CISD Tech Day
Security

Peter Comeaux
peterc@cisco.com
Consulting Systems Engineer
ccie 10661

 © 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

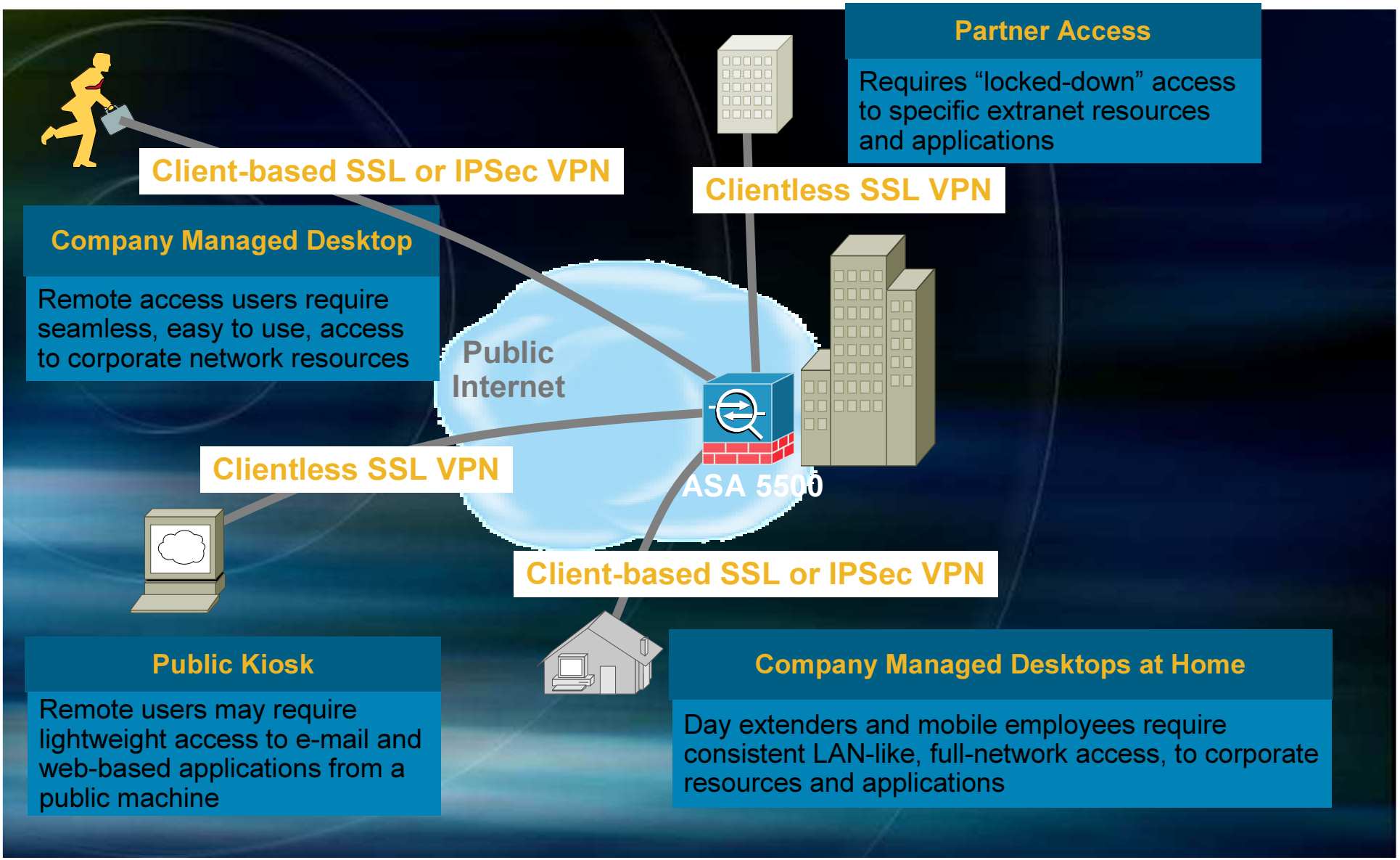
Agenda

- Physical Security
- IPSec VPN / SSL VPN
- Encryption
- Email Encryption
- Anti-Virus, Zero Day Attacks
- IPS
- Security Event Management

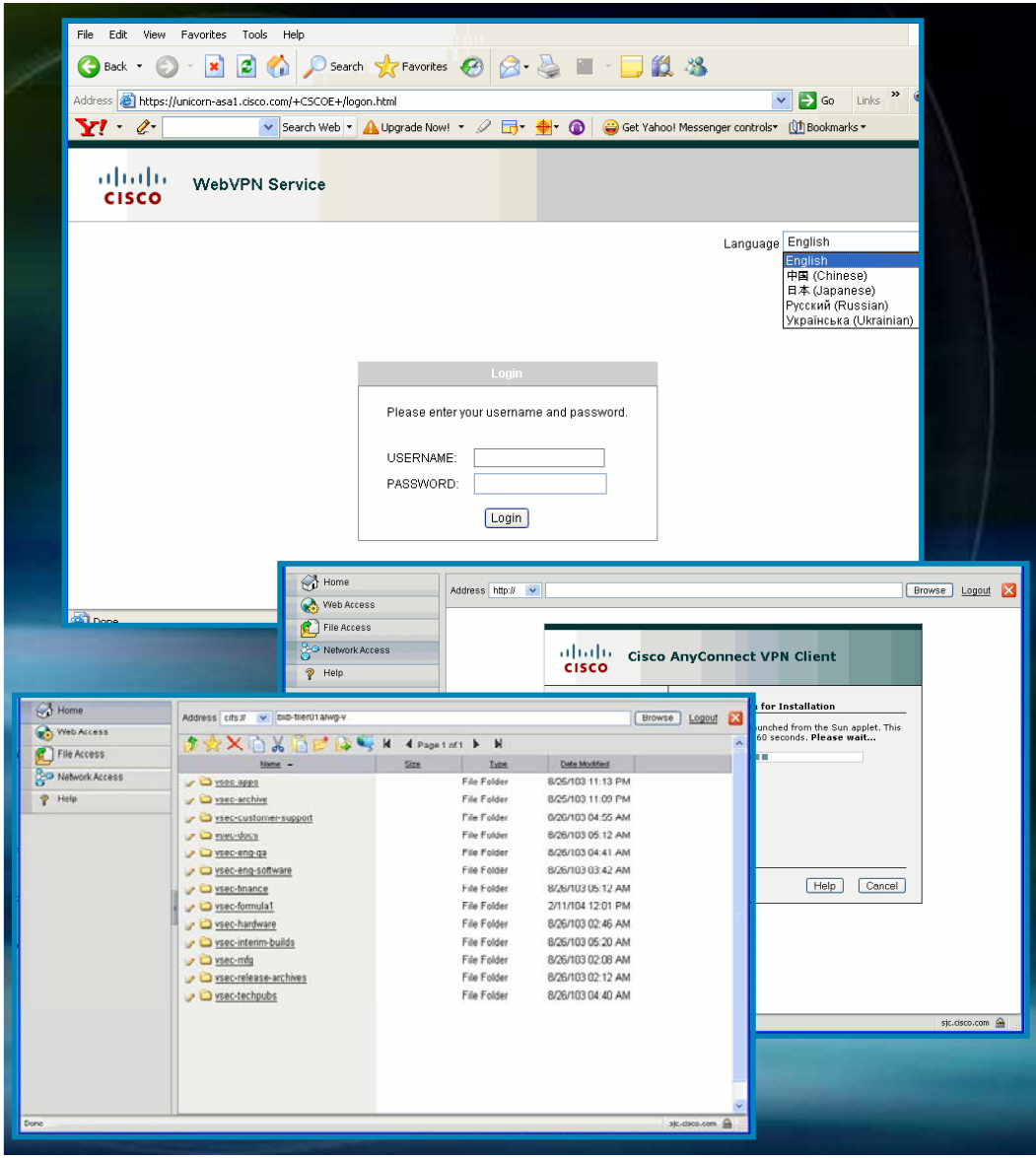
© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Comprehensive Secure Connectivity

VPN Services for Any Access Scenario



Cisco ASA 5500 Software v8.0 Introduces Significant Enhancements in Clientless Access



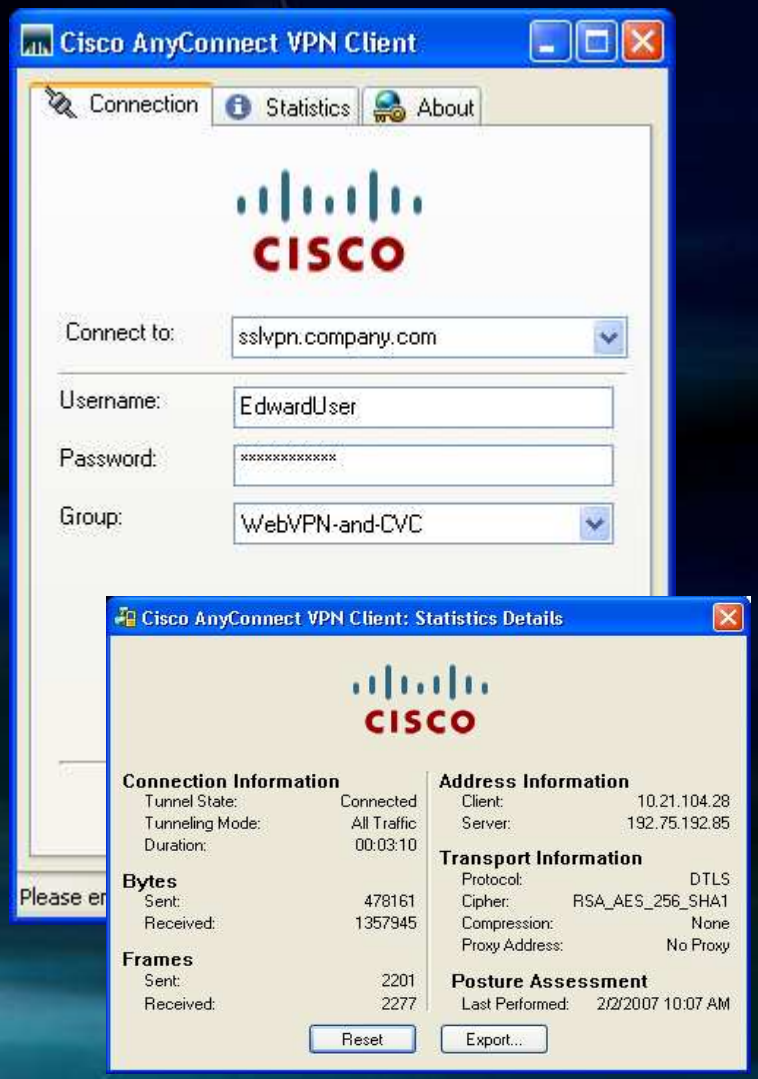
- Precise, granular access control to specific resources
- Enhanced Portal Design
  - Localizable
  - RSS feeds
  - Personal bookmarks
  - AnyConnect Client access
- Drag and Drop file access and webified file transport
- Transformation enhancements including Flash support
- Head-end deployed applets for telnet, SSH, RDP, and VNC, framework supports add'l plug-ins
- Advanced port-forwarder for Windows (Smart Tunnel) accesses TCP applications without admin privileges on Client PC

New in 8.0!

Cisco AnyConnect Client

New!

- **Next generation VPN client, available on many platforms including:**
  - Windows Vista 32- and 64-bit, Windows XP 32- and 64-bit, and Windows 2000
  - Mac OS X 10.4 (Intel and PPC)
  - Intel-based Linux
  - Windows Mobile Pocket PC Edition
- **Stand-alone, Web Launch, and Portal Connection Modes**
- **Start before Login (SBL) and DTLS support**
  - **Windows 2000 and XP only**



Comprehensive EndPoint Security

- Cisco Secure Desktop (CSD) now supports hundreds of pre-defined products, updated frequently

  New in 8.0!

