Cisco Tech Update
Security
Februar 2009

Christian Heinel – Systems Engineer

Rasmus Kamper Mathiasen – Systems Engineer

Agenda

- Cisco Security Strategy Moving Forward
- New Features in ASA, IPS and NAC
- Pause – 15 min
- Cisco Spam & Virus Blocker
- ACS
- CSA 6.0 1 Day Install
- Pause – 15 min
- CSA Live Demo

Agenda

- Cisco Security Strategy Moving Forward
- New Features in ASA, IPS and NAC
- Pause – 15 min
- Cisco Spam & Virus Blocker
- ACS
- CSA 6.0 1 Day Install
- Pause – 15 min
- CSA Live Demo

The Challenge Today

Countervailing Forces

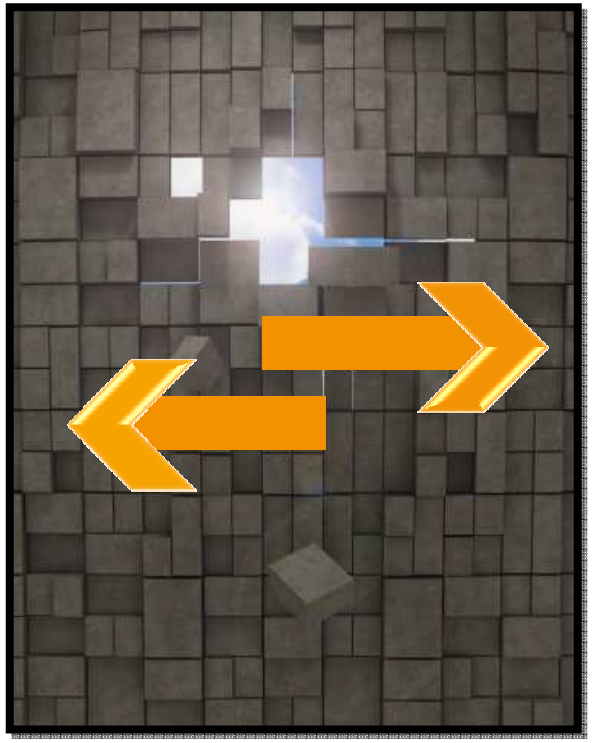
Globalization

Mobility

Collaboration

salesforce.com

Enterprise SaaS



Threats

Acceptable Use

Data Loss

Cisco Security Intelligence Operations

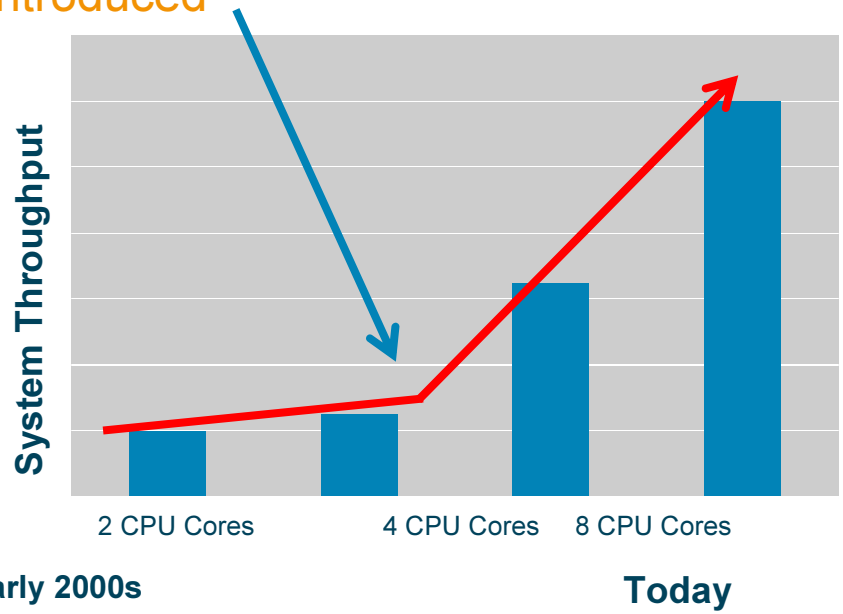
Security in every location

Security in every form factor

Appliance **Security Module** **Security Software**

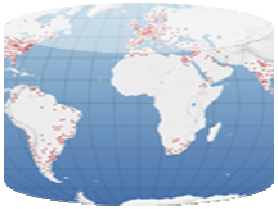
Fast and Accurate

Multi-Core Processors Introduced



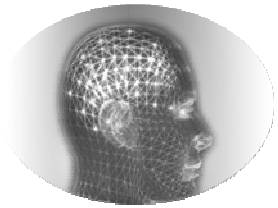
Cisco Threat Operation Center

SensorBase Network



World's largest real-time traffic monitoring network

Security Modeling & Research



Sophisticated algorithms and actionable alerts

Threat Analysts

500 analysts, 5 global locations, Cisco Fellow, 80+ with PhDs or a Cisco certification

Cisco Security Products Overview

Comprehensive Security, Flexible Delivery

Application Level ⟷ Network Level

Data Center / Campus

ACE Web App Firewall

Network Admission Control

IPS 4200

FWSM

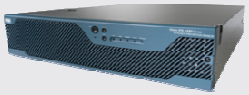
ASA 5500

Corporate HQ

Cisco IronPort C-Series

Cisco IronPort S-Series

IPS 4200



ASA 5500

Branch Office

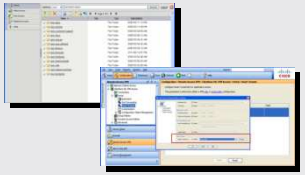
Cisco IronPort S-Series

ISR

ASA 5500

Teleworker

Clientless Network Access



Cisco AnyConnect VPN Client

Cisco Security Intelligence Operations

Centralized Management

Agenda

- Cisco Security Strategy Moving Forward
- New Features in ASA, IPS and NAC
- Pause – 15 min
- Cisco Spam & Virus Blocker
- ACS
- CSA 6.0 1 Day Install
- Pause – 15 min
- CSA Live Demo

AnyConnect Mobile

AnyConnect 2.3

- Windows Mobile 6.1, 6.0, 5.0
- Touch screen devices
- Secure remote access to enterprise applications from Windows Mobile

Enterprise VPN application access from Windows Mobile

Benefit

Apple iPhone VPN

Tunneling (Apple iPhone)

- Apple iPhone & iPod touch compatible
- Secure remote access to enterprise applications
- IPsec tunneling

Business Continuity Licenses

ASA 8.0.4 / VPN FLEX Licenses

- On average, 10-25% of VPN Remote Access users connect simultaneously
- Under exceptional circumstances, 90% of employees connect remotely
- Emergency situations, network outages, seasonal or event-based access

Affordable, flexible solution for short-term bursts of VPN users

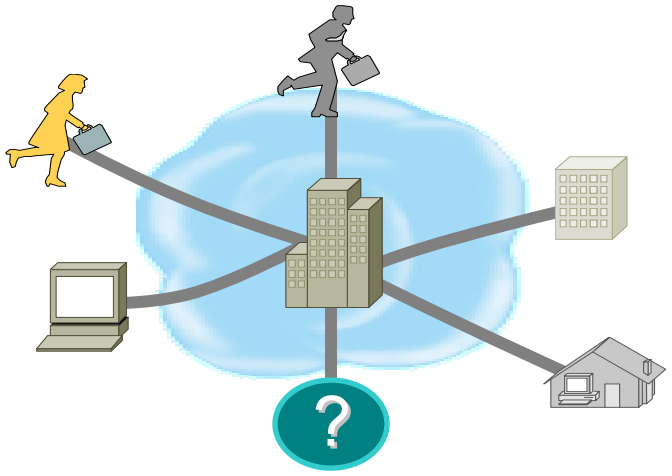
Benefit

Business Continuity Licenses
ASA 8.0.4 / VPN FLEX Licenses

- Emergency & Pandemic scenarios
- Planned surges of concurrent SSL VPN users
- Address competition's burst licenses offering

Solution Offering:

- 2-month, tiered SSL VPN licenses
- Requires ASA 8.0.4+ / 8.1.2
- Available on 5510-5580



Scenario
ASA 8.0.4 / VPN FLEX Licenses

- Customer has an ASA with a 1000 user permanent SSL license. Customer experiences a snow storm and 1500 employees need to work from home. The customer can apply a 500 user VPN Flex License for 1 day and then revert back to permanent license the following day.
- In this example the customer would have 59 days remaining on that SSL Flex License. Once the counter reaches Zero on a SSL VPN Flex License the customer will need to purchase another Flex license.

Many Compelling Benefits for Migrating to Cisco ASA 5500 Adaptive Security Appliances

Adaptive Security Offers Better, Flexible Protection

- Superior network protection from ever-changing threats through IPS, CSC, etc.
- Equal or better pricing provides lower TCO
- Better performance and scalability, solutions scaling to 10+ Gbps
- Flexible VPN solution with market-leading SSL VPN capabilities

Mature, Next-Generation Security Solution

- Built upon 10+ years of innovation in Cisco PIX, VPN 3000, and IPS 4200 solutions
- Hundreds of thousands of Cisco ASA 5500 units deployed worldwide
- GD quality software available (v7.0.7+)
- Common Criteria, FIPS, and NEBS-certified

Leverages Customer's Existing Cisco PIX Investment

- Cisco PIX knowledge directly transferable to Cisco ASA 5500 Series
- Consistent GUI and CLI interfaces as Cisco PIX security appliances
- Consistent syslog and SNMP monitoring
- Managed by Cisco Security Manager, MARS, and many third-party products

Cisco ASA 5500 Series and Cisco PIX Security Appliances Feature Comparison

	Cisco PIX	Cisco ASA	Cisco ASA 5500 Benefit
Flexible Access Control, Both IP and User-Based	☑	☑	Cisco ASA 5500 Supports More ACLs due to Increased Memory
Advanced Application Layer Firewall Services for over 30 Popular Protocols	☑	☑	Cisco ASA 5500 Offers Better Deep Packet Inspection Performance
Security Services for Encrypted Voice / Video Communications	☒	☑	Only Cisco ASA 5500 Enables Secure End-to-End Encrypted Voice / Video Communications
Cisco Easy VPN and Site-to-Site IPsec VPN	☑	☑	Cisco ASA 5500 Provides Superior VPN Performance
Clientless SSL VPN and Cisco AnyConnect SSL VPN	☒	☑	Cisco ASA 5500 Provides World-Class, Flexible SSL VPN Access
VPN Clustering and Load Balancing Support	☒	☑	Cisco ASA 5500 Provides Enterprise-Class VPN Scalability
Full-Featured, Hardware Accelerated IPS Services	☒	☑	Cisco ASA 5500 Provides Superior Protection from Attacks
Anti-Virus, Anti-Spam, Anti-Phishing, and URL Filtering Services from Trend Micro	☒	☑	Cisco ASA 5500 Protects from Malware, Helping Increase Employee Productivity
Consistent Management and Monitoring	☑	☑	Leverage Cisco PIX Knowledge and Tools with Cisco ASA 5500

Cisco PIX -> ASA

Cisco provides increased incentives for migrating from Cisco PIX to the Cisco ASA 5500 Series products.

Customers can contact their Cisco channel partner or Cisco AM in order to obtain information on the financial benefits of migrating from PIX to ASA

What's to come? – ASA 8.2 Titan

ASA Software release 8.2 will be available for the ASA5500 platform in the near future, and will contain a series of new and updated features inline with Cisco's security strategy.

More to come in the near future on specific features and details about the release.

New!

IPS Software Version 6.2 and E3 Engine

Extending Cisco's Market-Leading Threat Protection to IPv6 Networks with Cisco IPS 4200 Series

Compliance	• Meet key government and policy mandates
Investment Protection	• Future-proof your network for IPv6
Deployment Flexibility	• Protect your IPv4 and IPv6 networks with a single IPS sensor

ASA 5500 Series IPS Solution

High Performance

- Matched IPS and firewall throughput up to 650 Mbps
- Hardware-accelerated IPS not impact firewall or VPN throughput

Network-wide Protection

- Powerful protection for data, voice, video, and wireless networks

Intuitive management

- All-in-one IPS Manager Express simplifies provisioning, monitoring, troubleshooting and reporting

price drop!!

