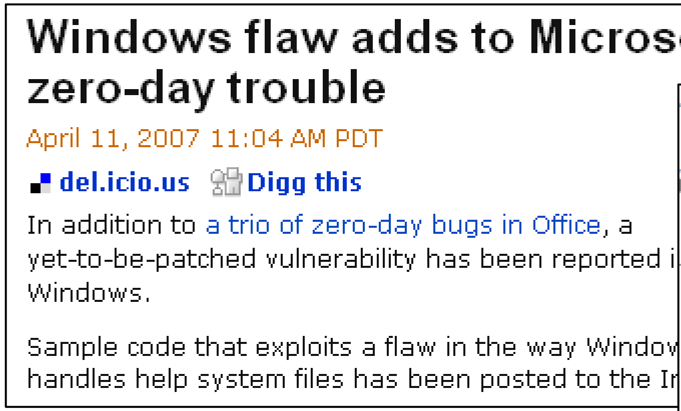
Desktop Security

Omar Contreras G. omcontre@cisco.com

Today's Security Concerns

The Driver for Advanced Endpoint Security

Day-Zero and Targeted Attacks



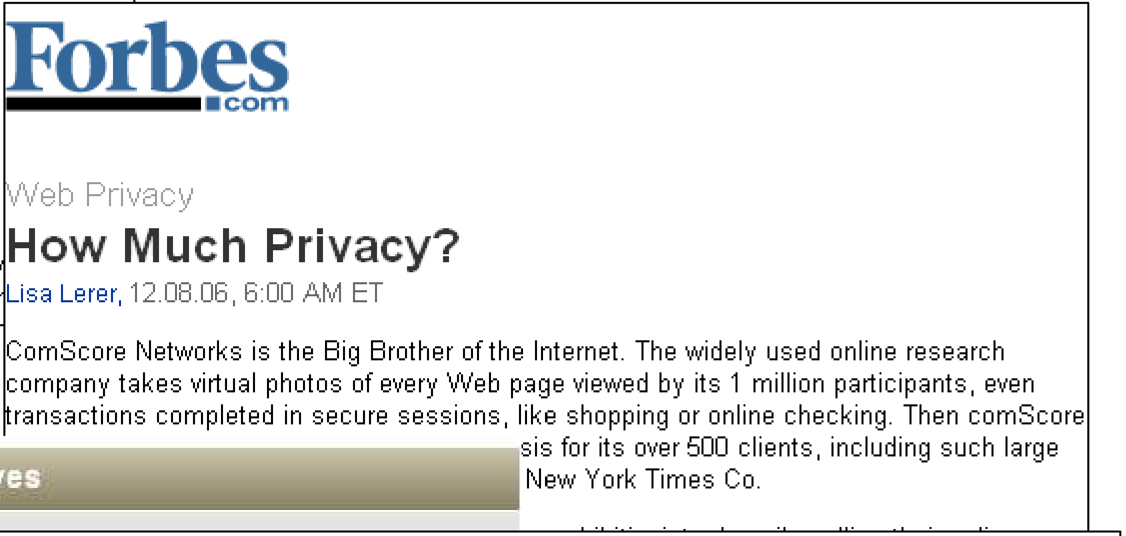
Windows flaw adds to Microsoft's zero-day trouble

April 11, 2007 11:04 AM PDT

del.icio.us Digg this

In addition to a trio of zero-day bugs in Office, a yet-to-be-patched vulnerability has been reported i Windows.

Sample code that exploits a flaw in the way Window handles help system files has been posted to the Ir



Forbes.com

Web Privacy

How Much Privacy?

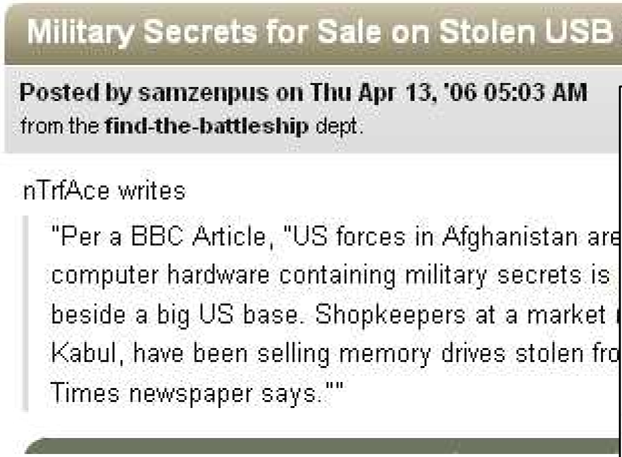
Lisa Lerer, 12.08.06, 6:00 AM ET

ComScore Networks is the Big Brother of the Internet. The widely used online research company takes virtual photos of every Web page viewed by its 1 million participants, even transactions completed in secure sessions, like shopping or online checking. Then comScore

sis for its over 500 clients, including such large

New York Times Co.

Hidden Activity



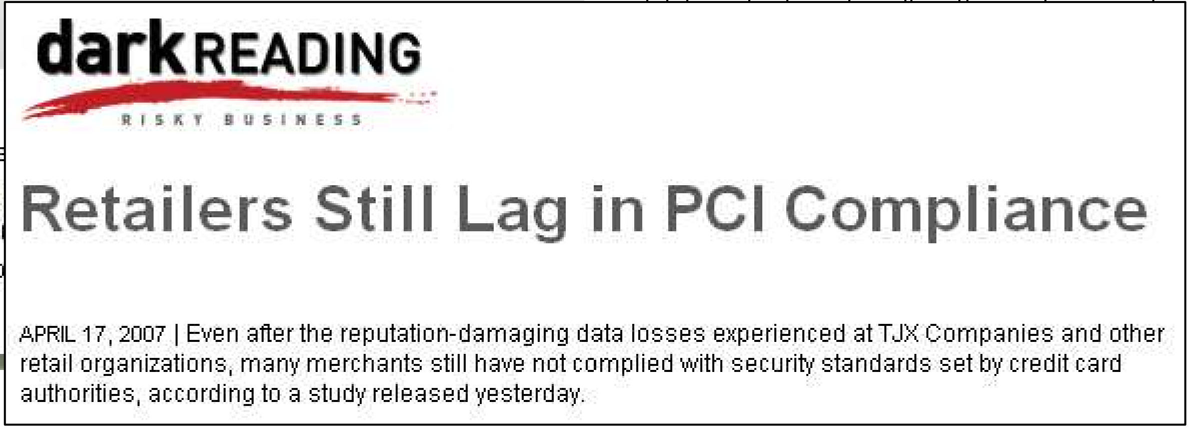
Military Secrets for Sale on Stolen USB Drives

Posted by samzenpus on Thu Apr 13, '06 05:03 AM
from the **find-the-battleship** dept.

nTrfAce writes

> "Per a BBC Article, "US forces in Afghanistan are
> computer hardware containing military secrets is
> beside a big US base. Shopkeepers at a market
> Kabul, have been selling memory drives stolen fro
> Times newspaper says.""

Data Leakage



darkREADING
RISKY BUSINESS

Retailers Still Lag in PCI Compliance

APRIL 17, 2007 | Even after the reputation-damaging data losses experienced at TJX Companies and other retail organizations, many merchants still have not complied with security standards set by credit card authorities, according to a study released yesterday.

Compliance Requirements

Changing Face of the Threat Landscape

Attackers Continue to Evolve

- Change in ***Purpose***

  Shift from fame to profit

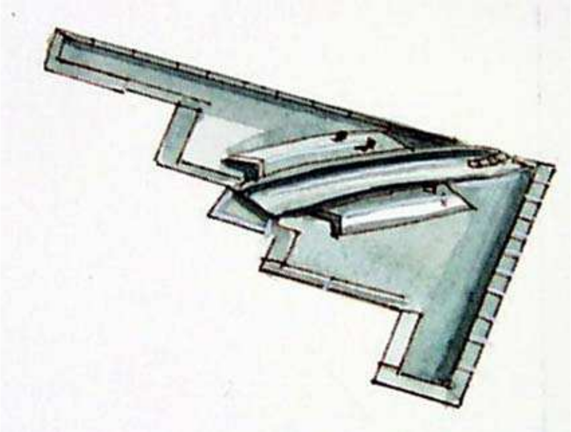
  Shift from attracting notice to developing an asset with economic value

- Change in ***Expected Behavior***

  Less Noisy

  More Sophisticated

  More Variants, smaller scope of each



Security Solutions

Typically Deployed

- Common security solutions involve:

  Firewalls to isolate and control communication between security domains

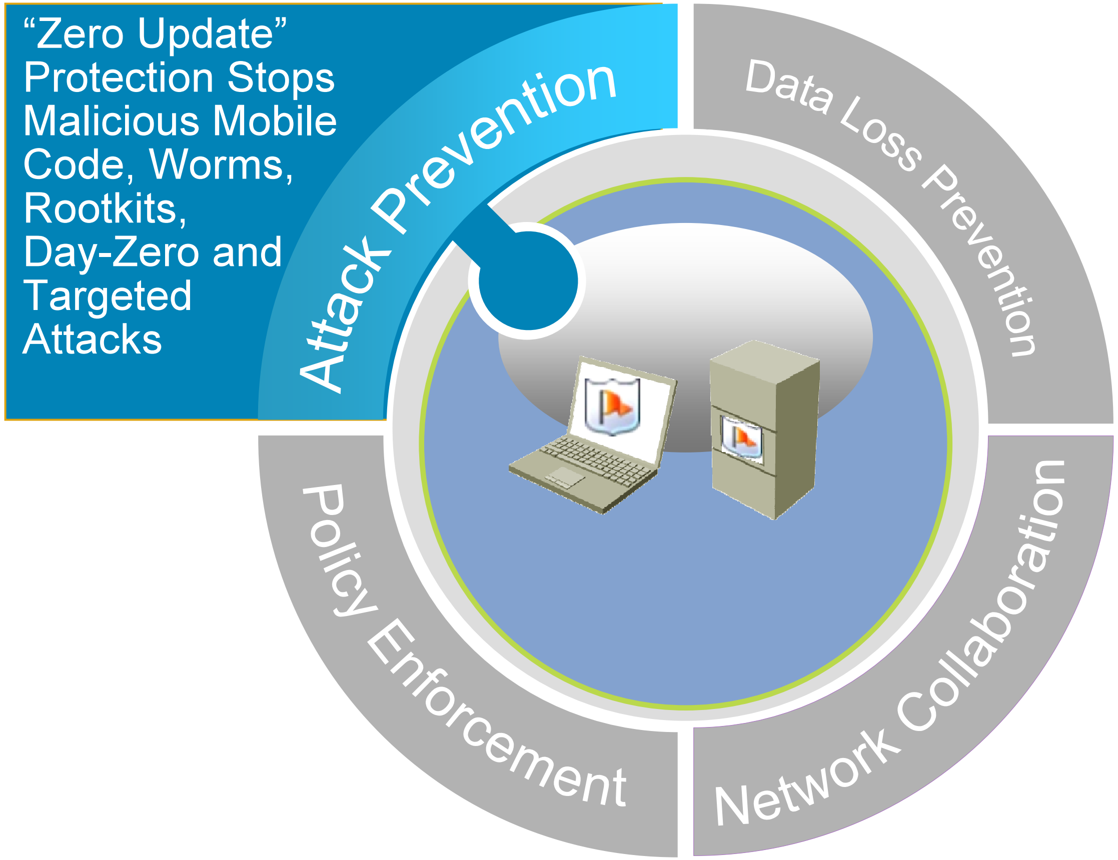
  Network IPS to detect and prevent malicious network activity

