



Cisco Security Architecture



Veronika Štorková

System Engineer, CCIE R&S #23705

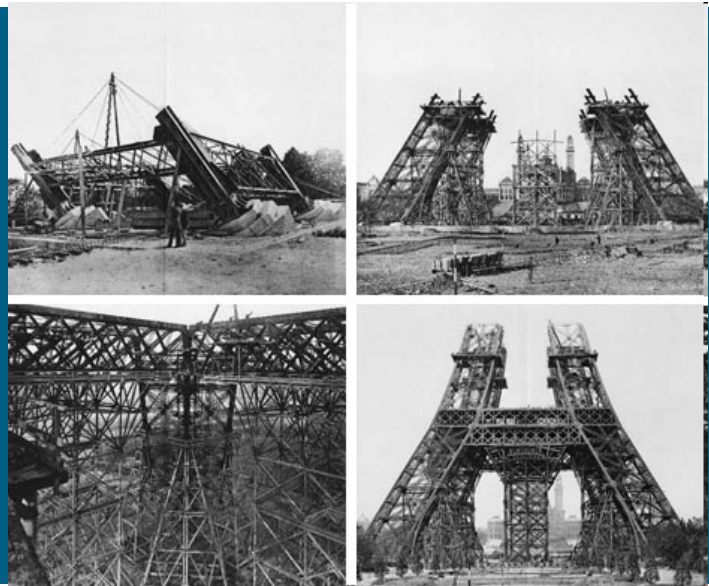
vstorkov@cisco.com

Agenda

- Cisco SAFE Architecture
- Cisco SAFE – Securing Campus/LAN Networks
 - Cisco Security Agent
 - Cisco Network Admission Control
 - Cisco IronPort
 - Cisco IPS – new features



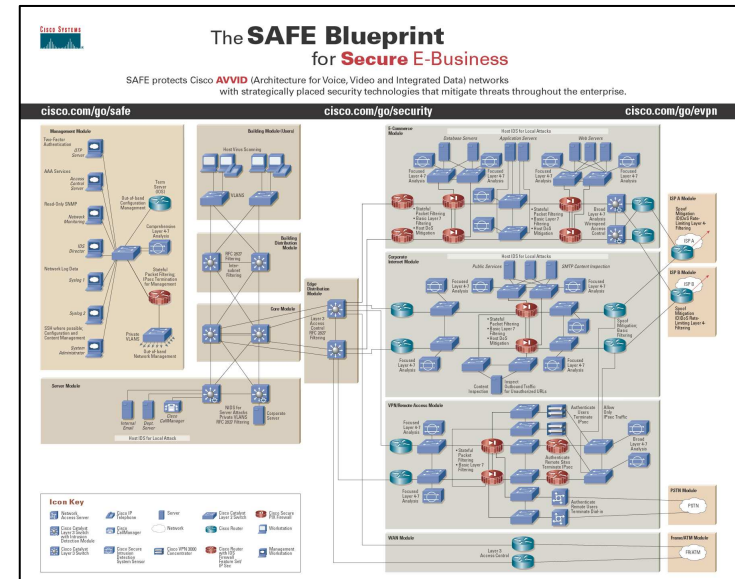
Cisco SAFE Architecture



Cisco SAFE

A Security Blueprint for Enterprise Networks

- Introduced in 2000
- Defense-in-depth
- Modular design
- Designs were validated
- Vendor/product agnostic
- Helped increase security awareness



Evolving Security Threats

- New technologies unprotected
 - Web 2.0, virtualization, cloud computing, etc.
- Lack of consistency and collaboration across products
- Accidental architecture
 - Fear-based security decisions
 - Product- or feature-of-the-moment purchases
- Siloed products and designs
- Poor security policy, control, management, and visibility



Today's Complex Security Threats Require Systemwide Collaboration

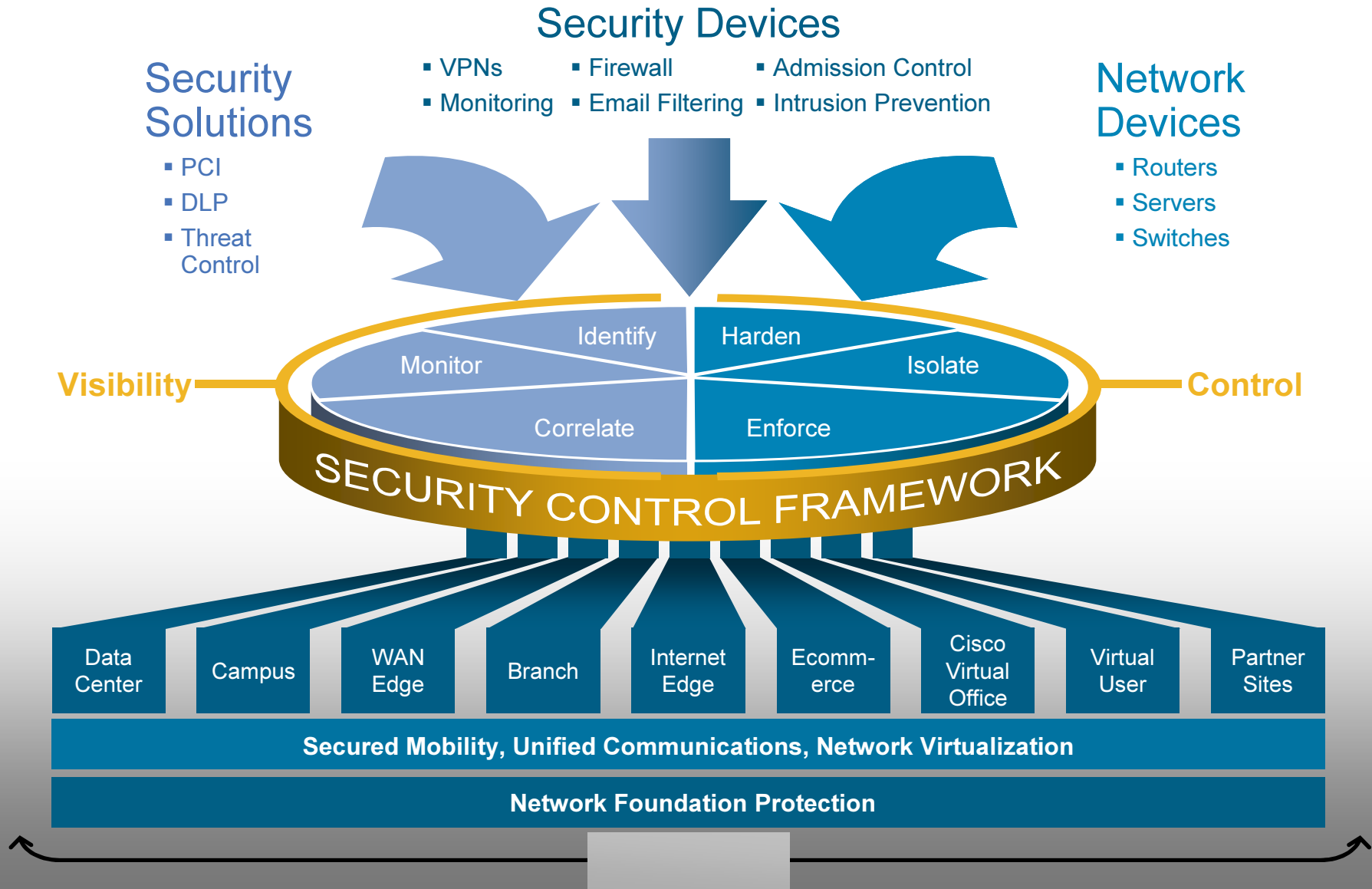
Top-Ten Cyber Security Menaces

- Sophisticated website attacks
- Increasing botnet sophistication and effectiveness
- Growing cyber espionage
- Emerging mobile phone threats
- Insider attacks
- Advanced identity theft
- Increasingly malicious spyware
- Web application security exploits
- Sophisticated social engineering
- Supply-chain attacks infecting consumer devices



Source: SANS Institute

SAFE Security Architecture Strategy



Why a new architecture?

The security landscape changed...

- Lots of new products and technologies introduced
- Effective deployment of security tools requires an understanding on platforms/features specifics and their impact to the network
- Threat sophistication and operational complexity mandates product/technology collaboration
- Operation and management is as important as the technologies themselves
- Guidance cannot be limited to design only, need to continue throughout the entire solution lifecycle

Architecture Principles

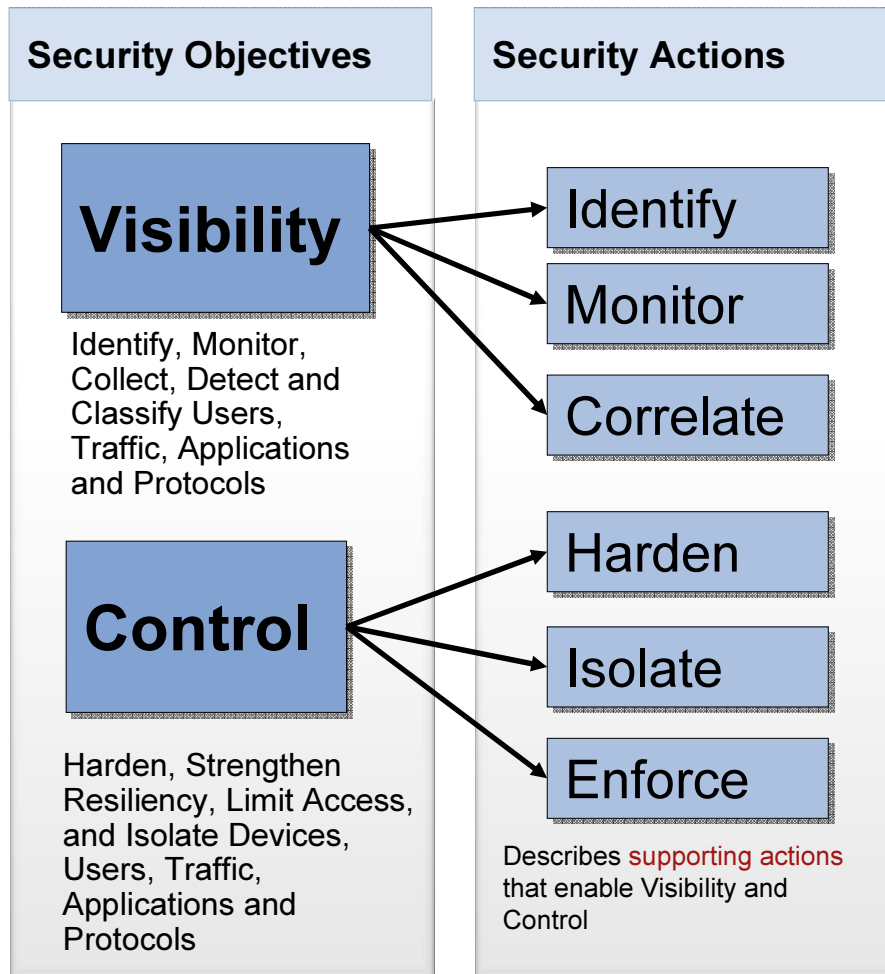
- Defense in Depth
- Modularity and Flexibility
- Service Availability and Resiliency
- Regulatory Compliance
- Auditable Implementations
- Strive for Operational Efficiency
- Network Intelligence and Collaboration

SAFE Axioms

- Infrastructure devices are targets
- Services are targets
- Endpoints are targets
- Networks are targets
- Applications are targets

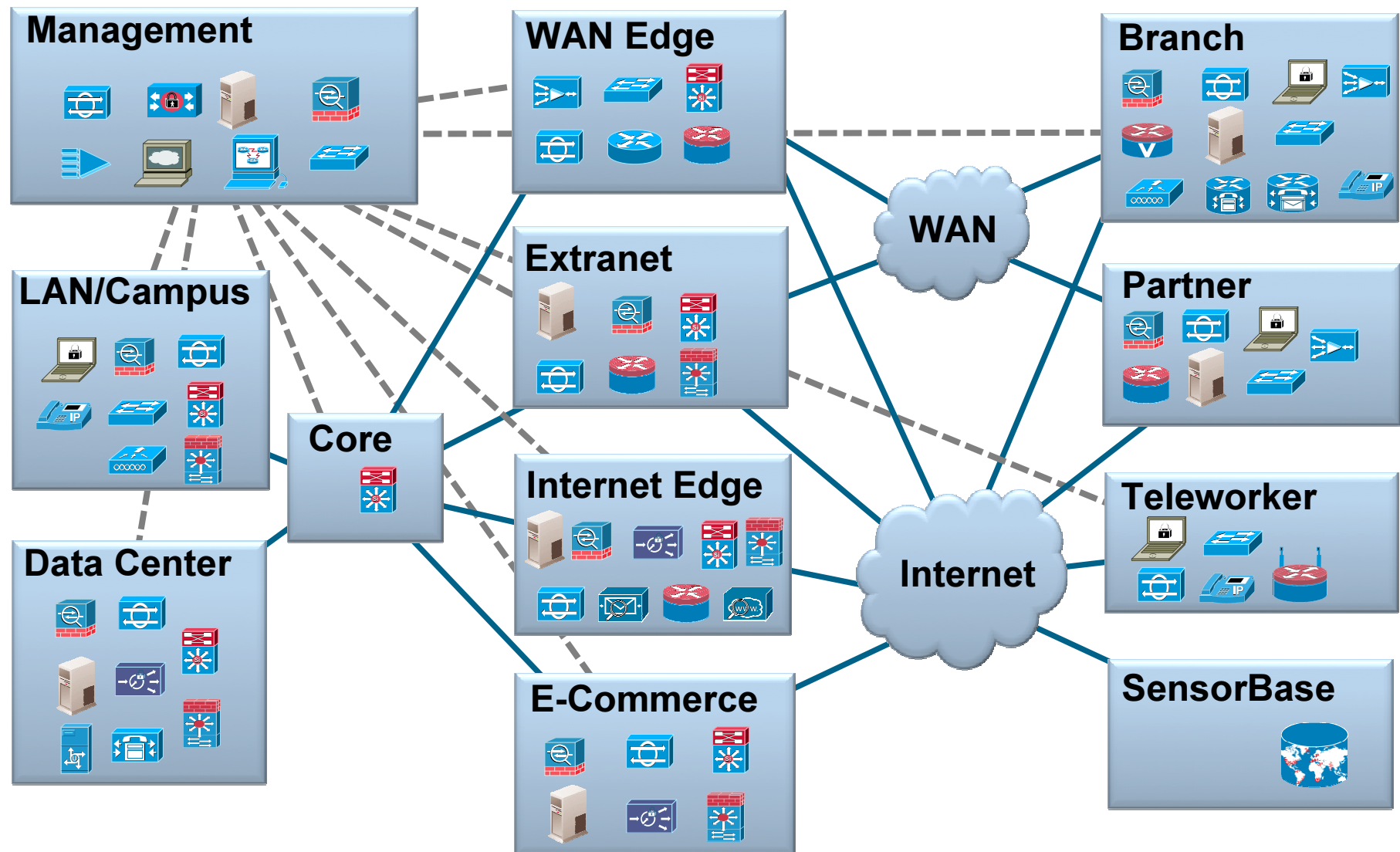
Cisco Security Control Framework

Service Integration



- Sets a common terminology and taxonomy
- Brings consistency between solutions and services
- Mandates attention to the operational aspects of the designs
- Helps identify threat vectors and drives the selection of technical controls

SAFE Security Architecture Modules



What's covered in this phase

- Network Foundation Protection
- Public Services DMZ (ASA, IPS)
- Corporate Internet Access (web, email security, ASA, IPS)
- Remote Access VPN (SSL VPN, EzVPN)
- WAN Edge (ASR, DMVPN w/PKI, IPS)
- Branch (IOS, ASA, IPS, FW)
- Campus (NAC, IBNS)
- Intranet Data Center (Nexus, IPS, ASA, WAF)
- Monitoring, Analysis & Correlation (Net Telemetry, CS-MARS)
- Threat Control and Containment (CSA, ASA, IPS, CSA+IPS, CSM+CS-MARS)

Platforms included in this phase

- ASR1004
- 7200 VXR G2
- IronPort C650
- IronPort S650
- CS-MARS
- CSM
- ACS
- CSA
- IPS4270
- IPS4260

- NAC3350
- NACMGR
- NAC3310
- Cat4506E
- Cat6504E
- Cat3750
- Nexus 7000
- Nexus 5000
- Nexus 1000

- ASA5580
- ASA5540
- ASA5520
- AIP-SSM
- AIM-IPS
- ISR 2821
- ISR 3845



Cisco SAFE Securing Campus/LAN Networks



Securing the LAN Infrastructure

Focused Attacks



- Data disclosure and modification
- Data interception and leakage
- Identity theft and fraud

Service Disruption



- Botnets, malware, spyware, viruses
- Buffer overflows, DoS, DDoS
- Infrastructure attacks

