Contrer les menaces Internet avec les Solutions de Sécurité Email et Web de Cisco

Frédéric HER – Senior Systems Engineer

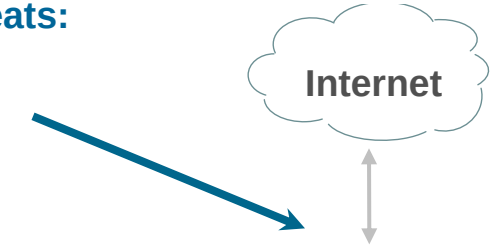
© 2010 Cisco and/or its affiliates. All rights reserved.

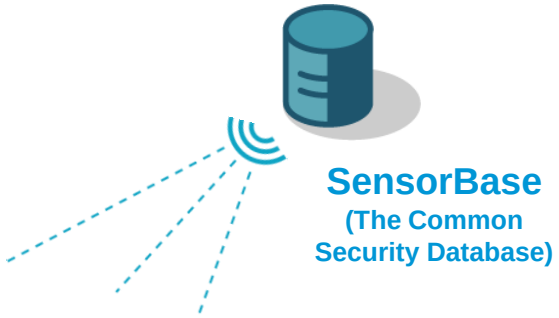
The Cisco IronPort Story

Application-Specific Security Gateways

BLOCK Incoming Threats:

- **Spam, Phishing/Fraud**
- **Viruses, Trojans, Worms**
- **Spyware, Adware**
- **Unauthorized Access**





SensorBase
(The Common Security Database)

APPLICATION-SPECIFIC SECURITY GATEWAYS

EMAIL
Security Gateway

WEB
Security Gateway

SECURITY MANAGEMENT
Appliance

© 2010 Cisco and/or its affiliates. All rights reserved.

Gartner Magic Quadrant

Email Security, 2010

The Magic Quadrant is copyrighted 2009 by Gartner, Inc. and is reused with permission. The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period. It depicts Gartner's analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor product or service depicted in the Magic Quadrant, and does not advise technology users to select only those vendors placed in the "Leaders" quadrant. The Magic Quadrant is intended solely as a research tool, and is not meant to be a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

This Magic Quadrant graphic was published by Gartner, Inc. as part of a larger research note and should be evaluated in the context of the entire report. The Gartner report is available upon request from Cisco.

© 2010 Cisco and/or its affiliates. All rights reserved.

Gartner Magic Quadrant

Secure Web Gateway, 2010

The Magic Quadrant is copyrighted 2009 by Gartner, Inc. and is reused with permission. The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period. It depicts Gartner's analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor product or service depicted in the Magic Quadrant, and does not advise technology users to select only those vendors placed in the "Leaders" quadrant. The Magic Quadrant is intended solely as a research tool, and is not meant to be a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

This Magic Quadrant graphic was published by Gartner, Inc. as part of a larger research note and should be evaluated in the context of the entire report. The Gartner report is available upon request from Cisco.

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco IronPort Email Security

© 2010 Cisco and/or its affiliates. All rights reserved.

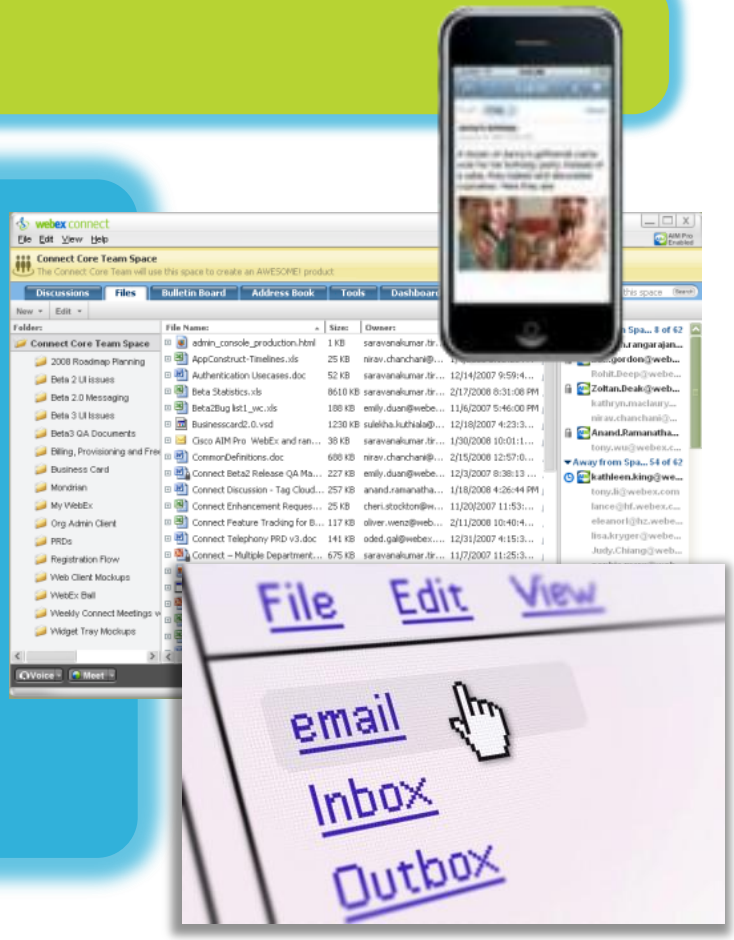
Business Collaboration Tools

Email remains the workhorse

Email #1 Business Collaboration Tool

FACTS

	TODAY	2013
Email Users	1.4 B	1.9 B
Email Traffic	247 B	507 B



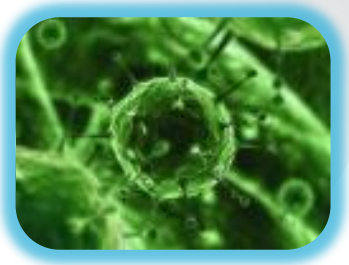
© 2010 Cisco and/or its affiliates. All rights reserved.

Email Challenges

Standard Email does not natively offer what is expected

Junk Mail

Privacy & Control

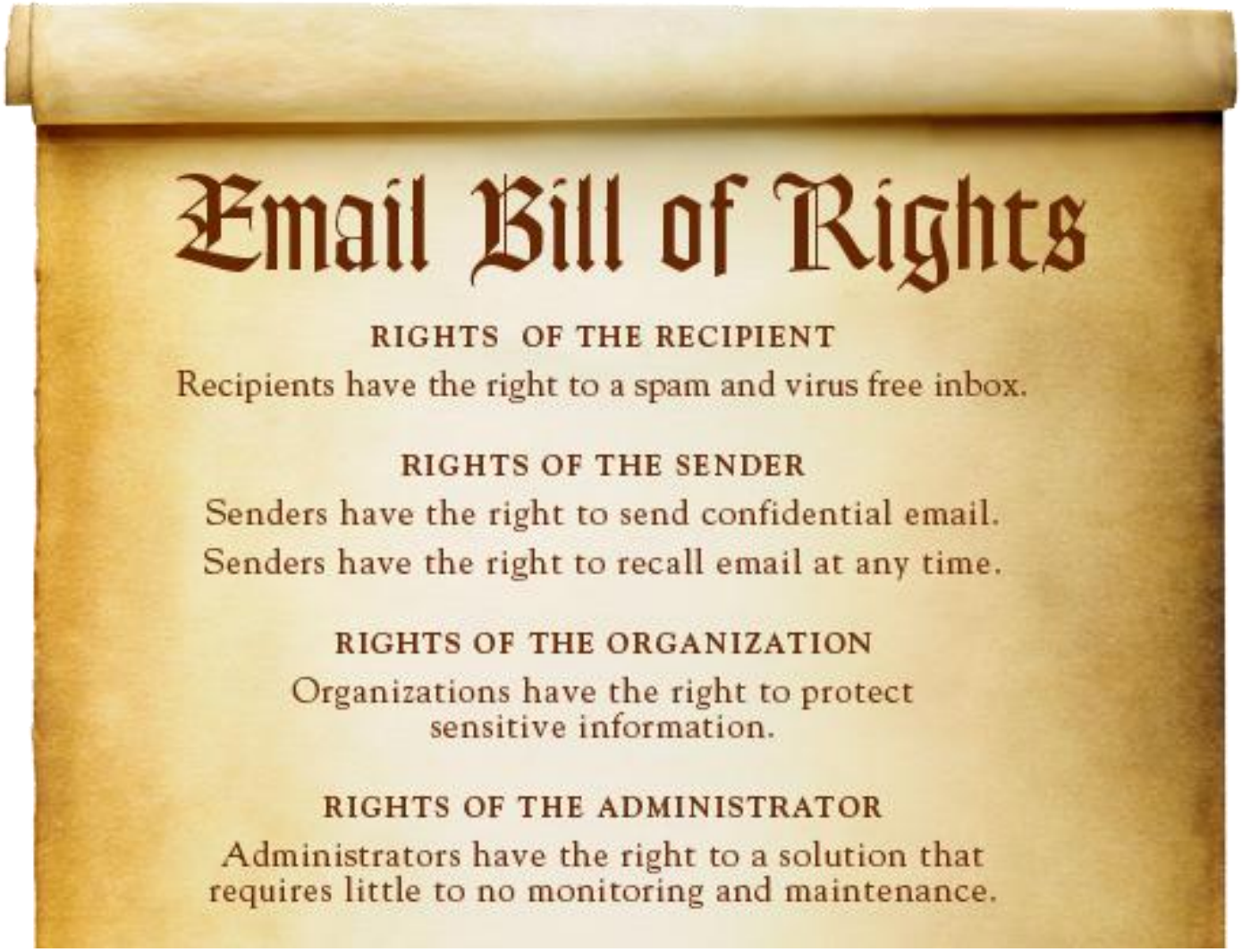


Viruses

Regulations

© 2010 Cisco and/or its affiliates. All rights reserved.

Email Bill of Rights

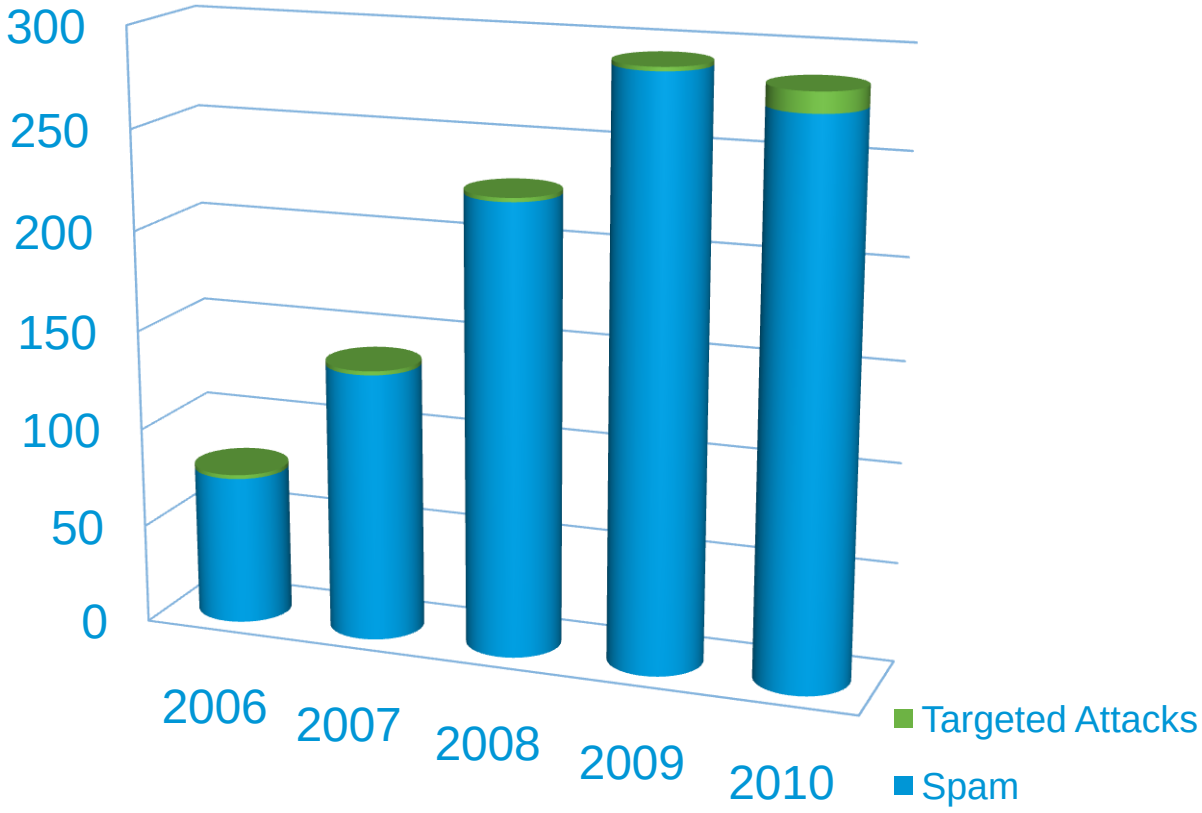


© 2010 Cisco and/or its affiliates. All rights reserved.

Email Security Threats

More and more targeted attacks

Daily Spam Volume (Billion)



Source: Cisco Threat Operations Center

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco IronPort SensorBase

- **Statistics on more than 30%** of the world's e-mail traffic
- New threats & alerts detection
- More than **200 parameters** to build reputation scores

- *Data Volume*
- *Message Structure*
- *Complaints*
- *Blacklists, whitelists*
- *Off-line data*

E-Mail Reputation Filters → **Reputation Score**

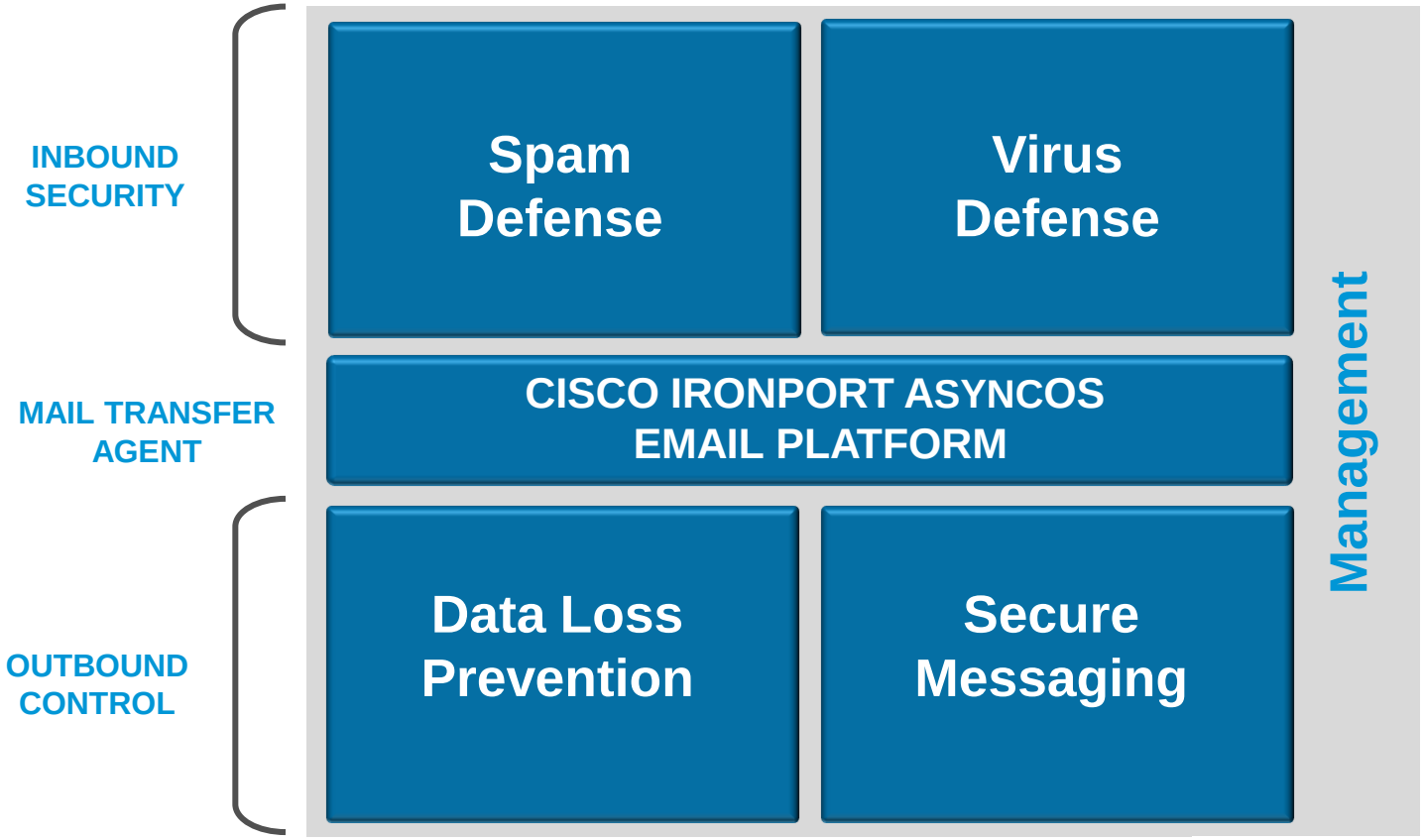
- *URL blacklists & whitelists*
- *HTML Content*
- *Domain Info*
- *Known "bad" URLs*
- *Website history…*

Web Reputation Filters → **Reputation Score**

© 2010 Cisco and/or its affiliates. All rights reserved.