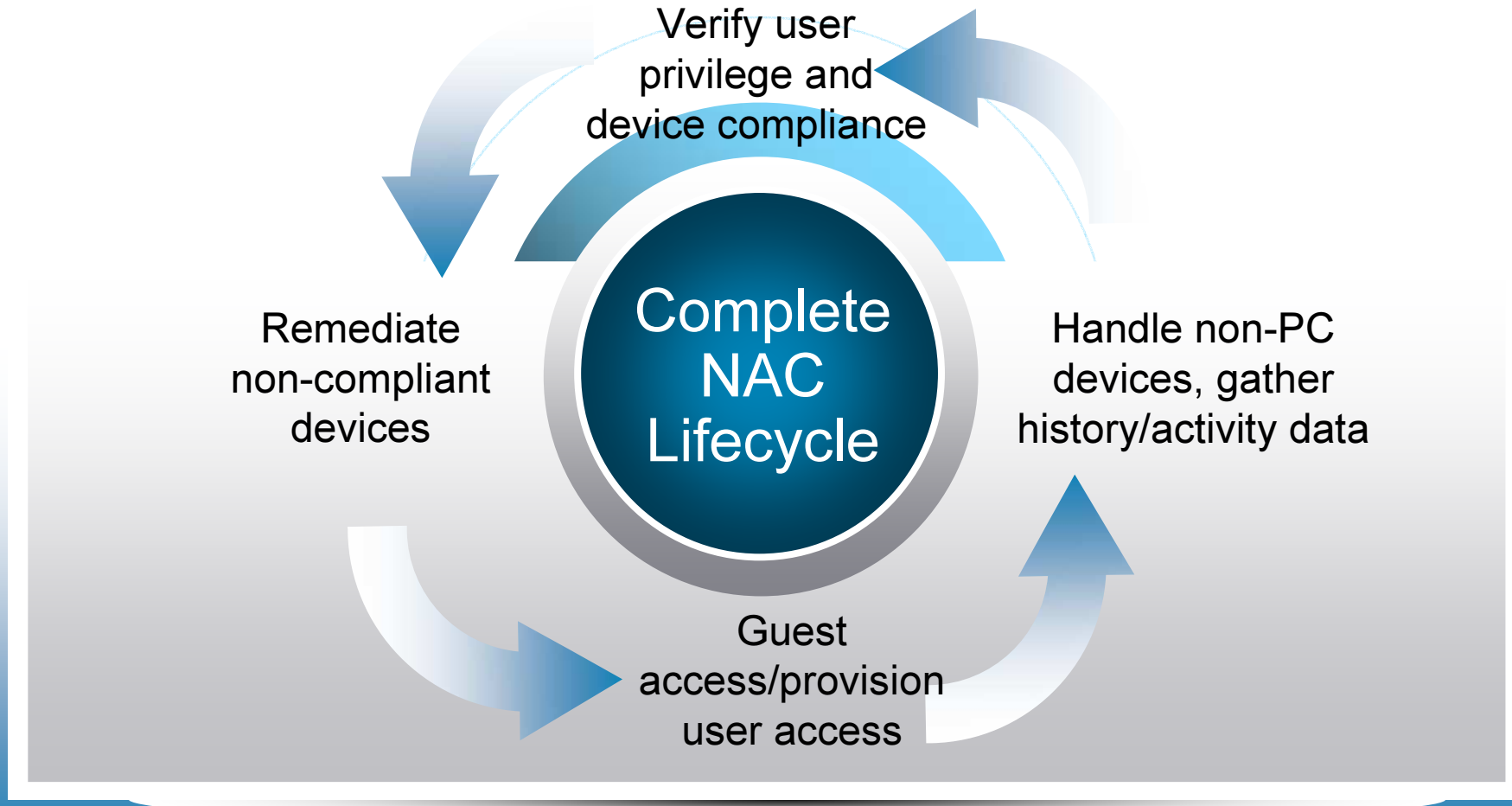
New Bundle!

Performance for Large and Small Organizations

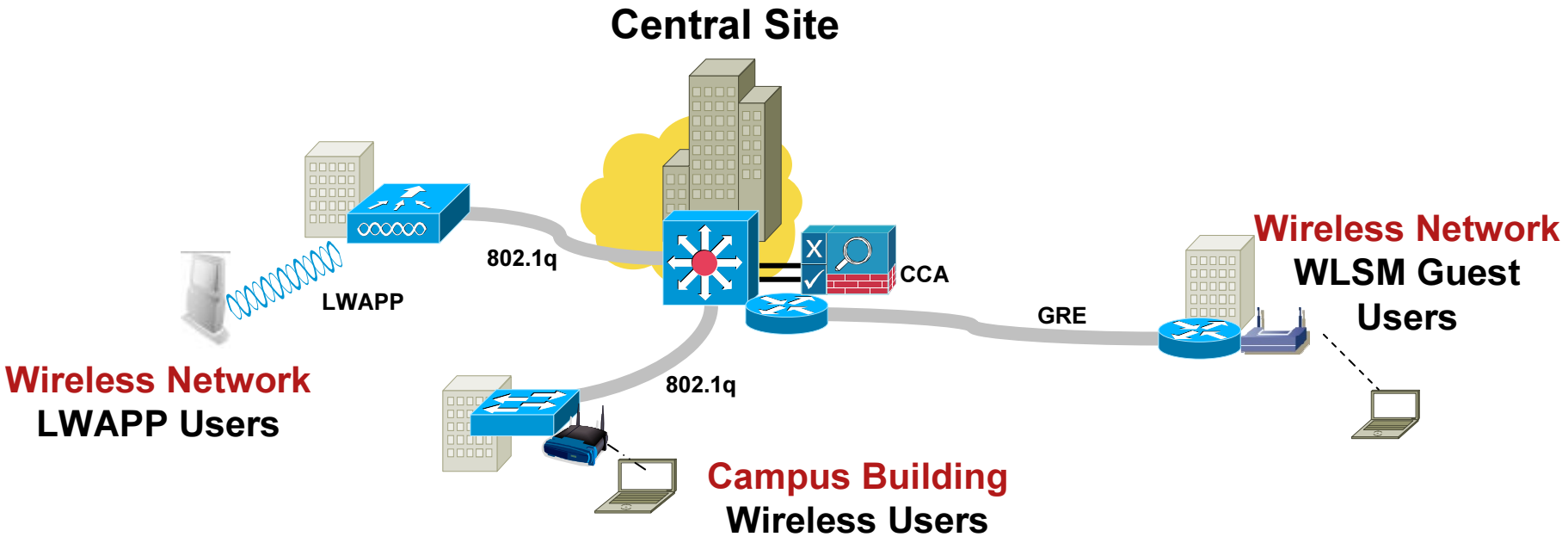
Solution	Performance IPS	FW
ASA 5510 with AIP SSM-10	150 Mbps	300 Mbps
ASA 5510 with AIP SSM-20	300 Mbps	300 Mbps
ASA 5520 with AIP SSM-40	450 Mbps	450 Mbps
ASA 5540 with AIP SSM-40	650 Mbps	650 Mbps

NAC Functions Defined

Ensuring role-based access and endpoint security policy compliance



Cisco NAC for Wireless Users



FEATURES	BENEFITS
▪ Supports 802.1q trunking ▪ Supports thin or thick wireless 802.11 APs ▪ Supports Wireless user sign-on ▪ Supports Wireless Out of Band in version 4.5	▪ Enables central deployment mode ▪ End user devices can be several hops away ▪ Extends enforcement to any wireless networks ▪ Leverages EAP sign-on for single-sign-on

Agenda

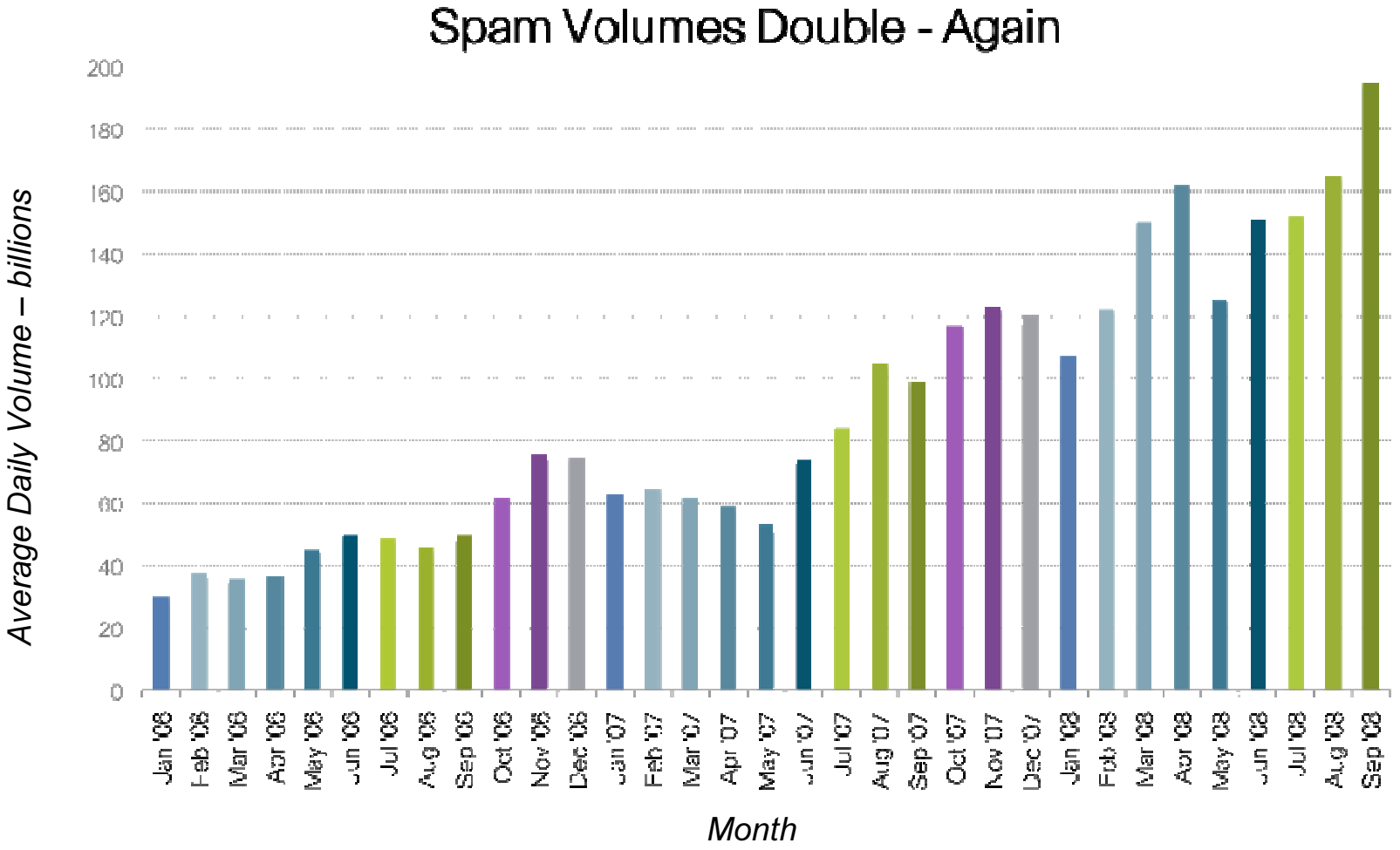
- Cisco Security Strategy Moving Forward
- New Features in ASA, IPS and NAC
- Pause – 15 min
- Cisco Spam & Virus Blocker
- ACS
- CSA 6.0 1 Day Install
- Pause – 15 min
- CSA Live Demo

Agenda

- Cisco Security Strategy Moving Forward
- New Features in ASA, IPS and NAC
- Pause – 15 min
- Cisco Spam & Virus Blocker
- ACS
- CSA 6.0 1 Day Install
- Pause – 15 min
- CSA Live Demo