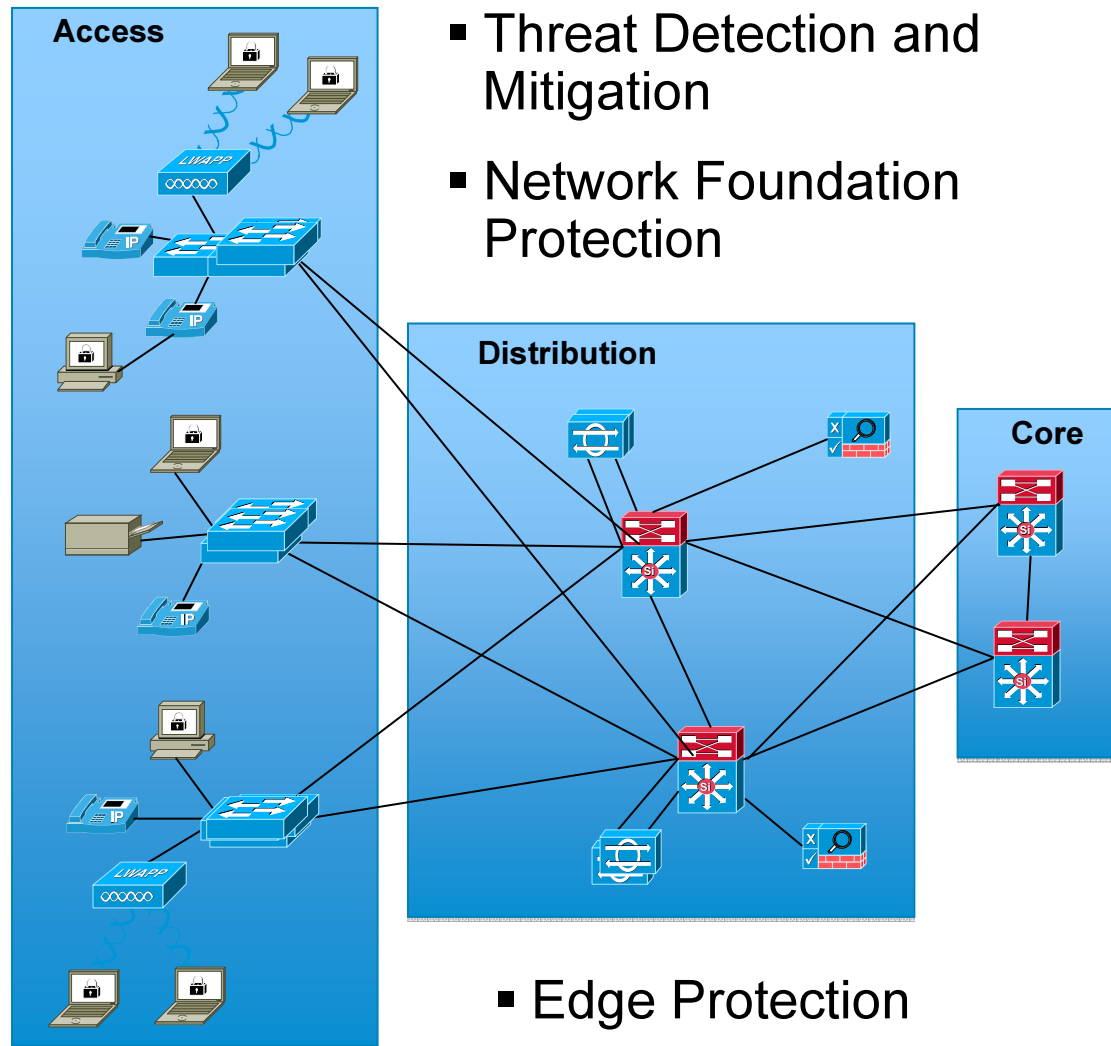
Network Abuse



- Unauthorized access
- Intrusions
- Application abuse
- Out of policy browsing

Campus/LAN

- Network Access Control
- Enhanced Availability and Resiliency
- Secure Unified Communications
- Secure Unified Wireless Network
- Endpoint Security



- Catalyst Integrated Security Features
- Threat Detection and Mitigation
- Network Foundation Protection

- Edge Protection

SAFE Threat Response

- Service Disruption
- Data Disclosure and Modification
- Unauthorized Access
- Network Abuse
- Data Leakage
- Identity Theft and Fraud

Increasing Visibility for the LAN

Identify	Monitor	Correlate
LAN/port Authentication User Authentication Firewall Deep Packet Inspection Traffic Classification	Intrusion Detection Network Management Event Monitoring Network Telemetry Syslog	Event Analysis and Correlation

Increasing Control for the LAN

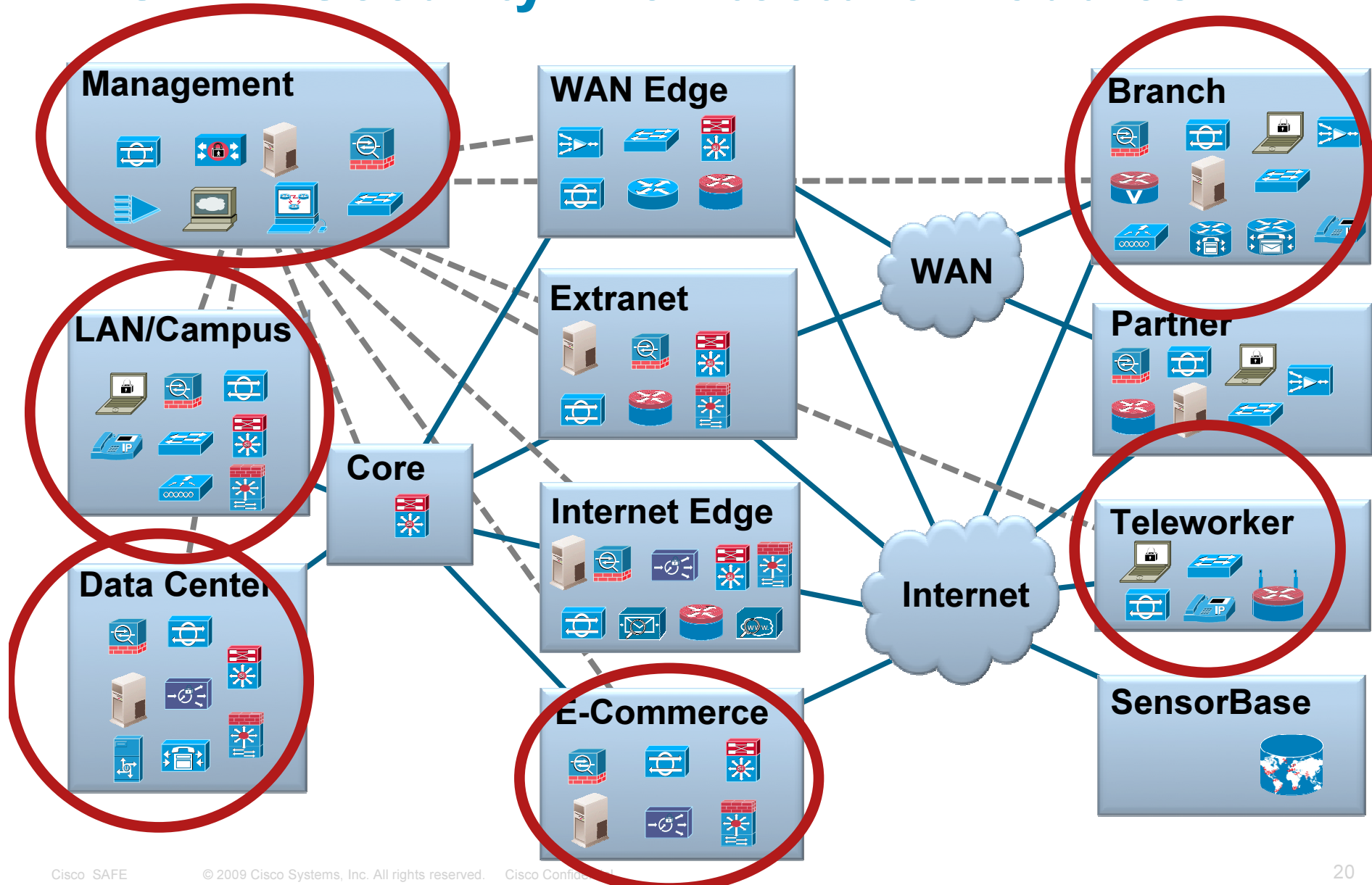
Harden	Isolate	Enforce
Network Foundation Protection OS Hardening CISF Endpoint Security Link and System Redundancy	VLANs Network Access Control IPS Firewall Access Control	Stateful Firewall Access Control ACLs, uRPF, Antispoofing DHCP Snooping Port Security Intrusion Prevention QoS Enforcement Network Access Control



Cisco Security Agent



SAFE Security Architecture Modules

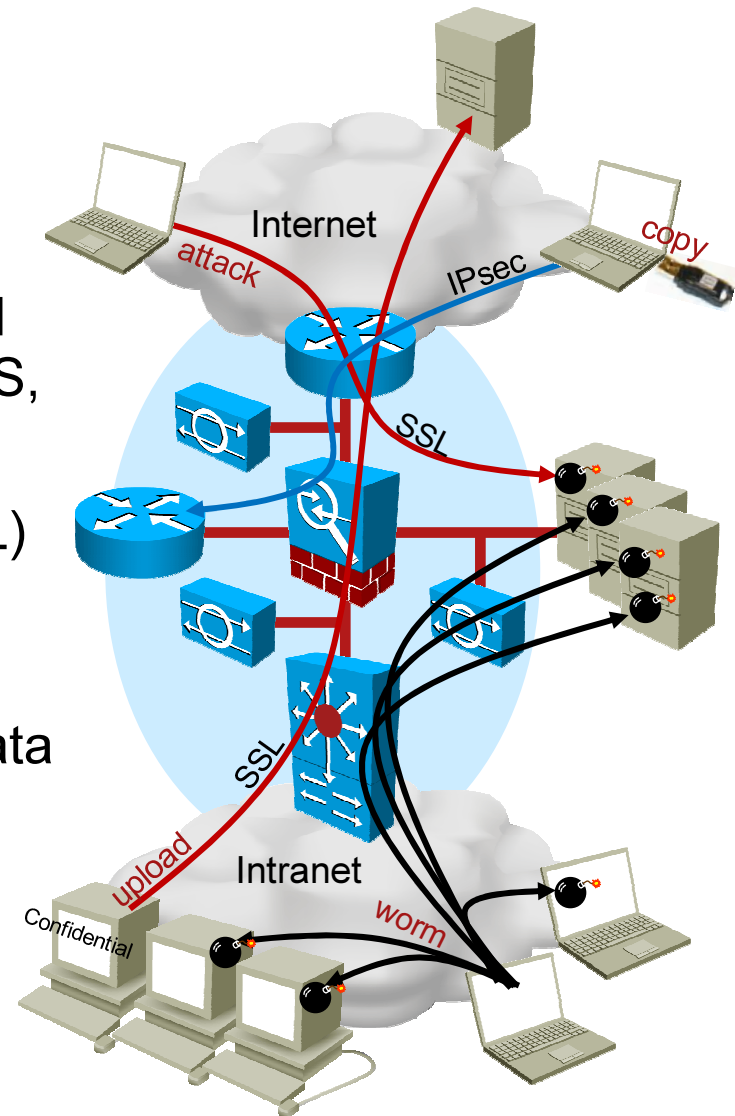


Advanced Endpoint Security

Drivers

Challenges facing common security practices:

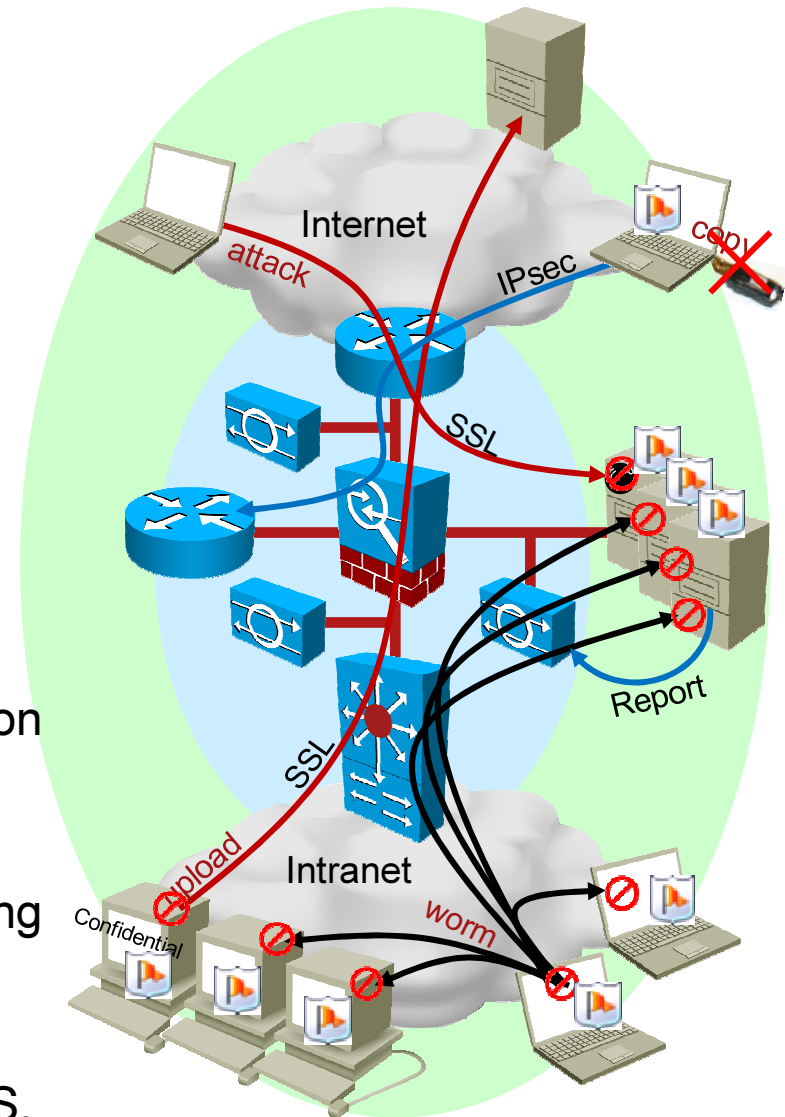
- New attacks that trick users into downloading malware cannot be stopped by signature-based mechanisms (e.g. IPS, AV)
- Encrypted end-to-end sessions (e.g. SSL) render firewalls and network IPS blind
- Network-based security devices cannot adequately control access to sensitive data (e.g. USB flash/disk, CD/DVD ROM, encrypted sessions)
- Security policies or regulatory requirements may be too demanding for the capabilities of network security solutions (e.g. PCI Compliance)



Advanced Endpoint Security

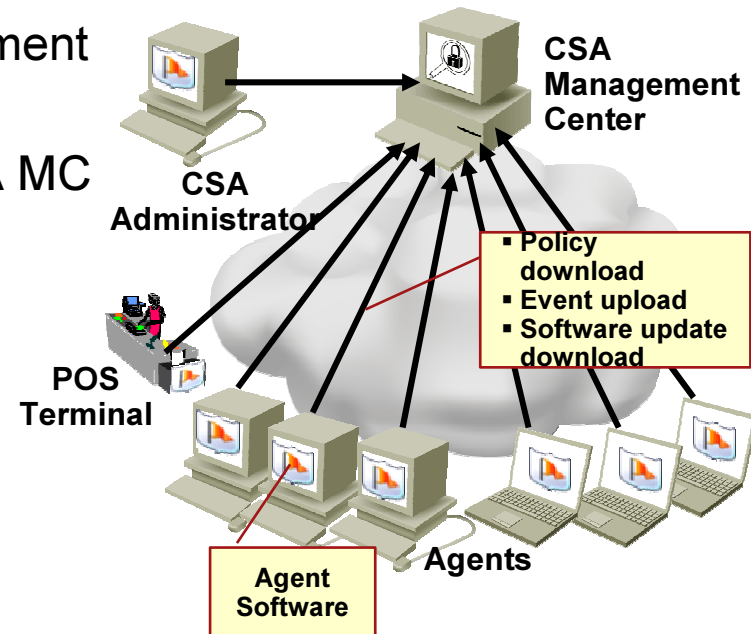
with Cisco Security Agent

- CSA extends network security solutions to end hosts
- Cisco Security Agent enhances security with:
 - **Zero Update protection** based on OS and application behavior
 - **Control of content** after decryption or before encryption (e.g. SSL, IPsec)
 - **Access control for I/O devices** based on process, network location and even file content
 - **Centralized management** and monitoring of events
 - **SDN Interaction** with other network solutions such as NAC, IPS, QoS, MARS, VOIP, etc



Security Characteristics, Features and Architecture of CSA

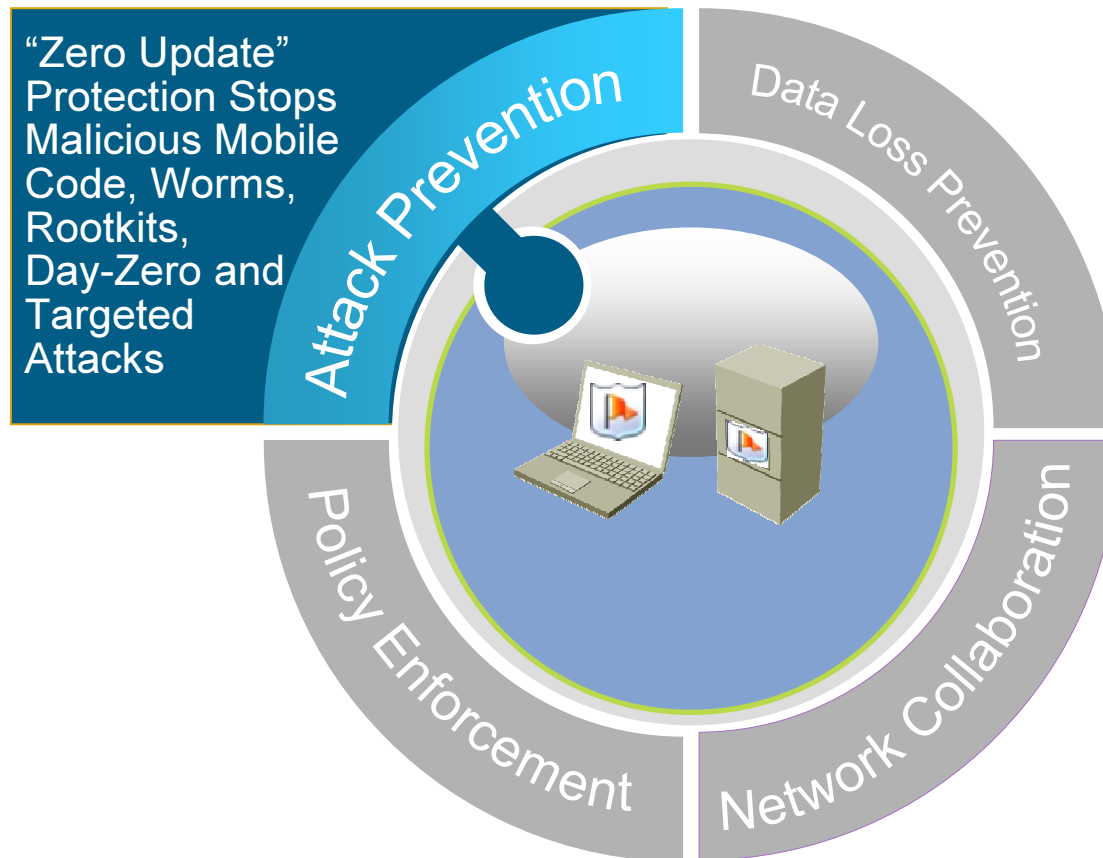
- CSA MC is used for centralized management and monitoring of agents (SSL)
- Agents periodically connect with the CSA MC to:
 - Upload event notifications
 - Download configuration changes
 - Download agent software and AV signature updates
- If CSA MC is unreachable:
 - Agents cache events (up to 300)
 - Apply a different (more restrictive) policy if so configured (e.g. when on the Internet)
- Up to 100,000 agents per CSAMC



