Securing the Intelligent Information Network

Cisco EXPO 22. marts 2006

Henrik Ballermann, hba@cisco.com

Teknisk Direktør, Cisco Systems

Agenda

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

CEO's Priorities…
Networked IT Enables Priorities

"CEOs call technology advances most important driver of change"… First year ever

The Economist
2005 CEO Briefing

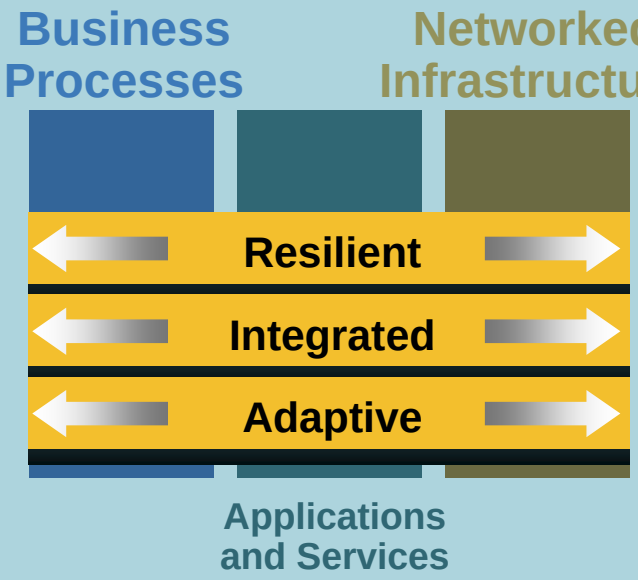
As technology becomes more business critical...
security becomes a business imperative

Intelligent Networking
Using the Network to Enable Business Processes

Cisco Network Strategy

Utilize the Network to Unite Isolated Layers and Domains to Enable Business Processes

Connectivity



Intelligent Networking

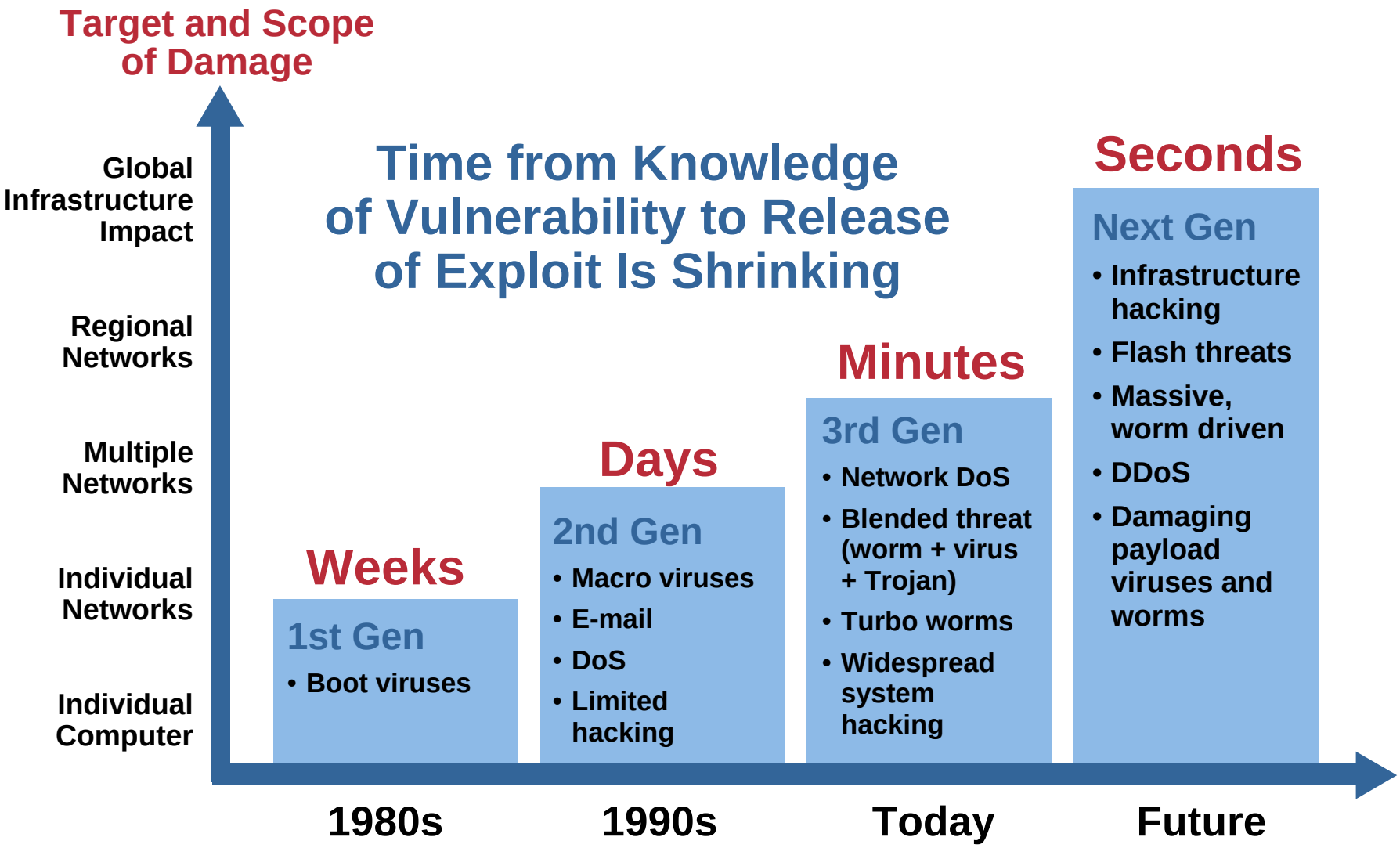
- **Active participation in application and service delivery**
- **A systems approach integrates technology layers to reduce complexity**
- **Flexible policy controls adapt this intelligent system to your business though business rules**

