



Securing Complexity with Cisco NAC Appliance (Clean Access)

Cisco NAC Appliance Team
June 2006

Agenda

- **Securing Complexity**
- **Cisco Network Admission Control (NAC) Solutions**
- **NAC Appliance Product Overview**
- **NAC Appliance Values to Business**



The Challenge of Securing Complexity

This is a story about network security.



**Specifically, how you can have
without compromising productivity.**



security

**More to the point, your company may already be
bristling with network defenses, but you still have
one glaring vulnerability—**your network users.****



Productivity Causes Complexity

- **What system is it?**
- **Who owns it?**
- **Where is it coming from?**
- **What's on it? Is it running?**
- **What's the preferred way to check/fix it?**

- Windows, Mac or Linux
- Laptop or desktop or PDA
- Printer or other corporate asset
- Company
- Employee
- Contractor
- Guest
- Unknown
- VPN
- LAN
- WLAN
- WAN
- Anti-virus, anti-spyware
- Personal firewall
- Patching tools
- Pre-configured checks
- Customized checks
- Self-remediation or auto-remediation
- Third-party software



Complexity Demands Defense-in-Depth

Endpoint Security

Anti-spyware
HIPS
Personal
Firewalls
Anti-virus



Endpoint security alone fails:

99% have AV, but infections persist!
Host based apps are easily manipulated—even unintentionally
Time gap between virus and virus def/repair

Identity

AAA
Guest access
Employee



Identity alone fails:

Protects against unauthorized access, but not malware
Identifies user, but not device

Network Security

IDS/IPS
VPNs
Perimeter
Firewalls



Network security alone fails:

Firewalls cannot block legitimate ports
VPNs cannot block legitimate users
Malware signatures must be known
Detection often occurs after-the-fact