#	Date	Host	Severity	Action	Event
3	2/22/2008 11:42:58 PM	localhost	Alert		TESTMODE: The process 'C:\WINDOWS\system32\cmd.exe' (as user 'LOCAL\NT AUTHORITY\SYSTEM') attempted to access 'C:\PROGRAM FILES\NORTON\NOD32\NOD32.EXE'. The file content matches 'Norton AntiVirus 8.5.0'. The attempted access was a read (operation = OPEN(READ)). The operation would have been denied. Details Rule 671 - Monitor Log
2	2/22/2008 8:04:44 PM	localhost	Alert		TESTMODE: The process 'C:\WINDOWS\system32\cmd.exe' (as user 'NT AUTHORITY\SYSTEM') attempted to access 'C:\PROGRAM FILES\NORTON\NOD32\NOD32.EXE'. The file content matches 'Norton AntiVirus 8.5.0'. The attempted access was a write (operation = OPEN(WRITE)). The operation would have been denied. Details Rule 671 - Monitor Log
1	2/22/2008 20:18:46 AM	localhost	Alert		TESTMODE: The process 'C:\Program Files\Internet Explorer\EXPLORE.EXE' (as user 'LOCAL\NT AUTHORITY\SYSTEM') attempted to access 'C:\PROGRAM FILES\NORTON\NOD32\NOD32.EXE'. The file content matches 'Norton AntiVirus 8.5.0'. The attempted access was a read (operation = OPEN(READ)). The operation would have been denied. Details Rule 671 - Monitor Log

Cisco Security Agent

Always Vigilant Comprehensive Endpoint Security



SINGLE INTEGRATED AGENT AND MANAGEMENT

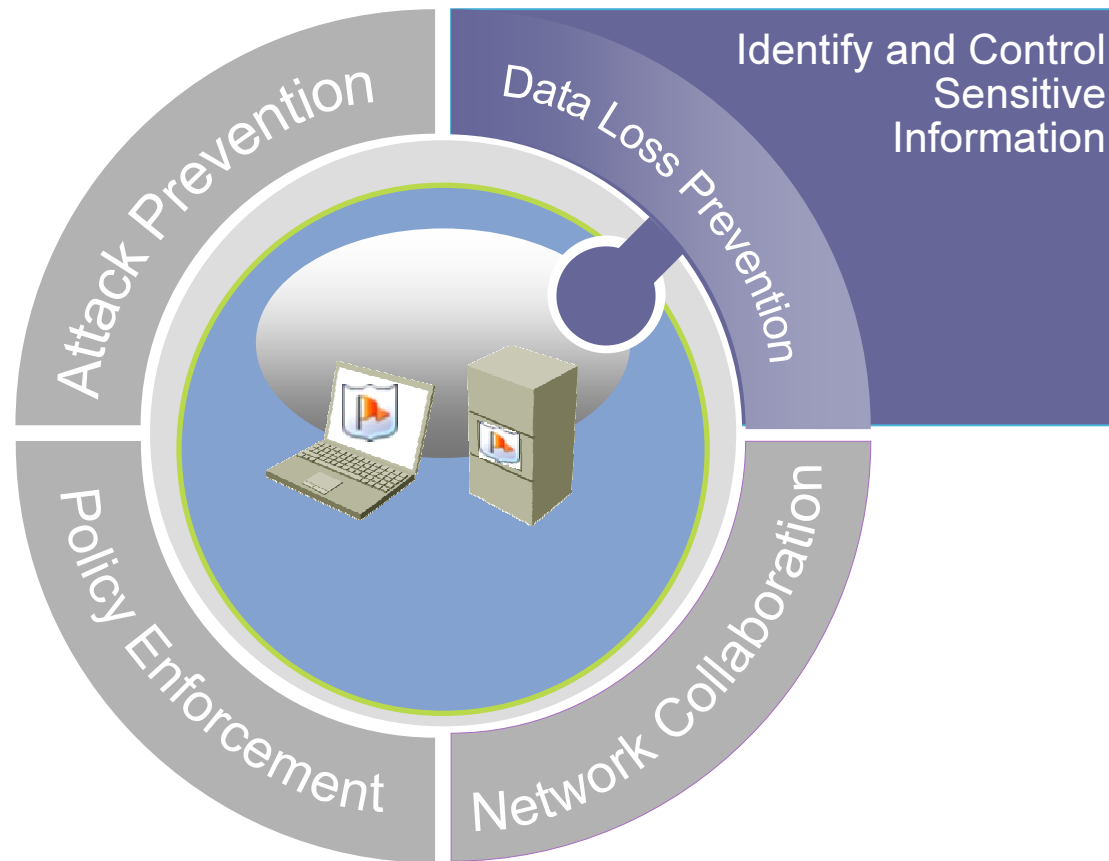
CSA's "Zero Update" Security Policies

Policy Description	Function
Security- Protect from Downloaded Applications- Protects systems from Untrusted Applications	Protects systems from Untrusted Applications – viruses, bots, trojans delivered via network attack
Security- Protect from Downloaded Data-	Protects systems from Untrusted Applications – viruses, bots, trojans delivered via downloaded data like poisoned PDF
Security- Protect from Spyware-	Protects against spyware & Trojans, will detect, and prevent spyware from attaching to browsers, and executing new applications
Security-Protect with a Distributed Firewall-	Provides a centrally managed Distributed Firewall for hosts, hardens exposed Windows kernel services
Security-Quarantine exploited hosts or application	Isolate system from network if rootkit detected; block infected application from communicating on the network

**CSA also includes a traditional signature-based antivirus engine
- this relies on daily updates from the CSAMC management server**

Cisco Security Agent

Always Vigilant Comprehensive Endpoint Security



SINGLE INTEGRATED AGENT AND MANAGEMENT

Creating a CSA Sensitive Information Policy – DLP Checklist

Corporate Security Policy regarding Sensitive Information	Establish/ Monitor	Enforce	Ensure/ Justification
Prevent sensitive information from being written to USB devices and other removable media			
Prevent remote clients from accessing sensitive information			
Prevent sensitive information from accessing the network TCP/UDP			
Prevent CD-ROM burning applications from accessing sensitive information			
Prevent Clipboard abuse			
Prevent sensitive information from being written to Network Drives			
Prevent Sensitive information from being copied			
Allow only authorized applications to access the sensitive information			
Impose restrictions for wireless, and remote users, they cannot copy sensitive information to removable media			
Protect authorized applications accessing sensitive information			

CSAMC DLP Audit Log - Alerts

Management Center for Cisco Security Agents V6.0 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://csa60bls/csamc60/webadmin

Google

Management Center for Cisco Security Agents V6.0

Events Systems Configuration Analysis Maintenance Reports Search Help

Home | Advanced | All OSes | Logout

Events > Event Monitor

Monitoring filter [change](#)

Displaying: last 50 events
Sort by: Order received
Filter out similar events: Yes
Next refresh: in 15 seconds
Refresh interval: 15 seconds

#	Date	Host	Severity	Action	Event
50	2/23/2008 10:05:34 AM	csa60bls	Notice	!	The process 'C:\WINDOWS\system32\notepad.exe' (as user CSA60BLDS\Administrator) attempted to access a resource which resulted in the user being shown the following notification. '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.' The user was queried and a 'No' response was received. The user provided the following justification. 'I need this data to work from home' Details Rule 1240 Wizard
49	2/23/2008 10:03:19 AM	csa60bls	Notice	+	The process 'C:\Program Files\VMware\VMware Tools\VMwareUser.exe' (as user CSA60BLDS\Administrator) attempted to read clipboard data written by process C:\WINDOWS\system32\winlogon.exe. The operation was allowed by default (rule defaults). Details Rule 1264 System State Wizard
48	2/23/2008 10:02:45 AM	csa60bls	Notice	+	The process 'C:\WINDOWS\system32\notepad.exe' attempted to access 'F:\Stolen jeCC117771#s.txt'. The operation was allowed by default (rule defaults). This caused a Data Scan, resulting in the Content Tag <credit_card><regulatory>. being applied to this file.

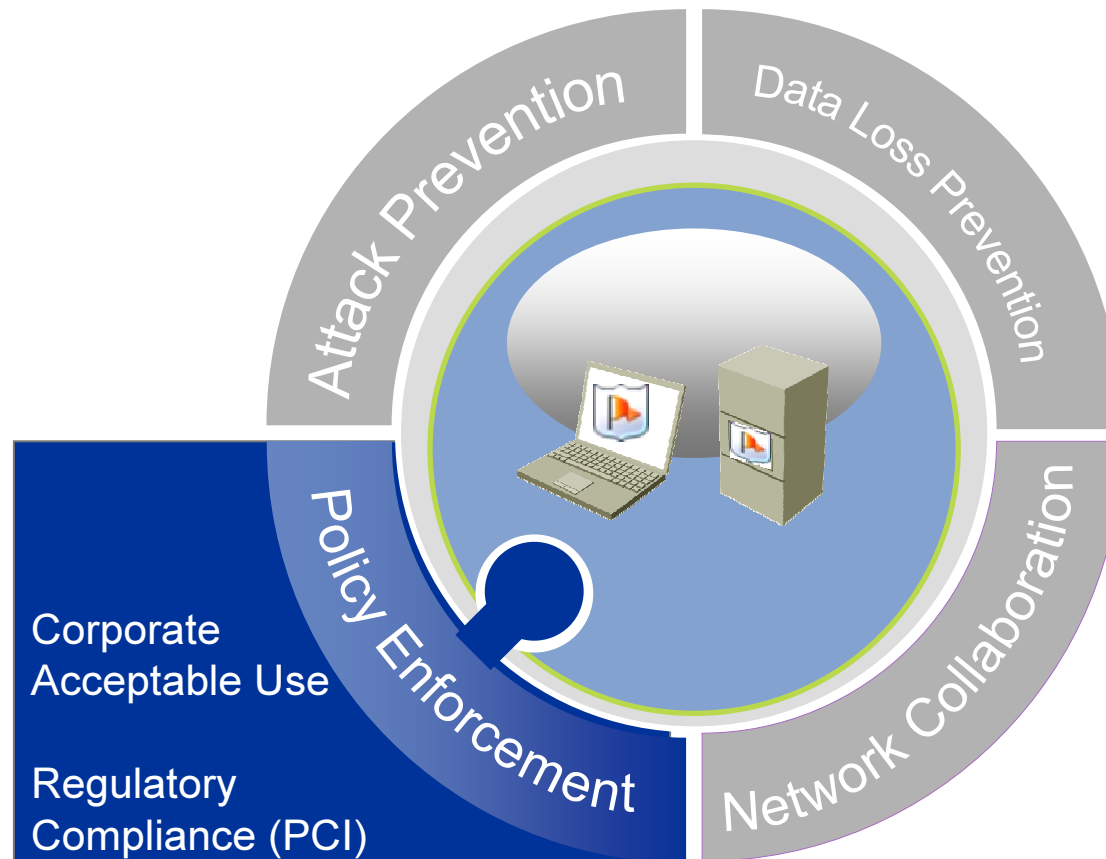
No rule changes pending [Generate rules](#)

Logged in as: admin

Transferring data from csa60bls...

Cisco Security Agent

Always Vigilant Comprehensive Endpoint Security



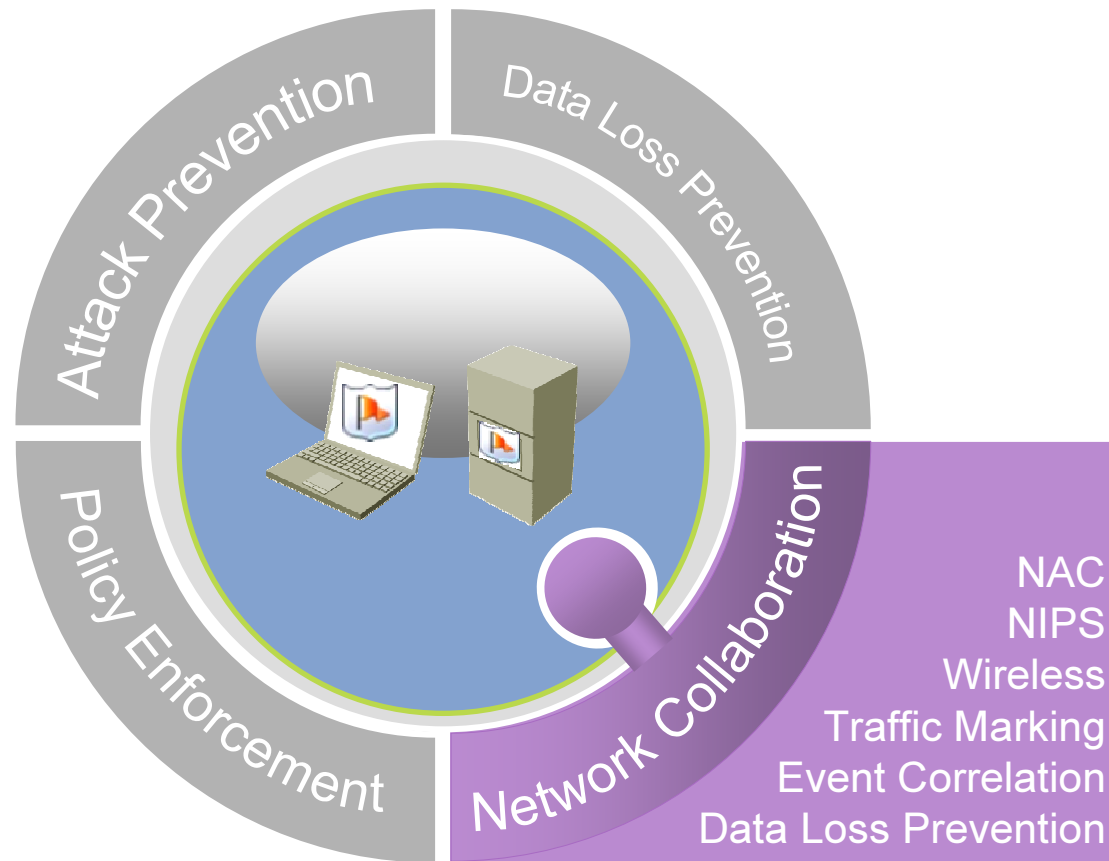
SINGLE INTEGRATED AGENT AND MANAGEMENT

CSA's Acceptable Use Policies

Policy Description	Function
Prevent writing data to USB devices	Control file access to USB memory sticks, floppy disks, CDs, and hard disks
Protect with Personal Firewall	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)
Various others	Available via CSAMC Advanced GUI function