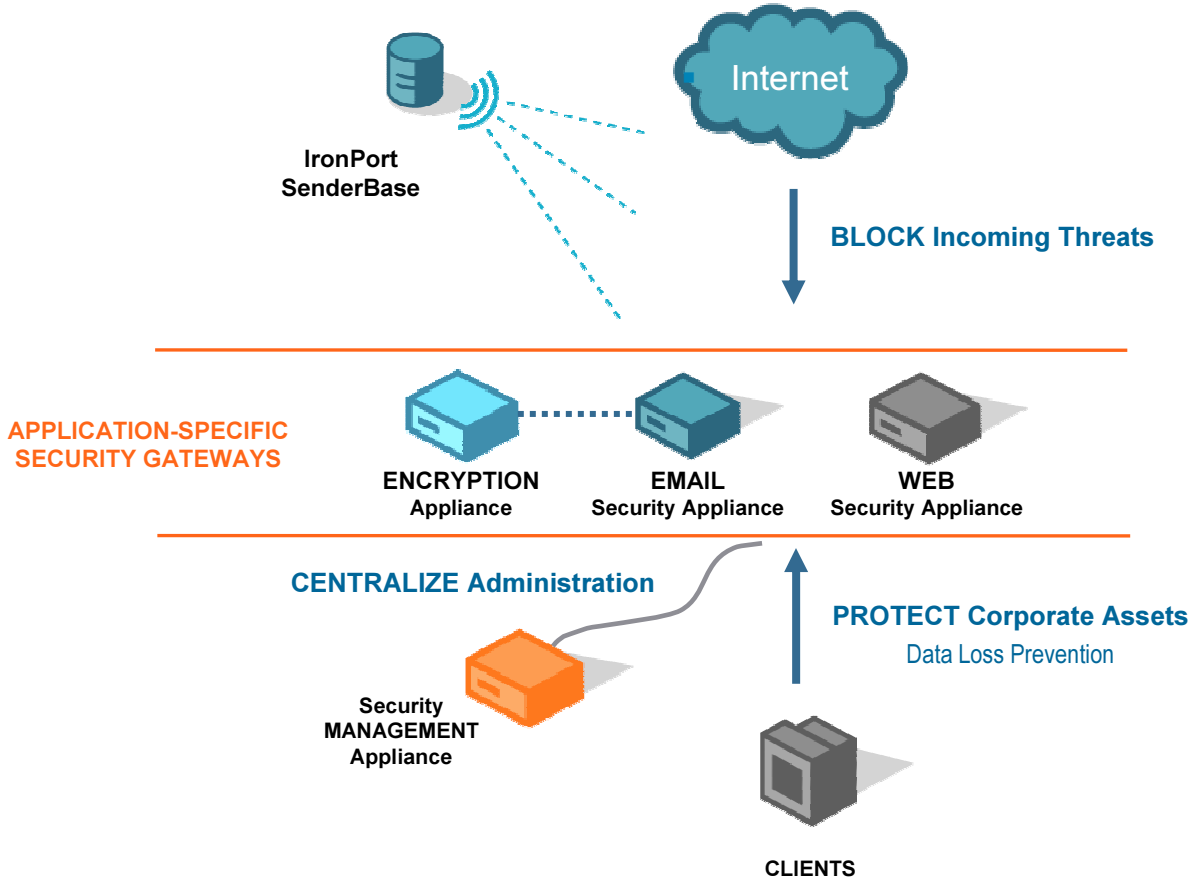
  Anti-virus, anti-spyware, personal firewall, and more
- Administrators can define custom checks including running processes
- CSD posture policy presented visually to simplify configuration and troubleshooting

Agenda

- Physical Security
- IPSec VPN / SSL VPN
- Encryption
- Email Encryption
- Anti-Virus, Zero Day Attacks
- IPS
- Security Event Management

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

IronPort® Gateway Security Products

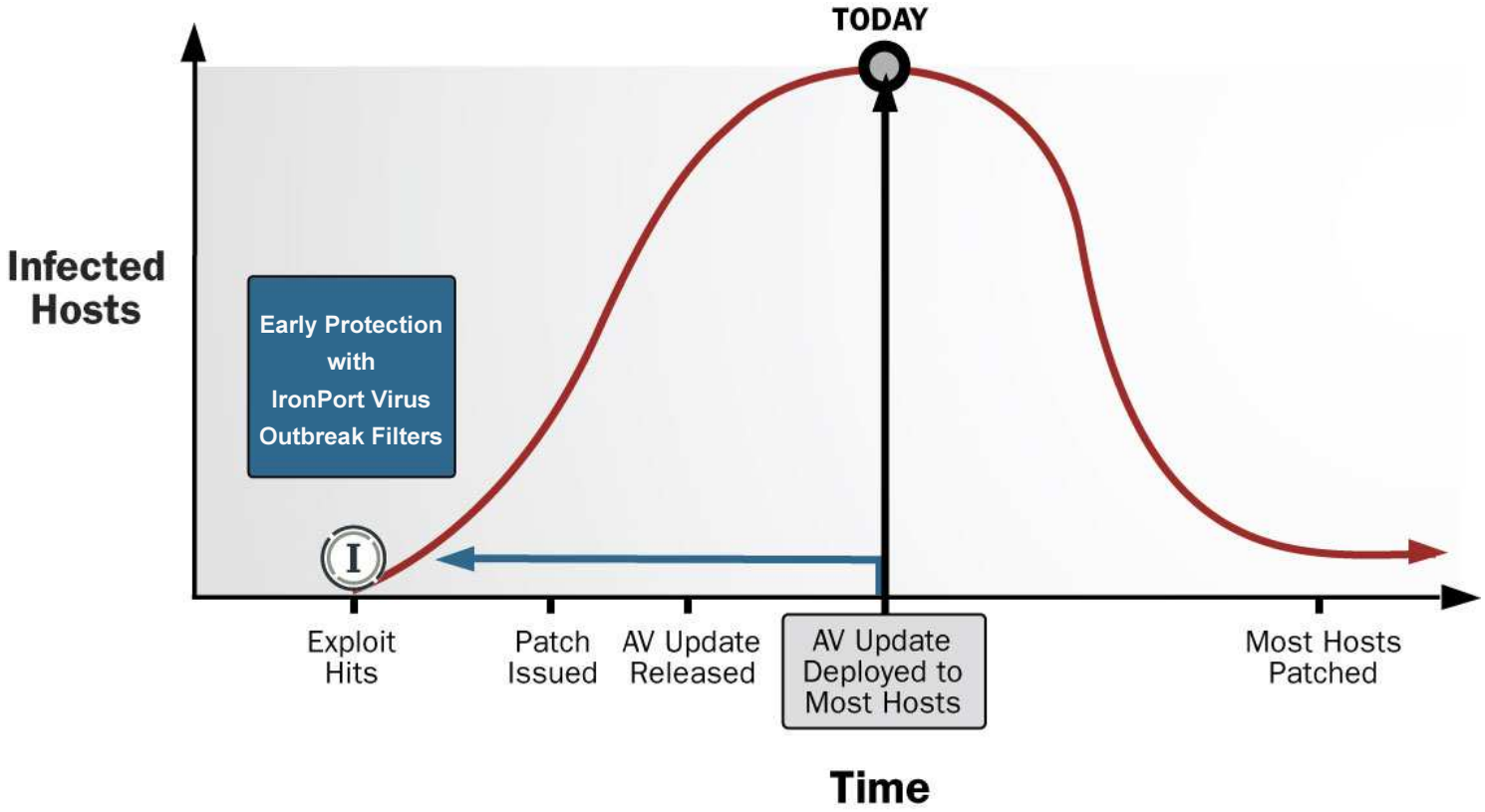


Web Security | **Email Security** | **Security Management** | **Encryption**

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

IronPort Virus Outbreak Filters

The First Line of Defense



© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

The IronPort Virus Outbreak Filters Advantage

Virus Name	Date	Virus Description	Lead Time (hh:mm)
Troj/Yar-A	5/24/07	Widely-spammed out email teaser promising a trailer of the film "Pirates of the Caribbean 3“. Downloads spyware onto infected computers.	3:20
Trojan.Dropper	5/10/07	Trojan that attempts to download malicious code.	10:40
W32.Virut!dr	4/12/07	Spammed email that asks recipients to open attachments entitled “document.txt.exe” and “video.zip”. Downloads spyware onto infected computers.	31:12
Troj/DwnLdr-GFN	3/4/07	Installs backdoor and communicates via HTTP, thus bypassing firewall filters.	17:31
W32/WowPWS-AU	3/3/07	Mass mailing worm that sends emails with the subject: "Chinese test missile obliterates satellite!“. Asks users to open attached file that, when opened, installs spyware.	6:51
Troj_Agent.JAW	1/14/07	Spammed email message that contains a seemingly benign PDF attachment. Once attachment is opened, backdoor is installed for remote hackers to access the PC.	20:08

Average lead time*……over 13 hours

Outbreaks blocked * ……175 outbreaks

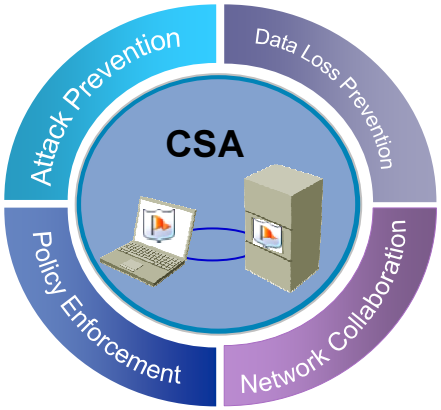
Total incremental protection*……over 94 days

**May 2006 – June 2007. Calculated as publicly published signatures from the following vendors: Sophos, McAfee , Trend Micro, Computer Associates, F-Secure, Symantec and McAfee. If signature time is not available, first publicly published alert time is used.*

Cisco Security Agent 6.0

Comprehensive, “Always Vigilant” Endpoint Security

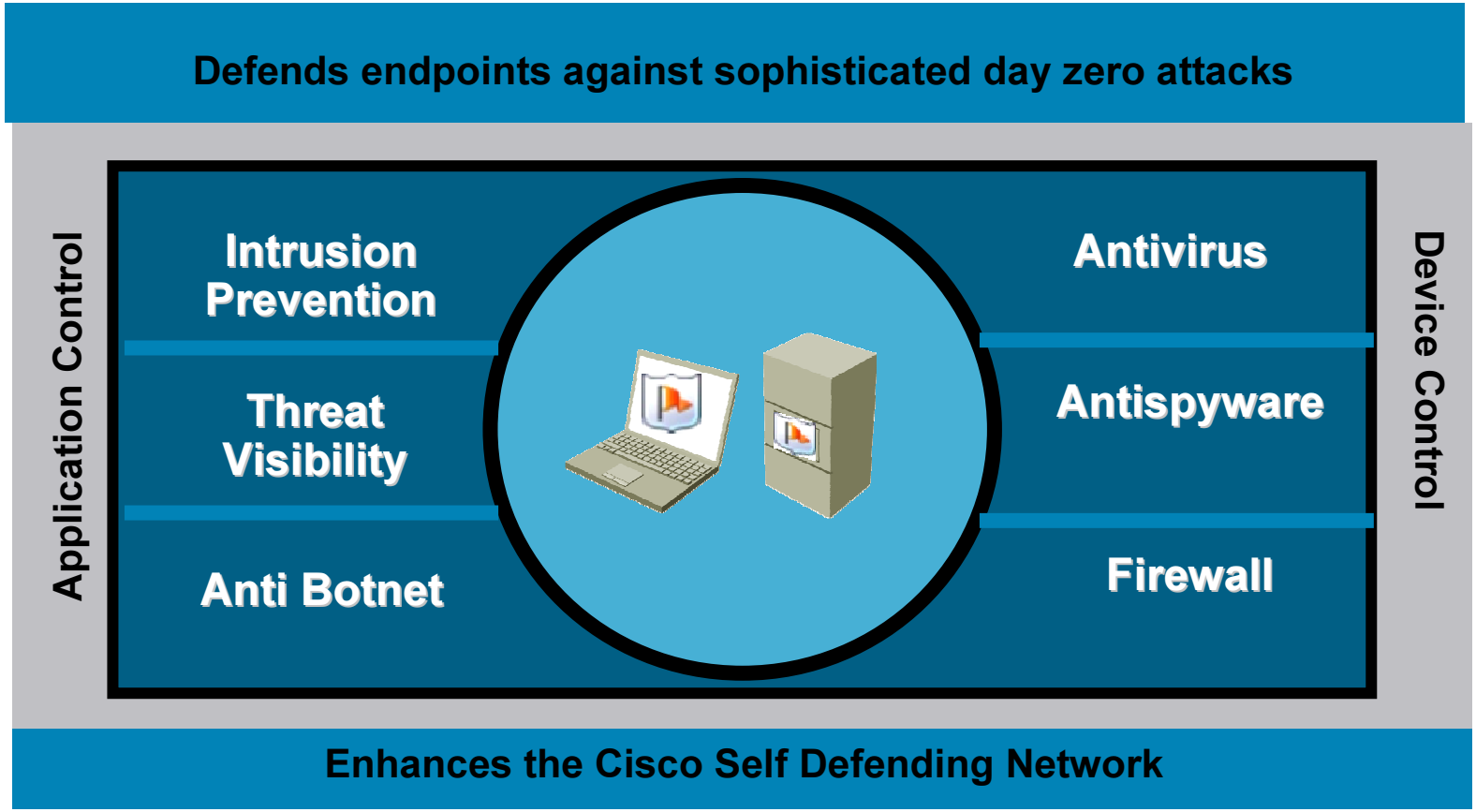
- Single Integrated Client, Simplified Management
- Protection against persistent and evolving threats
- Prevent loss of sensitive information
- Enforce appropriate use policies
- Enhance security through network collaboration
- Address corporate and regulatory compliance mandates



