





The Self-Defending Network 3.0



Agenda

- Cisco Self Defending Network 3.0

Factors That Impact Business Security



Collaboration and Communication

- TelePresence / Video / IM / Email
- Mobility
- Web 2.0 / Web Services / SOA



The New Threat Environment

- The Eroding Perimeter
- Spam / Malware / Profit-Driven Hacking
- Data Loss and Theft



The Business Impact of Security

- IT Risk Management
- Regulatory Compliance
- Security as Business Enabler

The Growing Need for Security Solutions

**Regulatory
Compliance**



Data Loss



A Systems Approach to Streamline IT Risk
Management for Security and Compliance

**Threat
Management**



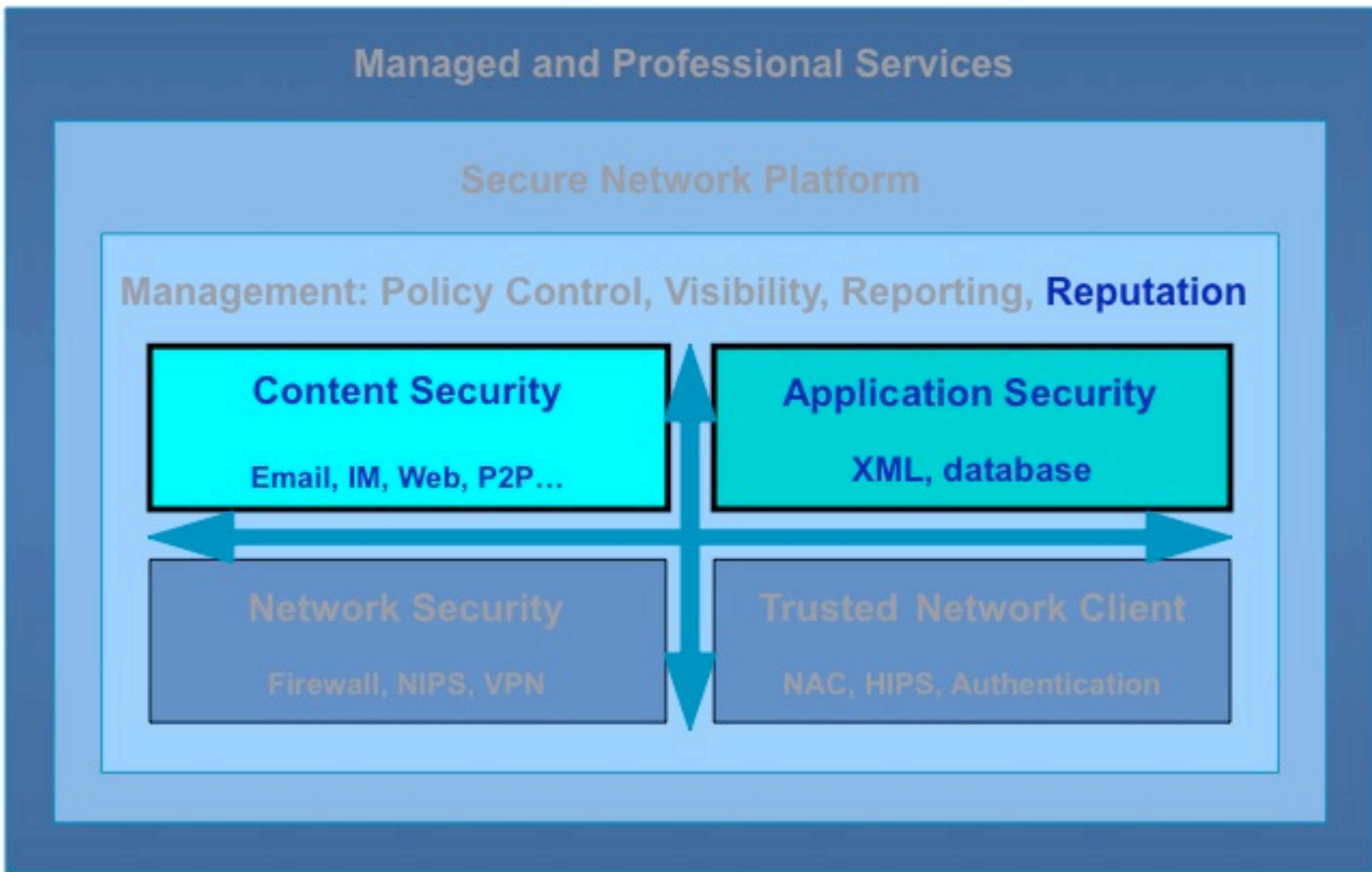
To Date: Self Defending Networks



- **Since introduction in 2004, Cisco has reached at 38% market share in a \$5B available market.**
- **Established leadership in 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

A New Framework for Deeper & Wider Security Solutions



Cisco Self-Defending Network Solutions for Business Security

System Management

Policy—Reputation—Identity

Application Security

Content Security

Network Security

Endpoint Security

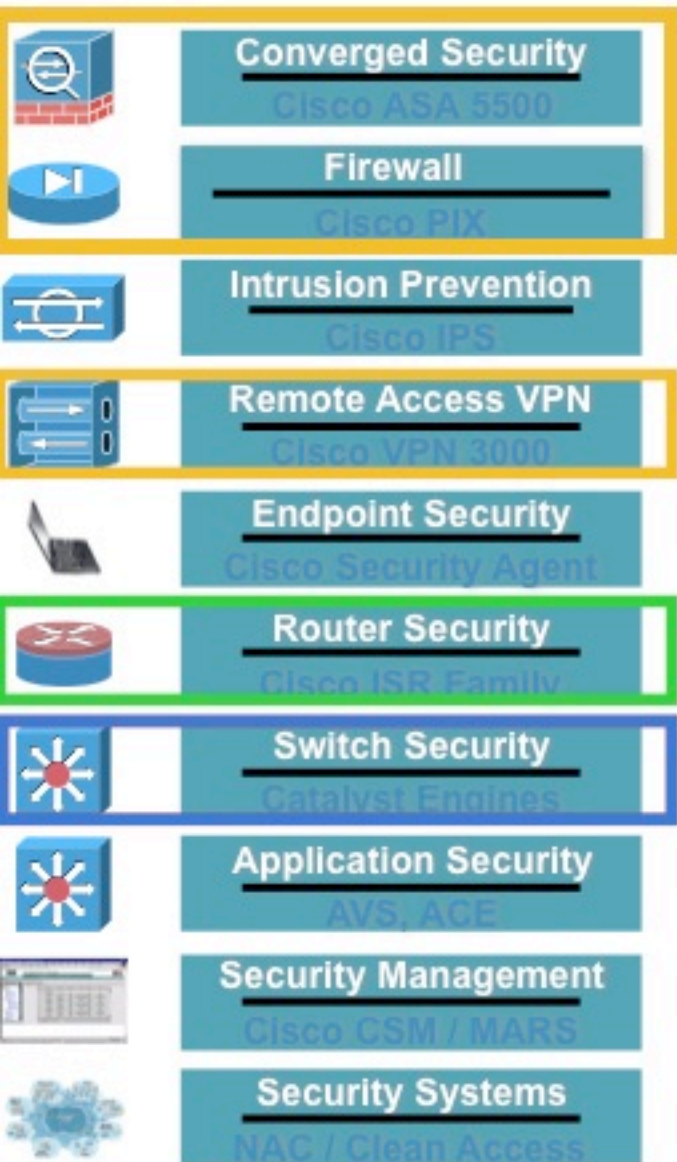
Cisco Self-Defending Network:

