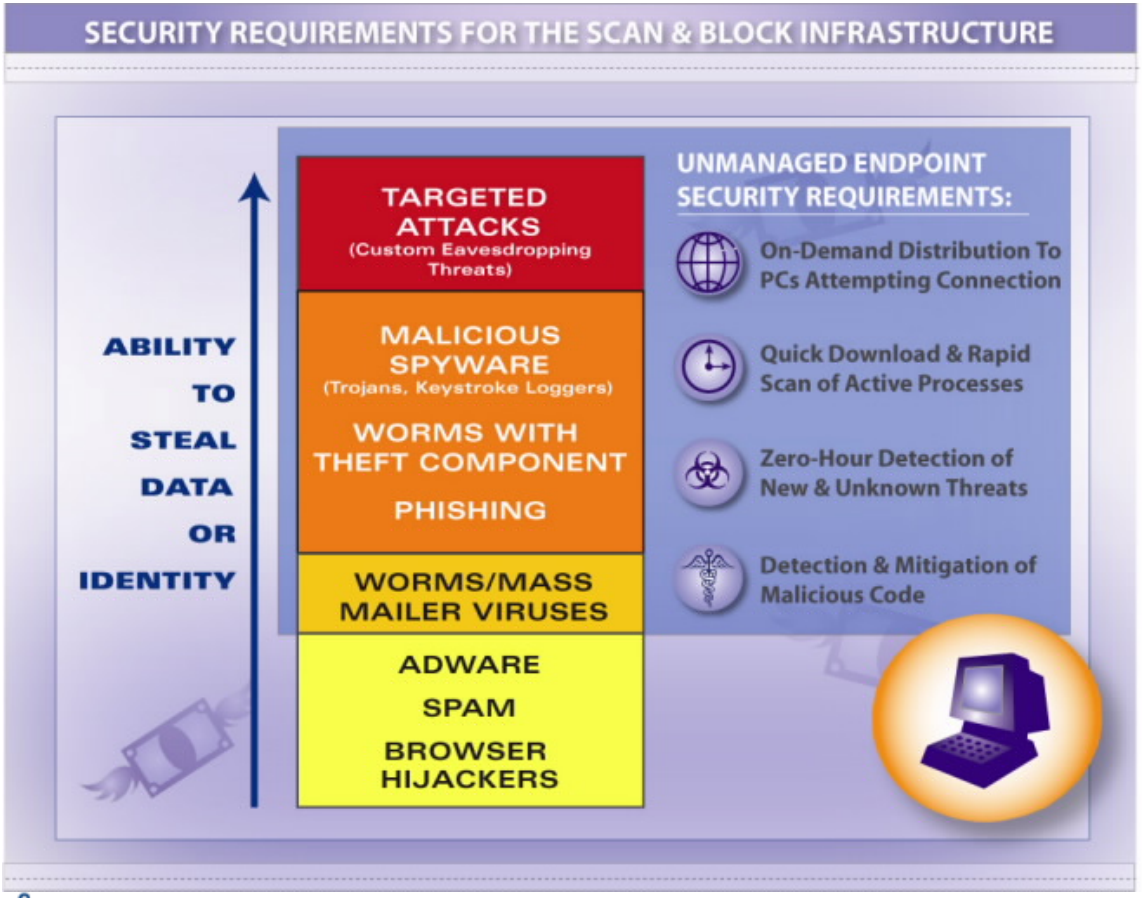
# Security Requirements for **MANAGED** Systems In the Scan & Block Infrastructure




