Cisco Expo 2007

Security Update

Philippe Roggeband – Emerging Markets

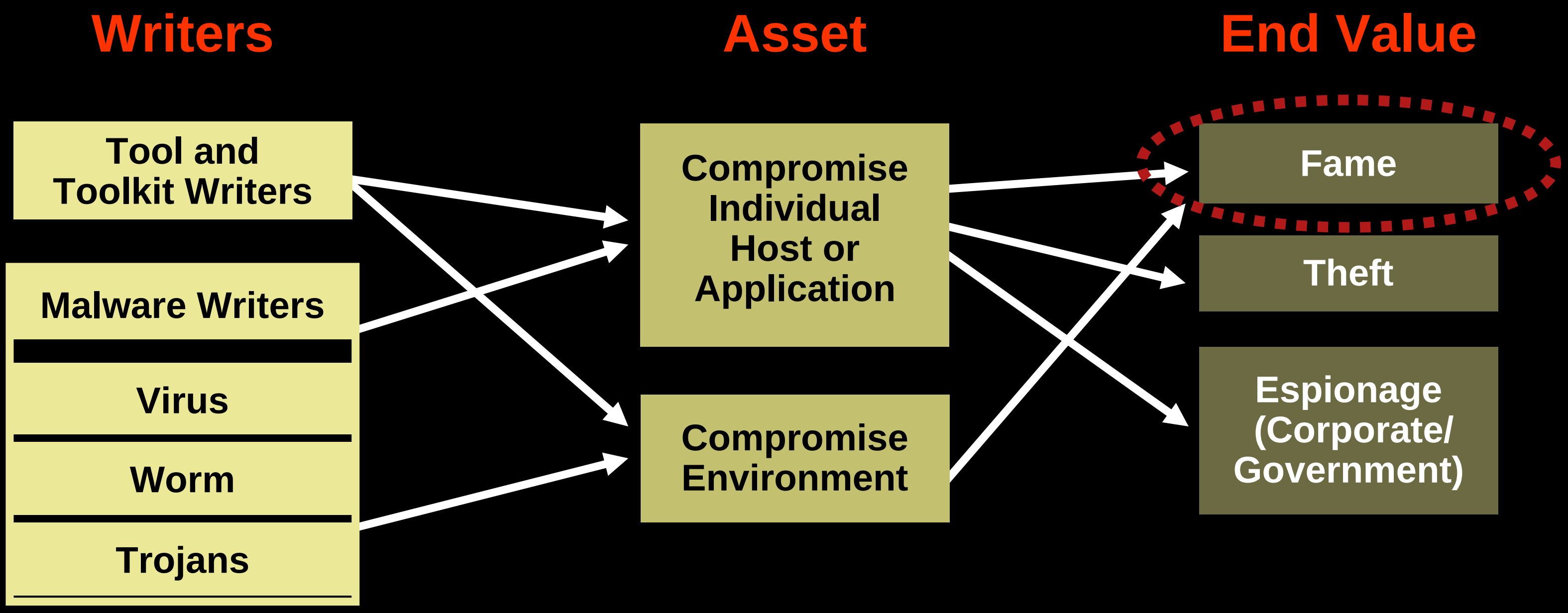
Security Product Manager

Enable Your Network
Empower Your Business

Agenda

- The threat context
- Cisco’s Self-Defending Network approach
- Product Update
- Q&A

Threat Economy: In the Past



Writers

Asset

End Value

Tool and Toolkit Writers

Malware Writers

Virus

Worm

Trojans

Compromise Individual Host or Application

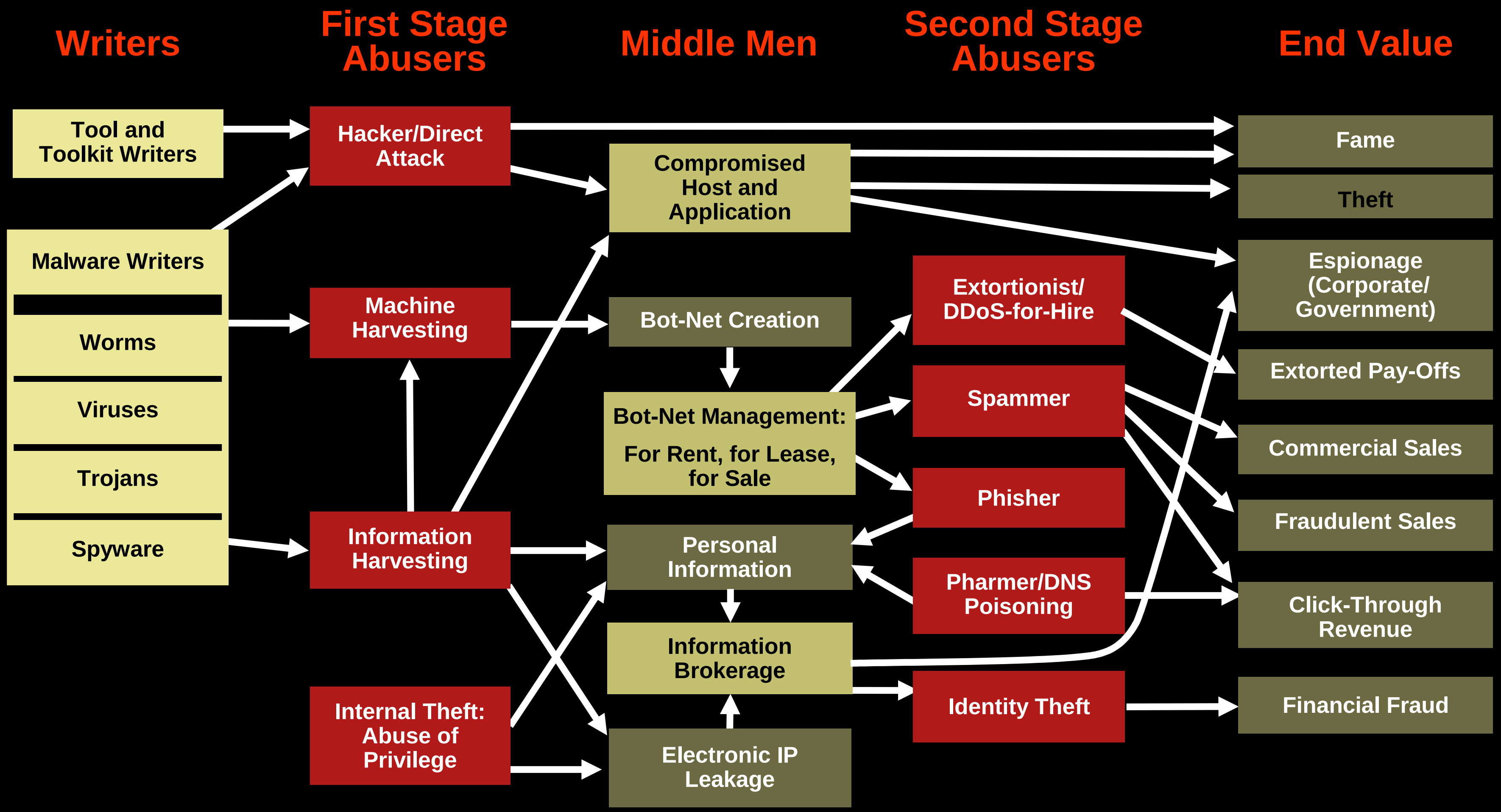
Compromise Environment

Fame

Theft

Espionage (Corporate/ Government)

Threat Economy: Today



Writers

Tool and Toolkit Writers

Malware Writers

Worms

Viruses

Trojans

Spyware

First Stage Abusers

Hacker/Direct Attack

Machine Harvesting

Information Harvesting

Internal Theft: Abuse of Privilege

Middle Men

Compromised Host and Application

Bot-Net Creation

Bot-Net Management:

For Rent, for Lease, for Sale

Personal Information

Information Brokerage

Electronic IP Leakage

Second Stage Abusers

Extortionist/ DDoS-for-Hire

Spammer

Phisher

Pharmer/DNS Poisoning

Identity Theft

End Value

Fame

Theft

Espionage (Corporate/ Government)