**Best of Breed Security in a
Systems Approach**

- Enforce business policies and protect critical assets
- Decrease IT administrative burden and reduce TCO
- Reduce security and compliance IT risk

Business Security

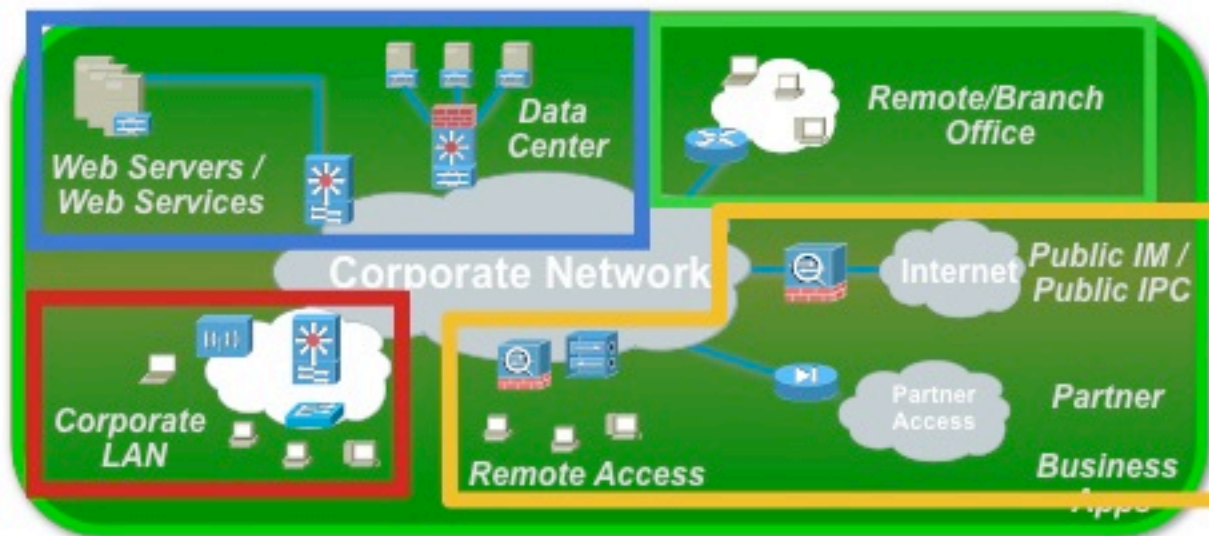
-- Cisco Security Solution & Portfolio



Foundation Security Solutions

Secure WAN
Secure Perimeter

Secure LAN
Secure Data Center



Advanced ATD Solutions

Day Zero
Application Security

Network Admission Control
Security Management and Operations

The Portfolio at a Glance...

Network and Endpoint Security

Network Security

- Integrate security pervasively into the network
- Converged services for fewer touch points
- Scale performance and services to meet any deployment needs

Product Highlights:



Adaptive Security Appliance



Integrated Services Router



Aggregation Services Router



Cisco Switch Security Modules

Endpoint Security

- Rich NAC and identity services
- Endpoint protection and control—host-based IPS and AV

Product Highlights:



CSA Desktop



CSA Server



NAC Appliance

Foundation of the Self-Defending Network: Network Security

Integrate
Advanced
Services

Advanced Technologies and Services

Malware Propagation

Automated Threat
Mitigation

Data Loss
Prevention

Endpoint Posture
Control

Dynamic DDoS
Mitigation

Application-Layer
Inspection

IPS

Security Point
Products

VPN

Firewall

Access Control

Content Security

Leverage
Existing
Infrastructure

IPS

IP Network

VPN

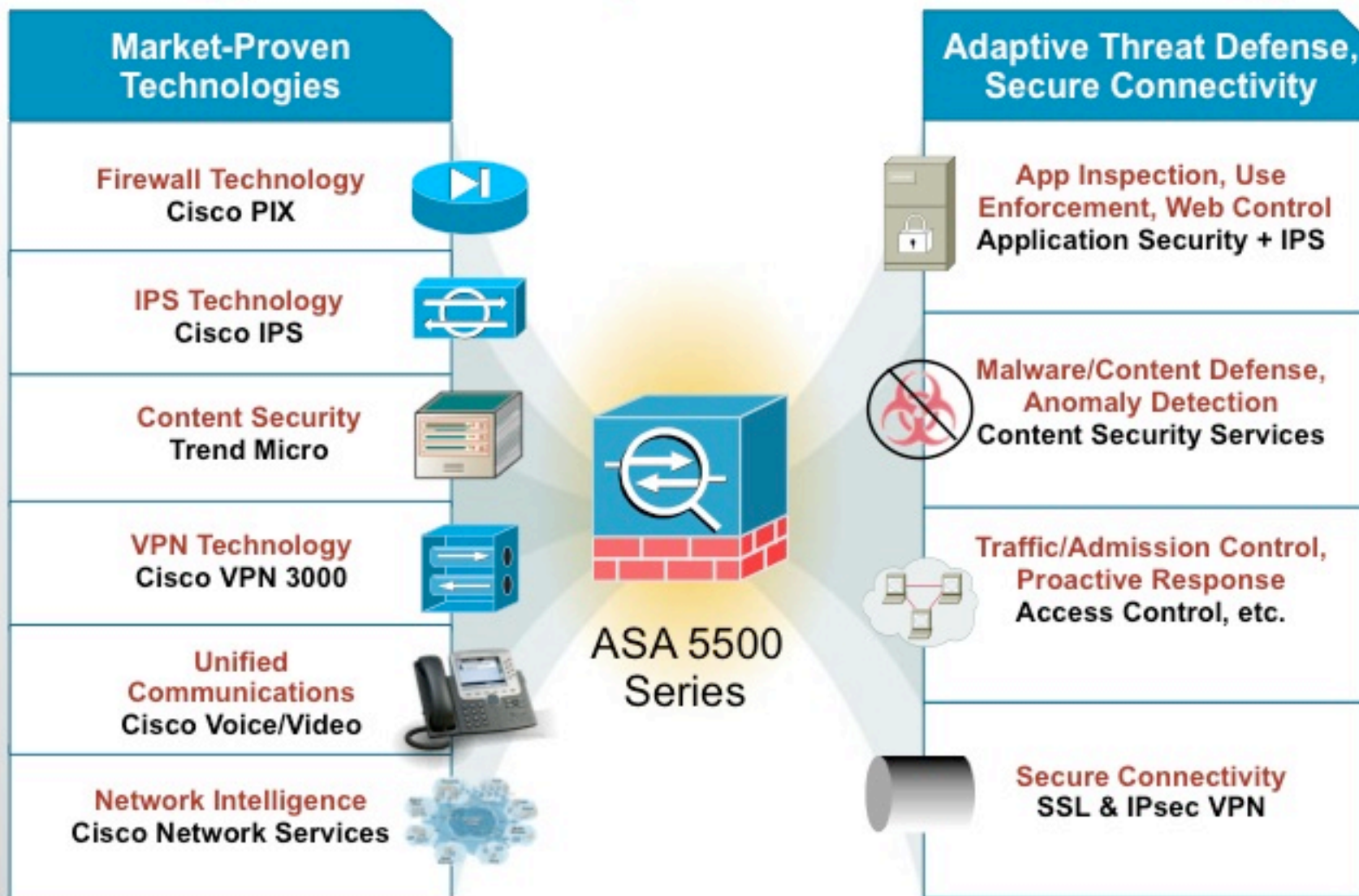
Firewall

Access Control

Content Security

Cisco ASA 5500 Series

Convergence of Robust, Market-Proven Technologies



Cisco Network Foundation Smart, Safe, and Strategic

Cisco IOS®



Embedded
Advanced Security



Video and
Content Modules



Voice Services



Networked
Storage



WLAN



High Performance,
Resilient, Flexible

Cisco Integrated Services Router

Security for the Branch/WAN



Secure Network Solutions



Business
Continuity



Secure
Voice



Secure
Mobility



Compliance

Integrated Threat Control



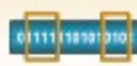
Advanced
Firewall



Content
Filtering



Intrusion
Prevention



Flexible
Packet
Matching



Network
Admission
Control



802.1x



Network
Foundation
Protection

Secure Connectivity



GET VPN



DMVPN



Easy VPN

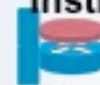


SSL VPN

Management and Instrumentation



SDM



Role-Based
Access



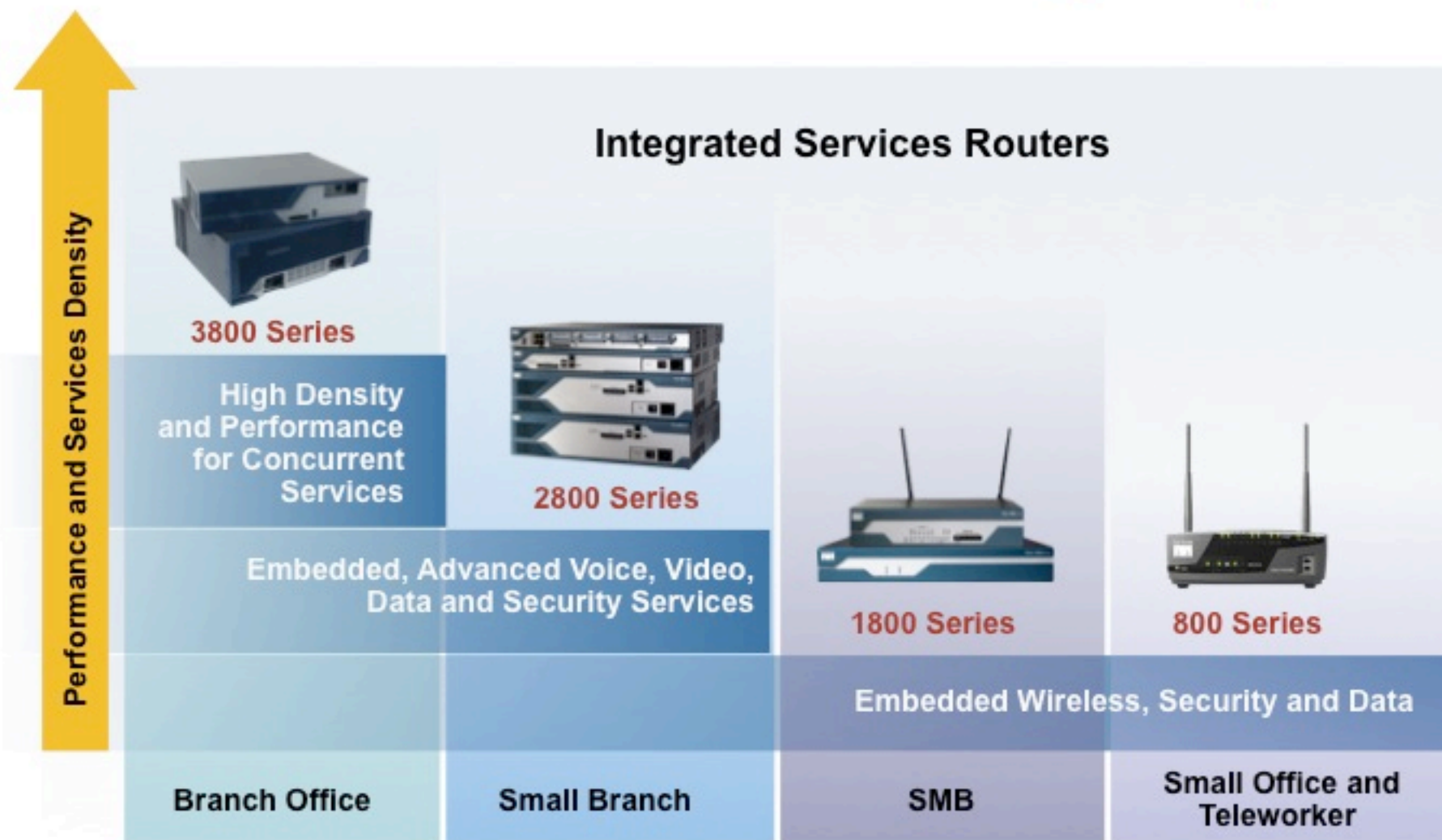
NetFlow



IP SLA

Cisco Integrated Services Router Portfolio

Scalable From Small Businesses to Large Enterprises



Cisco Catalyst 6500 Series Switch Security



Threat Defense



Defend the Edge:

Integrated FW/IPS
Service Module



Denial of Service Protection:

CoPP, CPU Rate Limiters,
Netflow, QoS



Protect the Interior:

Catalyst Integrated
Security Toolkit



Guard Against Infections and Worms:

Network Admissions Control (NAC)
Cisco Security Agent (CSA)



Defend Network Exploits:

Intrusion Protection System
(IPS)



Secure the Data in Transit:

IPSec VPN SPA

Trust and Identity



Identity-Based Networking

Control Who/What Has Access
Enforce endpoint Security Compliance

Secure Apps.

Deep Packet Inspection

Programmable Intelligent Service Accelerator (PISA)
Security and application intelligence

Catalyst 6500/7600 Integrated Services Platform



Firewall Service Module



Gigabit Network Analysis



SSL Service Module



Intrusion Detection Module



Content Switching Module



Communications
Media Module



Value-Added Services

Strengthens security, manageability, availability, and scalability in targeted places in the network

Lower Cost of Ownership

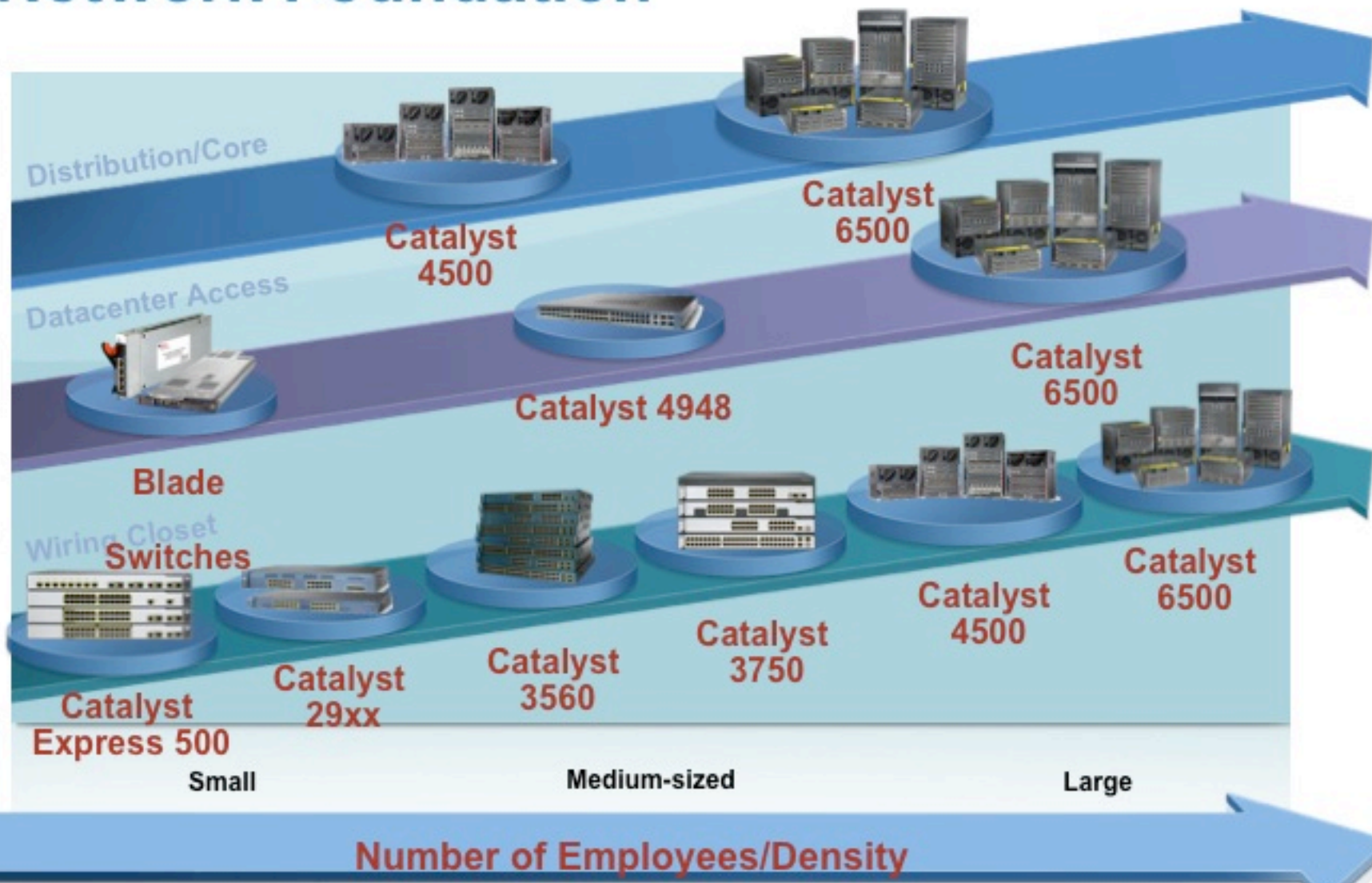
Reduced deployment, rack space, training, and management costs

Maximum Scalability

Sub-Gigabit to Multi-Gigabit performance ensures that service will scale as service demands increase

Switches for Cisco SMB Class Secure Network Foundation

Features, Scalability, Longevity



Cisco Security Agent

Server and Desktop Host-IPS

- Zero-update host-IPS and integrated antivirus
- Single client, single management interface
- Network collaboration with local threat remediation
- Identified and controls sensitive information



Business Benefits:

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

Cisco Network Admission Control (NAC)



Flexible Deployment

Layer 2, Layer 3
In-band, Out-of-band
Centralized, Distributed
SNMP, RADIUS

Innovative NAC Services

Posture Assessment
Remediation
Profiling
Guest

Features

- Role-based network access control and security policy compliance enforcement
- Full lifecycle: discovery, assessment, enforcement, and remediation

Benefits

- Securing both managed and unmanaged assets
- Providing guest access and preventing unauthorized access
- Reducing vulnerability-based exploits

The Portfolio at a Glance...

Content and Application Security

Content Security

- Reputation based, zero-day defense
- Capability to address diverse attacks types and techniques
- Secure all sources of attack

Product Highlights:



IronPort Email



IronPort Web



Intrusion Prevention Systems

Application Security

- Layer 7 protection for application and data vulnerabilities
- XML traffic validation and inspection
- Enhanced deep packet inspection

Product Highlights:



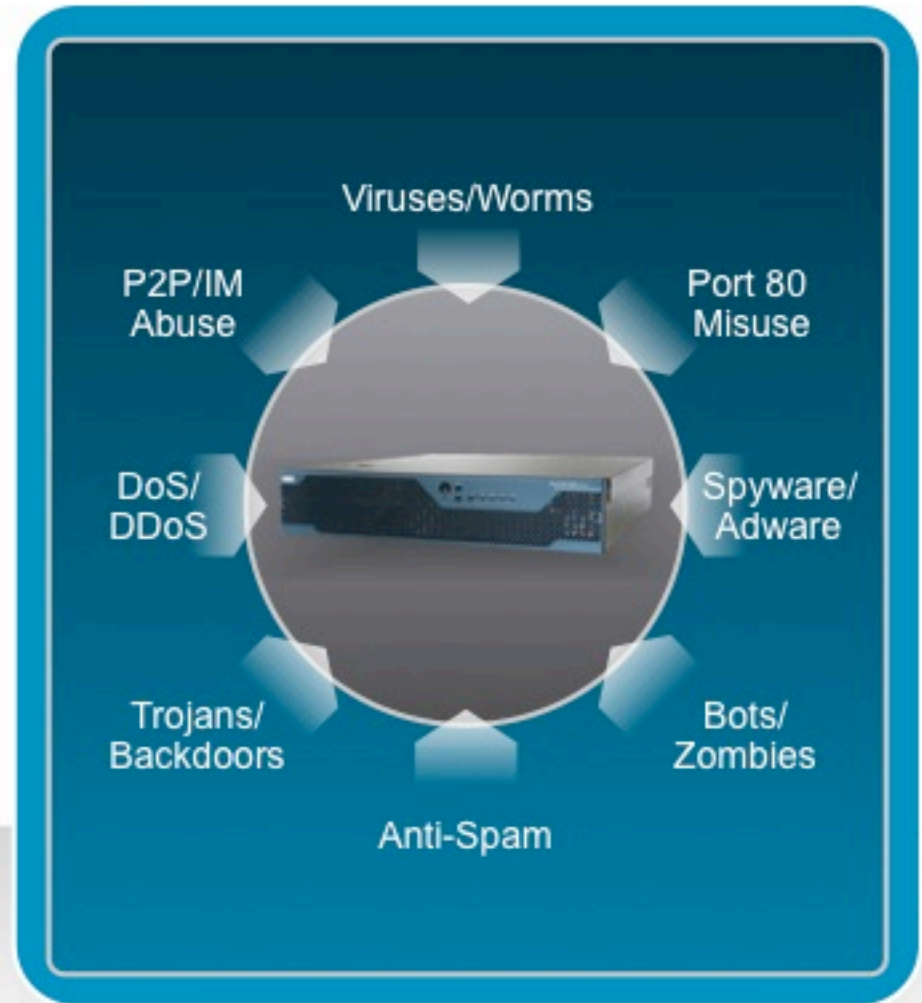
ACE XML Gateway



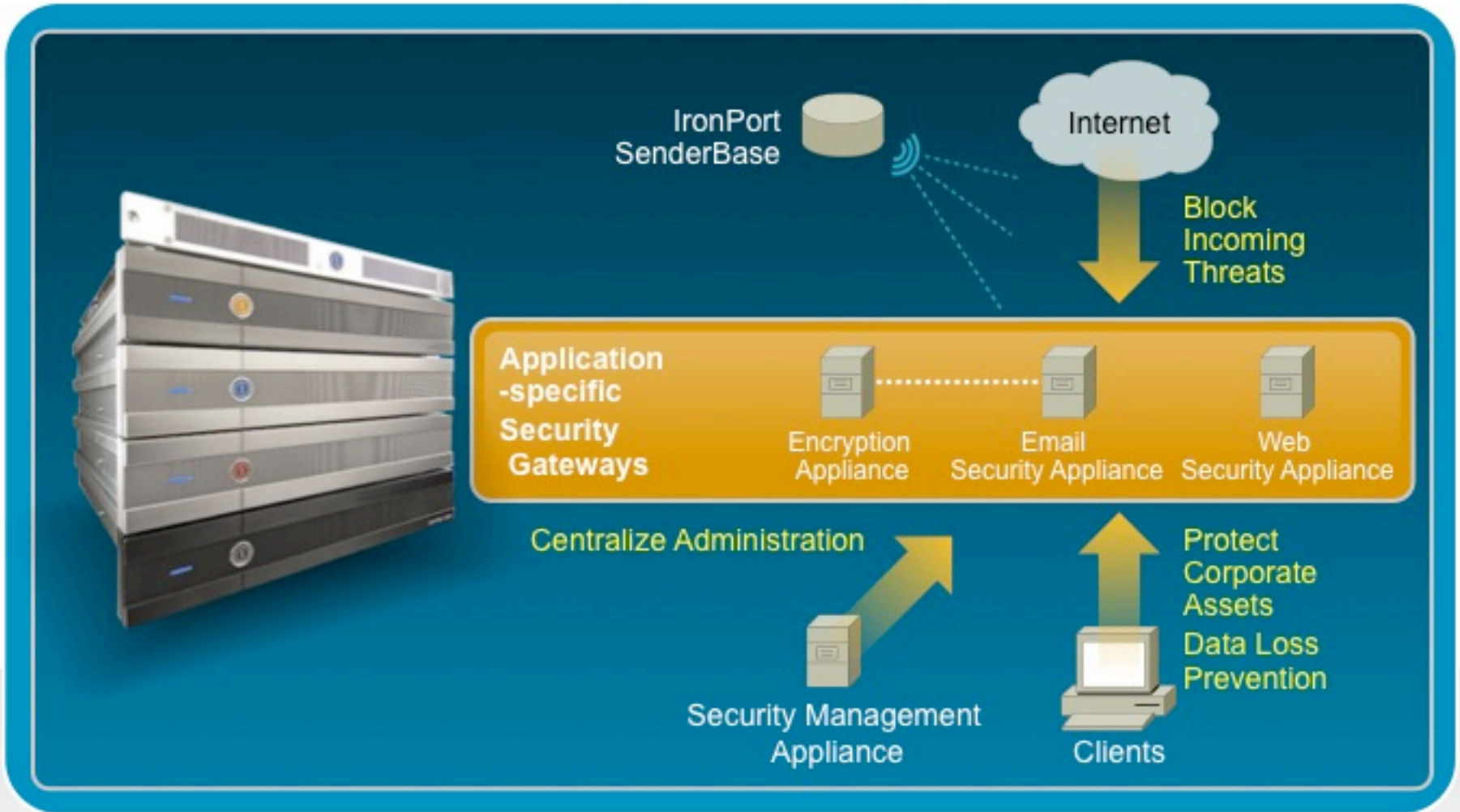
Web Application Firewall

Intrusion Prevention Systems

- Scans all traffic using deep (packet-level) inspection
- Accurate threat intelligence, which reduces false positives
- Coordinated response with existing network gear
- Application abuse: Inspects and controls IM, P2P, backdoor
- Trend Micro partnership: For latest breaking malware updates



IronPort Gateway Security Products



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

IronPort SenderBase

Real-Time Knowledge of Threat Environment

150 Parameters

- Complaint reports
- Spam traps
- Message composition data
- Global volume data
- URL lists
- Compromised host lists
- Web crawlers
- IP blacklists and whitelists
- Additional data

The Dominant Force in Global Email and Web Traffic Monitoring...

- 30B+ queries daily
- 150+ email and Web parameters
- 25% of the world's email traffic



SenderBase
Data



Data Analysis/
Security Modeling



SenderBase
Reputation Scores
-10 to +10

The Portfolio at a Glance...

Systems and Security Management

Security Management

- Operationalize security with automation to optimize resources
- Align monitoring and policy for a closed loop system
- Leverage identity information within the policy framework
- Provide comprehensive view for IT risk management

Product Highlights:



Cisco Security MARS



Cisco Security Manager



CiscoSecure ACS

Total Security System Management



Reduced complexity for more effective risk analysis and operational control

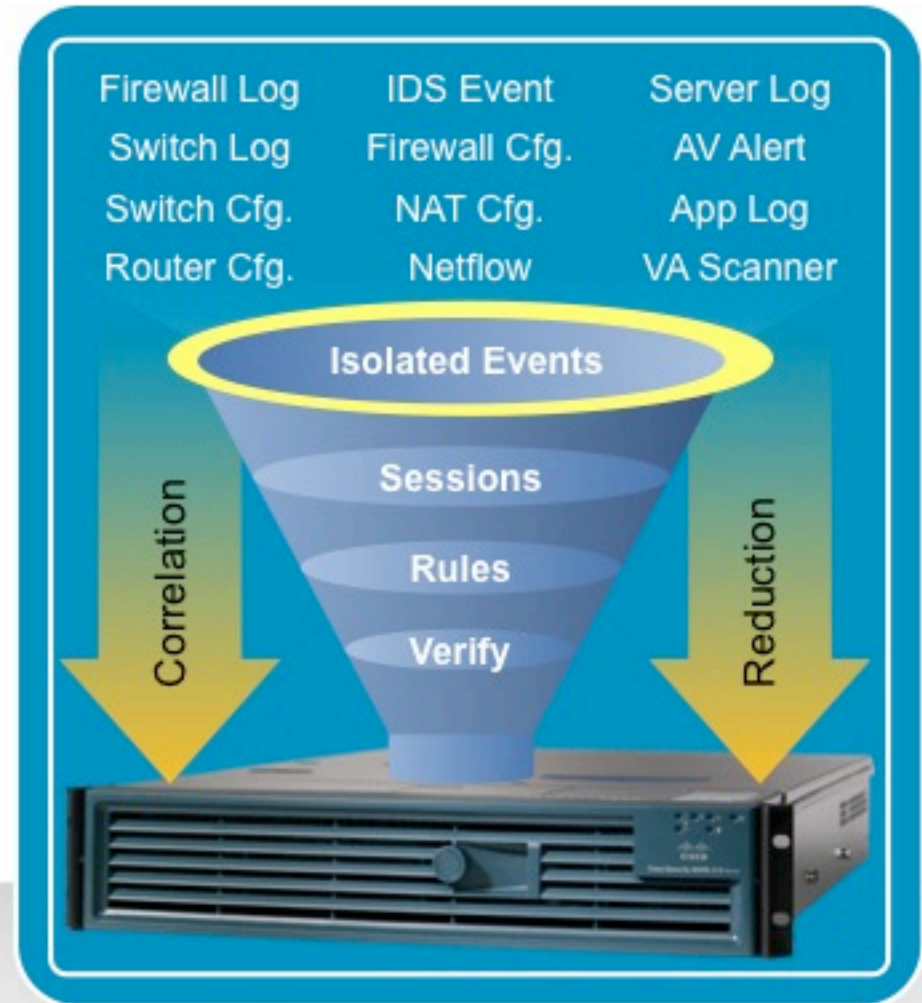
Cisco Security Manager



- Unified services management for security including firewall, VPN, and IPS
- Intuitive, feature-rich user interface
- Different views for different administrative preferences
 - Device View
 - Topology View
 - Policy View
- Efficient management architecture for large-scale security deployments

Cisco Security MARS

- MARS is an acronym = Monitoring, Analysis, and Response System
- Security threat mitigation appliance
- Rapid threat detection, isolation and mitigation, topologically aware
- Command and control for your existing network security
- Correlates data from across disparate multi-vendor security devices and applications



Cisco Secure ACS

Connecting All Elements of Your Network Identity



Pivotal Keystone for ID and Access Strategy

- Multiple authentication databases
- Posture, auditing and compliance

Powerful Robust Access Platform for All Sizes

- Scalable performance
- Compliance, accounting and audit

Trusted The World's #1 ID and Access System

- Over 100,000 units sold
- 94% overall customer satisfaction*

*Results of customer survey January 2008

Self-Defending Network Applied: Cisco Solution Architectures for Security

- PCI Compliance



PCI Applies to Nearly Every Industry



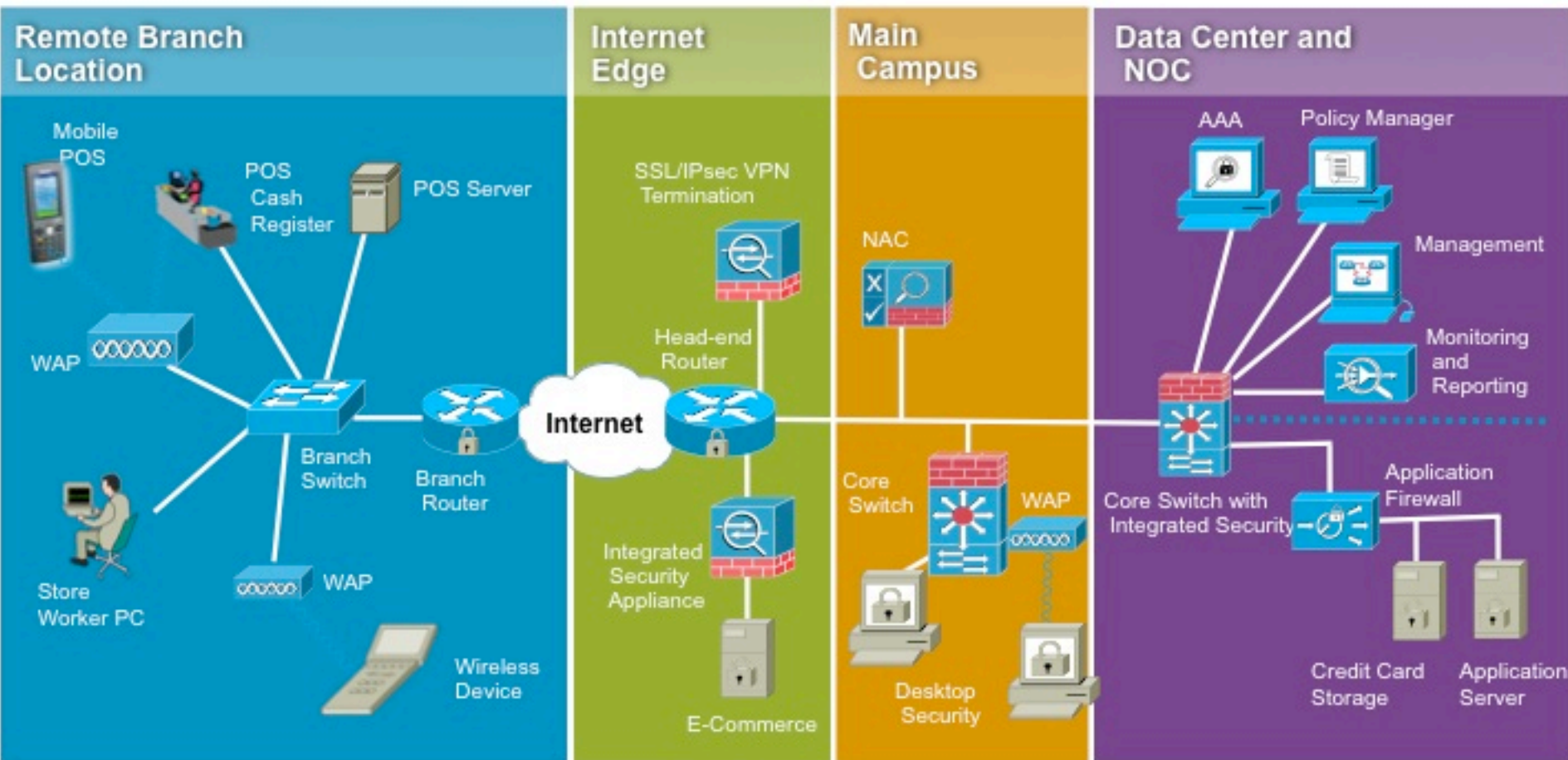
The Payment Card Industry (PCI) Data Security Standard

- Published January 2005
- Impacts ALL who **process, transmit, or store** cardholder data
- Also applies to 3rd-party hosting companies, information storage companies, etc.
- Monthly fines ranging from \$5,000 to \$50,000 for missed deadlines
- Has global reach**

Theater	Level 1	Level 2	Level 3
US	SEP 2007	DEC 2007	DEC 2008
Western Europe	Negotiated individually	MAR-DEC 2008	MAR-DEC 2008
Asia	DEC 2009	DEC 2009	DEC 2009
Canada	2008 TBD	2008 TBD	2008 TBD
Latin American CEMEA	Not Published yet		
CEMEA Americas Latin	Not Published yet		
CEMEA	2008 TBD	2008 TBD	2008 TBD

Source: pcisecuritystandards.org

Cisco Security Portfolio—Offers End-to-End Compliance with PCI Requirements



Confidentiality, Data Integrity, Availability, Auditing, and Reporting

Self-Defending Networks:

Solutions That Help You Business Minimize Risk

**Regulatory
Compliance**

ASA, CSA,
IPS, App FW,
CSM, MARS

CSA, IronPort,
NAC, Trustsec,
Securent,
ACS

Data Loss

A Systems Approach to Streamline IT Risk
Management for Security and Compliance

**Threat
Management**

IPS, CSA,
MARS, App
FW, Ironport



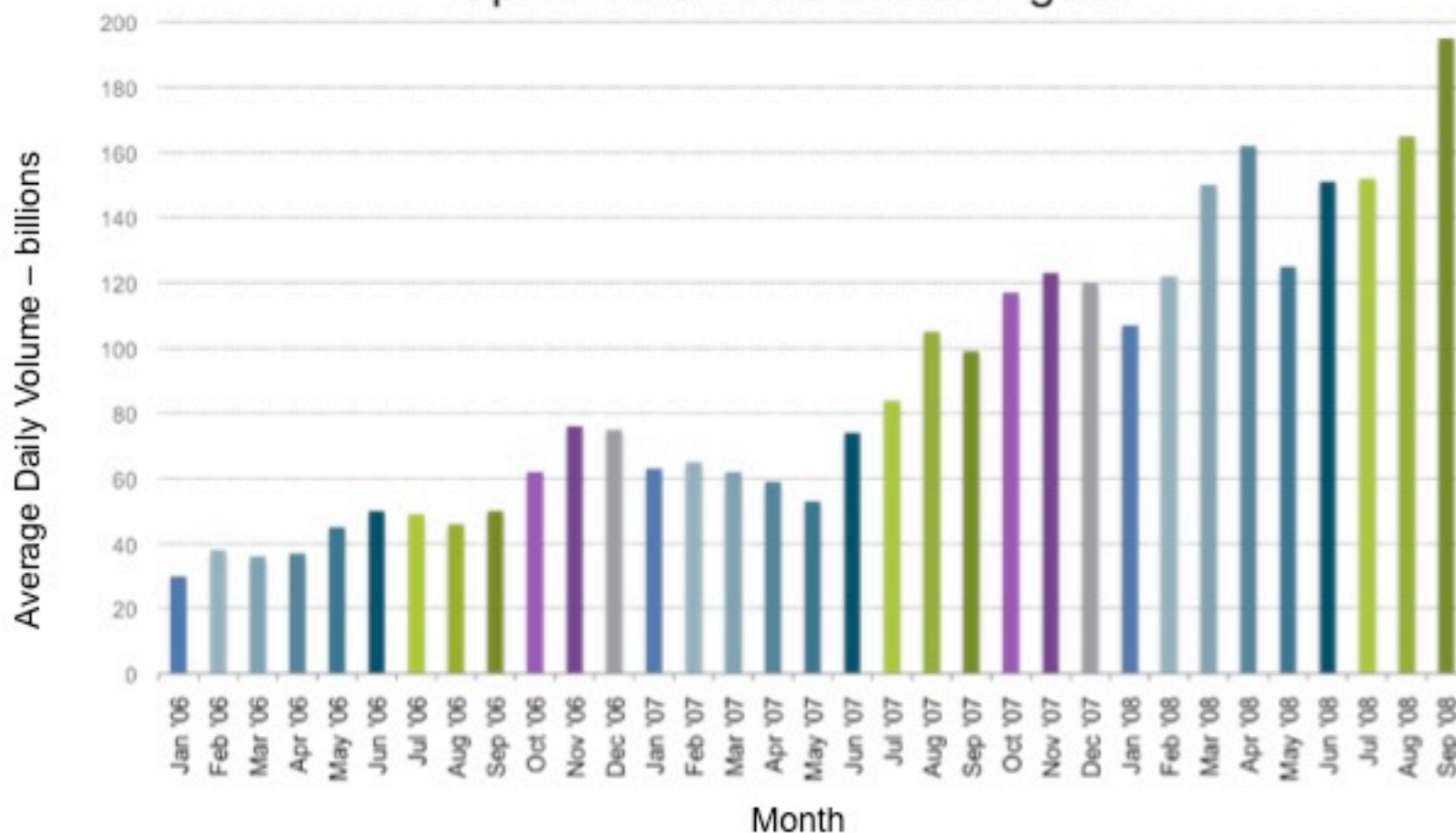
New SMB Security Product: Cisco Spam & Virus Blocker





Spam Trends Through September 2008

Spam Volumes Double - Again





Product Overview



The Cisco Spam & Virus Blocker is a dedicated email security appliance for small business with up to 250 email users.

It provides powerful protection against spam, viruses and other email threats to secure your network and business data while improving productivity.



Accurate



- Virtually eliminates spam, viruses, and other email threats
- Accurate protection right out of the box after initial setup
- Block non-business email
- Retains accuracy with continuous and automatic updates
- Stop spam and viruses and save productivity



Always Protected



- Continuous automatic security updates without admin intervention
- Automatic connection to and threat updates from the SenderBase® network
- Additional support from Threat Operation Center security experts
- Immediate response to new, emerging and evolving threats
- “Set it and forget it” approach eases administration





Easy Installation and Use



- Quick and easy installation into most networks within minutes
- Provides immediate protection out of the box once installed in network
- Automatic threat updates to the appliance with no intervention required
- Simple browser-based wizards support management and reporting
- Reduce operational costs of administration



Email



Internet



Firewall



Cisco Spam
& Virus
Blocker



Groupware
(Exchange, Notes,
Groupware)



Clients



Everything Included



- Appliance hardware
- Preinstalled appliance software
- Email user license
- Cisco Software and Support Subscription (yearly)
 - Includes automatic spam, virus, and threat updates
 - Software upgrades and new releases
 - Next business day hardware replacement
 - Technical support from Cisco Small Business Support Center





Peace of Mind



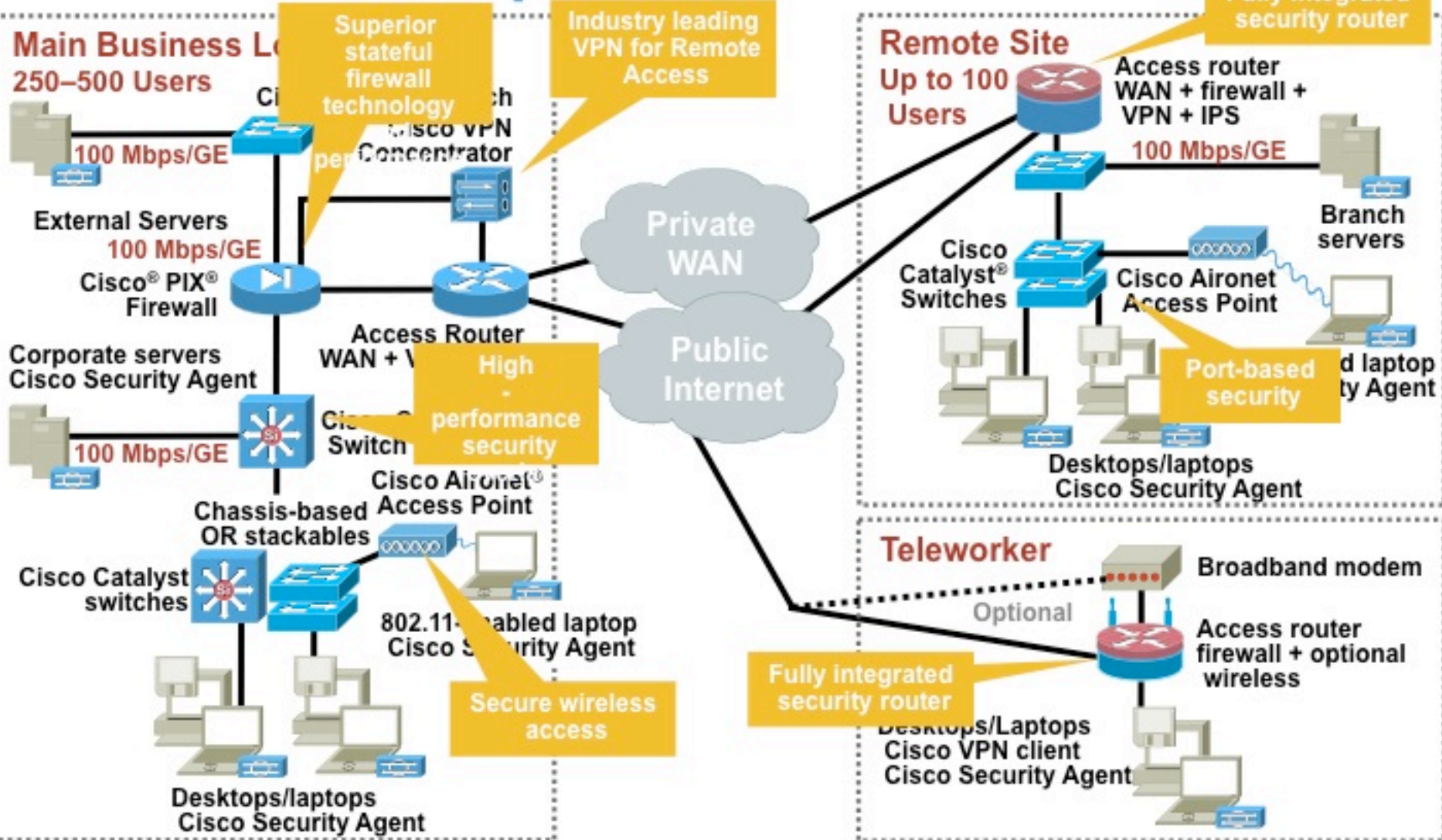
The Cisco Spam & Virus Blocker proves a “Set it. Forget it. It just works.” solution to protect your business and allow you to focus on your business.



Summary



Network Blueprint



Datacenter Security from Cisco.com



Worldwide [change] | [Log In](#) | [Register](#) | [About Cisco](#)

datacenter security

Go

[Solutions](#)

[Products & Services](#)

[Ordering](#)

[Support](#)

[Training & Events](#)

[Partner Central](#)

How Can We Help You?

Cisco offers business applications, products, and integrated solutions designed to empower retailers and transform the customer experience.

[> Learn More](#)



Learn about the solutions that matter most to the retail industry.



Information for:

- » [Small & Medium Business](#)
- » [Large Enterprise](#)
- » [Service Provider](#)
- » [Home & Home Office](#)

Quick Links

- [Partner Locator](#)
- [Find a Service Provider](#)
- [Security Center](#)
- [Documentation](#)
- [Career Opportunities](#)
- [RSS Feeds](#)
- [Investor Relations](#)
- [Discussion Forums](#)

Recommended Results

[Cisco Security Center](#)

<http://www.cisco.com/cisco/security/center/home.x>

[Enterprise Data Center - Solutions](#)

The Data Center Network Architecture evolves the network into a platform that enhances the application, server, and storage solutions.

http://www.cisco.com/en/US/netsol/ns340/ns394/ns224/networking_solutions_packages_list.html

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 1992-2007 Cisco Systems Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Recommended Reading

- Continue your event learning experience with further reading for this session from Cisco Press®
- Check out - Self Defending Networks: The Next Generation of Network Security

Available at www.ciscopress.com