  VPNs (IPsec, SSL) to provide confidentiality, authenticity and integrity of data traversing an untrusted network (e.g. Internet)

  Endpoint protection mechanisms (e.g. OS file access control, anti-virus software, host firewall) to harden end devices (servers and desktops)

Security Agent

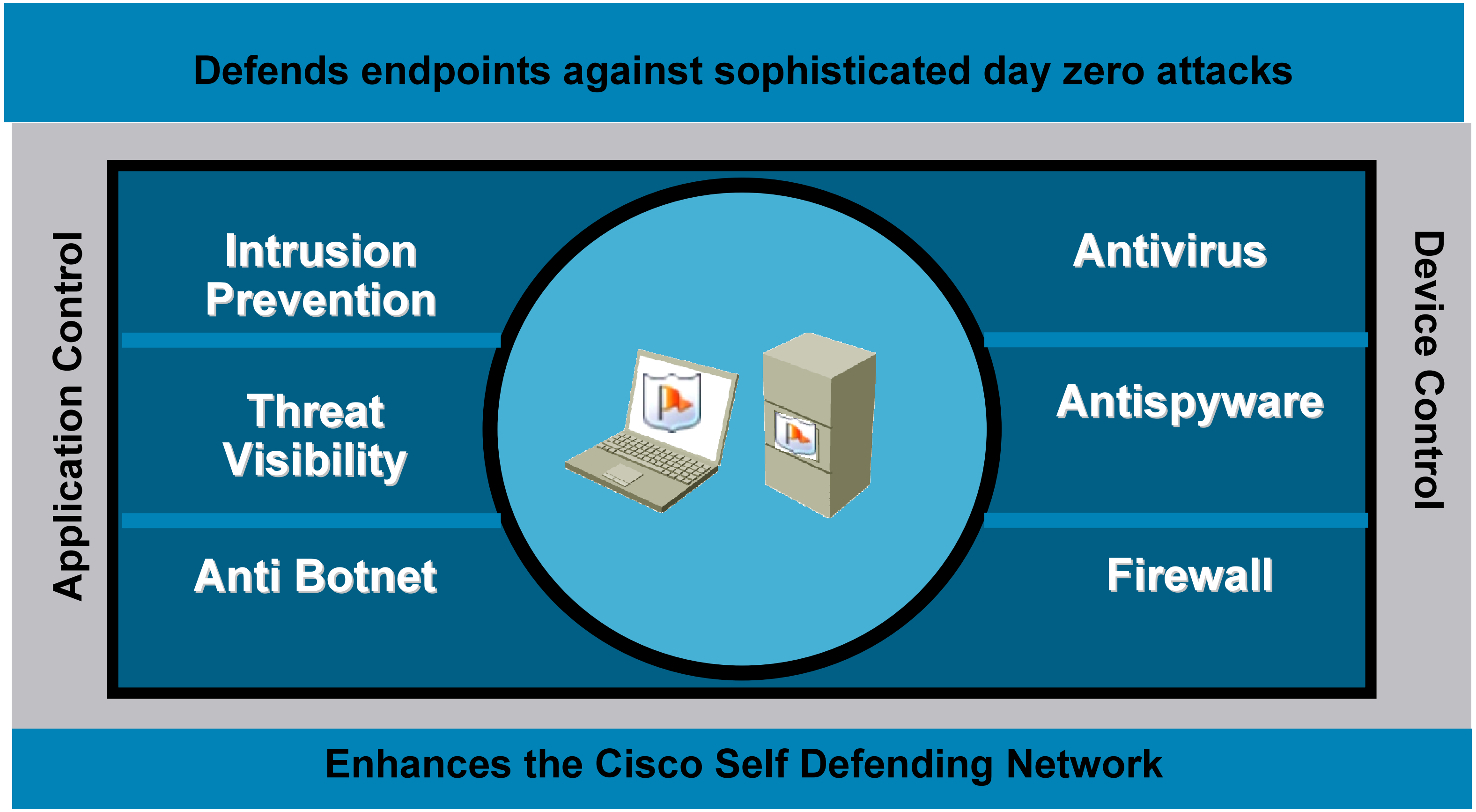
Always Vigilant Comprehensive Endpoint Security



“Zero Update” Protection Stops Malicious Mobile Code, Worms, Rootkits, Day-Zero and Targeted Attacks

SINGLE INTEGRATED AGENT AND MANAGEMENT

Complete Endpoint Security



Defends endpoints against sophisticated day zero attacks

Application Control

Intrusion Prevention

Threat Visibility

Anti Botnet

Antivirus

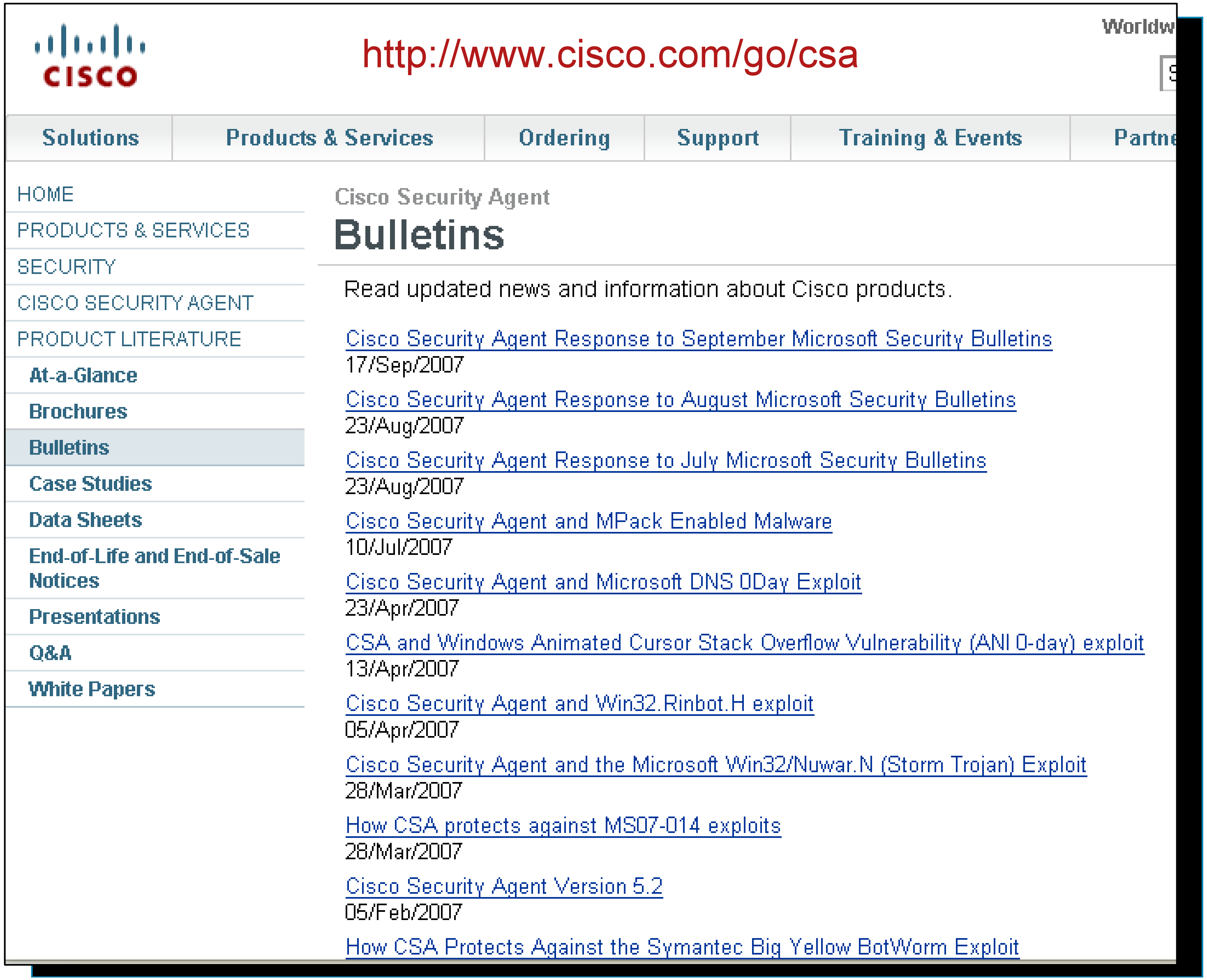
Antispyware

Firewall

Device Control

Enhances the Cisco Self Defending Network

Detailed Zero-Update Malware Notes



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

Cisco Security Agent

Bulletins

Read updated news and information about Cisco products.

Cisco Security Agent Response to September Microsoft Security Bulletins
17/Sep/2007

Cisco Security Agent Response to August Microsoft Security Bulletins
23/Aug/2007

Cisco Security Agent Response to July Microsoft Security Bulletins
23/Aug/2007

Cisco Security Agent and MPack Enabled Malware
10/Jul/2007

Cisco Security Agent and Microsoft DNS 0Day Exploit
23/Apr/2007

CSA and Windows Animated Cursor Stack Overflow Vulnerability (ANI 0-day) exploit
13/Apr/2007