Cisco
Spam & Virus Blocker

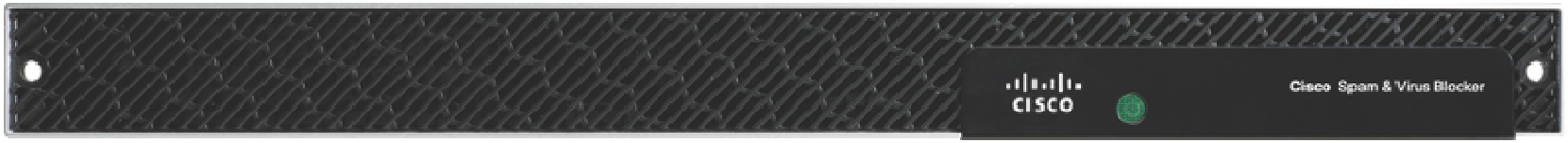
Spam Trends Through September 2008



Product Overview

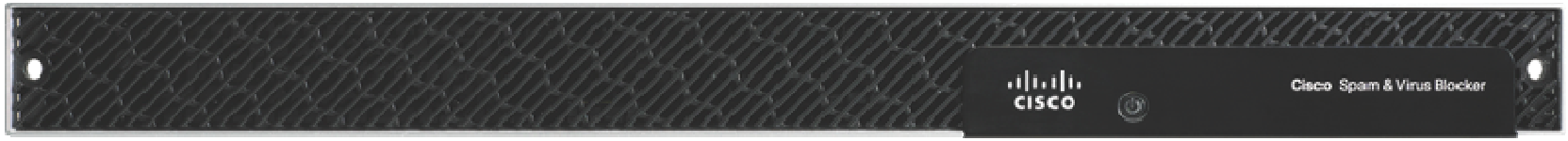
The Cisco Spam & Virus Blocker is a dedicated email security appliance for small business with up to 250 email users.

It provides powerful protection against spam, viruses and other email threats to secure your network and business data while improving productivity.



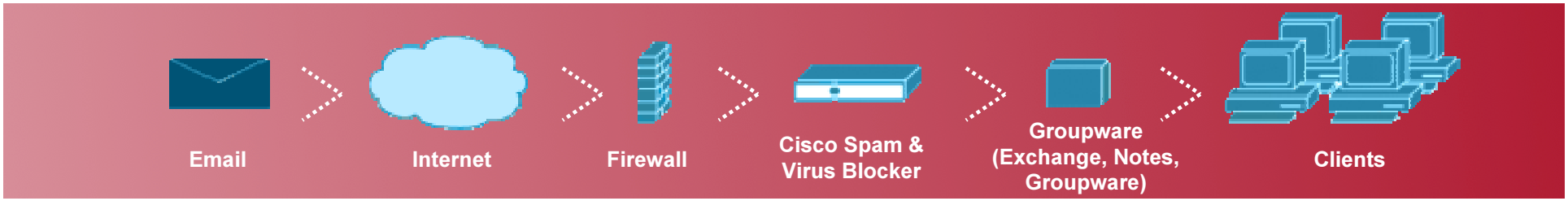
Always Protected

- Continuous automatic security updates without admin intervention – Enkelt køb inkluderer alt!
- Automatic connection to and threat updates from the SenderBase® network
- Additional support from Threat Operation Center security experts
- Immediate response to new, emerging and evolving threats
- “Set it and forget it” approach eases administration



Benefit Highlight: Easy Installation and Use

- Quick and easy installation into most networks within minutes. (Starter med wizard og kan derefter tunes)
- Provides immediate protection out of the box once installed in network.
- Automatic threat updates to the appliance with no intervention required.
- Simple browser-based wizards support management and reporting.
- Per user policies inkl. content filtering.

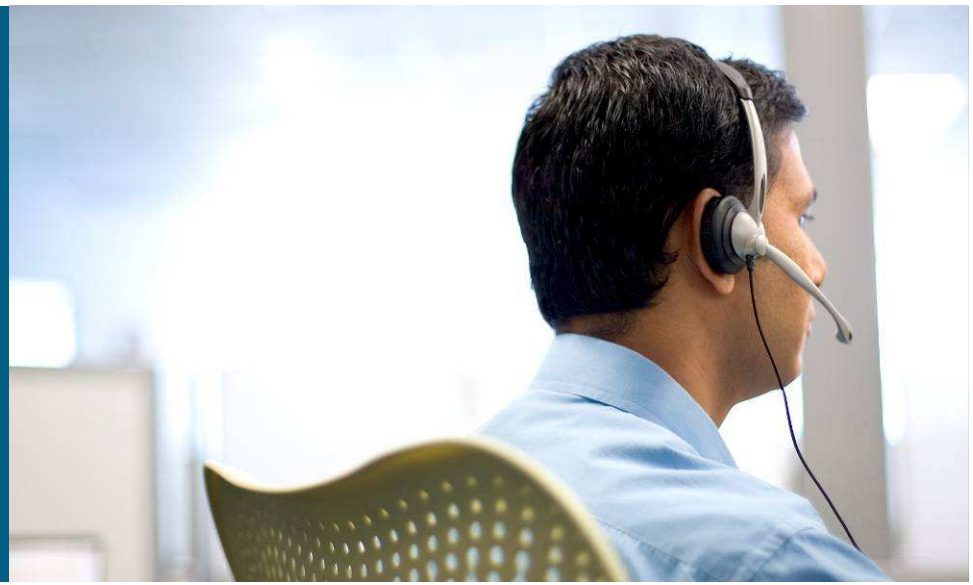


Agenda

- Cisco Security Strategy Moving Forward
- ASA
- New Features in ASA, IPS and NAC
- Pause – 15 min
- Cisco Spam & Virus Blocker
- ACS
- CSA 6.0 1 Day Install
- Pause – 15 min
- CSA Live Demo

The next generation

Cisco Secure ACS 5.0



Powerful performance, complete visibility, simple to manage

© 2002, Cisco Systems, Inc. All rights reserved.

30

Why should you care about ACS 5.0?

1. Simple & powerful rule-based policy model

   Attribute-driven model provides greater flexibility in addressing policy needs

   Authorization is not limited by group membership

   Allows dynamic policies and “compose-able” ID solutions

2. Simple & visible

   Intuitive Web-based GUI

   Easy to control and master

   Comprehensive monitoring, reporting & troubleshooting

ACS 5.0 currently supports many but not all access scenarios

Please evaluate ACS 5.0 and ACS 4.2 before making a purchase decision

Nowadays

The Human Network @ Work

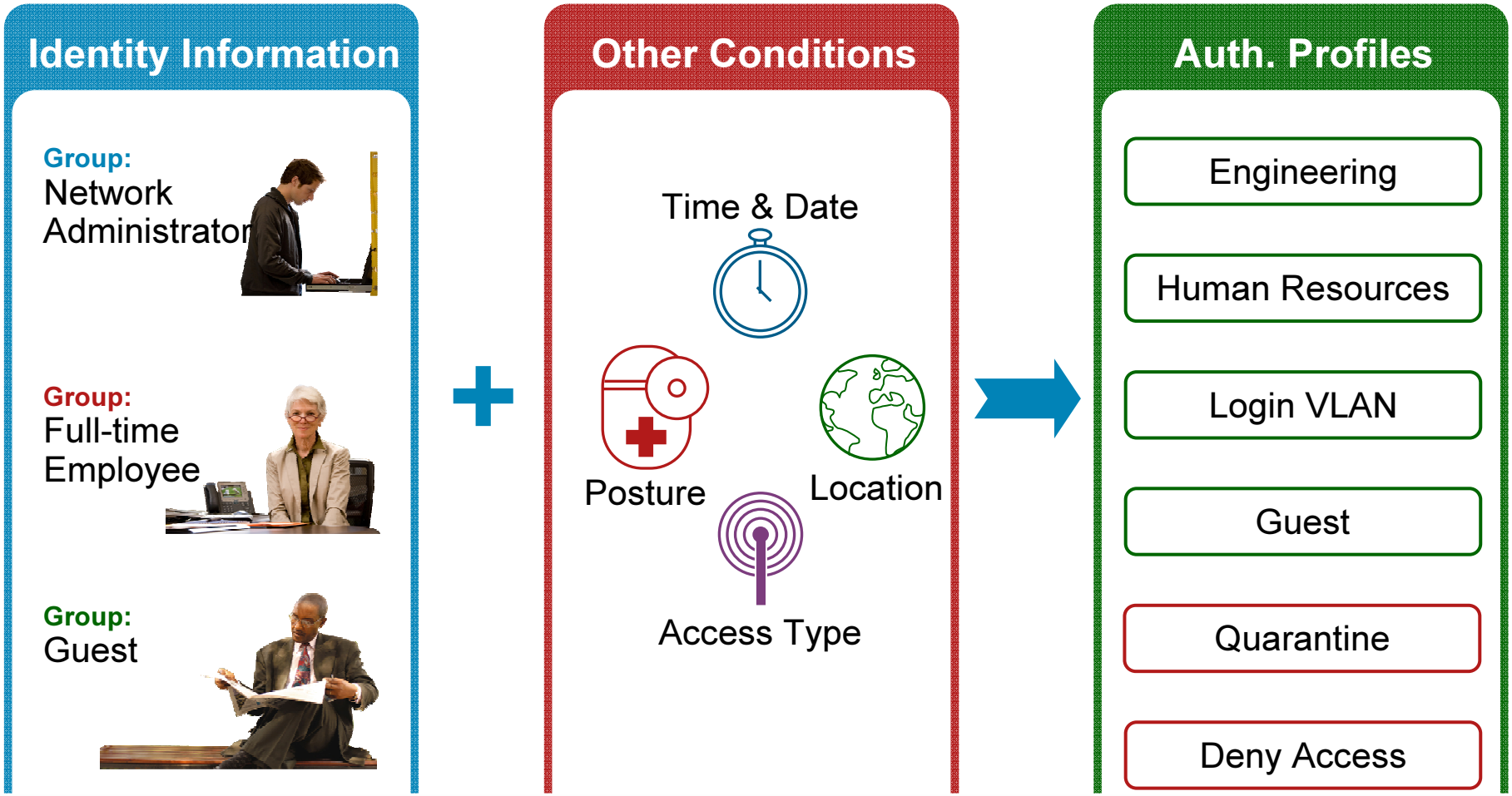
Coming up…

Even more complex dynamic policies

Greater need for flexible & “compose-able” ID & access solutions

And ever changing compliance regulations…

ACS 5: Rule-based policy



Authorization based on identity plus context

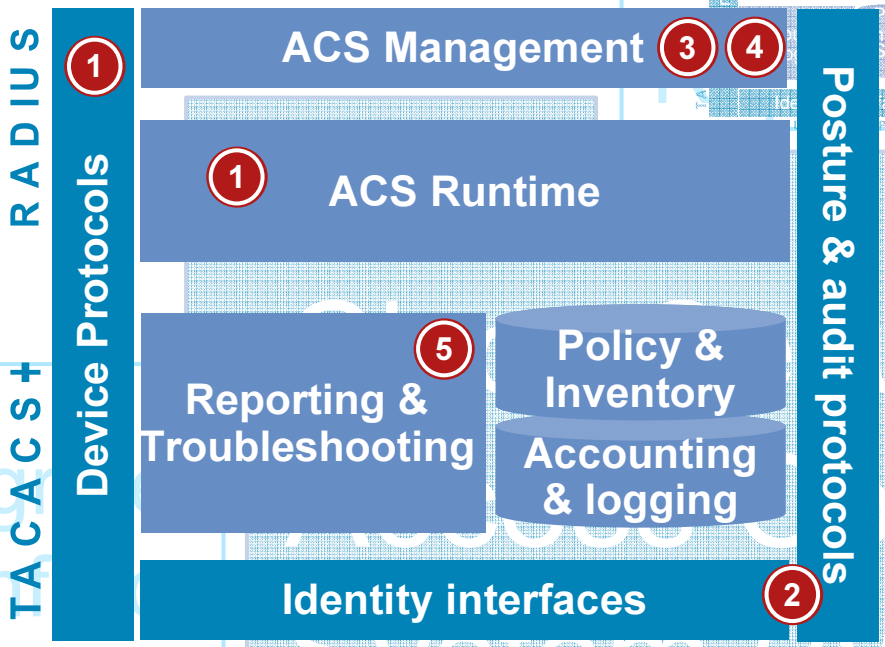
Conditions are specified as policy rules - IF <conditions> THEN <permission>