Business Benefits:

- **Empower IT to address Business risks**
- **Enforce policies and protect business critical assets**
- **Decrease IT administrative burden**
- **Reduce expenses**

Complete Endpoint Security



© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Intrusion Prevention
"Zero Update" Track Record

- CSA has a proven track record of stopping brand new exploits, botnets, targeted attacks, worms, and viruses over past 7 years:
  - 2001 – Code Red, Nimda (all 5 exploits), Pentagone (Gonner)
  - 2002 – Sircam, Debploit, SQL Snake, Bugbear,
  - 2003 – SQL Slammer, So Big, Blaster/Welchia, Fizzer
  - 2004 – MyDoom, Bagle, Sasser, JPEG browser exploit (MS04-028), RPC-DCOM exploit (MS03-039), Buffer Overflow in Workstation service (MS03-049)
  - 2005 – Internet Explorer Command Execution Vulnerability, Zotob
  - 2006 – USB Hacksaw, IE VML exploit, WMF, IE Textrange, RDS Dataspace
  - 2007 – Rinbot, Storm Trojan, Big Yellow, Word(MS07-014), MS ANI 0Day, MS DNS 0Day

No signatures, or configuration updates required

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Detailed Zero-Update Malware Notes

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

Solutions | Products & Services | Ordering | Support | Training & Events | Partne

- HOME
- PRODUCTS & SERVICES
- SECURITY
- CISCO SECURITY AGENT
- PRODUCT LITERATURE
  - At-a-Glance
  - Brochures
  - Bulletins
  - Case Studies
  - Data Sheets
  - End-of-Life and End-of-Sale Notices
  - Presentations
  - Q&A
  - White Papers

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

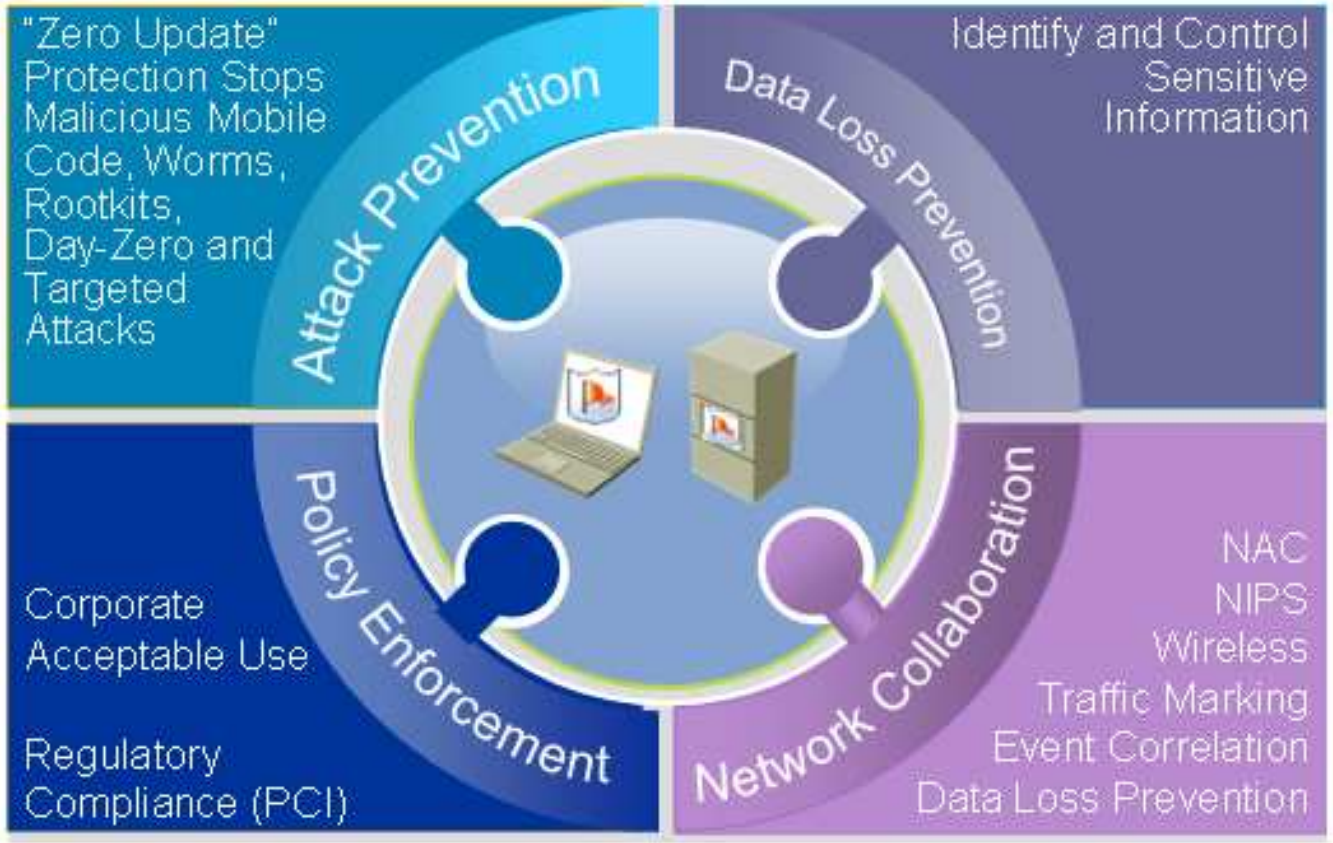
How CSA protects against MS07-014 exploits
28/Mar/2007

Cisco Security Agent Version 5.2
05/Feb/2007

How CSA Protects Against the Symantec Big Yellow BotWorm Exploit

Cisco Security Agent

Always Vigilant Comprehensive Endpoint Security



Laptop – Desktop Protection

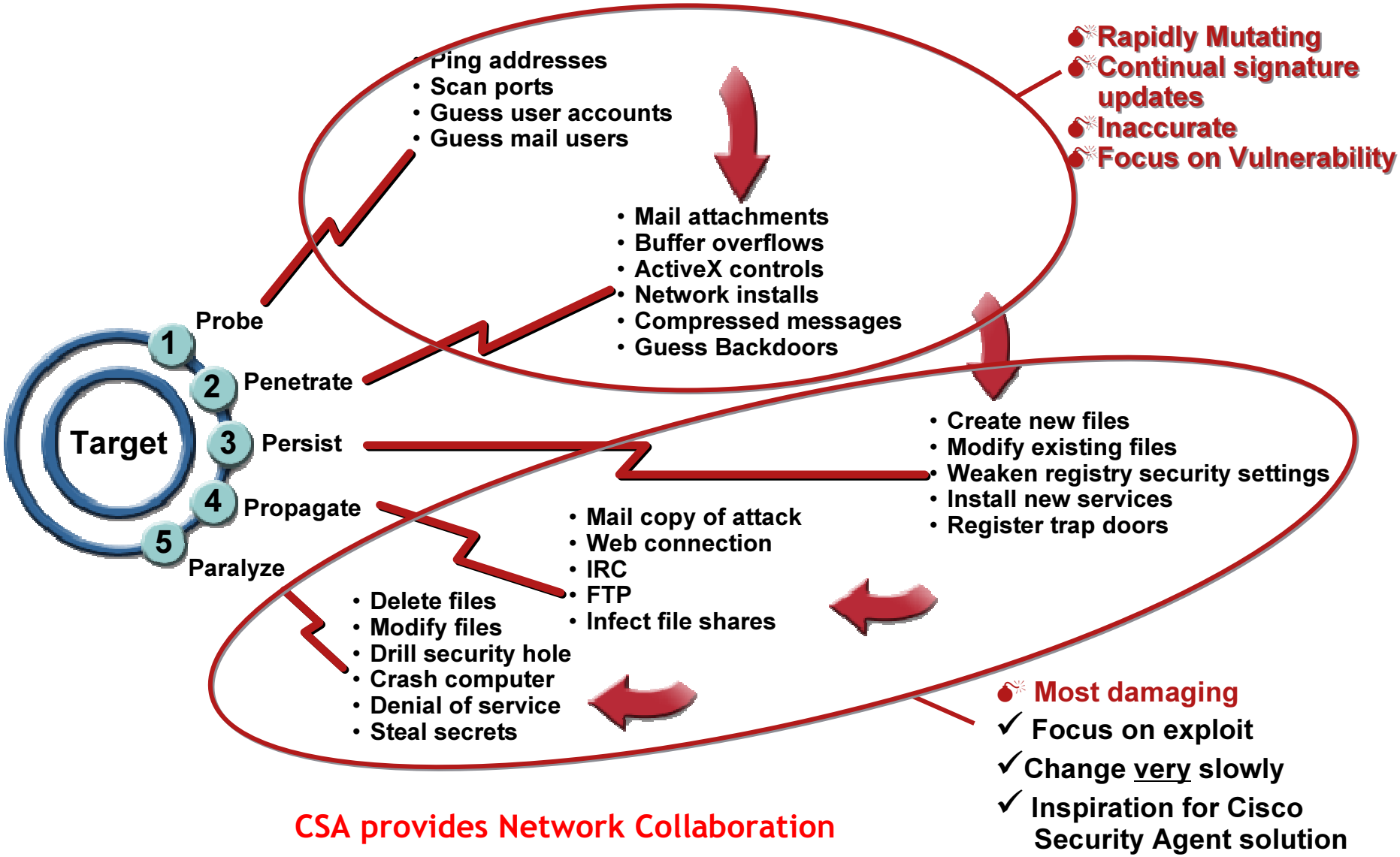
Server Protection

POS Protection

SINGLE INTEGRATED AGENT AND MANAGEMENT

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

CSA Approach:
Behavioral Protection for Endpoints



CSA provides Network Collaboration

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Basic, Advanced & Targeted Attacks

- **All attacks come in via the network**
  - **Will be a combination of exploits, payload, malware, and binary code, targeted at DoS, financial data.**
  - **CSA pays particular attention to Downloaded data**

- **Payload-based Attacks are becoming increasingly common, targeting internal users**
  - **Malware delivered via Cross Site Scripting appears as benign when observed from the network**
  - **"Drive by" downloads install without user's knowledge**
  - **CSA pays particular attention to Downloaded data**

- **Most data loss occurs from the inside, through accidental disclosure, intentional misuse by non-sophisticated users, or intentional misuse by sophisticated users**
  - **Downloaded application accessing sensitive data are key to successful targeted attack**
  - **CSA pays particular attention to Downloaded data**