Cisco Security Agent

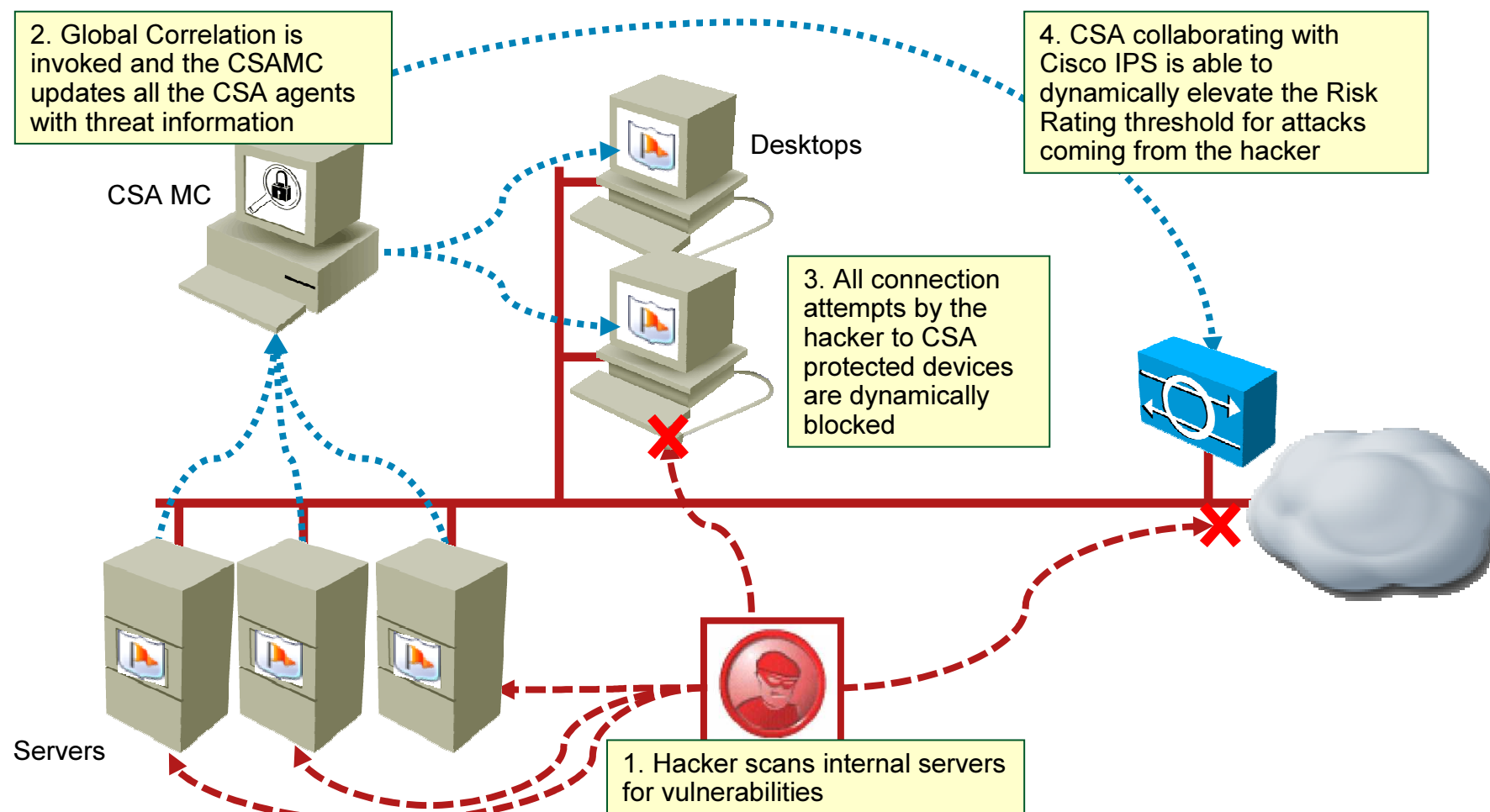
Always Vigilant Comprehensive Endpoint Security



SINGLE INTEGRATED AGENT AND MANAGEMENT

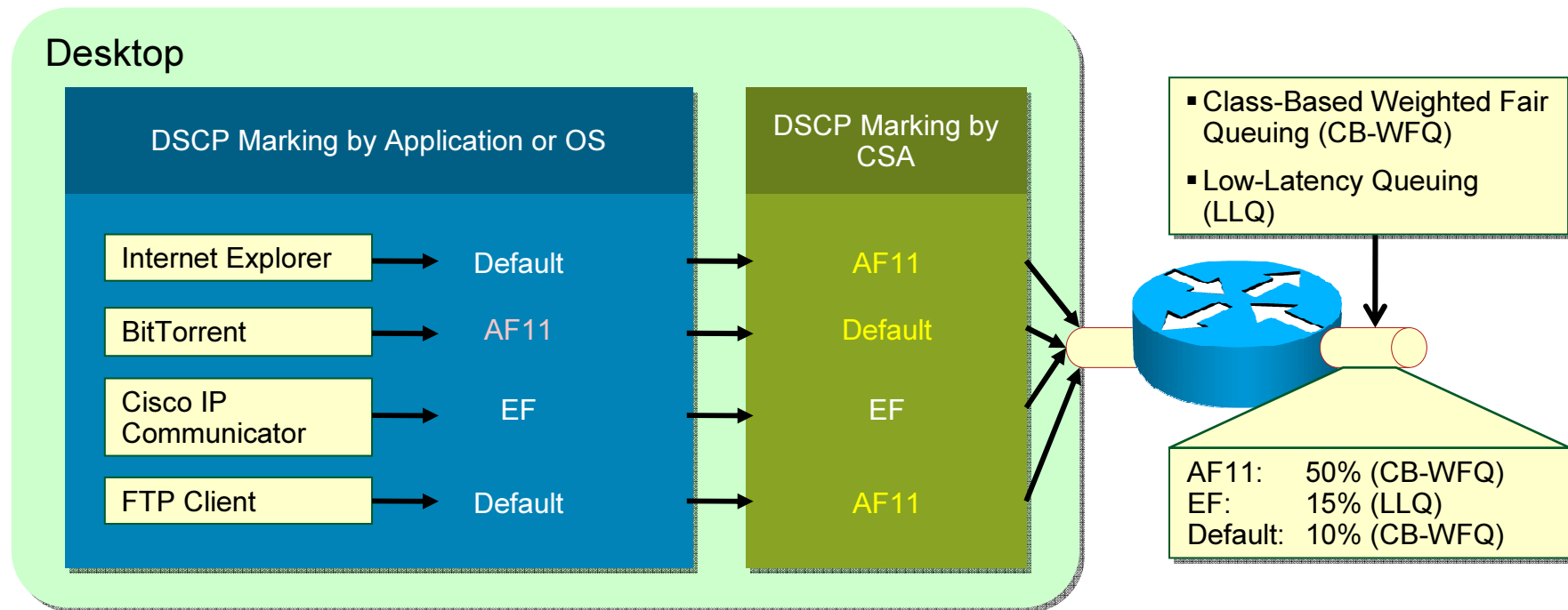
Inform NIPS of Hostile Hosts

Configured via CSAMC Advanced GUI option



Per-Application Network Optimization (QoS)

Available via Advanced GUI option on CSAMC



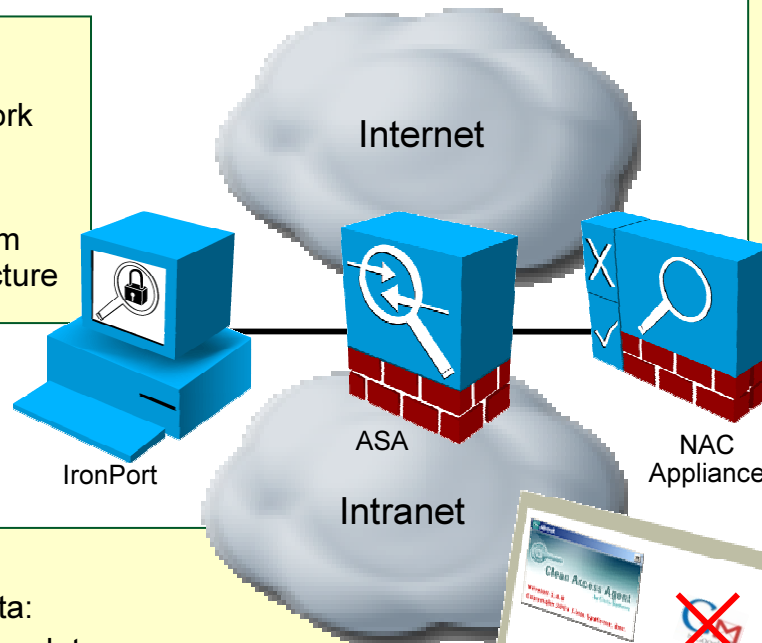
- “Bad” software can mark packets to:
 - Get a better service from the network
 - To perform an attack (e.g. flooding with EF-marked packets can cause DoS for IP telephony)
- Use CSA to remark packets according to QoS design

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

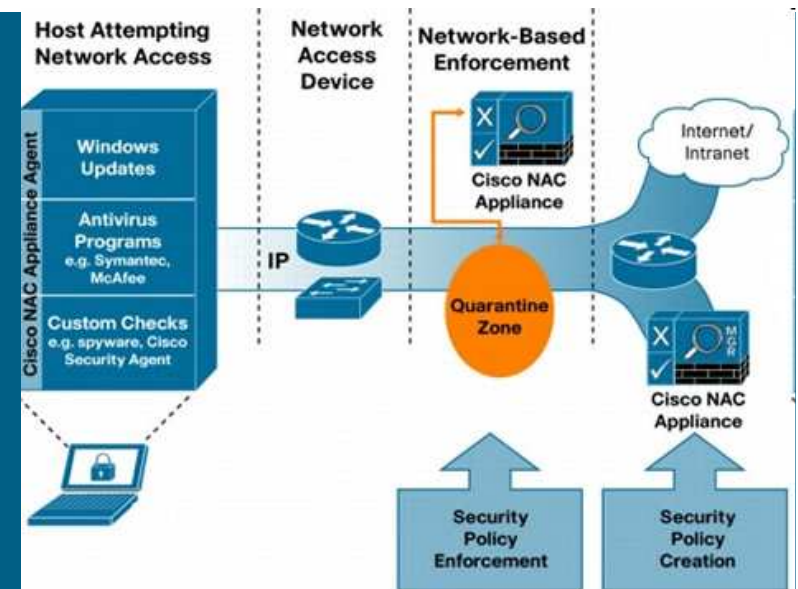
- Prevent loss of sensitive data:
 - Scan data files for sensitive data
 - Prevent copying to external media (USB flash and disk, IR/Bluetooth devices)
 - Prevent using with (inter)network applications (e-mail, IM, browser)
- Prevents bypass of IronPort network protection

New features in CSA 6.0.1

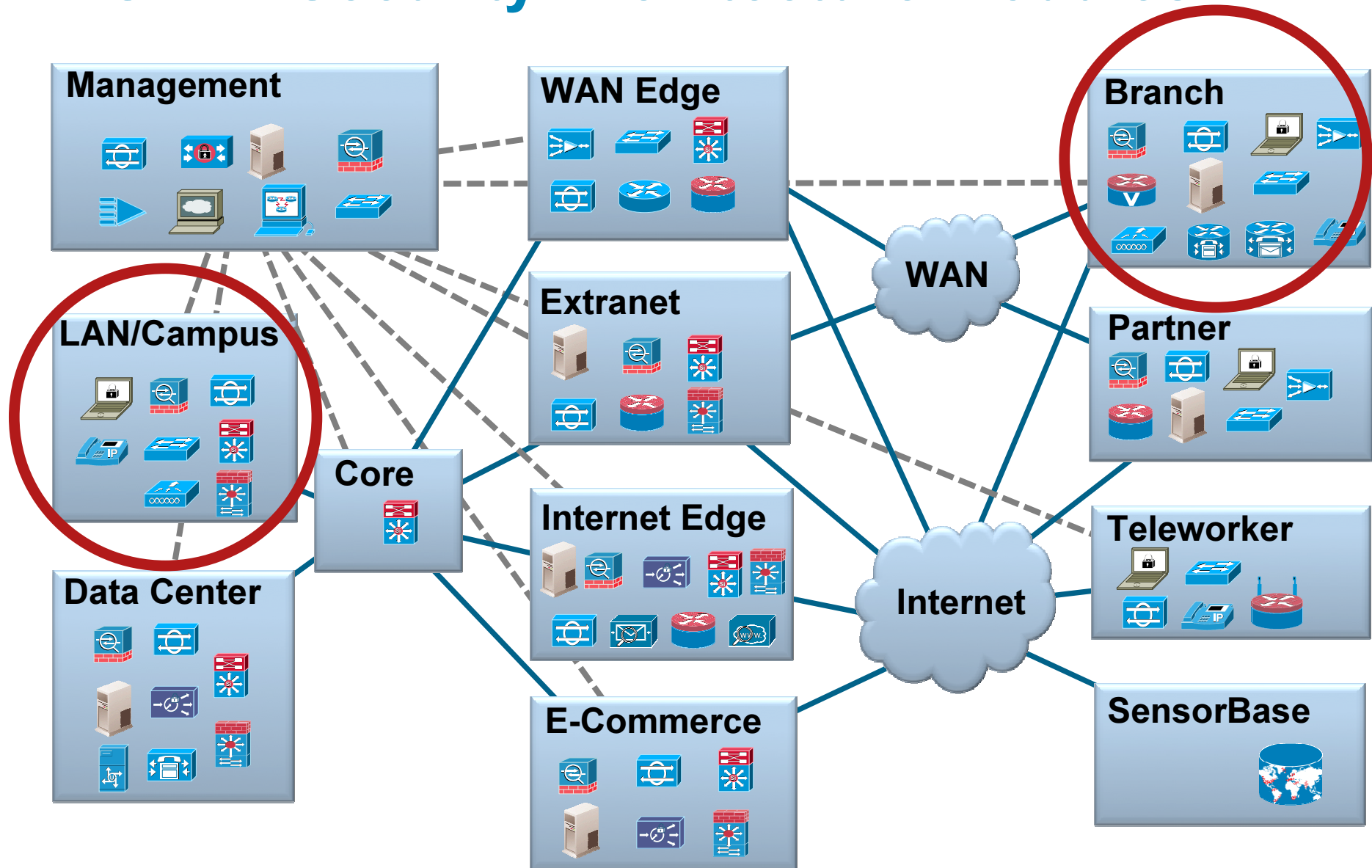
- CSA Management center High Availability
- CSA Management center VMWare support
- Platform support:
Red Hat Enterprise Linux 5.0, Solaris 10, SUSE Linux 10
- Management summary reports
Daily Events by Event Type, Top 20 Infected Hosts, Top 20 Identified Viruses etc.
- Digital signature identification
- Scheduling Software Update wizard
- Resource – Release Notes CSA 6.0.1
http://www.cisco.com/en/US/docs/security/csa/csa601/release_notes/CSA601RN.html



Cisco Network Admission Control



SAFE Security Architecture Modules



Evolution of Network Access Control

Topology Aware to Role Aware



Network Admission Control (NAC)

- Posture validation endpoint policy compliance



Identity-Based Access Control

- Flexible authentication options:
802.1x, MAB, WebAuth, FlexAuth
- Comprehensive post-admission control options:
dACL, VLAN assignment, URL redirect, QoS...



Network Address-based Access Control

- ACL, VACL, PACL, PBACL etc



NAC Tasks

- Role-based access

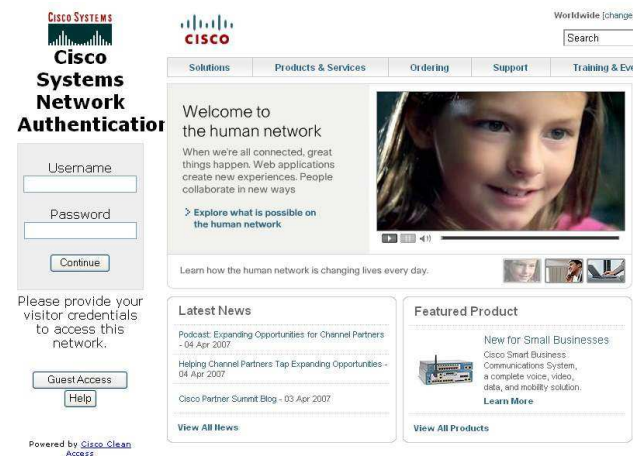


List of Roles	New Role	Traffic Control	Bandwidth	
Role Name	IPSec	Roam	VLAN	Description
Unauthenticated Role	deny	deny		Role for unauthenticated users
Temporary Role	deny	deny		Role for users to download requirements
Quarantine Role	deny	deny		Role for quarantined users
Allow All	deny	deny		Full Access
Guest Access	deny	deny	:666	guest privileges
consultant access	deny	deny	:55	consultant privileges