Cisco Security Agent and Win32.Rinbot.H exploit
05/Apr/2007

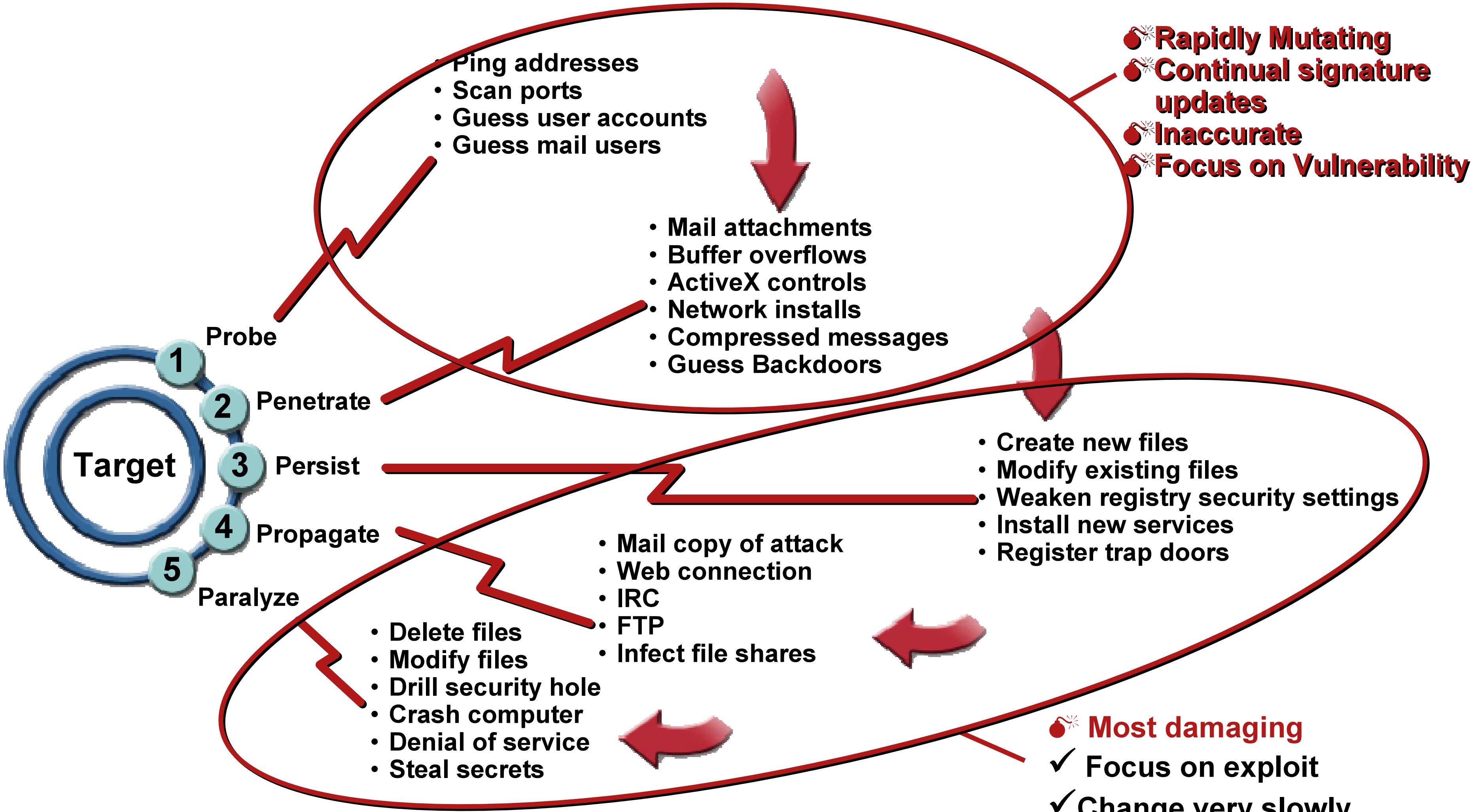
Cisco Security Agent and the Microsoft Win32/Nuwar.N (Storm Trojan) Exploit
28/Mar/2007

How CSA protects against MS07-014 exploits
28/Mar/2007

Cisco Security Agent Version 5.2
05/Feb/2007

How CSA Protects Against the Symantec Big Yellow BotWorm Exploit

Behavioral Protection for Endpoints



Target

1 Probe

2 Penetrate

3 Persist

4 Propagate

5 Paralyze

- Ping addresses
- Scan ports
- Guess user accounts
- Guess mail users

- Mail attachments
- Buffer overflows
- ActiveX controls
- Network installs
- Compressed messages
- Guess Backdoors

- Create new files
- Modify existing files
- Weaken registry security settings
- Install new services
- Register trap doors

- Mail copy of attack
- Web connection
- IRC
- FTP
- Infect file shares

- Delete files
- Modify files
- Drill security hole
- Crash computer
- Denial of service
- Steal secrets

- Rapidly Mutating
- Continual signature updates
- Inaccurate
- Focus on Vulnerability

- Most damaging

✓ Focus on exploit

✓ Change very slowly

✓ Inspiration for Cisco Security Agent solution

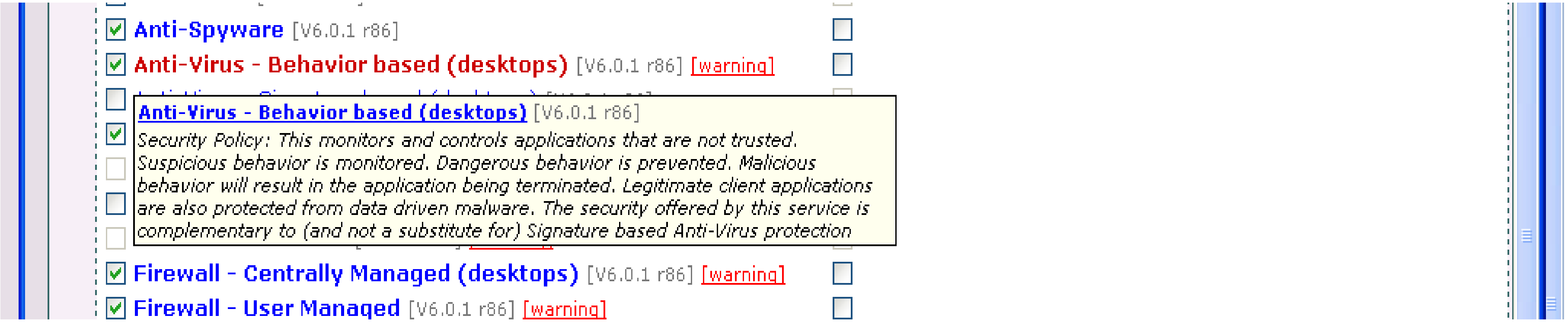
“Host” Security Policies

Policy Description	Function
Antivrus-Behavior-Based (Main Policy)	This monitors and controls applications that are not trusted. Suspicious behavior is monitored. Dangerous behavior is prevented. Malicious behavior will result in the application being terminated. Legitimate client applications are also protected from data driven malware.
Anti-Spyware	This protects against Spyware. It detects applications which monitor user input, as well as media devices. It also detects the modification of browser settings.
Anti-Rootkit	This detects the modification of the operating system kernel functionality by rootkits.
Firewall- Centrally Managed	This provides a centrally managed distributed firewall for Desktop Systems. Outgoing connections are allowed. Incoming connections to fixed or well known server ports are denied. Protection from network based attacks is also provided. This includes protection against Buffer Overflows, as well as IP packet based exploits.

“Zero Update” Security Policies

Policy Description	Function
Quarantined Compromised Hosts	This quarantines systems that have been compromised by a rootkit, preventing communication on the network.
Quarantined Compromised Applications	This quarantines compromised applications, and prevents them from harming the system or other applications
Audit System Inetgrity	This detects suspicious behavior on hosts, as well as system configuration changes which may affect system integrity.

Security- Antivirus- Behavior Based



☑ Anti-Spyware [V6.0.1 r86] □

☑ Anti-Virus - Behavior based (desktops) [V6.0.1 r86] [warning] □

Anti-Virus - Behavior based (desktops) [V6.0.1 r86]

Security Policy: This monitors and controls applications that are not trusted. Suspicious behavior is monitored. Dangerous behavior is prevented. Malicious behavior will result in the application being terminated. Legitimate client applications are also protected from data driven malware. The security offered by this service is complementary to (and not a substitute for) Signature based Anti-Virus protection

☑ Firewall - Centrally Managed (desktops) [V6.0.1 r86] [warning] □

☑ Firewall - User Managed [V6.0.1 r86] [warning] □

–Downloaded applications are executable file types

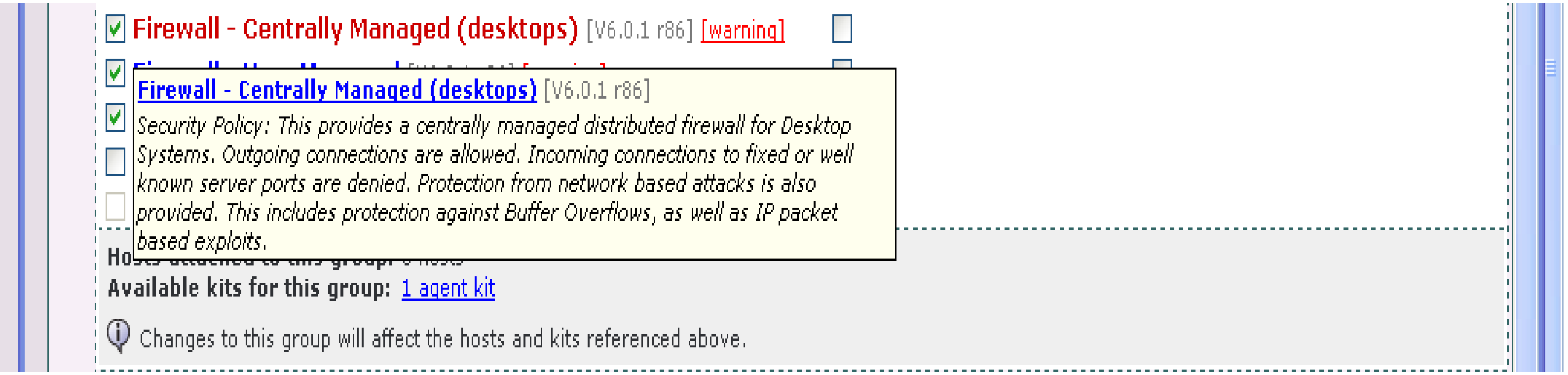
–Downloaded data are non-executable files containing scriptable executable code, or a buffer overflow exploit

–User expects “Funny Bunny” game – user gets Funny Bunny trojan

–Data can arrive via any protocol or client

- Email, browser, Instant Messenger, P2P, file shares, etc
- Content can include Office, Video, Audio, PDF, etc

Security - Firewall Centrally Managed



☑ Firewall - Centrally Managed (desktops) [V6.0.1 r86] [warning] □

☑

☑

□

□

Firewall - Centrally Managed (desktops) [V6.0.1 r86]

Security Policy: This provides a centrally managed distributed firewall for Desktop Systems. Outgoing connections are allowed. Incoming connections to fixed or well known server ports are denied. Protection from network based attacks is also provided. This includes protection against Buffer Overflows, as well as IP packet based exploits.

Ho

Available kits for this group: 1 agent kit

Changes to this group will affect the hosts and kits referenced above.