Cisco Secure Access Control System (ACS)

Connecting all elements of your network identity

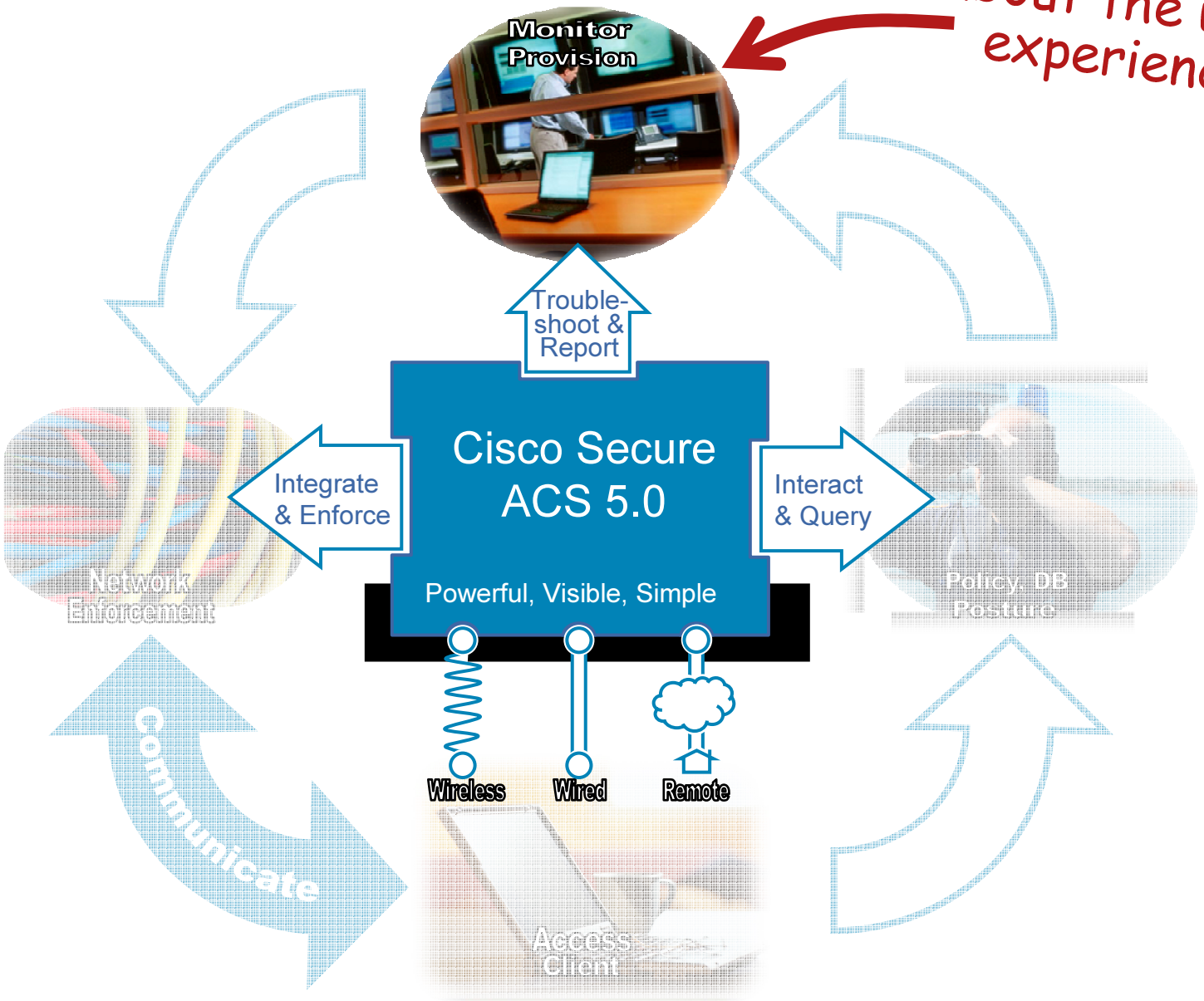
Key architecture

1. Includes both RADIUS & TACACS+ for complete N/W control and operation flexibility
2. Multiple identity interfaces allows flexible integration to multiple DB and ID resources
3. Replication mechanism allows deployment of multiple instances increasing availability and robustness
4. Administration of large scale deployments
5. Industry leading reporting, troubleshooting & compliance tools



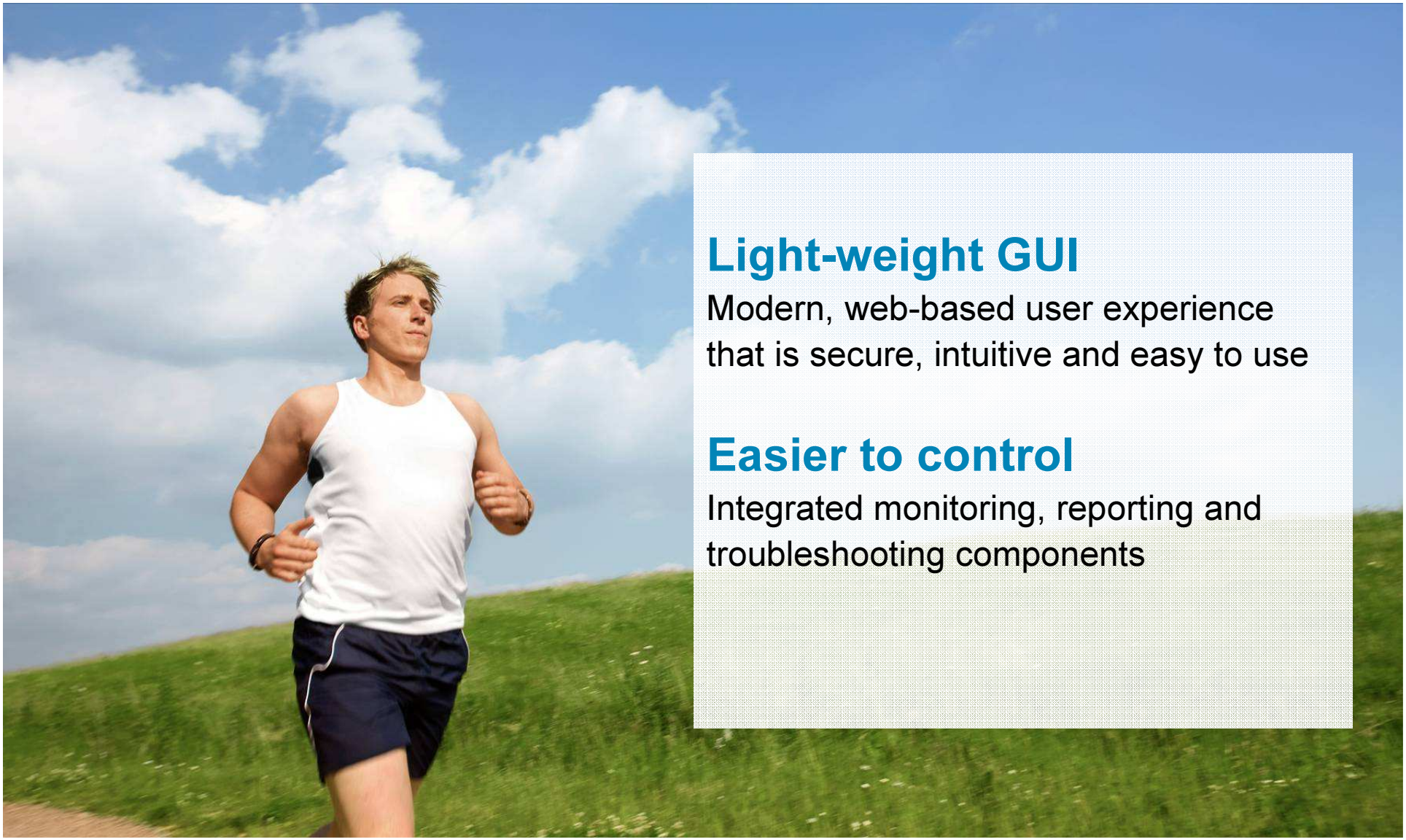
Rule-based policy with ACS 5.0

Now let's talk about the user experience



ACS 5.0 new user experience

Visibility equals control



Light-weight GUI

Modern, web-based user experience that is secure, intuitive and easy to use

Easier to control

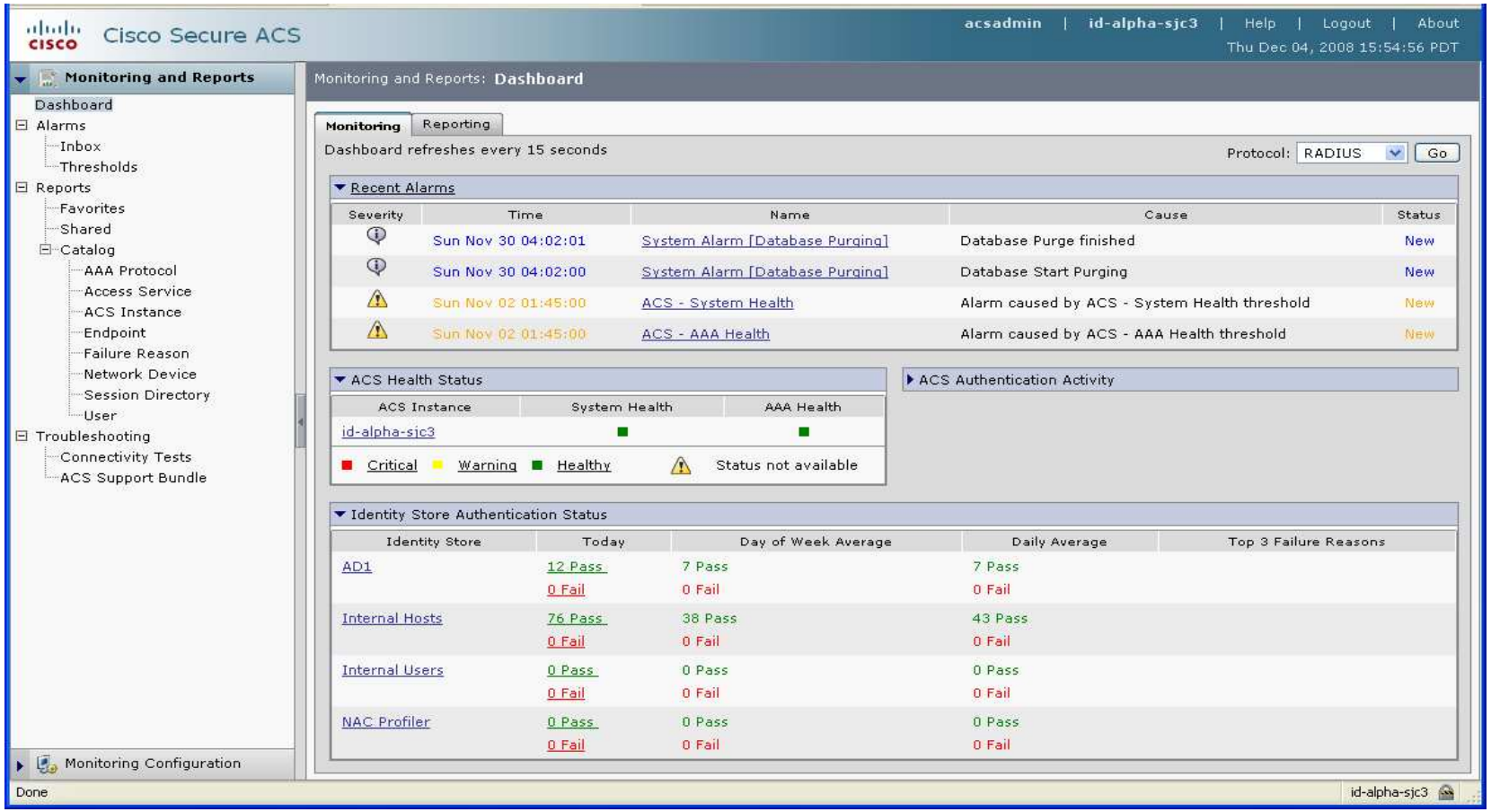
Integrated monitoring, reporting and troubleshooting components

ACS 5.0 Graphical User Interface

- Lightweight, secure, intuitive and easy to use web-based GUI
- Does not require additional client software for GUI access

ACS 5.0 Monitoring & Reports Component

- Integrated advanced monitoring, reporting & troubleshooting capabilities for maximum control and visibility
  - Easy to use GUI
  - Flexible presentation tools
- Consolidation of data across an ACS deployment



ACS 5.0: Reports

- Authentication

  Authentication summary, failed authentication summary, MAC authentication reports, access service authentication reports

- AAA

  RADIUS/TACACS+ authentication and accounting ,TACACS+ authorization

- Health/Operations Status

  Diagnostics, health summary

- ACS Administration

  Administrator logins, configuration changes

- Command Audit

  Command audit by user/device, command authorization by user/device

“Should I use ACS 5.0 or 4.2?”