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

How Malware Works

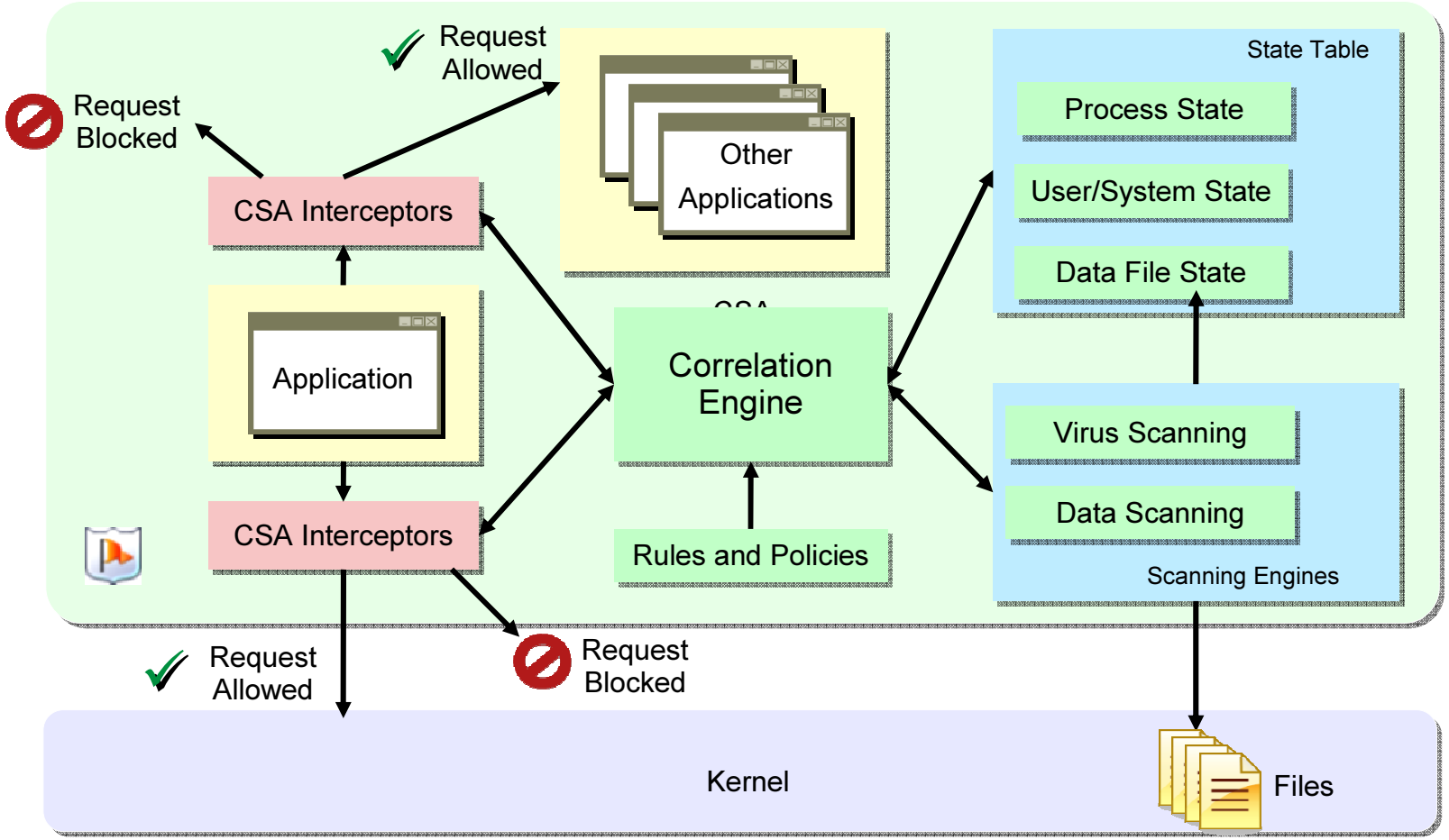
- All attacks come in via the network
  - Attacker needs to deliverable executable bits to target.
- Many delivery options, but result is network application writes executable bits
  - Cross Site Scripting (browser), Phishing (E-mail, Instant Messaging), Network worm (Windows kernel)
- To be useful to attacker, the malware must do several things:
  - Execute, make itself persistent, phone home, capture data (keyboard, cache)

Malware Behaviors
Access or Modify System Configuration
Buffer overflow
Invoking Command Shell or Config Apps
Modify another process
Monitor User Input
Network Protocols
Network Worm Client

- CSA correlates and dynamically classifies “untrusted content” into “Application Classes” to detect and prevent Day-Zero and Targeted-based Attacks.
- CSA’s other “Zero-Update” policies provide added protection.

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

How CSA works
Intercepting and Correlating Operating System Calls



- CSA intercepts calls to the operating system, and also is verifies application calls for system resources against the policy
- “Zero Update” Architecture- policy based control, you don’t a new signature to stop an attack

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

CSA'S Unique Policy Structure & Classes of Malware

CSA "Application Classes"	Virus/Worms	Spyware/Adware	Botnets	Acceptable Use Policy Control
Access or Modify System Configuration	X	X	X	X
Buffer overflow	X	X	X	X
Invoking Command Shell or Config Apps	X		X	X
Modify another process		X		X
Monitor User Input				X
Network Protocols		X	X	X
Network Worm Client	X			X

CSA observes behavior, correlates the behavior with previous behaviors, and classifies applications into various categories

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Network Integrated Solutions

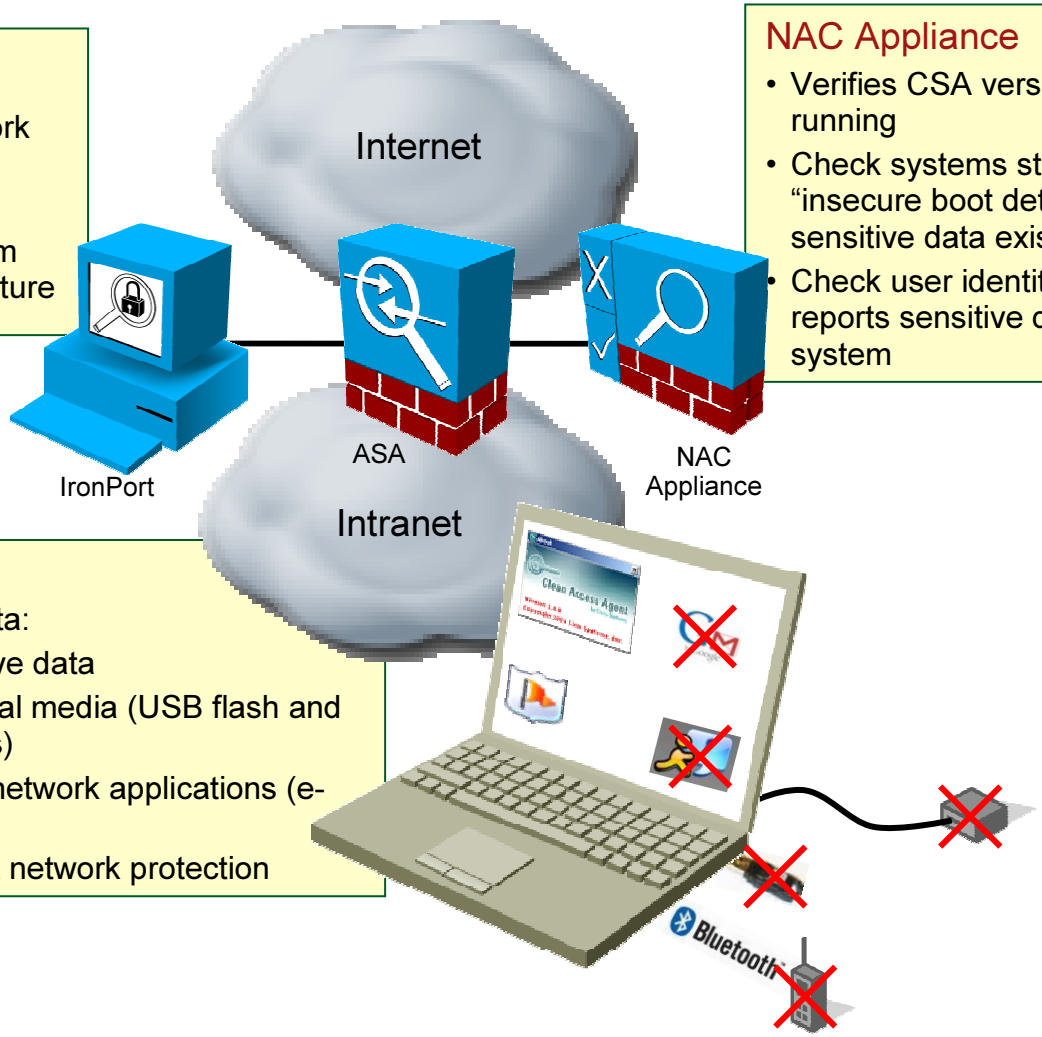
CSA with NAC, DLP and IronPort

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

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

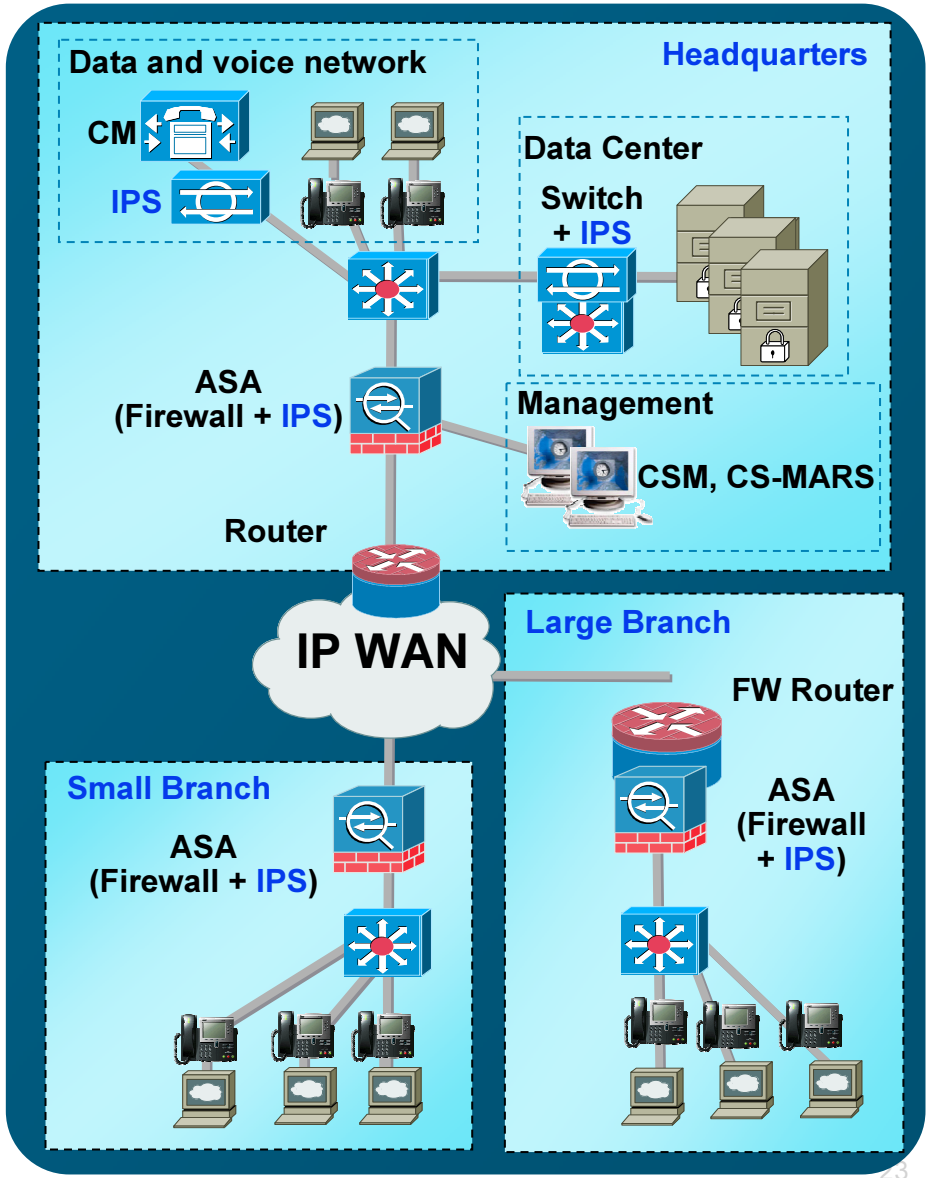
Agenda

- Physical Security
- IPSec VPN / SSL VPN
- Encryption
- Email Encryption
- Anti-Virus, Zero Day Attacks
- IPS
- Security Event Management

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Flexible Deployment:
IPS Throughout the Environment

- Holistic network security solution
- IPS at all points in the network
- ASA integration (FW and IPS)
- Branch-office integration (Cisco ISR)
- Common Policy Management
- Comprehensive, timely signature coverage



© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cisco IPS Intelligent Detection Capabilities:
Vulnerability and Exploit-based Signatures

IPv4 and IPv6 protection

Adware/Spyware
- Perfect Keylogger Activity
- Hotbar Activity

DDOS/DOS
- ICMP/UDP/TCP Floods

Secure Voice
- SIP
- H323
- H225

Web Server
- Apache
- Internet Information Server (IIS)

Network, L2/3/4
- BGP
- DHCP
- DNS
- TCP/UDP
- IP
- IP Fragment

Worm/Virus/Trojan
- Storm
- Mega-D
- Blaster
- Nimda
- Sasser
- Code Red
- Slammer
- Backdoor Trojan Spirit
- Backdoor Beast
- Fatso Worm
- Kelvir Worm

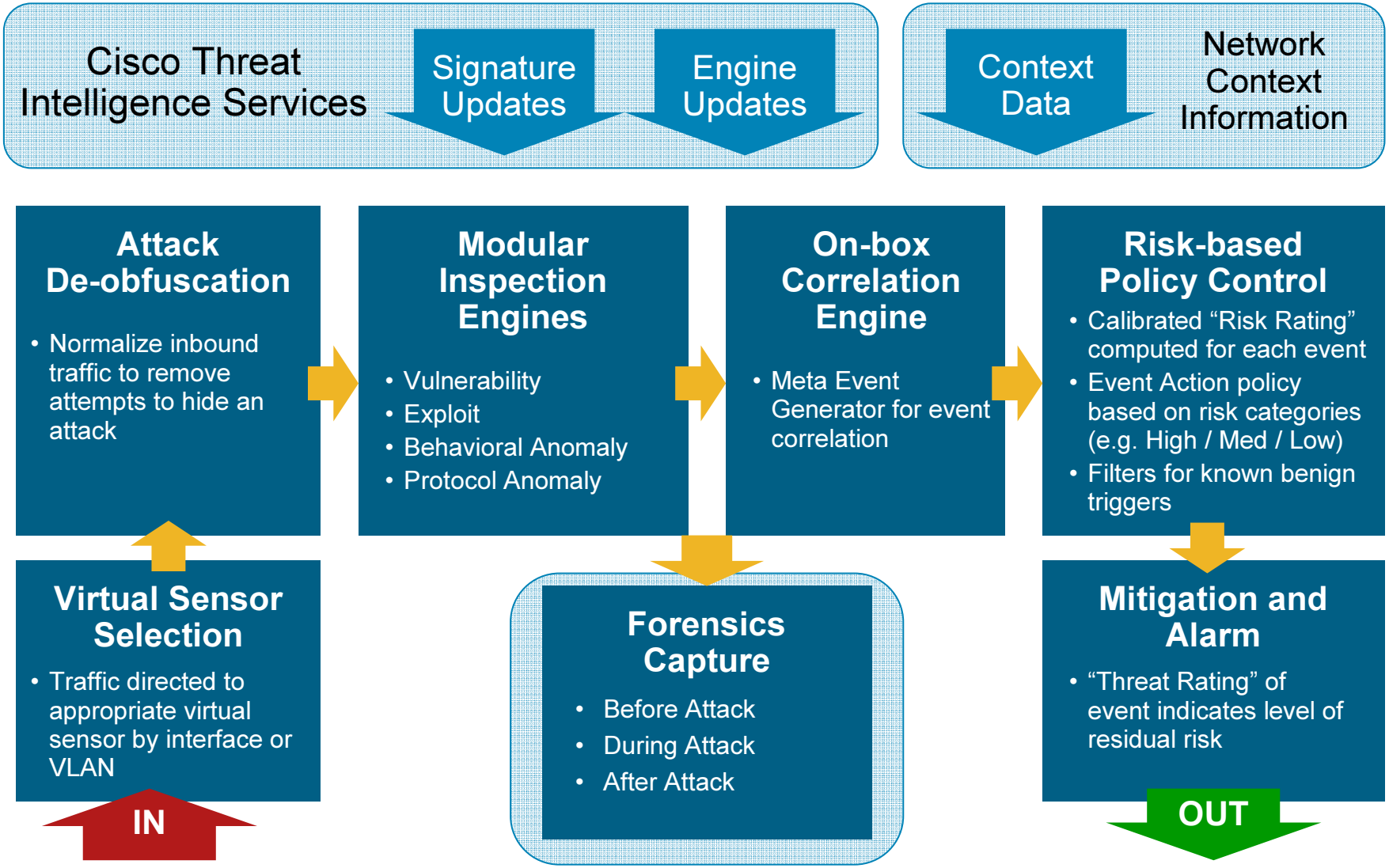
P2P/IM
- AIM/ICQ
- AOL
- MSN
- Sametime
- Yahoo
- BitTorrent
- Kazaa
- eDonkey
- Jabber

Reconnaissance
- ICMP host sweeps
- TCP Port Sweeps
- TCP/UDP Combo Sweeps
- UDP Port Sweeps

Email
- POP
- IMAP
- SMTP
- Microsoft Exchange

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

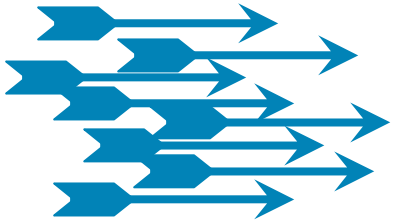
Cisco IPS Architecture
Intelligent Detection and Precision Response



© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Vulnerability-Focused Signatures
for Unparalleled Coverage

Countless Exploit Variants yet to be written



30,000 Known Exploits and Variants

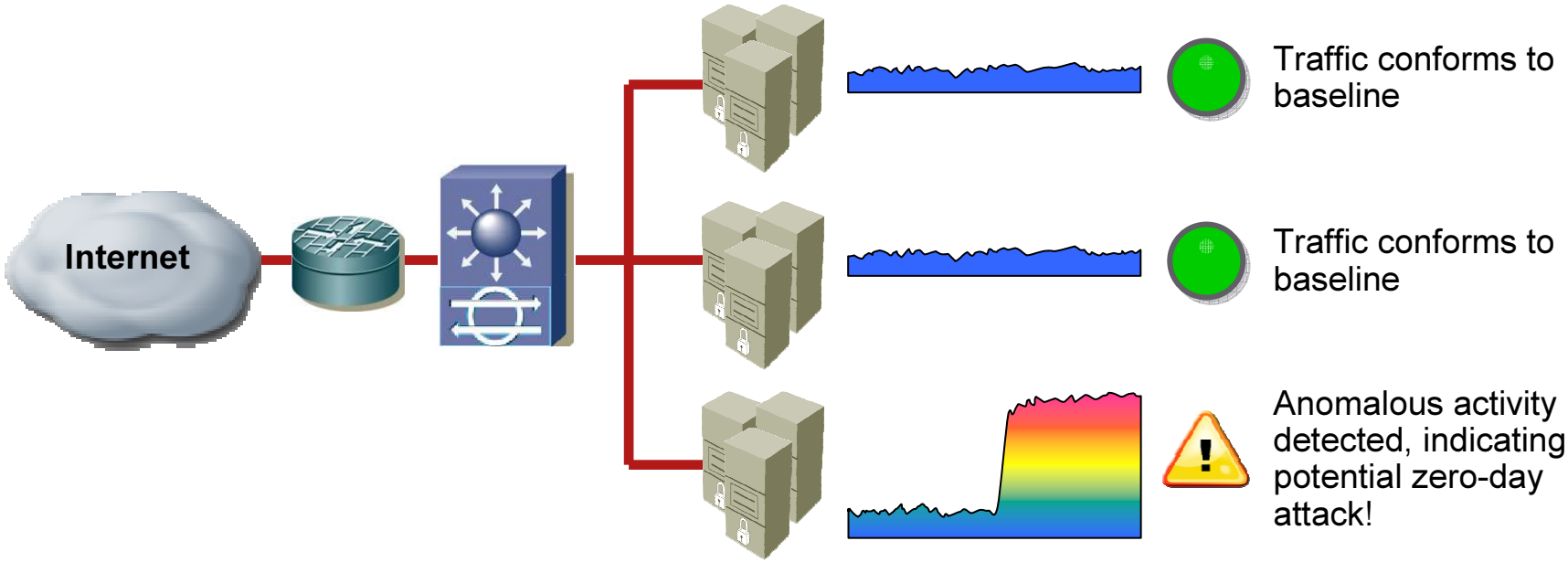
3000 Vulnerability-Focused Signatures

Cisco's commitment to vulnerability-focused signatures provides unparalleled detection of both known and tested exploits as well as exploits yet to be written (zero-day exploits.)

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

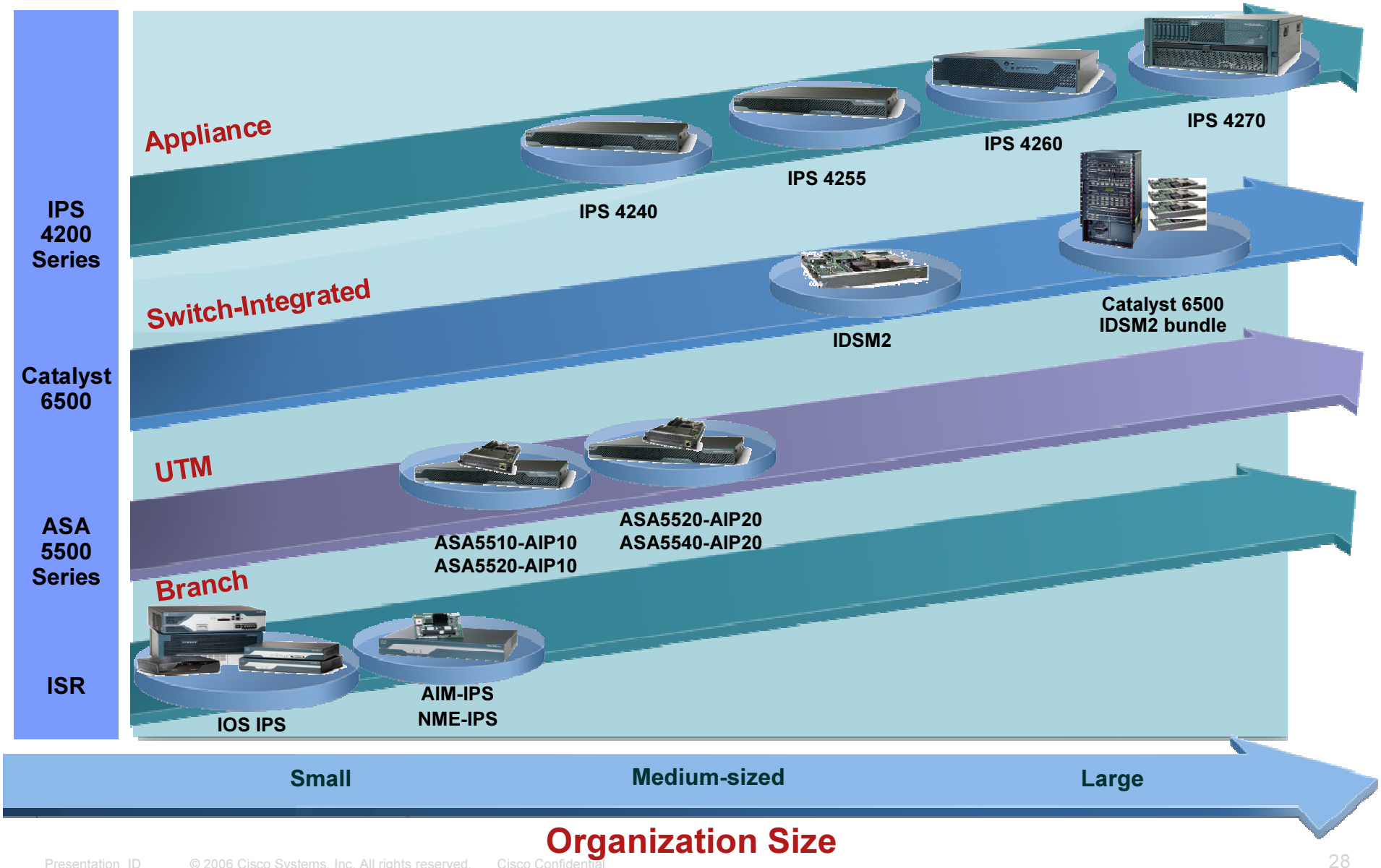
Real-Time Anomaly Detection for Day Zero Threats