- Device compliance

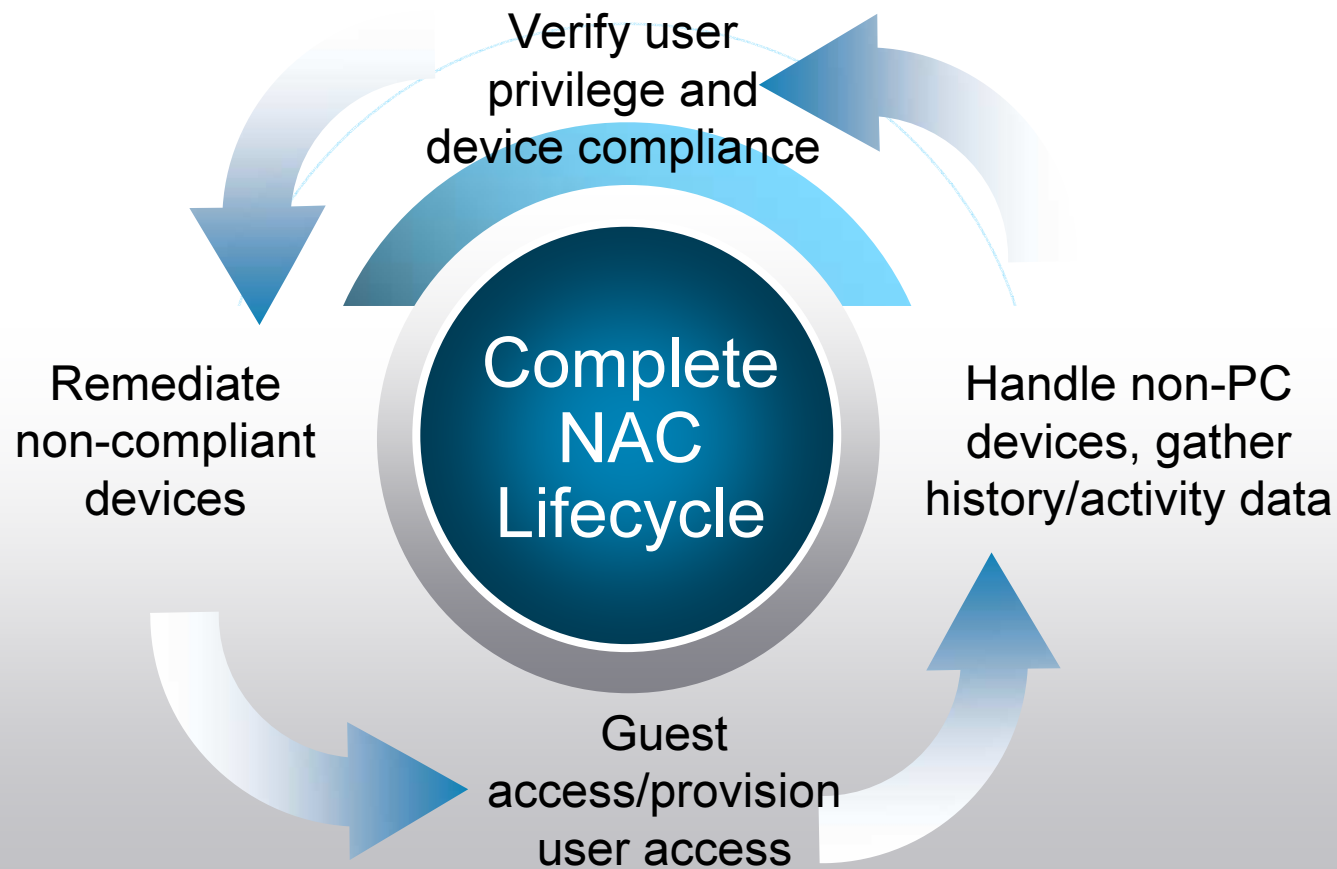


- Guest Lifecycle Management



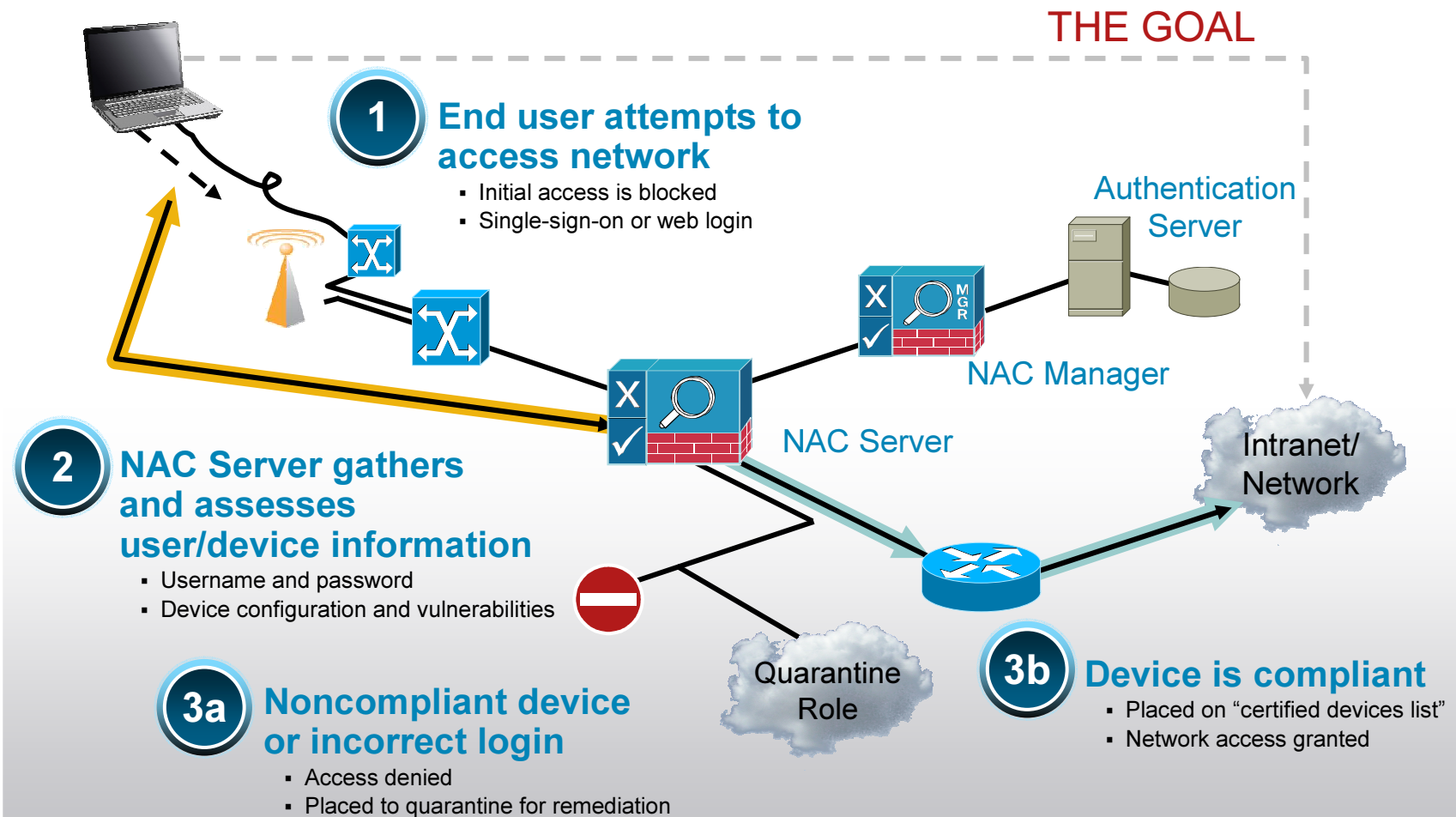
NAC Functions Defined

Ensuring role-based access and endpoint security policy compliance



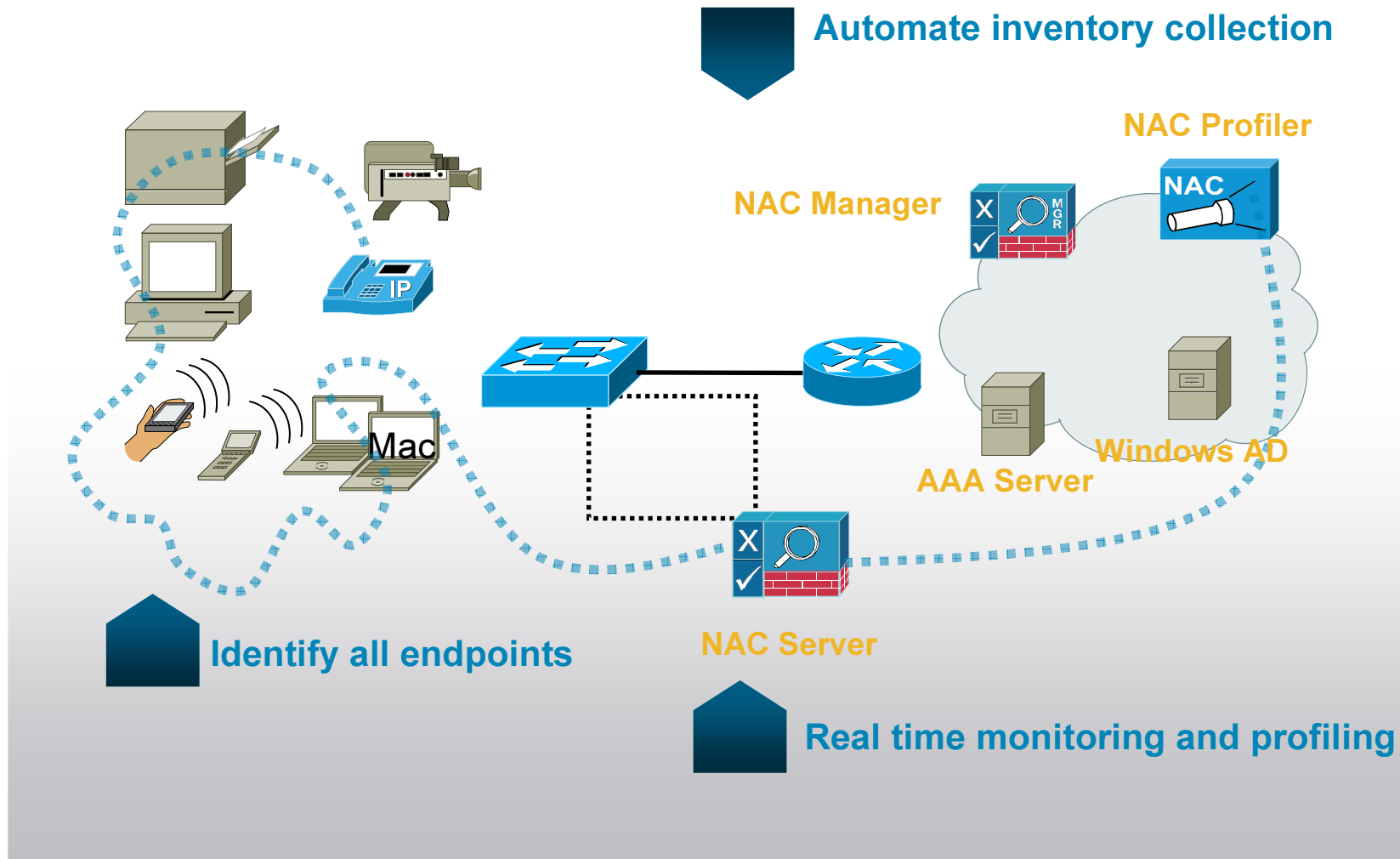
How Cisco NAC Works

A Conceptual View

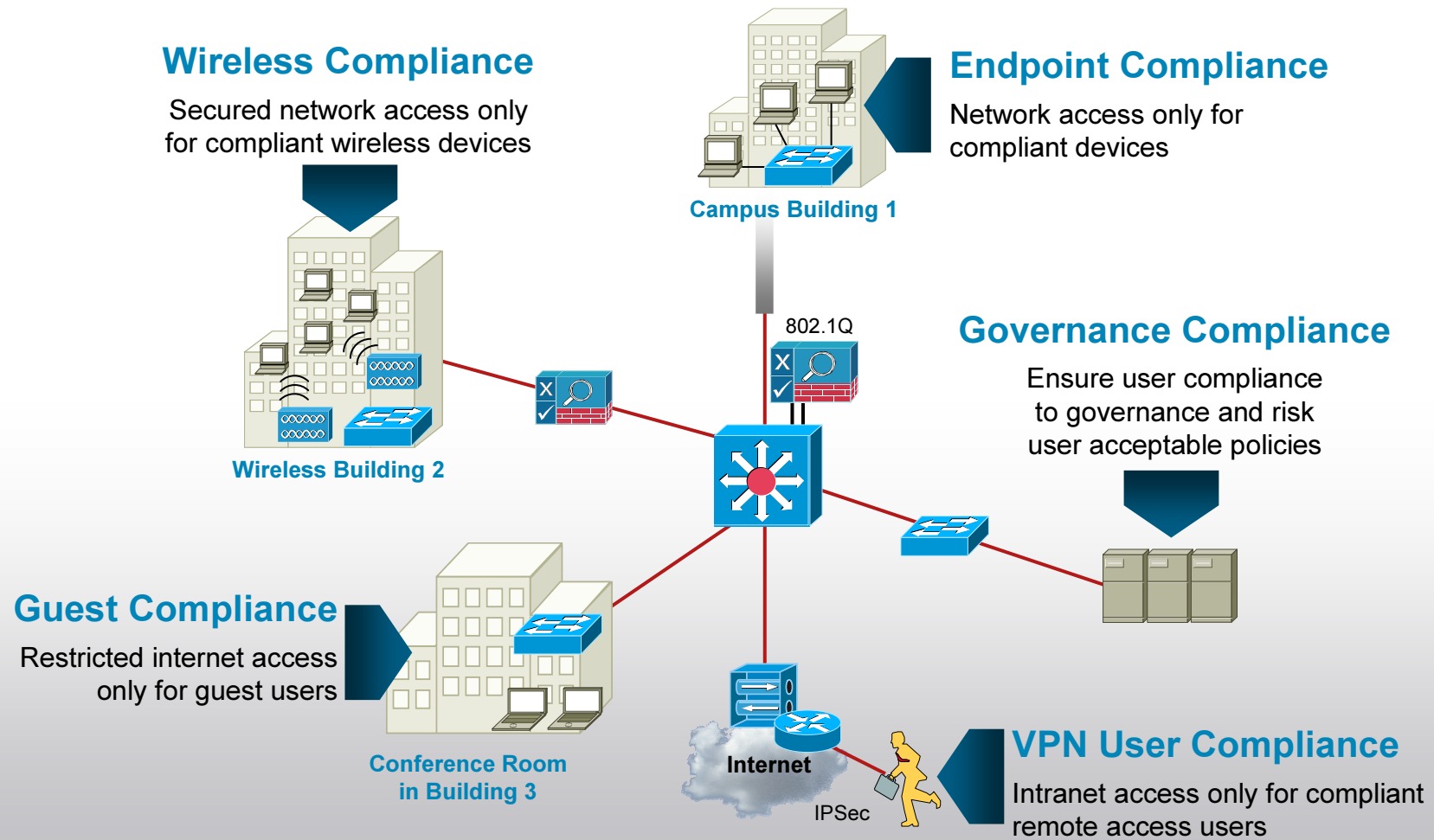


Device Profiling

Cisco NAC Profiler: Visibility, Intelligence, and Automation



Cover All Use Cases



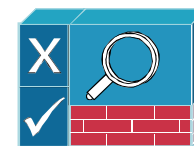
Cisco NAC Key Ingredients

NAC Manager and Server (Required)



NAC Manager

Centralized management, configuration, reporting, and policy store



NAC Server

Posture, services and enforcement

NAC Profiler, Guest Server and ACS (Optional)



NAC Profiler

Profiles unmanaged devices



NAC Guest Server

Full-featured guest provisioning server



ACS Server

Access policy system for 802.1x termination

Endpoint Components (Optional)



NAC Agent

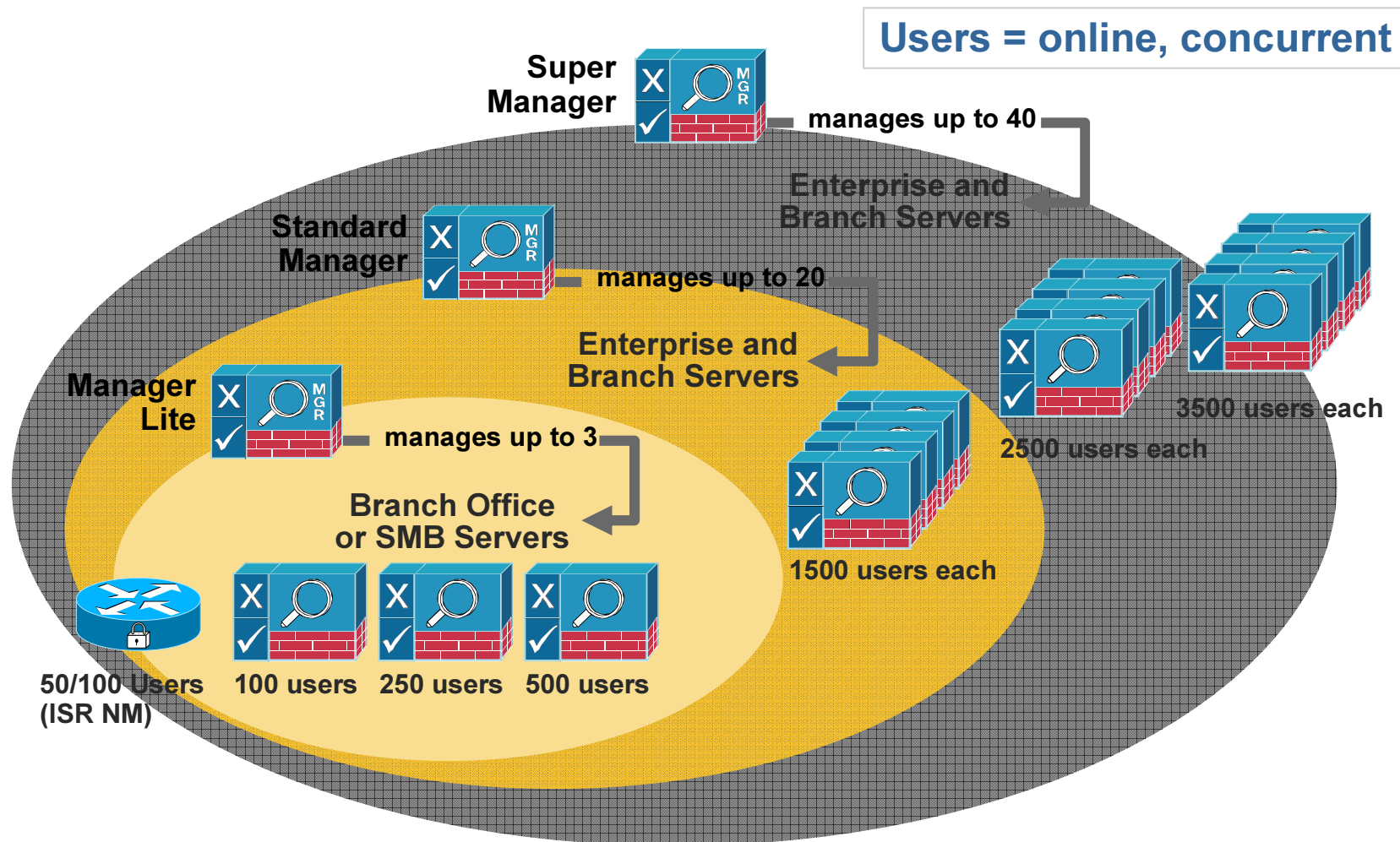
No-cost client: Persistent, dissolvable, or web