Email Security Architecture

Cisco IronPort Email Security Appliance

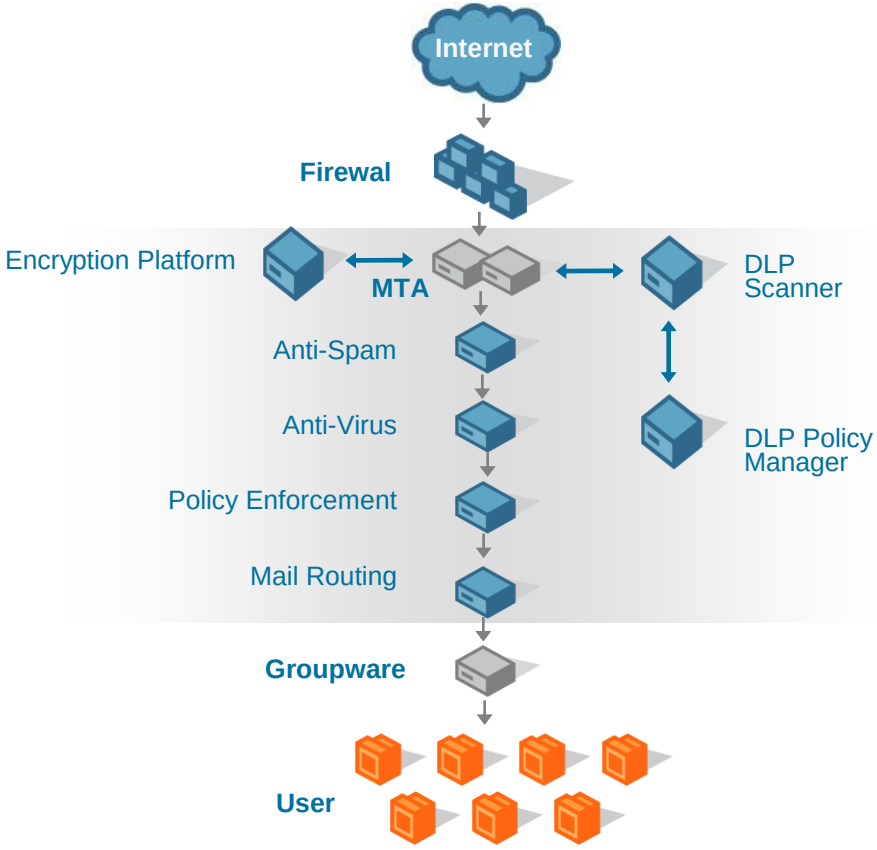


© 2010 Cisco and/or its affiliates. All rights reserved.

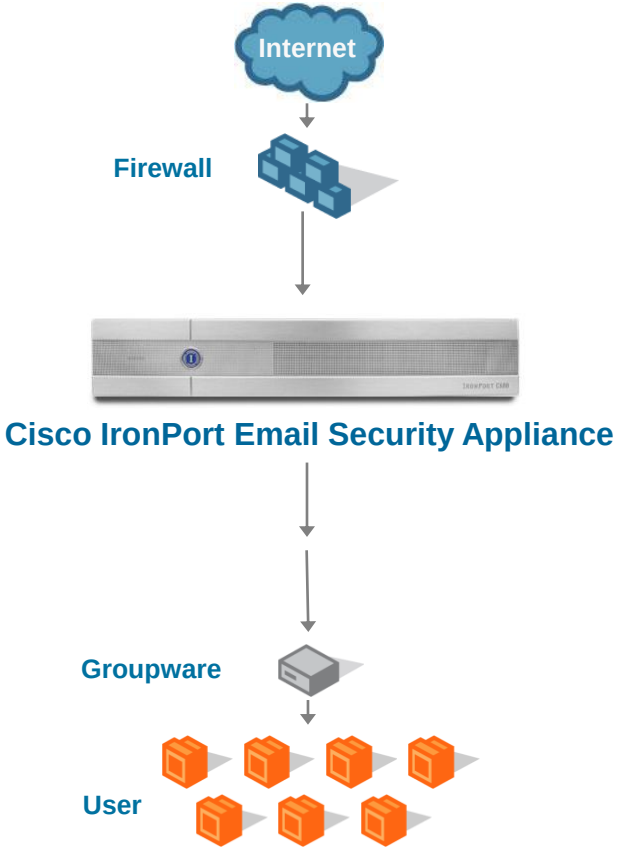
Cisco IronPort Consolidates the Network Perimeter

For Security, Reliability and Lower Maintenance

Before Cisco IronPort

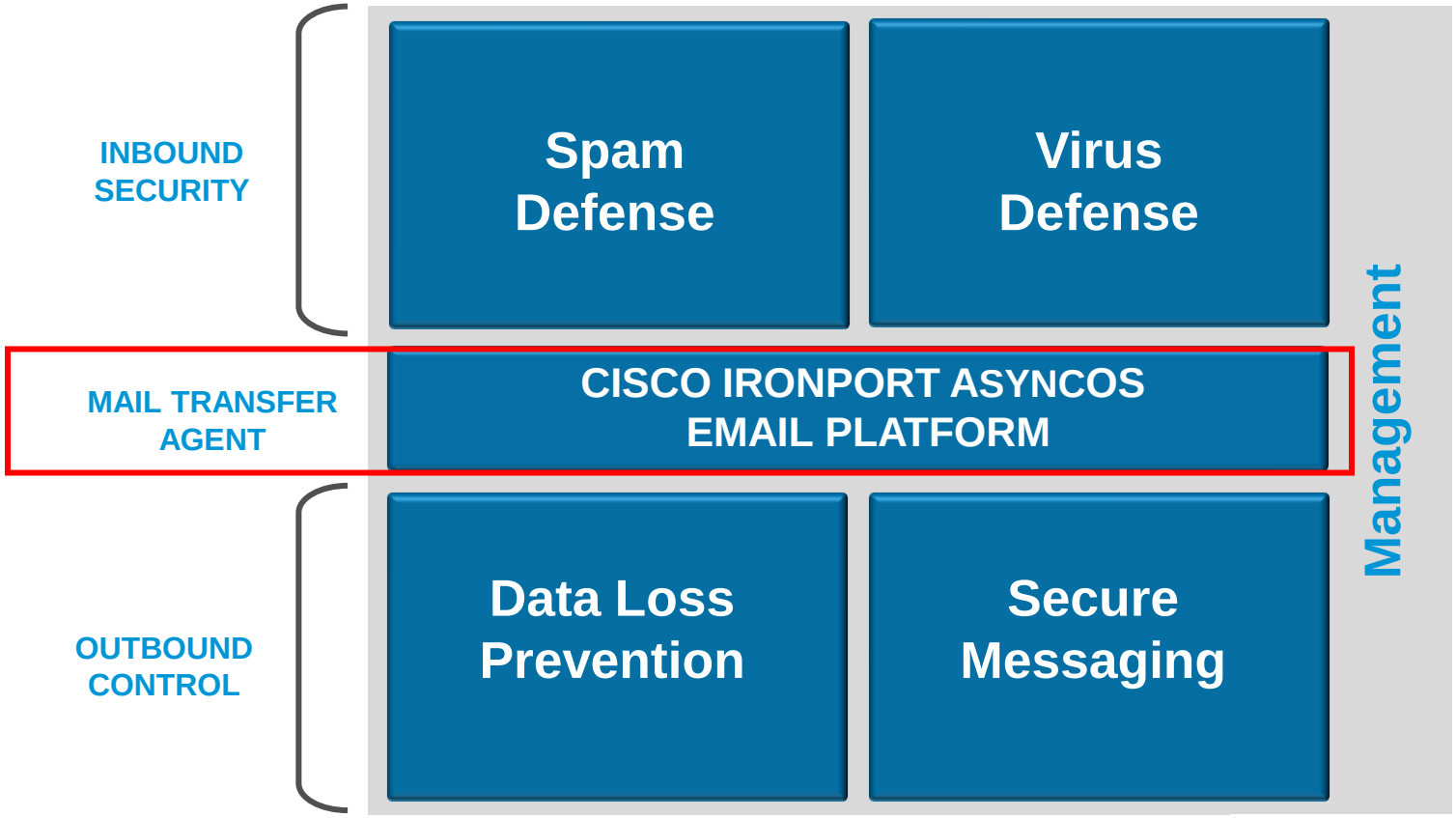


After Cisco IronPort



Email Security Architecture

Cisco IronPort Email Security Appliance



© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco IronPort AsyncOS

Revolutionary Email Delivery Platform

Traditional Email Gateways and Other Appliances

Cisco IronPort Email Security Appliances

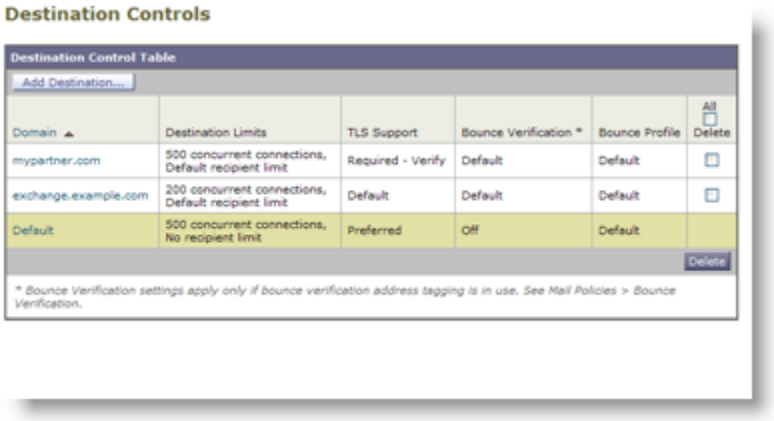
200 Connections	→ Low Performance/ Peak Delivery Issue	**1K – 10K** Connections	→ High Performance/ Sure Delivery
Disk I/O Bottlenecks	→ Unable To Leverage Full Capability Components	**CPU**	→ Limited Solely By CPU Capacity

© 2010 Cisco and/or its affiliates. All rights reserved.

Advanced Controls for Security and Efficiency

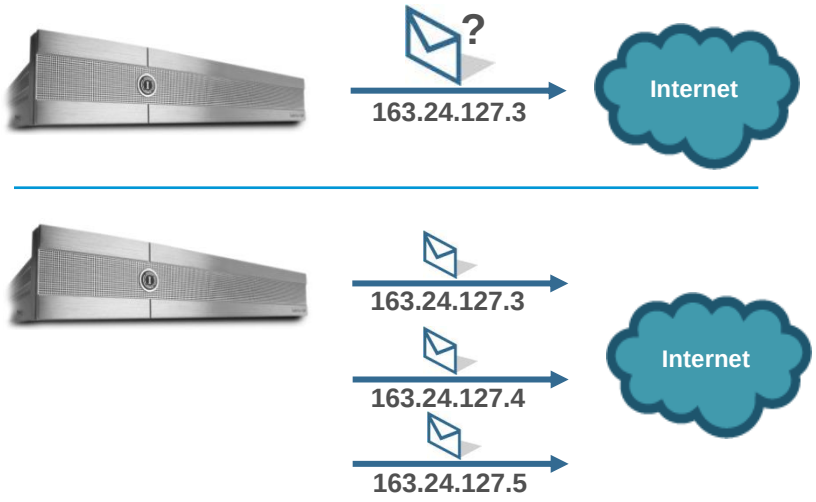
And to protect against the risk of being blacklisted

Destination Controls



- Protect internal servers
- Rules per destination domain

Virtual Gateways



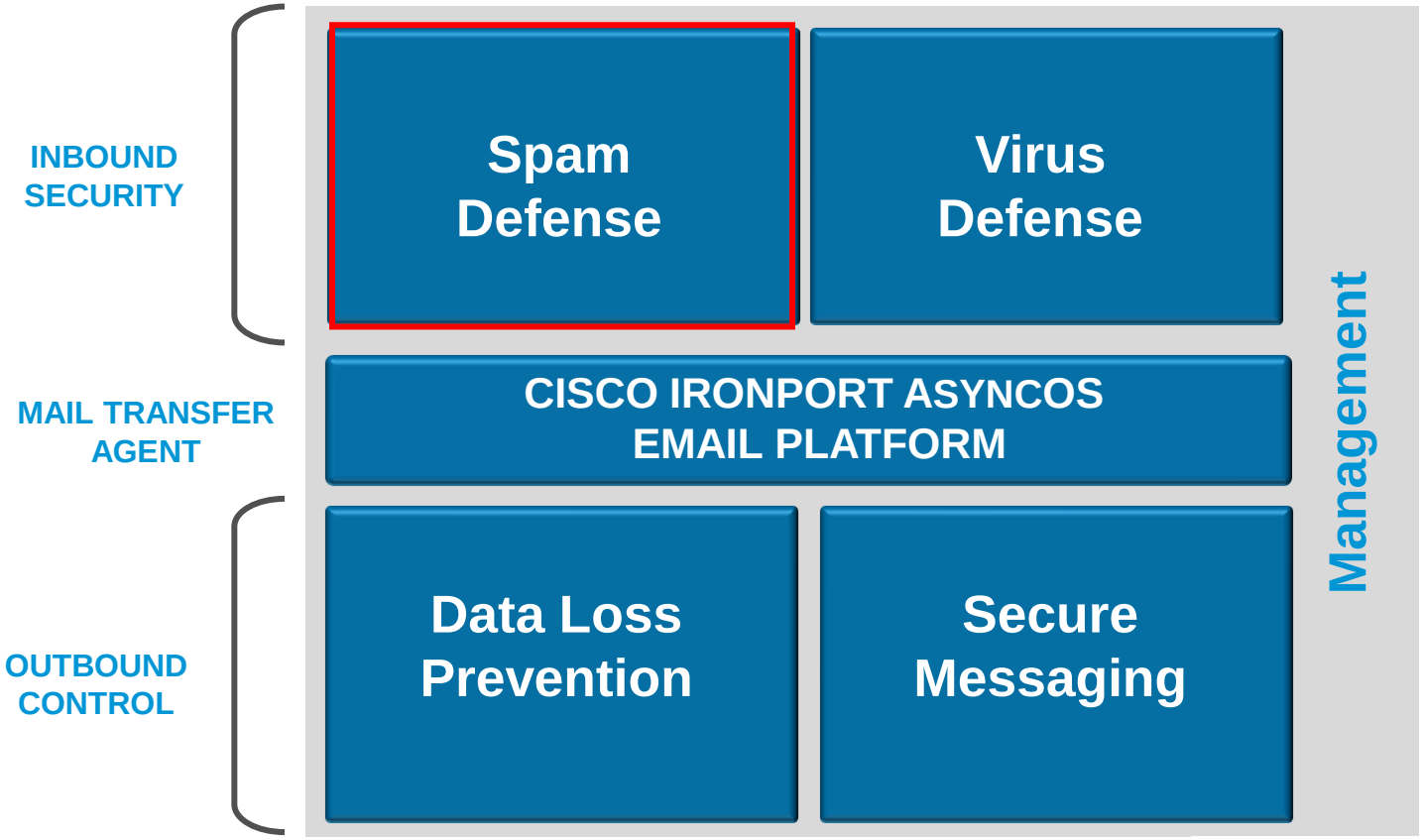
- Protects the reputation of a domain
- Relies on different IP addresses for sending messages

Email Authentication (DomainKeys, DKIM, SPF, SIDF)

© 2010 Cisco and/or its affiliates. All rights reserved.

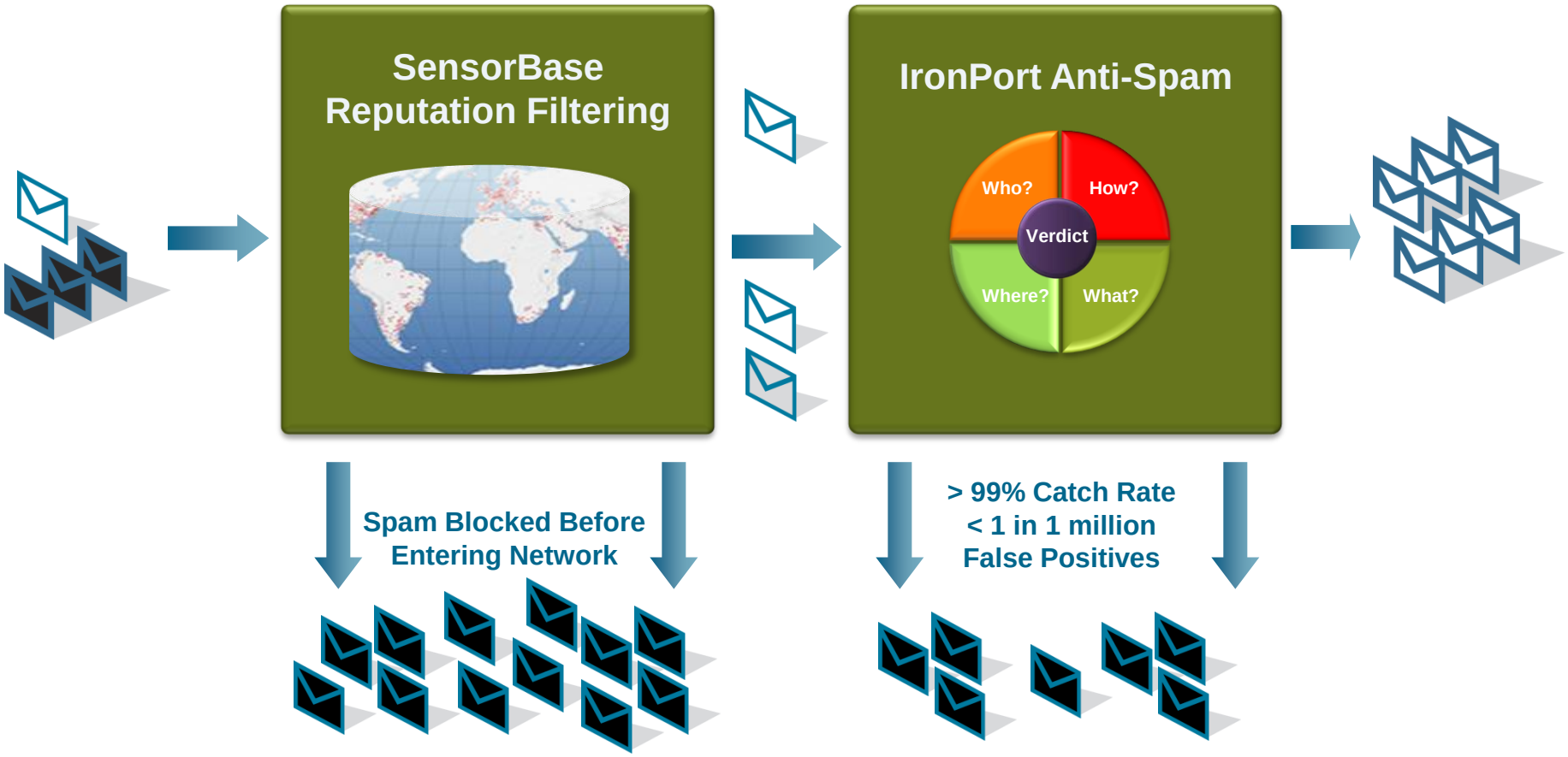
Email Security Architecture

Cisco IronPort Email Security Appliance



© 2010 Cisco and/or its affiliates. All rights reserved.