Information Security Objectives: Security as a Business Enabler

- **Align security practice and policy to business requirements**
- **Use IT investments to "go on the offense"**
- **Reduce complexity of the overall environment**
- **Gain protection, control, and visibility over incidents and threats**

- **The network touches all parts of the infrastructure**
- **It is uniquely positioned to help solve these issues**

Evolution of Security Challenges

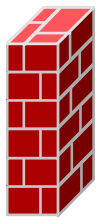


Vulnerable Custom Applications:
Focus of Attacks Moves to the Application Layer

75% of Attacks Focused Here

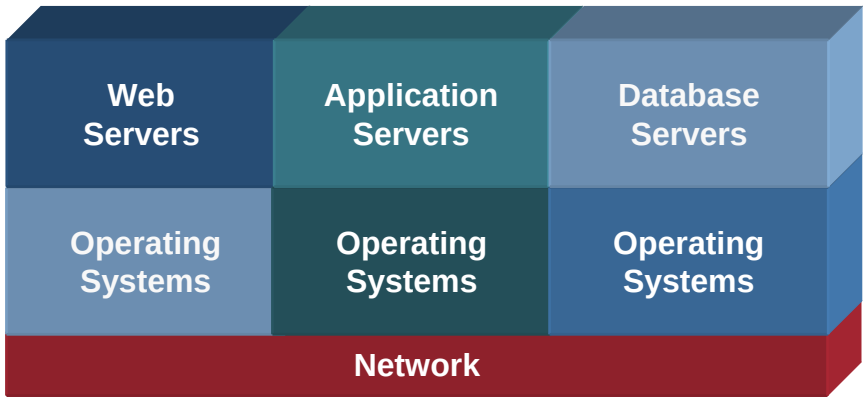
No Signatures or Patches

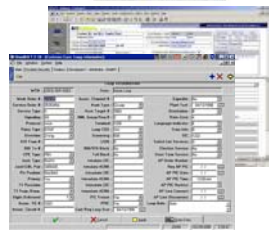
Custom Web Applications
- Customized packaged applications
- Internal and third-party code
- Business logic and code



Network Firewall

IDS IPS





Why Cisco?
We Are Committed to Security

Product and Technology Innovation

- 1500 security-focused engineers
- 15 acquisitions added to our solution portfolio
- 65+ NAC partners worked collaboratively with us to deliver an unprecedented security vision

Responsible Leadership

- NIAC Vulnerability Framework Committee
- Critical Infrastructure Assurance Group
- PSIRT—responsible disclosure
- MySDN.com—intelligence and best practices 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