WHOLESECURITY

RSA Conference 2005

# On-Demand Security for **UNMANAGED** Systems In the Scan & Block Infrastructure




WHOLESECURITY

RSA Conference 2005

# Policy Infrastructure Perspective: InfoExpress

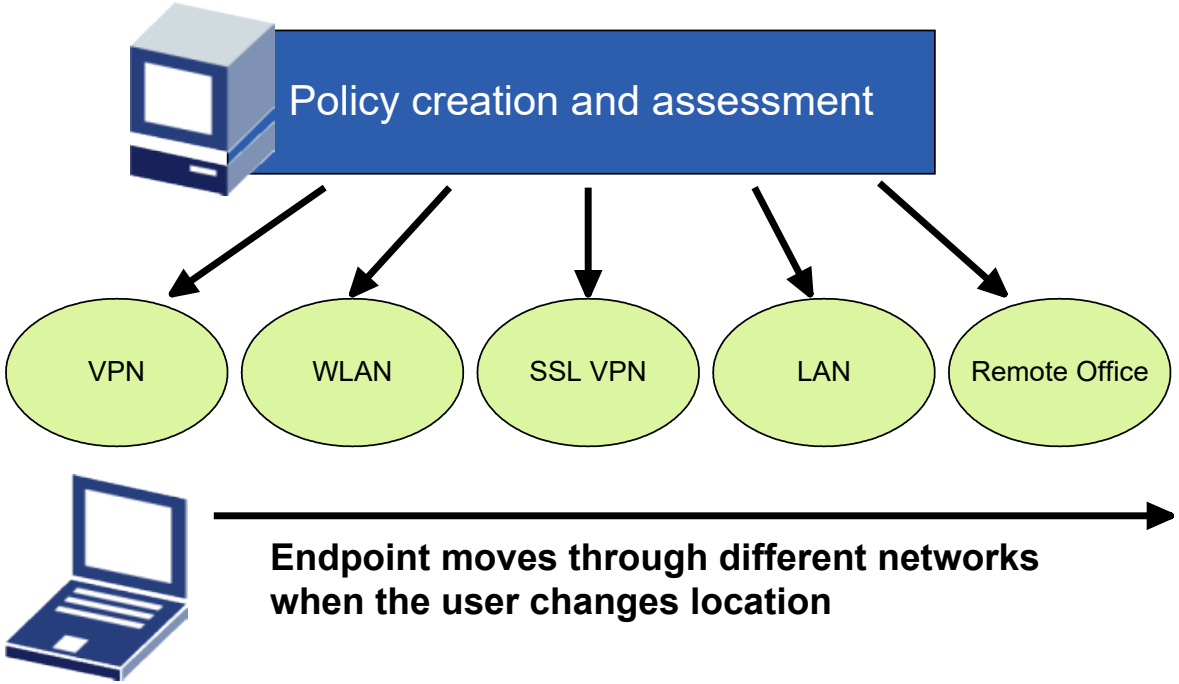
- **Scan and Block - Real time steps**
  - Assessment, access control, and remediation
- **Compliance considerations**
  - Endpoint auditing – standard vs custom configurations
  - Quarantine capabilities – fail close and infrastructure support
  - Remediation actions for non-compliant endpoints
- **Scalability considerations**
  - Central management – policies, reports, and logs
  - Infrastructure support - remote, LAN, wireless, SSL VPN, etc.
  - Endpoint support – Windows, Linux, Mac, consultants, guests, devices



INFOEXPRESS ,INC. - EX2486
CISCO SYSTEMS, INC. , et al. v. INFOEXPRESS, INC. [IPR2024-00675]

# Layering Policies Over the Network

- Ensure policy compliance across multiple network infrastructures
- Provide seamless administrative and end user experience