Extorted Pay-Offs

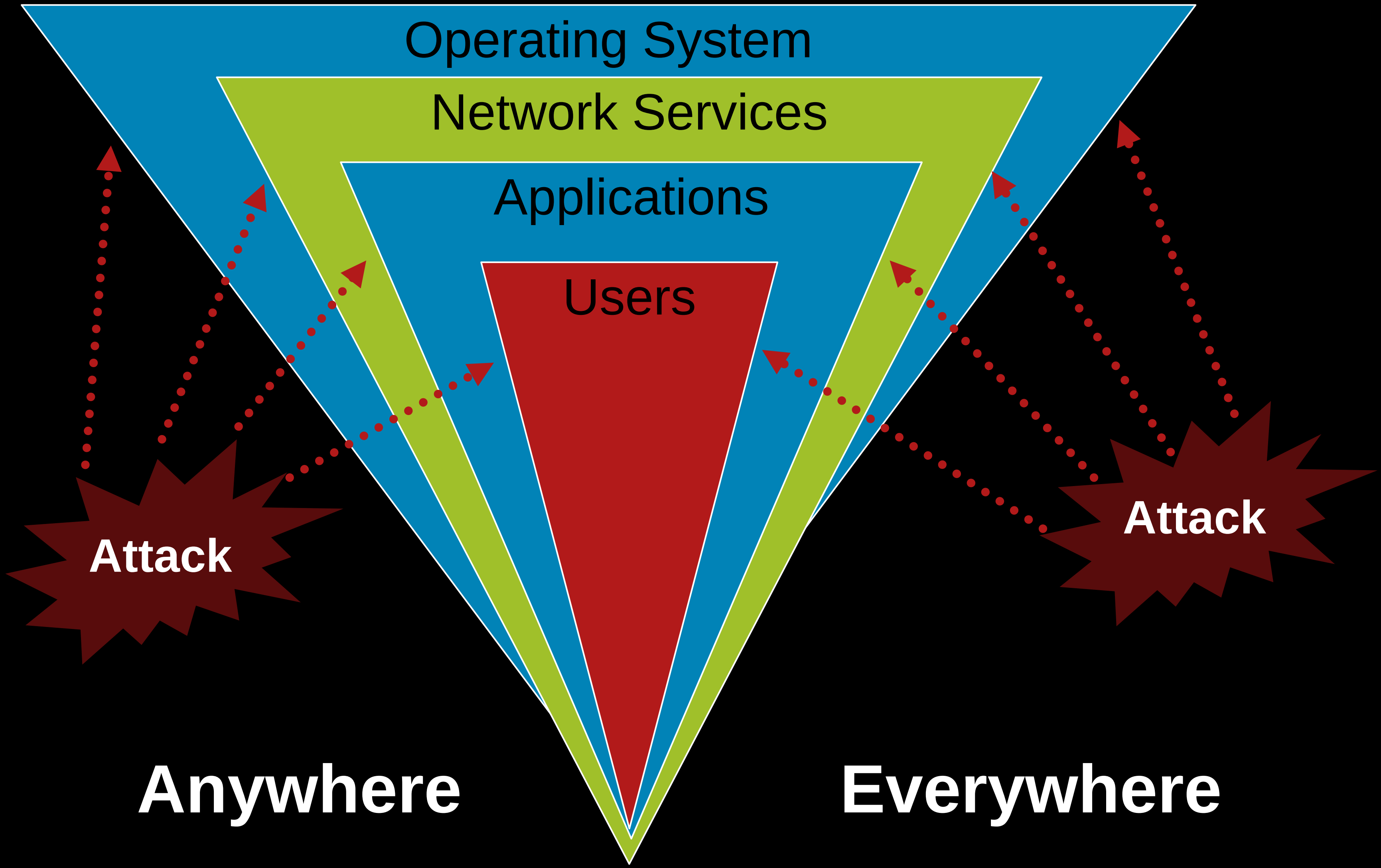
Commercial Sales

Fraudulent Sales

Click-Through Revenue

Financial Fraud

Where Can I Get Attacked?



Anywhere **Everywhere**

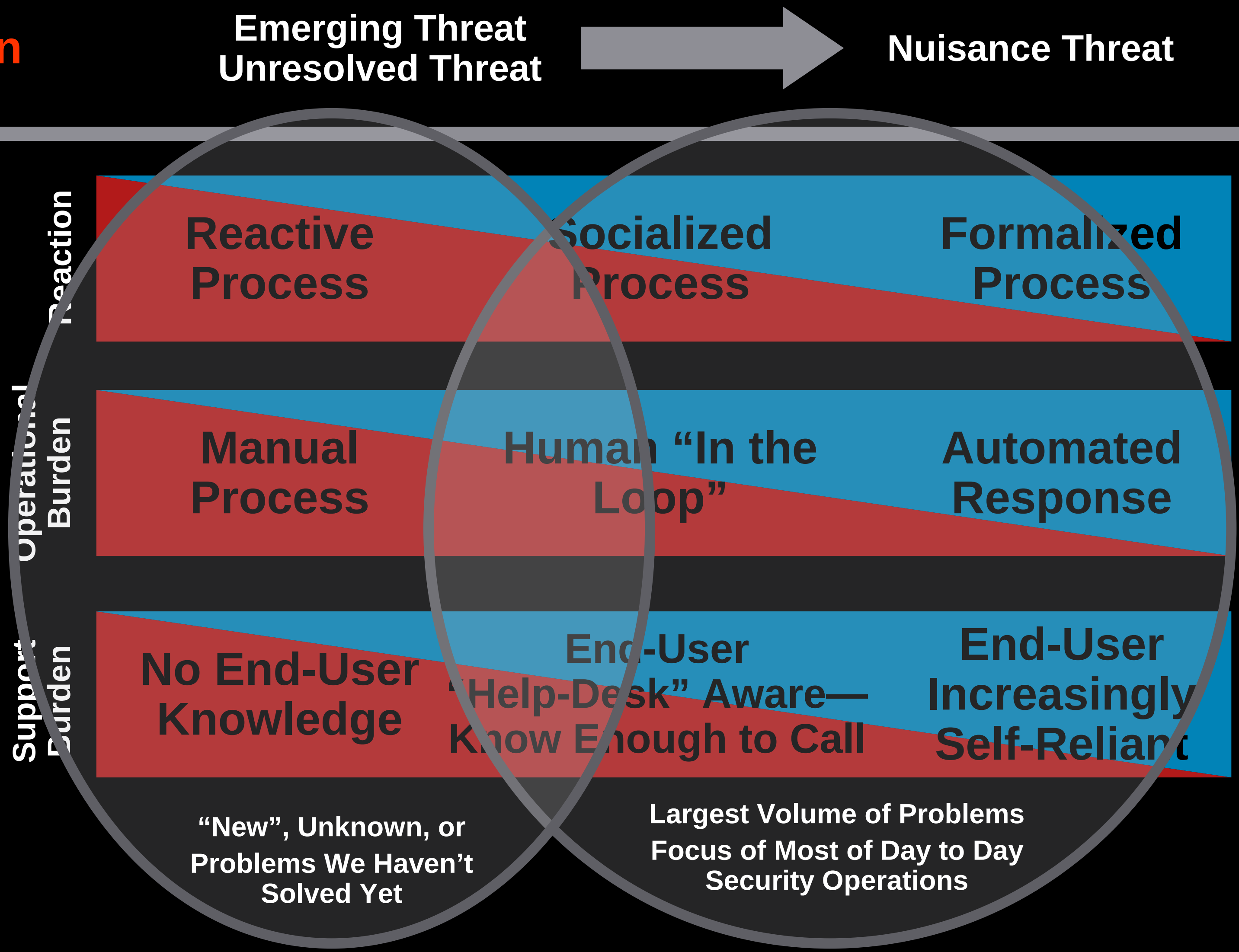
Operational Evolution of Threats

Threat Evolution

Emerging Threat
Unresolved Threat → Nuisance Threat

Policy and Process Definition	Reaction	Reactive Process	Socialized Process	Formalized Process
Mitigation Technology Evolution	Operational Burden	Manual Process	Human “In the Loop”	Automated Response
End-User Awareness	Support Burden	No End-User Knowledge	End-User “Help-Desk” Aware—Know Enough to Call	End-User Increasingly Self-Reliant

Operational Evolution of Threats



Threat Evolution	Emerging Threat Unresolved Threat		Nuisance Threat
Policy and Process Definition	Reactive Process	Socialized Process	Formalized Process
Mitigation Technology Evolution	Manual Process	Human “In the Loop”	Automated Response
End-User Awareness	No End-User Knowledge	End-User “Help-Desk” Aware—Know Enough to Call	End-User Increasingly Self-Reliant

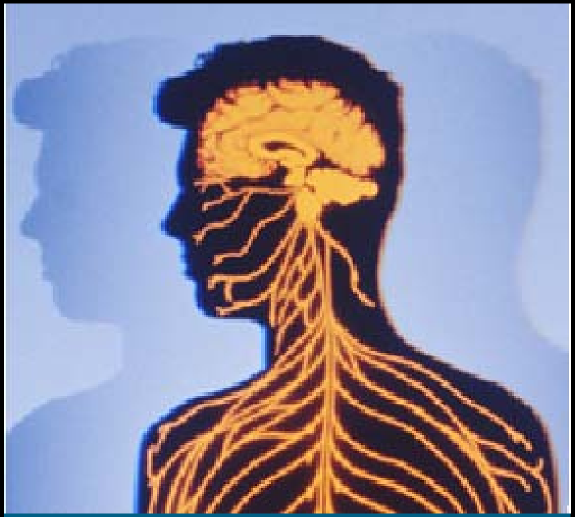
“New”, Unknown, or Problems We Haven’t Solved Yet

Largest Volume of Problems
Focus of Most of Day to Day Security Operations

Cisco’s Self-defending Network

Self-Defending Networks

Cisco's Security Strategy



Integrated

Enabling every element to be a point of defense and policy enforcement

Adaptive

Proactive security technologies that automatically prevent threats

Collaborative

Collaboration among the services and devices throughout the network to thwart attacks

Systems Approach Required

Interaktiv
Aktionen & Gewinne
News & Events
Entertainment
START STOP ENGINE
SWR3 - Live
SWR3 - SWR3 Live
00:00:56/LIVE
Track 1/1
40 KBit/s
MENU
RADIO

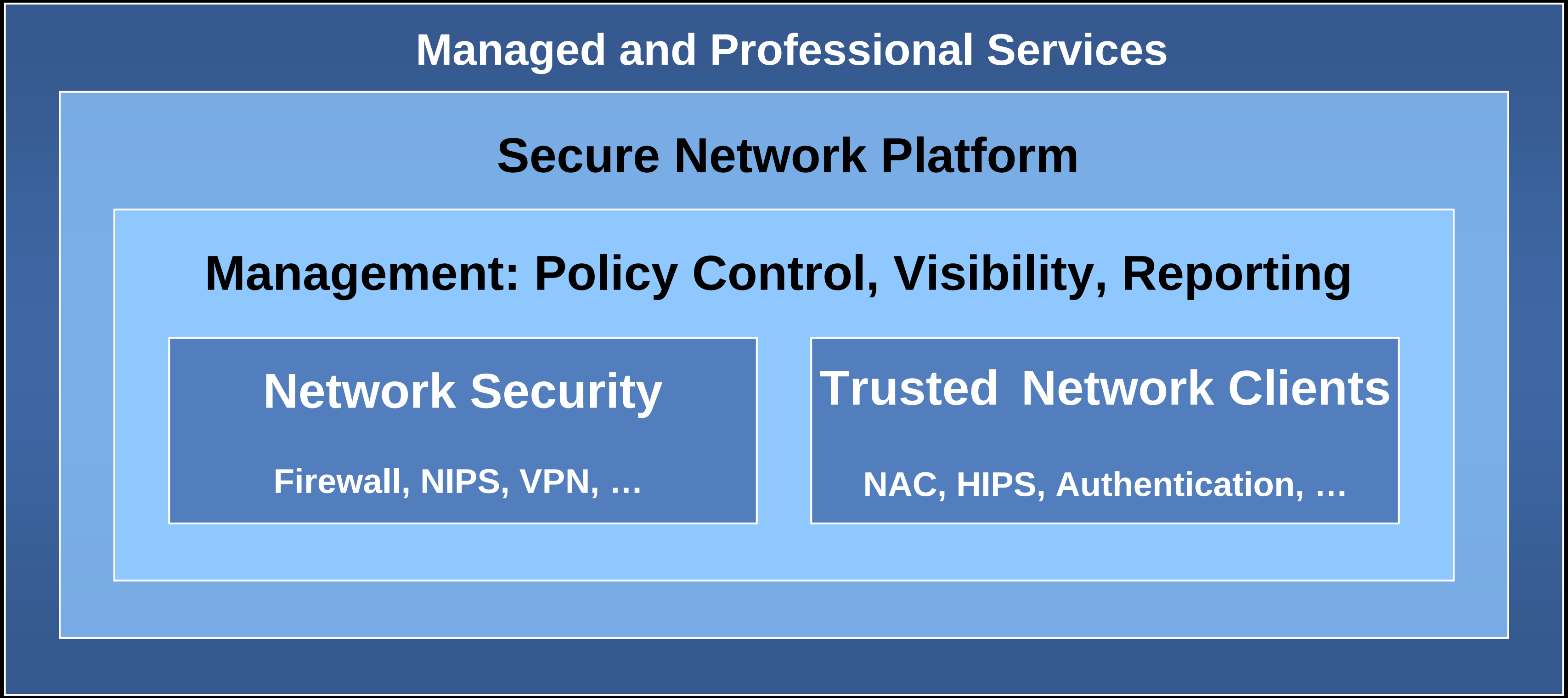
Complex | **Simple**

Impaired Usability ← Effectiveness → Easy to Use

Gaps & Inconsistencies ← Efficiency → Tightly Integrated

High Cost ← Expense → Lower TCO

To Date: Self Defending Networks



Managed and Professional Services

Secure Network Platform

Management: Policy Control, Visibility, Reporting

Network Security

Firewall, NIPS, VPN, …

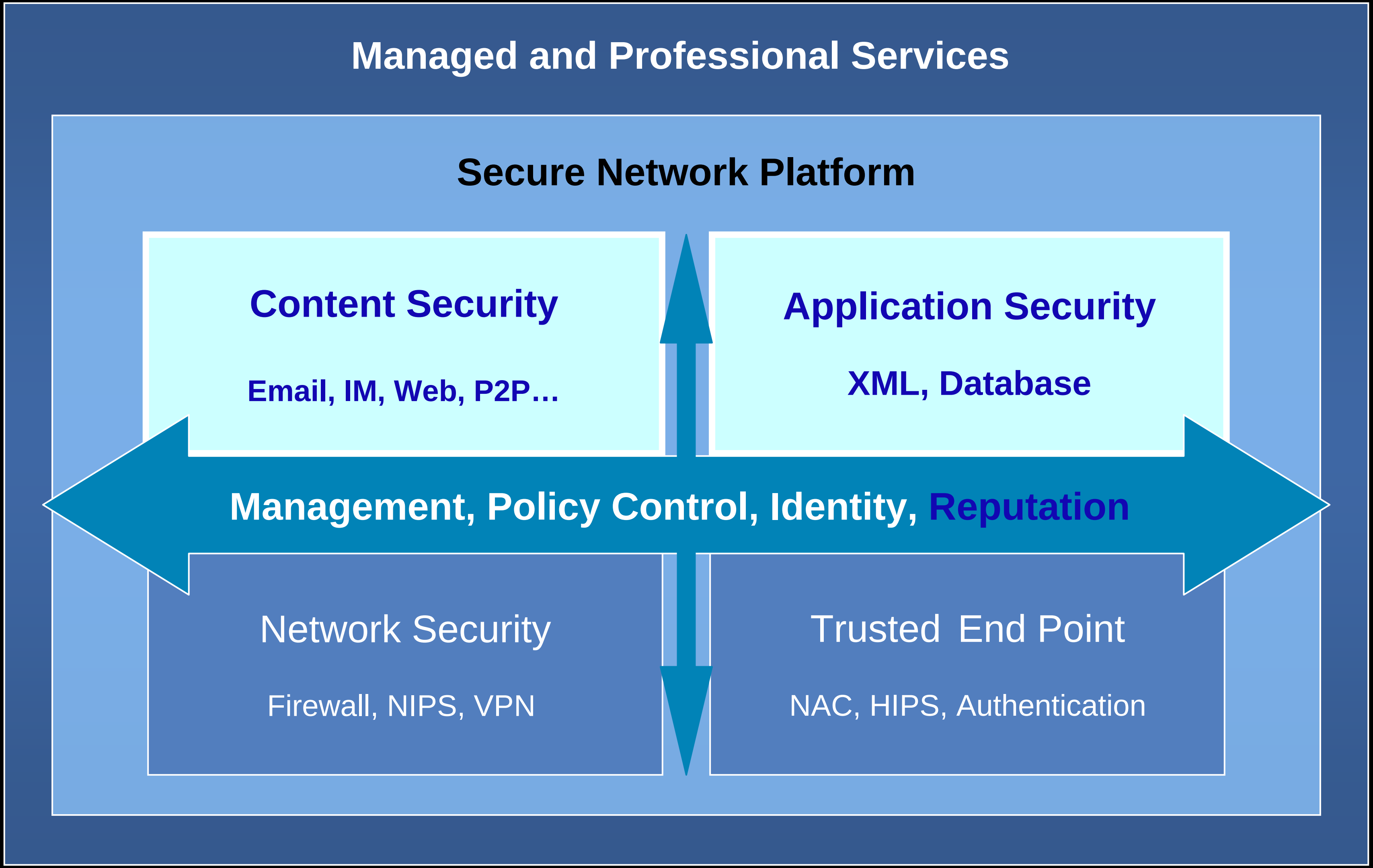
Trusted Network Clients

NAC, HIPS, Authentication, …

- Since introduction in 2003, Cisco has reached a 38% market share of a $5B available market.
- Established leadership in HW/SW NAC, VPN, Firewall, and IPS Markets
- Proof point for the value of Collaborative and End-to-End network based solutions

Self Defending Networks 3.0

Framework for Deeper and Wider Security Solutions



Managed and Professional Services

Secure Network Platform

Content Security

Email, IM, Web, P2P…

Application Security

XML, Database

Management, Policy Control, Identity, Reputation

Network Security

Firewall, NIPS, VPN

Trusted End Point

NAC, HIPS, Authentication

Security Product Update

What happened since the last Expo ?

- Threat Control & Containement Launch
- Ironport Acquisition
- Empowered Branch 3.0 Launch

Threat Control & Containement

360º Visibility and Protection

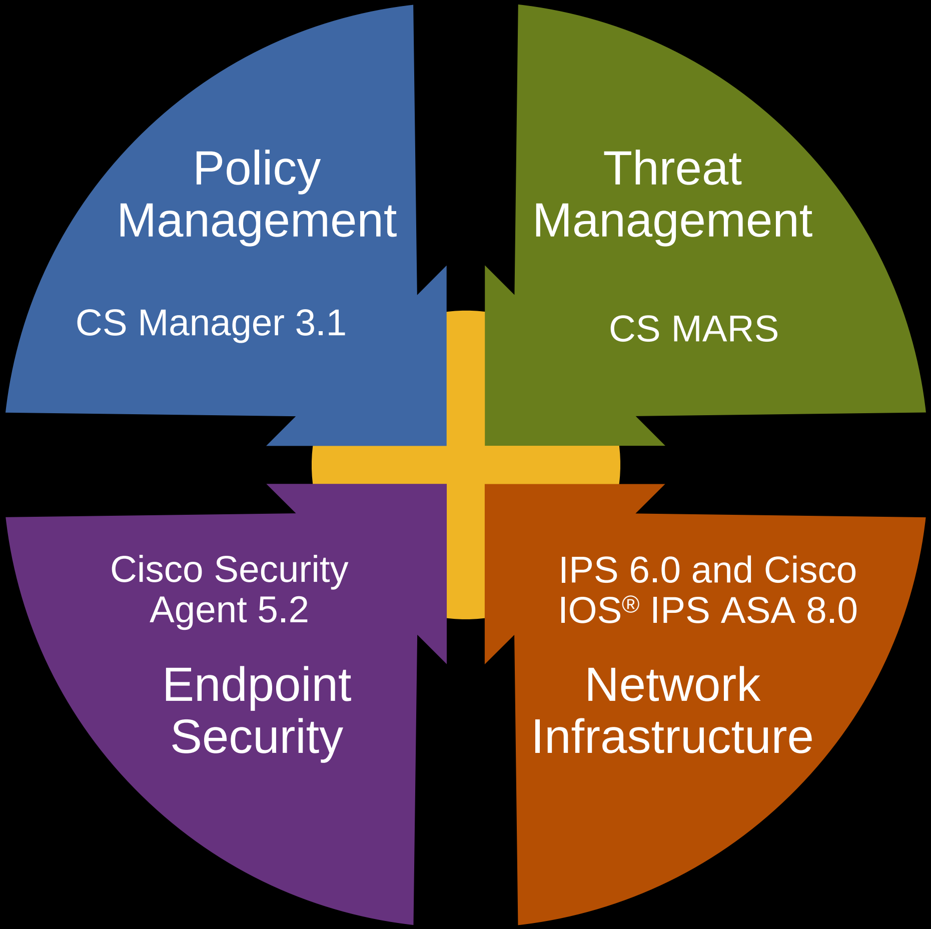
Delivering Comprehensive and Proactive Network Defense

Simplified Control

Streamlining Policy and Threat Management Across the Network

Business Resiliency

Ensuring the Enterprise's Operations



Launch Highlights

Threat Visibility Infrastructure-wide Threat Intelligence and Threat Correlation, and Collaboration Across Systems and Endpoints	IPS 6.0
Proactive Protection and Resource Access Real-Time Threat Prevention and Mitigation, Enhanced Admission Control	CS-Manager 3.1
SSL VPN Advancements To Decrease TCO, Streamline Management, and Control User Resource Access on the Flagship Cisco ASA 5500 SSL/IPSec VPN Edition	ASA 8.0
Reduced Time to Respond Enhanced Threat Visibility: Reporting and Correlation, Simplifying Threat Detection and Risk Analysis	CSA 5.2

Innovations in Intrusion Prevention

Enhancements in IPS 6.0

- Integrated

  Multivector protections across the product portfolio in the network, desktop, and server endpoints

  Visibility into endpoint context through passive OS fingerprinting

  Static OS mapping to include environment specific OS assignments

  Database protection

  Insight into user and endpoint credentials

- Collaborative

  Increased contextual analysis of endpoint

  Ability to use CSA inputs to influence IPS actions

- Adaptive

  Day zero anomaly detection

  Dynamic risk rating adjustment based on attack relevance

  Automated event and action filtering based on OS match

- Hardware platforms: All IPS4200 Sensors, ASA5500 Series AIP modules, Cisco Access Router NM-CIDS modules, and Cisco Catalyst® IDSM-2 modules

CSA 5.2 Highlights

Collaborative Security Enhances Threat Control

CSA Establishes Endpoint-Network Relationship
Which Enhances Total Network Security

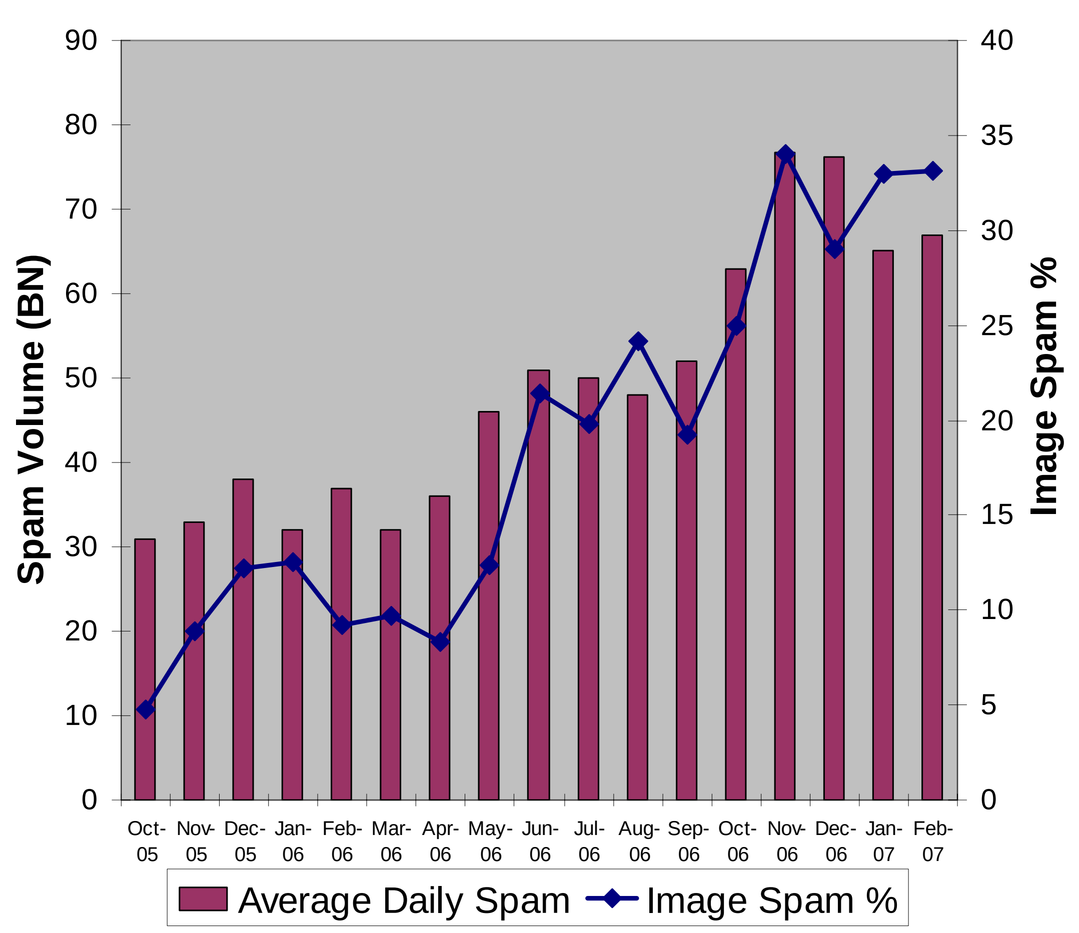
- Application- and user-based QoS tagging
- QoS and wireless policy controls provide Wi-Fi optimization and security
- Data protection capabilities provide flexible policy control
- CSA and IPS: Real-time information sharing providing improved signature fidelity

What happened since the last Expo ?

- Threat Control & Containement Launch
- Ironport Acquisition
- Empowered Branch 3.0 Launch

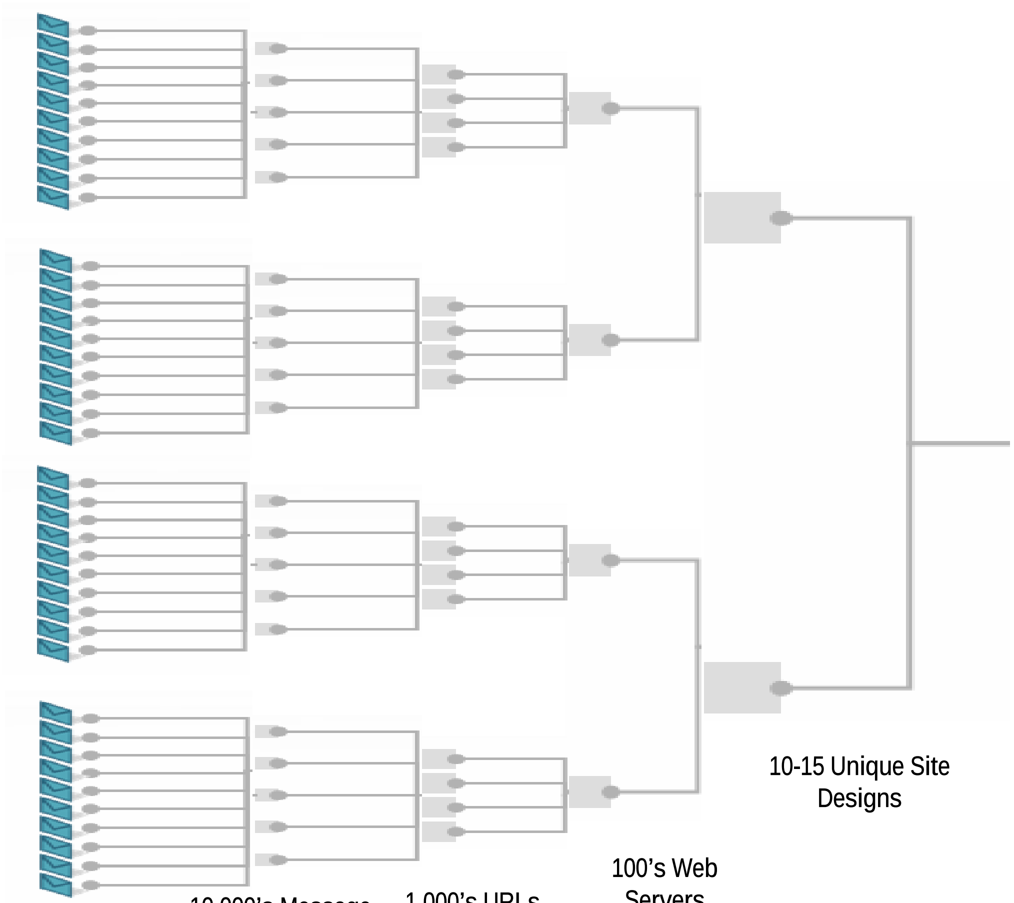
Spam Trends

Through Mid-February, 2007



- Spam volumes up 109% year-over year
- Image spam % up to 33.1%, highest level of all time
- Spam creeping upward after lull in January 2007

Identifying the Command & Control



One Support Website

One Pharmacy

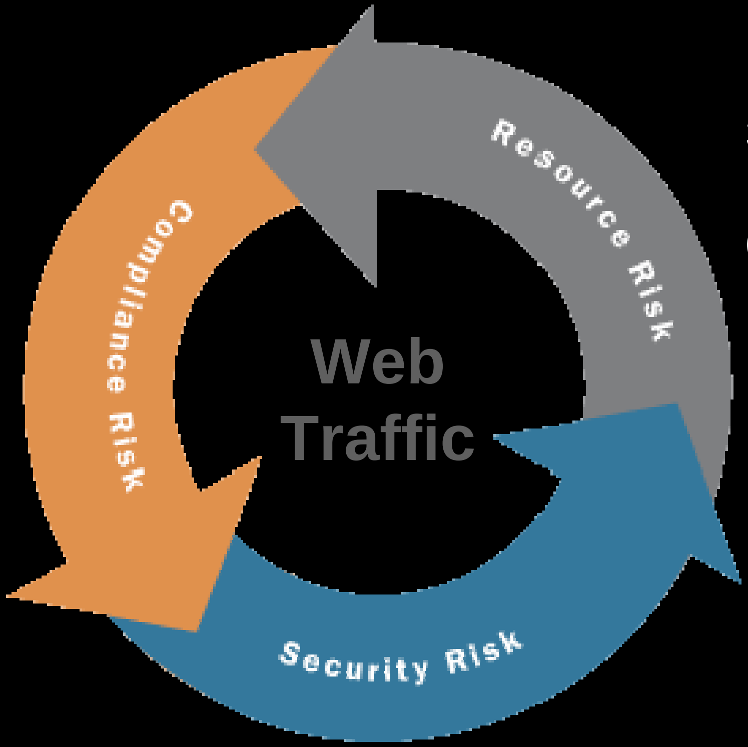
One Merchant Account

Web Traffic: Clear & Present Risks

The Circle of Risk

Malware &

AUP violations



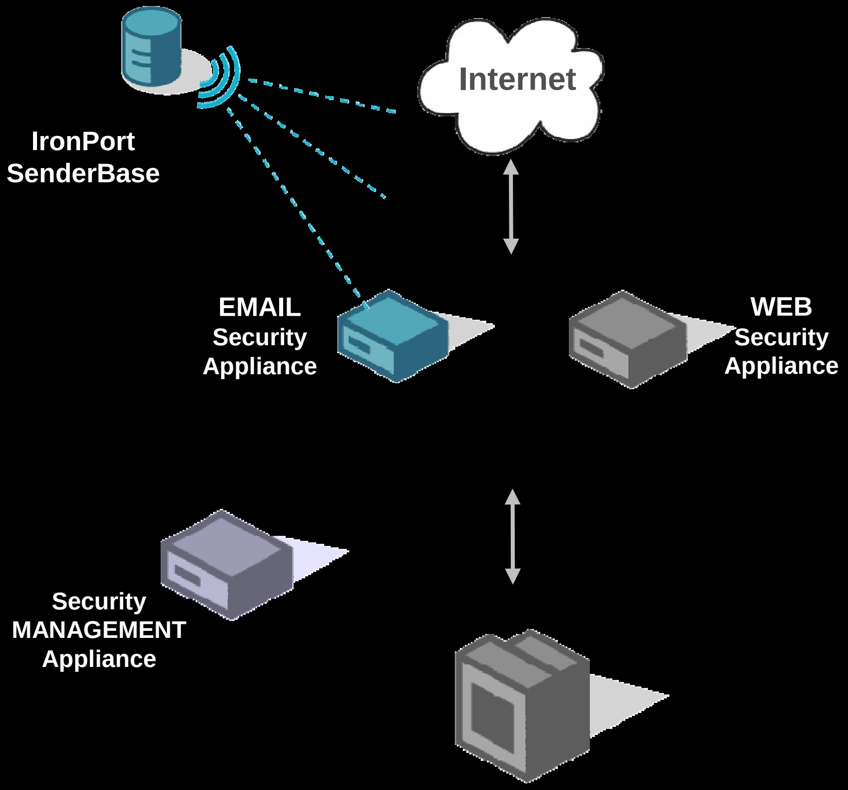
35-40% of Web usage is non-business related

(Source: IDC Research)

75%+ of enterprises infected with spyware & malware

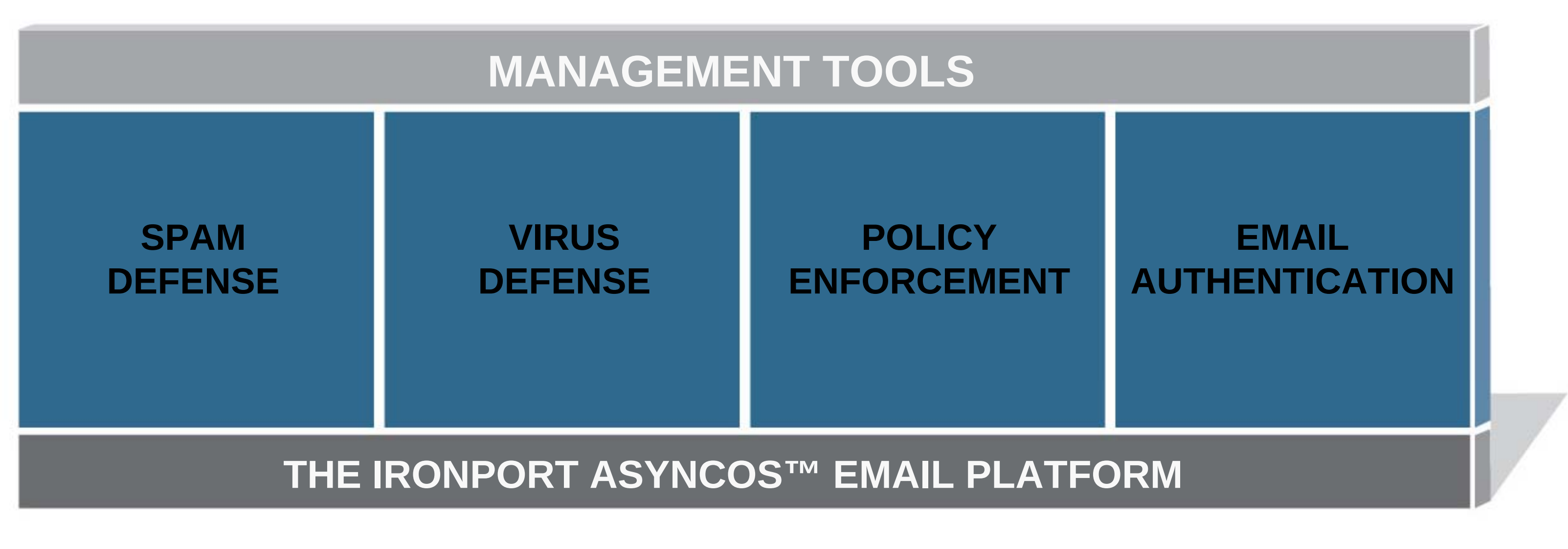
(Source: IDC Research)

IronPort Perimeter Security Appliances



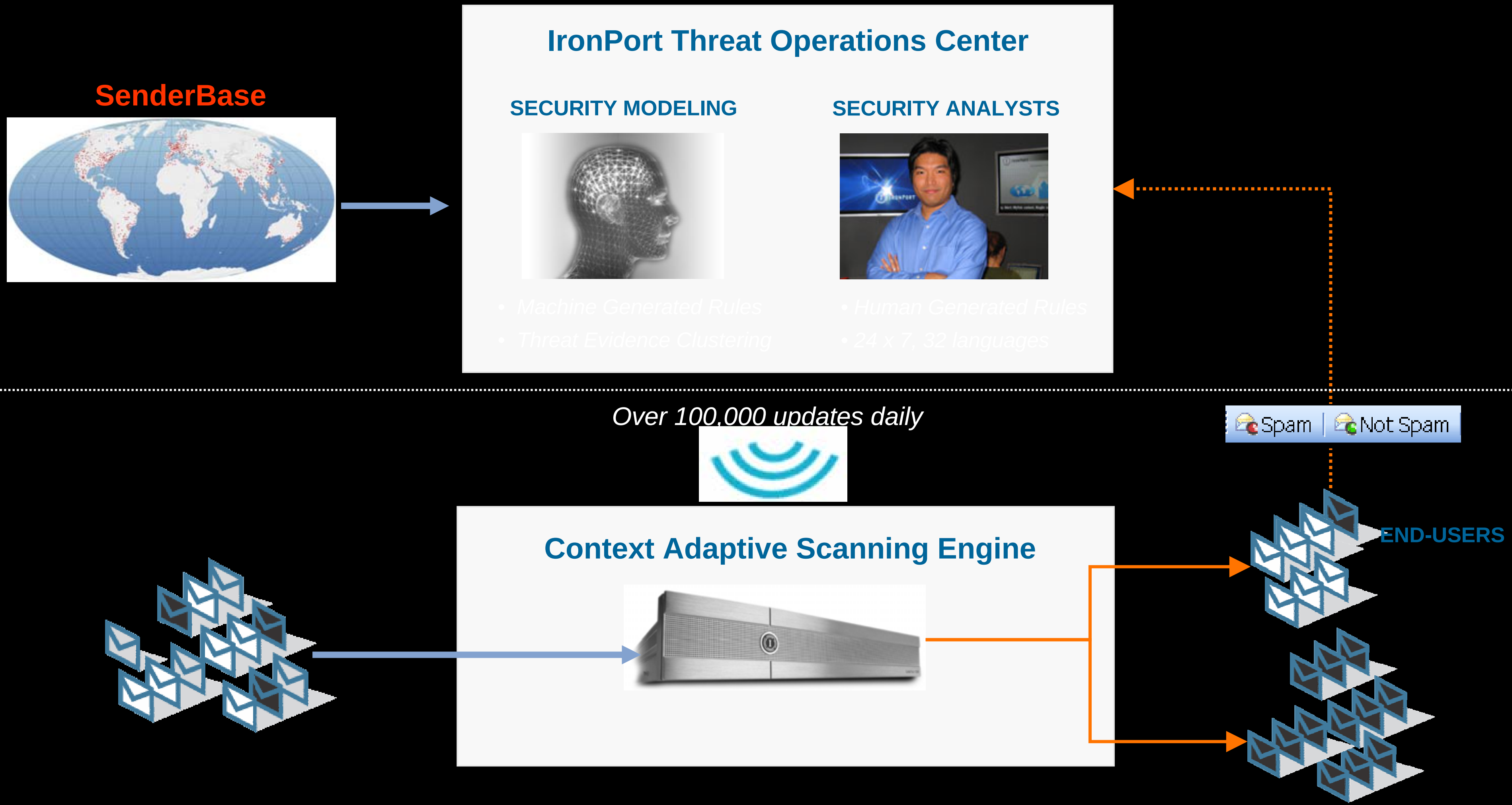
Web Security | Email Security | Security management

IronPort Architecture for Multi-Layered Email Security



IronPort Anti-Spam

Backed By The Industry’s Most Advanced Infrastructure



SenderBase

IronPort Threat Operations Center

SECURITY MODELING

- Machine Generated Rules
- Threat Evidence Clustering

SECURITY ANALYSTS

- Human Generated Rules
- 24 x 7, 32 languages

Over 100,000 updates daily

END-USERS

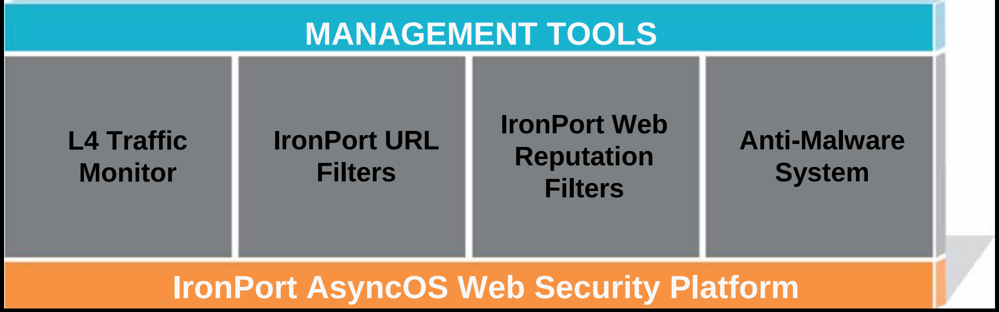
Context Adaptive Scanning Engine

IronPort S-Series

Next Generation Web Security Platform

- L4 traffic monitor inspects all traffic
- Web reputation for preventive filtering
- Integrated complete content inspection
- Acceptable Use URL filtering for corporate policy

IronPort S650/S350



Ironport SenderBase® Reputation Network

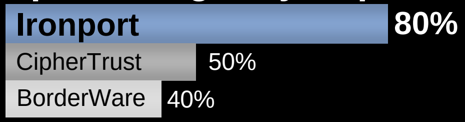
Global Reach Yields Benchmark Accuracy

The Dominant Force in Global Email and Web Traffic Monitoring…

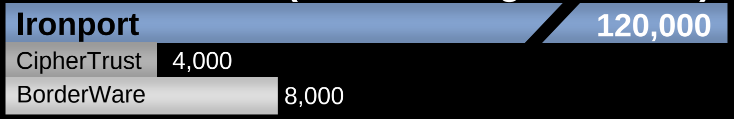
- **5B+** queries daily
- **150+** Email and Web parameters
- **>25%** of the World’s Email Traffic

…Results in Accuracy and Advanced Protection

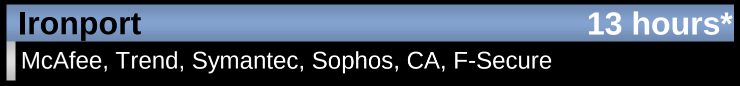
Spam Caught by Reputation



Network Reach (Contributing Networks)



Virus Protection Lead

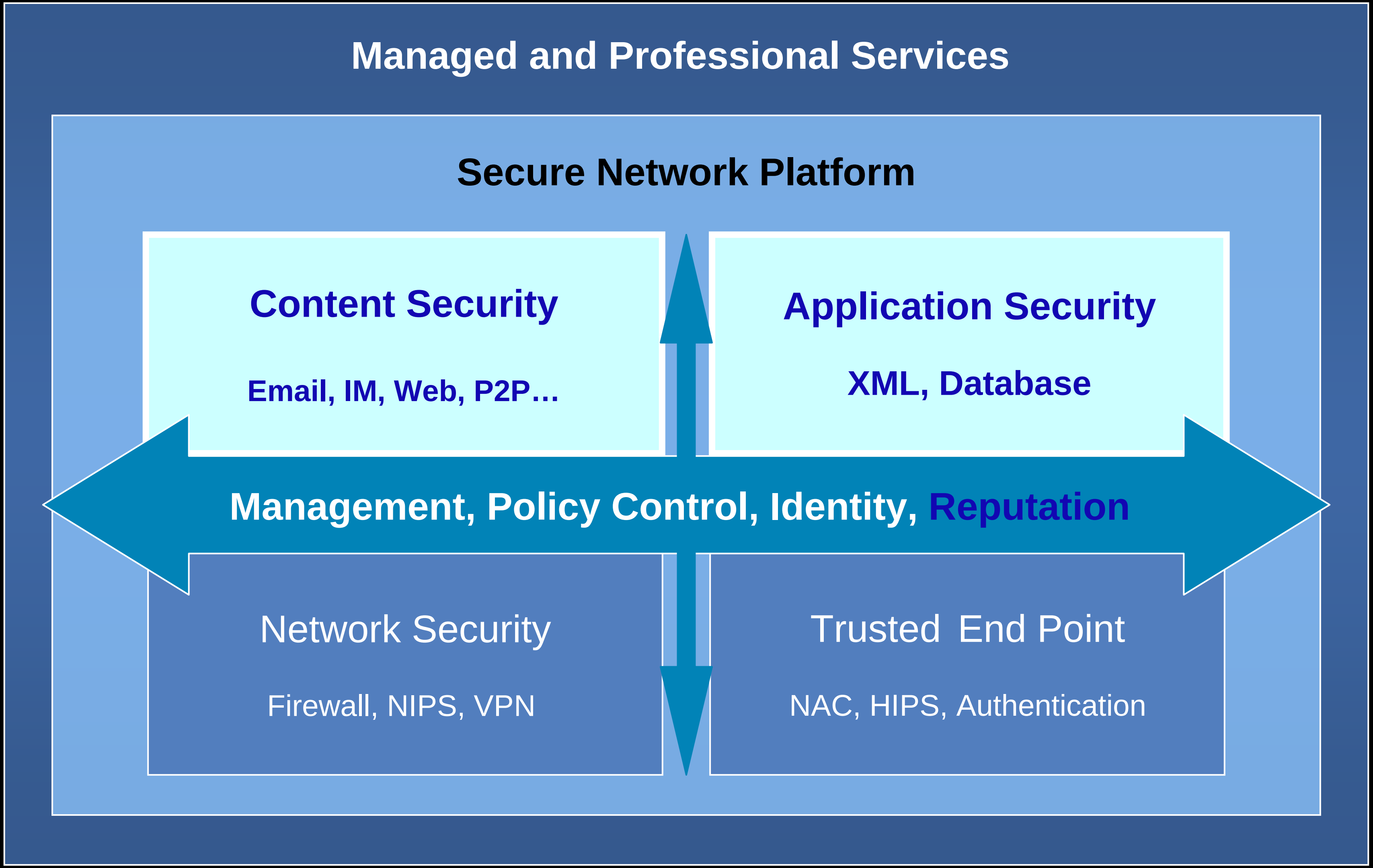


* 6/2005 – 6/2006. 175 outbreaks identified. Calculated as publicly published signatures from the listed vendors.

Source: www.ciphertrust.com and www.borderware.com, August 6, 2006

Self Defending Networks 3.0

Framework for Deeper and Wider Security Solutions



Managed and Professional Services

Secure Network Platform

Content Security

Email, IM, Web, P2P…

Application Security

XML, Database

Management, Policy Control, Identity, Reputation

Network Security

Firewall, NIPS, VPN

Trusted End Point

NAC, HIPS, Authentication

What happened since the last Expo ?

- Threat Control & Containement Launch
- Ironport Acquisition
- Empowered Branch 3.0 Launch

Empowered Branch 3 Launch

Unified Network Services
Integrated Security
Routing
Switching
Management
Mobility
Application Intelligence

- Routing and Switching:
  - Cisco 1861 Integrated Services Router
  - Cisco Catalyst 2960 switches with LAN Lite
  - Stacking capabilities between Etherswitch StackWise module on Cisco ISR and Catalyst 3750/-E switches
  - Unified Network Services:
- Unified Messaging Gateway
  - Cisco Unity Express 3.1 with Interactive Voice Response
  - Cisco Unified Call Manager Express 4.2 with Contact Center features
  - Survivable Remote Site Telephony with E911,
- **Integrated Security:**
  - NAC Network Module for Cisco Integrated Service Router
  - Intrusion Prevention Module (IPS AIM) for IPS Acceleration
- Application Intelligence:
  - Performance Routing (PfR) for Application-based Route Optimization;
  - New higher capacity WAAS Network Module; Digital Media Gateway Network Module
- Mobility:
  - 802.11 n on Wireless LAN Controller Module for Cisco Integrated Services Router

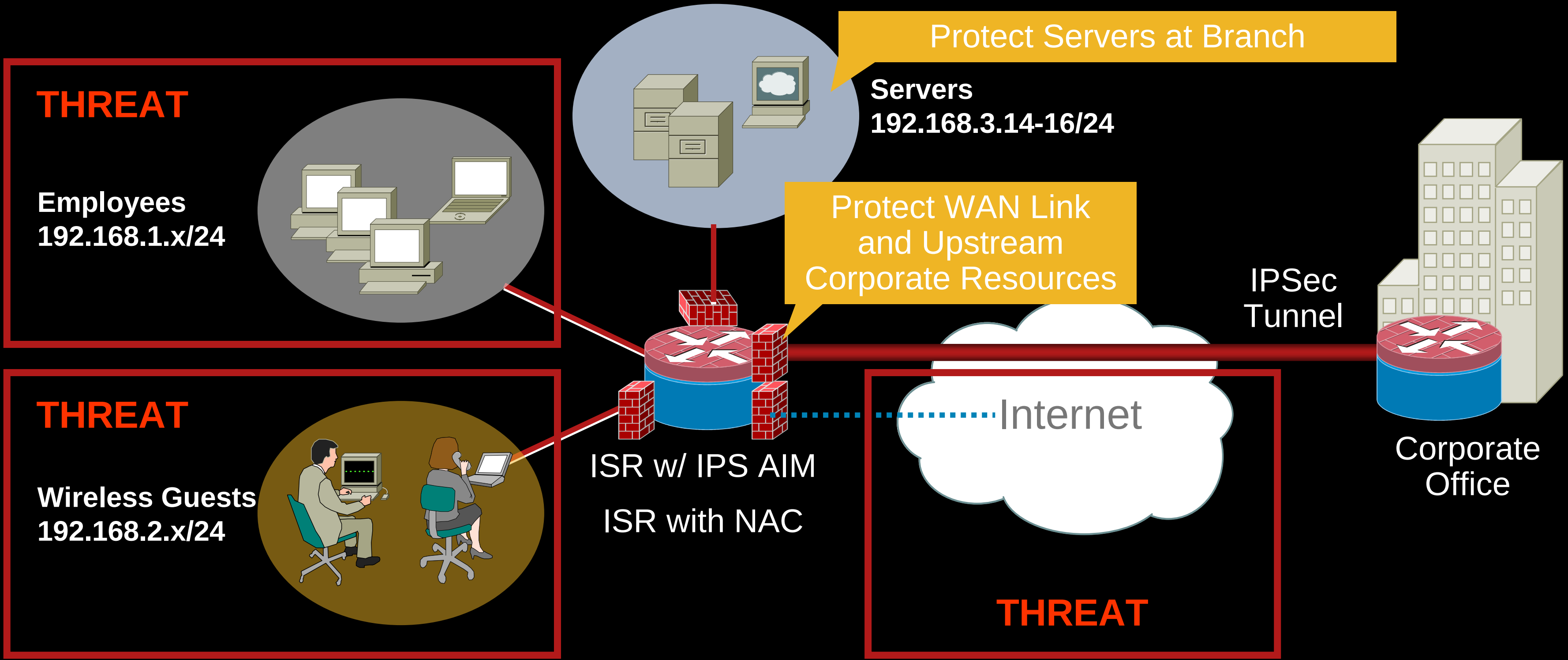
Branch Needs for Self Defending Network

Trends

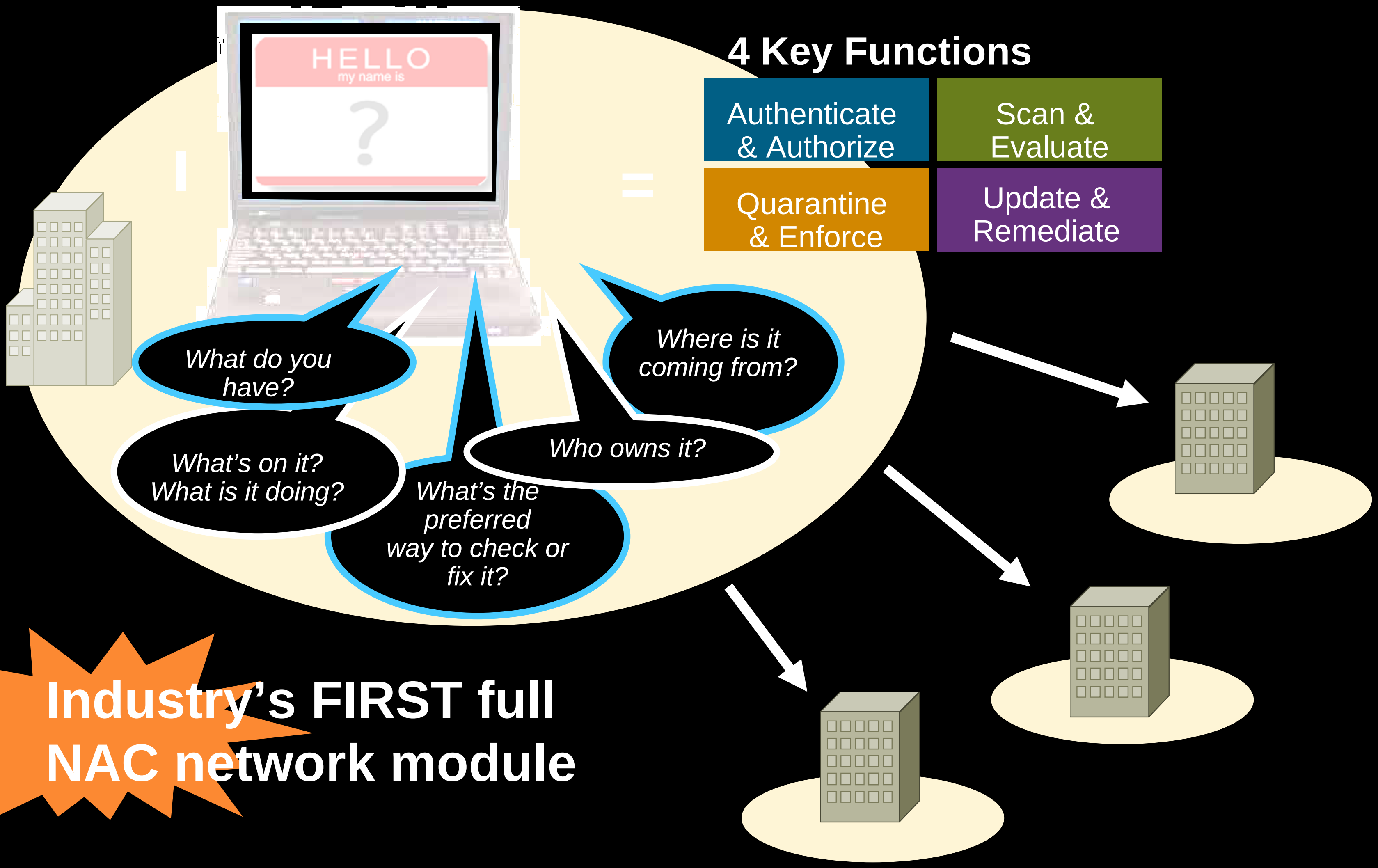
- PCI Compliance (Retail); HIPAA (Healthcare); Sarbanes-Oxley/GLBA (Finance)
- Prone to attacks from split tunnels, contaminated laptops and rogue APs

Security

- Moves protection to the edge before threats enter corporate or SP network
- Helps to Manage Unmanaged Devices



Extending NAC with Cisco ISR Network Module

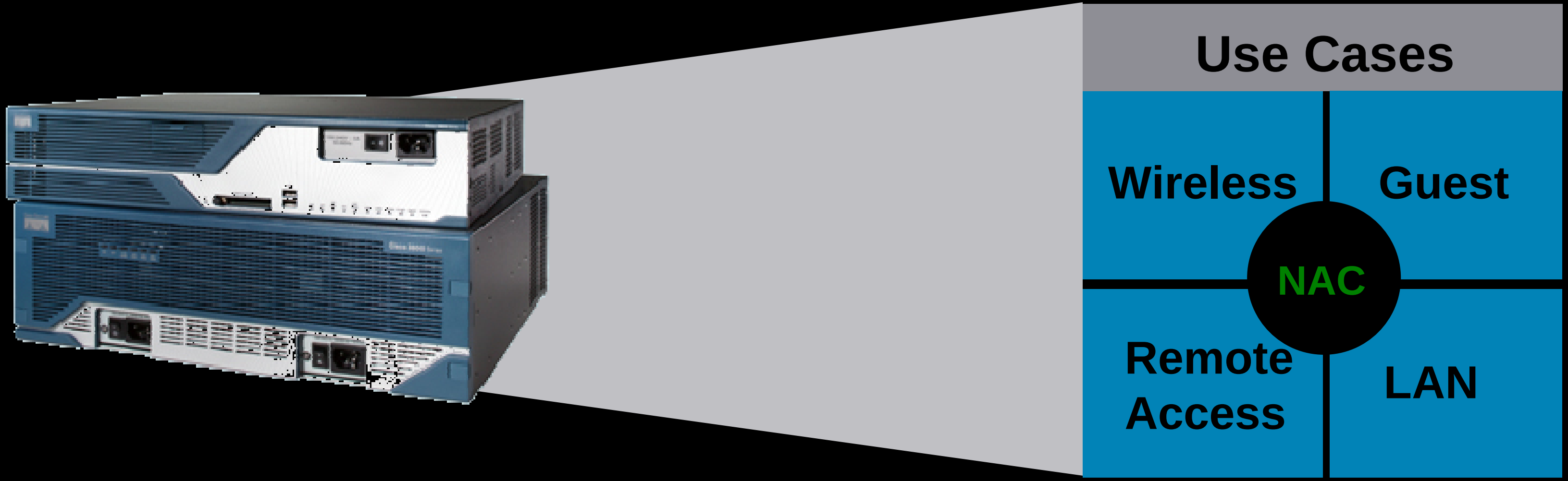

HELLO
my name is
?
What do you have?
What's on it? What is it doing?
What's the preferred way to check or fix it?
Who owns it?
Where is it coming from?

4 Key Functions

Authenticate & Authorize	Scan & Evaluate
Quarantine & Enforce	Update & Remediate

Industry's FIRST full NAC network module

NAC Network Module on Cisco ISR



BENEFITS:

Pervasive Security

One product for all use cases and locations

Consistent Policy

One policy store for consistent application across entire organization

Seamless Deployment

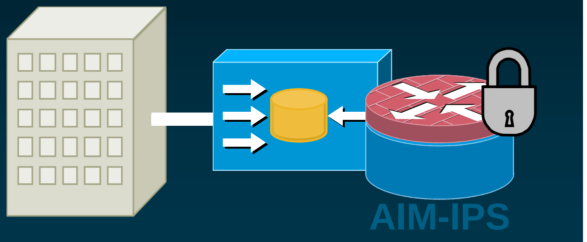
Integrated in the router for easier deployment, troubleshooting, and management

Intrusion Prevention System (IPS) Advanced Integration Module

AIM-IPS-K9

[redacted]
2007

For Cisco 1841,
Cisco 2800, Cisco 3800
Integrated Services Routers



Integrated Threat Control for Cisco ISR

- Enables Inline Intrusion Prevention (IPS)
- Runs same software (CIPS 6.0) and enables same features as Cisco IPS 4200
- Performance Improvement by Hardware Acceleration
  - Up to 45 Mbps on Cisco 3845
  - Dedicated CPU and DRAM to offload host CPU
- Management through Cisco IPS Device Manager, Cisco Security Manager (Tentative 3.2)
- Supported by CS-MARS on event monitoring and correlation

Going forward…

- Secure Everything

  Secure Unified Communications

  Secure Wireless

  Secure Data Center

Cisco Is Committed to Security

- Product and Technology Innovation

  1500+ security-focused engineers

  Nine acquisitions added to our solution portfolio in last two years

  100+ partners worked collaboratively with us to deliver an unprecedented security vision

- Industry Leadership

  Critical Infrastructure Assurance Group

  Responsible disclosure

  Cisco Security Center web destination

  Intellishield — security intelligence and best practice sharing

“ Because the network is a strategic customer asset, the protection of its business-critical applications and resources is a top priority.”

John Chambers,
CEO, Cisco Systems®

Some Closing Thoughts

- Don’t get overwhelmed
- Small steps can make a big difference
- Remember, you don’t have to be the “best protected”—you just need to be a less inviting target than the next guy

Q and A

Ne zaboravite da se prijavite na Cisco Networkers 2008!

http://www.cisco.com/web/europe/cisco-networkers/2008/index.html