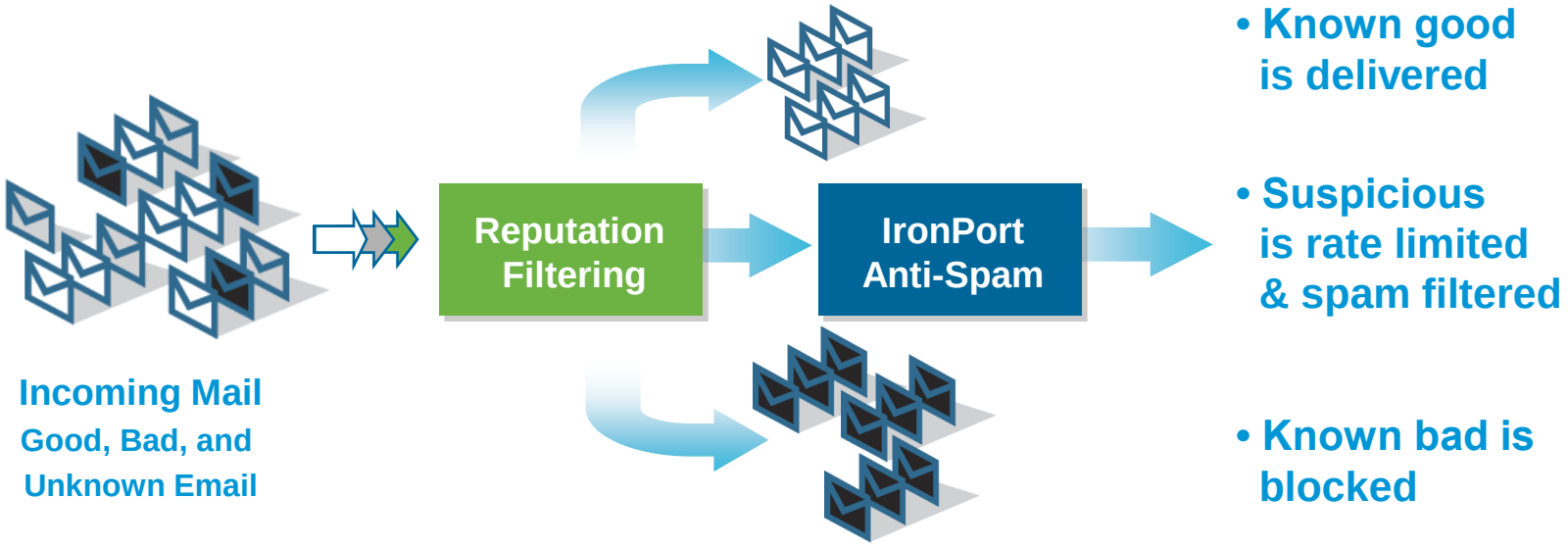
Anti-Spam Defense in Depth



© 2010 Cisco and/or its affiliates. All rights reserved.

SensorBase Reputation Filtering

Real Time Threat Prevention



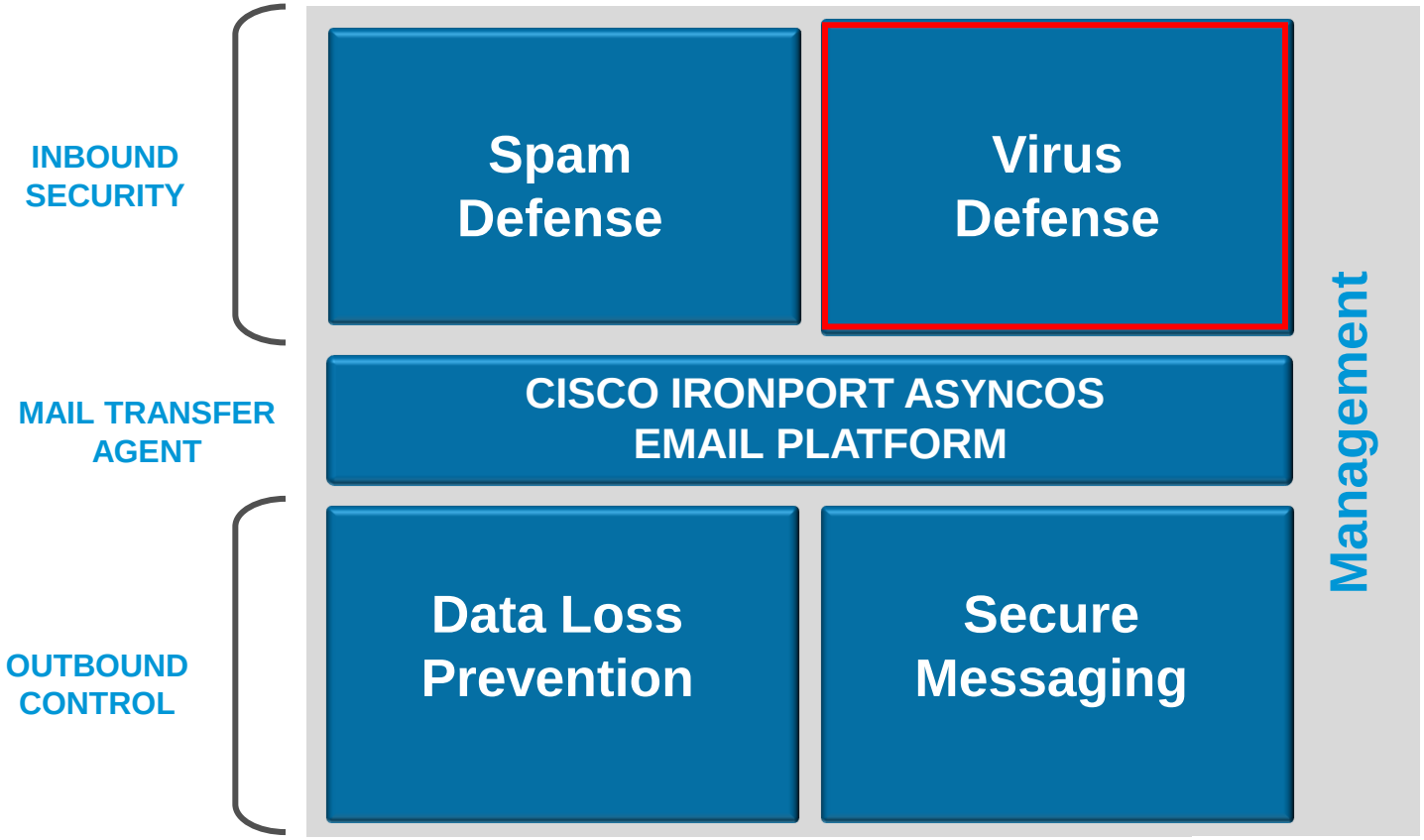
Cisco's Internal Email Experience:

Message Category	%	Messages
Stopped by Reputation Filtering	**93.1%**	700,876,217
Stopped as Invalid recipients	0.3%	2,280,104
Spam Detected	2.5%	18,617,700
Virus Detected	0.3%	2,144,793
Stopped by Content Filter	0.6%	4,878,312
Total Threat Messages:	**96.8%**	**728,797,126**
Clean Messages	3.2%	24,102,874
Total Attempted Messages:		**752,900,000**

© 2010 Cisco and/or its affiliates. All rights reserved.

Email Security Architecture

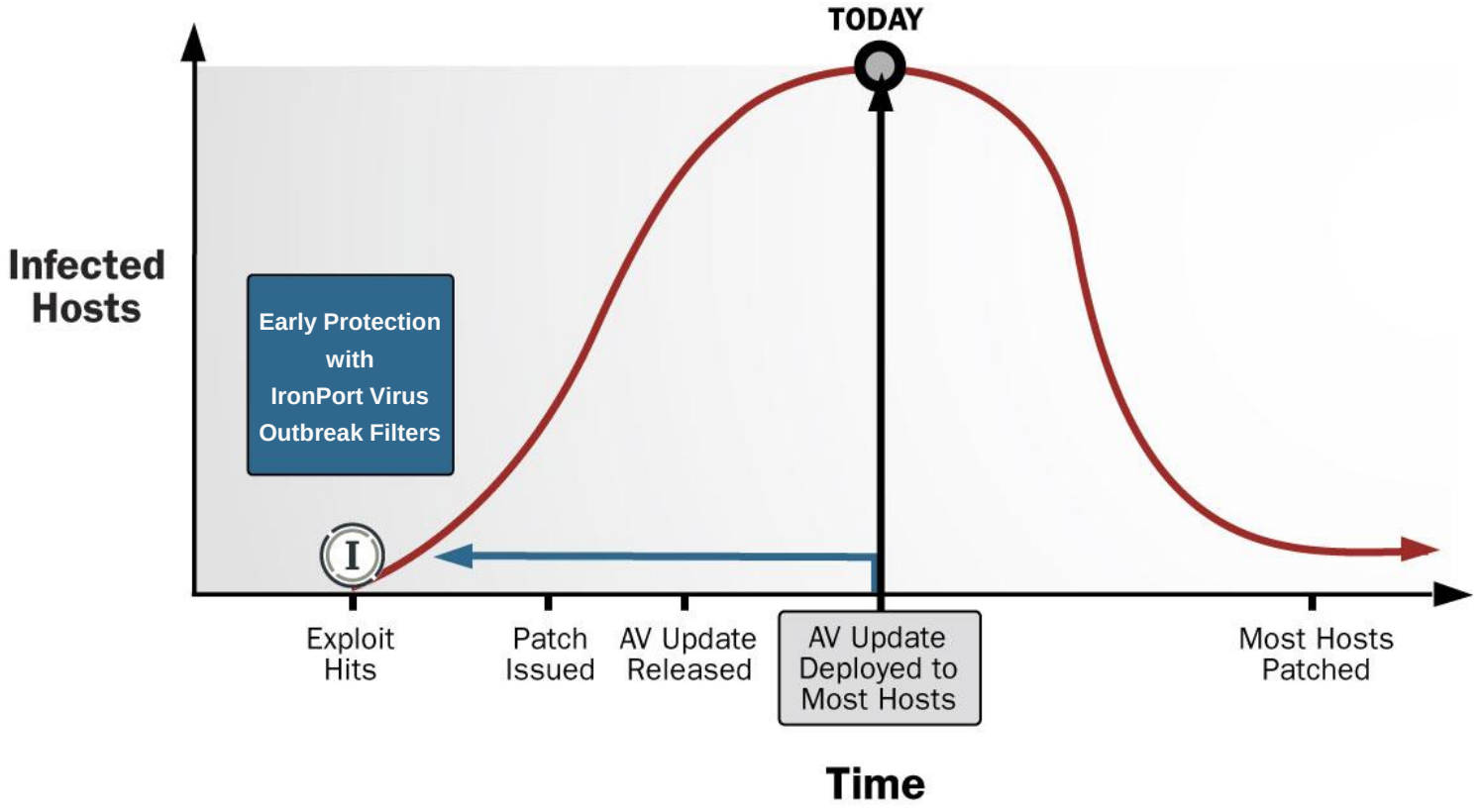
Cisco IronPort Email Security Appliance



© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco IronPort Virus Outbreak Fliters

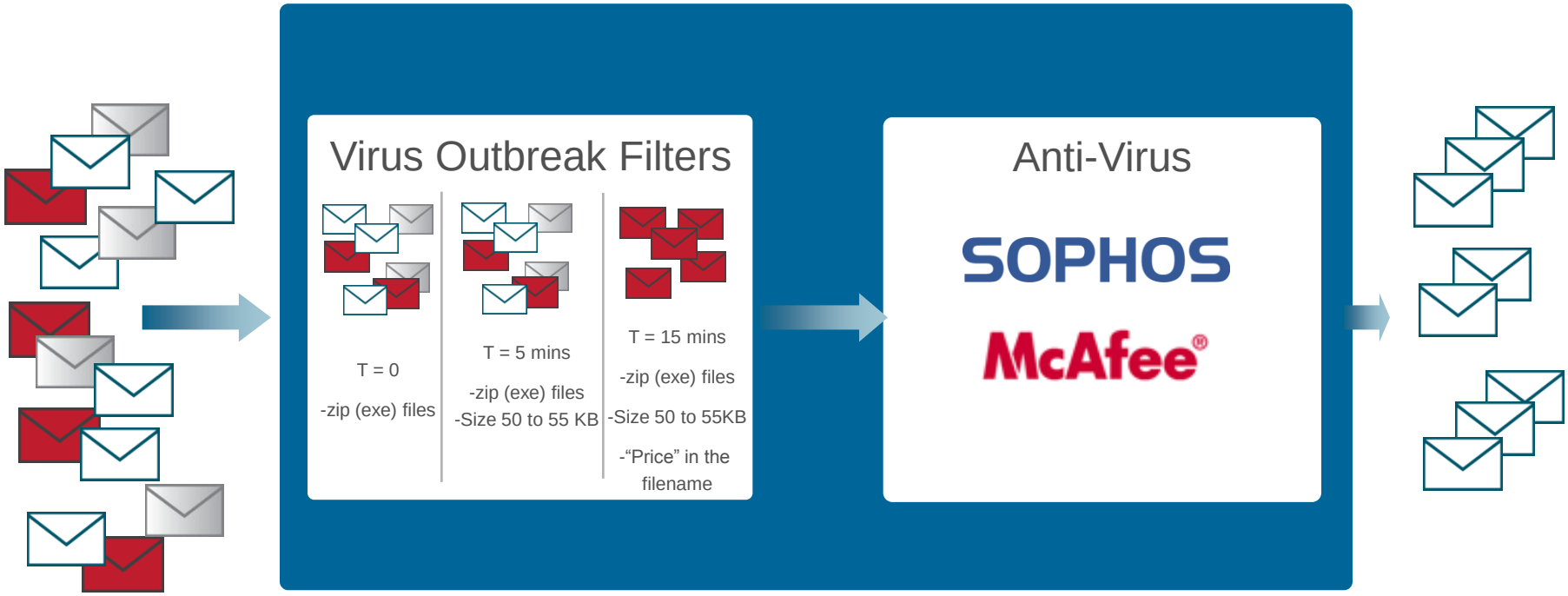
The First Line of Defense



© 2010 Cisco and/or its affiliates. All rights reserved.