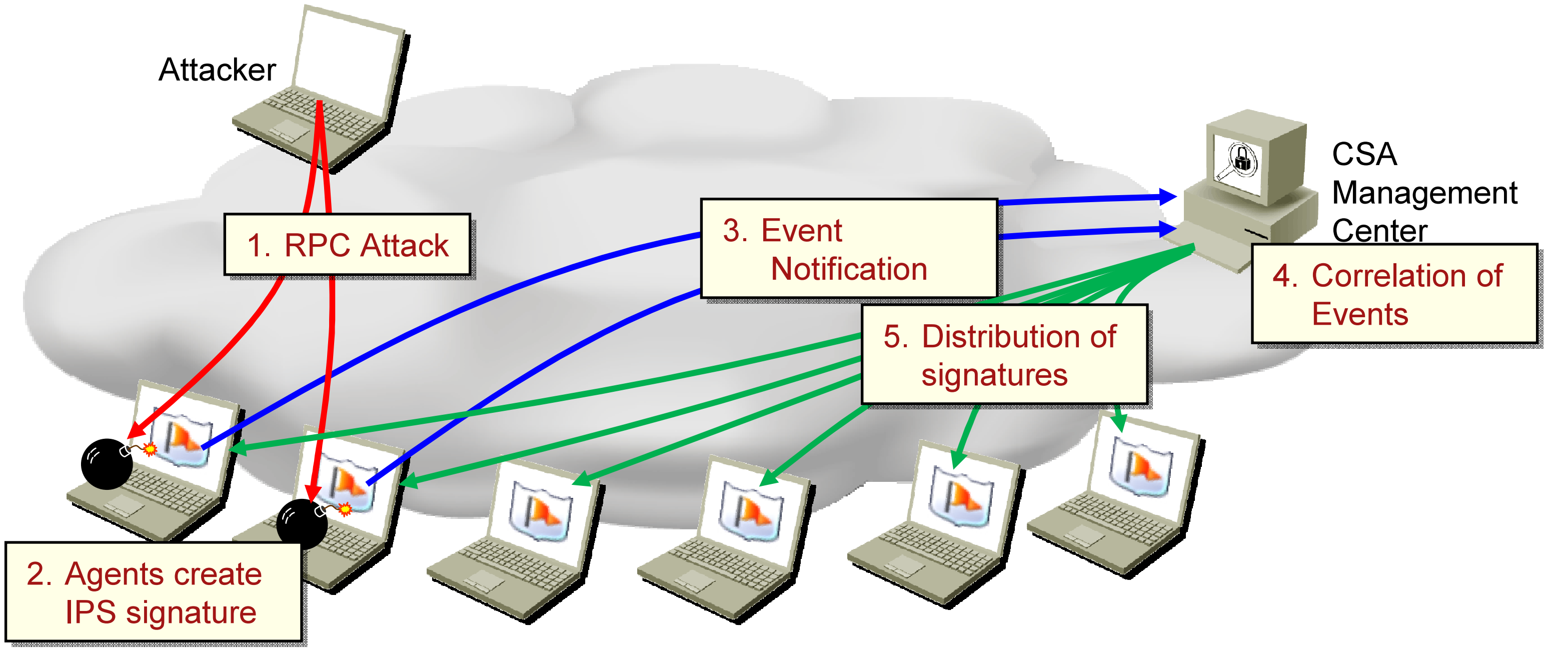
–Centrally defined per-application port blocking

–Inside-the-office/outside-the-office control

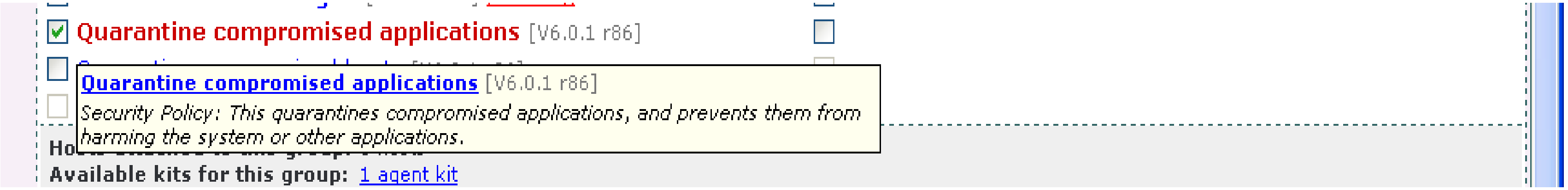
–Blocks network worms

–Windows service shielding/Buffer Overflow prevention and remediation

Dynamic Service Shielding



Security – Quarantine Compromised Applications



☑ Quarantine compromised applications [V6.0.1 r86]

Quarantine compromised applications [V6.0.1 r86]
Security Policy: This quarantines compromised applications, and prevents them from harming the system or other applications.

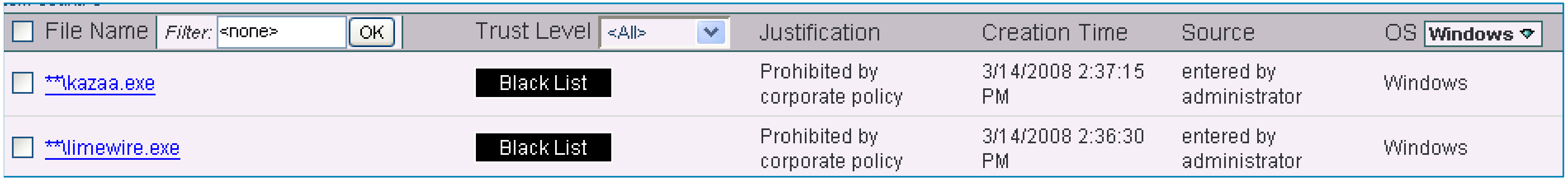
Available kits for this group: 1 agent kit

–Application quarantined if it is in “Suspect Virus Applications” state

- New variant, mutated virus – no signature yet

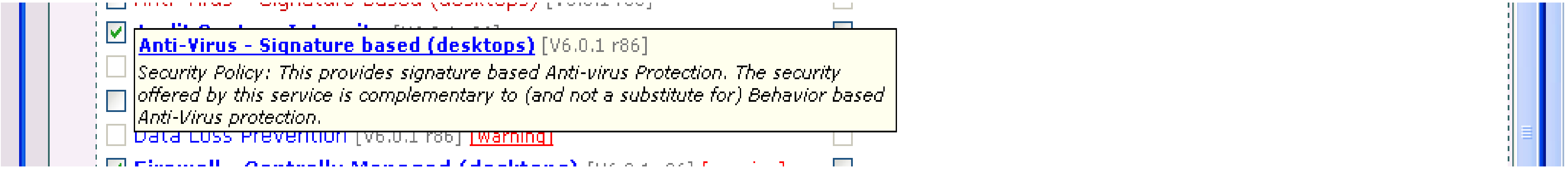
–Application quarantined if on centrally defined “Black List”

- Prohibit use of undesired applications like Limewire



□	File Name Filter: <none> OK	Trust Level <All>	Justification	Creation Time	Source	OS Windows
□	**\kazaa.exe	Black List	Prohibited by corporate policy	3/14/2008 2:37:15 PM	entered by administrator	Windows
□	**\limewire.exe	Black List	Prohibited by corporate policy	3/14/2008 2:36:30 PM	entered by administrator	Windows

AV Signature Based



☑ **Anti-Virus - Signature based (desktops)** [V6.0.1 r86]

Security Policy: This provides signature based Anti-virus Protection. The security offered by this service is complementary to (and not a substitute for) Behavior based Anti-Virus protection.

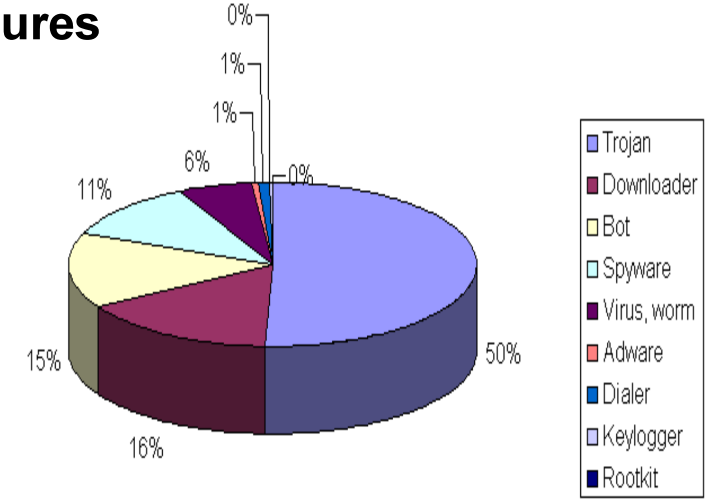
□ Data Loss Prevention [V6.0.1 r86] [warning]

- –CSA Day-Zero prevention stops virus execution
- –Open Source ClamAV detects malware by name
- –CSA quarantines and/or deletes malware identified by ClamAV
- –Enabled by CSA ClamAV Policy
- –Full scans can be performed on a weekly, and monthly schedule.
- –On demand-scans can also be performed by end user.

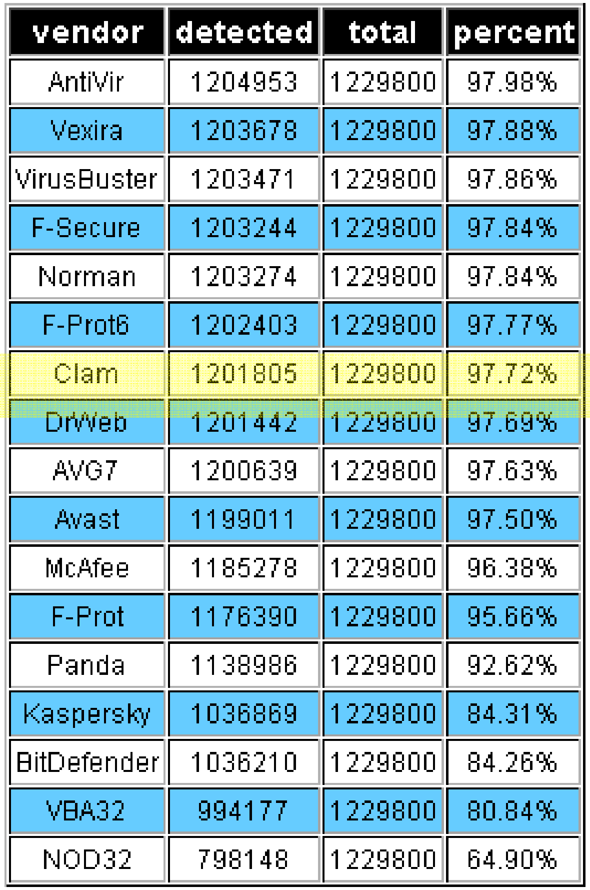
Integrated Agent

with Clam Antivirus

- ClamAV is widely deployed on UNIX/Linux e-mail servers
  - **–Scrubs e-mail traffic for malware**
  - **– Protects millions of Windows desktops**
  - **–Database contains over 200,000 unique signatures**



Shadowserver Foundation independent research: ClamAV has high degree of malware detection accuracy.