802.1x Supplicant

CSSC or Vista embedded supplicant

Cisco NAC Appliance Sizing

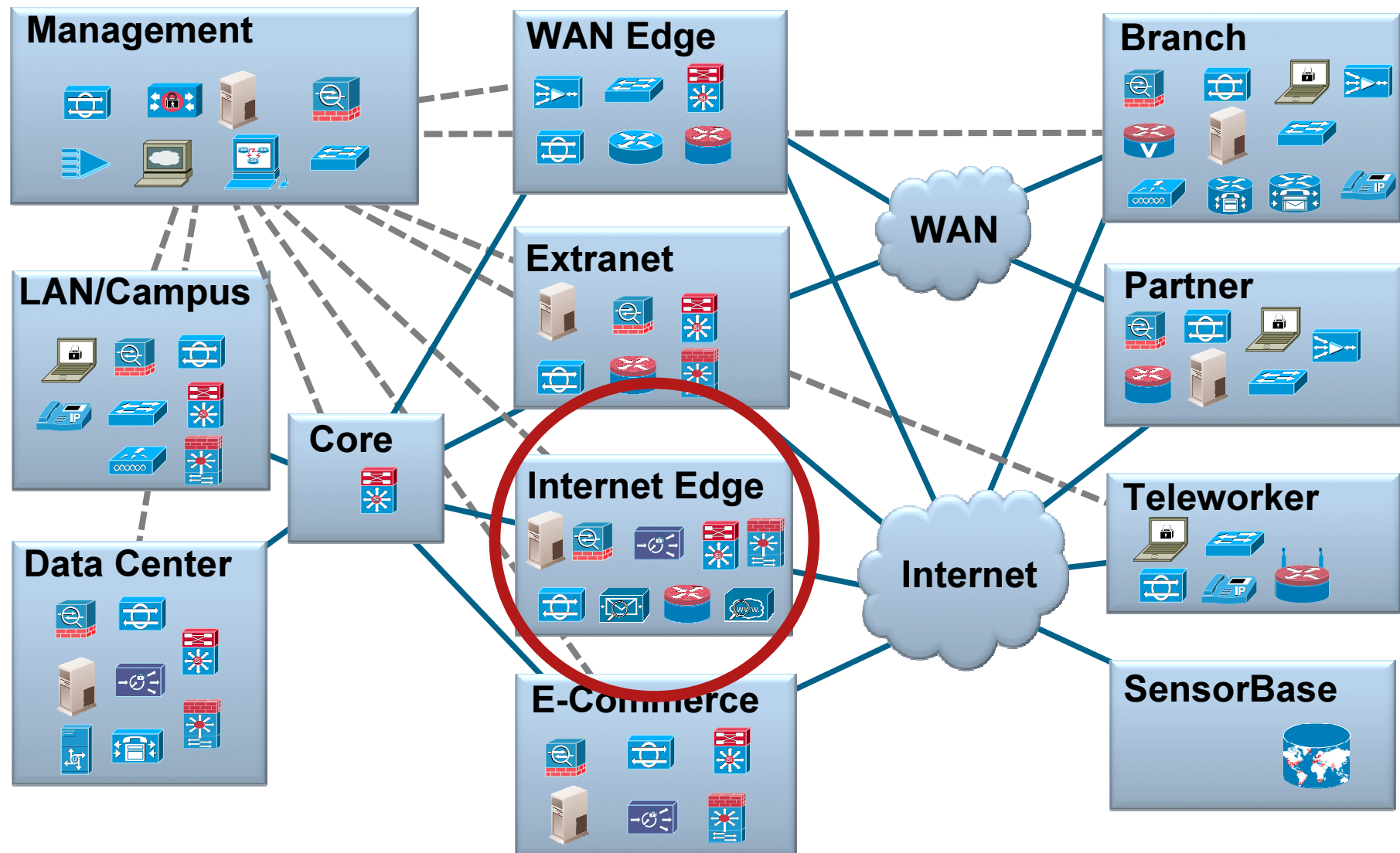




Cisco IronPort Email Security



SAFE Security Architecture Modules



Key Threats in the Internet Edge

- Botnets
- Denial of Service (DoS)
- Distributed DoS
- Spyware, malware, adware
- Phishing, email spam
- Intrusions and takeovers
- Network abuse
- Identity theft, fraud
- Data leakage



ATTACHMENT SPAM
(PDF, EXCEL, MP3)