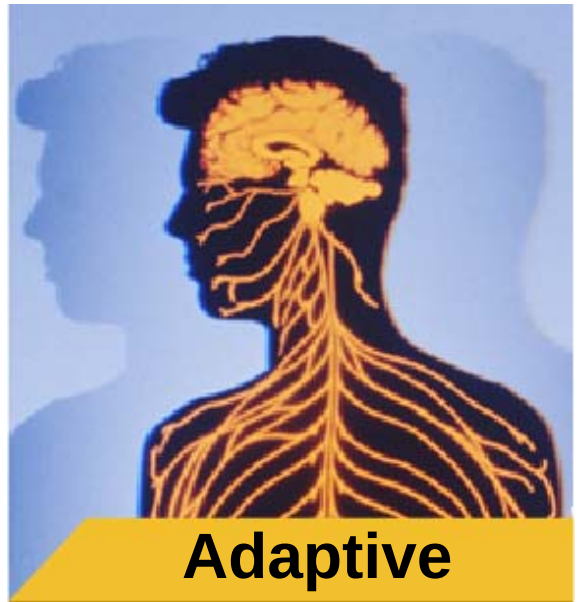
Cisco Self-Defending Network:
Using the Network to Identify, Prevent, and Adapt to Threats

Integrated

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

Collaborative

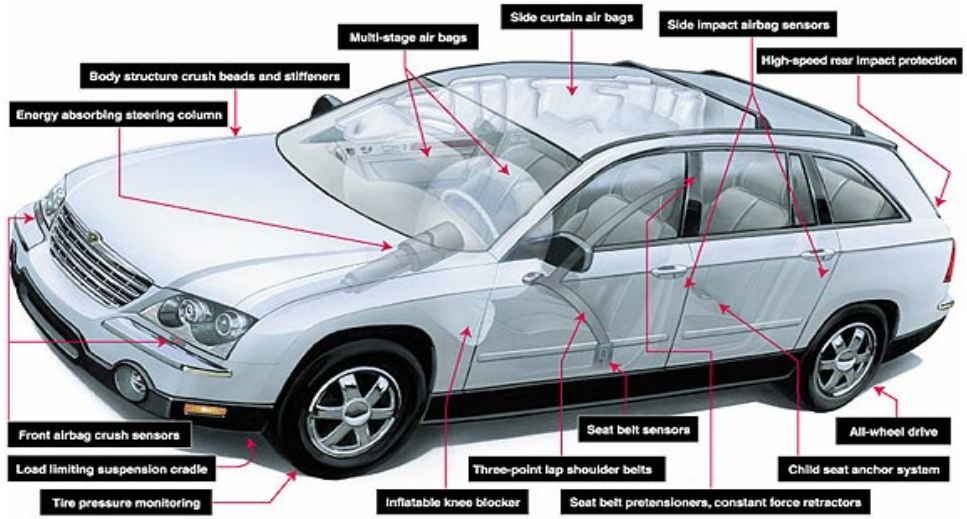
Collaboration among the services and devices throughout the network to thwart attacks



Adaptive

Proactive security technologies that automatically prevent threats

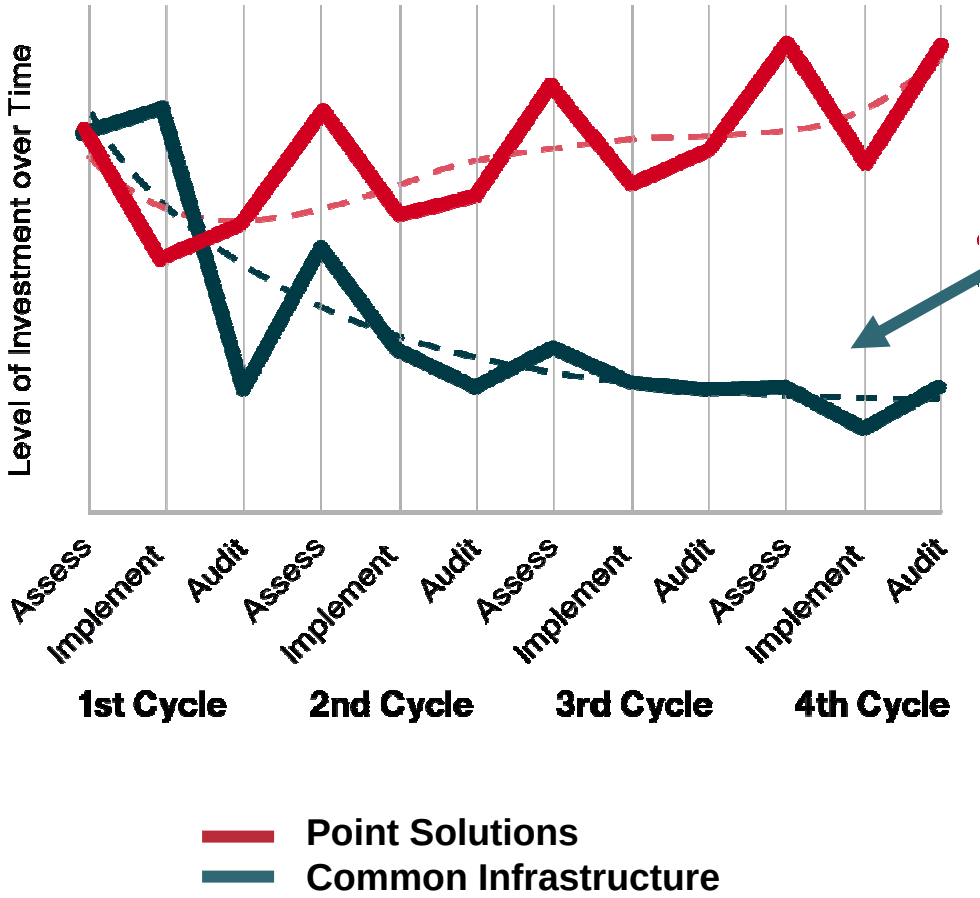
Benefits of a Systems Approach



- Complex environment
- Gaps and inconsistency
- Lower visibility
- More difficult to manage
- Higher TCO

- Simplified environment
- Tighter integration = tighter security
- Greater visibility
- Easier to deploy and manage
- Lower TCO

Benefits of Cisco Self-Defending Networks



Improved Value:

- **Reduces integration costs—security is already integrated into the network**
- **Allows proactive, planned upgrades at traditional IT refresh cycles**
- **Improves efficiency of security management**

Security Virtues of a Common Infrastructure, J. Tiller, INS

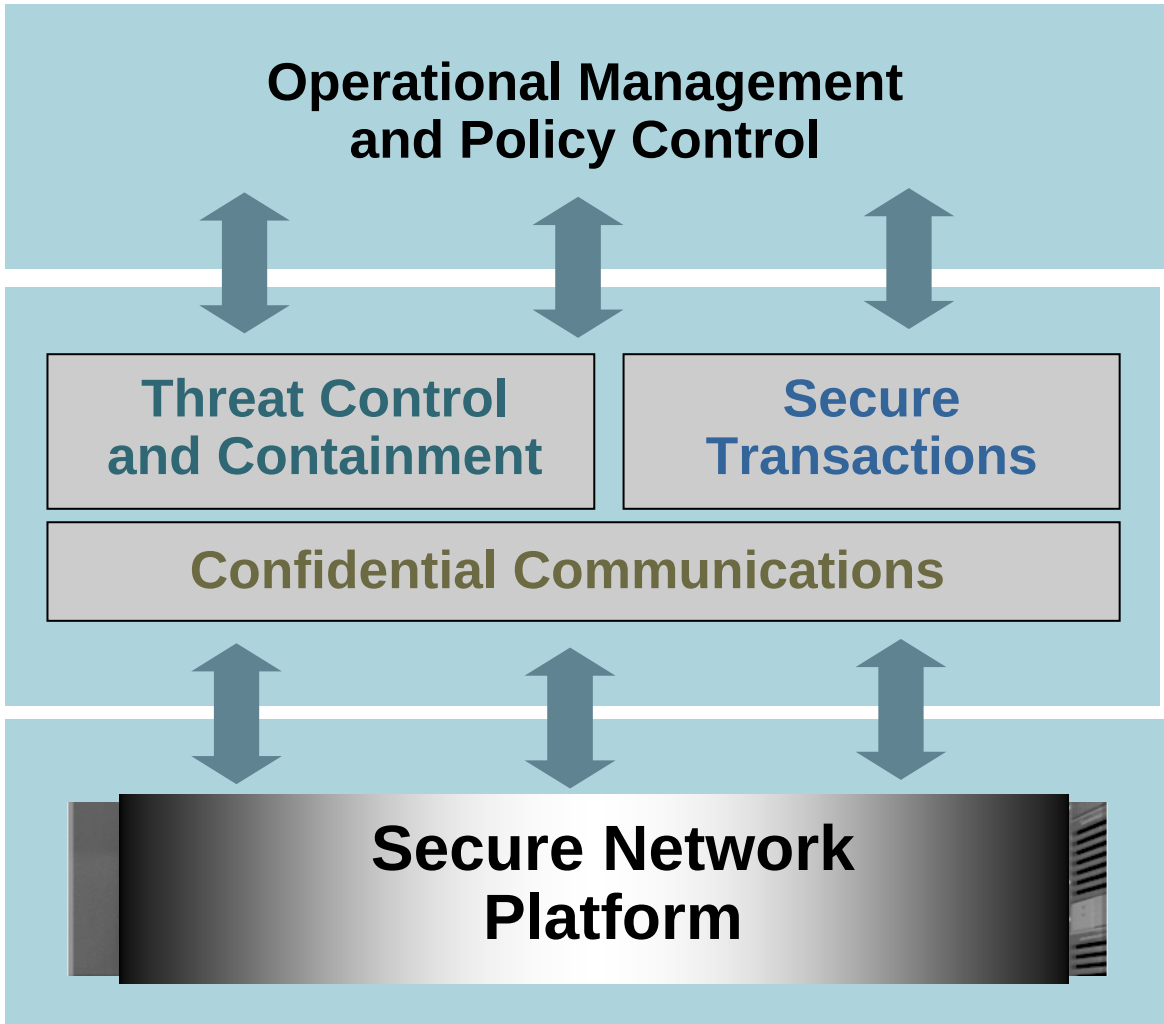
Self-Defending Network Defined

Efficient Security Management, Control, and Response

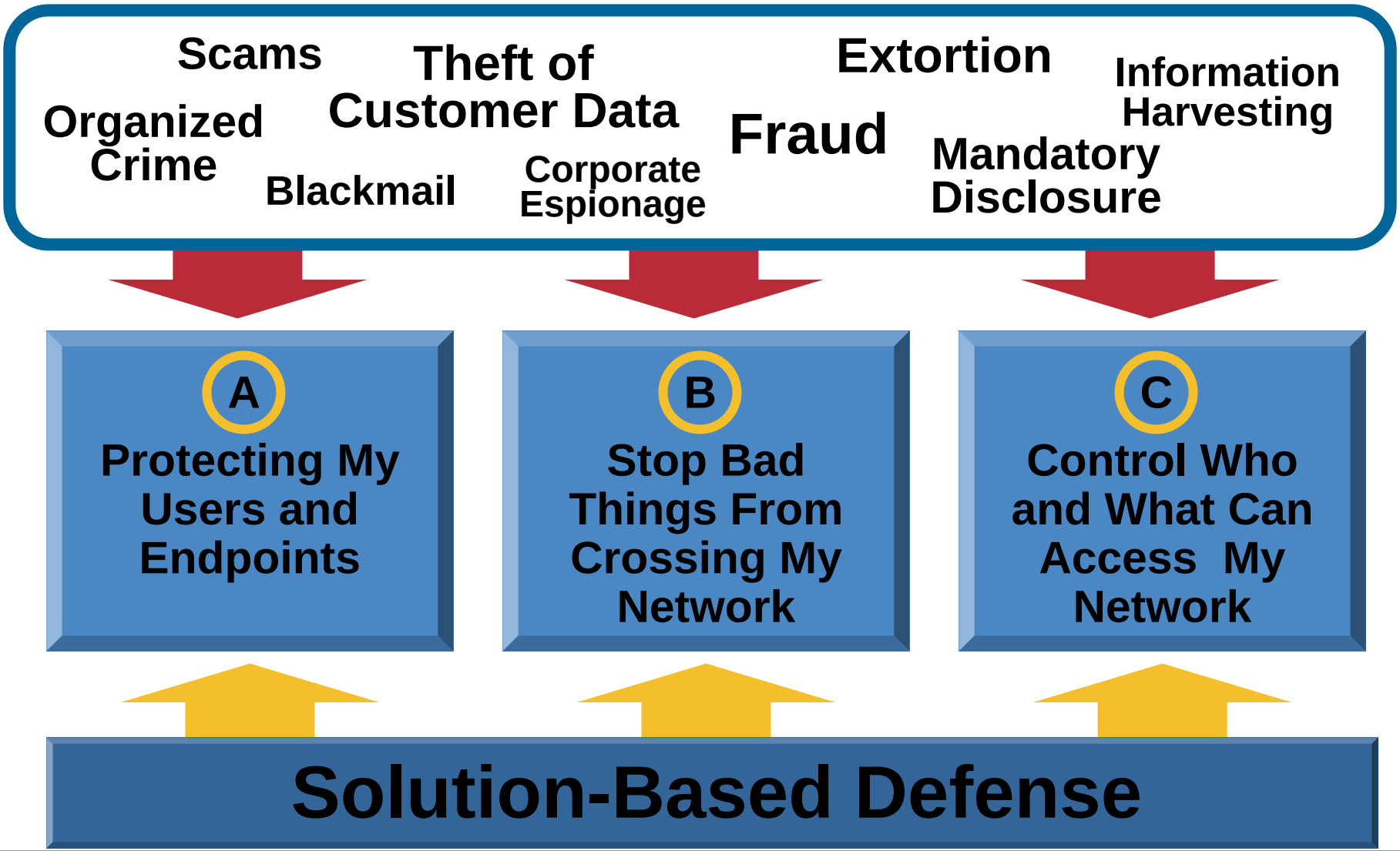
Advanced technologies and security services to

- **Mitigate the effects of outbreaks**
- **Protect critical assets**
- **Ensure privacy**

Network as Platform



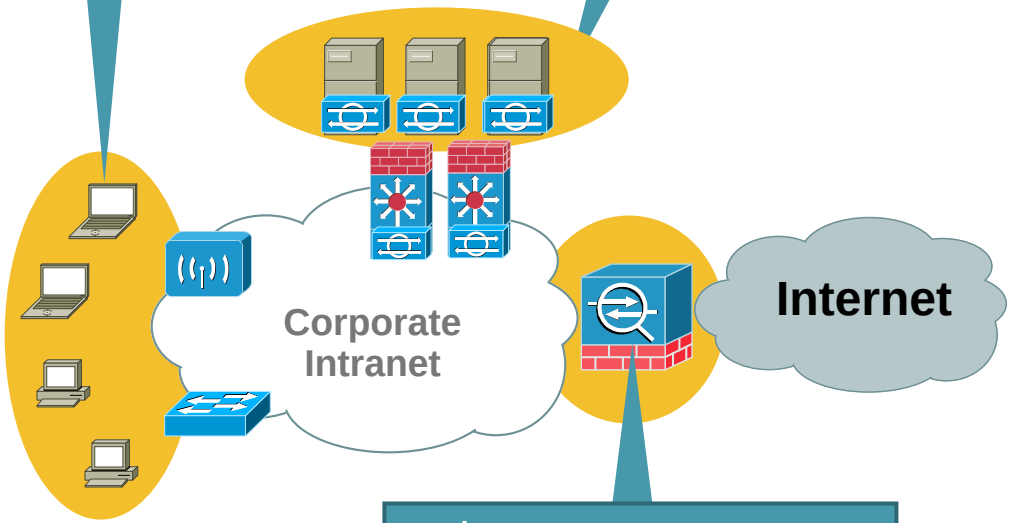
Root Causes: Back to Basics



Protecting My 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:

Cisco Security Agent Desktop

- A Personal Firewall, Host-based IPS, and Behavioral Protection System all in one.
- For high value, "at risk" machines