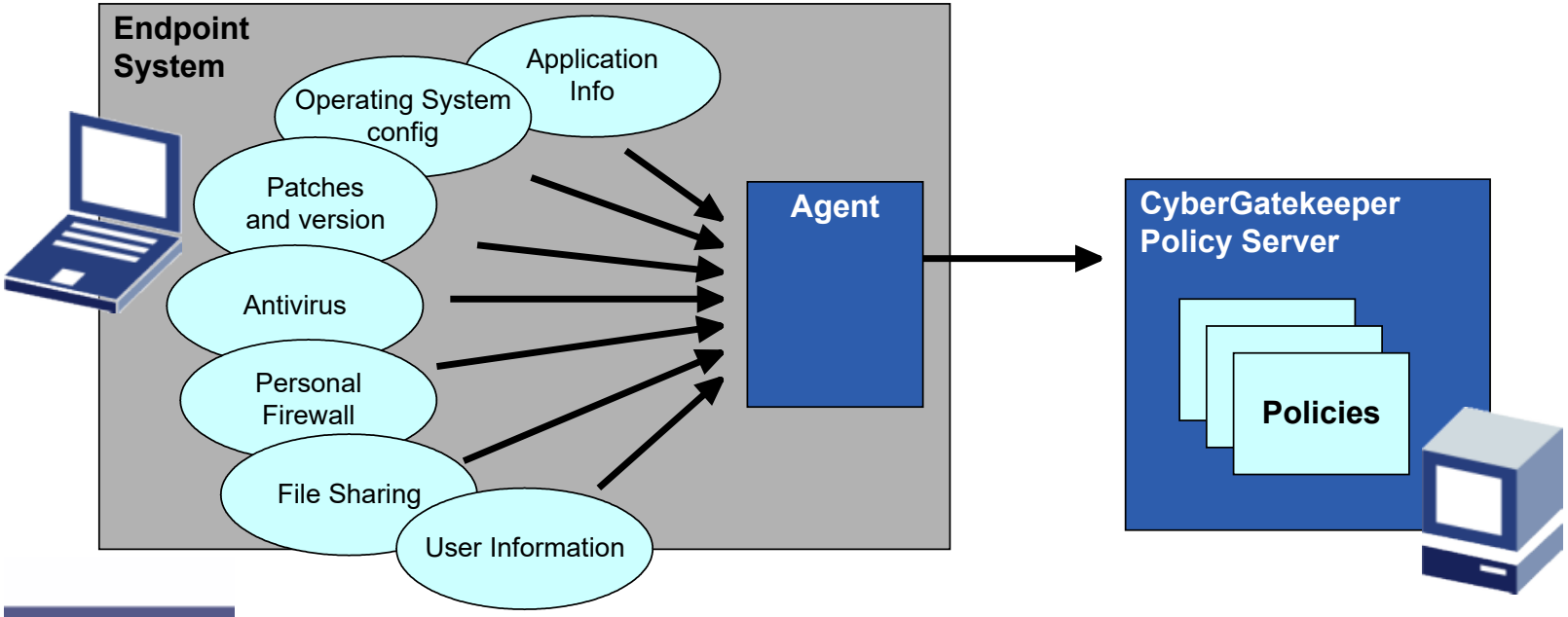



infoexpress

RSA Conference 2005

# Endpoint Auditing

- Endpoint - Check AV, OS, patches, file sharing, logon, custom apps, configurations, user information, groups.
- Assessment - Multiple policies for different OS and devices

