

THE PRICE OF ADMISSION...

© 2009 Cisco Systems, Inc. All rights reserved. 1

Agenda

Cisco.com

- **The Myths of Endpoint Security**
- **The Endpoint Security Problem**
- **Compliance Enforcement as a Best Practice**
- **Standards and Initiatives**
- **Vendor Approaches in Market**
- **ROI with Endpoint Security Enforcement**

© 2009 Cisco Systems, Inc. All rights reserved. 2

Agenda

Cisco.com

- **The Myths of Endpoint Security**
- **The Endpoint Security Problem**
- **Compliance Enforcement as a Best Practice**
- **Standards and Initiatives**
- **Vendor Approaches in Market**
- **ROI with Endpoint Security Enforcement**

© 2009 Cisco Systems, Inc. All rights reserved. 3

Myth One

Cisco.com

"IT can and should restrict the types of users, endpoint platforms, and access technologies that may connect to the enterprise network."



© 2009 Cisco Systems, Inc. All rights reserved.

4

Myth Two

Cisco.com

"The traditional network security perimeter provides adequate protection against endpoint security threats."



© 2009 Cisco Systems, Inc. All rights reserved.

5

Myth Three

Cisco.com


"End-users can be trusted to follow best practices to maintain a secure endpoint environment."




© 2009 Cisco Systems, Inc. All rights reserved.

6

Myth Four Cisco.com




"We can wait until next year to worry about regulatory compliance issues."



© 2009 Cisco Systems, Inc. All rights reserved. 7

Myth Five Cisco.com



"If I keep my computing and network systems patched I'll avoid malware."

© 2009 Cisco Systems, Inc. All rights reserved. 8

Agenda Cisco.com

- The Myths of Endpoint Security
- **The Endpoint Security Problem**
- Compliance Enforcement as a Best Practice
- Standards and Initiatives
- Vendor Approaches in Market
- ROI with Endpoint Security Enforcement

© 2009 Cisco Systems, Inc. All rights reserved. 9

Yankee Group Recommendations

Cisco.com

- **Embrace the inevitable**
 - Your perimeter will get more porous
 - Attacks on endpoints will get more sophisticated
 - Your perimeter won't stop endpoint-borne attacks
 - You will have to **enforce endpoint security policy**
- **Don't wait too long to act**
 - Regulatory issues, rogue threats are here **now**



© 2009 Cisco Systems, Inc. All rights reserved.

10

Enterprise Perimeter – Extended and Diluted

Cisco.com

- Weak security practices and enforcement for dynamic workforce
- “Easy access” at odds with “secure network”
- Persistent security vulnerabilities on complex endpoints

“Re-infection from worms, viruses and trojans are most often caused by remote users who have not protected their machines with the most up-to-date security patches and signatures.”

Endpoint Security Management, Maximizing Best-of-Breed, IDC, 2004

WORST OUTBREAKS EVER

Name, Year	Worldwide Impact*
1. Love Bug , 2000	\$8.75 billion Hopelessly lonely recipients think they are getting a real love letter in their e-mail.
2. MyDoom , 2004	\$4.75 billion At its peak, infects one in 12 e-mails on the Internet.
3. Sasser , 2004	\$3.5 billion German cybercop nab its teenage author, Sven Jaschan. An IT security firm then offers him a job.
4. NetSky , 2004	\$2.75 billion One of its variants disguises itself as a Harry Potter computer game.
5. SoBig , 2000	\$2.75 billion Hits a week after Blaster (No. 8), helping cause a summer of pain for computer users and Microsoft.

* Estimated cost to corporations

SOURCE: FORTUNE, October 19, 2004

© 2009 Cisco Systems, Inc. All rights reserved.

11

Agenda

Cisco.com

- The Myths of Endpoint Security
- The Endpoint Security Problem
- Compliance Enforcement as a Best Practice
- Standards and Initiatives
- Vendor Approaches in Market
- ROI with Endpoint Security Enforcement

© 2009 Cisco Systems, Inc. All rights reserved.

12

There's Got To Be A Better Way

Cisco.com

- New approach to meet coordinated, automated threats
- Assess, achieve, and report on security policy compliance
- Coordinated enforcement of OS security patches, security applications, and endpoint configuration

"By the first quarter of 2005, enterprises that don't enforce security policies during network login will experience 200% more network downtime than those that do."

Scan, Block and Quarantine to Survive Worm Attacks, Gartner Group, 2004

© 2005 Cisco Systems, Inc. All rights reserved.