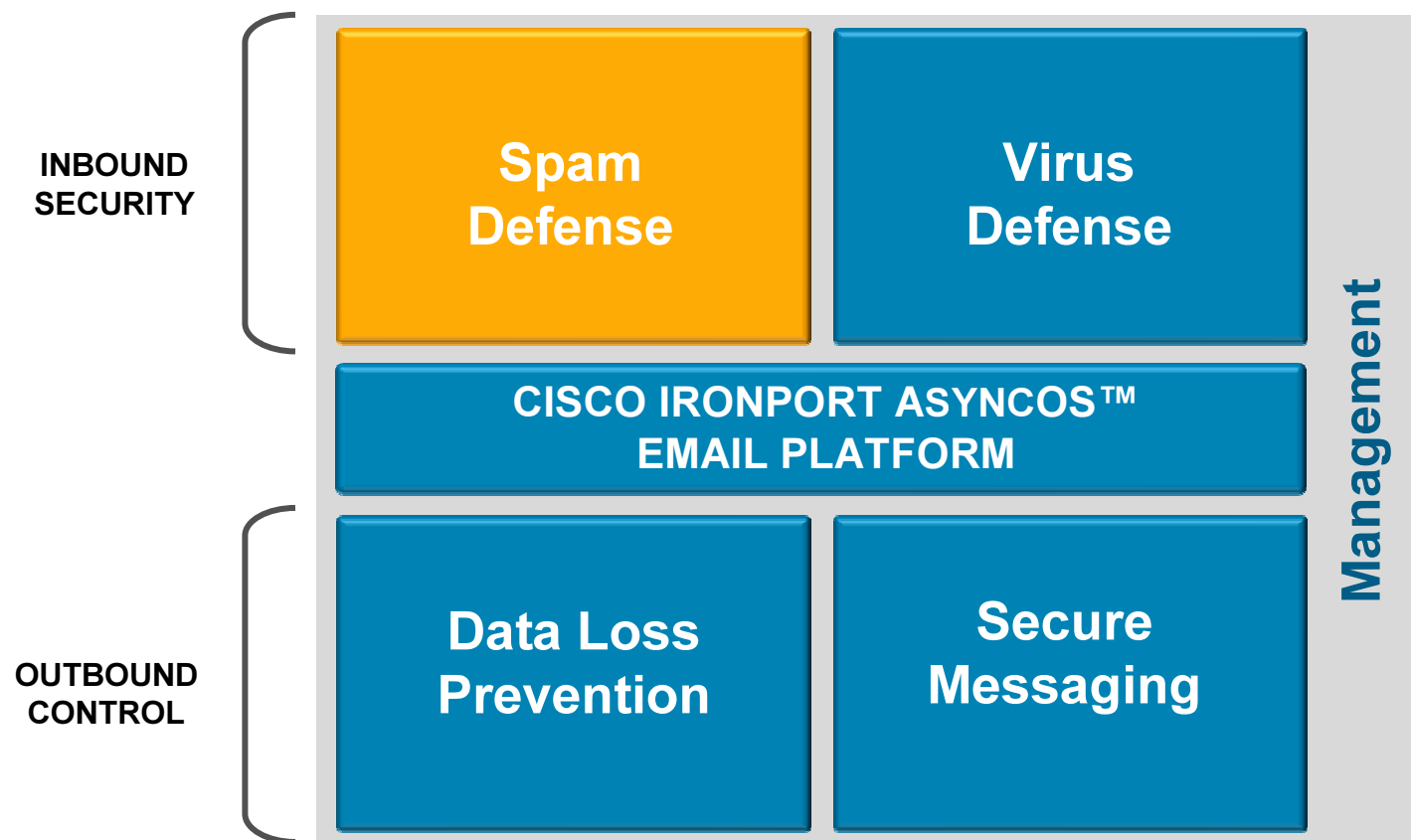
IMAGE SPAM

TARGETED ATTACKS



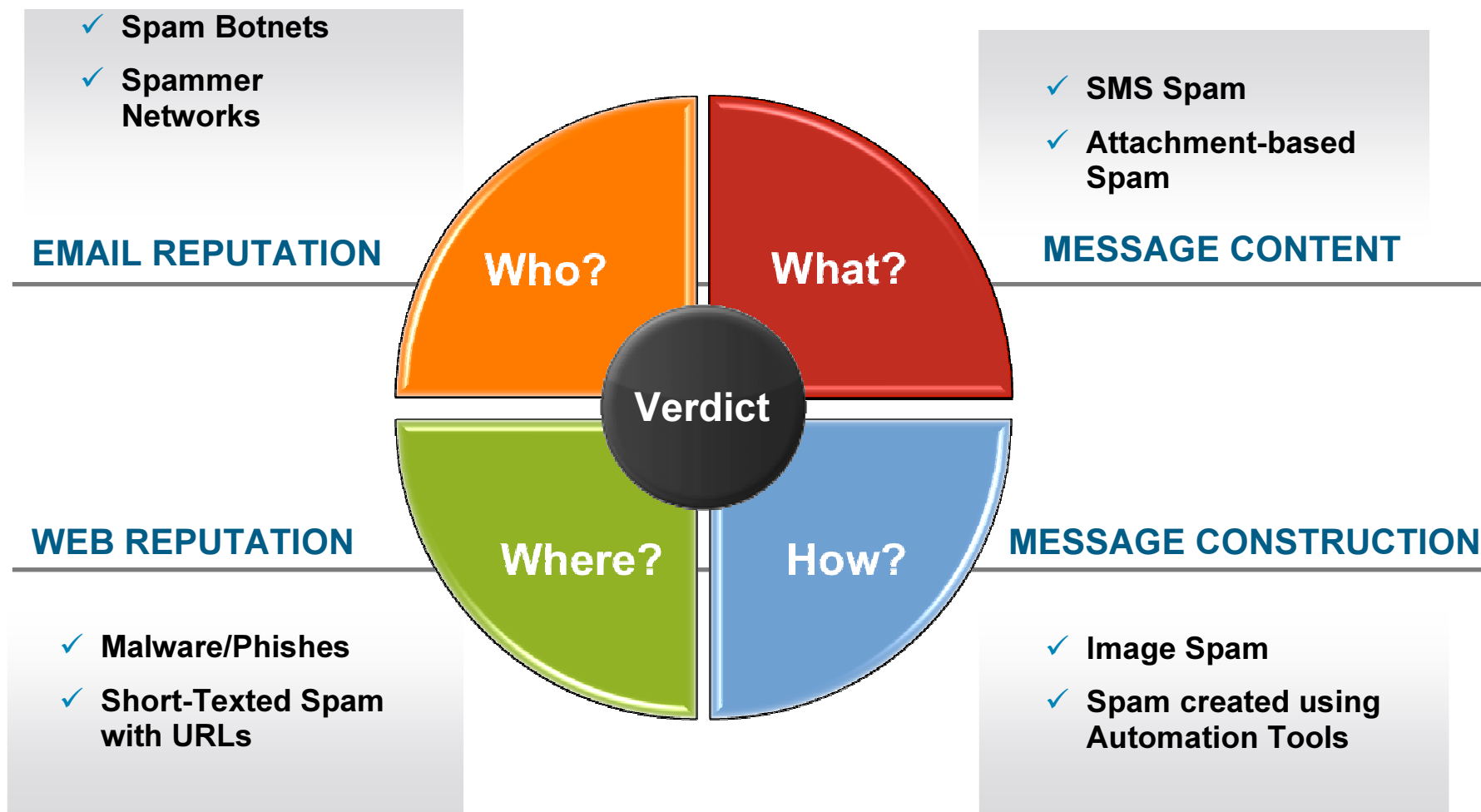
Email Security Architecture

Inbound Security, Outbound Control



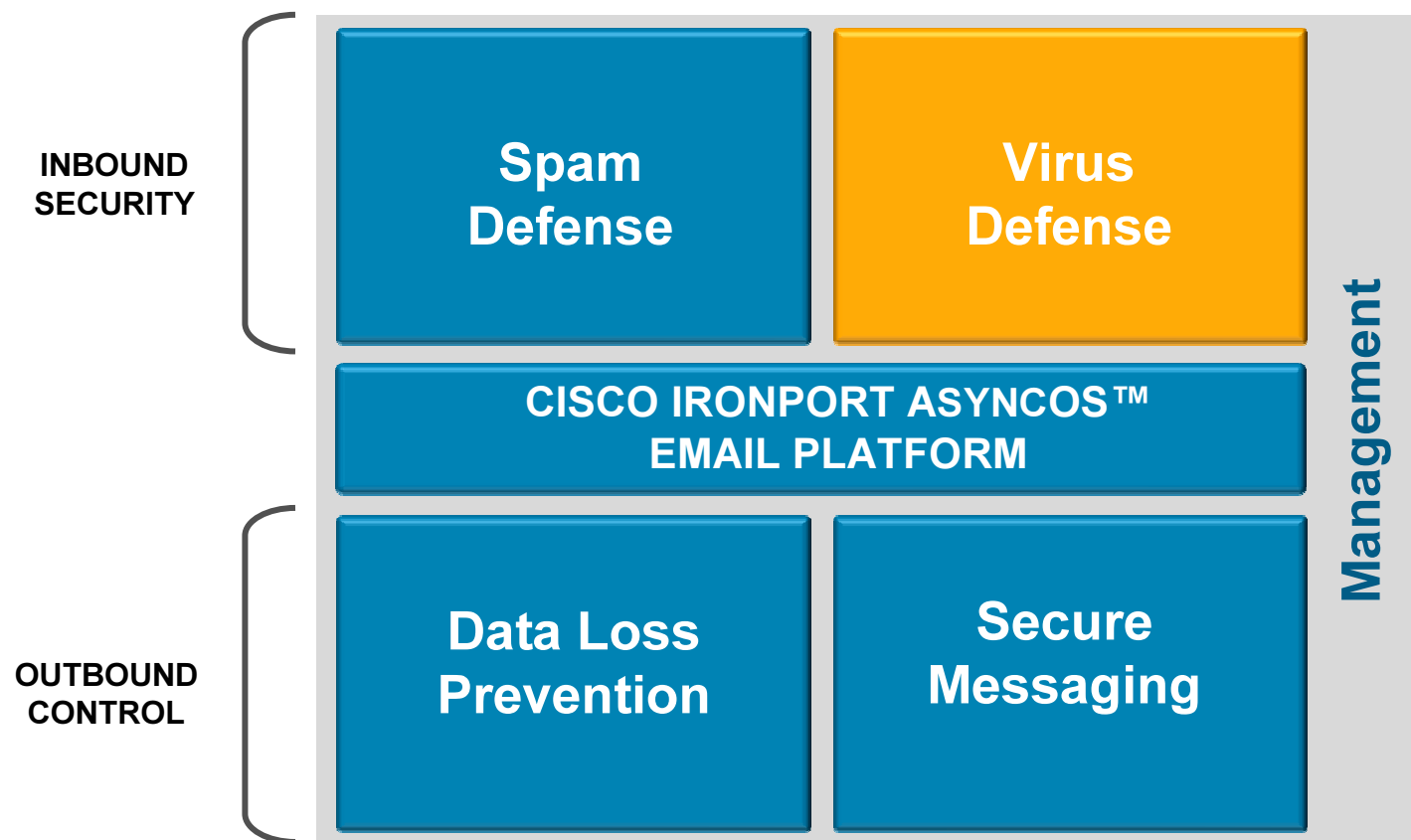
Cisco IronPort Anti-Spam

Defense in Depth Spam Protection

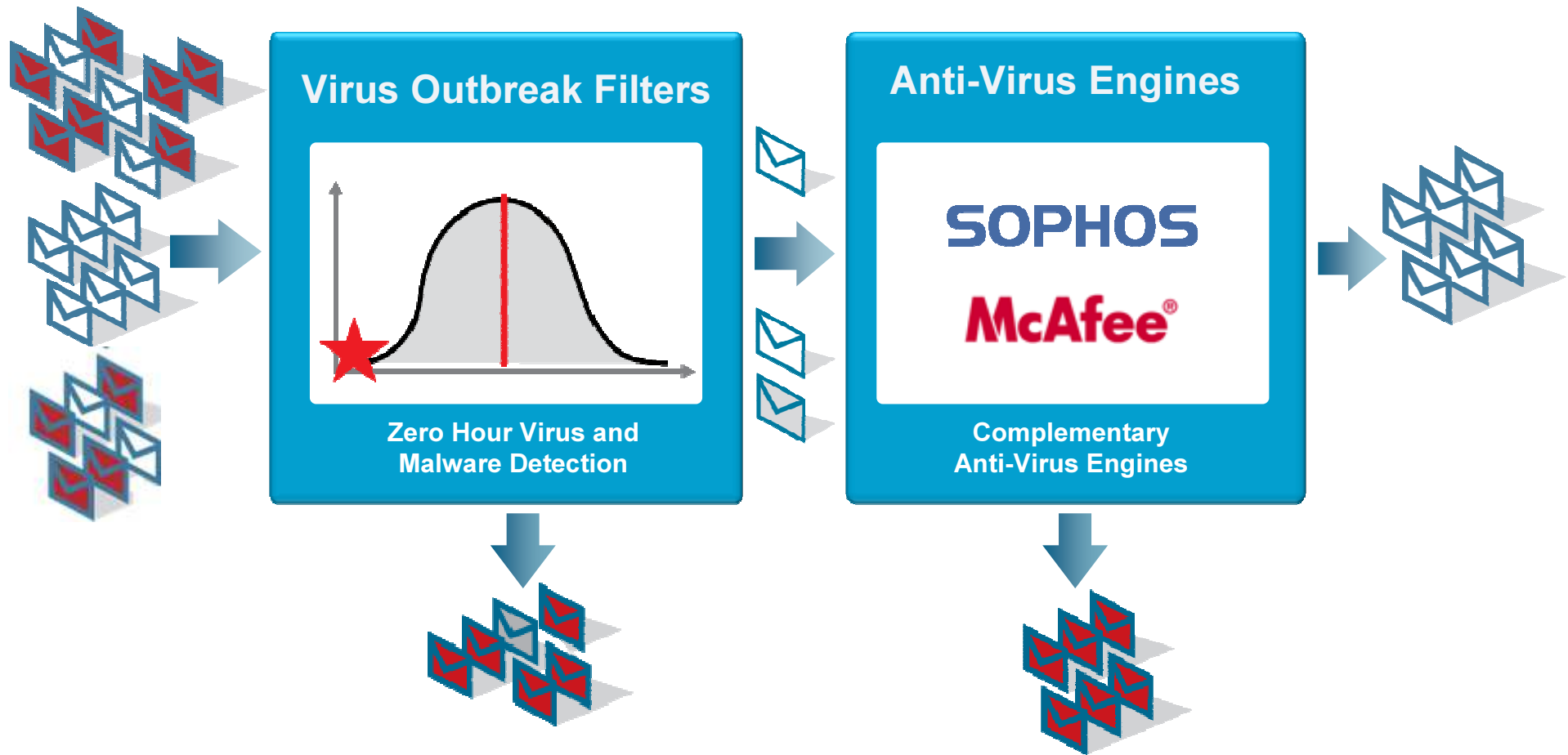


Email Security Architecture

Inbound Security, Outbound Control



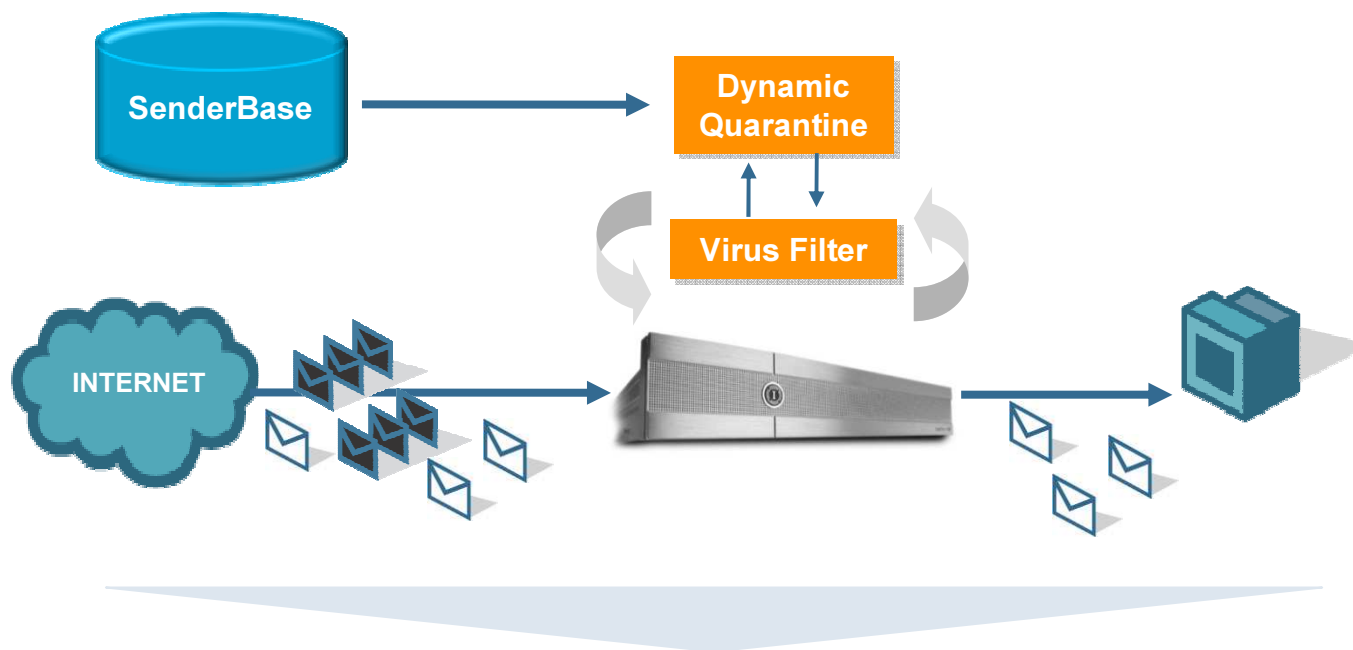
Anti-Virus Defense in Depth



Cisco IronPort Virus Outbreak Filters

Zero Hour Malware Prevention

Virus Outbreak Filters In Action



Virus Outbreak Filters Advantage

Average lead time*.....over 13 hours
Outbreaks blocked*291 outbreaks
Total incremental protection*..... over 157 days

"Since VOF we have not had a single virus outbreak!"



"Over 24,000 virus positive messages stopped in 9 months"

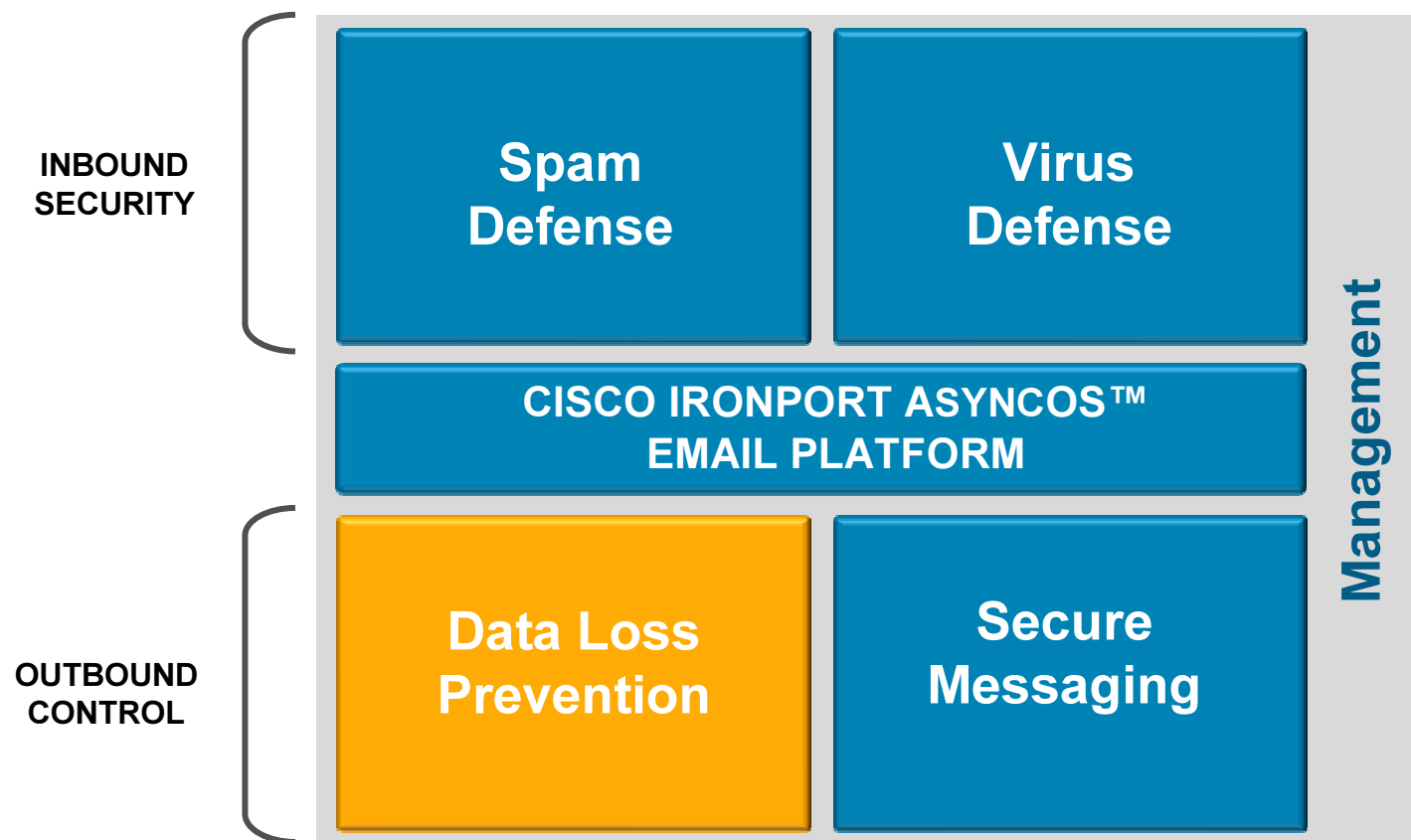


"VOF has stopped more than 12,000 separate viral messages in the last year"



Email Security Architecture

Inbound Security, Outbound Control



Data Loss Prevention

Simple Set Up

- Easy “3 click” set-up using content filters
- Use pre-defined content categories or create / customize your own
- Can be applied to specific users under specific conditions

Message Body or Attachment

Does the message body or attachment contain text that matches a specified pattern?

- ☐ Contains text:
 *
- ☒ Contains smart identifier:
ABA Routing Number ▼
- ☐ Contains term in content dictionary:
HIPAA-Dictionary_txt ▼

Number of matches required: (1-1000)

For content dictionaries, the number of matches is term weight.

☒ Import from local computer:

☐ Import from the *configuration* directory on your IronPort appliance

- GLBA-Dictionary.txt
- HIPAA-Dictionary.txt
- PCI-Dictionary.txt
- README
- SOX-Dictionary.txt
- config.dtd

▼ Smart Identifiers: ?

Enable Smart Identifiers	Weight
☒ Credit Card Numbers	1 ▼
☒ Social Security Numbers	1 ▼
☒ ABA Routing Numbers	1 ▼
☒ CUSIPs	1 ▼

Data Loss Prevention

Comprehensive Remediation & Reporting

- Multiple remediation actions – encrypt, quarantine, drop, bounce, BCC, strip content
- Offending content highlighted in quarantine for easy analysis
- Reporting on a per policy and per user basis

The screenshot displays the Cisco Data Loss Prevention quarantine interface. On the left, a list of remediation actions is shown, including 'Strip Attachment by Content', 'Strip Attachment by File Info', 'Add Disclaimer Text', 'Bypass Outbreak Filter Scanning', 'Send Copy (Bcc:)', 'Notify', 'Change Recipient to', 'Send to Alternate Destination Host', 'Deliver from IP Interface', 'Strip Header', 'Add Header', 'Encrypt and Deliver (Final Action)', 'Bounce (Final Action)', 'Deliver (Final Action)', and 'Drop (Final Action)'. On the right, the 'Quarantine' section explains that it flags messages to be held in one of the areas. It includes a dropdown menu for 'Send message to quarantine' set to 'Policy'. Below this, there is a checkbox for 'Duplicate message' with a descriptive note: 'Send a copy of the message to the specified area. The original message will continue processing the original message actions will apply to the original message.'

Quarantine
Strip Attachment by Content
Strip Attachment by File Info
Add Disclaimer Text
Bypass Outbreak Filter Scanning
Send Copy (Bcc:)
Notify
Change Recipient to
Send to Alternate Destination Host
Deliver from IP Interface
Strip Header
Add Header
Encrypt and Deliver (Final Action)
Bounce (Final Action)
Deliver (Final Action)
Drop (Final Action)

Quarantine

Flags the message to be held in one of the areas.

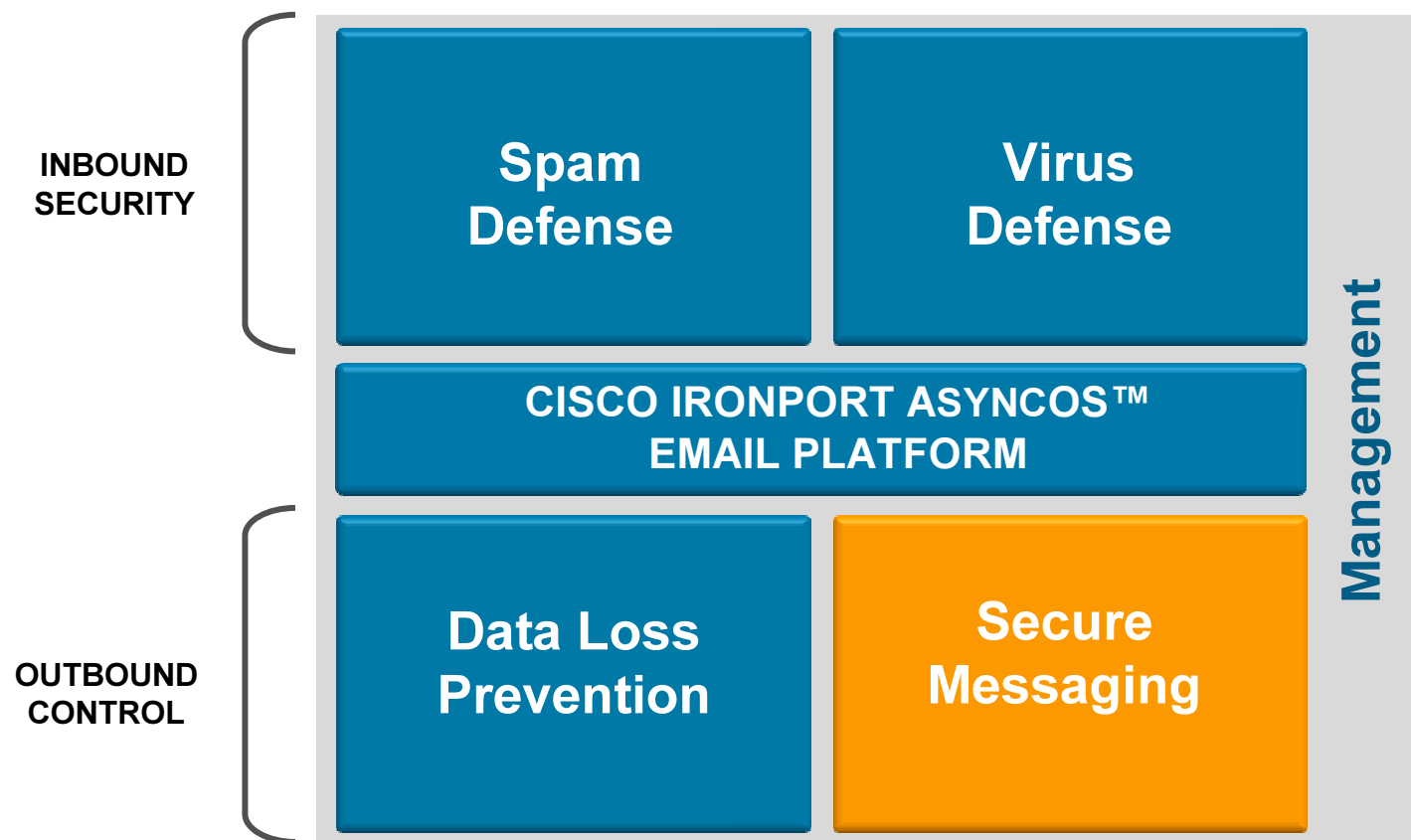
Send message to quarantine: Policy ▼

☐ Duplicate message

Send a copy of the message to the specified area. The original message will continue processing the original message actions will apply to the original message.

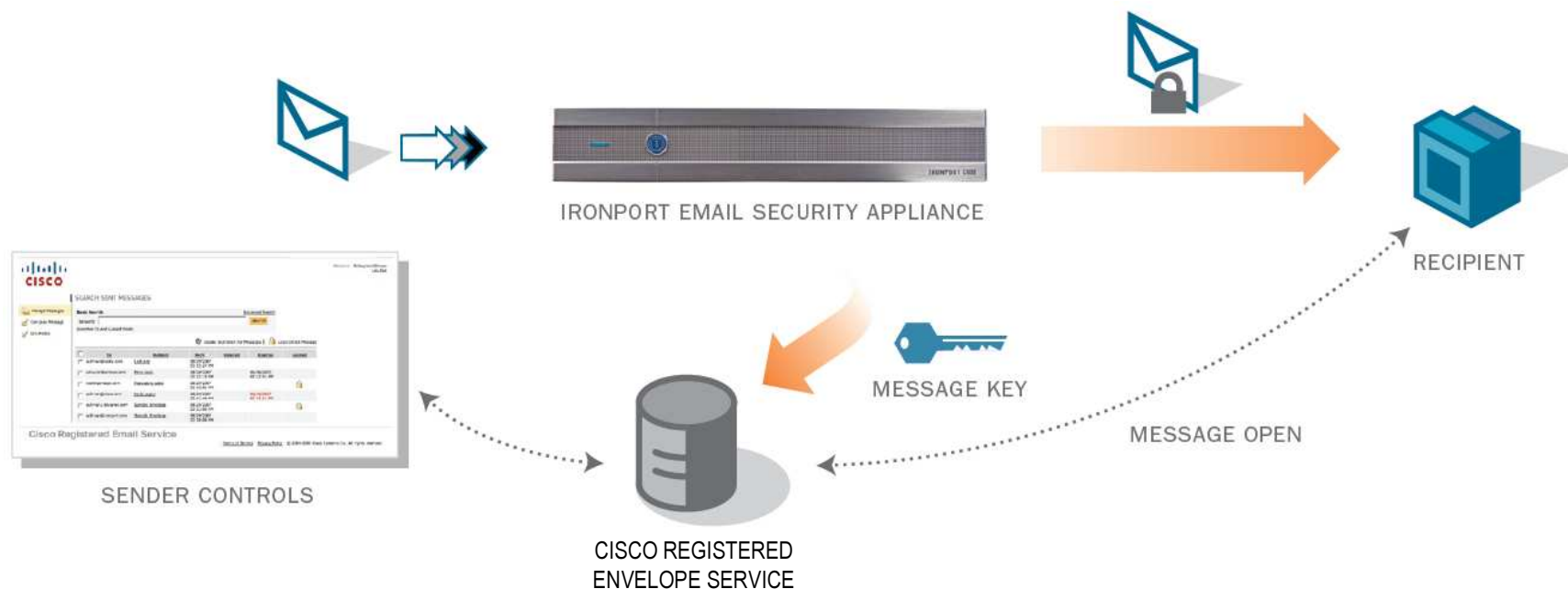
Email Security Architecture

Inbound Security, Outbound Control



Cisco IronPort Email Encryption

Easy for the Sender. . .