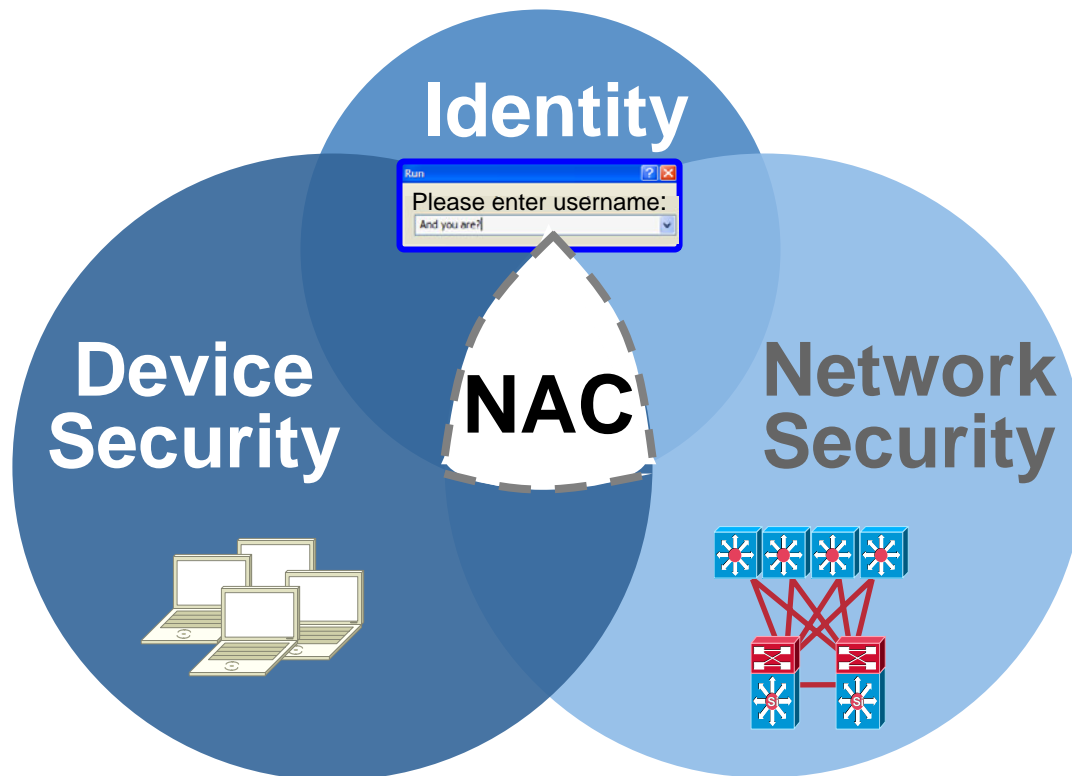
Agenda

- **Securing Complexity**
- **Cisco Network Admission Control (NAC) Solutions**
- **NAC Appliance Product Overview**
- **NAC Appliance Values to Business**



What Is Network Admission Control?

Using the network to enforce policies ensures that incoming devices are compliant.



Four Key Capabilities of NAC

	Securely Identify Device and User	Enforce Consistent Policy	Quarantine and Remediate	Configure and Manage
What it means	Uniquely identifies users and devices, and creates associations between the two	Assess and enforce a ubiquitous policy across the entire network	Acts on posture assessment results, isolates device, and brings it into compliance	Easily creates comprehensive, granular policies that map quickly to user groups and roles
Without it . . .	Critical to associate users and devices with roles to know which policies apply; prevents device spoofing.	A decentralized policy mechanism (e.g. on endpoint) can leave gaping security holes.	Just knowing a device is non-compliant is not enough—someone still needs to fix it.	Policies that are too complex or difficult to create and use will lead to abandonment of project.

A robust NAC solution must have all four capabilities.

Before We Continue, You May Be Asking ...

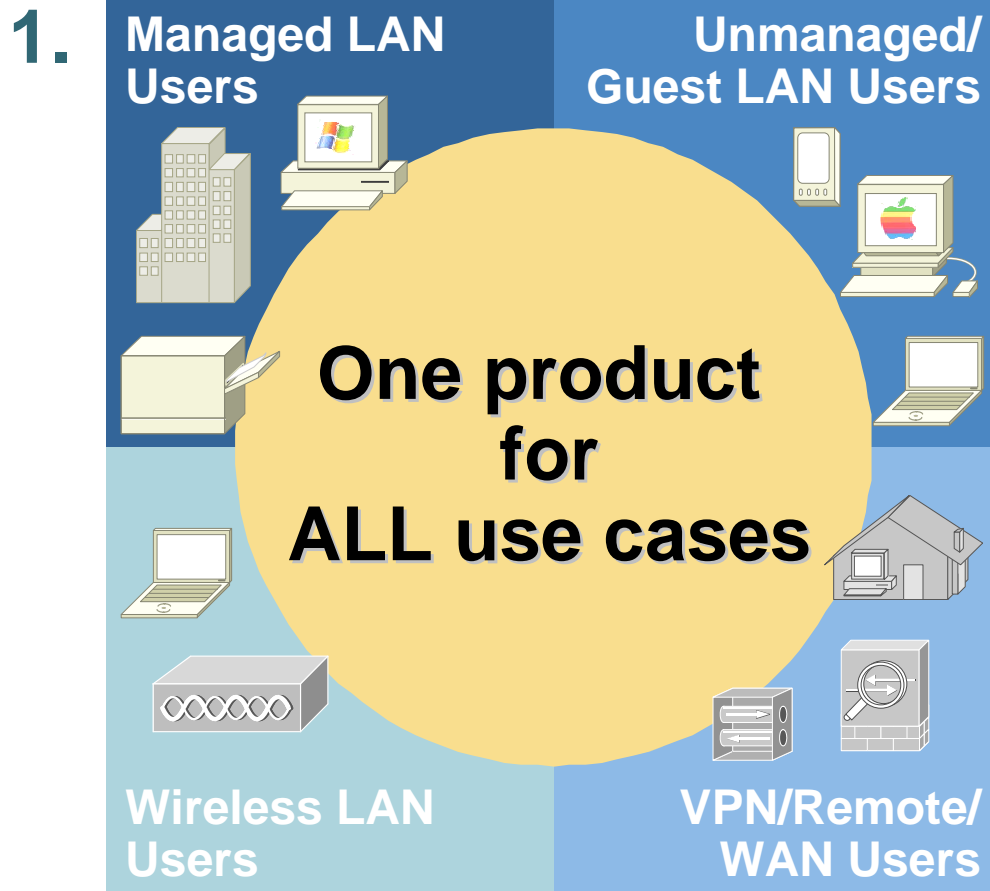
- **Do I need separate solutions for my VPN users, my LAN users, my unmanaged users?**
- **Am I your guinea pig? What's your experience in deploying NAC?**
- **Is this going to take months to deploy?**
- **How can I be sure that this solution will fit MY situation?**
- **Do I need to upgrade my entire infrastructure?**