- Anomaly detection algorithms to detect and stop Day-Zero threats
- Real-time learning of normal network behavior
- Automatic detection and policy-based protection from anomalous threats to the network
- **Result:** Protection against attacks for which there is no signature



© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cisco IPS Product Portfolio



© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Agenda

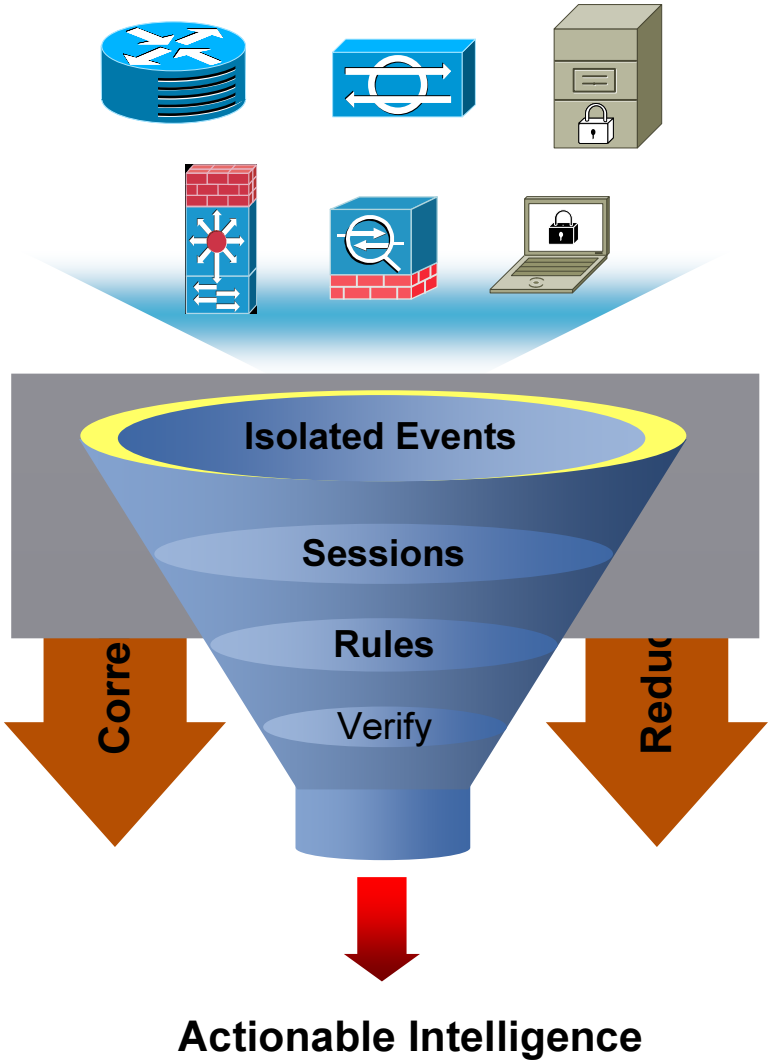
- **Physical Security**
- **IPSec VPN / SSL VPN**
- **Encryption**
- **Email Encryption**
- **Anti-Virus, Zero Day Attacks**
- **IPS**
- **Security Event Management**

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cisco Security MARS

Real time Security Threat Detection and Resolution

- Focuses IT on real threats – reduces the number of "false positive" alarms and alerts
- Builds topological network view and adds visualization of traffic flows
- Identifies the source of anomalous behavior



Raw Logging Data

15,427,105 Events

5,666,129 Sessions

102 Incidents

40 High Severity Incidents

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cisco Security MARS

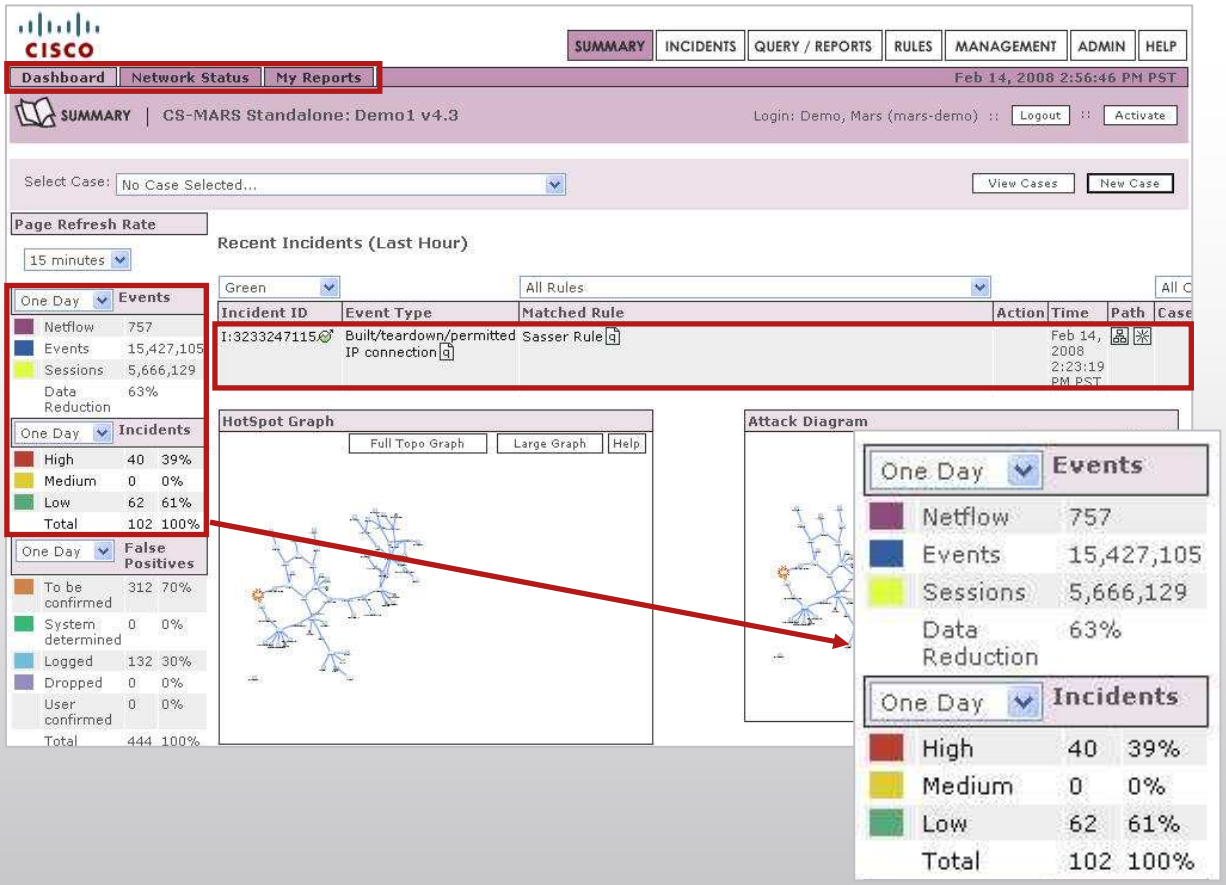
Appliance Based, Purpose-Built Solution

- **Scalable from SMB through Enterprise markets**
  - **Standalone Appliances**
  - **Distributed Standalone Appliances**
  - **Tiered Appliances utilizing a Global Controller**
- **Collector, Database, and Reporting engine all in one box, saving power and rack space**
- **Simple licensing – no administrator licenses and no agent costs**
- **Hardened OS is pre-installed, shortening the installation time**
- **Database is pre-installed, self-contained, and self-maintaining**
  - **No DBA Staff required**
  - **Helps in controlling ongoing expenses**
- **Models available with redundant drives and power supplies to increase solution uptimes**

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cisco Security MARS

Intuitive Operational Dashboard



Incident Dashboard

- Aggregate
- Correlate
- Summarize

15,427,105 Events

5,666,129 Sessions

102 Incidents

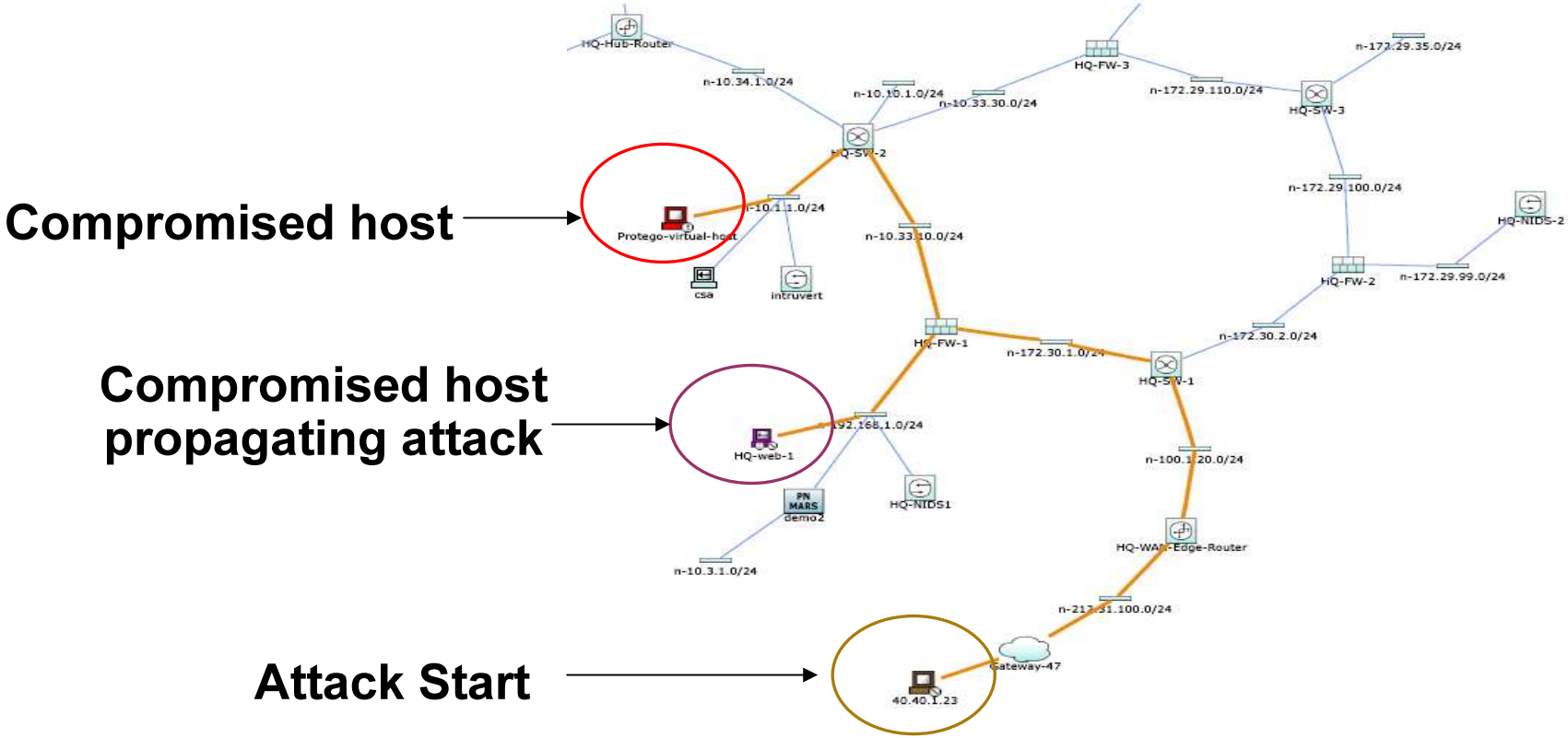
40 High Severity Incidents

- Device configuration, logging, and network topology information enables MARS to build a threat resolution dashboard
- Rapidly identify and resolve threats via Real-time Data Reduction, Allows Administrators to Focus On Priorities

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Attack Path and Topology Awareness

Rapid Threat Identification Improves Response Time



- **CS-MARS builds an understanding of the network topology and uses this in displaying the path an attack takes through the network.**