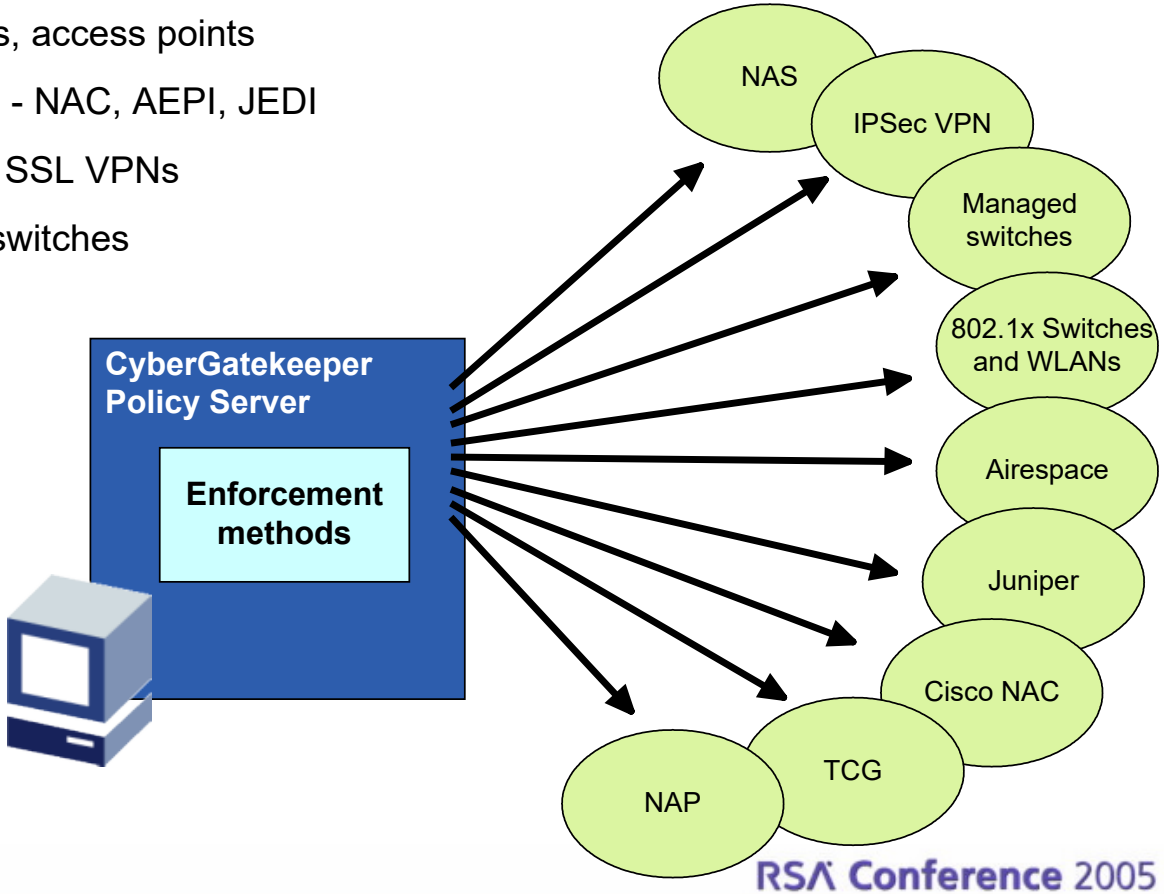



infoexpress

RSA Conference 2005

# Multi-vendor Network Enforcement

- Equipment and interfaces supported today
  - 802.1x – Switches, access points
  - Vendor interfaces - NAC, AEPI, JEDI
  - Gateway - VPNs, SSL VPNs
  - SNMP – Legacy switches
- Future interfaces
  - NAP, TCG, more gateways