- ACS 5.0 supports many access scenarios, but not all ACS 4.2 features
- Additional ACS 5.x releases are planned for 2009

Consult ACS 5.0 documentation for more information

References provided later in this slide deck

ACS 5.0 Platform Options

- Linux Appliance
  - One rack-unit (1RU) security-hardened, Linux-based appliance

- VMWare version
  - Software application and Linux operating system image for installation on VMware ESX 3.5

Migration and Upgrades

- ACS 5.0 includes a migration tool to assist in migrating existing ACS data
  - The new ACS 5.0 policy model may require that some policies be reconfigured

More Information

- ACS 5.0 home page

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

- ACS 5.0 documentation

  http://cisco.com/en/US/products/ps9911/tsd_products_support_series_home.html

- ACS 4.2 and 5.0 comparison

  http://cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.0/user/guide/migrate.html#wp1052549

Agenda

- Cisco Security Strategy Moving Forward
- New Features in ASA, IPS and NAC
- Pause – 15 min
- Cisco Spam & Virus Blocker
- ACS
- CSA 6.0 1 Day Install
- Pause – 15 min
- CSA Live Demo

The One Day CSA Install

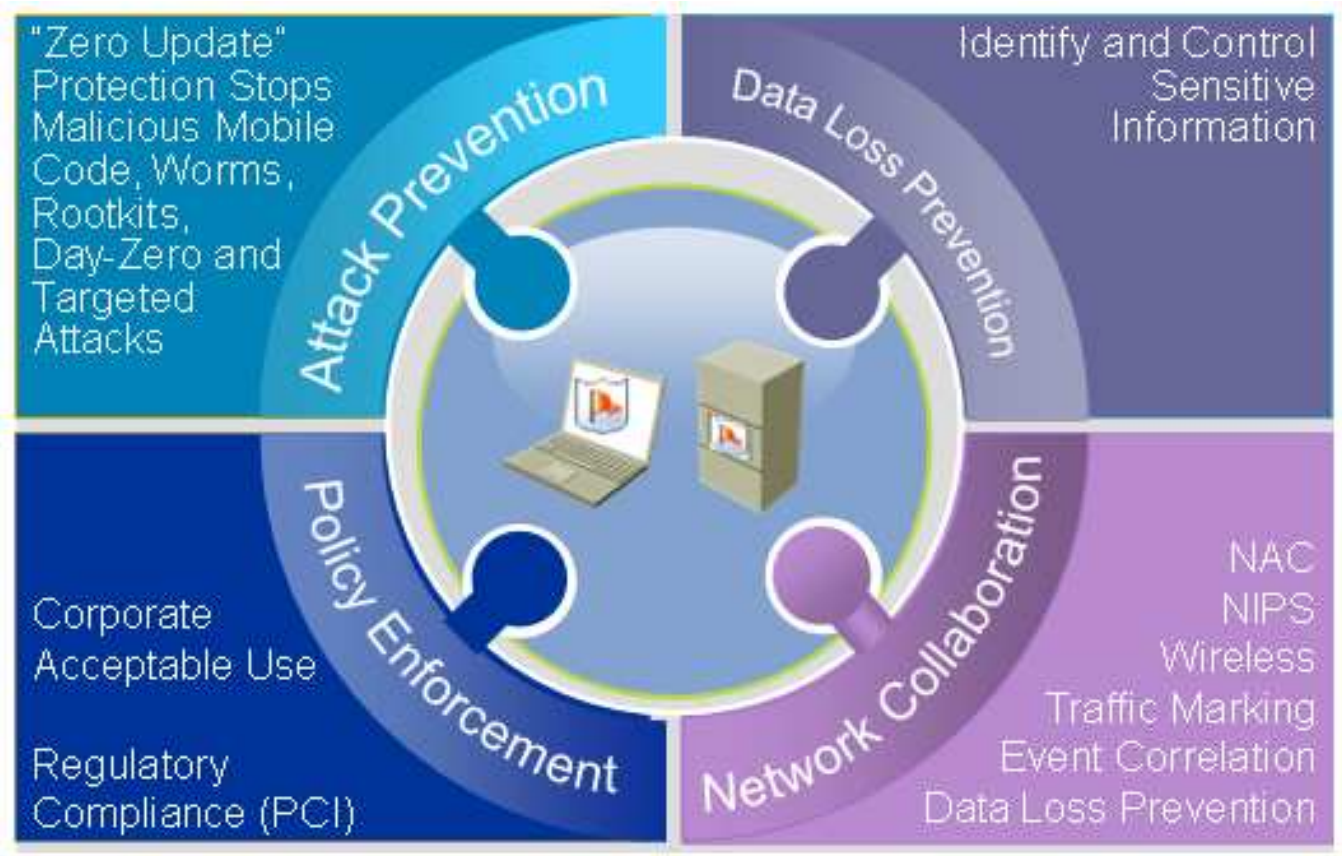
What's Easy
What's Harder
What Should Be Customized

What's New in CSA 6.0

What is this? One-day install

Cisco Security Agent

Always Vigilant Comprehensive Endpoint Security



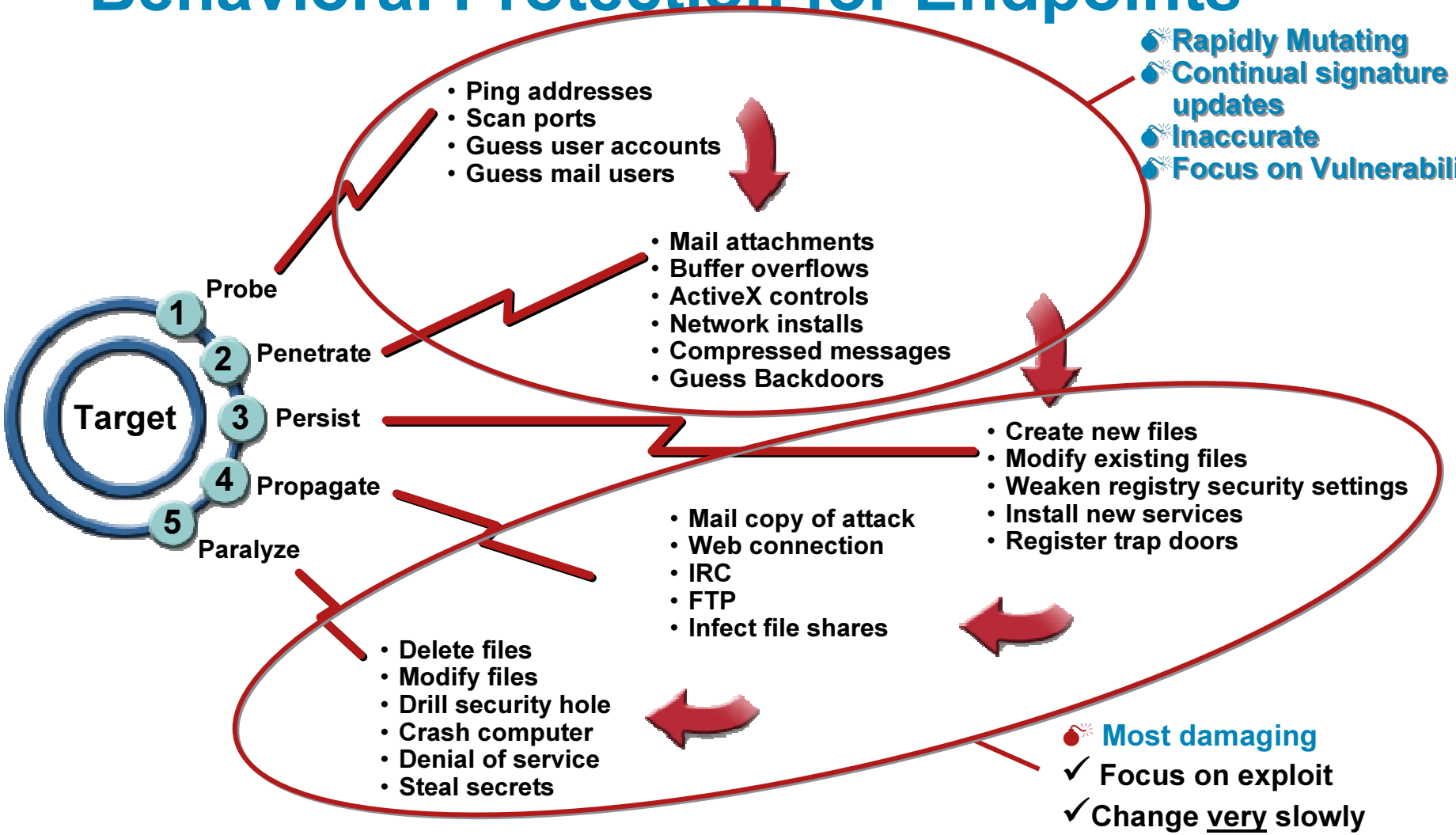
Laptop – Desktop Protection

Server Protection

POS Protection

SINGLE INTEGRATED AGENT AND MANAGEMENT

CSA Approach: Behavioral Protection for Endpoints



CSA with ClamAV Integrated, Synergistic

Feature	ClamAV™ Only	CSA + ClamAV™ combo
Signature database >200,000 sigs	✓	✓
Bulk file system scan	✓	✓
Rapid Signature Update	✓	✓
On-Demand scan	✗	✓
Quarantine file	✗	✓
Delete malware New in CSA 6.0!	✗	✓
Day zero protection	✗	✓
Rootkit protection	✗	✓

vendor	detected	total	percent
AntiVir	1204953	1229800	97.98%
Vexira	1203678	1229800	97.88%
VirusBuster	1203471	1229800	97.86%
F-Secure	1203244	1229800	97.84%
Norman	1203274	1229800	97.84%
F-Prot6	1202403	1229800	97.77%
Clam	1201805	1229800	97.72%
DrWeb	1201442	1229800	97.69%
AVG7	1200639	1229800	97.63%
Avast	1199011	1229800	97.50%
McAfee	1185278	1229800	96.38%
F-Prot	1176390	1229800	95.66%
Panda	1138986	1229800	92.62%
Kaspersky	1036869	1229800	84.31%
BitDefender	1036210	1229800	84.26%
VBA32	994177	1229800	80.84%
NOD32	798148	1229800	64.90%

Source: Shadowserver.org wild testing

Data Loss Prevention

Identify and Control Sensitive Information

Discover

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

Monitor

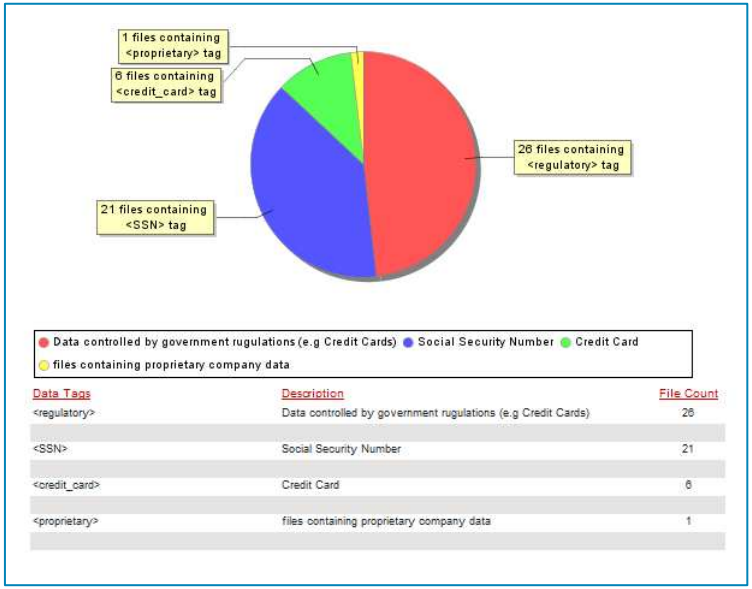
- Reporting
  - Track the location and usage of sensitive data

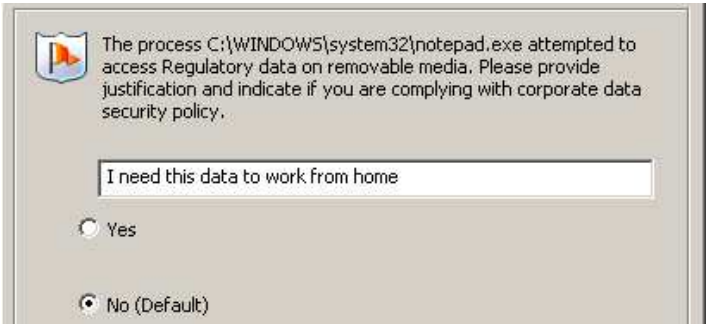
Educate

- Enhanced user education
  - Query user and audit

Enforce

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

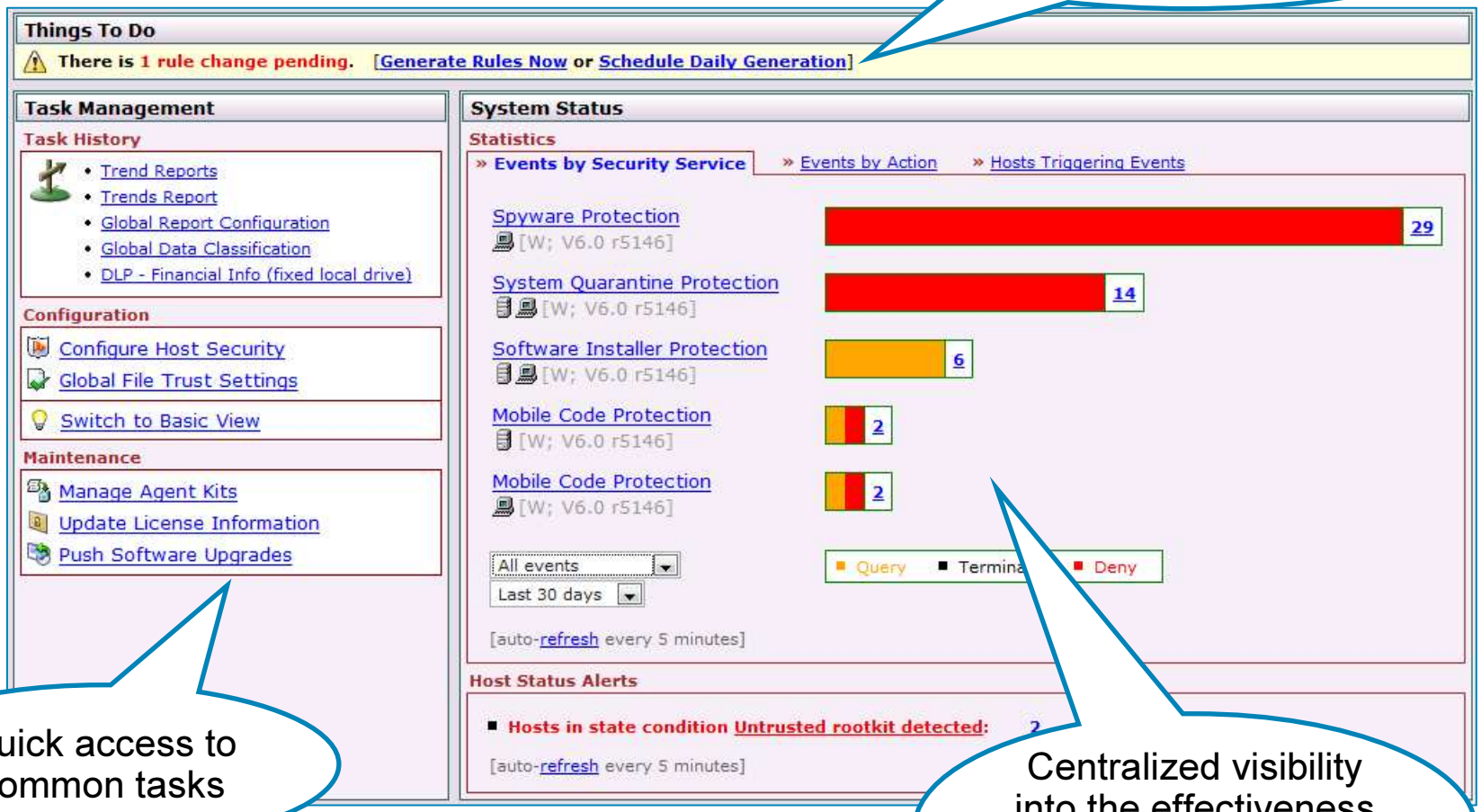




Easier to Use

Administrator Dashboard

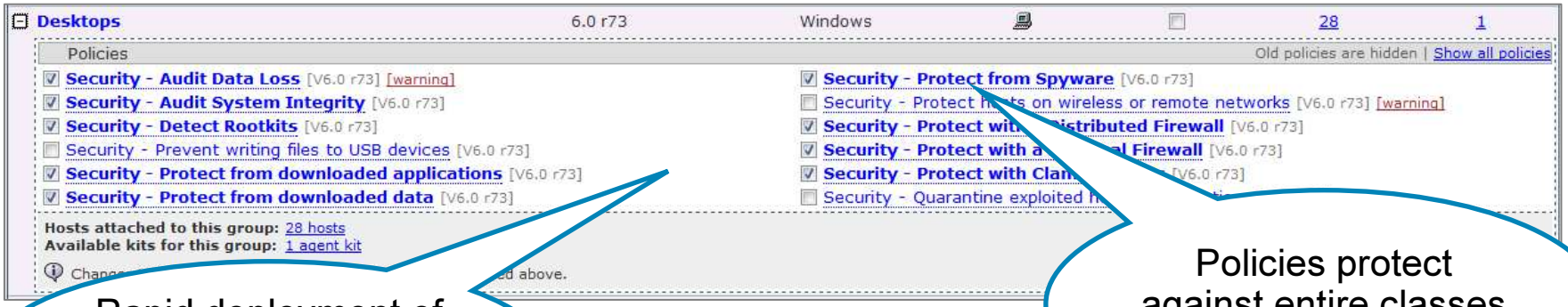
The dashboard helps the administrator see what needs to be done today



Quick access to common tasks

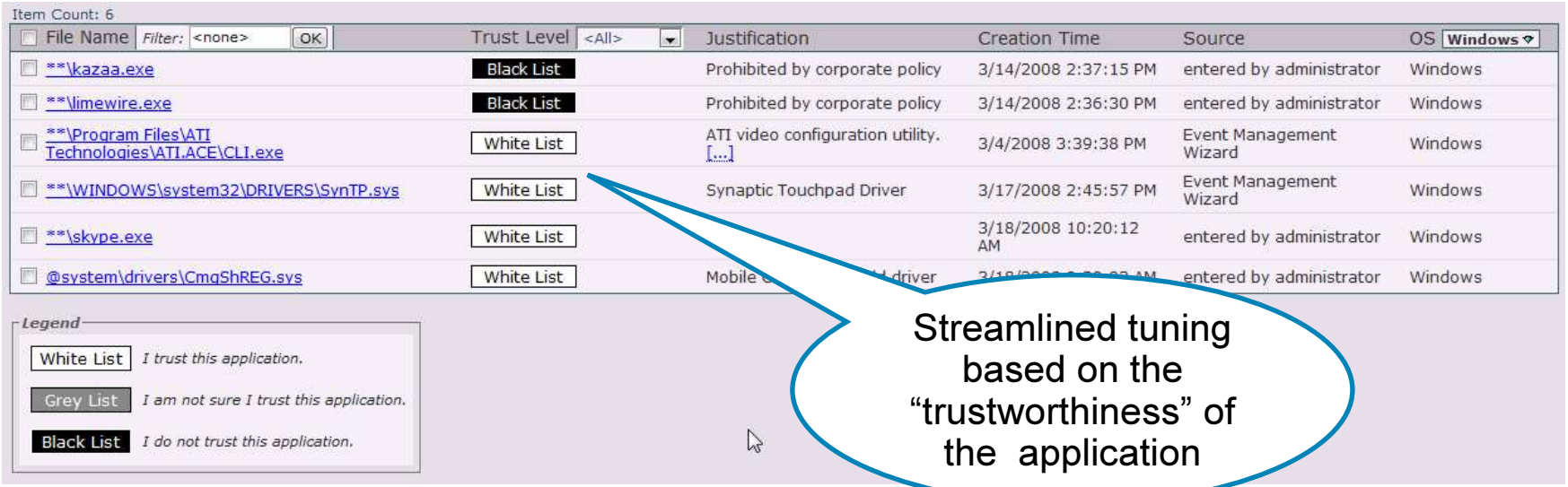
Centralized visibility into the effectiveness of your endpoint protection

Easier to Deploy and Tune



Rapid deployment of endpoint protection with default services

Policies protect against entire classes of attacks



Streamlined tuning based on the "trustworthiness" of the application

Deployment Overview

Rapid Deployment Guide

- Install the MC and update License
- Choose your policies and generate rules
- Deploy agents
- Tune events using the Wizard
- Let things run for a week or so, and then follow up with a 1 day “Check Up” final tuning session

Rapid Deployment Guide for
Desktops Cisco Security Agent 6.0

Install the CSAMC

- This has changed little from prior releases
- Remember to use a Windows 2003 R2 system

  If you don't use R2, you will get a message at install saying this is a non-supported configuration

- For demo/eval, you can run the MC in VMWare

  Don't do this for actual operations

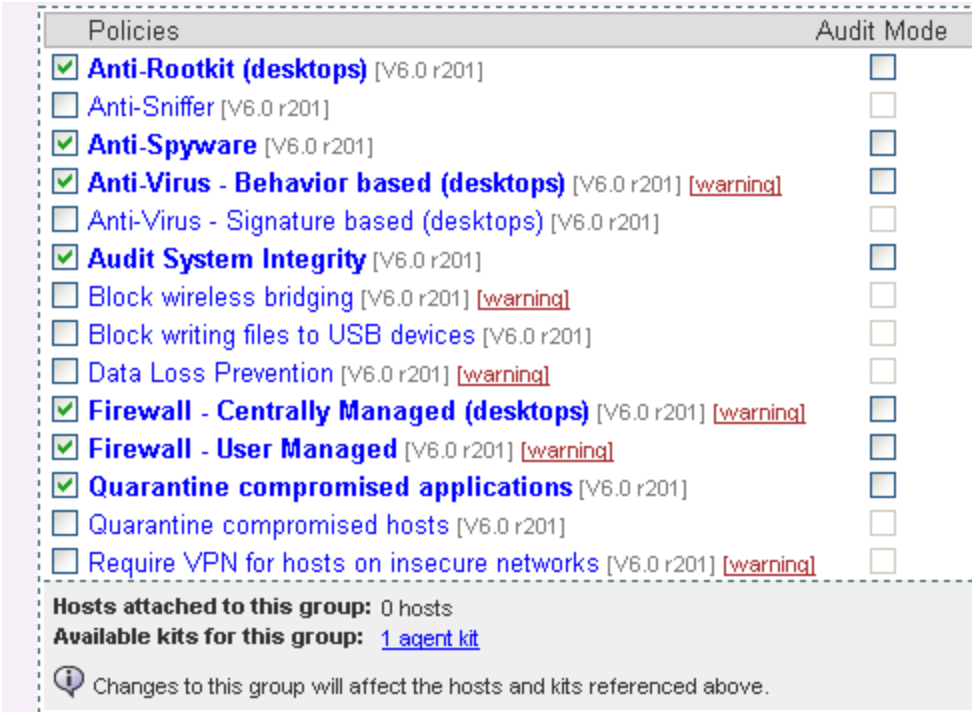
- You'll want the license when you install – the installer will ask you for it

  You can always add it later, but this is easiest

- Request a 30-day eval license online

Choose the policies

- This is VERY different from earlier versions
- The Simplified GUI has a “Host Security Page” with checkboxes to select policies
- The checkboxes map to CSA Policies, but you have to go into the “Advanced View” to see these
- Each policy can be in “Audit Mode” (renamed “Test Mode”), or the group can be in Audit mode
- If there’s configuration required, you will get a red “Warning” link next to the policy name
- Remember to Generate rules

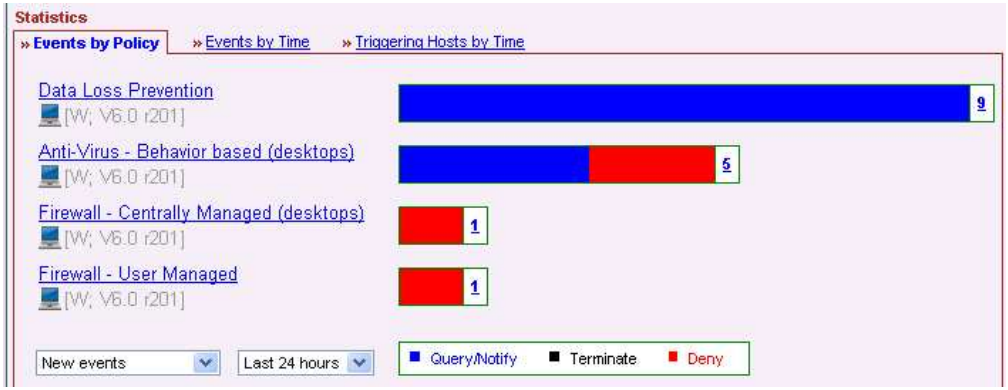


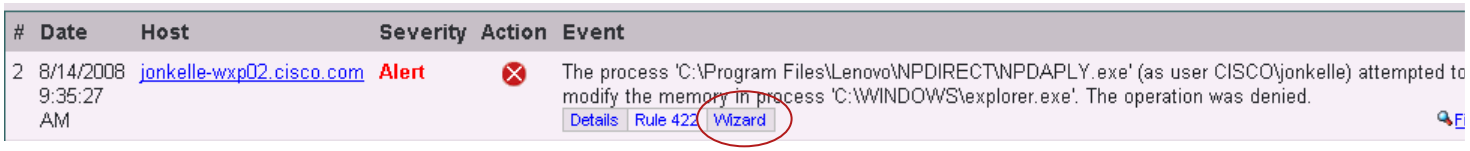
Deploy Agents

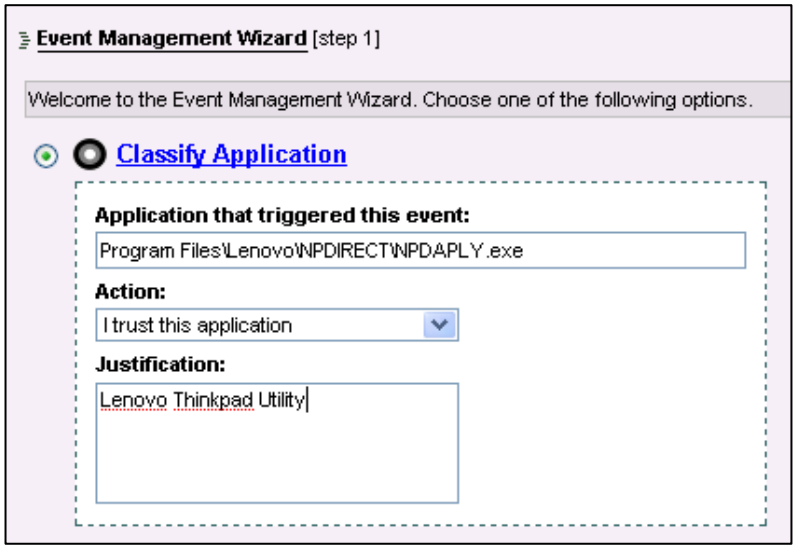
- This is the same as older versions
- The CSAMC builds installable “Agent Kits”
  - Installshield executable, tarball, Solaris package
  - Contains binaries, policy, CSAMC SSL certificate
- Easiest way to get kit to system is to use web download from CSAMC
- Can also use SMS, Bigfix, etc.

Tune the events

- Click on event graph to see specific events
- Wizard link in event takes you to Tuning Wizard
- Wizard walks you through 99% of tuning
- Most early deployment tuning will be using White List







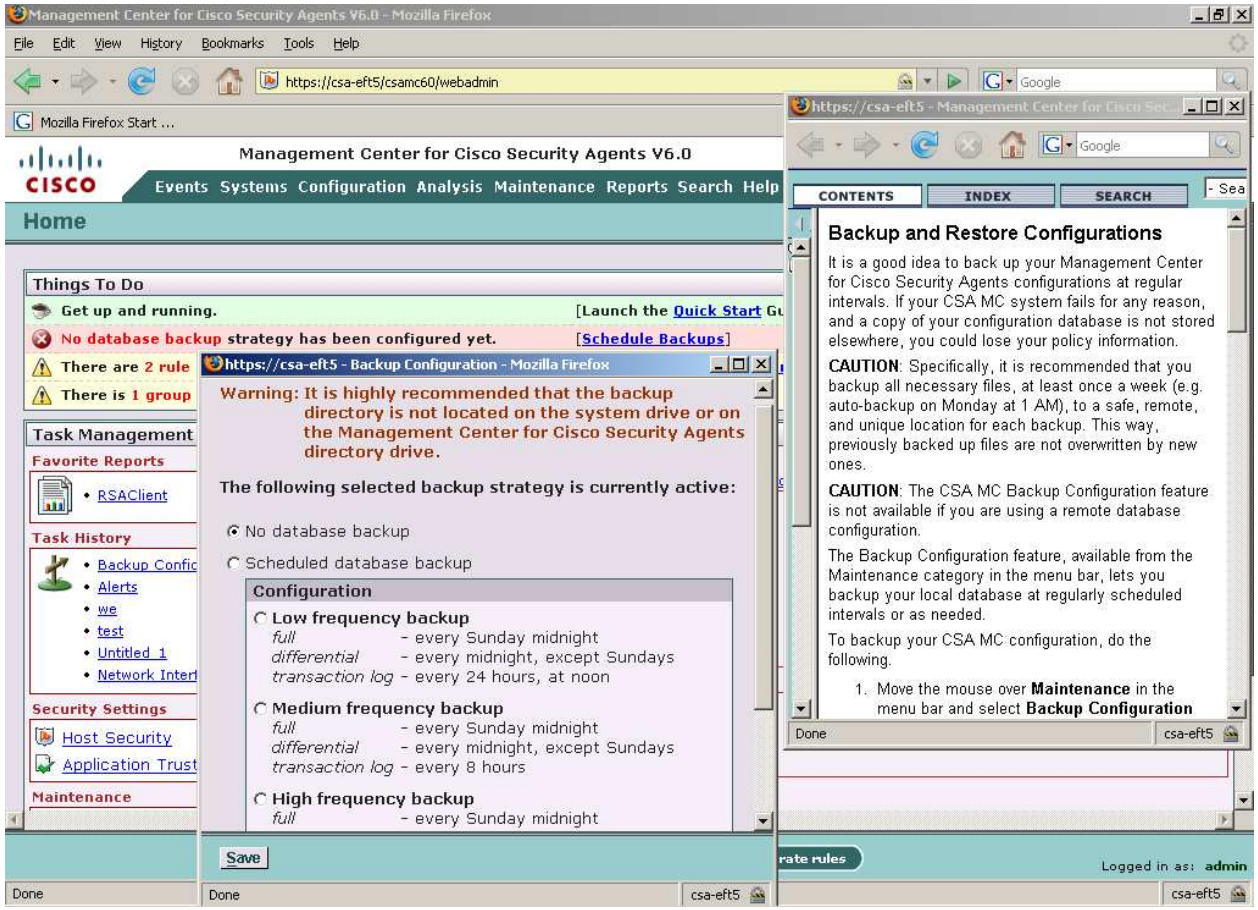
What To Use
What Not To Use

CSA Feature Summary – Low and Medium Difficulty

Acceptable Usage Policies			
Name	**Initial Configuration Level**	**Tuning Overhead**	**Time Estimated for Deployment**
Require VPN hosts on insecure networks	Low	Low	1-day
Block Wireless Bridging	Low	Low	1-day
Block Writing Files to USB Devices	Low	Low	1-day
Audit System Integrity	Low	Low	1-day
Anti-Sniffer	Low	Low	1-day
PCI Compliance	High	High	More than 1 week
Data Loss Prevention for Desktops	High	High	More than 1 week
Protection from Zero-Day, direct and indirect attacks			
Name	**Initial Configuration Level**	**Tuning Overhead**	**Time Estimated for Deployment**
Anti-Virus – Signature Based	Low	Low	1 week
Anti-Virus-Behavior-based	Low	Medium	1 week
Anti-Spyware	Low	Medium	1 week
Firewall Centrally Managed	Low	Medium	1 week
Firewall User Managed	Low	Low	1 week
Anti-Rootkit	Low	Medium	More than week
Quarantine Compromised Applications	Low	Medium	More than 1 week
Quarantine Compromised Hosts	Low	Medium	More than 1 week

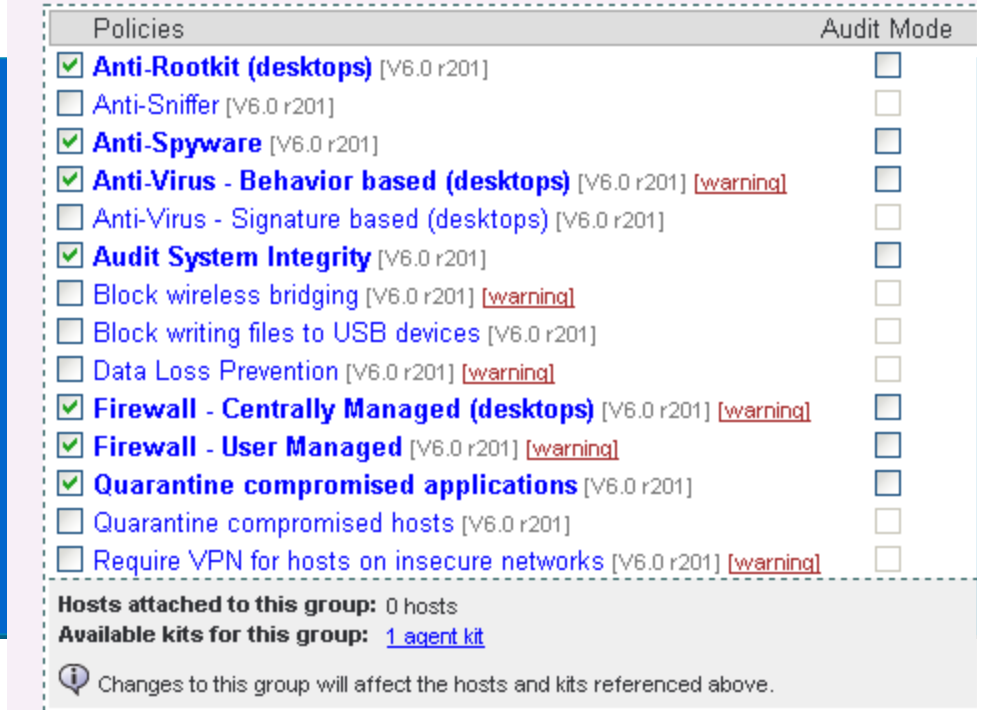
Check the To-Do List And Eliminate Warnings