Cisco Security Agent Server

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

Cisco Intrusion Prevention

- Network Intrusion Prevention complements a host-based strategy

B

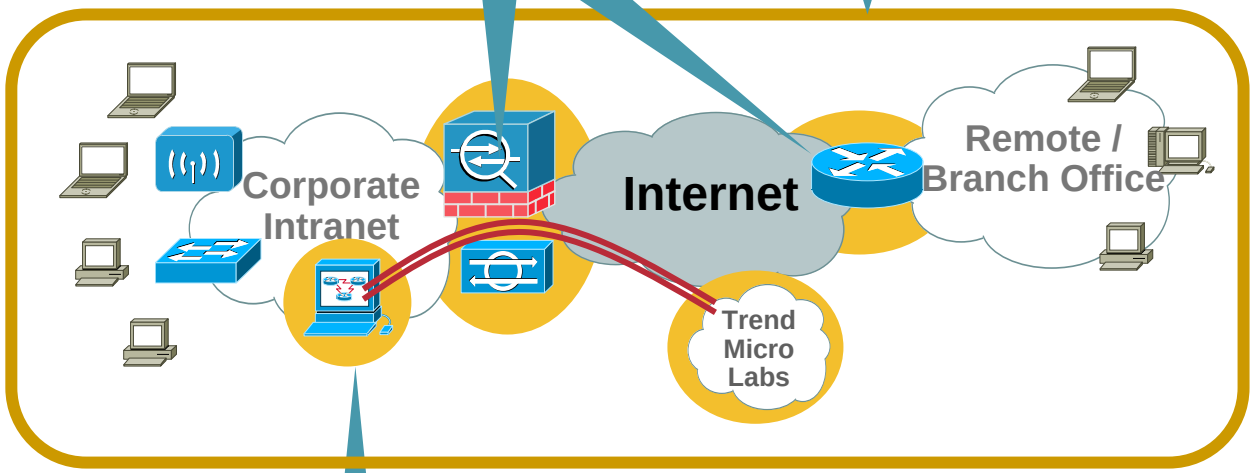
Stop Bad Things From Crossing My Network

(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

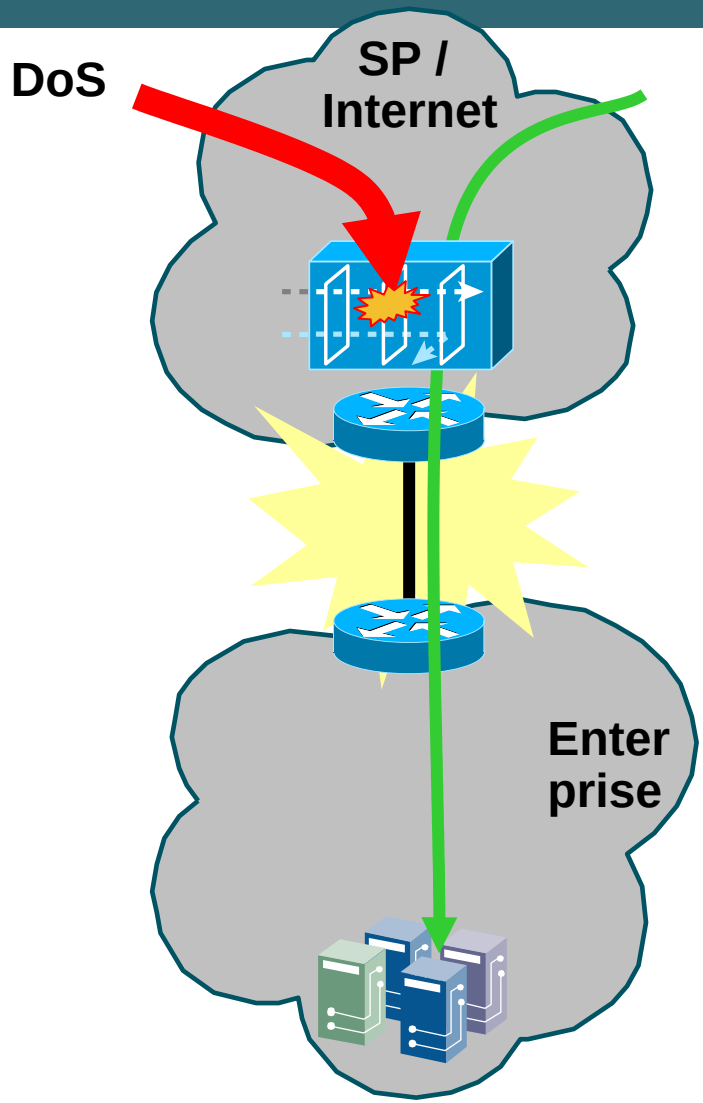
The Approach

1. **Cisco Intrusion Prevention Systems**
   - Stand alone service, or IOS-IPS extends the solution to ISR Routers
2. **CS-MARS**
   - Correlation among several devices from multiple vendors
   - Mitigation
3. **Incident Control System**
   - Most rapid response – from hours to minutes

Control Who and What Can Access My Network?

1. Non-compliant endpoint attempts connection
2. Quarantine remediation
3. Infection containment; endpoints secured

Protecting the Victim: The Enterprise
(incoming DoS attack):



Integrated/Convergence… D/V/V/M Requires Integrated, Pervasive Security

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