Multi-Layer Virus Defense

Zero Hour Malware Prevention and AV Scanning



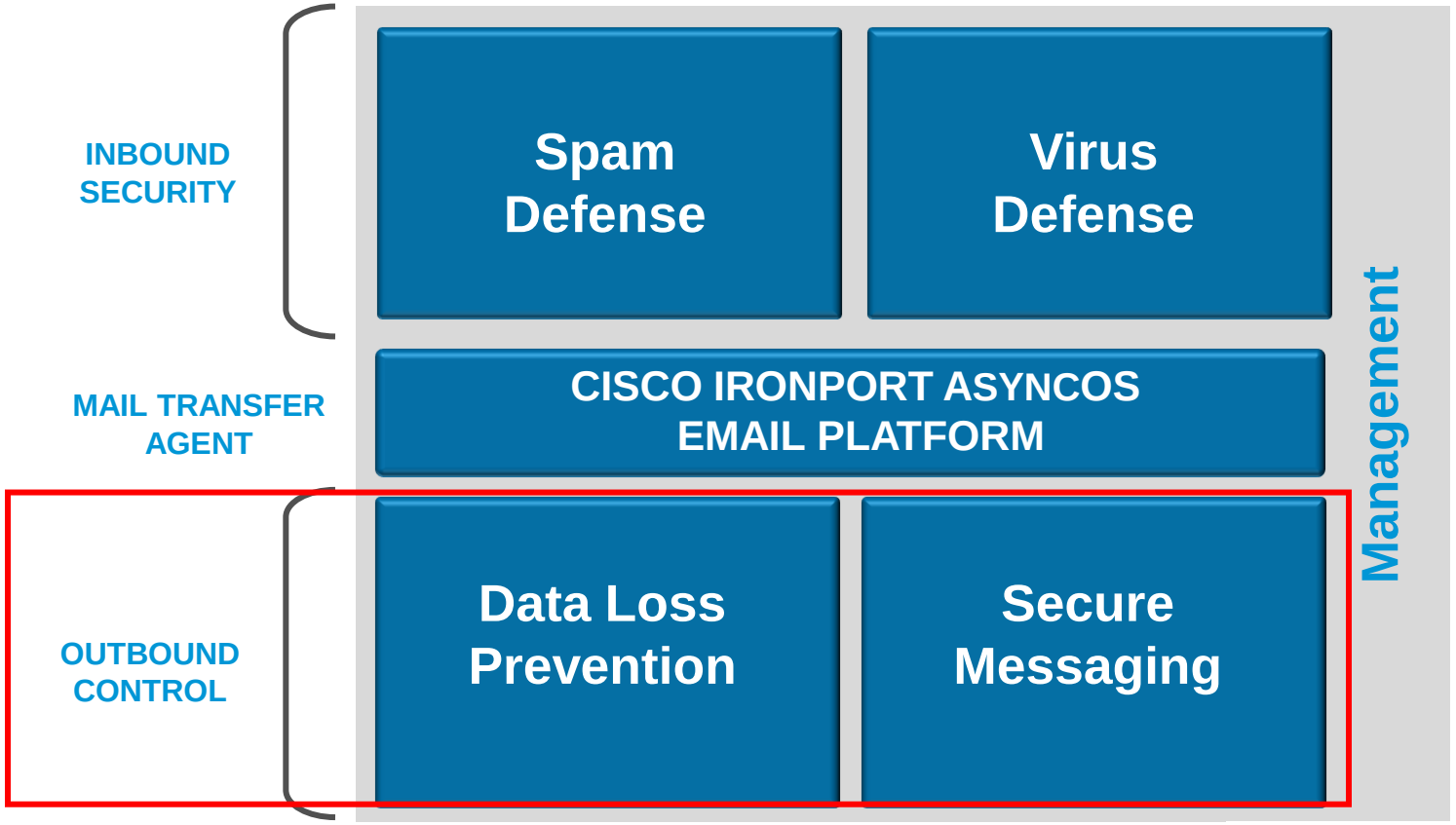
An analysis over one year:

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

© 2010 Cisco and/or its affiliates. All rights reserved.

Email Security Architecture

Cisco IronPort Email Security Appliance



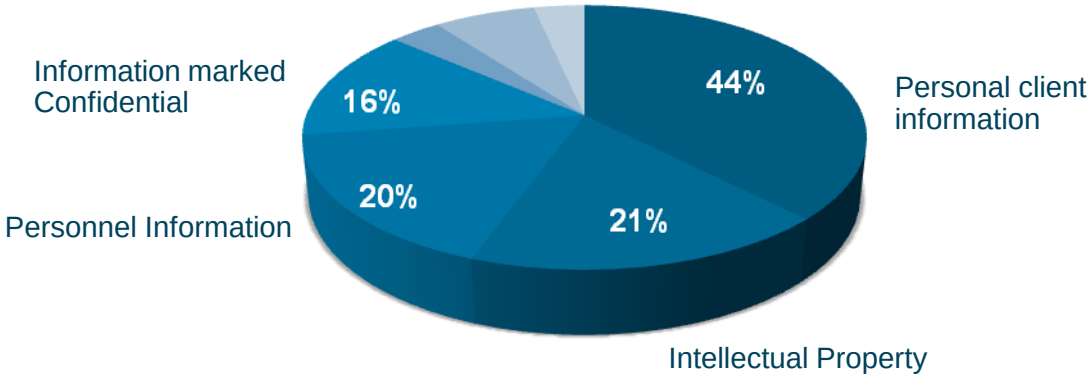
© 2010 Cisco and/or its affiliates. All rights reserved.

Risks for the Organization

Top Risk: Employees

Biggest Impact: Customer Data

Top Data Loss Types



© 2010 Cisco and/or its affiliates. All rights reserved.

Data Loss Prevention

Comprehensive, Accurate, Easy

RSA SECURITY

Comprehensive

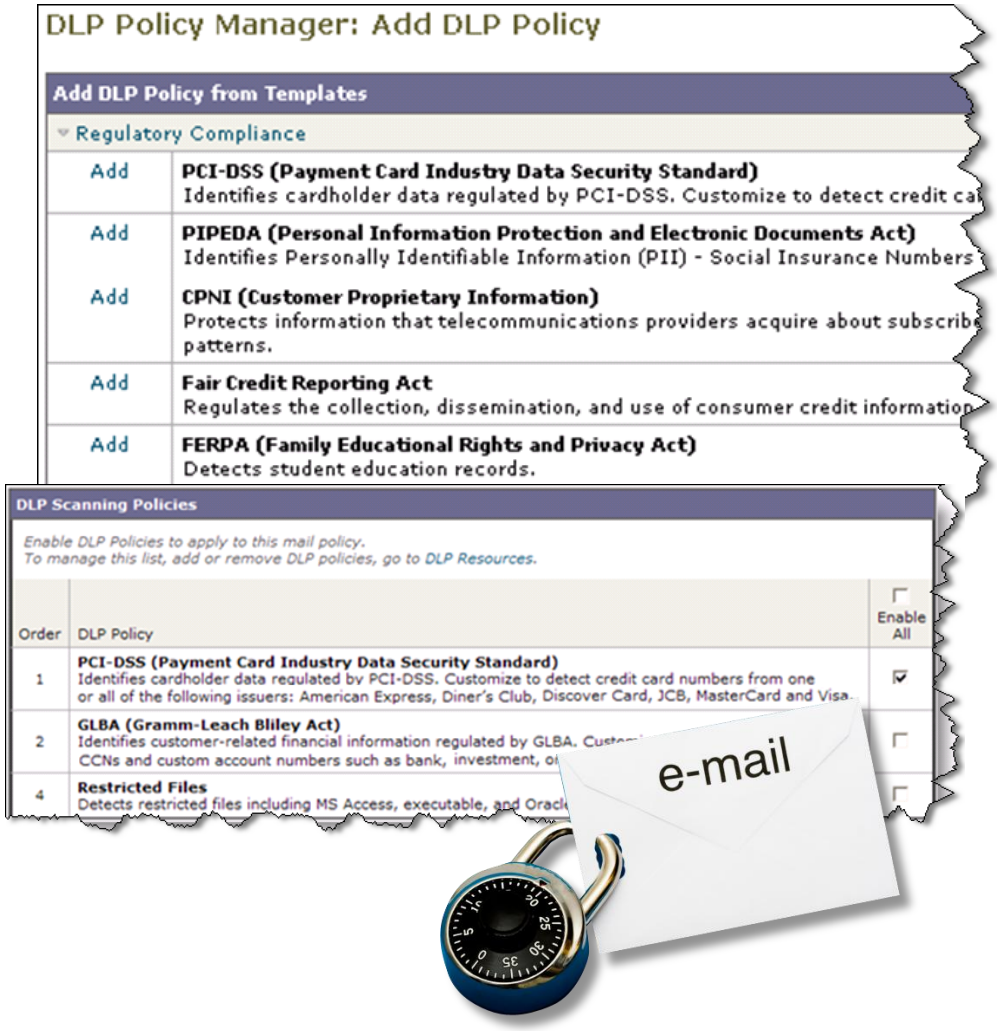
- 100+ Pre-defined templates
- Regulatory compliance

Easy

- One-click activation
- Policy enable/disable

Accurate

- Multiple parameters
- Key words, proximity, etc.



© 2010 Cisco and/or its affiliates. All rights reserved.

Data Loss Prevention

Comprehensive, Accurate, Easy

RSA SECURITY

Comprehensive

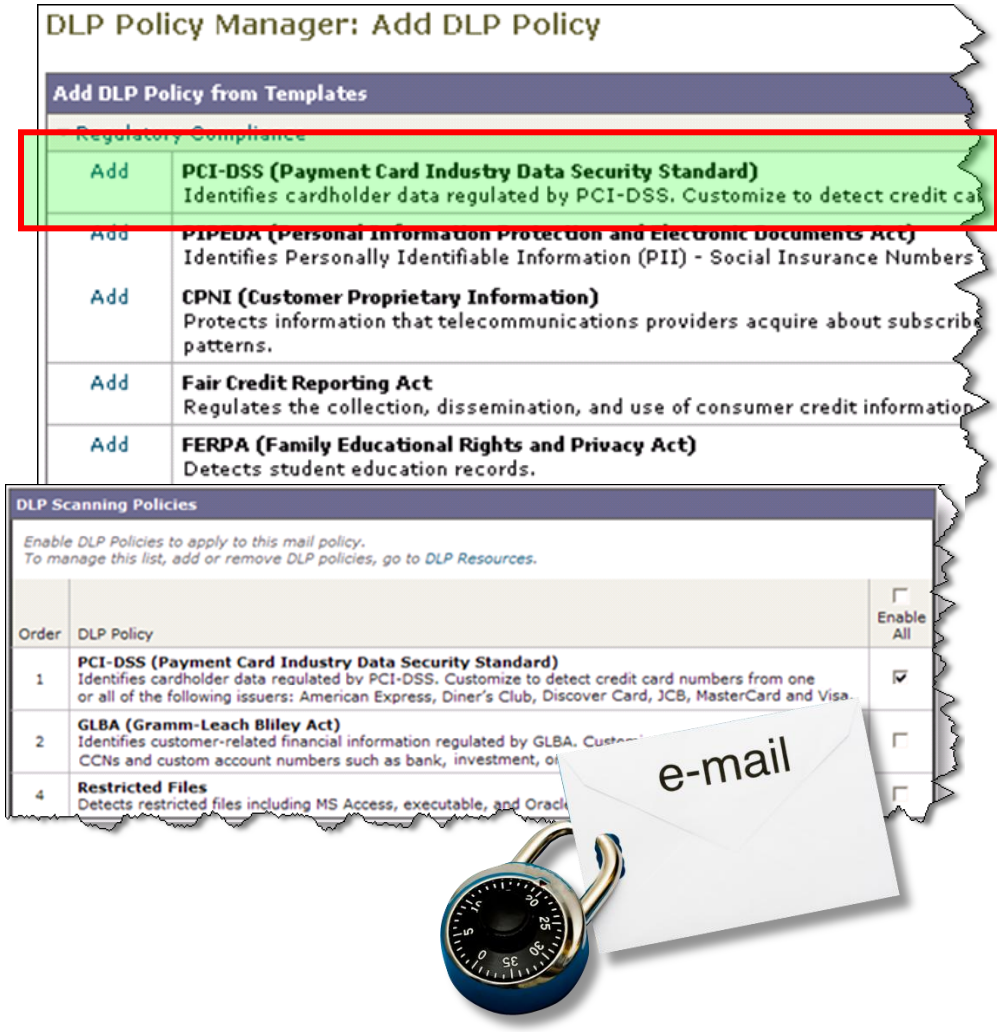
- 100+ Pre-defined templates
- Regulatory compliance

Easy

- One-click activation
- Policy enable/disable

Accurate

- Multiple parameters
- Key words, proximity, etc.



© 2010 Cisco and/or its affiliates. All rights reserved.

Cost of Non-compliance

- Penalties/fines from PCI: up to $500,000
- Cost to notify victims
- Cost to replace cards
- Cost for any fraudulent action
- Cost for forensics
- Etc..

And what about the impact on the image of the company?
What about bad publicity and brand damage?
Priceless?

© 2010 Cisco and/or its affiliates. All rights reserved.

What has to be protected

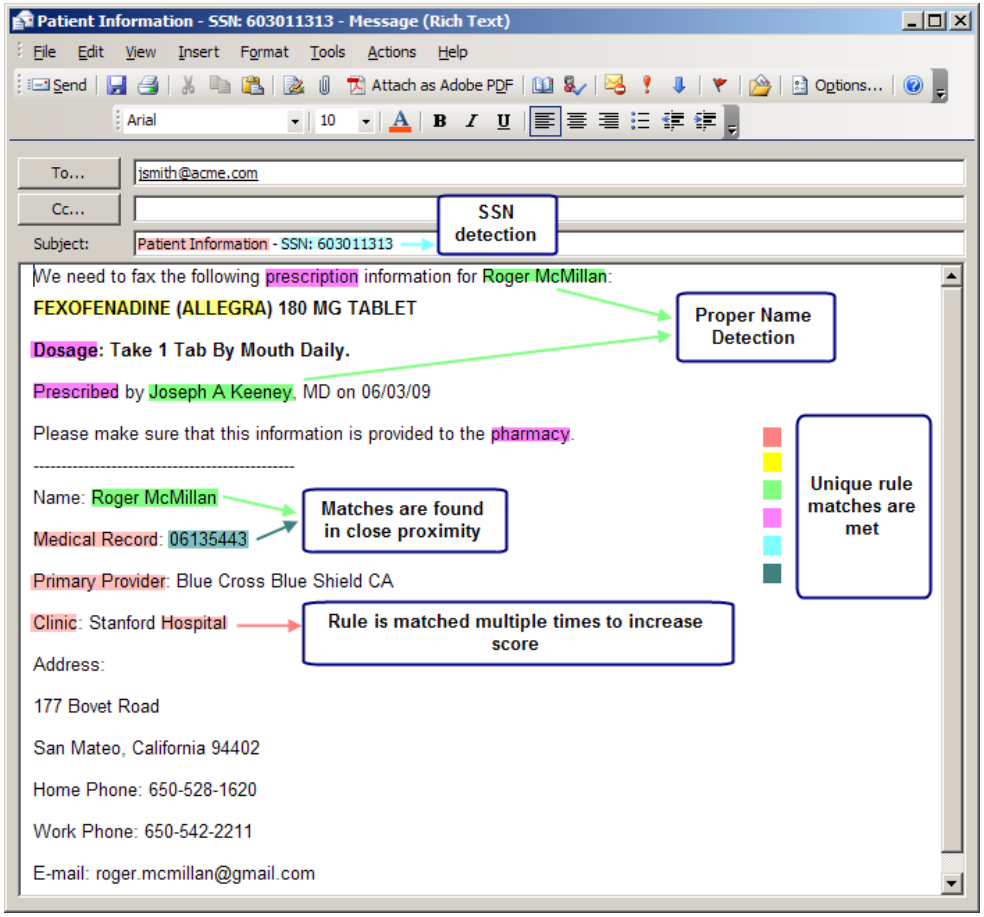
	Data Element	Storage Permitted	Protection Required
Cardholder Data	Primary Account Number (PAN)	Yes	Yes
	Cardholder Name [1]	Yes	Yes [1]
	Service Code [1]	Yes	Yes [1]
	Expiration Date [1]	Yes	Yes [1]

- Not just the PAN, but smarter detection methods needed:
  multiple data elements, proximity detection, etc…
- Avoid false positives

1: these data elements must be protected if they are used in conjonction with the PAN

© 2010 Cisco and/or its affiliates. All rights reserved.

In Depth Analysis Enables Accuracy



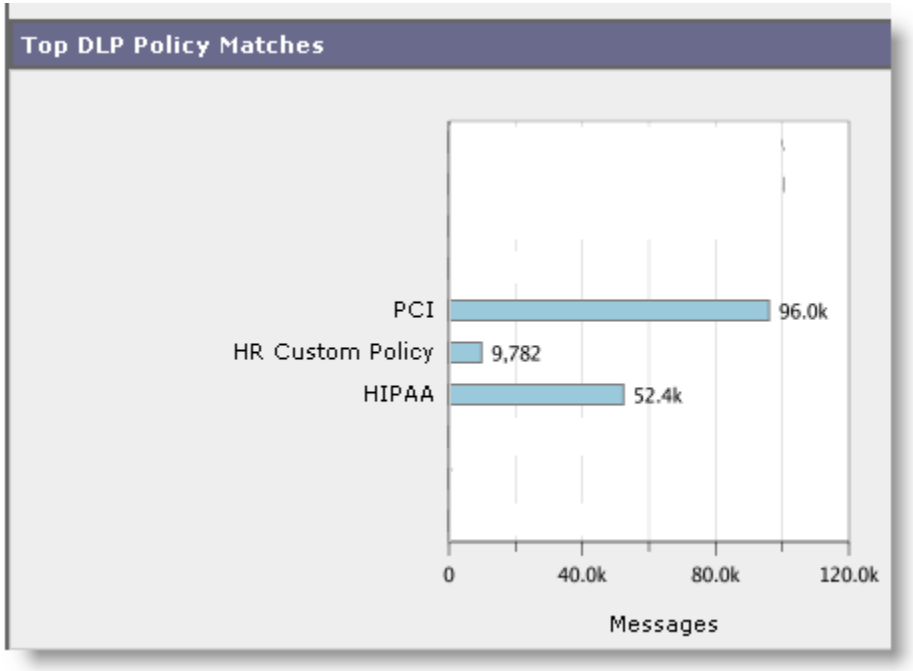
RSA SECURITY™

- Ranked as “Leader” in Gartner Magic Quadrant
- Focus on accuracy: large research team staffed specifically to write and refine content polices

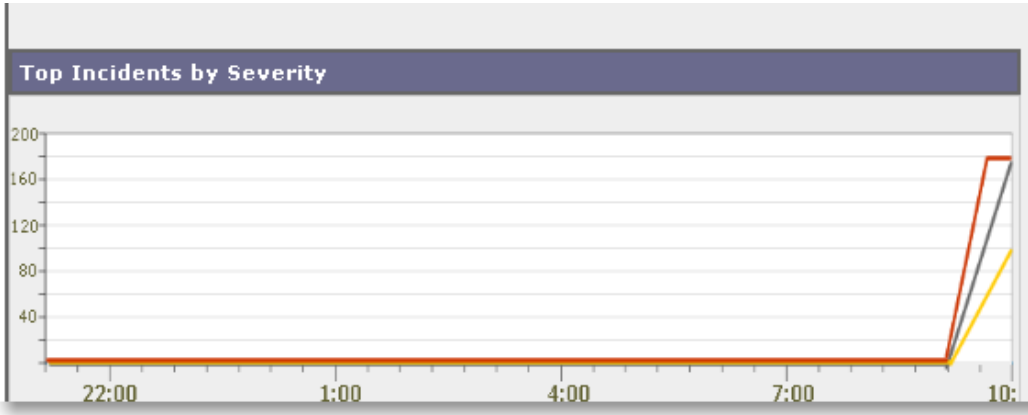
“RSA has strong described content capabilities enabled by a formal knowledge-engineering process” - Gartner

© 2010 Cisco and/or its affiliates. All rights reserved.

Easy to Monitor



- Reports by severity and policy
- Real time and scheduled reports available

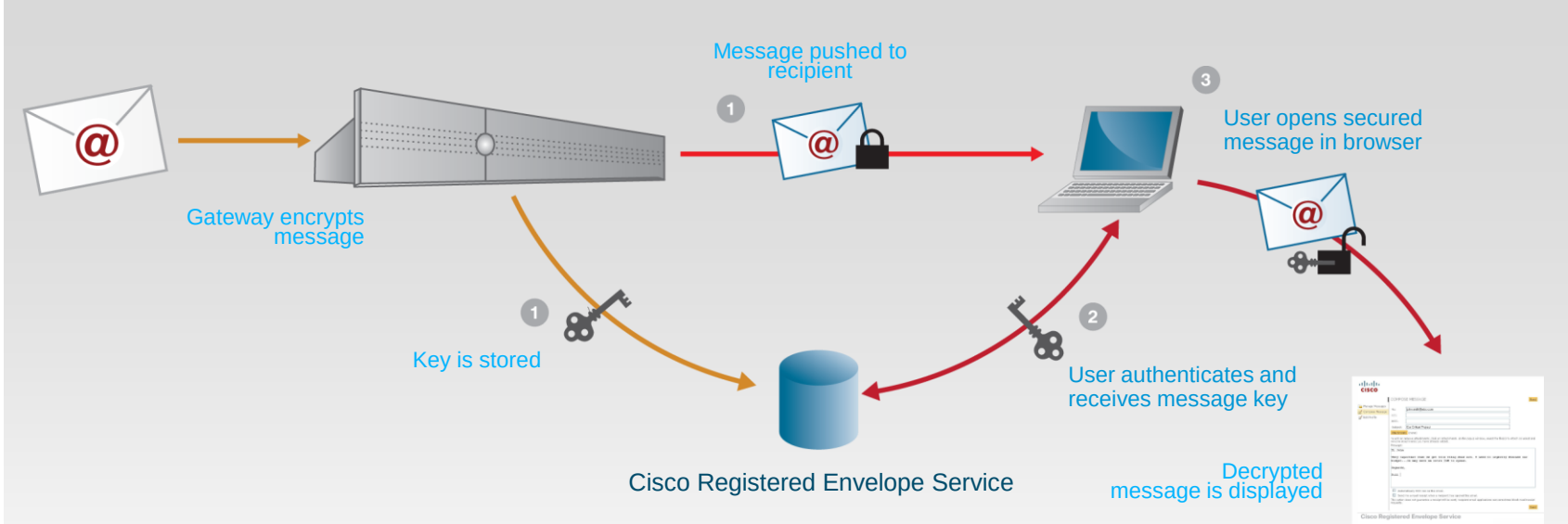


Incident Summary

Severity	%	Messages
Critical	54.0%	11.3k
High	5.0%	29.9k
Medium	18.0%	75.1k
Low	6.0%	12.0k
Total	**100.0%**	**36.0k**

Remediation example: Email Encryption

Instant Deployment, Zero Management Cost

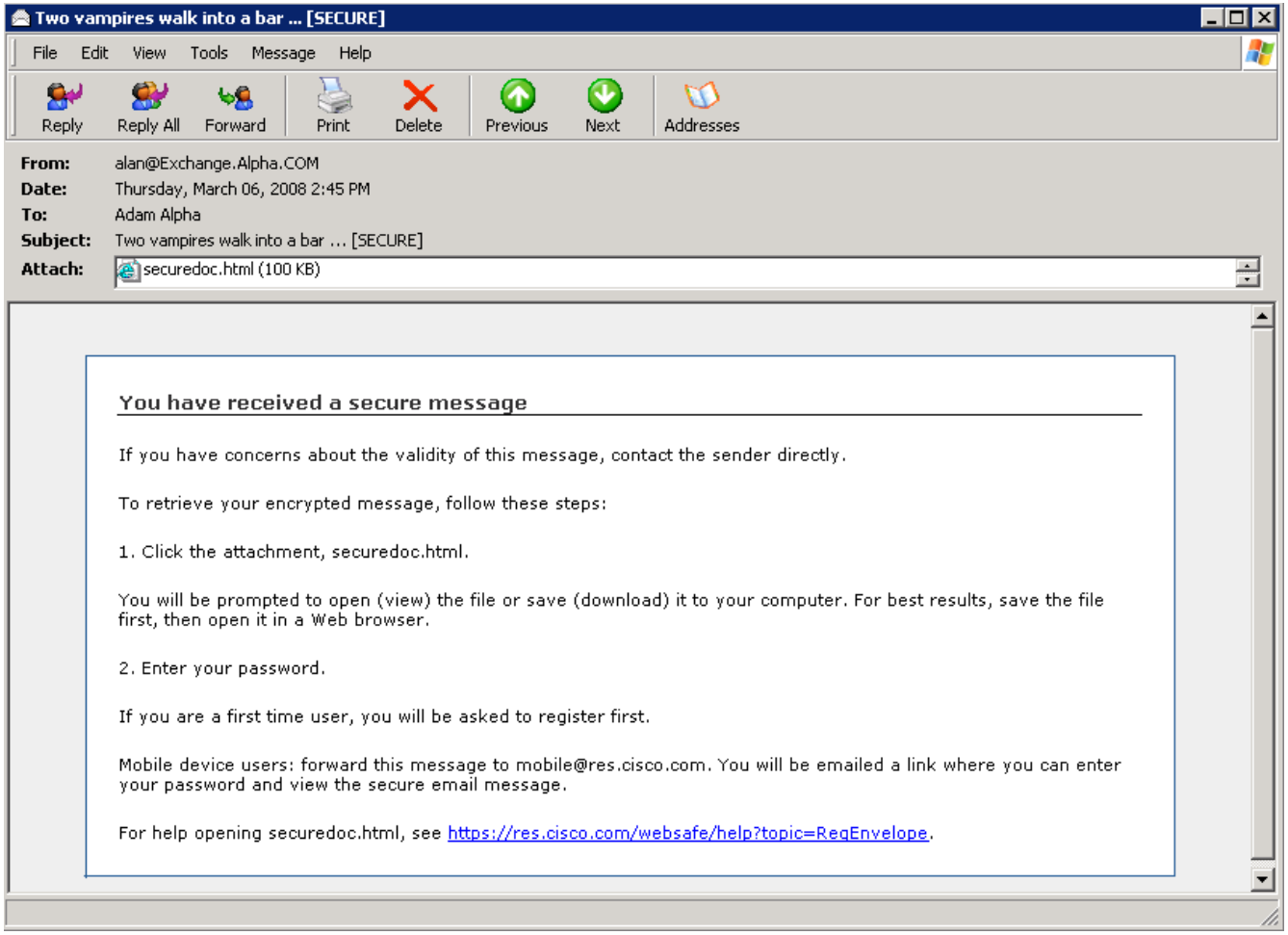


- Automated key management
- No desktop software requirements
- No new hardware required

© 2010 Cisco and/or its affiliates. All rights reserved.

Opening an Encrypted Message

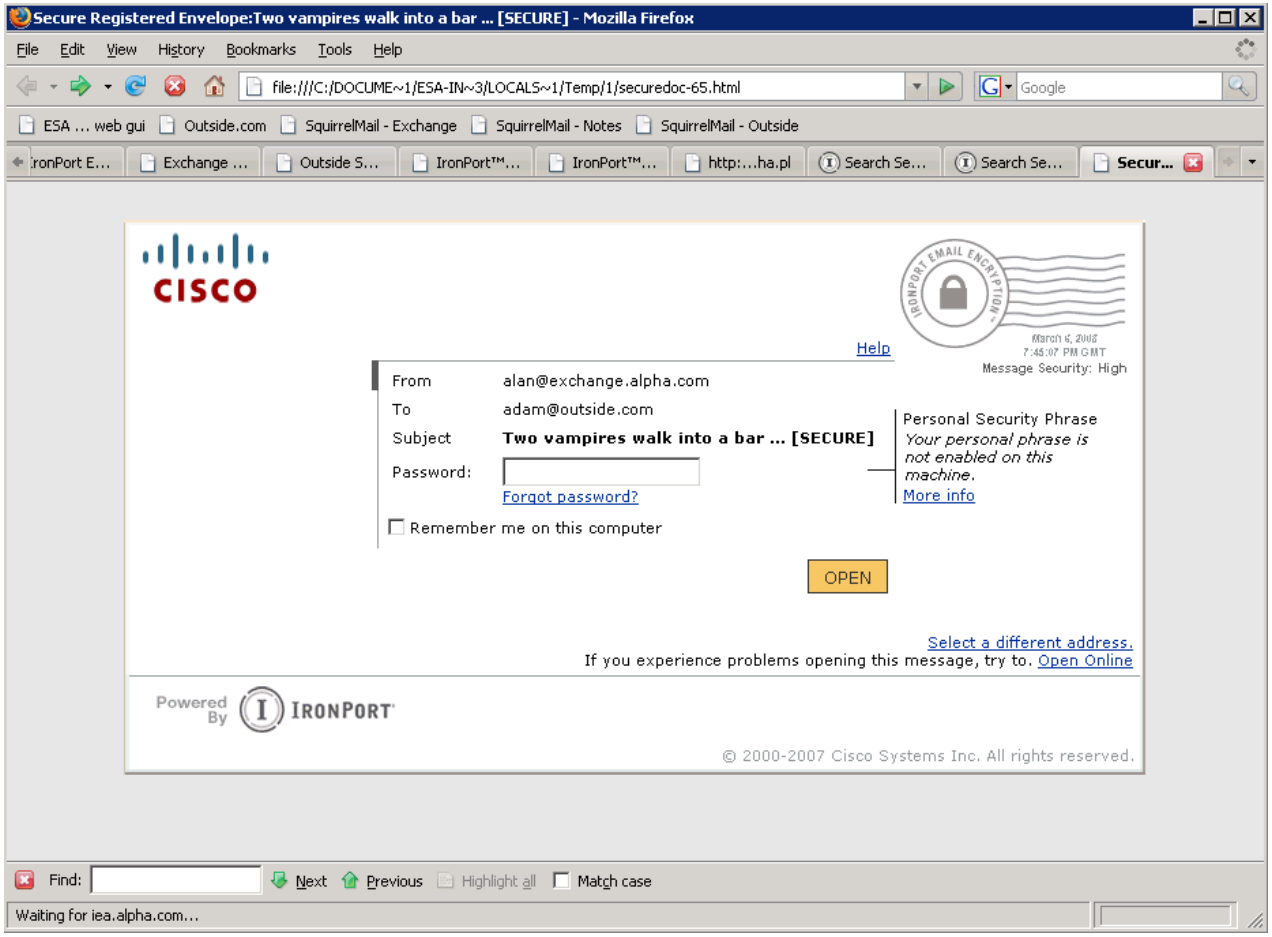
Receive email, click to open attachment



© 2010 Cisco and/or its affiliates. All rights reserved.

Opening an Encrypted Message

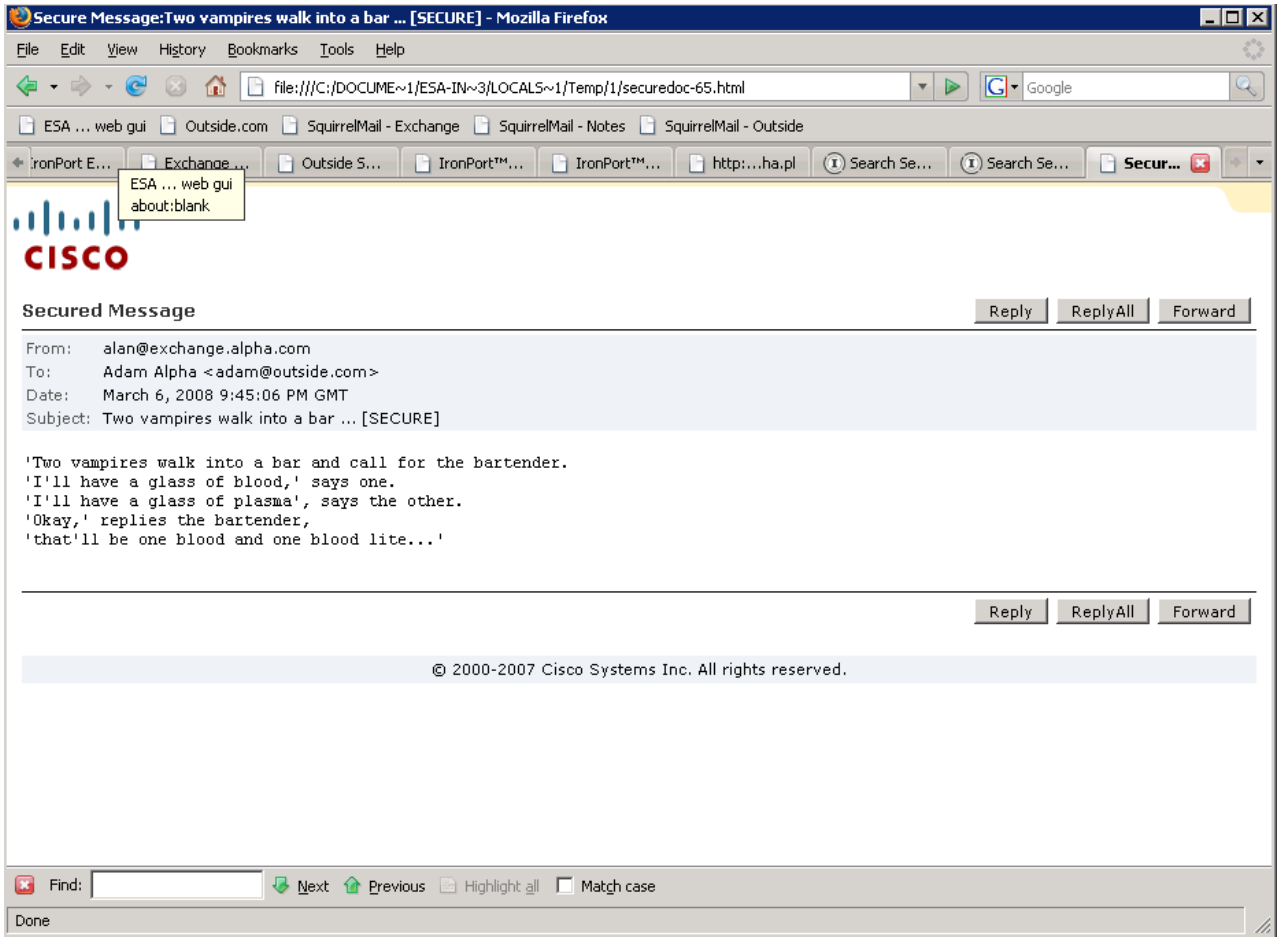
Enter password



© 2010 Cisco and/or its affiliates. All rights reserved.