infoexpress

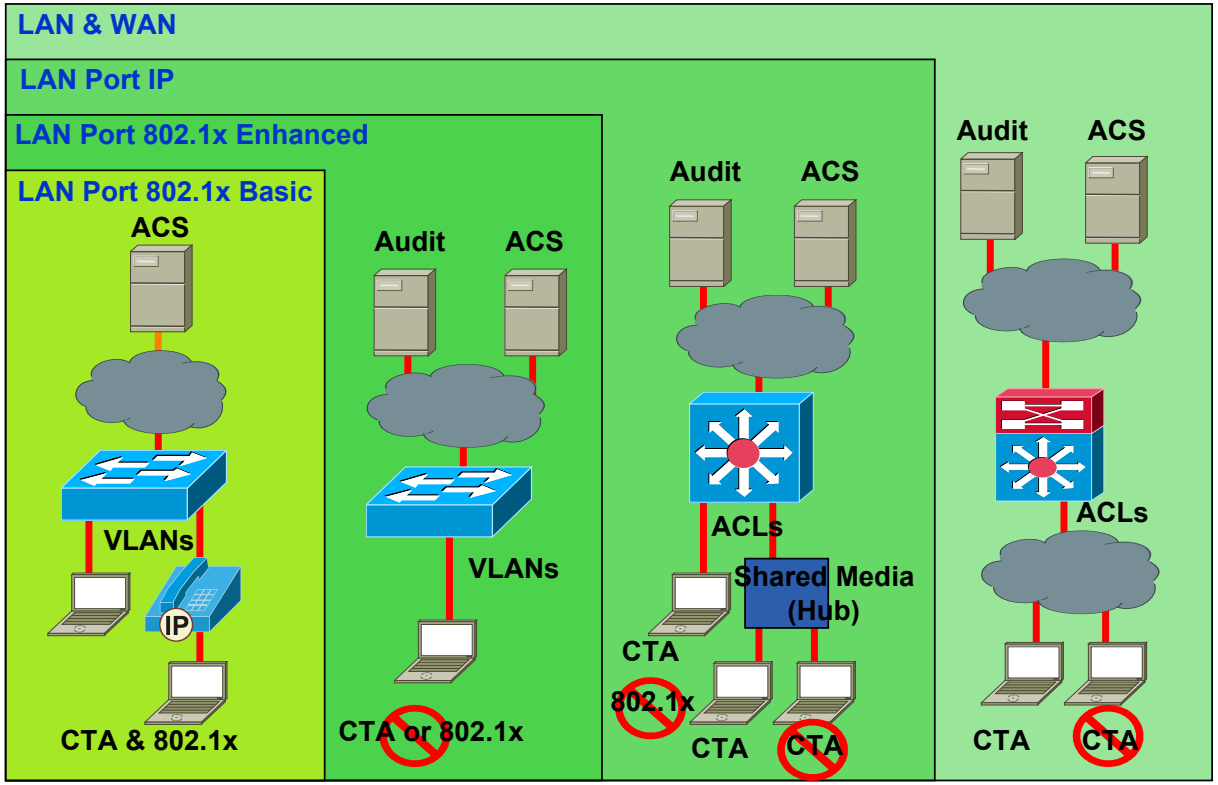
RSA Conference 2005

# Network Infrastructure Perspective: Cisco

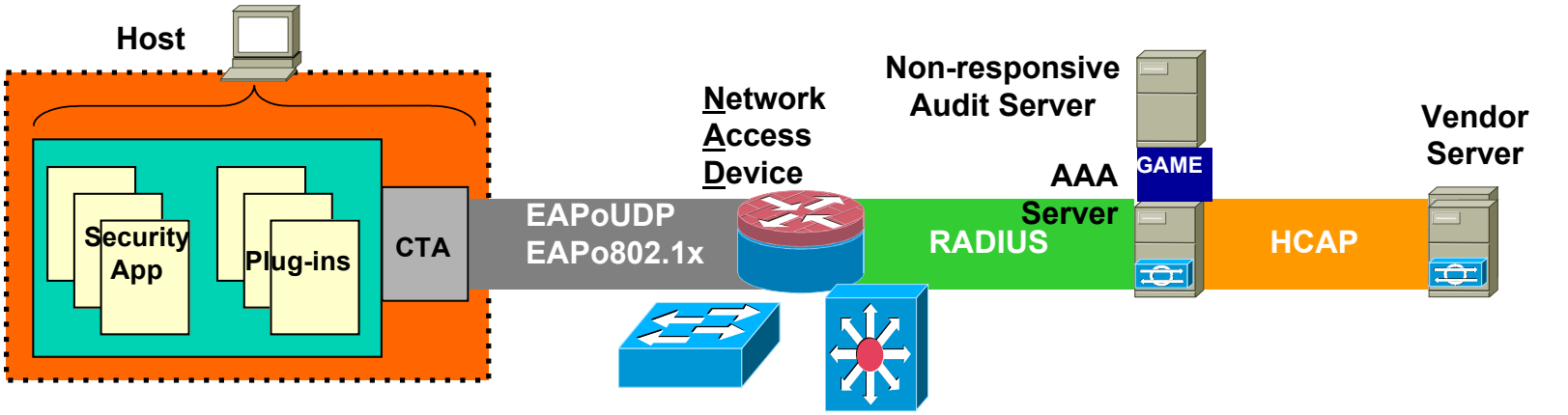
- **Discovery & enforcement must grant 100% visibility & control (*miss nothing*)**
  - Assess all endpoints: managed & unmanaged, anything with an IP address
  - Consistent approach regardless of endpoint ingress method
  - State collection demands IB & OOB "credential"/state gathering methods
- **Authorization ties to segmentation services (*"quarantine segment", "visitor segment"*)**
  - Leverage existing L2 & L3 methods: likely hybrid environments
  - Access layer adoption => network design implications ("trust zones")
- **Drives evolution of "related" technologies & tools (*we're not in Kansas anymore*)**
  - Entitlement control => identity of user ID, asset ID, state, behavior, location
  - OOB assessment => on-access (& ongoing) scanning, ties to entitlement
  - Network segmentation => VLAN, L3 segmentation, routing…
  - Remediation => patch & host management tools
  - Policy control => endpoint state checking & control, regulatory compliance…
- ***Basically, Scan & Block is AAA, with a broader notion of Authentication & Remediation***

# Switch Functional Deployment Scenarios

- LAN solution is the "golden child"
- LAN is hardest to solve, traditionally lacks chokepoints and pre-DHCP
- Must limit manual exception handling
- 802.1x is new & useful, but not enough
- Build "trust zones"