Agenda

- **Securing Complexity**
- **Cisco Network Admission Control (NAC) Solutions**
- **NAC Appliance Product Overview**
- **NAC Appliance Values to Business**



The Cisco NAC Appliance Advantage



- 2.** 600+ customers across all use cases: No. 1 NAC solution
- 3.** Most deployments ready under 5 days
- 4.** Scales from 100 users to 100,000+ user, across 150+ locations
- 5.** Does not require infrastructure upgrade

NAC Appliance Enforces Compliance

**Who's on?
What's on?**

**What are the
requirements
for access?**

**What are the
steps to meet
requirements?**

**How do I create
or modify
requirements?**

Securely Identify Device and User

**Authenticates and
authorizes users
(local db, RADIUS,
LDAP, Kerberos, AD,
etc.)**

**Supports all access
methods (LAN,
wireless,
remote/VPN, WAN)**

Enforce Consistent Policies

**Centralized policy
supports multiple
user roles**

**Scans for infections,
port vulnerabilities,
hotfixes, AV, AS,
services running,
and files**

Quarantine and Remediate

**Isolates non-
compliant devices
using MAC and IP
addresses; effective
at a **per-user** level**

**Network-based, self-
guided remediation**

Helpdesk integration

Configure and Manage

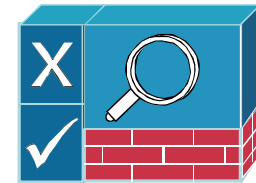
**Pre-configured
checks simplify
policy configuration
and rule creation**

**Web-based interface
for easy
management of
roles, policies, and
remediation steps**

NAC Appliance (formerly known as Clean Access) Components

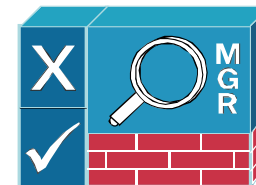
- **Cisco Clean Access Server**

Serves as an in-band or out-of-band device for network access control



- **Cisco Clean Access Manager**

Centralizes management for administrators, support personnel, and operators



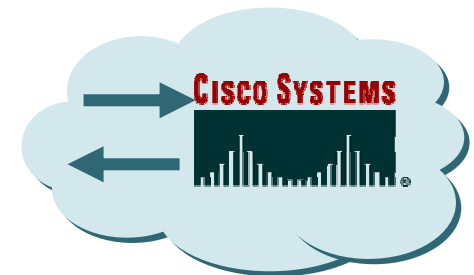
- **Cisco Clean Access Agent**

Optional lightweight client for device-based registry scans in unmanaged environments



- **Rule-set Updates**

Scheduled automatic updates for anti-virus, critical hot-fixes and other applications