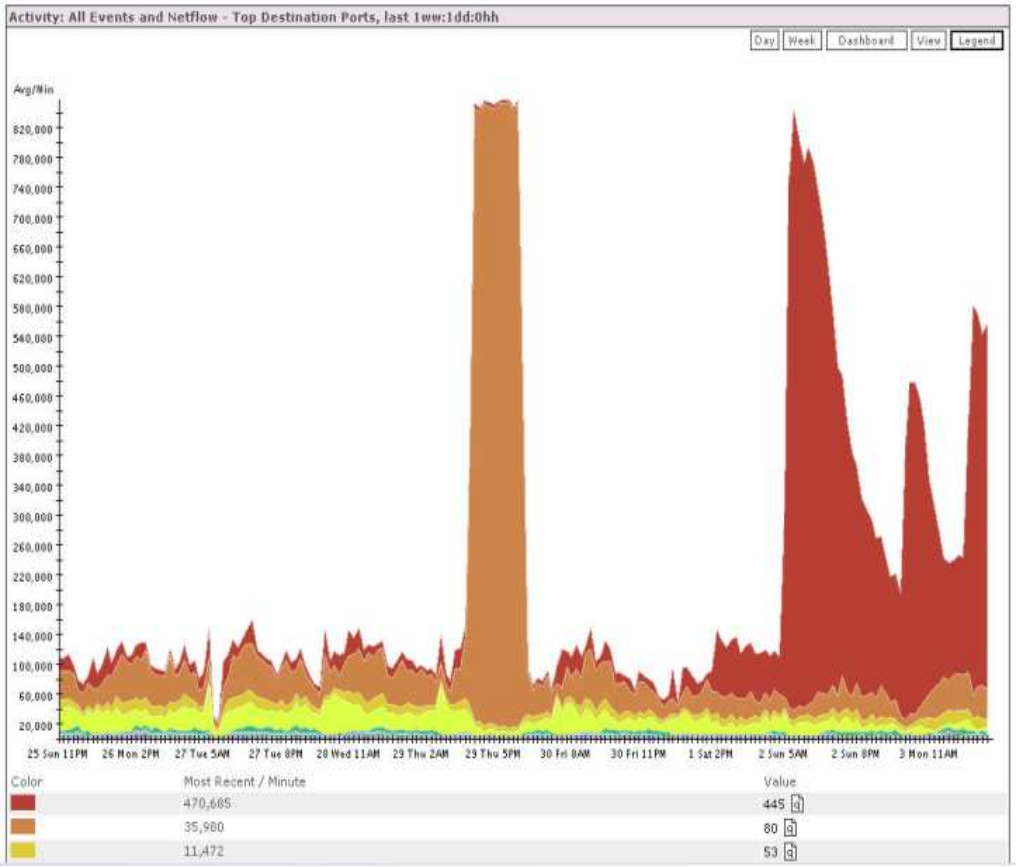
- **Color coding of elements allows for rapid identification of troubled devices while the topological layout helps to improve troubleshooting and response times.**

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Anomaly Detection

Day Zero Threat Detection Improves Response Time

- **Leverages NetFlow or firewall Syslog messages to profile the network usage**
- **Detect statistically significant anomalous behavior from computed baseline, including viruses, worms, and policy violations such as peer-to-peer file sharing**
- **Correlate anomalous behavior to attacks and other events reported by Network IDS systems.**
- **Enables detection of attacks where IDS/IPS signatures do not exist and firewalls allow traffic through**

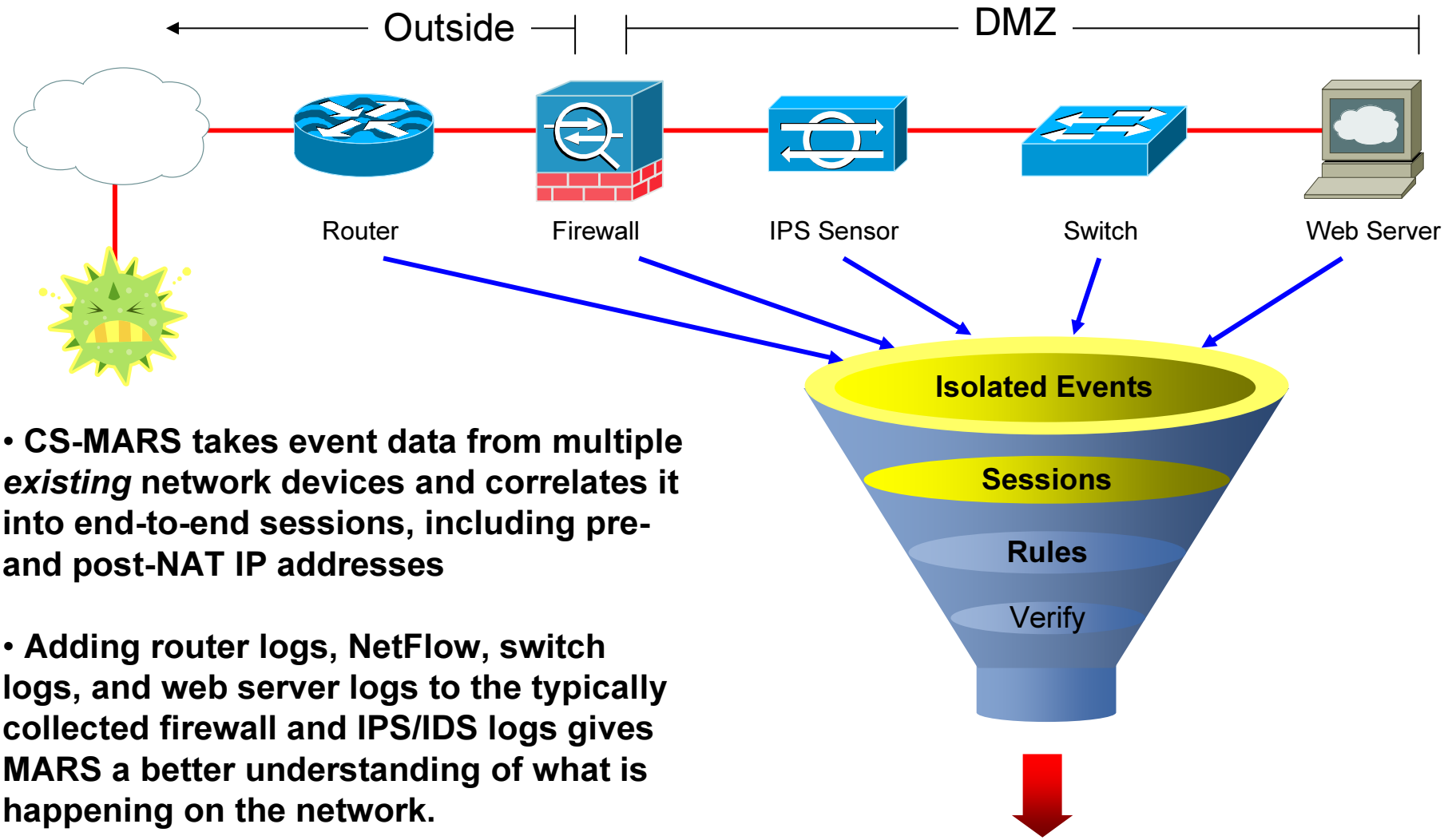


Example of a Sasser-D breakout from a customer's site

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Data Correlation

Increase the ROI for your Existing Equipment



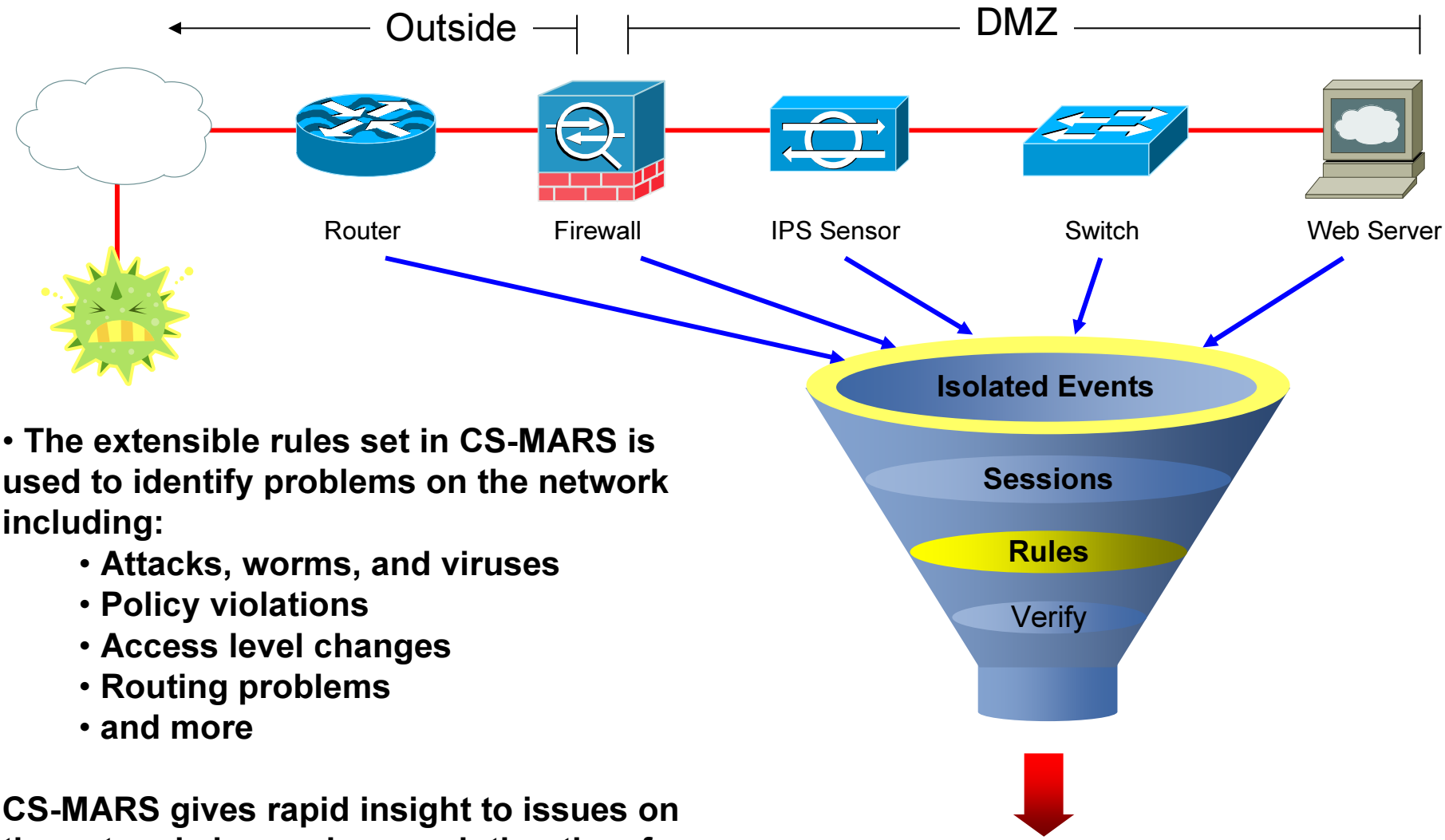
- **CS-MARS takes event data from multiple *existing* network devices and correlates it into end-to-end sessions, including pre- and post-NAT IP addresses**

- **Adding router logs, NetFlow, switch logs, and web server logs to the typically collected firewall and IPS/IDS logs gives MARS a better understanding of what is happening on the network.**

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Threat Identification

Lessen the Impacts of Threats/Outbreaks



- **The extensible rules set in CS-MARS is used to identify problems on the network including:**
  - **Attacks, worms, and viruses**
  - **Policy violations**
  - **Access level changes**
  - **Routing problems**
  - **and more**