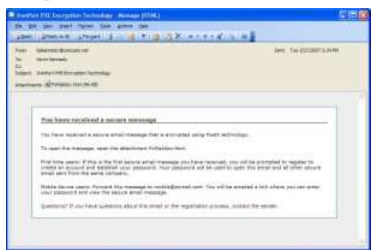


- Automated key management
- No desktop software requirements
- Send to any email address seamlessly

Cisco IronPort Email Encryption

Easy for the Recipient. . .

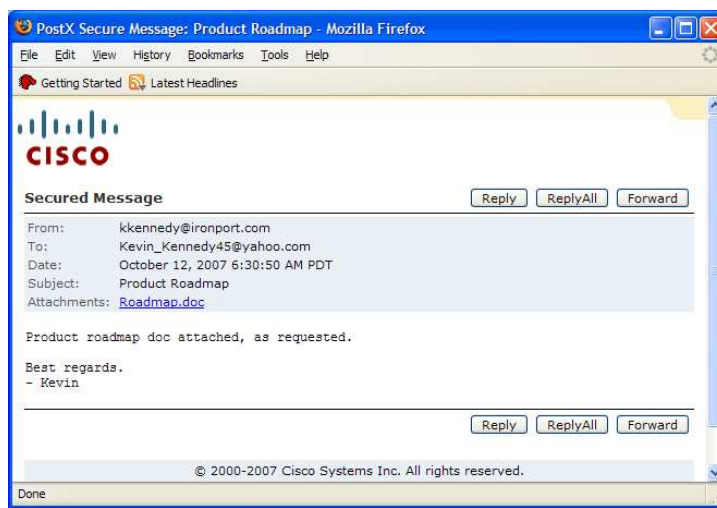
1. Open Attachment



2. Enter password



3. View message



Internet Edge Threat Mitigation

	Botnets	DDoS	Unauthorized Access	Phishing Spam	Spyware, Malware	Network Abuse	Data Leakage	Visibility	Control
Host-based IPS (CSA)	●	●	●	●	●		●	●	●
IronPort Secure Messaging				●	●	●	●	●	●
IronPort Secure Web			●			●	●	●	●
Edge Filtering		●	●					●	●
Nettflow, syslog, etc								●	
Firewall		●	●			●		●	●
IPS	●	●			●	●		●	●
VPN			●					●	●
System and Topological Redundancy	●	●							●
User/Group-based access policies			●			●		●	●

IronPort Security Appliances

Integrated Security Appliances For The Network Perimeter

- Unique Anti-spam solution, C-Series
- Integrated DLP Scanning and Remediation For Email
- Encryption Without any Additional Hardware Required
- Cisco Spam Blocker, C160, C360, C660, X1060



IronPort C-Series
EMAIL SECURITY APPLIANCE

-
- Unique Web-protection solution, S-Series
 - Acceptable Use Policy (AUP) Management
 - Industry-leading Malware and Spyware Filtering
 - S160, S360, S660



IronPort S-Series™
WEB SECURITY APPLIANCE

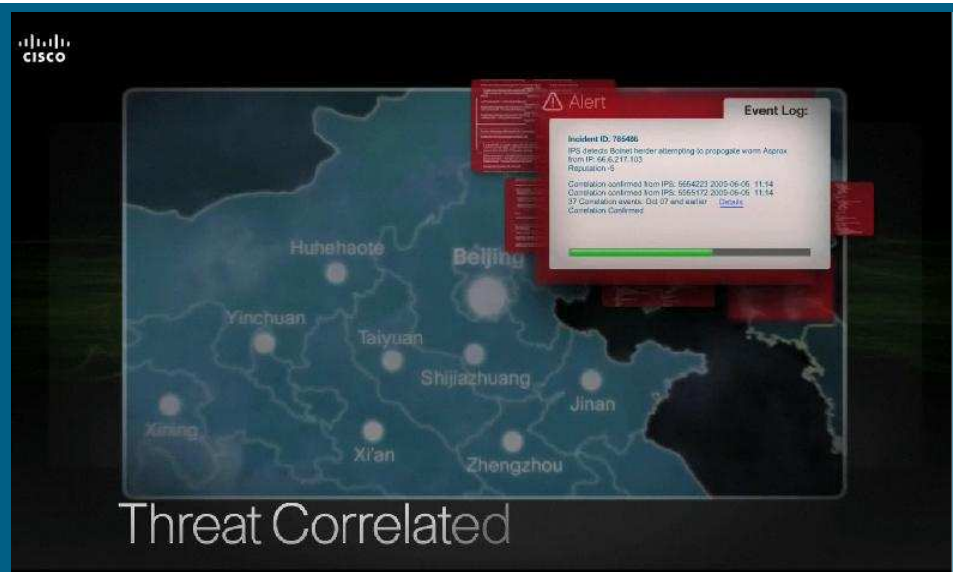
-
- Centralized Reporting
 - Centralized Tracking
 - Centralized Policy Management
 - Centralized Archiving
 - M160, M360, M1060



IronPort M-Series™
SECURITY MANAGEMENT APPLIANCE

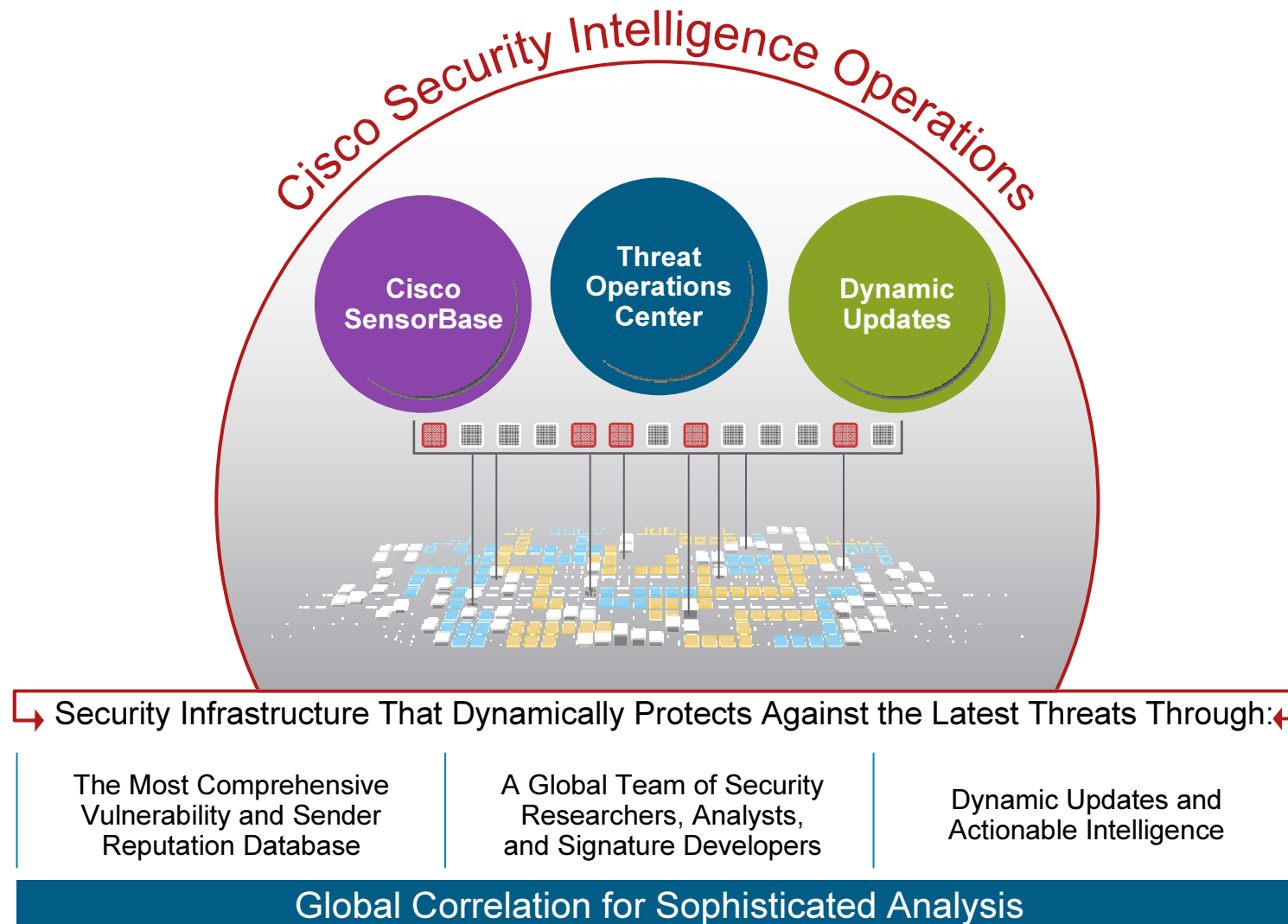


Cisco IPS New Features

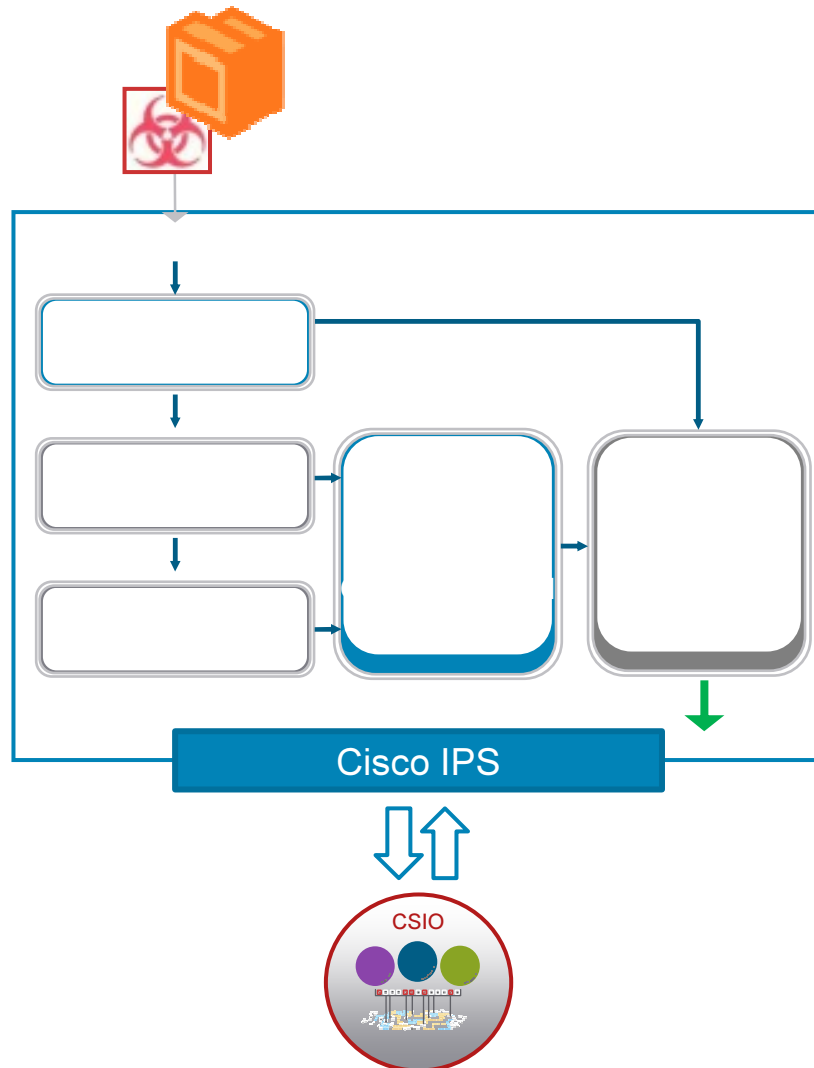


Comprehensive Threat Intelligence

Unique Threat Tracking System



Cisco IPS with Global Correlation



- **Automated operations component of Cisco SIO**
 - Automatically correlates SensorBase threat data
 - Creates sophisticated, actionable data
- **Fast response to emergent threats**
 - Enhances detection capabilities
 - Reduces the window of exposure
- **Pinpoint Accuracy**
 - Analyzes the attacker as well as the attack
 - Leverages reputation filters to stop known attackers
 - (50% of attackers are repeat offenders)

IPS Global Correlation in Action

Network IPS to Global IPS

08:00 GMT

- A sensor in Australia detects new malware
- A sensor in Russia detects a botnet issuing new commands
- A sensor in Korea detects a virus mutating
- A sensor in Florida detects a hacker probing major financial institutions



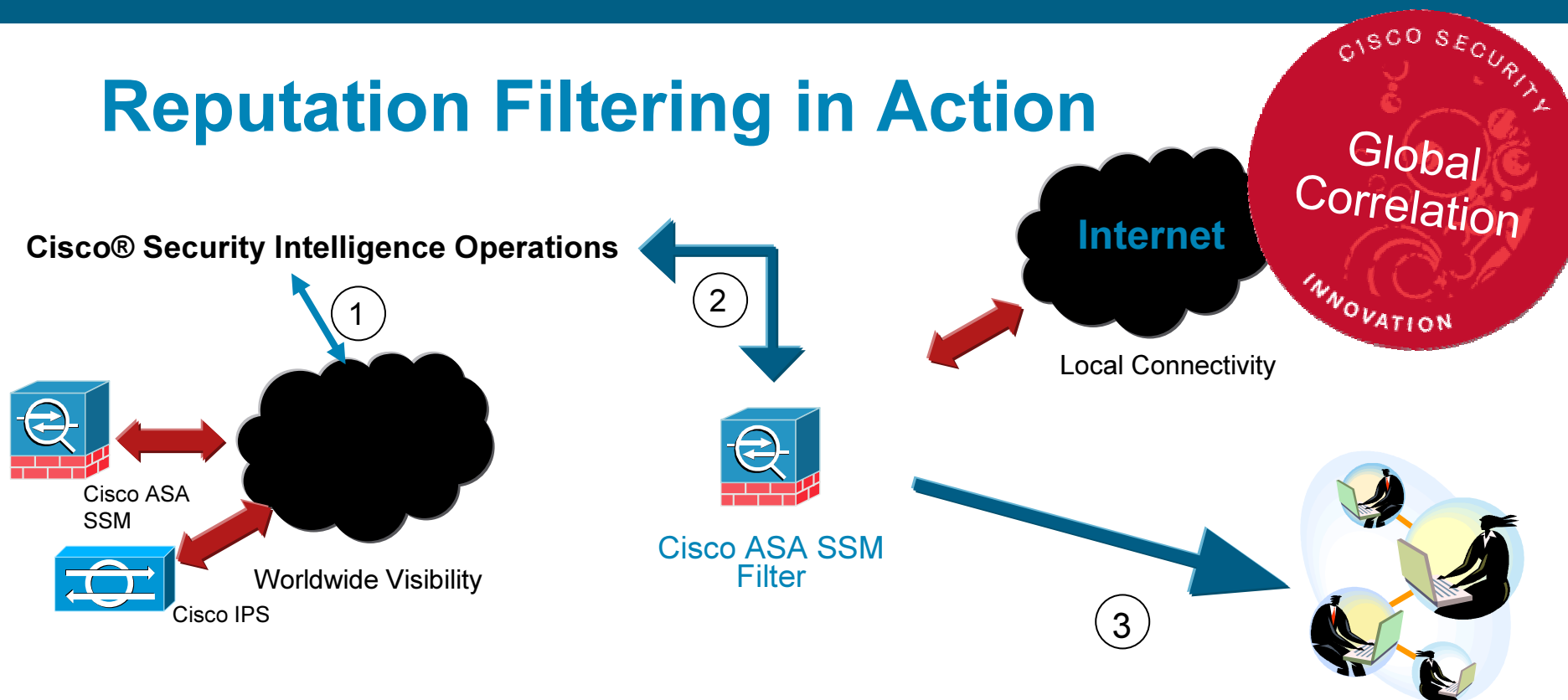
08:15 GMT

- **All Cisco® IPS customers protected**

*Fast, Complete, and Accurate
Protection Using Global IPS Data*

Cisco IPS has **twice** the IPS deployments of the next vendor, collecting billions of data points worldwide

Reputation Filtering in Action



Step 1:

The sensor base network within the Cisco SIO gathers telemetry data from other sensors across the world

Step 2:

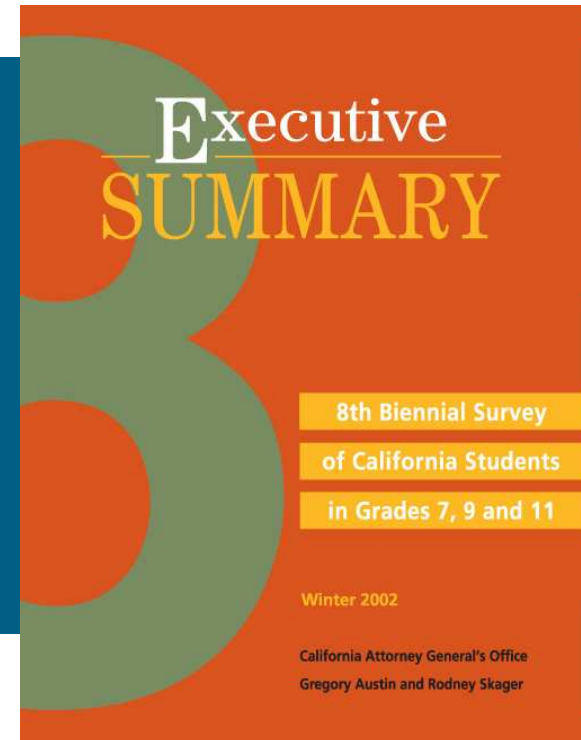
Cisco ASA SSM gets updated reputation filter list; influences policy decisions (deny or drop attacker, etc.)

Step 3:

Alerts go out to the security teams for prevention, mitigation, and remediation



Summary



SAFE Resources

- Cisco SAFE:

<http://www.cisco.com/go/safe>

- Cisco Design Zone:

<http://www.cisco.com/go/cvd>

- Cisco Security Lifecycle Services:

<http://www.cisco.com/go/services/security>

- Cisco's Security Products:

<http://www.cisco.com/go/security>