Sampling of Pre-Configured Checks

Critical Windows Updates

Windows XP, Windows 2000,
Windows 98, Windows ME



Anti-Virus Updates



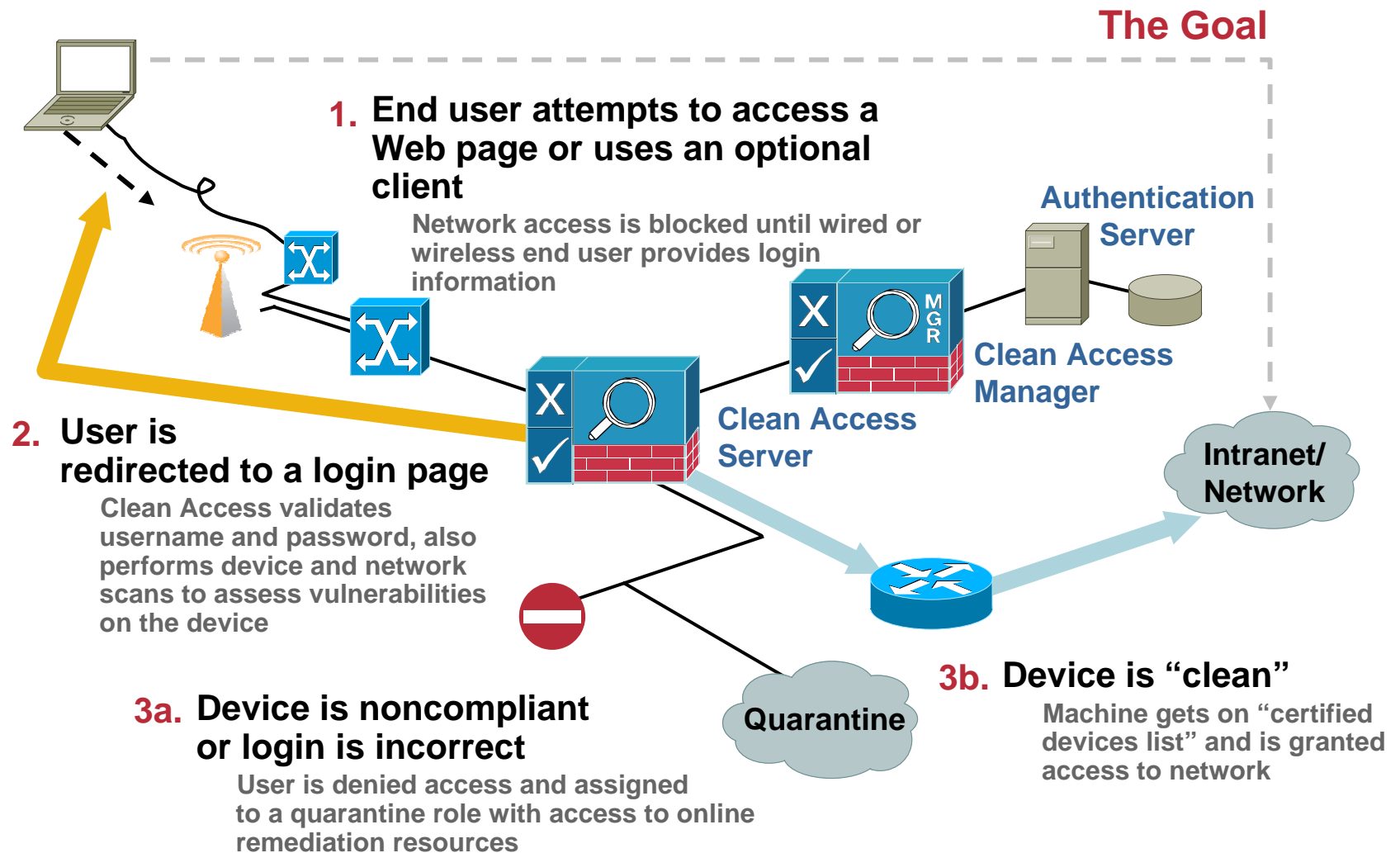
Anti-Spyware Updates

Other 3rd Party Checks



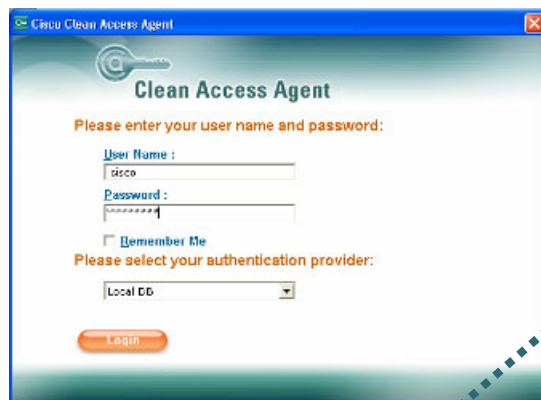
Customers can easily add customized checks

Product User Flow Overview



User Experience with Agent

Login Screen



Cisco Clean Access Agent

Clean Access Agent

Please enter your user name and password:

User Name :

Password :

☐ Remember Me

Please select your authentication provider:

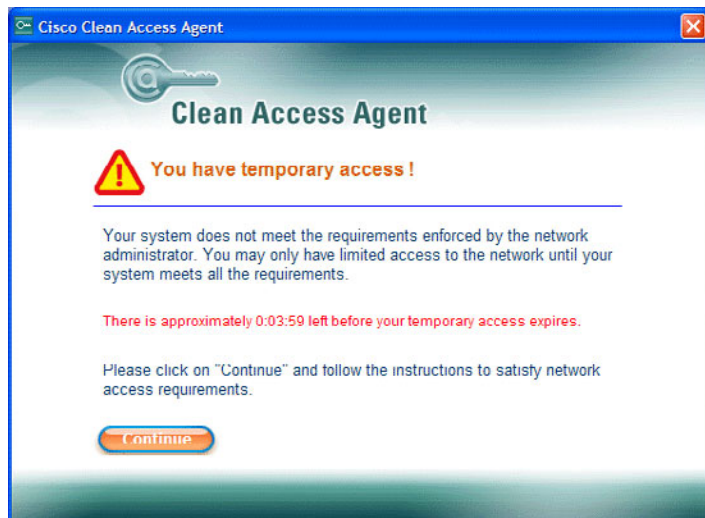
Local DB

Login

Scan is performed
(types of checks depend on user role)

Scan fails

Remediate



Cisco Clean Access Agent

Clean Access Agent

! You have temporary access !

Your system does not meet the requirements enforced by the network administrator. You may only have limited access to the network until your system meets all the requirements.

There is approximately 0:03:59 left before your temporary access expires.

Please click on "Continue" and follow the instructions to satisfy network access requirements.

Continue



Cisco Clean Access Agent

Clean Access Agent

! Please download and install the required software before accessing the network.

Required Software (0:03:10 left)

Name : Anti-Spyware (Optional) Software

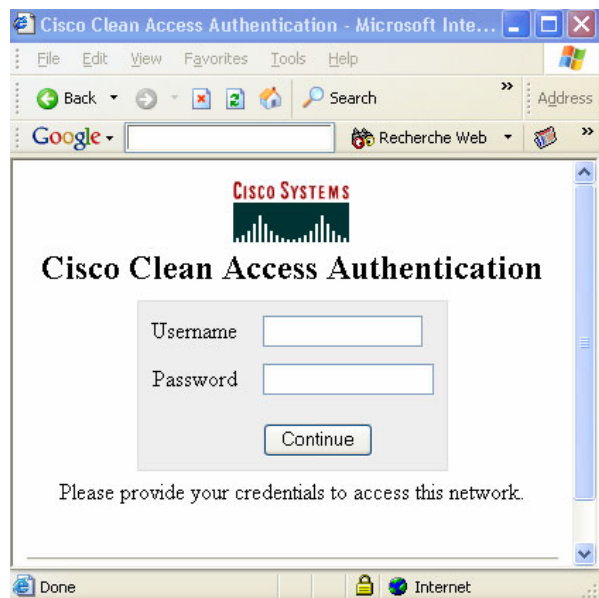
Version :

Location : <http://www.lavasoft.com/support/download/>

Description : Our security policy recommends that you download an anti-spyware program. Click Go To Link to download a free Anti-Spyware program or click Next to skip.

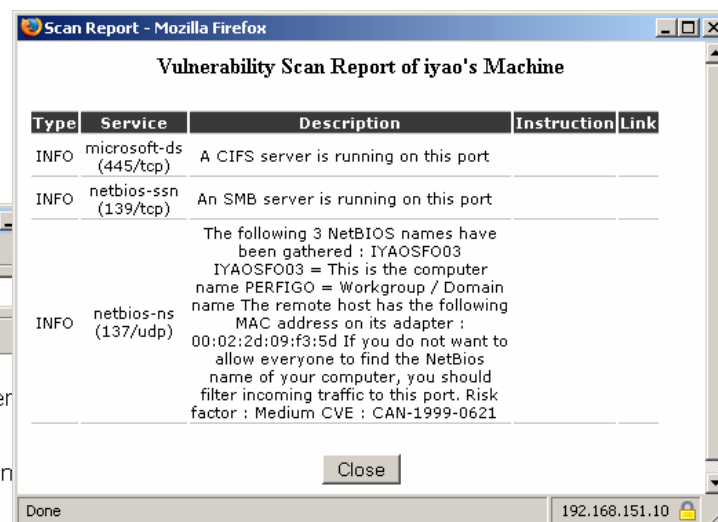
Go To Link Next Cancel

User Experience via Web Browser



Login
Screen

Scan is performed
(types of checks depend on user role/OS)



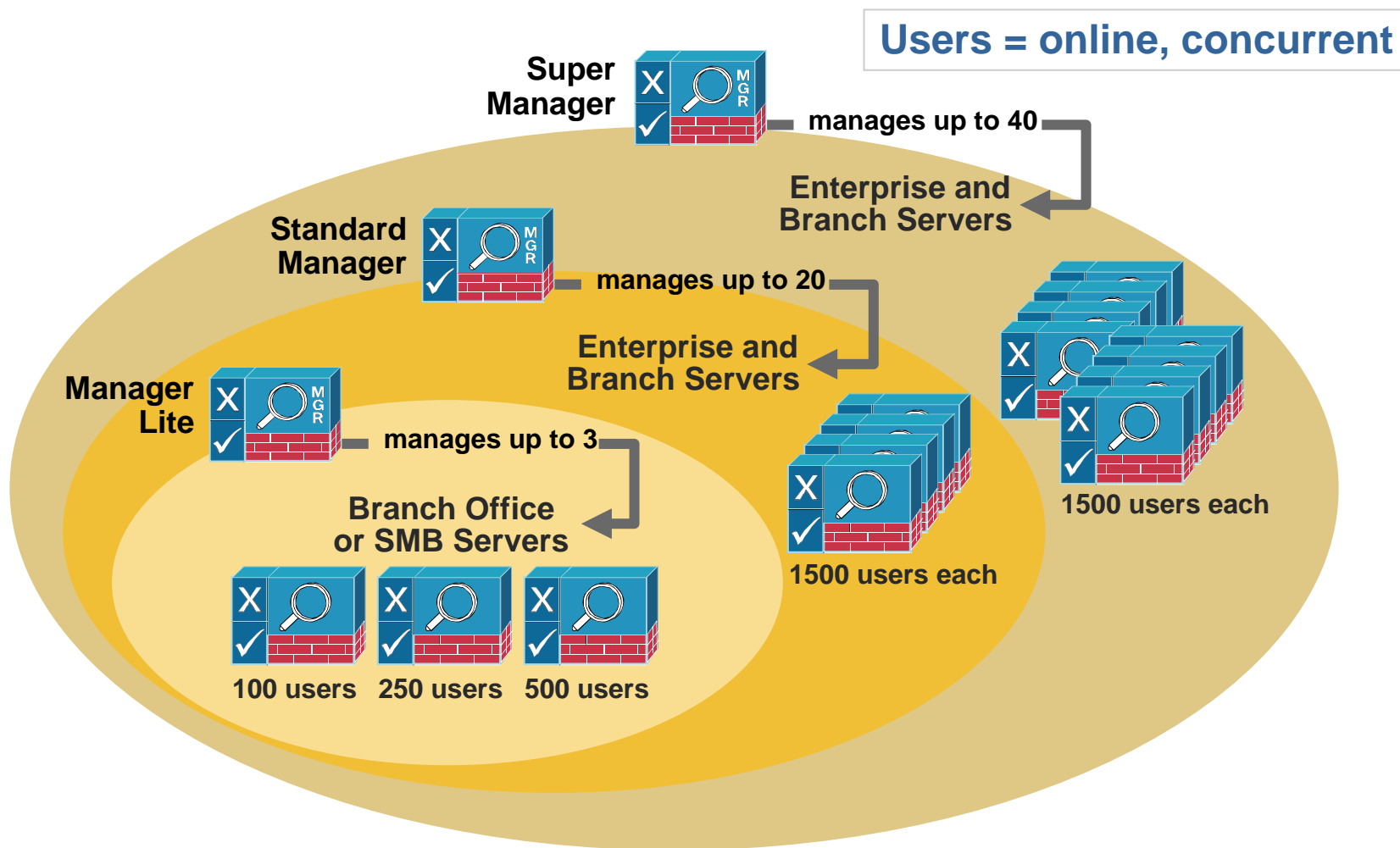
Note that all existing anti-virus software should be removed from your computer before installing the Anti-Virus software. For complete installation instructions, see the How-To document.

The ITS Support Center will be delighted to answer any questions you have about the procedure. Contact

Accept Decline

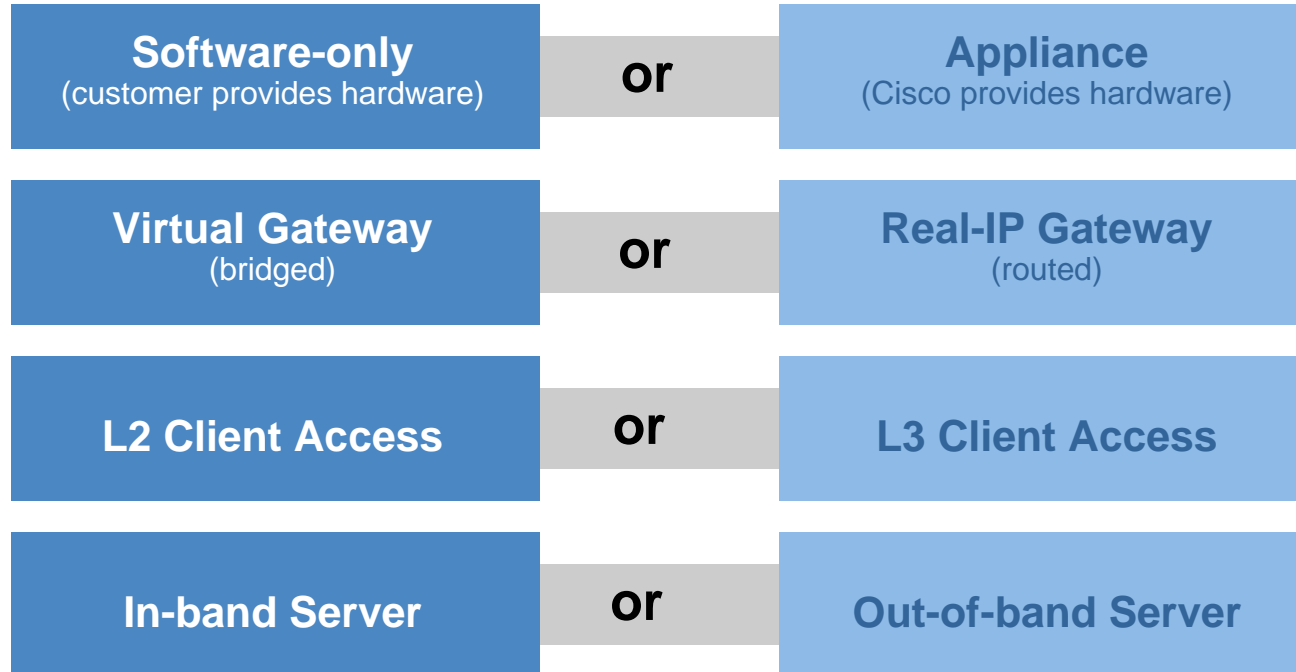
Guided self-remediation

NAC Appliance Sizing



NAC Appliance Options

Customers can choose from a variety of product and deployment options to tailor NAC Appliance for individual networks