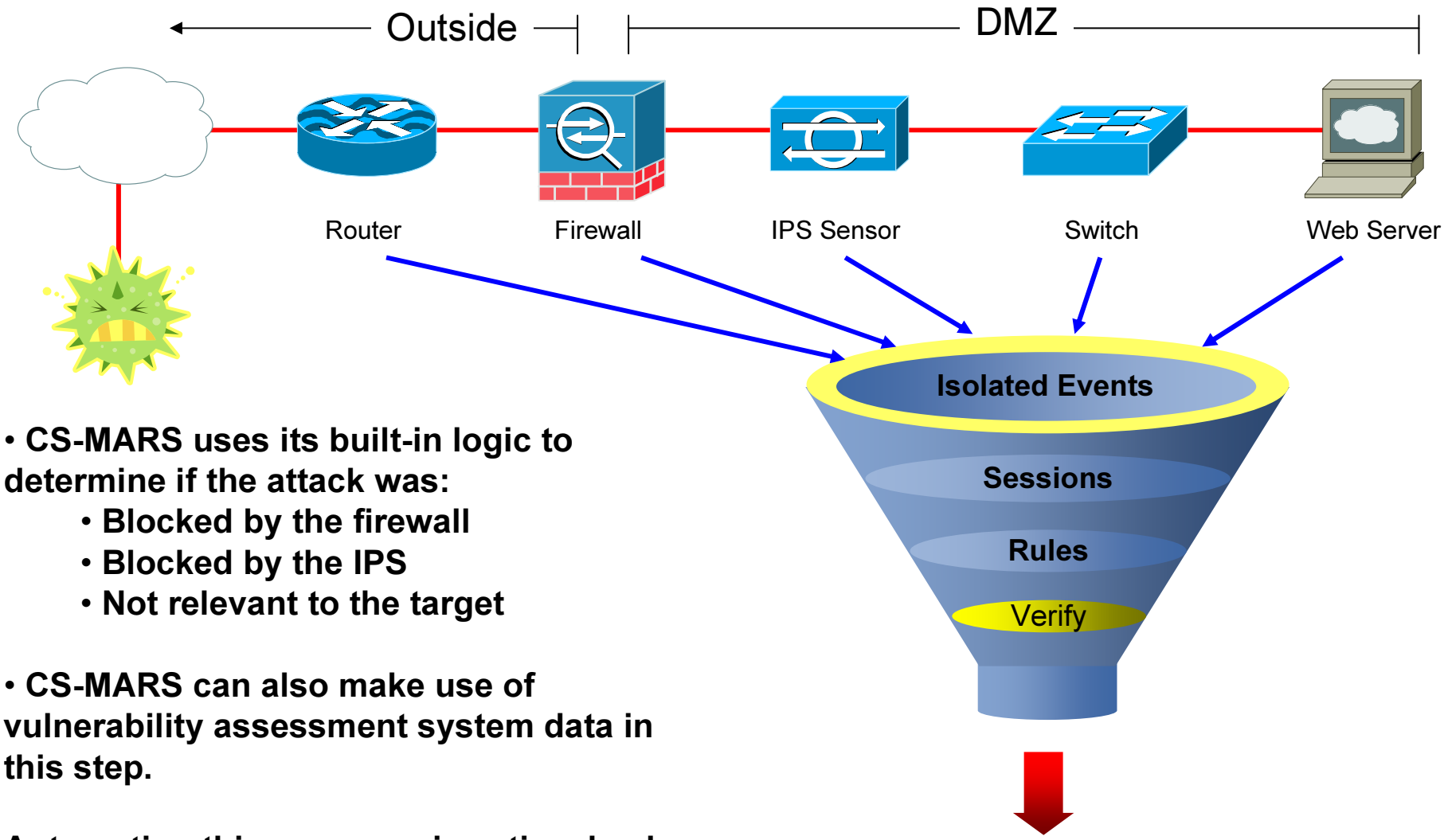
CS-MARS gives rapid insight to issues on the network, improving resolution time frame

Actionable Intelligence

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

False Positive Verification

Reducing Operational Expenses



- **CS-MARS uses its built-in logic to determine if the attack was:**
  - **Blocked by the firewall**
  - **Blocked by the IPS**
  - **Not relevant to the target**

- **CS-MARS can also make use of vulnerability assessment system data in this step.**

Automating this process gives time back to employees to do other tasks

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Internal Threat Resolution

Improve Threat Response Times

- **Use control capabilities within your infrastructure**
  - **Layer 2/3 attack path is clearly visible**
  - **Enforcement devices are identified**
  - **Resolution commands are provided**
  - **Alternate enforcement devices also suggested**

Enforcement Device: switch_server, Suggested

Enforcement Device Information

Device	Type	Manager	Children	Log To	Collects From	Info
switch_server	Cisco Switch-IOS 12.2	Protego Networks MARS 1.0 on pnvalis		N/A		

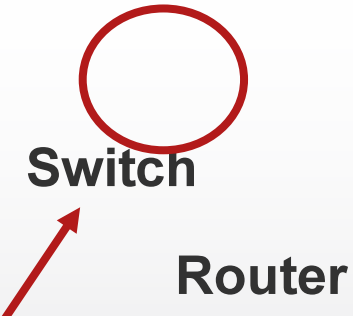
Interface Information

Direction	IP Address	Interface Name	DNS Name	MAC Address	MAC Update Time

Recommended Policy/Command

```
configure t
interface FastEthernet0/4
  no ip address
  shutdown
```

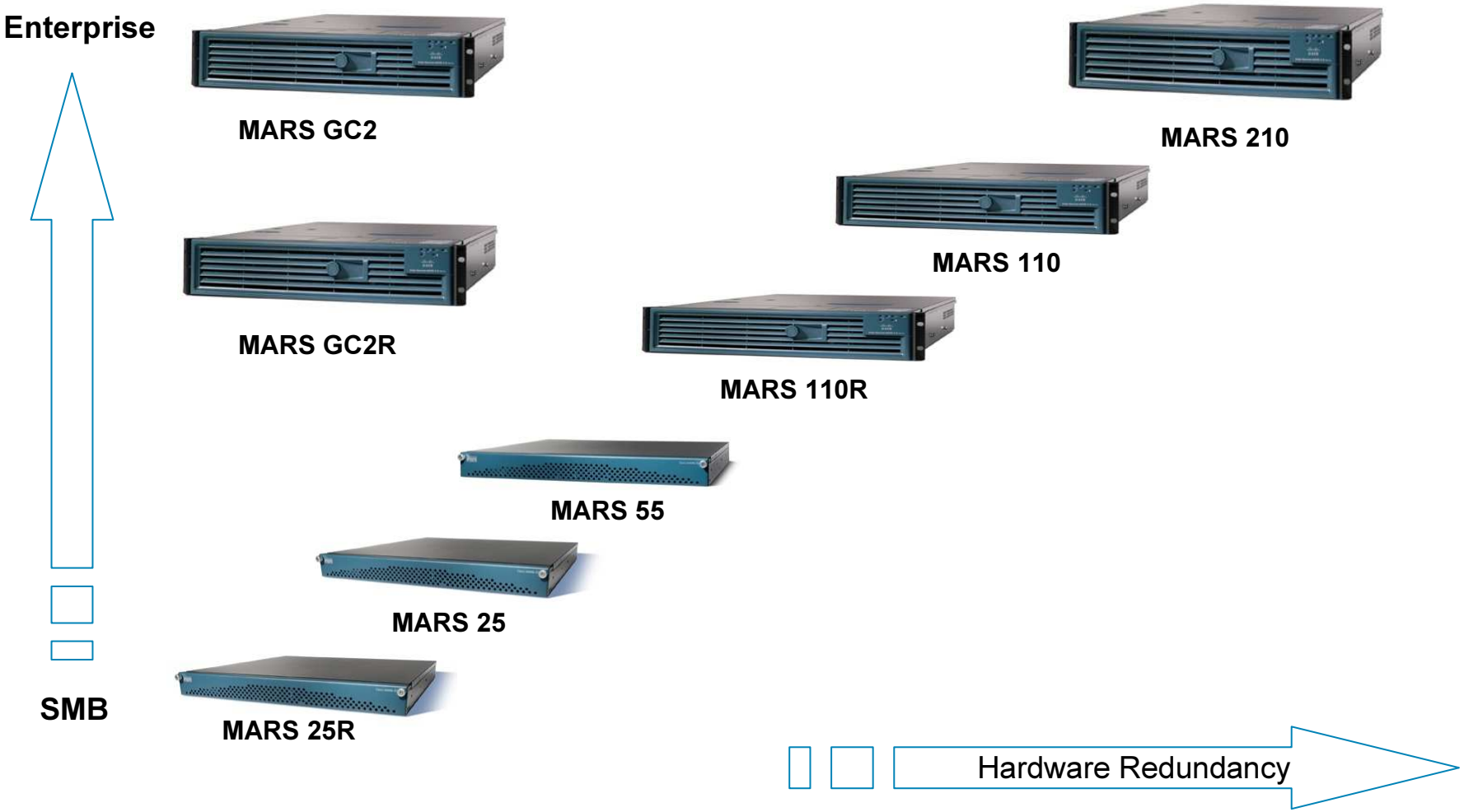
Push Cancel



Reduce the time it takes to identify where and how to block an attack

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cisco Security MARS
Scalable Appliance Models



© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cisco Security MARS

Appliance Details

Local Controller Models	Storage	Rack Unit	Power
Cisco Security MARS 25R	250 GB (non-RAID)	1 RU x 20 in. x 19 in. (W)	350W, 120/240V autoswitch
Cisco Security MARS 25	250 GB (non-RAID)	1 RU x 20 in. x 19 in. (W)	350W, 120/240V autoswitch
Cisco Security MARS 55	500 GB RAID 1	1 RU x 25.5 in. x 19 in. (W)	350W, 120/240V autoswitch
Cisco Security MARS 110R	1500 GB RAID 10 hot-swappable	2 RU x 27.75 in. (D); 3.44 in. (H); 19 in. (W)	2x 750W dual-redundant, 120/240V autoswitch
Cisco Security MARS 110	1500 GB RAID 10 hot-swappable	2 RU x 27.75 in. (D); 3.44 in. (H); 19 in. (W)	2x 750W dual-redundant, 120/240V autoswitch
Cisco Security MARS 210	2000 GB RAID 10 hot-swappable	2 RU x 27.75 in. (D); 3.44 in (H); 19" (W) in.	2x 750W dual-redundant, 120/240V autoswitch

Global Controller Models	Local Controller Models Supported	Maxi Connections	Storage	Rack Unit	Power
Cisco Security MARS GC2R	Cisco Security MARS 25/55 only	5	2 TB RAID 10 hot-swappable	2 RU x 27.75 in. (D); 3.44 in. (H); 19 in. (W)	2x 750W dual-redundant, 120/240V autoswitch
Cisco Security MARS GC2	All Cisco Security MARS	Not restricted	2 TB RAID 10 hot-swappable	2 RU x 27.75 in. (D); 3.44 in. (H); 19 in. (W)	2x 750W dual-redundant, 120/240V autoswitch

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cisco Security MARS

Ordering Information

Part Number	Cisco SMARTnet Service Part Number	Description
CS-MARS-25R-K9	CON-SNT-MARS25R	Cisco Security MARS 25R
CSMARS-25-LIC-K9=	CON-SNT-MARS25U	Cisco Security MARS 25R upgrade license to CS-MARS-25-K9
CS-MARS-25-K9	CON-SNT-MARS25	Cisco Security MARS 25
CS-MARS-55-K9	CON-SNT-MARS55	Cisco Security MARS 55
CS-MARS-110R-K9	CON-SNT-MARS110R	Cisco Security MARS 110R
CSMARS-110-LIC-K9=	CON-SNT-MARS110U	Cisco Security MARS 110R upgrade license to CS-MARS-110-K9
CS-MARS-110-K9	CON-SNT-MARS110	Cisco Security MARS 110
CS-MARS-210-K9	CON-SNT-MARS210	Cisco Security MARS 210
CS-MARS-GC2R-K9	CON-SNT-MARSGC2R	Cisco Security MARS GC2R
CSMARS-GC2-LIC-K9=	CON-SNT-MARSGC2L	Cisco Security MARS GC2R upgrade license to CS-MARS-GC2-K9
CS-MARS-GC2-K9	CON-SNT-MARSGC2	Cisco Security MARS GC2

FRUs not shown here, available in pricing tool

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cisco Security MARS

Resources on the Net

- **Product Links**

  General Info

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

  Software Download

  http://www.cisco.com/cgi-bin/tablebuild.pl/cs-mars

  Documentation

  http://www.cisco.com/en/US/products/ps6241/tsd_products_support_series_home.html (Product Documentation)

  http://www.cisco.com/en/US/docs/security/security_management/cs-mars/6.0/user/guide/combo/appXML.html (XML Schema)

  Helpful Links

  http://www.cisco.com/go/netpro (NetPro Forums)

  http://www.cisco.com/security (Cisco Security Center Website)

  http://wwwin.cisco.com/go/mars (Cisco internal only)

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential

 © 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential