Adaptive Secure Network

A Proactive Approach to Information Security

Kanyarat Fhaikhao
Systems Engineer
kanyarat@cisco.com

Agenda

- Issues and Challenges
- Cisco® Self-Defending Network Solution
- Solution Components
- Getting Started

Top Security Challenges for 2006

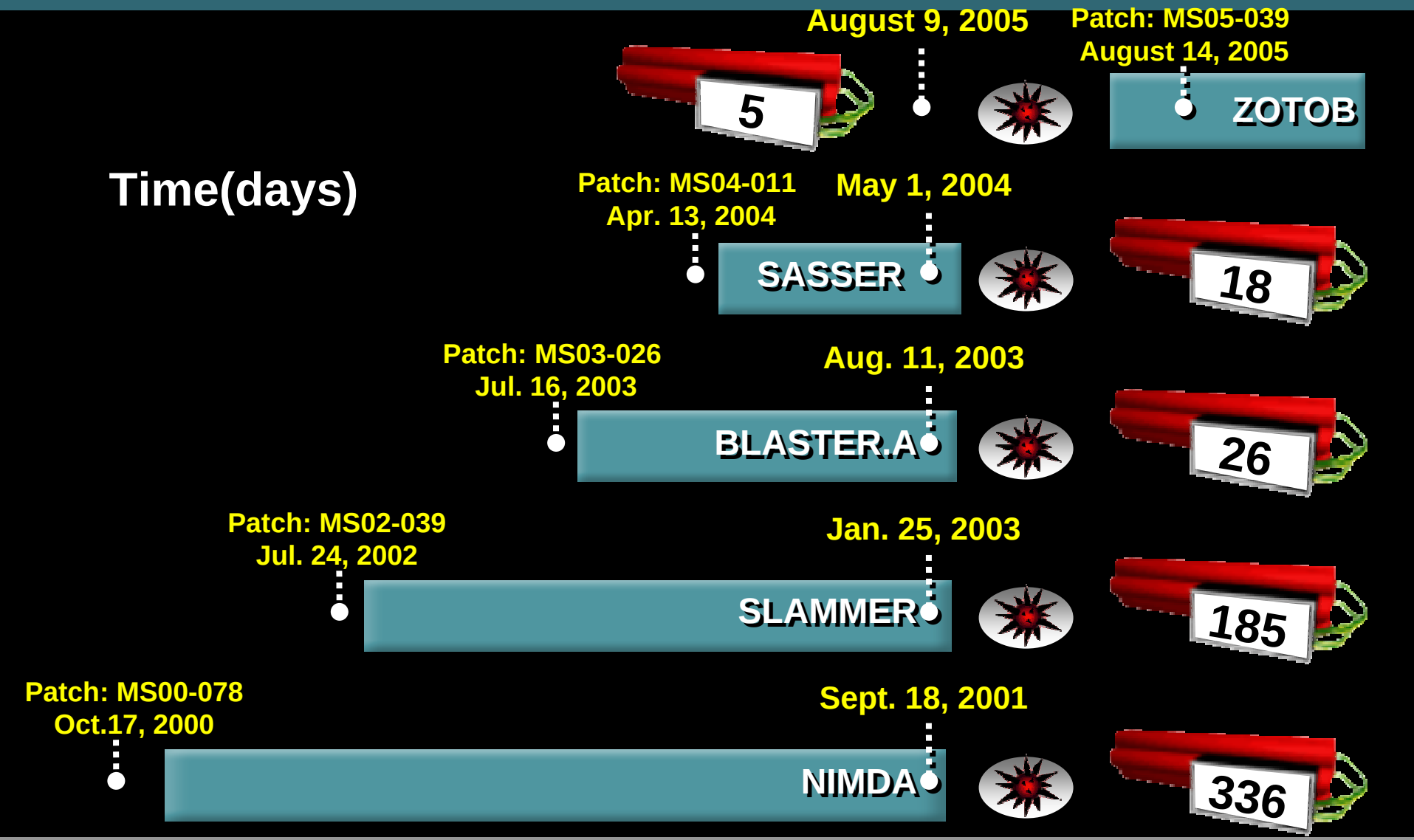
"Risk management, e-commerce risk and application security were among the key topics discussed at the London launch of the CSO Interchange, a high level initiative geared to bringing senior security executives together to discuss burning issues of the day. "

CSO Interchange – London, December 2005
http://www.csointerchange.org/press/pr.php/2005-12-13

Key Findings:

- **48% felt their organizations saw security as a "necessary evil" – rather than e.g. a business enabler**
- **43% were more involved than last year in driving compliance within their organization and 89% saw their responsibilities in this area increasing in the next two years**
- **A clear majority favored the introduction of personal security tokens for a more secure E-Commerce implementation**
- **63% declared that their organization had no application security related key performance indicators**

Virus/Worm exploit time is decreasing



Current Investment Is Misdirected

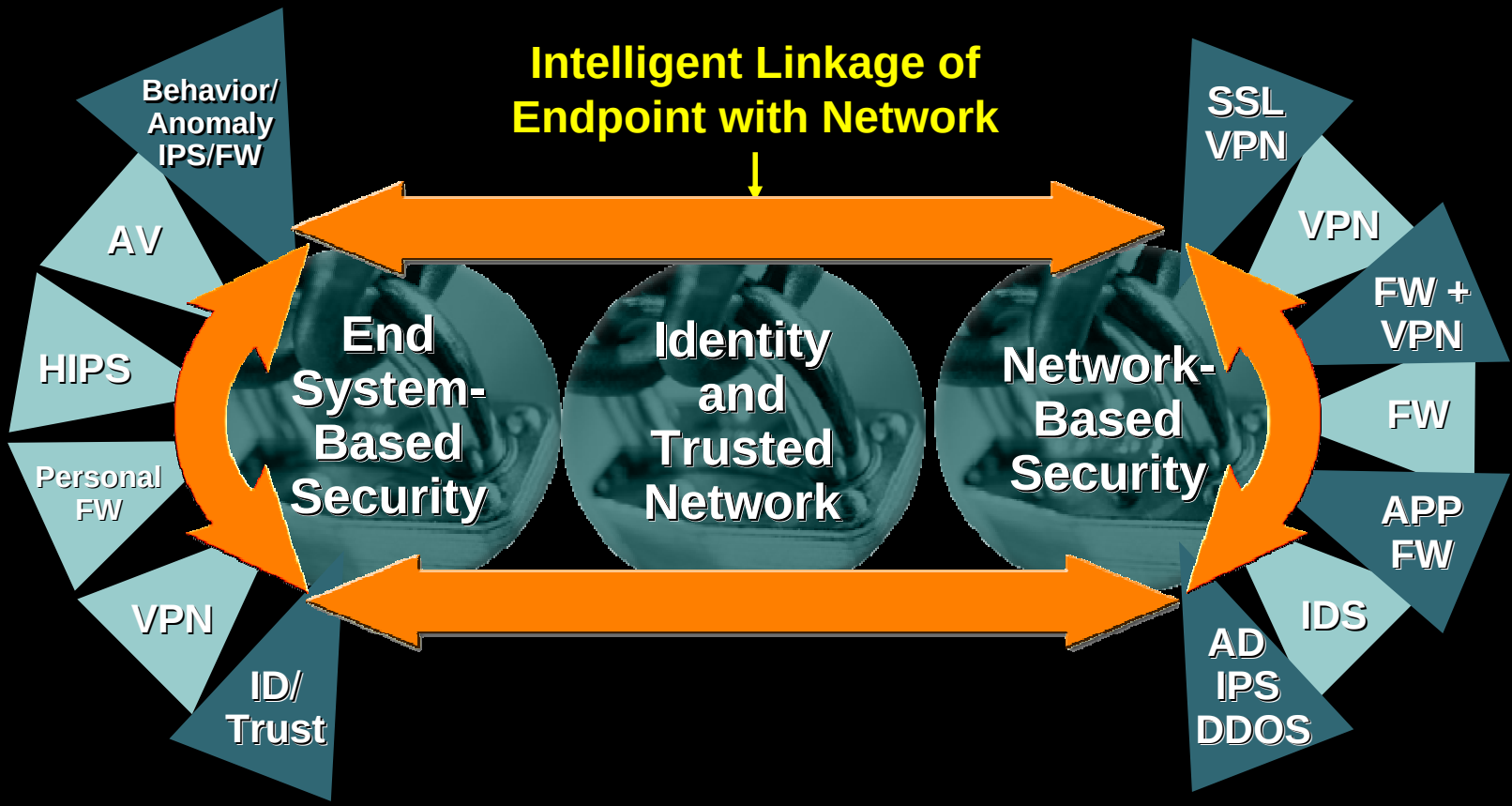
Prevention and Containment

Patching, Restoration and Recovery

"Respondents spend most of their time in reactive mode: responding to incidents, deploying firewalls, and dealing with everyday nuisances like spam and spyware. Ironically, the most common proactive step respondents take is to develop business continuity and disaster recover plans. So even their proactive steps are investments in reactive measures."

—*CSO Magazine,* 2005 State of Information Security Survey

A Logical Strategic Response
Self-Defending System



An integrated system

- Endpoint security solutions know security context and posture
- Policy servers know compliance/access rules
- Network infrastructure provides enforcement mechanisms

Cisco Self-Defending Network:
Using the Network to Identify, Prevent, and Adapt to Threats

Integrated

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

Collaborative

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

Adaptive

Proactive security technologies that automatically prevent threats

Cisco Security: Product and Solution Portfolio

Converged Security
Cisco ASA 5500

Firewall
Cisco PIX

Intrusion Prevention
Cisco IPS

Remote Access VPN
Cisco VPN 3000

Endpoint Security
Cisco Security Agent

Router Security
Cisco ISR Family

Switch Security
Catalyst Engines

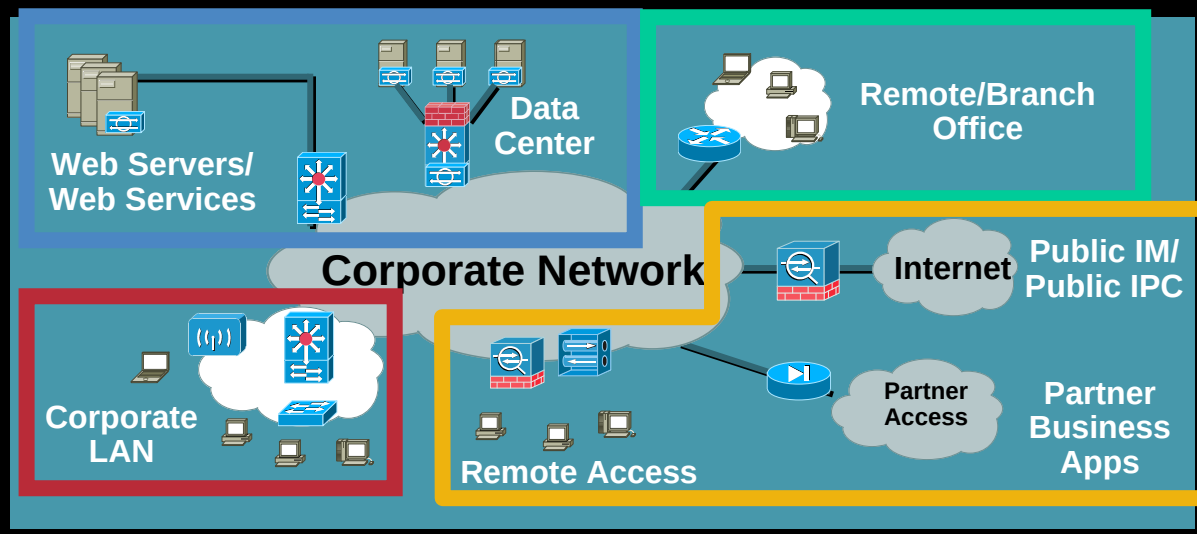
Application Security
AVS, ACE

Security Management
Cisco VMS/MARS

Security Systems
NAC/Clean Access

Foundation Security Solutions

Secure WAN
Secure LAN
Secure Perimeter
Secure Data Center



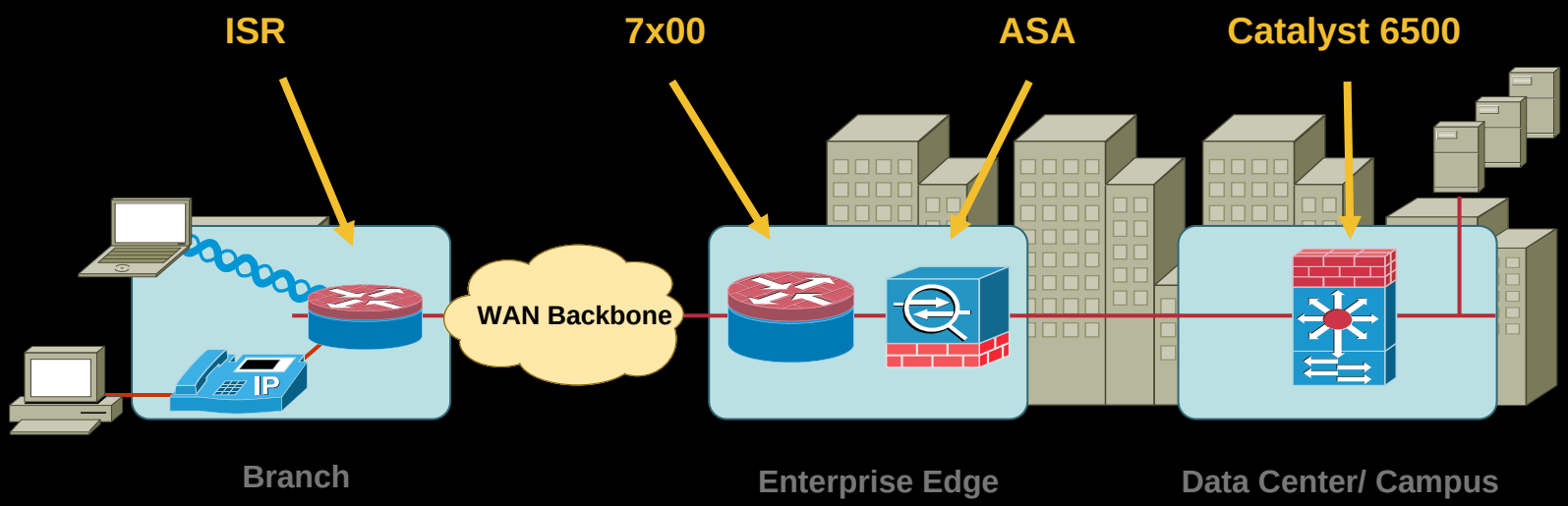
Advanced Security Solutions

Anti-X
Network Admission Control
Application Security
Security Management
and Operations

Foundation Security

Why Foundation Security?

- Every branch needs security
- Need for investment protection, higher scalability and virtualization
- Maintain consistent security policy at network perimeters



Network as Platform for Security

Integrated Services Routers (ISR)

- Integrate Cisco® IOS® Firewall, VPN, and Intrusion Prevention System (IPS) services across the Cisco router portfolio
- Deploy new security features on your existing routers using Cisco IOS Software
- NAC-enabled

Cisco Catalyst® Switches

- Denial-of-service (DoS) attack mitigation
- Integrated security service modules for high-performance threat protection and secure connectivity
- Man-in-the-middle attack mitigation
- NAC-enabled

Adaptive Security Appliances (ASA)

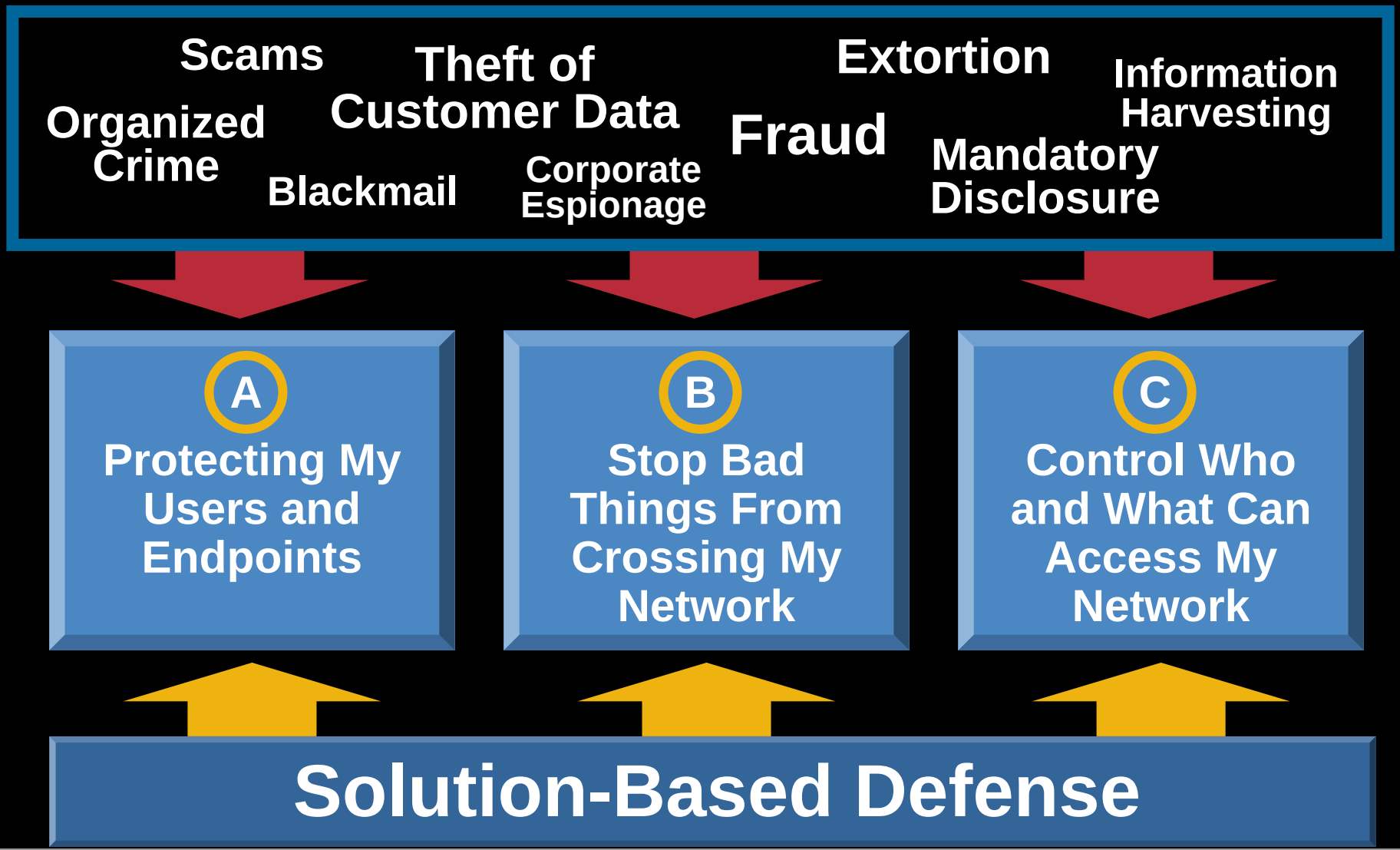
- High-performance firewall, IPS, network antivirus, and IPSec/SSL VPN technologies all in one unified architecture
- Device consolidation reduces overall deployment and operations costs and complexities
- NAC-enabled

“Comprehensive and simple—almost the holy grail.”

—Garth Brown, President, Semaphore

Advanced Security Solutions

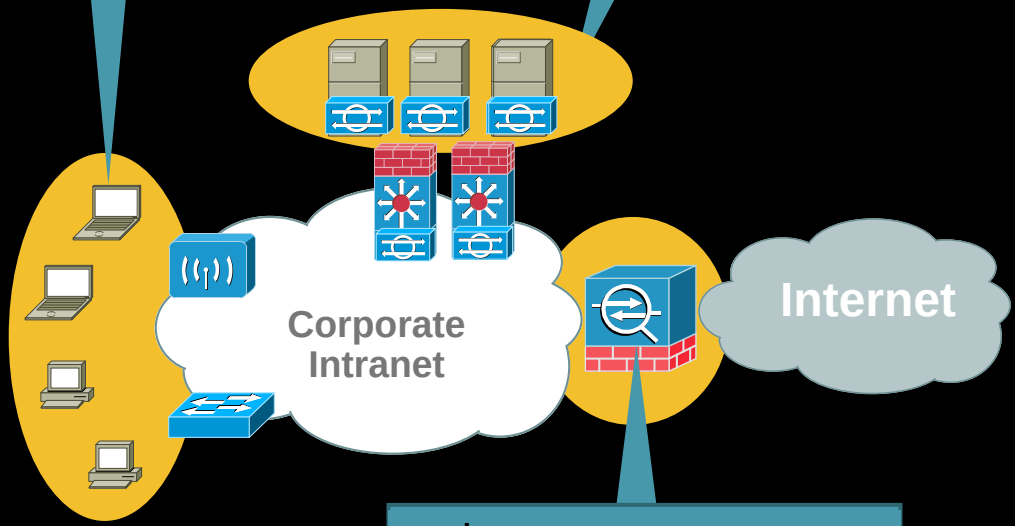
Root Causes: Back to Basics



Protecting Users and Endpoints

(1st) Secure the Desktops:
Stop infections at the source with CSA Desktop

(2nd) Secure the Servers:
Protect the critical assets of an organization with CSA Server



(3rd) Network-based Intrusion Prevention:
Protect all hosts, regardless of endpoint security posture

The Approach:

First Step:

Cisco Security Agent Desktop

- A personal firewall, host-based IPS, and behavioral protection system all in one
- Initial deployment for high value, "at risk" machines

Second Step:

Cisco Security Agent Server

- A more centralized protection: harden the business application servers from attack

Third Step:

Cisco Intrusion Prevention

- Network intrusion prevention complements a host-based strategy
- If other endpoint software is deployed, network-based Intrusion Prevention Services can be an effective strategy

Product Spotlight: Cisco Security Agent

What makes CSA valuable?

- **Market Leader in Endpoint Security**
  - CSA Desktop: Beat ISS, Symantec, and McAfee in Gartner Magic Quadrant
  - CSA Server: Grown to #2 market share (Infonetics)
- **Proven Technology**
  - 2.5 million Agent Ships
  - Multiple deployments of more than 100,000 agents

Case Study: Enterprise-Wide Deployment

- Started with 1000 desktops for Remote Access VPN
- Came back and deployed for 2000 and critical desk tops
- Came back for 4000 more
- Now coming back for an enterprise-wide roll-out

CSA Desktop and Remote Access VPN:

- When deploying Remote Access VPN, always ask how do we intend to protect those remote end points
- Personal firewall alone does not address endpoint security issues
- CSA enforces desktop application standard to comply to security and business policies

CSA Server and IP Telephony:

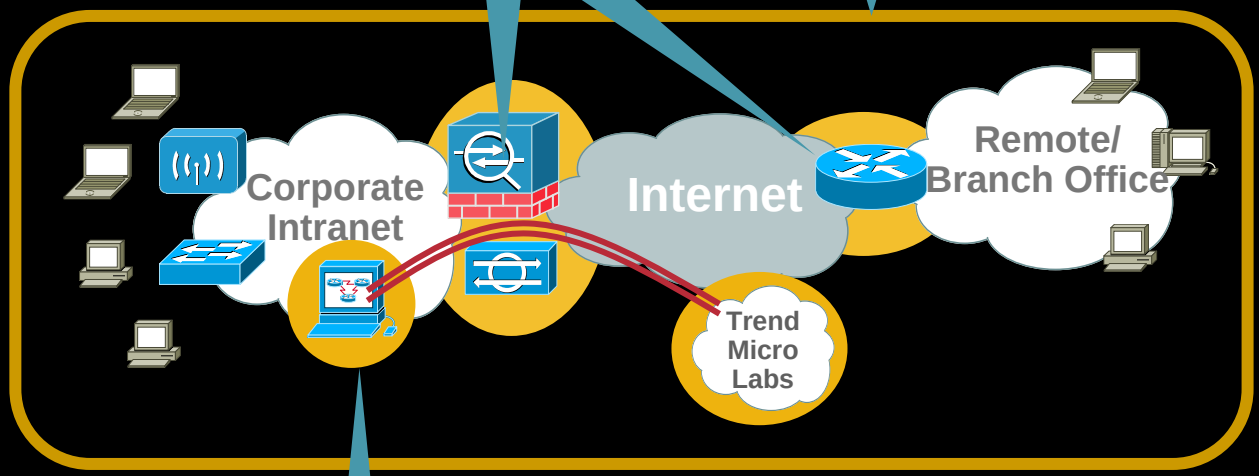
- Provides a “breathing room” for patch management process.
- Telephony servers ship with CSA

B

Halting the Spread of Malware

(1st) Network-based Intrusion Prevention:
Your primary technology for threat mitigation

(2nd) CS-MARS
Correlate security events across the network for rapid incident response

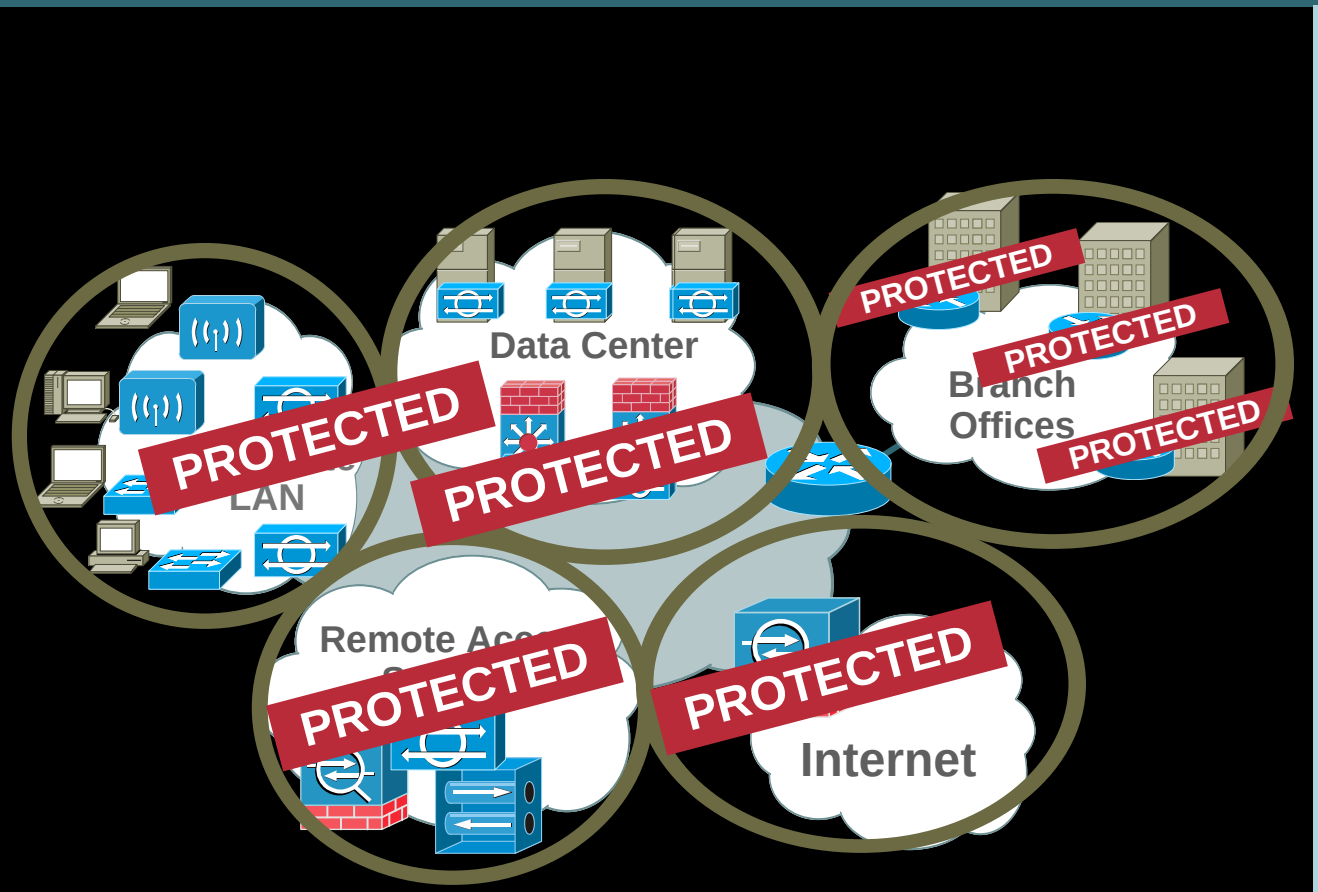


(3rd) Incident Control System
Live security intelligence for near zero-time responsiveness to threats

The Approach

1. **Cisco Intrusion Prevention Systems**
   - Deployed as stand alone appliance or integrated with Catalyst 6500
   - IOS-IPS extends the solution to ISR Routers
2. **CS-MARS**
   - Brings the "wow" factor to the solution
   - Deployed in a multi-device multi-vendor environment
3. **Incident Control System**
   - Unique solution - the industry's most rapid response— from hours to minutes

Product Spotlight: Cisco Intrusion Prevention Systems



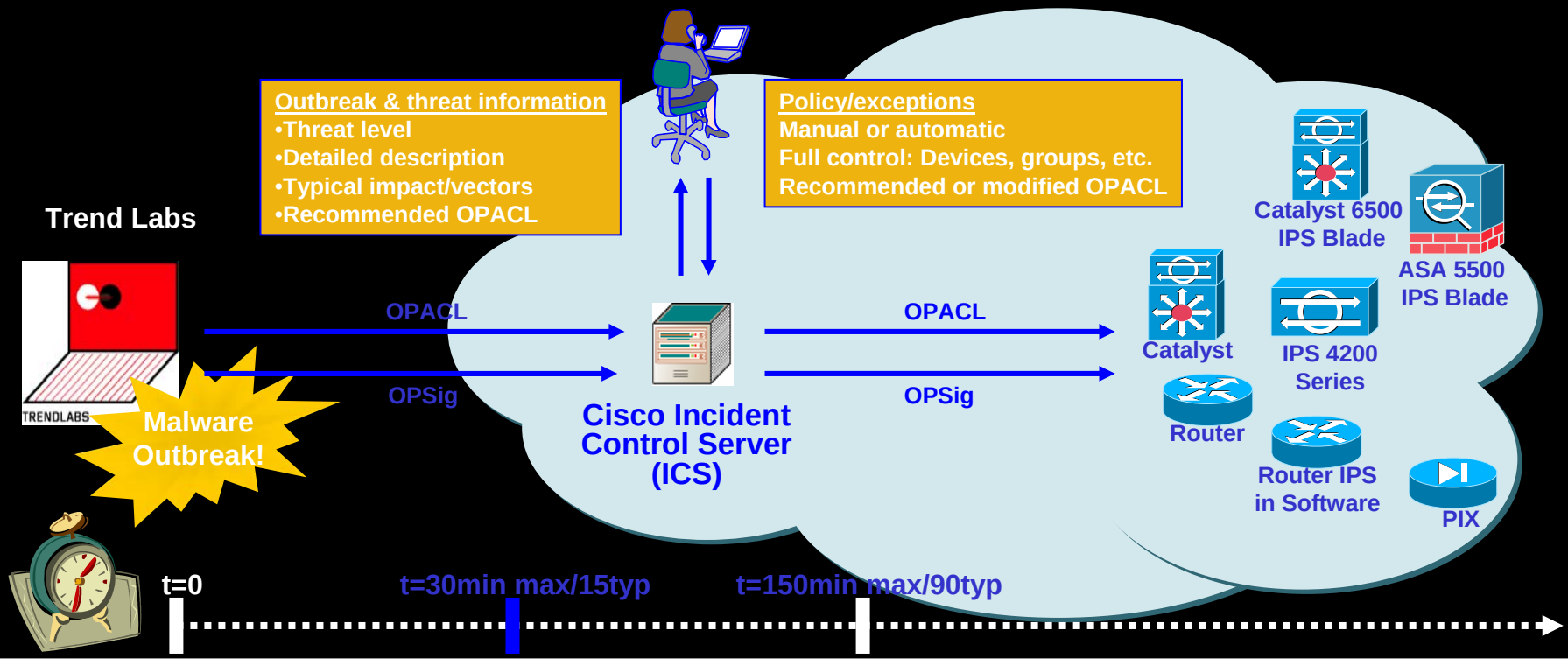
Cisco IPS Solution: Superior to the Competition

- **Greater accuracy:** Use advanced technologies like Risk Rating to mitigate false positives
- **Integrated into the network:** Through integration into the network and security infrastructure, Cisco IPS can protect the entire network, not just a few locations

Product Spotlight: Cisco Incident Control System (ICS)

Components

- Trend Labs world-wide real-time monitoring and signature development infrastructure
- Software: Cisco Incident Control Server – Vehicle for administration and delivery of virus and worm related solutions
- Mitigation network devices that are recipients of the service

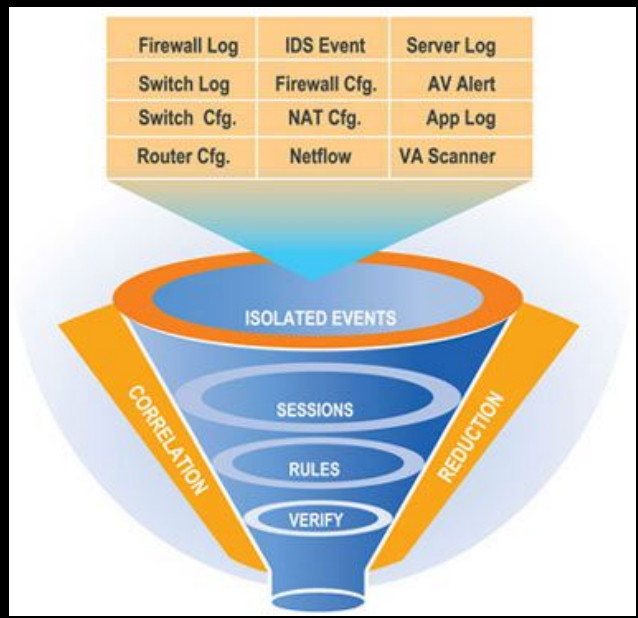


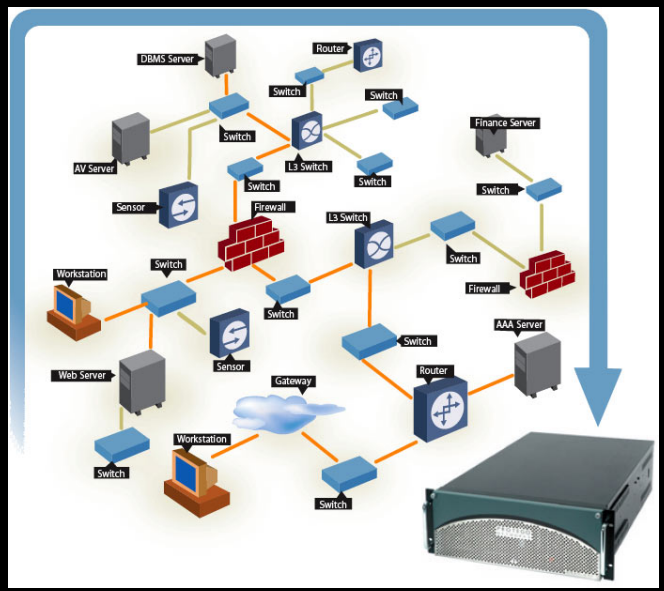
Product Spotlight: Cisco Security MARS

- **Leverage YOUR existing investment to build "pervasive security"**
- **Correlate data from across the Enterprise**

  NIDS, Firewalls, Routers, Switches, CSA

  Syslog, SNMP, RDEP, SDEE, NetFlow, Endpoint event logs
- **Rapidly locate and mitigate attacks**





- **Key Features**

  Determines security *incidents* based on device *messages*, *events*, and "*sessions*"

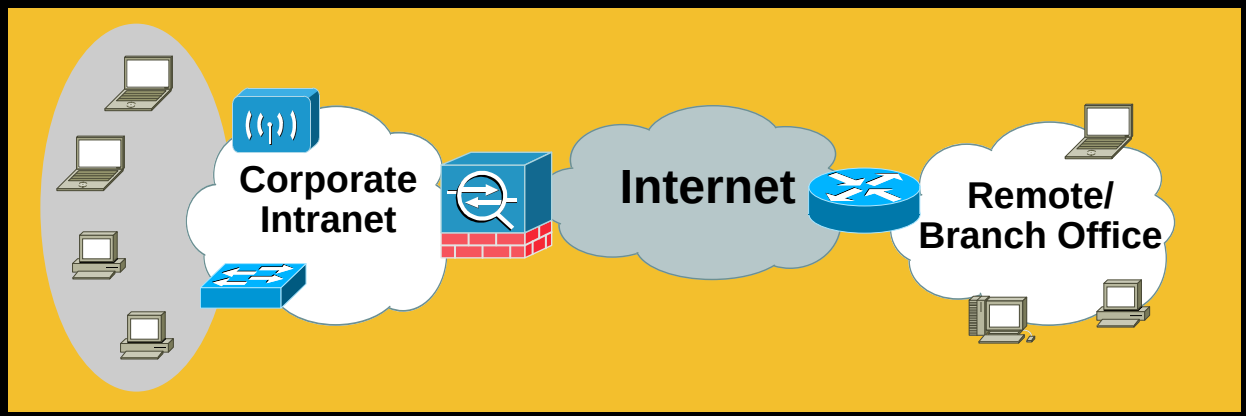
  ***Incidents* are topologically aware for visualization and replay**

  Mitigation on L2 ports and L3 chokepoints

  Efficiently scales for real-time use across the Enterprise

Controlling Network Access

- **What is NAC?**
  - Controls access of all devices (managed, unmanaged, rogue)
- **What does Cisco offer?**
  - 1. The best turnkey appliance product for all verticals, Cisco Clean Access (CCA)
  - 2. The best technological approach for Enterprise, NAC Framework
- **We've got you covered, regardless of budget or needs**



The Approach

First Step:

Address Immediate Pain-Points

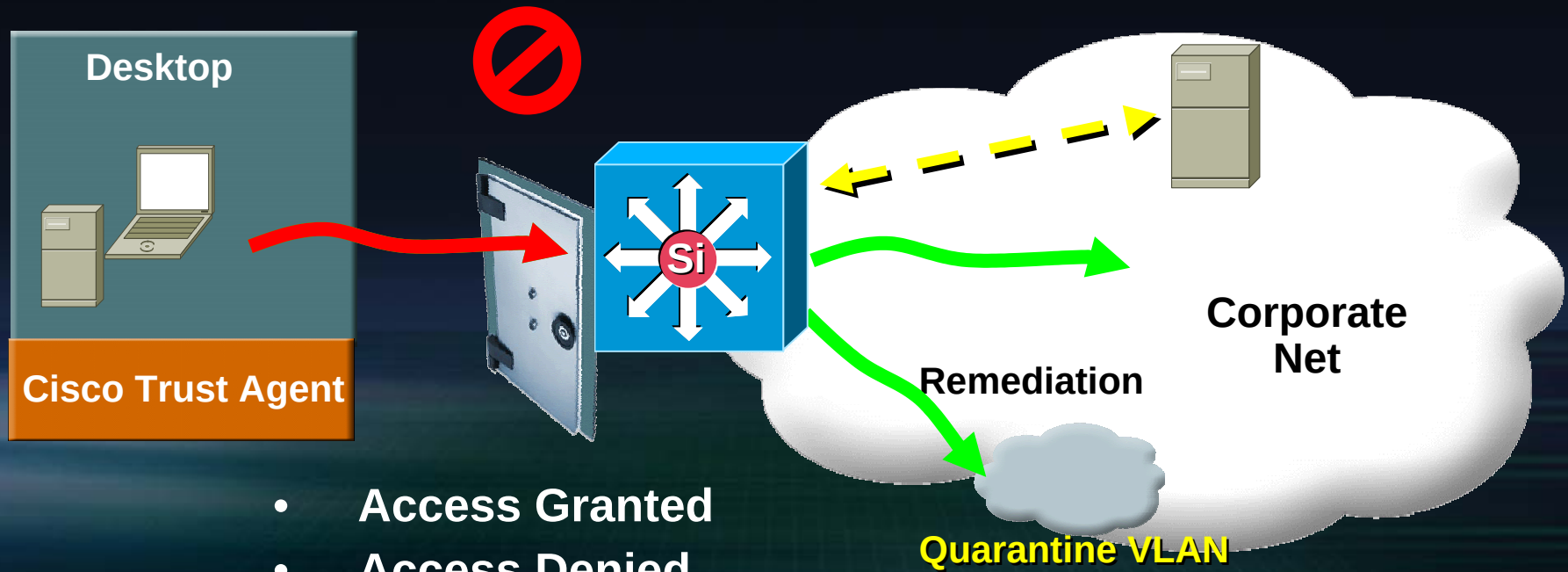
- **Rapidly Deployable Cisco Clean Access Provides Immediate Benefits**

Second Step:

Long-Term Enterprise Architected Solution

- **Engage with Evals and Pilots of Enterprise-Wide NAC Framework**

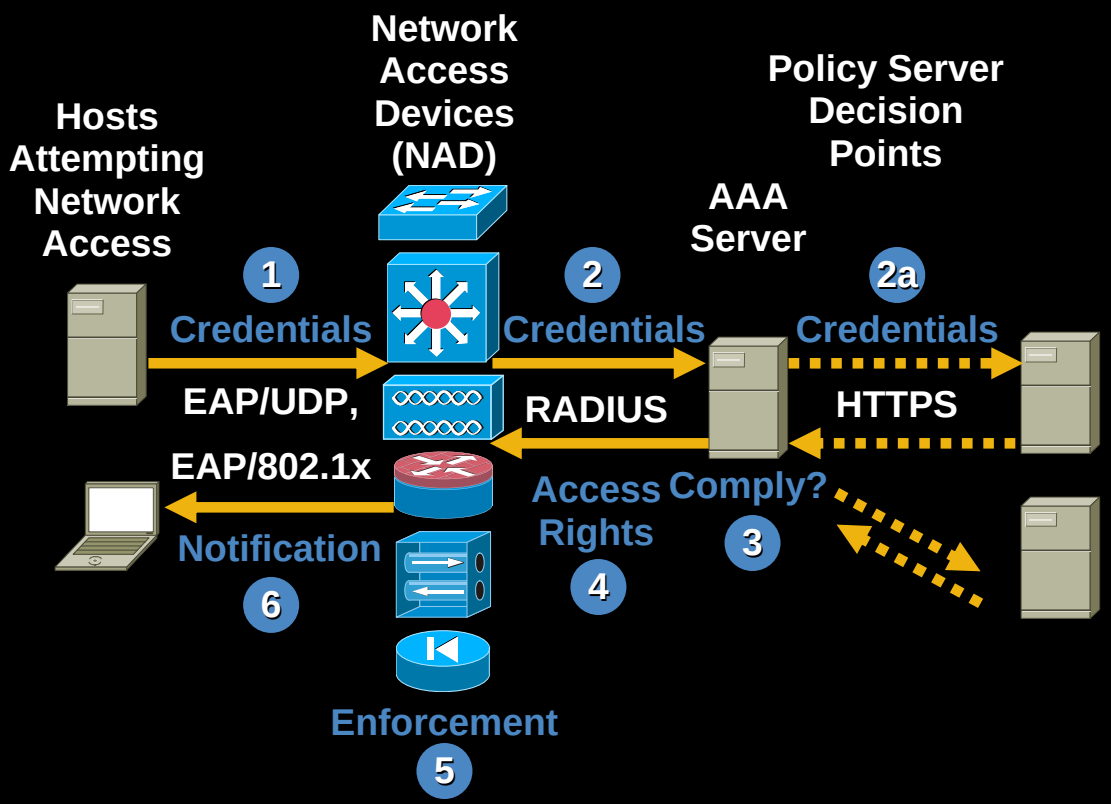
Network Admission Control (NAC) Overview



- Access Granted
- Access Denied
- Quarantine Remediation

Solution Spotlight: NAC Framework

NAC Solution: Leverage the network to intelligently enforce access privileges based on endpoint security posture



NAC Characteristics:

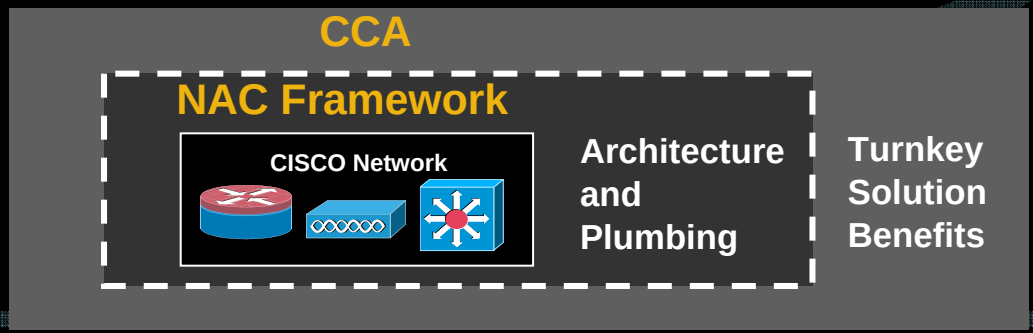
- Ubiquitous Solution For All Connection Methods
- Validates All Hosts
- Leverages Existing Network and Security and Mgmt SW
- Applications Gather and Assess Credentials, Remediation Services
- Network Provides Visibility, Forces Authentication, Isolation Services

Strong NAC Partner Program

http://www.cisco.com/en/US/partners/pr46/nac/partners.html

Product Spotlight: Cisco Clean Access (CCA)

- **Comprehensive NAC functionality**
  - Scan, block, quarantine, remediate and enforce
  - Covers all use cases for LANs, branch offices, remote access, wireless users, and guest users
- **Largest market share**
  - Enforces over 2.5 million end users
  - Largest deployment of 63,000 users
  - 300+ customer deployments
- **CCA benefits carry forward to Framework**
  - CCA + Framework = best of both worlds
  - Investment is protected
  - Keeps competition out



salesforce.com
experience success.

"This is the greatest product: I don't have to worry about my conference rooms ever again"

ASU
Arizona State University

"With Clean Access, the number of security incidents fell from 6,000 a year to fewer than 50."

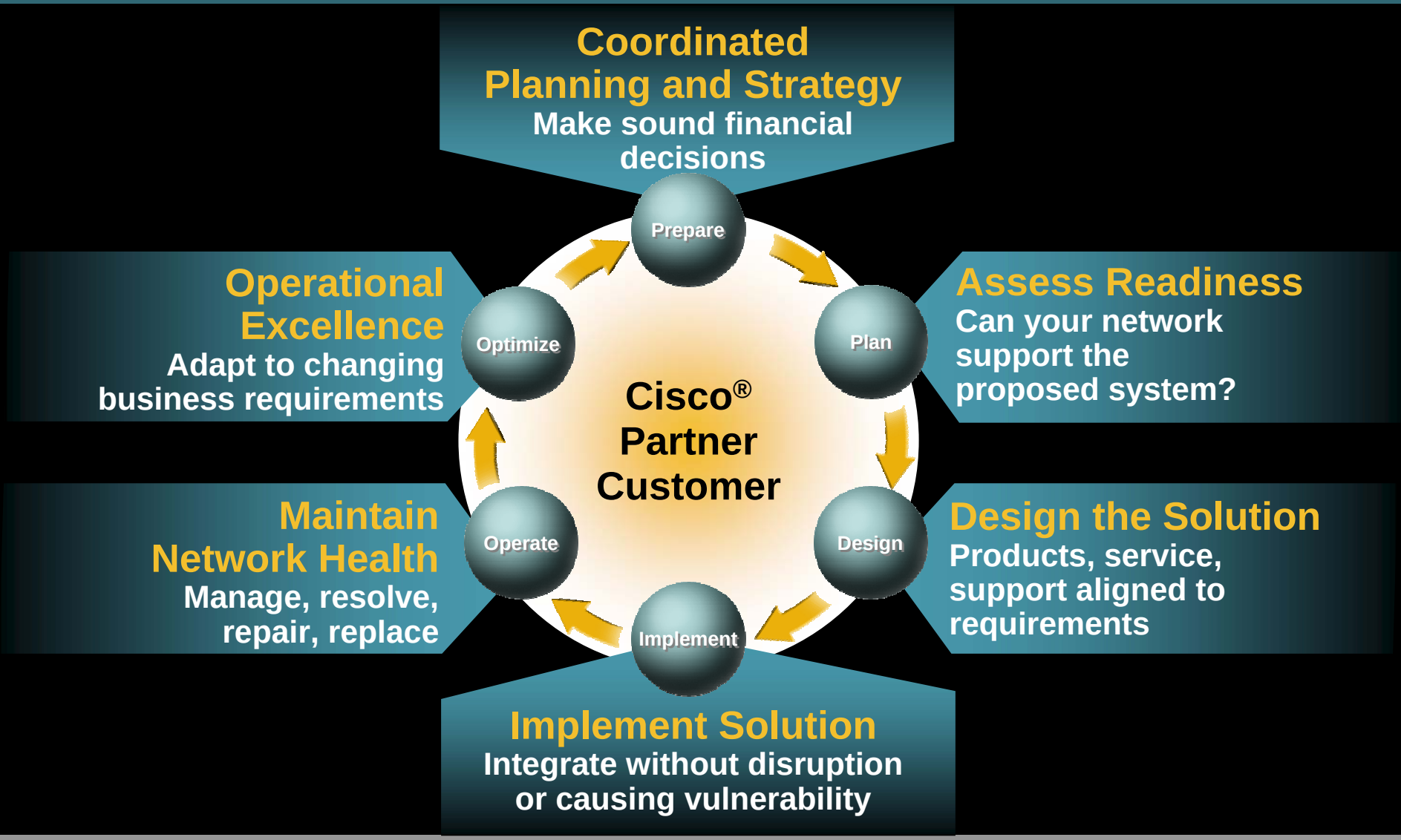
Customer Sampling

Anne Arundel Medical Center
PIM
pjm
Toys"R"Us
Jack In The Box
New England BioLabs
University of South Carolina

Getting Started

- **Build-out foundation security solutions:**
  - Protect critical traffic and network segments
  - Integrate security into the network infrastructure
- **Establish pilot deployment for advanced security solutions:**
  - Anti-X, Zero-Day Mitigations, Secure Application
- **Review architectural readiness**
  - Network Admission Control
  - Enterprise-wide Security Event Management

A Lifecycle Approach to Security Service and Support



Cisco: Helping Our Customers Make the Journey from Point Solutions to Self-Defending Networks

- Self-Defending Network: integrated, collaborative, adaptive
- Enable business-driven security practice
- Risk gaps are reduced; complexity is reduced; total cost of ownership is lower
- Protect, optimize, and grow your business

cisco.com/go/security