- The CSAMC admin GUI has a To-Do list at the top of the Home Page
- Each entry has a link to a Wizard
- Use the Wizard to Eliminate the warnings
- For example, configure DB backup schedule

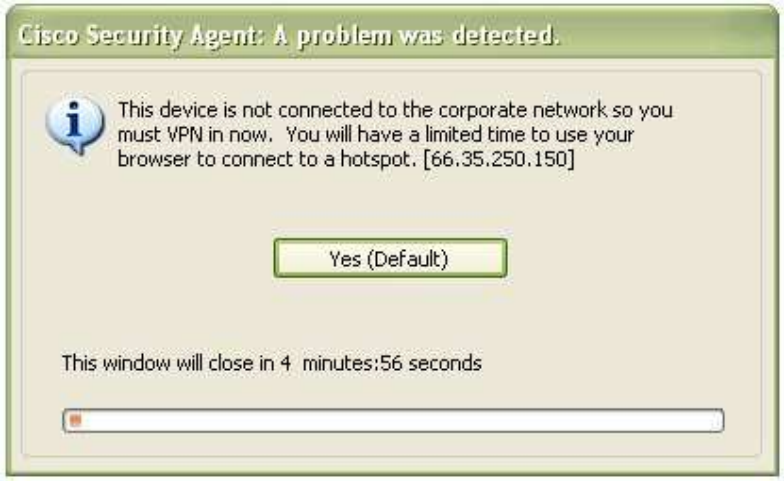


Deployment Phase II

Choosing Your Policies



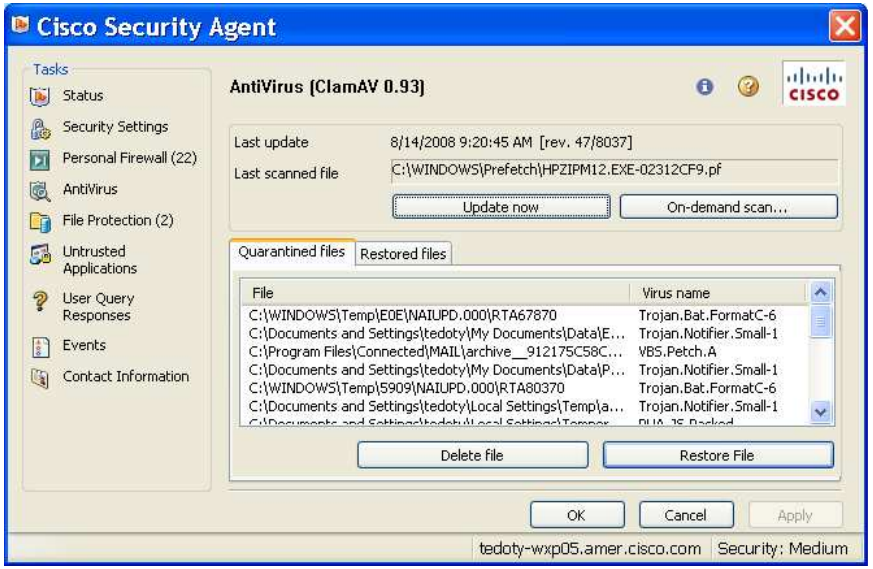
What The Policies Do (VPN, WiFi)



- Require VPN When Out Of Office
  - If user is not in office, apps must use VPN tunnel, or CSA blocks app
  - 5 minutes to let user connect to hotspot
  - You need to configure DNS name, SSIDs
- Block Wireless Bridging
  - If Ethernet is active, no apps allowed to communicate via WiFi adapters
  - No configuration required
  - Note that WiFi adapter will associate with Access Point – this allows immediate failover to the WiFi LAN when you undock

What The Policies Do (A/V, PFW)

- Signature-based Antivirus
  - This is ClamAV
  - Agent GUI has antivirus tab
  - Wizard has way to tune false positives
  - Likely these will be “PUA” – Potentially Unwanted Applications
  - CSA/Clam will not coexist well with Symantec or McAfee



- Centrally Managed Personal Firewall
  - Allows outgoing connections
  - Blocks incoming connections to well-known or fixed ports
  - Stops network packet attacks and buffer overflows
  - No end user interaction involved

What The Policies Do (Behavioral A/V)

- Behavior Based Antivirus

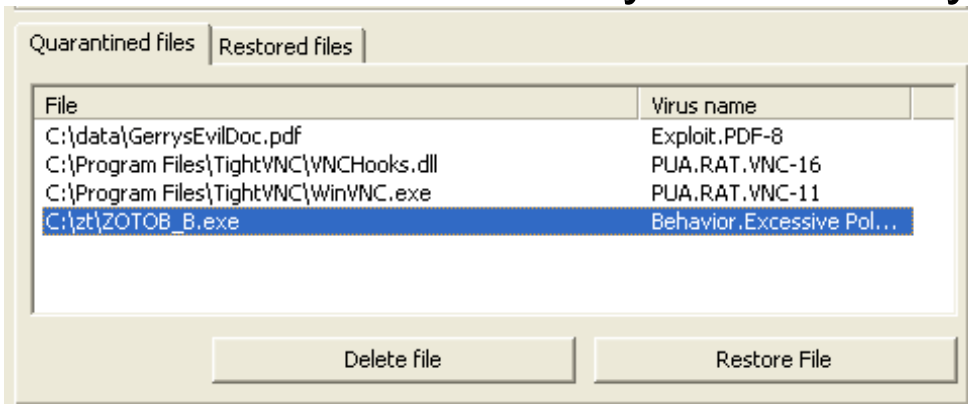
  This is the classic CSA Day Zero Protection

  Expect 2 types of user queries:

  "Are you installing software?"

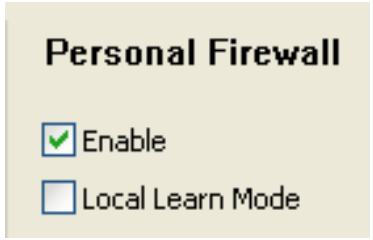
  "I've never seen this application on this system before" (First-time execute)

  Malware detected here will show up in Quarantine, just like if a signature had identified it. It will say "Behaviorally identified"

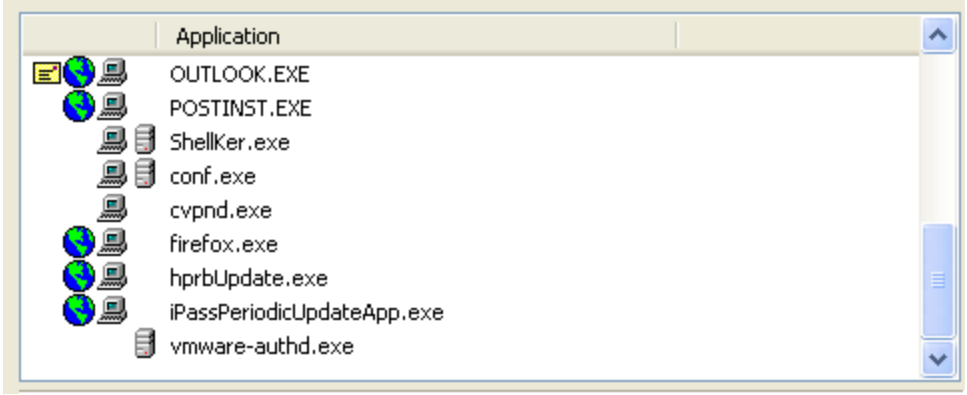


What The Policies Do (Spyware, PFW)

- Anti-Spyware
  - Monitors for Spyware and Trojan like behavior
  - Hooking keyboard, create user accounts and install services, modify system configuration, etc
  - Downloaded or “Untrusted” applications are the ones monitored
  - Moderate tuning required, via the Wizard



- User Managed Personal Firewall
  - ZoneAlarm style PFW.
  - Populates list of apps allowed to connect to network, by asking user
  - User can run in “Learn Mode” for a period of time where list is automatically populated.



What The Policies Do (Audit System Integrity, Block Files Writing to USB Devices)

- Audit System Integrity

  Detects suspicious behavior on hosts or system configuration, changes which may affect system integrity.

  “Monitors” only.

- Block Files Writing to USB Devices

  Preventing written access to removable media, based on Corporate Data Security Policy.

What The Policies Do (Quarantine Apps, Hosts)

- Applications

Quarantines compromised applications, i.e.worm propagation,

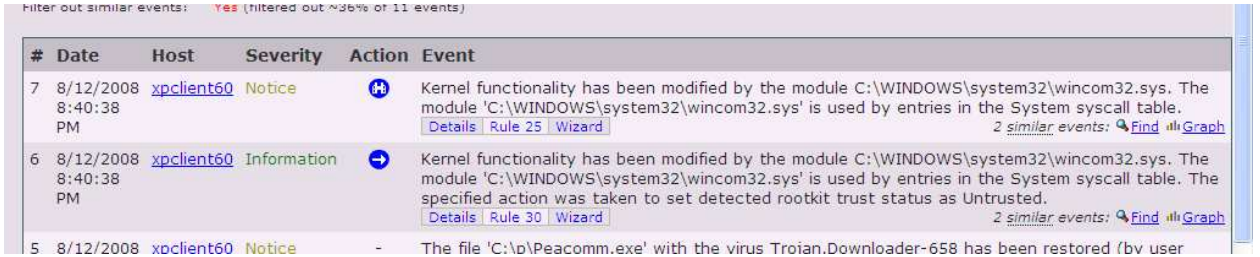
Prevents applications from infecting system.

- Hosts

Isolates hosts containing suspected rootkits from the network, i.e. Storm Trojan

Works in conjunction with the Anti-Rootkit Policy.

Reset CSA agent either locally or centrally from CSA MC to bring back original state of system.



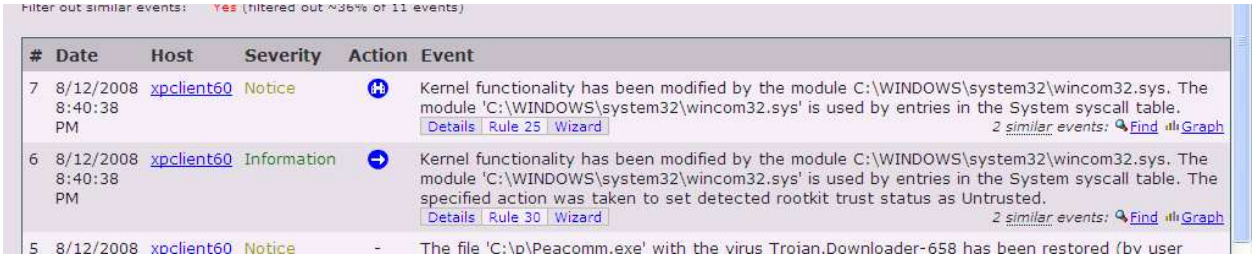
What The Policies Do (Anti-Sniffer, Anti-Root Kit)

- Anti-Sniffer

  Detects packet sniffers and unknown protocols, i.e. systems should not have Wireshark installed unless you belong to the Networking Group.

- Anti-Rootkit

  Detects unauthorized kernel activity upon startup and kernel modifications.



Agenda

- Cisco Security Strategy Moving Forward
- New Features in ASA, IPS and NAC
- Pause – 15 min
- Cisco Spam & Virus Blocker
- ACS
- CSA 6.0 1 Day Install
- Pause – 15 min
- CSA Live Demo

Agenda

- Cisco Security Strategy Moving Forward
- New Features in ASA, IPS and NAC
- Pause – 15 min
- Cisco Spam & Virus Blocker
- ACS
- CSA 6.0 1 Day Install
- Pause – 15 min
- CSA Live Demo

Q and A