Agenda

- **Securing Complexity**
- **Cisco Network Admission Control (NAC) Solutions**
- **NAC Appliance Product Overview**
- **NAC Appliance Values to Business**



NAC Appliance Top Values to Business

Proven Product

With 500+ deployments, we understand both the technical—and organizational—impact on your business

Complete Solution

NAC Appliance is self-contained, rapidly-deployable, and possesses all 4 key NAC capabilities

Flexible Deployment

The wide breadth of NAC Appliance deployment options fits your network—not the other way around

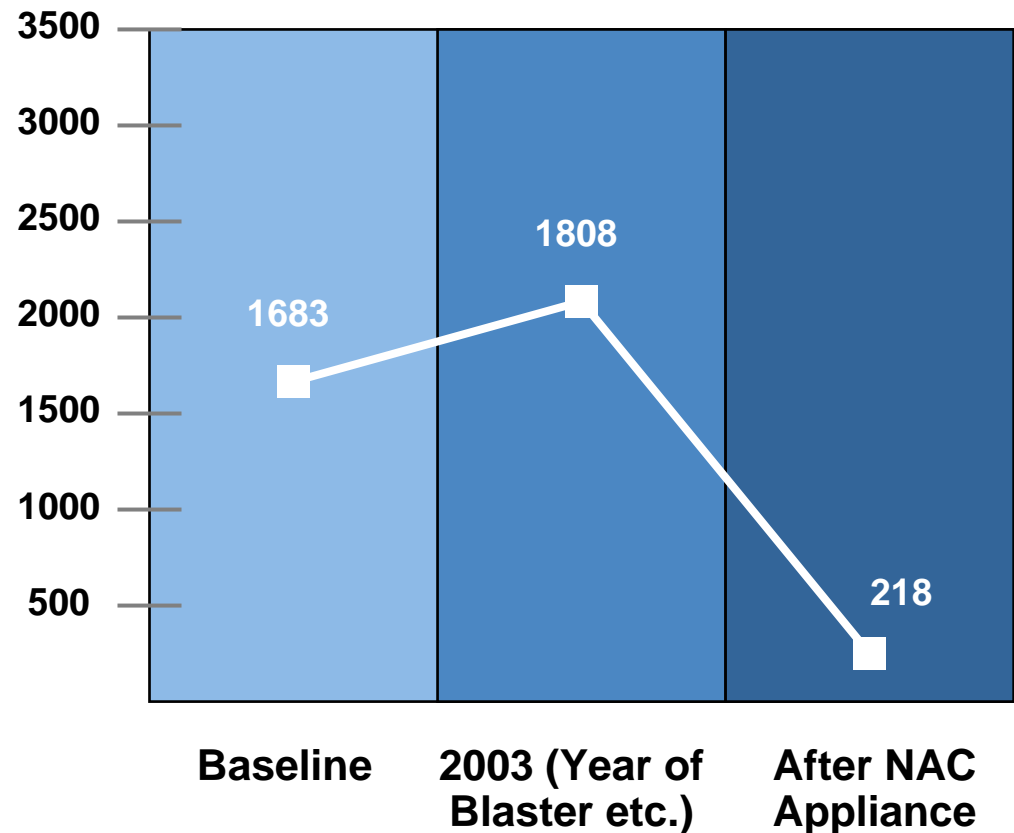
Future Proof

NAC Appliance is core to Cisco's strategic NAC vision and can be leveraged across all future deployment options

Customer Return on Investment

Average number of infected computers requiring help desk intervention per year, as reported by customers.

Assuming \$200 per intervention cost, average savings = \$318,000



Source: Customer reports, average customer size = 5,000 users

Q and A



CISCO SYSTEMS