13

Rogue Devices

Contractors / Vendors / Customers / Students / Outsiders

Cisco.com

• ISSUE:

Inability to control network admission exposes significant risk

Accidental or malicious in nature

May lead to network downtime or exposure of sensitive information

• SOLUTION:

Allow only authorized devices onto the network

Provide enforcement by leveraging existing network infrastructure

Maximize existing hardware and software investments

Enable an easy path to emerging enforcement technologies

© 2005 Cisco Systems, Inc. All rights reserved.

14

Mobile Users

Home Workers / VPN

Cisco.com

• ISSUE:

Trusted User but Untrusted Device Problem

VPN secures the path, but the endpoint device exposes risk

Intruders and malware can enter the corporate network through compromised VPN endpoints

• SOLUTION:

Prior to network admission assure that even untrusted devices comply with corporate policy

Fill the missing link: assesses endpoint security software before gaining access

Leverages existing investments

Enable flexible machine utilization (home, privately-owned)

© 2005 Cisco Systems, Inc. All rights reserved.

15

LAN Desktops
Devices with Persistent Connectivity

Cisco.com

- **ISSUE:**
 - Numerous difficult to manage devices in an unknown state present significant risk
 - May be an entrance vector for intruders and malware
 - Facilitates rapid re-infections making clean-up extremely difficult
- **SOLUTION:**
 - Prior to network admission assure that all devices comply with corporate policy
 - Continuous re-evaluation to ensure devices comply with policy
 - Leverage existing investments with minimal network changes
 - Enable an easy implementation path to emerging enforcement technologies

© 2005 Cisco Systems, Inc. All rights reserved. 16

Agenda

Cisco.com

- The Myths of Endpoint Security
- The Endpoint Security Problem
- Compliance Enforcement as a Best Practice
- **Standards and Initiatives**
- Vendor Approaches in Market
- ROI with Endpoint Security Enforcement

© 2005 Cisco Systems, Inc. All rights reserved. 17

Evolving Market Standards and Initiatives

Cisco.com

- **IEEE 802.1X Standard**
 - Low-level network protocol
 - Enables VLAN-based enforcement & quarantine in switches and wireless access points
 - Available today in modern network gear from all major vendors
- **Cisco Network Admission Control (NAC) Program**
 - API-level enforcement & quarantine technology being built into Cisco network infrastructure
 - Available in phases through 2005
 - Multiple vendors in program announcing support for program

© 2005 Cisco Systems, Inc. All rights reserved. 18

Evolving Market Standards and Initiatives

Cisco.com

- **Microsoft Network Access Protection (NAP)**
 - API-level enforcement & quarantine technology in Microsoft Windows Operating Systems
 - Available in Longhorn, 2007 (4Q 2005 Beta)
 - Multiple vendors in program announcing support
- **Trusted Computing Group (TCG)**
 - Creating TNC (Trusted Network Connect) Standard
 - Multiple API-level interfaces
 - Very early stages

© 2005 Cisco Systems, Inc. All rights reserved.

19

Enforcement Alternatives

Cisco.com

	Appliance	ActiveX / Java	Agent
Assessment	Client Log-in	Downloadable ActiveX control	Endpoint Agent
Quarantine	Proprietary VLAN	SSL Gateway	Industry Standard RADIUS, 802.1x
Industry Perspective	Point Solution	Point Solution	Cisco NAC Microsoft NAP Trusted Computing Group
Supported Use Cases	SMB LAN	SSL VPN	Road Warrior Weekend Warrior LAN Dweller Rogue

© 2005 Cisco Systems, Inc. All rights reserved.

20

Agenda

Cisco.com

- The Myths of Endpoint Security
- The Endpoint Security Problem
- Compliance Enforcement as a Best Practice
- Standards and Initiatives
- Vendor Approaches in Market
- ROI with Endpoint Security Enforcement

© 2005 Cisco Systems, Inc. All rights reserved.

21

Cisco Network Admission Control (NAC)

<http://www.cisco.com/en/US/partners/pr46/naac/partners.html>

Cisco.com

ANTI VIRUS

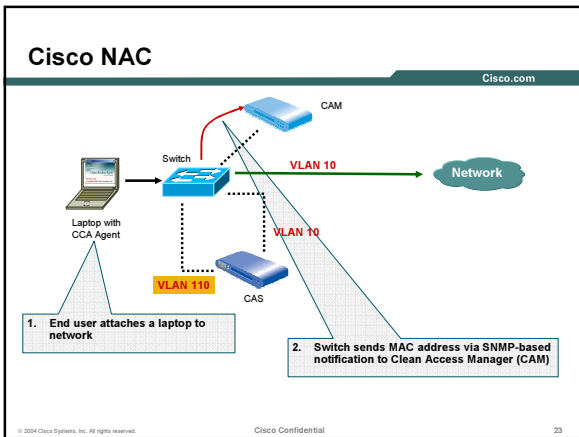
- McAfee, Symantec, Trend Micro, IBM, Altriris
- AhnLab, CA, 金山在线, BIGFIX, Altiris
- F-Secure, Norman, Sophos, Panda, LANDesk, iPass, PatchLink

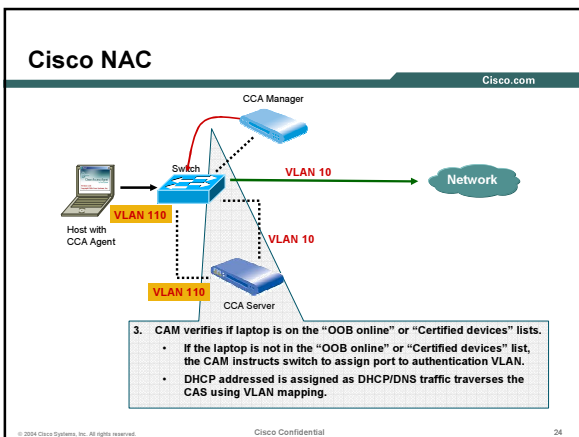
REMEDATION

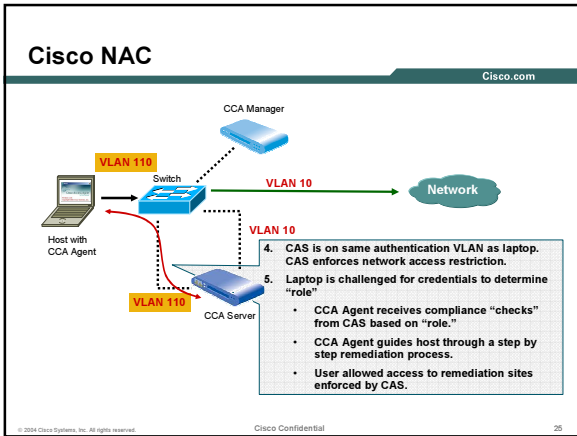
- Secure Elements, Belarc, Citadel, Netcordia, OFSWAT, Secure Elements
- Credant, New Boundary, PredatorWatch, Senforce
- Infoexpress, Endforce, Phoenix, Stiisecure
- BlueLight Networks, Preventsys, TriGeo, Sygate, Safend, BullSecurity
- GuardedNet

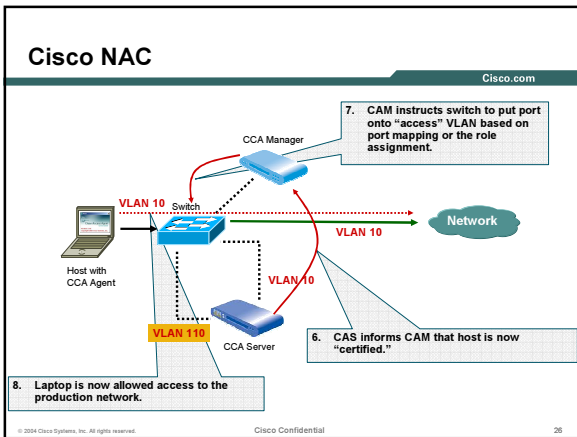
CLIENT SECURITY

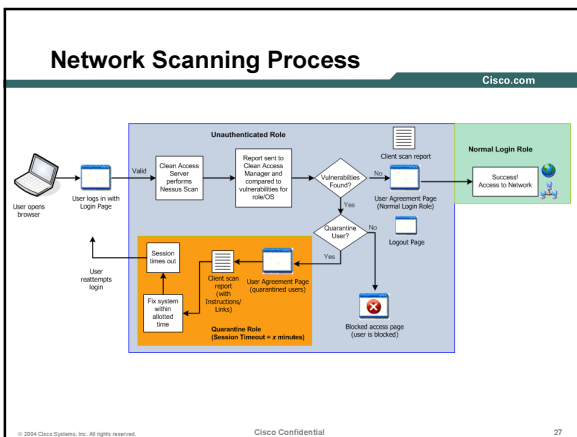
© 2004 Cisco Systems, Inc. All rights reserved. Cisco Confidential 22









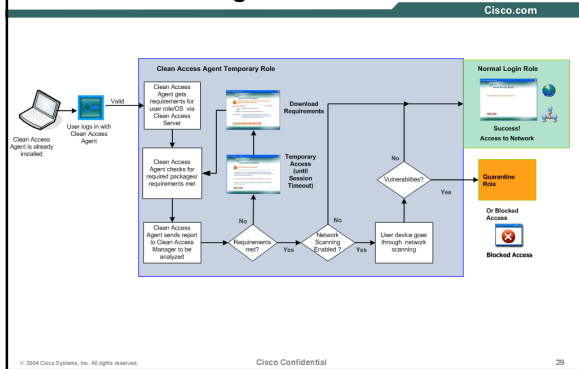


End User Experience: Web-based

Cisco.com

Cisco Confidential 28

Clean Access Agent Process



End User Experience: with Agent

Cisco.com

Cisco Confidential 30

Microsoft / Cisco Joint Announcement

October 18, 2004

Cisco.com



Cisco and Microsoft Team to Improve Network Security

Companies will work toward compatibility, interoperability of respective security architectures

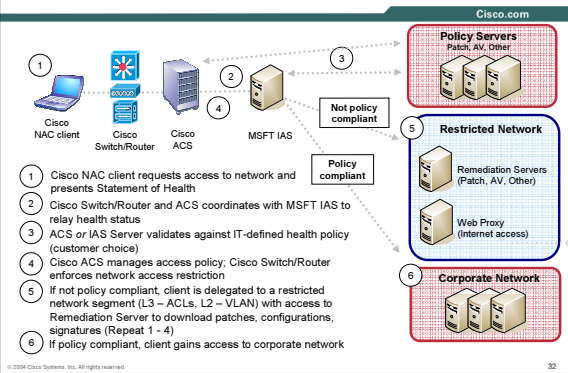
This month the two companies announced they will work together to ensure compatibility and develop interoperability between their respective security architectures. For Cisco this collaboration further demonstrates the company's commitment to reinventing network security.

Interoperability Integration Standardization

© 2004 Cisco Systems, Inc. All rights reserved.

31

NAC & NAP Collaboration Concept





Windows Server Roadmap Update

Windows Server Security Updates

- SP1
 - New features like Security Configuration Wizard drawing raves from users
- New wave of security guidance now available for Windows Server and XP SP2
- Windows Update Services
 - Beta in November
- Network Access Protection
 - VPN Quarantine in Windows Server 2003 SP1 & R2
 - Industry partnership momentum continues

 Windows Server System

Microsoft – Cisco NAP Collaboration

- Long-term agreement to share plans and integrate network security and health assurance technologies around Microsoft's Network Access Protection (NAP) and Cisco's Network Admissions Control (NAC)
- Benefit is that mutual customers will be able to better address the increased threat and impact malicious software
- Cisco and Microsoft will collaborate on three key deliverables:
 - Ensure compatibility between Cisco NAC and Microsoft NAP
 - Drive interoperability efforts between their two architectures as these solutions evolve and are delivered to customers
 - Lead industry standards in the network admissions and access control arenas to help promote broad market adoption and integration with industry leading ISV solutions.
- Gives customers what they've asked us for: a more integrated Cisco/Windows solution

 Windows Server System

Agenda

Cisco.com

- The Myths of Endpoint Security
- The Endpoint Security Problem
- Compliance Enforcement as a Best Practice
- Standards and Initiatives
- Vendor Approaches in Market
- ROI with Endpoint Security Enforcement

© 2009 Cisco Systems, Inc. All rights reserved.

36

What To Expect In A Solution

Cisco.com

- **Maximize Current Security and Network Investments**
 - Vendor neutral architecture that provides the ability to work with current Network Infrastructure and Endpoint Security Elements
 - Minimal (if any) network changes
 - Avoids technology "lock in" as networks change and evolve
- **Low Total Cost of Ownership**
 - Low Administrative Overhead – Easy to implement and maintain
 - Centralized definition, management and reporting of enforcement and quarantine policy
- **Support Multiple Enforcement Mechanisms**
 - Supports Migration to Industry Standards When Available (NAC, NAP, TCG, Etc.)
 - Remote and LAN Based – IPSec VPN, SSL VPN, Dial, 802.1X, DHCP, and Client

© 2009 Cisco Systems, Inc. All rights reserved.

27

Where is the ROI ?

Cisco.com

- Maximize ROI on existing patch management, anti-virus, personal firewall and network infrastructure elements
- Lower costs of remediating and patching infected endpoints
- Lower costs of network infection by immediately responding to new virus and worm attacks
- Increases workforce productivity through safe and secure remote access to networks through VPN and Wireless access
- Increase security of the network and corporate information and resources
- Increase compliance with IT governance regulations

© 2009 Cisco Systems, Inc. All rights reserved.

28

Q and A



© 2009 Cisco Systems, Inc. All rights reserved.

29