# NAC Logical Roles




**Subject**

- Offers ID & state
- Assist remediation
- Managed & unmanaged

**Policy Enforcement Point**

- Visibility & assessment trigger
- Authorization control

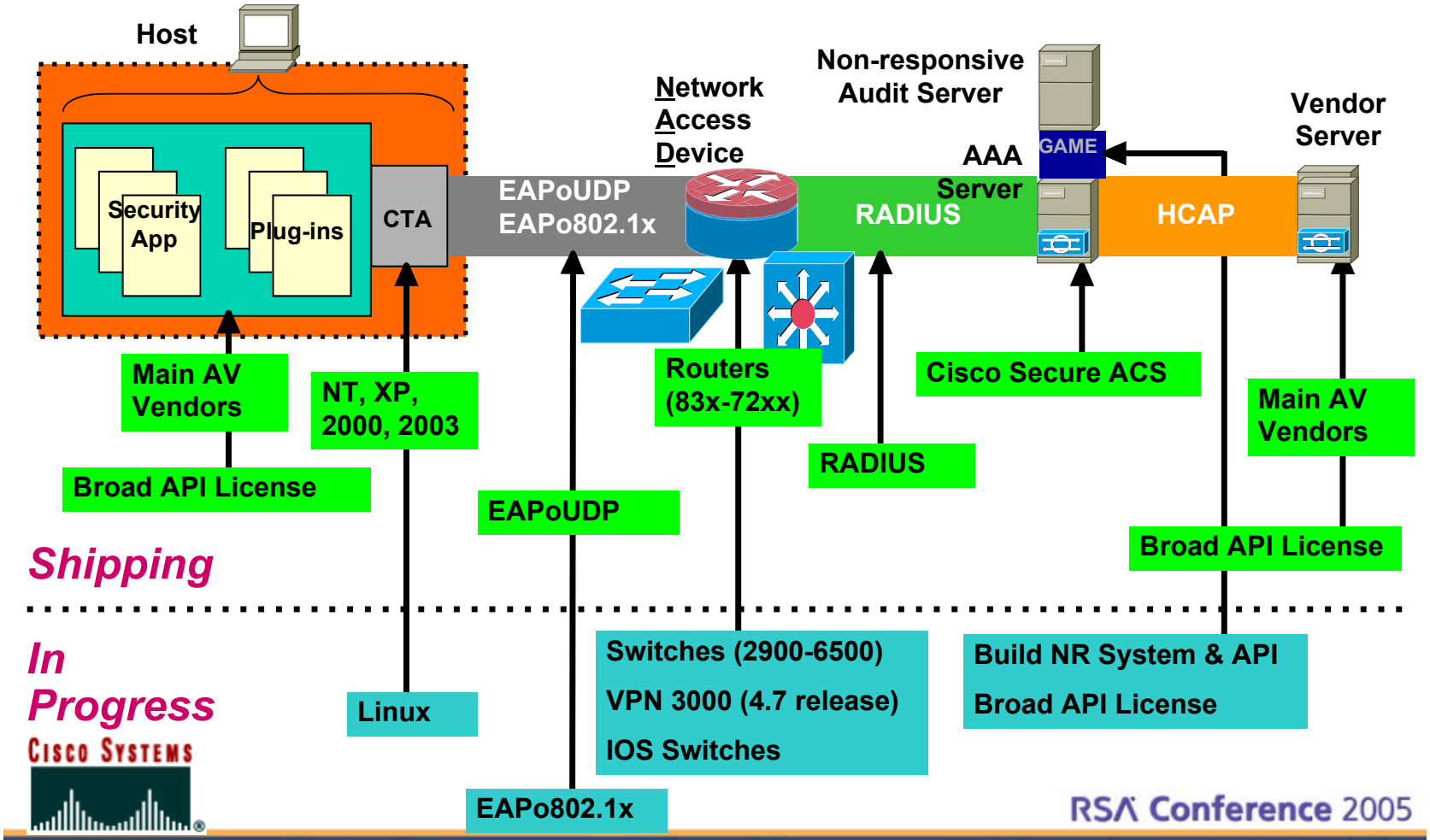
**Policy Decision Point**

- AAA function
- Remediation services
- Ties to many existing (and new) services/tools

CISCO SYSTEMS

RSA Conference 2005

# NAC Logical Components



# Protecting your Network: Scan and Block

- Panel participants
  - Phil Schacter, VP and Service Director, Burton Group
  - Scott Olson, SVP Marketing, WholeSecurity
  - Stacey Lum, CEO, InfoExpress
  - Russell Rice, Director Marketing, Cisco



INFOEXPRESS ,INC. - EX2486
CISCO SYSTEMS, INC. , et al. v. INFOEXPRESS, INC. [IPR2024-00675]

# Protecting your Network: Scan and Block

- Audience Q&A

- References and Links:
  - Burton Group www.burtongroup.com
  - Whole Security www.wholesecurity.com
  - InfoExpress www.infoexpress.com
  - Cisco's NAC Program http://www.cisco.com/go/nac



INFOEXPRESS ,INC. - EX2486
CISCO SYSTEMS, INC. , et al. v. INFOEXPRESS, INC. [IPR2024-00675]