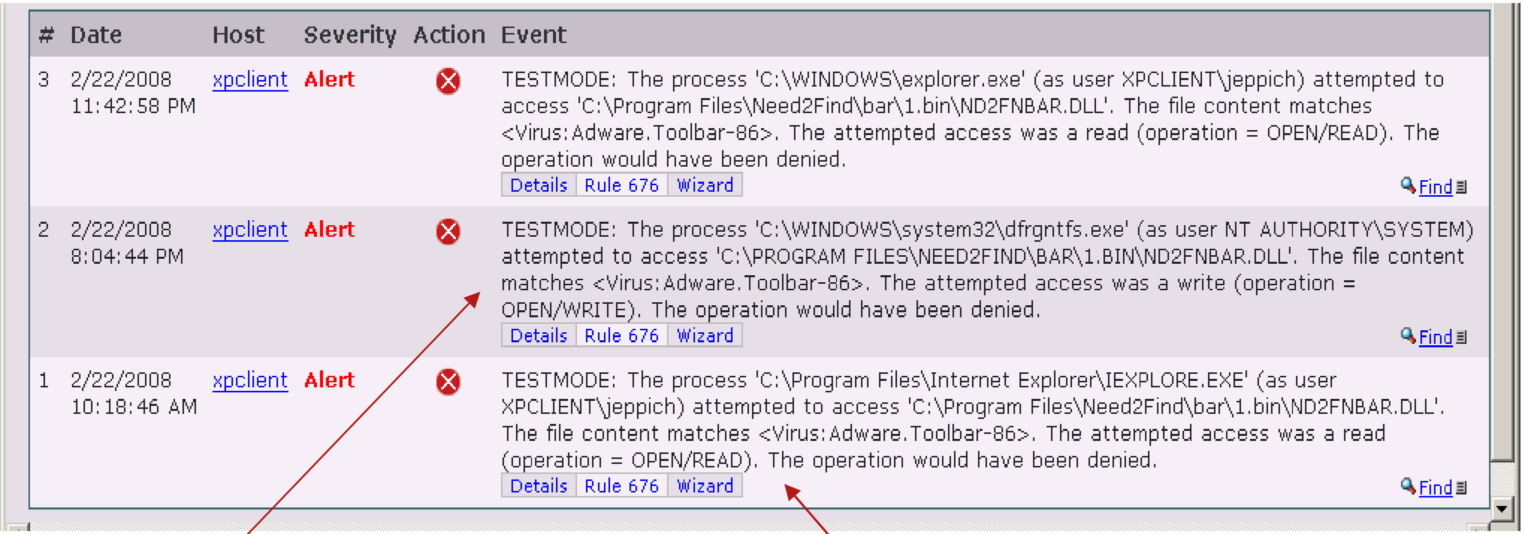
vendor	detected	total	percent
AntiVir	1204953	1229800	97.98%
Vexira	1203678	1229800	97.88%
VirusBuster	1203471	1229800	97.86%
F-Secure	1203244	1229800	97.84%
Norman	1203274	1229800	97.84%
F-Prot6	1202403	1229800	97.77%
Clam	1201805	1229800	97.72%
DrWeb	1201442	1229800	97.69%
AVG7	1200639	1229800	97.63%
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

CSA + ClamAV – A complete antivirus solution

Feature	Clam Only	CSA + Clam combo
Signature database	✓	✓
Bulk file system scan	✓	✓
Rapid Signature Update	✓	✓
On-Demand scan	✗	✓
Quarantine & delete malware	✗	✓
Centralized mgmt & reporting	✗	✓
Protection from day zero threats	✗	✓
Rootkit protection	✗	✓

CSA agent sends antivirus alerts to the CSA MC



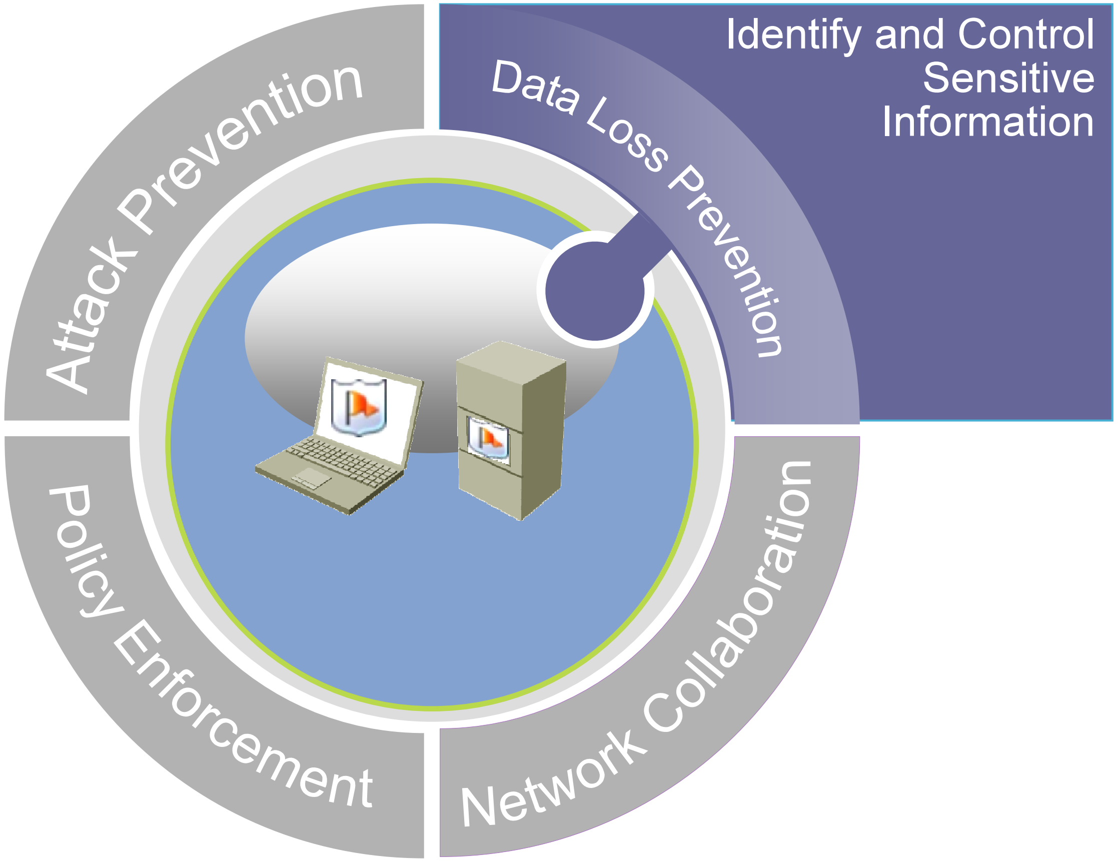
#	Date	Host	Severity	Action	Event
3	2/22/2008 11:42:58 PM	xpclient	Alert	⊗	TESTMODE: The process 'C:\WINDOWS\explorer.exe' (as user XPCLIENT\jeppich) attempted to access 'C:\Program Files\Need2Find\bar\1.bin\ND2FNBAR.DLL'. The file content matches <Virus:Adware.Toolbar-86>. The attempted access was a read (operation = OPEN/READ). The operation would have been denied. Details | Rule 676 | Wizard Find
2	2/22/2008 8:04:44 PM	xpclient	Alert	⊗	TESTMODE: The process 'C:\WINDOWS\system32\dfrgntfs.exe' (as user NT AUTHORITY\SYSTEM) attempted to access 'C:\PROGRAM FILES\NEED2FIND\BAR\1.BIN\ND2FNBAR.DLL'. The file content matches <Virus:Adware.Toolbar-86>. The attempted access was a write (operation = OPEN/WRITE). The operation would have been denied. Details | Rule 676 | Wizard Find
1	2/22/2008 10:18:46 AM	xpclient	Alert	⊗	TESTMODE: The process 'C:\Program Files\Internet Explorer\IEXPLORE.EXE' (as user XPCLIENT\jeppich) attempted to access 'C:\Program Files\Need2Find\bar\1.bin\ND2FNBAR.DLL'. The file content matches <Virus:Adware.Toolbar-86>. The attempted access was a read (operation = OPEN/READ). The operation would have been denied. Details | Rule 676 | Wizard Find

CSA Prevents malware installation

Clam AV detects malware

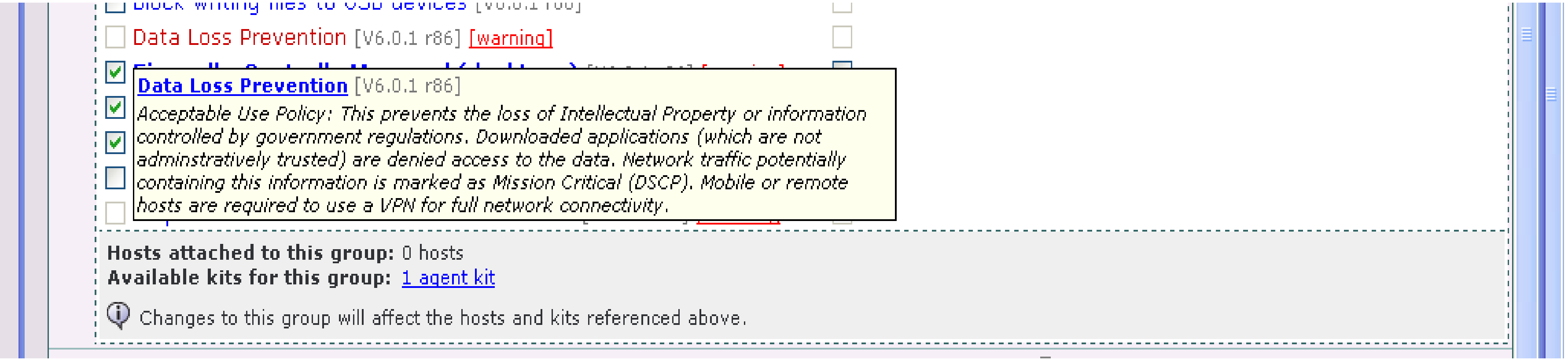
Cisco Security Agent

Always Vigilant Comprehensive Endpoint Security



SINGLE INTEGRATED AGENT AND MANAGEMENT

Data Loss Prevention



□ Block writing files to USB devices [V6.0.1 r86] □

□ Data Loss Prevention [V6.0.1 r86] [warning] □

Data Loss Prevention [V6.0.1 r86]

Acceptable Use Policy: This prevents the loss of Intellectual Property or information controlled by government regulations. Downloaded applications (which are not adminstratively trusted) are denied access to the data. Network traffic potentially containing this information is marked as Mission Critical (DSCP). Mobile or remote hosts are required to use a VPN for full network connectivity.

Hosts attached to this group: 0 hosts

Available kits for this group: 1 agent kit

Changes to this group will affect the hosts and kits referenced above.

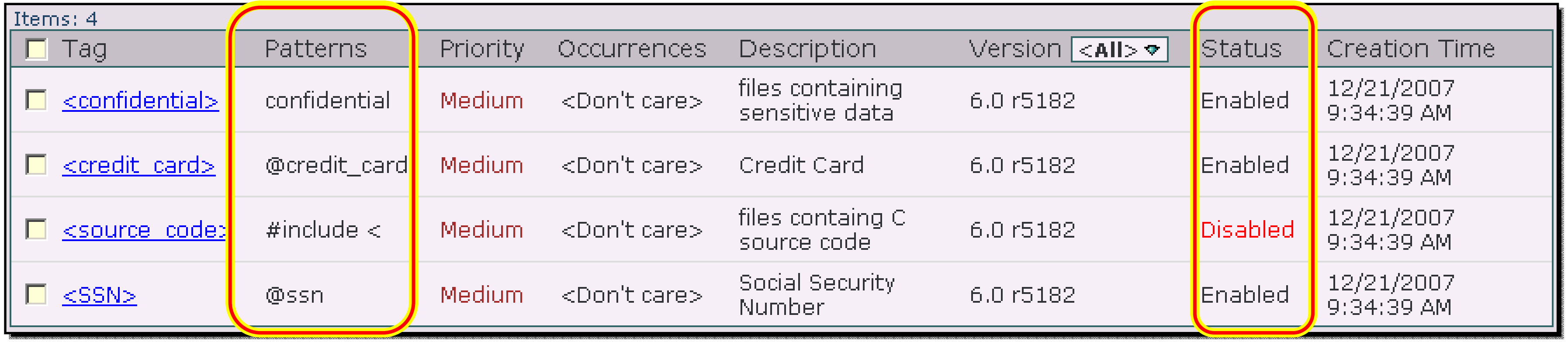
CSA incorporates DLP Policy and controls to educate or prevent users from Violating Corporate Security Policies surrounding sensitive information.

These policies also protect the information from malicious threats.

Remote users must have VPN connection established in order to access corporate sensitive data.

Identify Sensitive Data – *Content* or *Context*

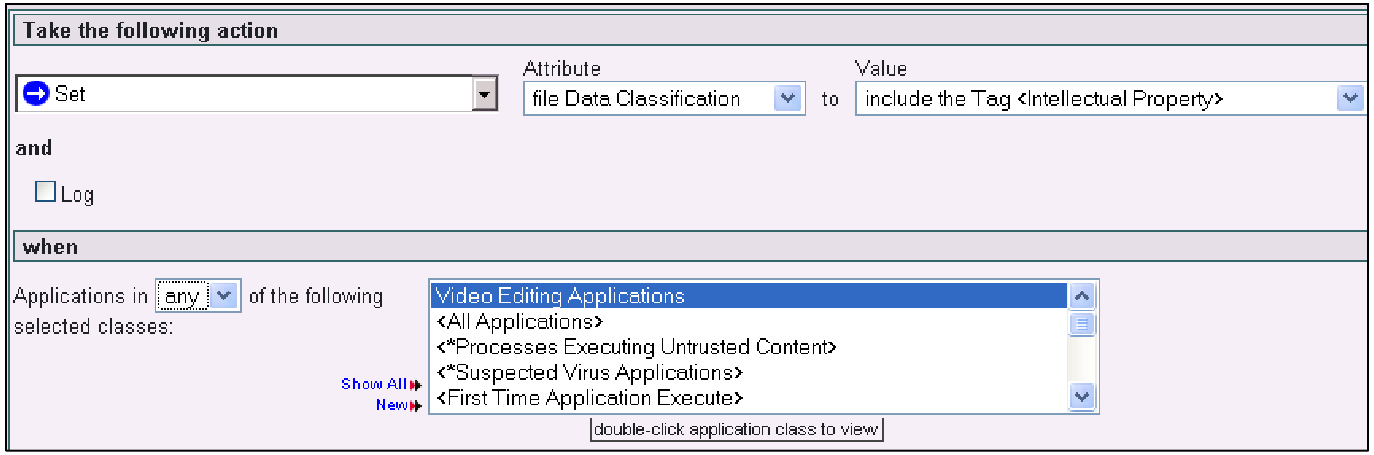
File Content – certain data patterns are recognized



Items: 4

□ Tag	Patterns	Priority	Occurrences	Description	Version <All>	Status	Creation Time
□ <confidential>	confidential	Medium	<Don't care>	files containing sensitive data	6.0 r5182	Enabled	12/21/2007 9:34:39 AM
□ <credit_card>	@credit_card	Medium	<Don't care>	Credit Card	6.0 r5182	Enabled	12/21/2007 9:34:39 AM
□ <source_code>	#include <	Medium	<Don't care>	files containg C source code	6.0 r5182	Disabled	12/21/2007 9:34:39 AM
□ <SSN>	@ssn	Medium	<Don't care>	Social Security Number	6.0 r5182	Enabled	12/21/2007 9:34:39 AM

File Context – data written by certain applications is known to be sensitive



Take the following action

Set

Attribute: file Data Classification to Value: include the Tag <Intellectual Property>

and

□ Log

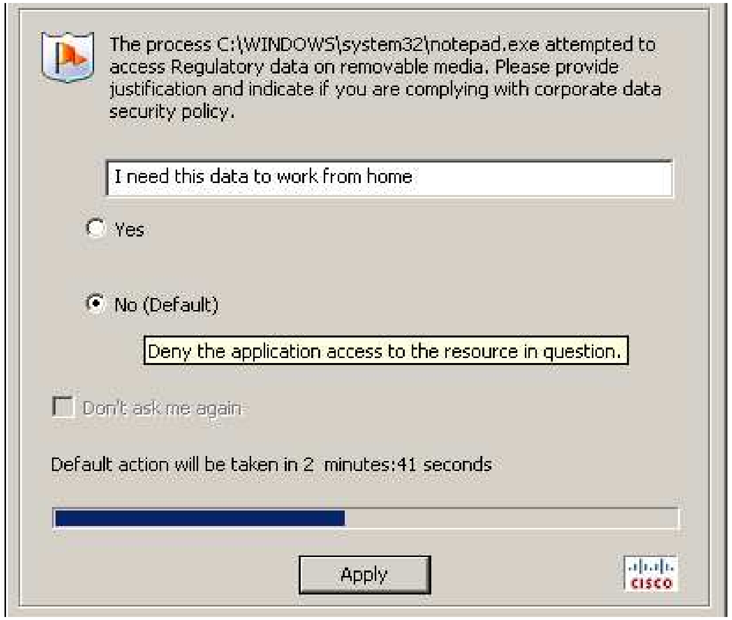
when

Applications in any of the following selected classes:

- Video Editing Applications
- <All Applications>
- <*Processes Executing Untrusted Content>
- <*Suspected Virus Applications>
- <First Time Application Execute>

Educate /and or Enforce

- Educate the user, if the user is non-compliant, business justification notices can be applied.



The process C:\WINDOWS\system32\notepad.exe attempted to access Regulatory data on removable media. Please provide justification and indicate if you are complying with corporate data security policy.

I need this data to work from home

○ Yes

● No (Default)

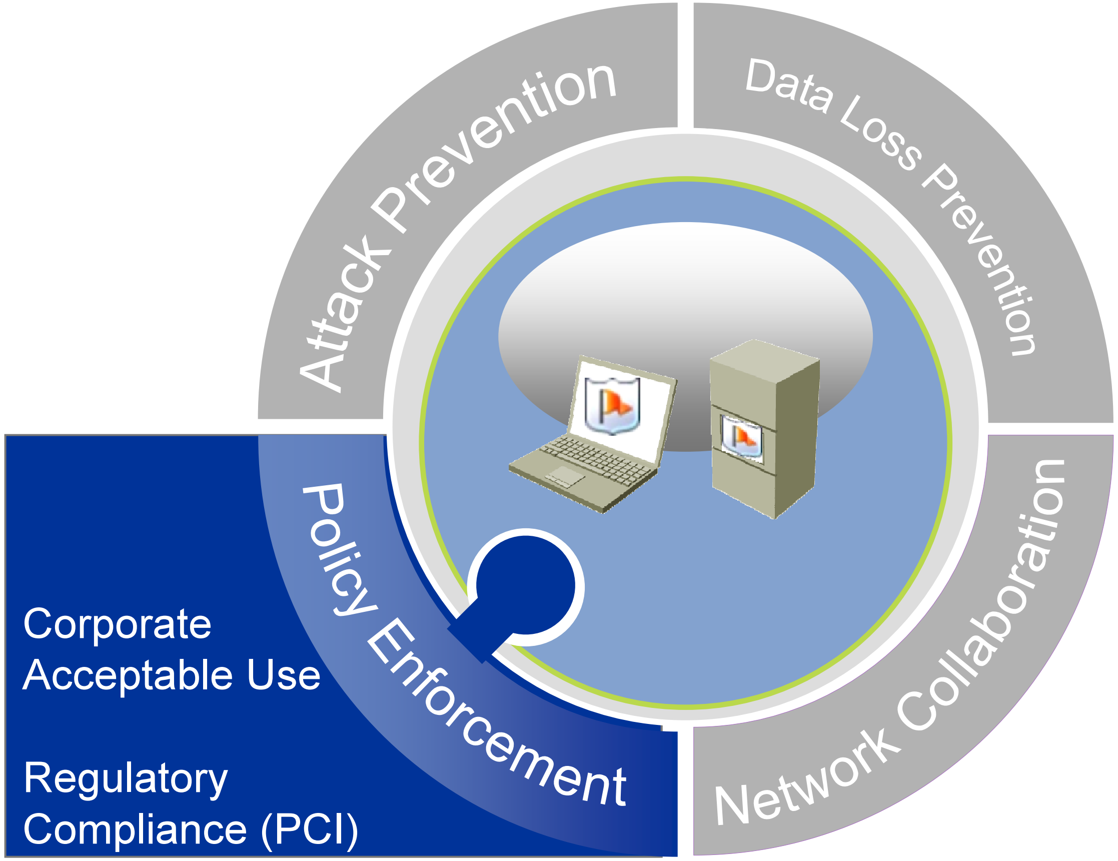
Deny the application access to the resource in question.

□ Don't ask me again

Default action will be taken in 2 minutes:41 seconds

Cisco Security Agent

Always Vigilant Comprehensive Endpoint Security

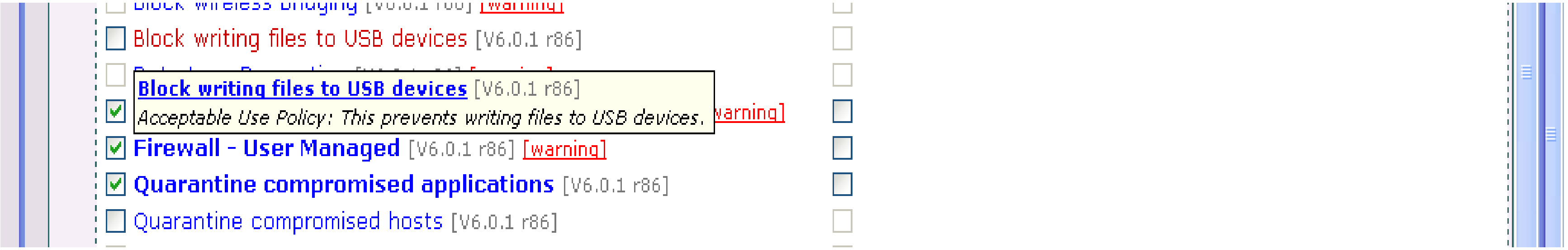


SINGLE INTEGRATED AGENT AND MANAGEMENT

CSA’s Acceptable Use Policies

Policy Description	Function
Block Writing Files to USB Devices	This prevents writing files to USB devices
Firewall - User Managed	Allow end users to further restrict network access above Distributed Firewall controls
PCI policies	PCI-certified policies for 9 out of 12 PCI requirements (available from Cisco on request)
Require VPN Hosts on Insecure Networks	This requires hosts on insecure wireless or remote networks, establish a VPN to the corporate network for full Internet connectivity.
Block Wireless Bridging	This prevents wireless network connectivity on hosts that are directly connected to the corporate (wired) ethernet.

Acceptable Use – Block writing files to USB



□ Block wireless bridging [V6.0.1 r86] [warning]

□ Block writing files to USB devices [V6.0.1 r86]

Block writing files to USB devices [V6.0.1 r86]

Acceptable Use Policy: This prevents writing files to USB devices.

☑ warning]

☑ **Firewall - User Managed** [V6.0.1 r86] [warning]

☑ **Quarantine compromised applications** [V6.0.1 r86]

□ Quarantine compromised hosts [V6.0.1 r86]

–Controls all USB file system types

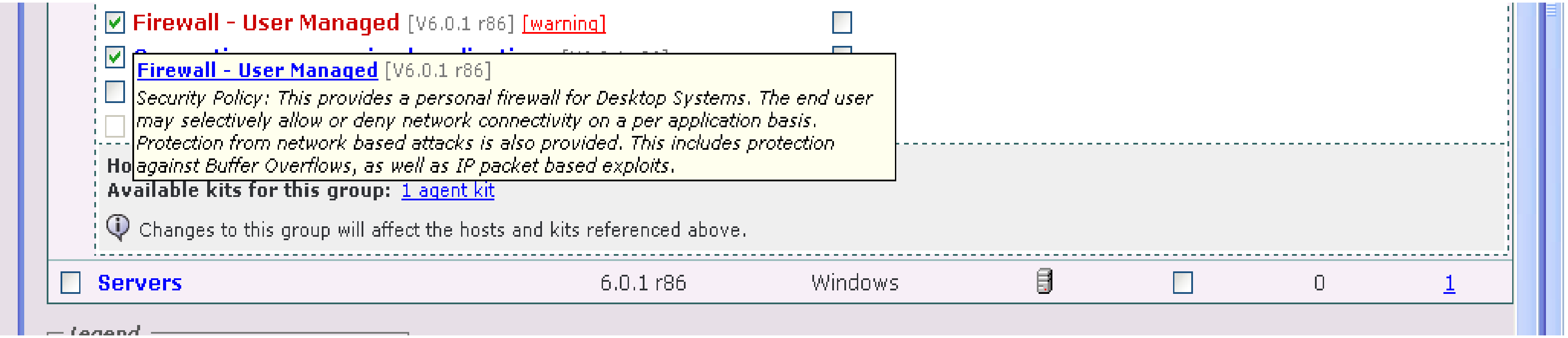
–Removable (memory stick) or fixed (iPod)

–Floppy, CD, Flash, Hard disk

–Default: Ask user to justify action

–Custom: Silent audit or block

Acceptable Use – Personal Firewall



☑ Firewall - User Managed [V6.0.1 r86] [warning] □

Firewall - User Managed [V6.0.1 r86]

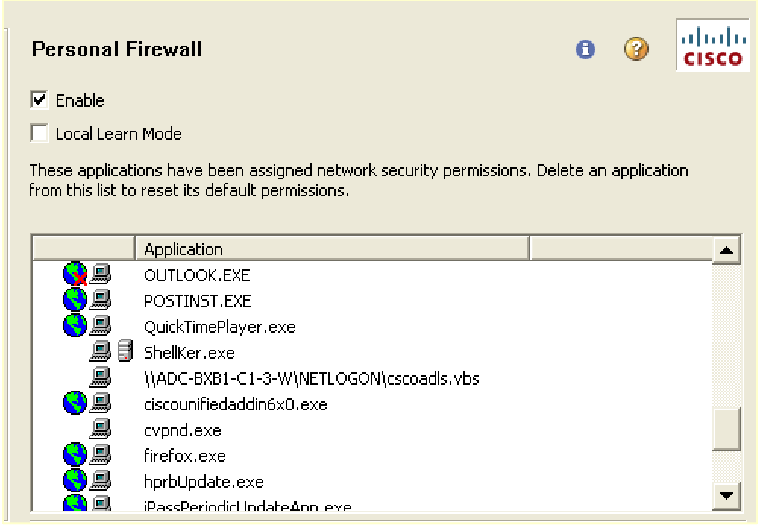
Security Policy: This provides a personal firewall for Desktop Systems. The end user may selectively allow or deny network connectivity on a per application basis. Protection from network based attacks is also provided. This includes protection against Buffer Overflows, as well as IP packet based exploits.

Available kits for this group: 1 agent kit

Changes to this group will affect the hosts and kits referenced above.

□ Servers 6.0.1 r86 Windows □ 0 1

- Allow end user to require more stringent control than central, distributed firewall policy
- Controlled via agent GUI
- User can Allow/Deny each application when it tries to use the network



Personal Firewall

☑ Enable

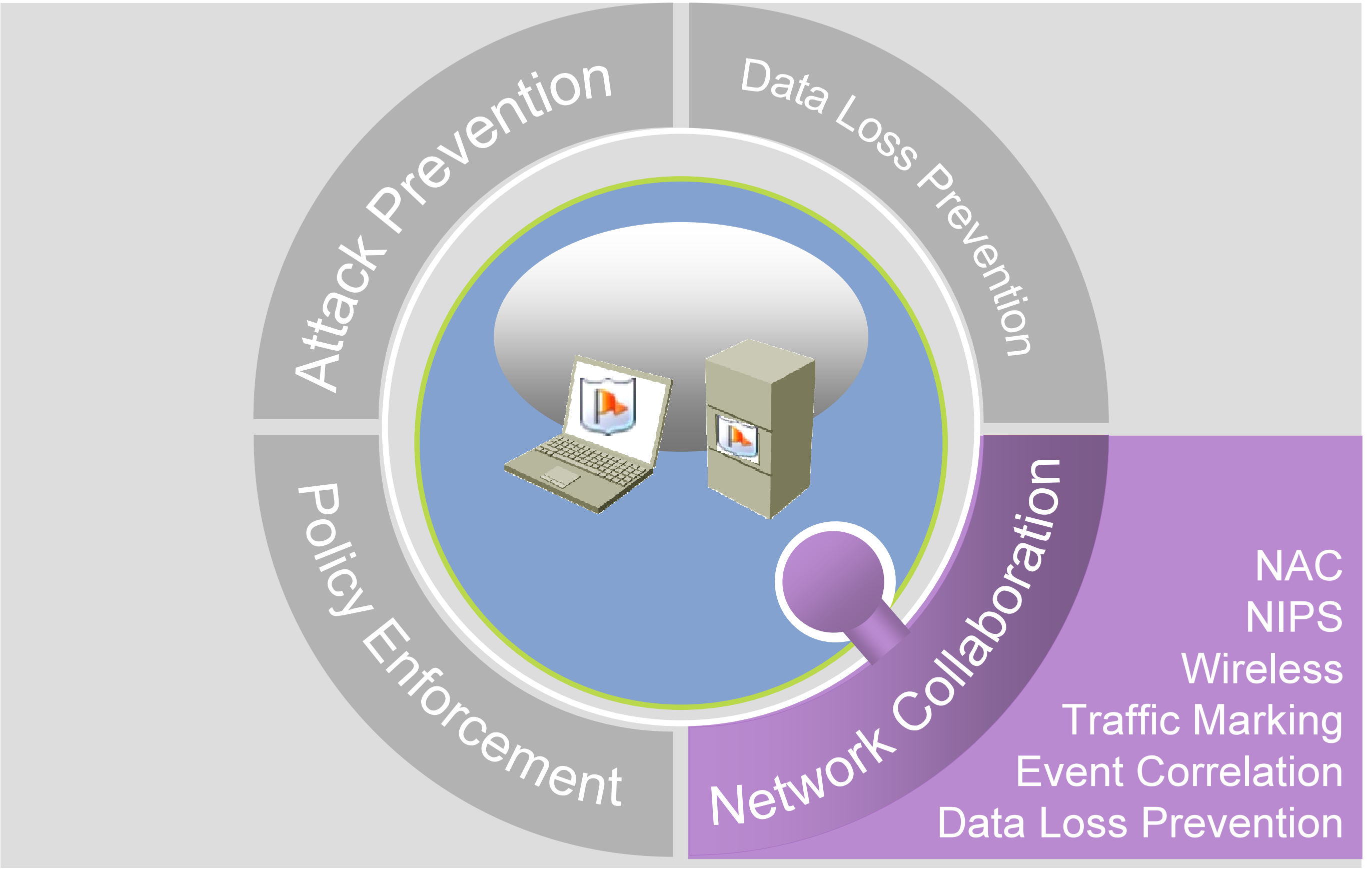
□ Local Learn Mode

These applications have been assigned network security permissions. Delete an application from this list to reset its default permissions.

Application
OUTLOOK.EXE
POSTINST.EXE
QuickTimePlayer.exe
ShellKer.exe
\\ADC-BXB1-C1-3-W\NETLOGON\cscoadls.vbs
ciscounifiedaddin6x0.exe
cvpnd.exe
firefox.exe
hprbUpdate.exe
iPassPeriodicUpdateApp.exe

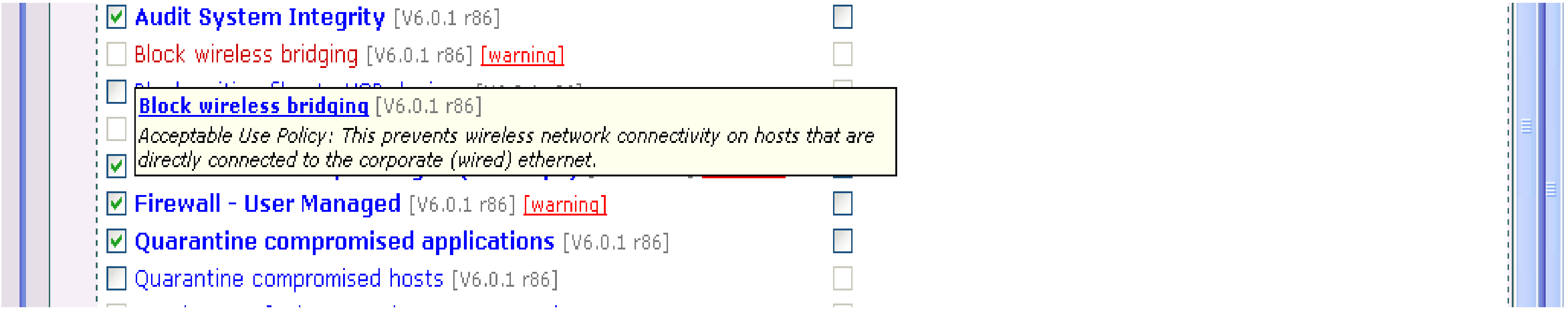
Cisco Security Agent

Always Vigilant Comprehensive Endpoint Security



SINGLE INTEGRATED AGENT AND MANAGEMENT

Acceptable Use – Wireless or Remote Hosts



☑ **Audit System Integrity** [V6.0.1 r86]

□ Block wireless bridging [V6.0.1 r86] [warning]

Block wireless bridging [V6.0.1 r86]

Acceptable Use Policy: This prevents wireless network connectivity on hosts that are directly connected to the corporate (wired) ethernet.

☑ **Firewall - User Managed** [V6.0.1 r86] [warning]

☑ **Quarantine compromised applications** [V6.0.1 r86]

□ Quarantine compromised hosts [V6.0.1 r86]

–Enforce corporate Wireless security policy

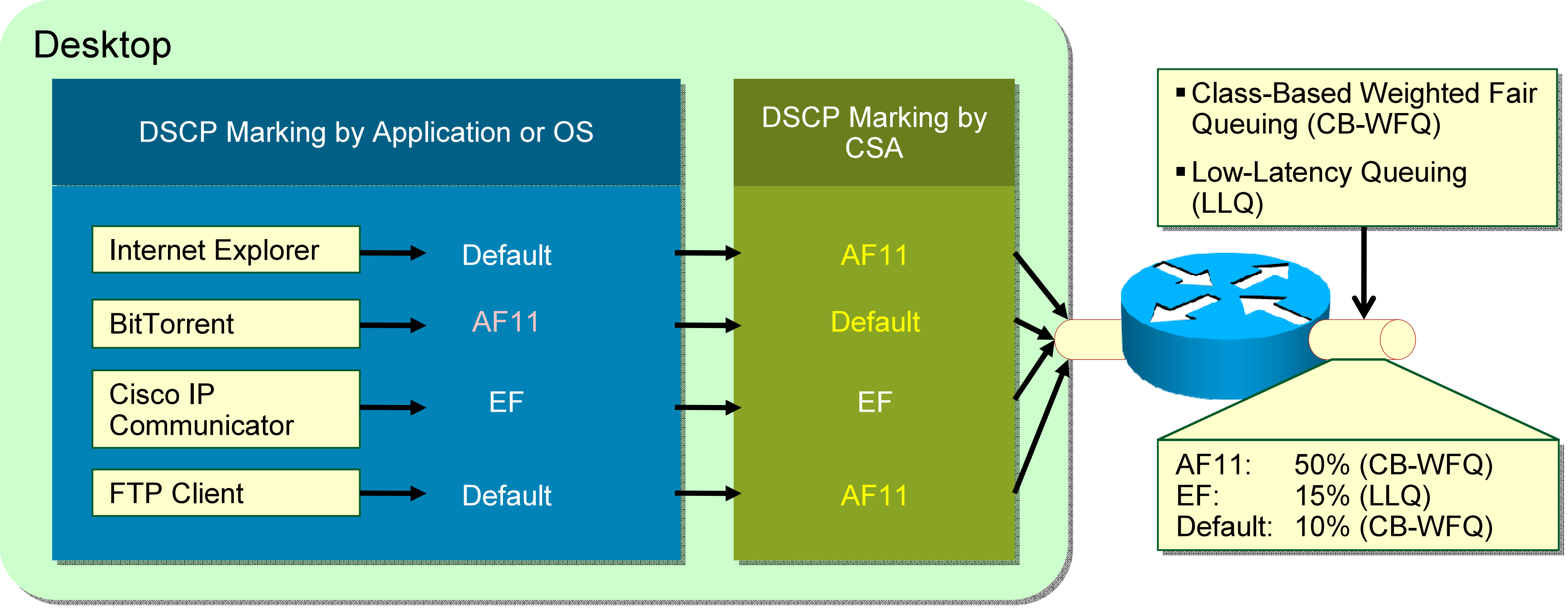
- Block use of Ad Hoc mode
- Block wireless-to-wired bridging when docked in office

–Require use of VPN if user is out of the office

–Optional: Require use of corporate SSID and encryption when available

Per-Application Network Optimization (QoS)

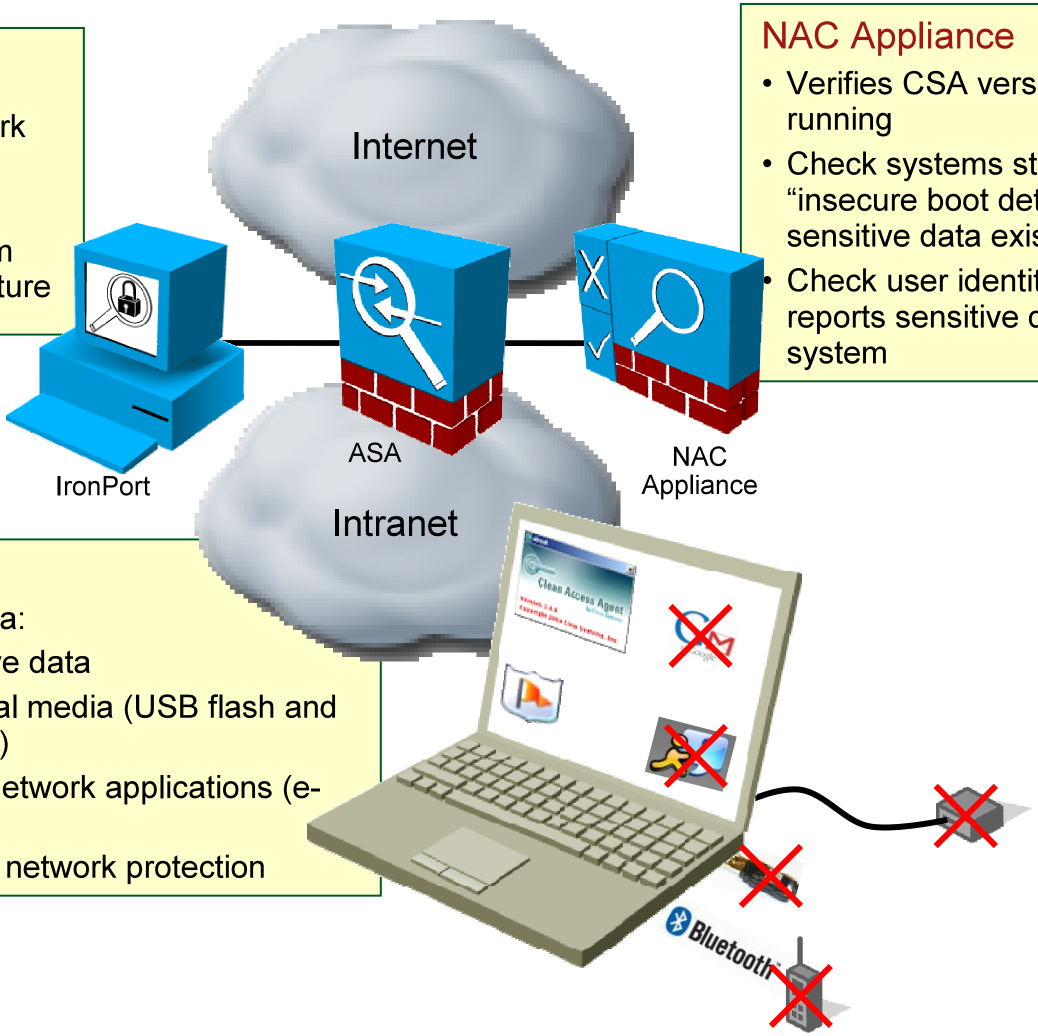
Available via Advanced GUI option on CSAMC



- “Bad” software can mark packets to:
    - Get a better service from the network
    - To perform an attack (e.g. flooding with EF-marked packets can cause DoS for IP telephony)
- Use CSA to remark packets according to QoS design

Network Integrated Solutions

CSA with NAC, DLP and IronPort



IronPort

- Prevent Data Loss at Network Perimeter
- Multi-Protocol Scanning
- Leverage Existing Anti-Spam and Anti-Spyware Infrastructure

NAC Appliance

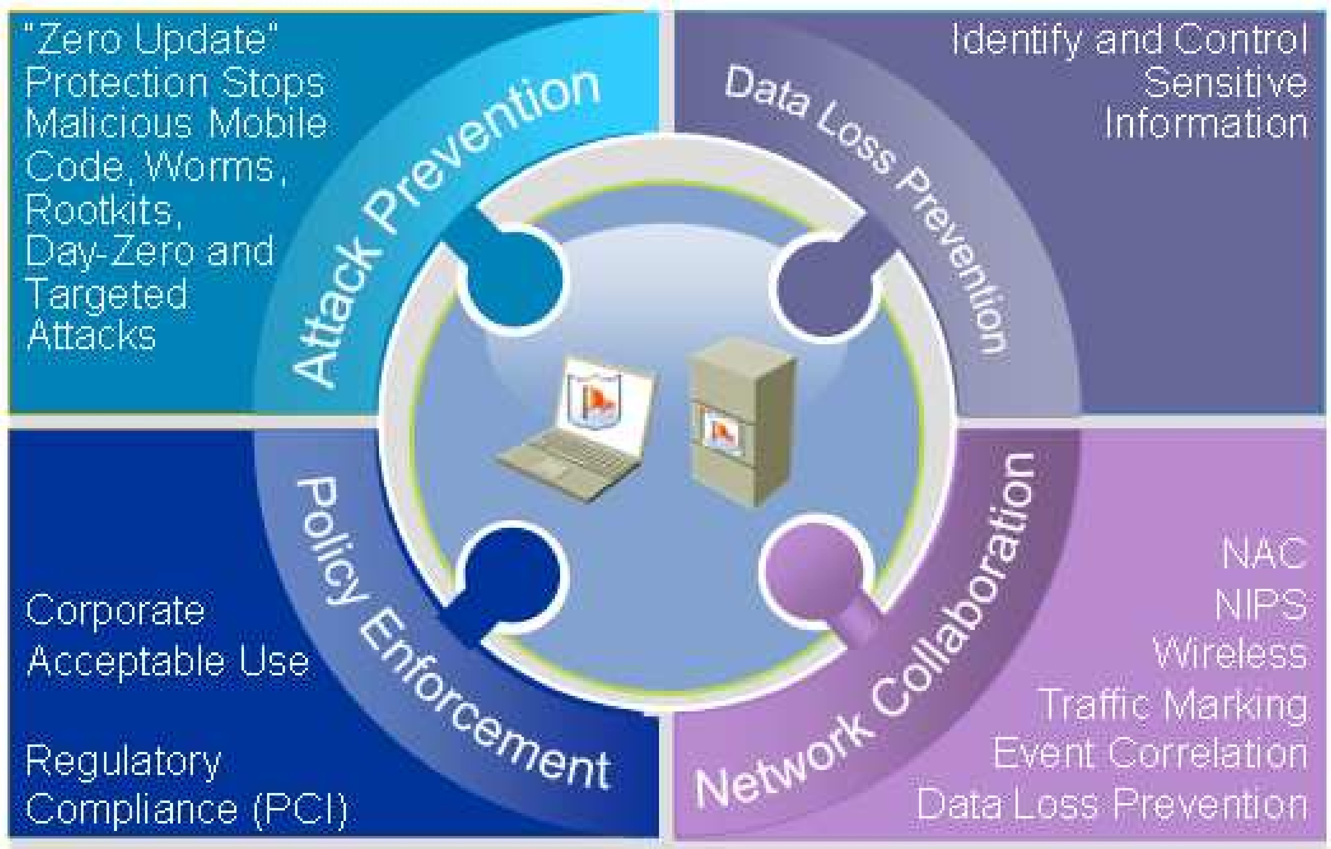
- Verifies CSA version and if it's running
- Check systems states like "insecure boot detected" and if sensitive data exists
- Check user identity if CSA reports sensitive data is on system

Cisco Security Agent

- Prevent loss of sensitive data:
  - Scan data files for sensitive data
  - Prevent copying to external media (USB flash and disk, IR/Bluetooth devices)
  - Prevent using with (inter)network applications (e-mail, IM, browser)
- Prevents bypass of IronPort network protection

Cisco Security Agent

Always Vigilant Comprehensive Endpoint Security



"Zero Update" Protection Stops Malicious Mobile Code, Worms, Rootkits, Day-Zero and Targeted Attacks

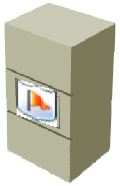
Identify and Control Sensitive Information

Corporate Acceptable Use

Regulatory Compliance (PCI)

NAC
NIPS
Wireless
Traffic Marking
Event Correlation
Data Loss Prevention

Laptop – Desktop Protection



Server Protection

POS Protection

SINGLE INTEGRATED AGENT AND MANAGEMENT