Opening an Encrypted Message

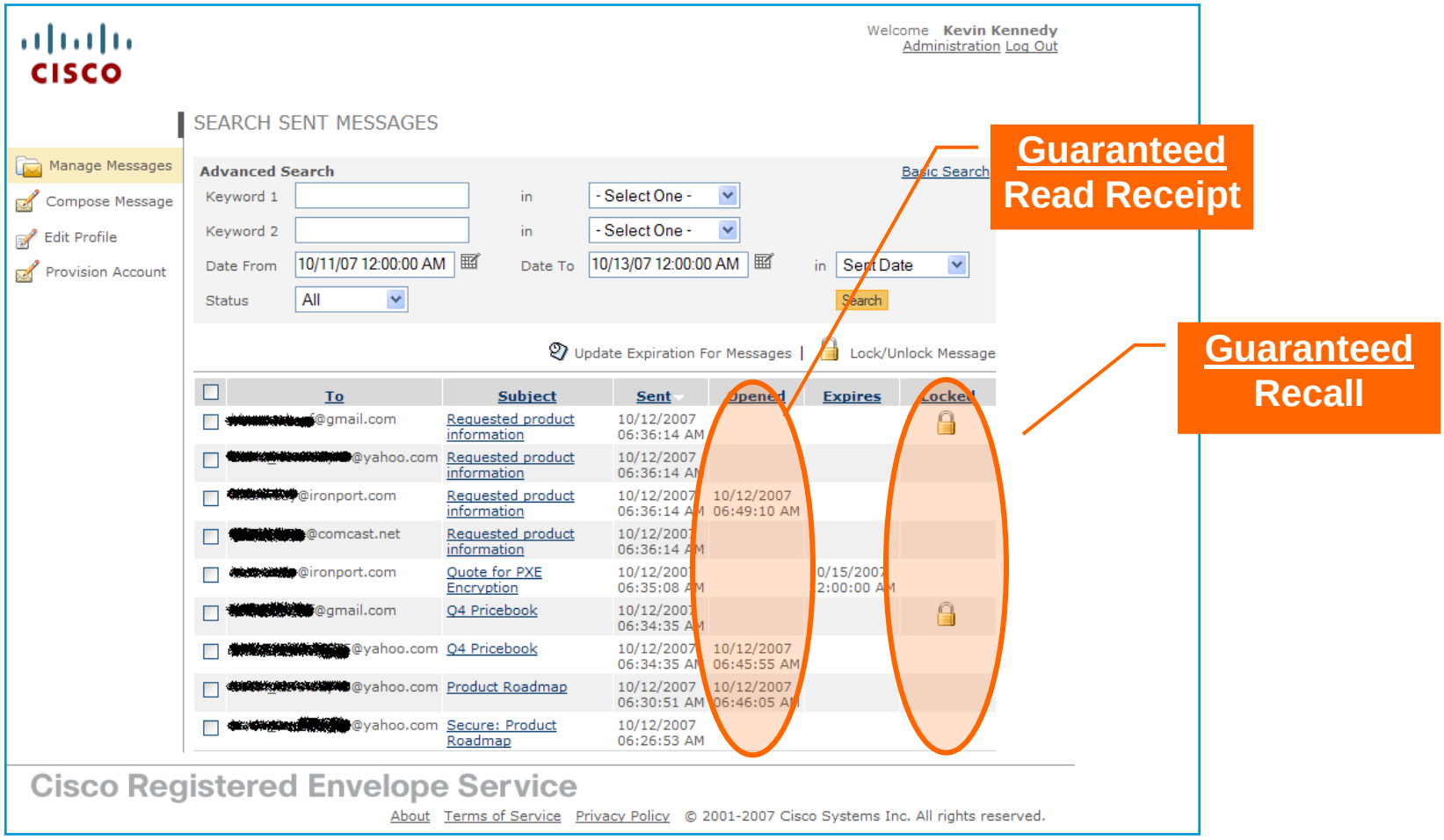
View secure message



© 2010 Cisco and/or its affiliates. All rights reserved.

End-User Message Management

Visibility and Control



© 2010 Cisco and/or its affiliates. All rights reserved.

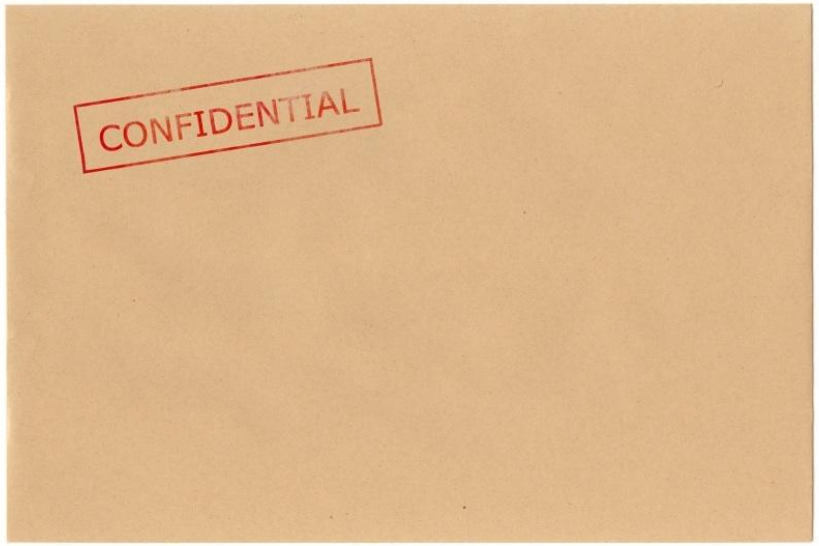
The result: Business Class Email

Confidential Contents

No Forwarding Allowed without Permission

Guaranteed Recall

Guaranteed Read Receipts



Message Expiry

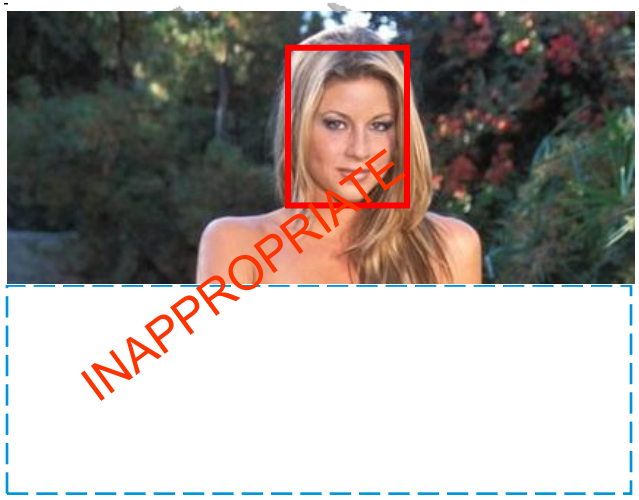
© 2010 Cisco and/or its affiliates. All rights reserved.

Detecting inappropriate images

A Management Tool for monitoring, risk assessment or enforcement

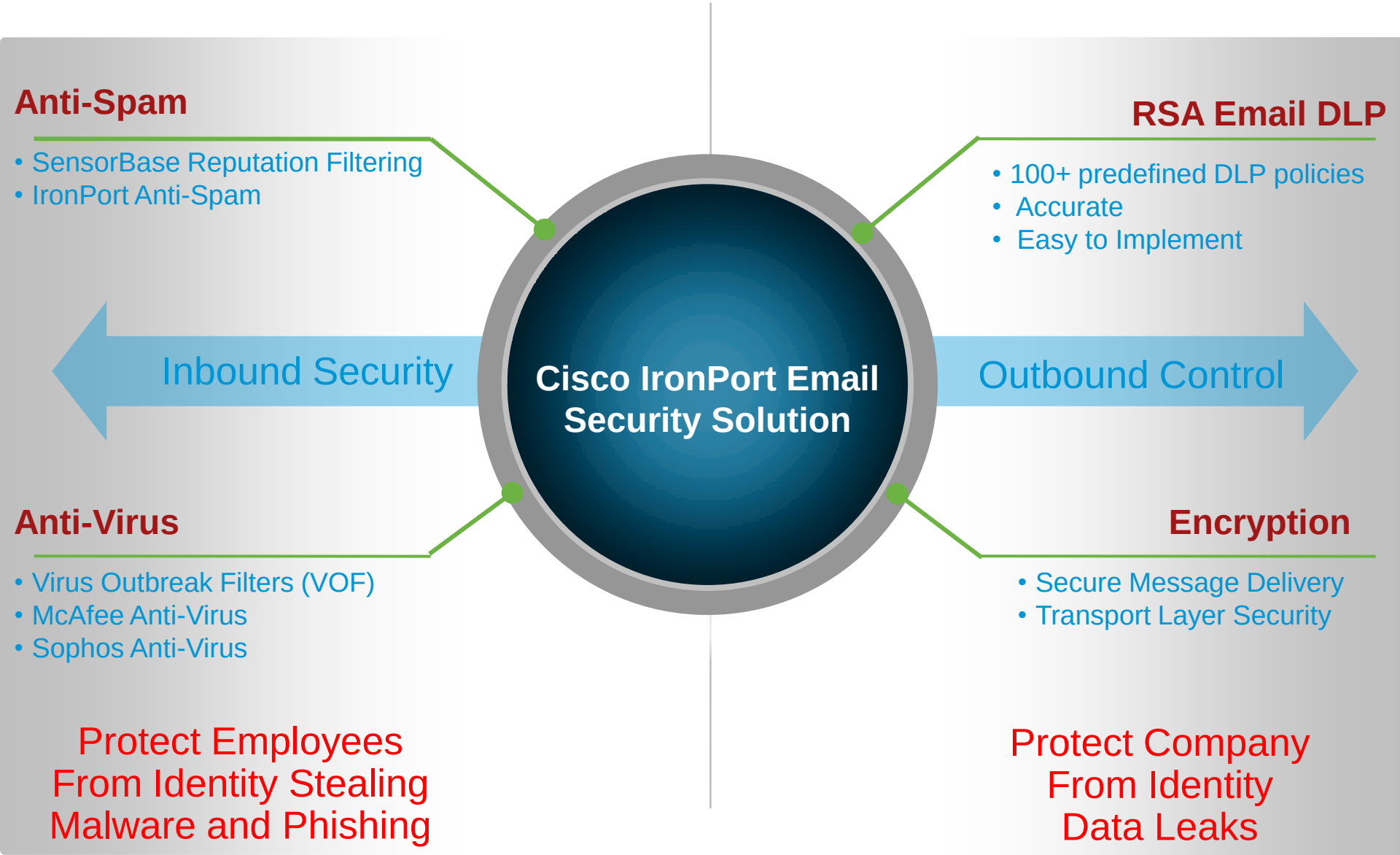
Different detection methods to determine if image is inappropriate:

- ✓ Image Cleanup
- ✓ Skin Detection
- ✓ Background Elimination
- ✓ Edge Detection
- ✓ Body Part Separation
- ✓ Curvature Identification
- ✓ Negative Curvature Rejection
- ✓ Body Part Elimination
- ✓ Face Detection
- ✓ Body Part Layout



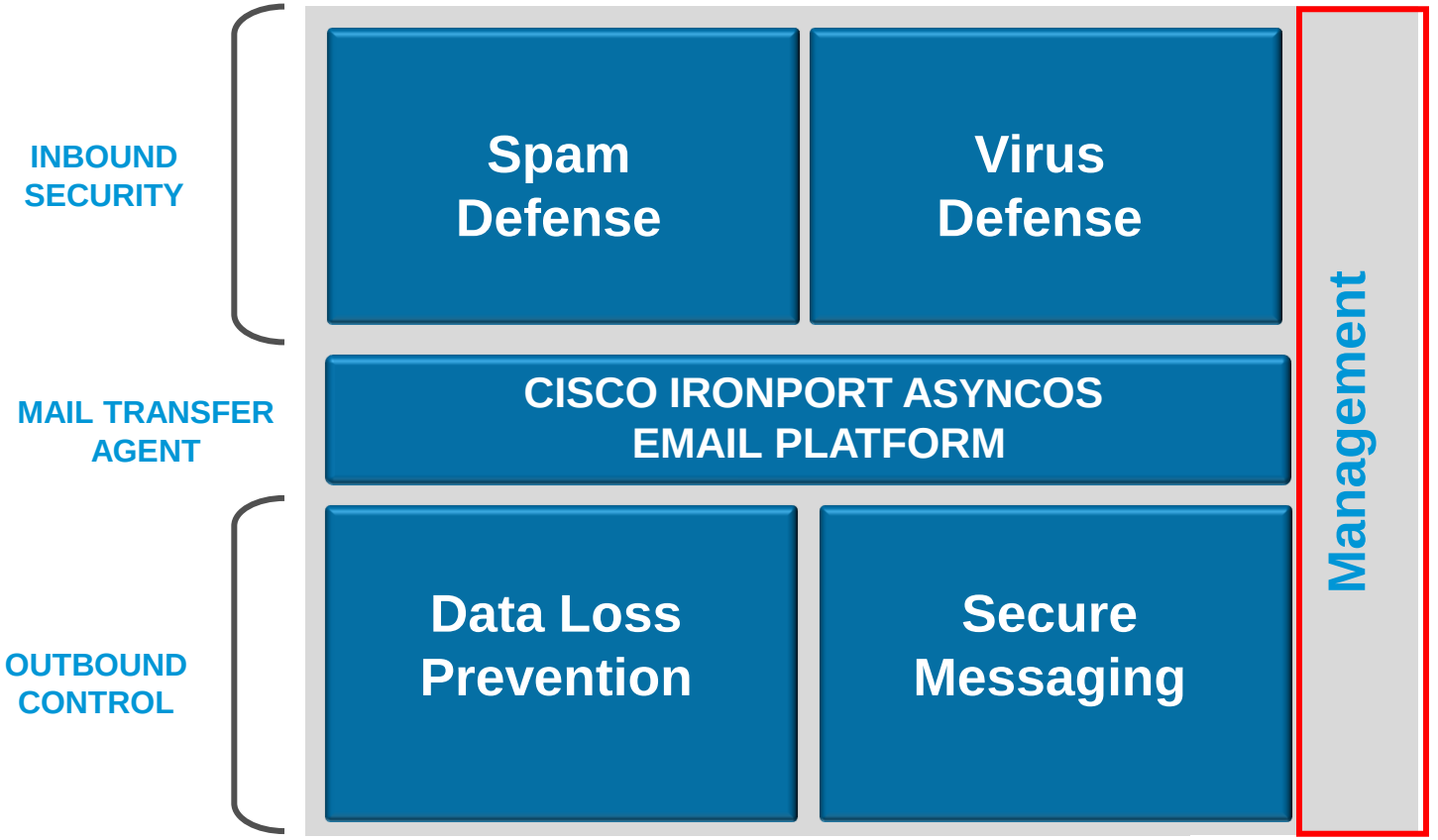
© 2010 Cisco and/or its affiliates. All rights reserved.

360 Degrees of Privacy Protection



Email Security Architecture

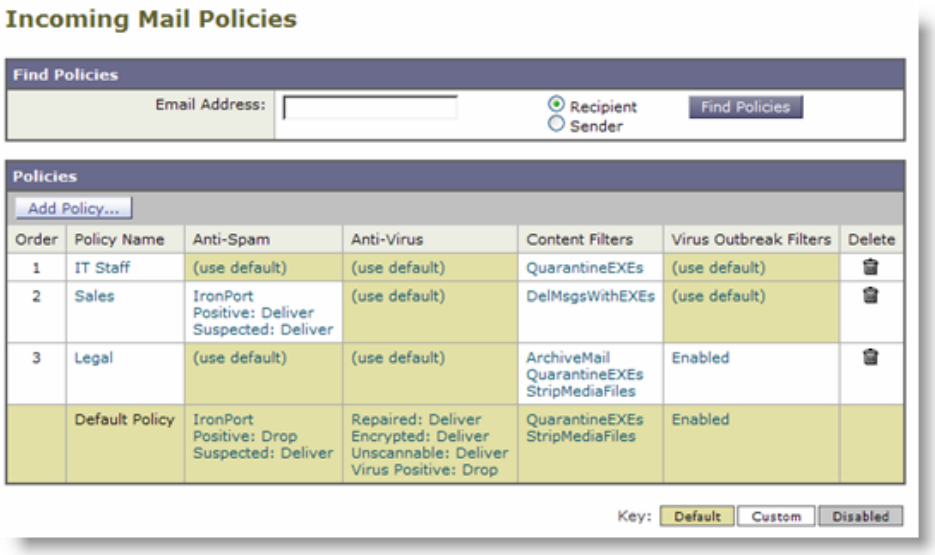
Cisco IronPort Email Security Appliance



© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco IronPort Email Security Manager

Single view of policies for the entire organization



Incoming Mail Policies

Find Policies

Email Address: ( ) Recipient ( ) Sender — Find Policies

Policies

Add Policy...

Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Virus Outbreak Filters	Delete
1	IT Staff	(use default)	(use default)	QuarantineEXEs	(use default)	
2	Sales	IronPort Positive: Deliver Suspected: Deliver	(use default)	DelMsgsWithEXEs	(use default)	
3	Legal	(use default)	(use default)	ArchiveMail QuarantineEXEs StripMediaFiles	Enabled	
	Default Policy	IronPort Positive: Drop Suspected: Deliver	Repaired: Deliver Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	QuarantineEXEs StripMediaFiles	Enabled	

Key: Default | Custom | Disabled

Categories: by Domain, Username, or LDAP

- Allow all media files
- Quarantine executables

- Mark and Deliver Spam
- Delete Executables

- Archive all mail
- Virus Outbreak Filters disabled for .doc files

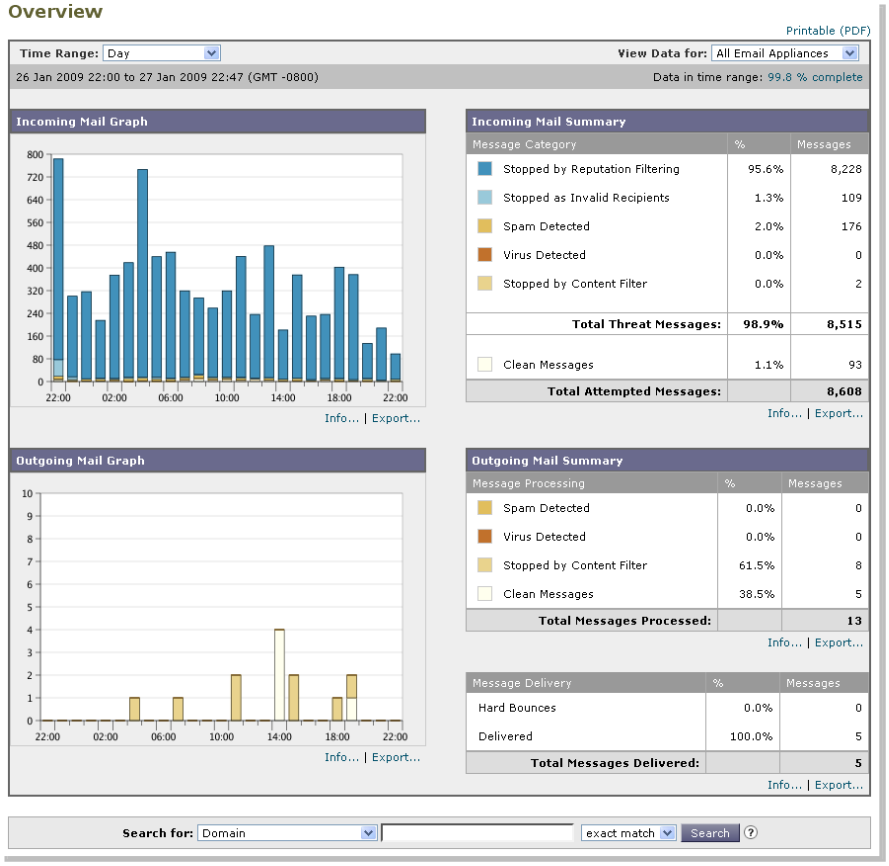
"IronPort Email Security Manager serves as a single, versatile dashboard to manage all the services on the appliance." *– PC Magazine*

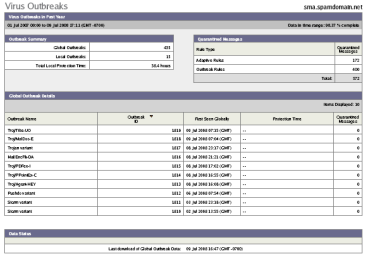
Comprehensive Insight

Unified Business Reporting

- Single view across the organization
- Real Time insight into email traffic and security threats
- Actionable drill down reports

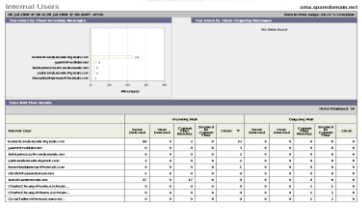
Consolidated Reports





Multiple data points

- Email Volumes
- Spam Counters
- Policy Violations
- Virus Reports
- Outgoing Email Data
- Reputation Service
- System Health View



© 2010 Cisco and/or its affiliates. All rights reserved.

Visibility Into Email Messages

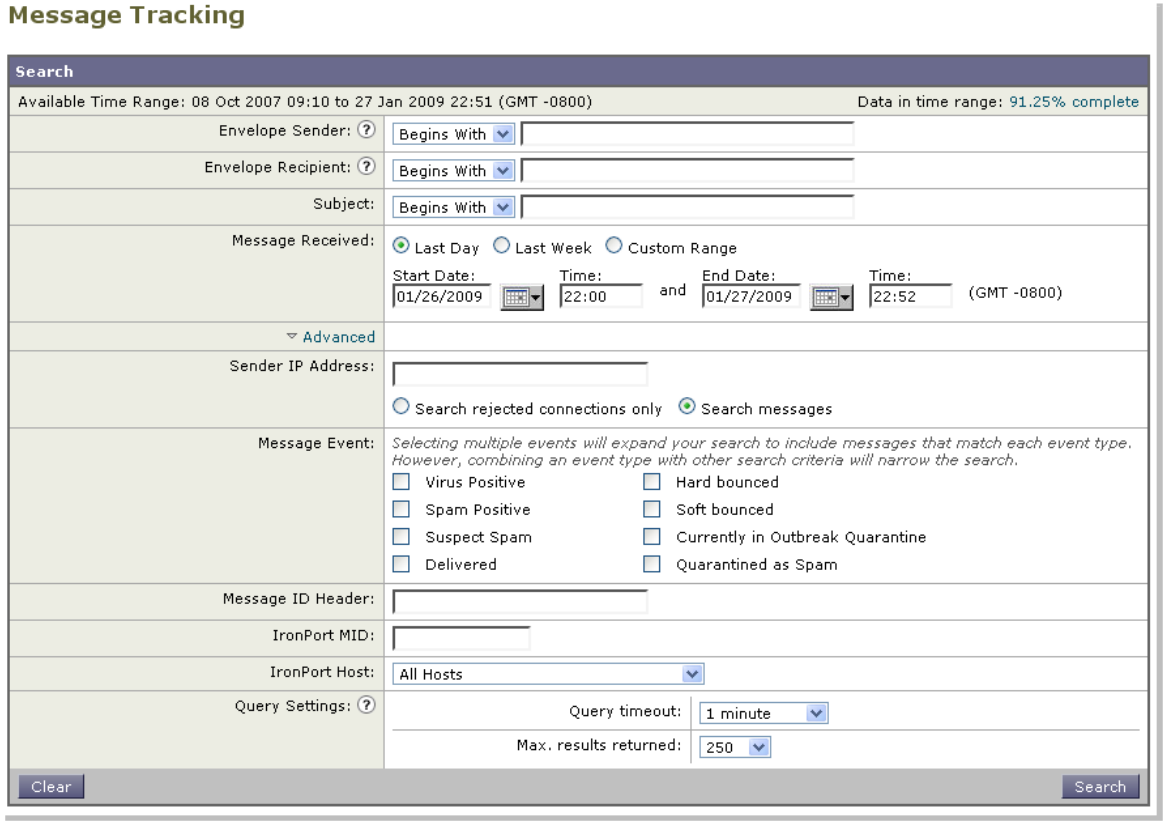
Message Tracking

What happened to the email I sent 2 hours ago?

- ✓Track Individual Email Messages

Who else received similar emails?

- ✓ Forensics to Ensure Compliance



© 2010 Cisco and/or its affiliates. All rights reserved.

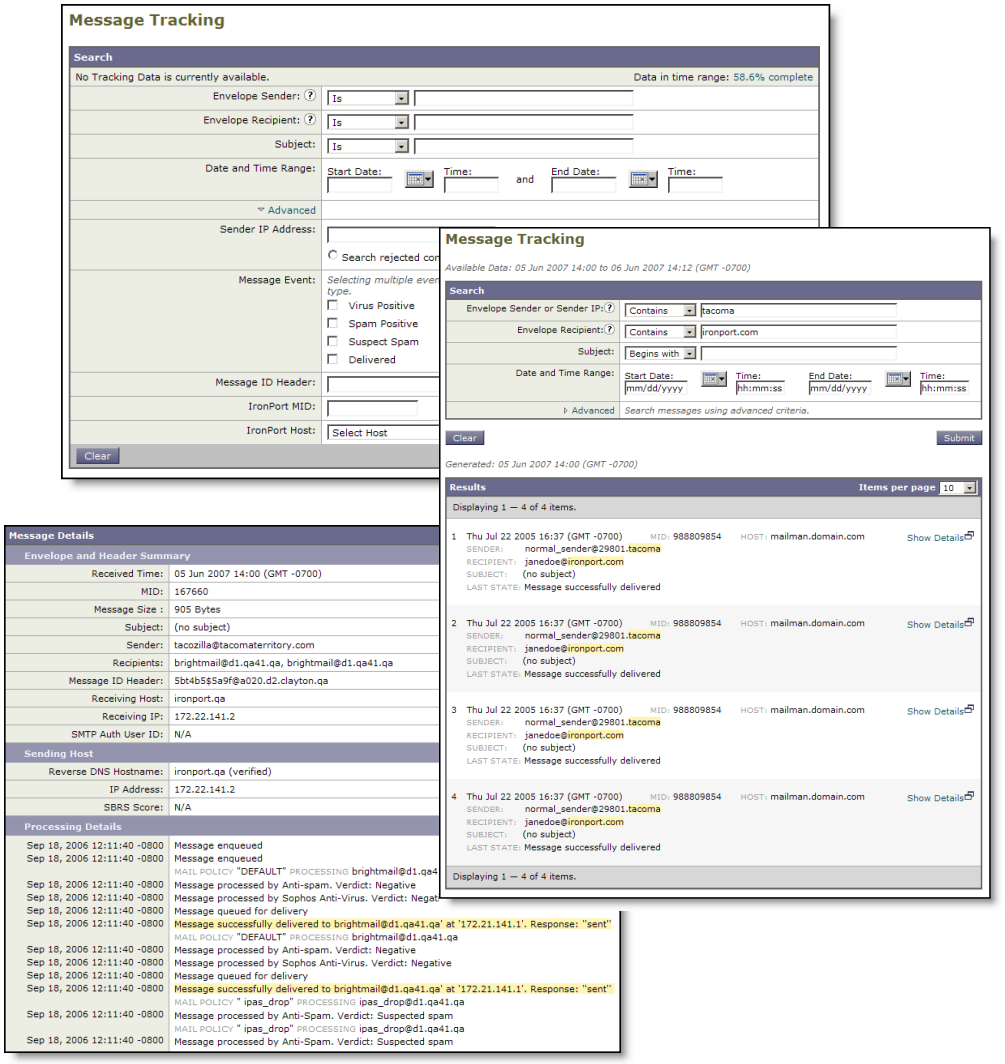
Cisco IronPort Security Management Appliance

Centralized Quarantine, Reporting and Message Tracking

- Aggregated IronPort Email Security Monitor reports available on a central IronPort SMA interface
- Helps administrators answer help desk calls quickly and easily

  "Joe sent me an email, but I never received it."
- Easier alternative to searching log files

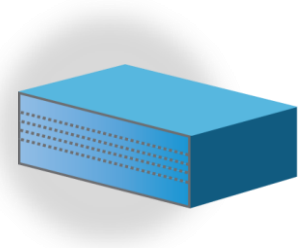
  Gives one place to search for messages across different appliances



© 2010 Cisco and/or its affiliates. All rights reserved.

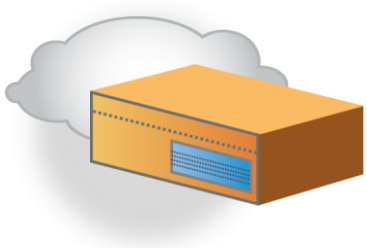
Appliance or Cloud ?

Appliances



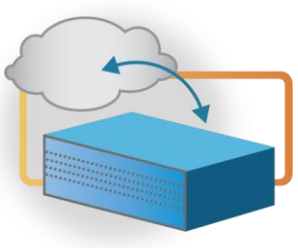
Award-Winning Technology

Hosted



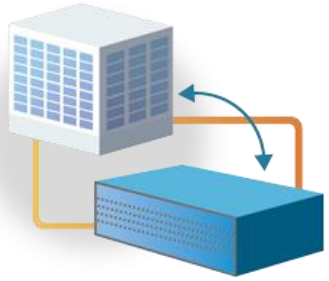
Dedicated SaaS Infrastructure

Hybrid Hosted



Best of Both Worlds

Managed



Fully Managed on Premises

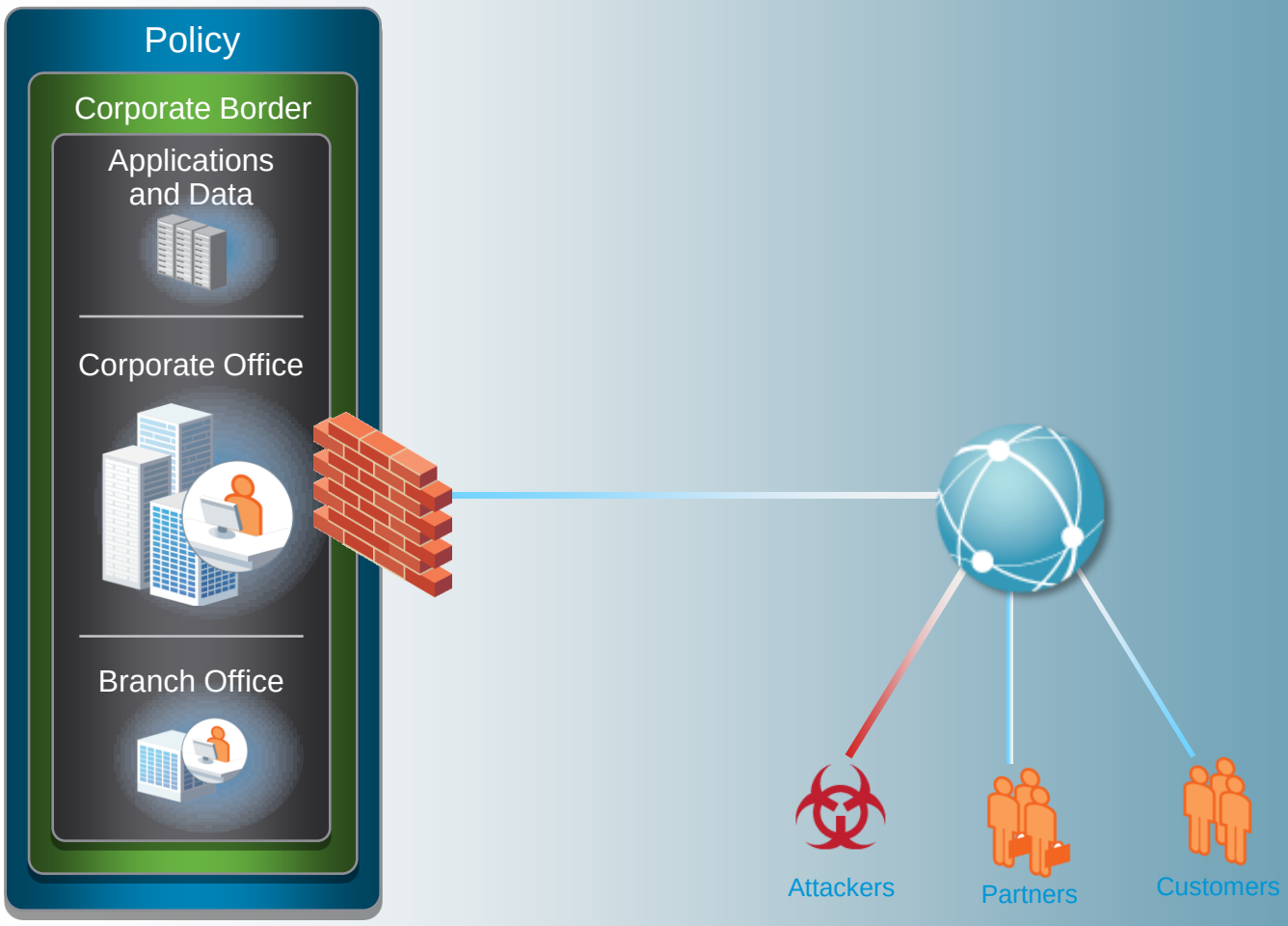
Backed by Service Level Agreements

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco IronPort Web Security

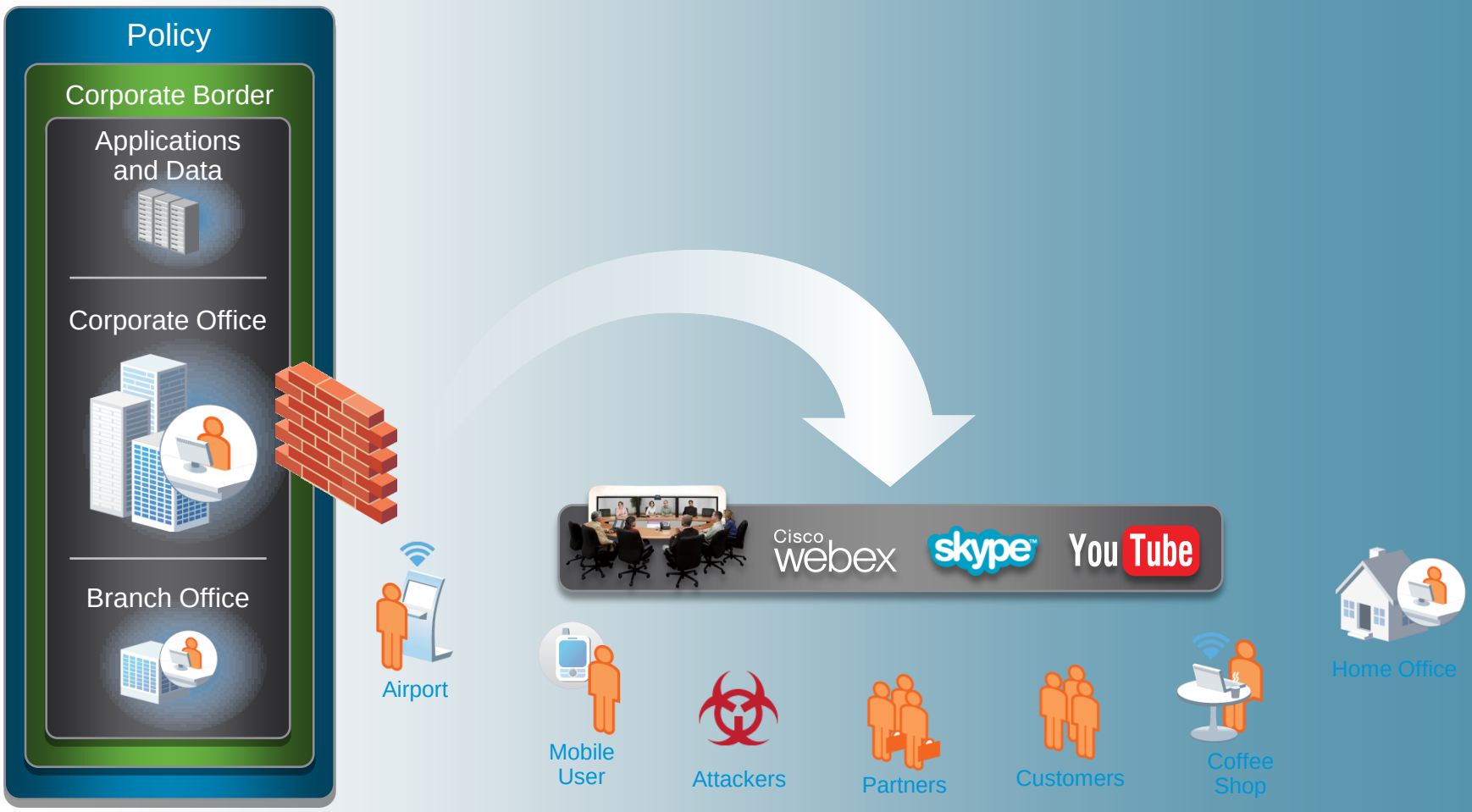
© 2010 Cisco and/or its affiliates. All rights reserved.

Traditional Corporate Border



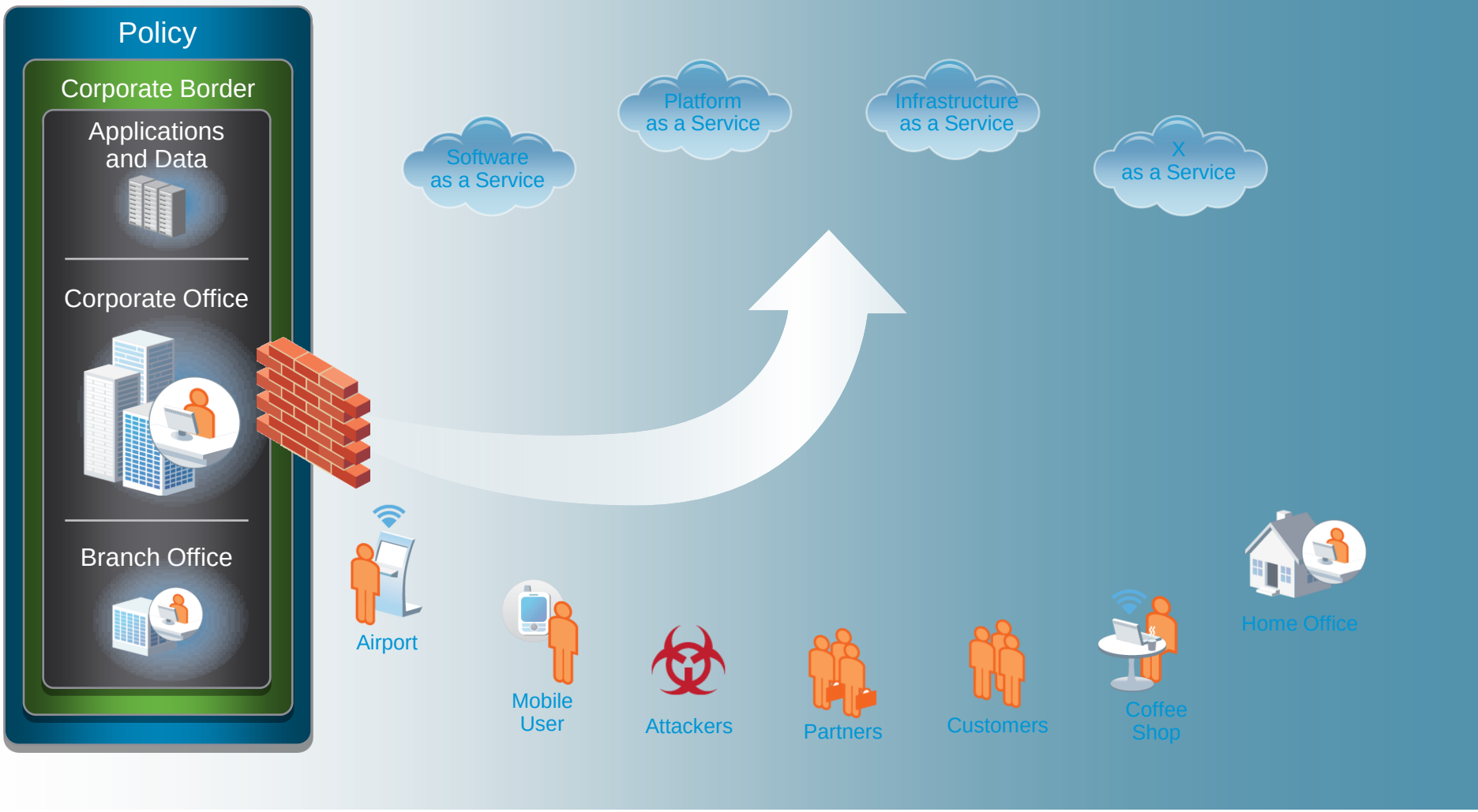
© 2010 Cisco and/or its affiliates. All rights reserved.

Mobility and Collaboration Are Dissolving the Internet Border



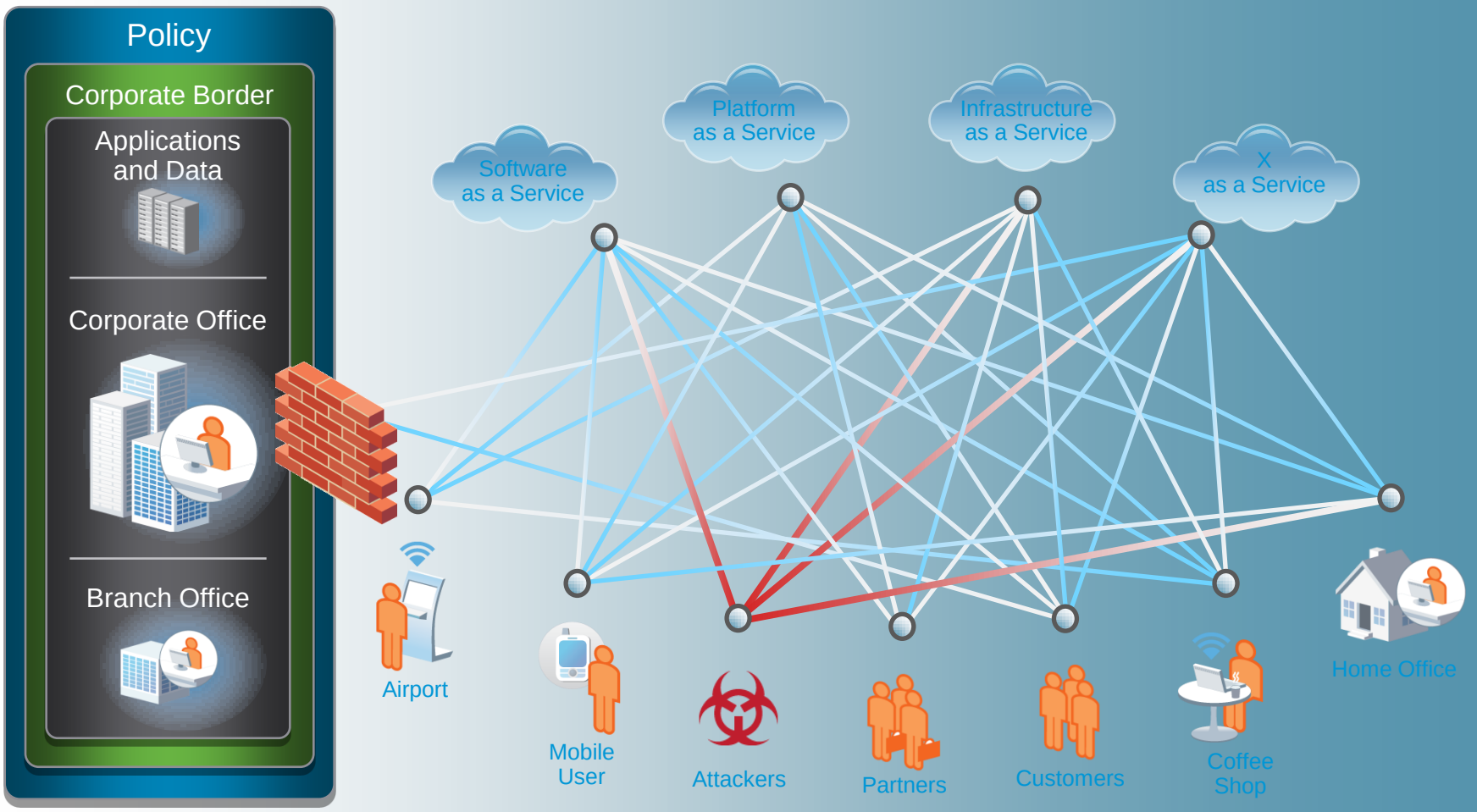
© 2010 Cisco and/or its affiliates. All rights reserved.

Cloud Computing Is Dissolving the Data Center Border



© 2010 Cisco and/or its affiliates. All rights reserved.

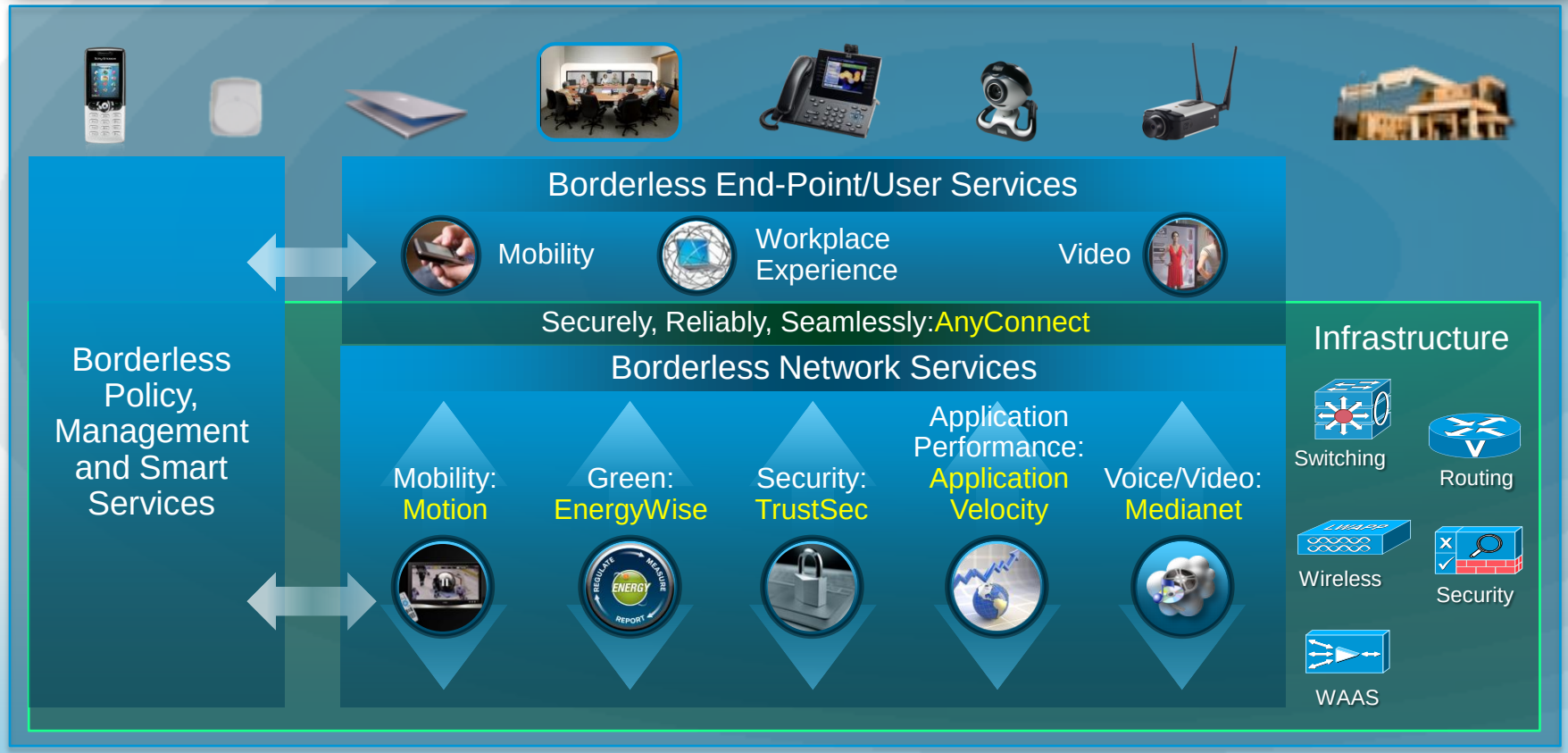
Business Without Borders



© 2010 Cisco and/or its affiliates. All rights reserved.

Borderless Network Architecture

Architecture for Agile Delivery of the Borderless Experience

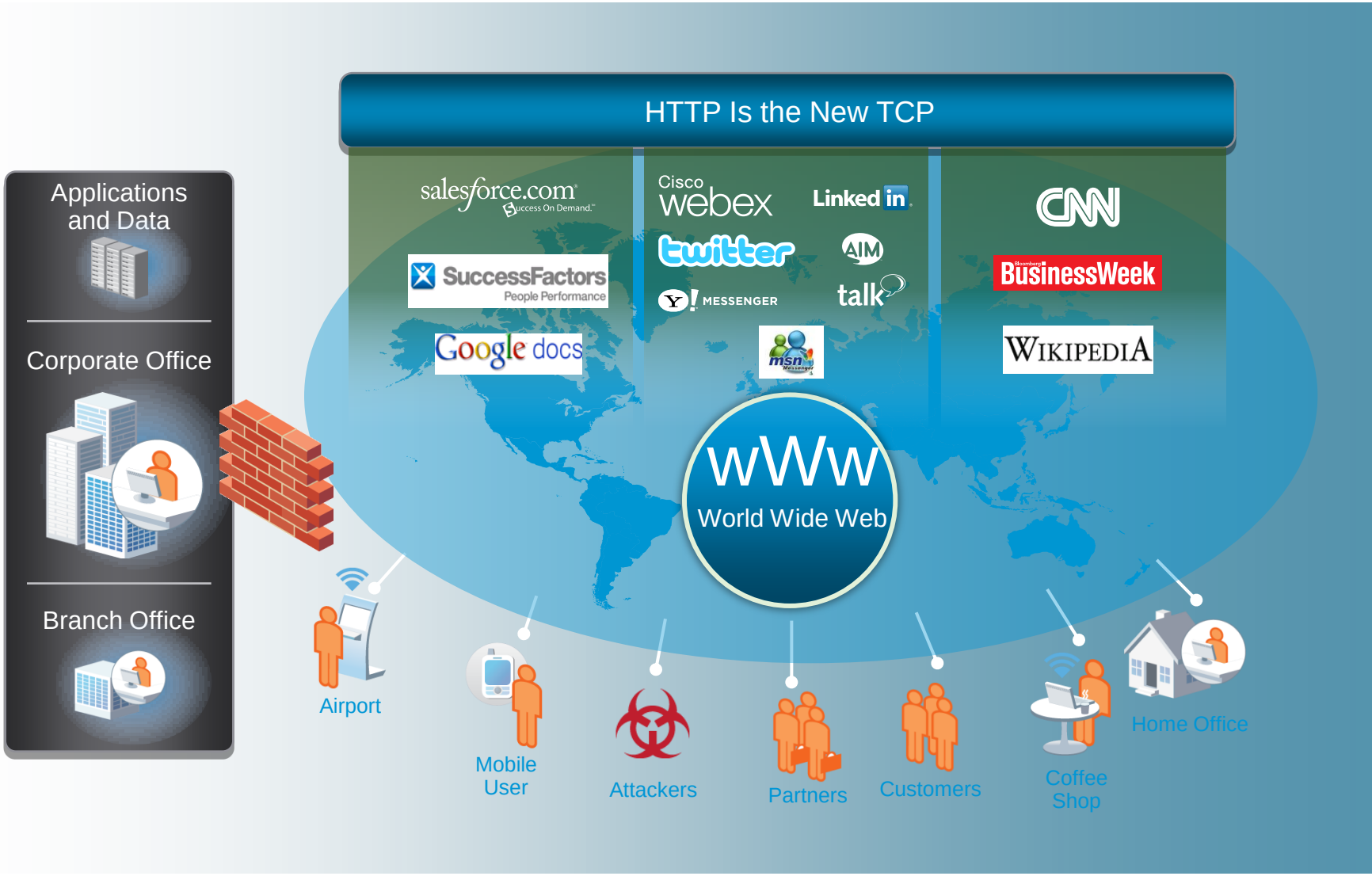


PROFESSIONAL SERVICES:
Realize the Value of Borderless Networks Faster

Cisco's Architecture for Borderless Network Security

© 2010 Cisco and/or its affiliates. All rights reserved.

Web: Enabling the Borderless Experience



© 2010 Cisco and/or its affiliates. All rights reserved.

Web Business Challenges

Acceptable Use Control

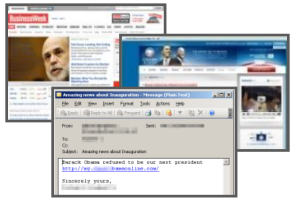
twitter

Y! MESSENGER

facebook

LinkedIn

Malware Protection



Data Loss Prevention

SaaS Access Control

webex

salesforce

Google docs

Policy

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco IronPort Web Security Appliance

Industry Leading Secure Web Gateway

© 2010 Cisco and/or its affiliates. All rights reserved.

The challenge of the Dark Web

80% of the web is uncategorized, highly dynamic or unreachable by web crawlers

- Botnets
- Dynamic content
- Password protected sites
- User generated content
- Short life sites

The Known Web

20% covered by URL lists

Danger

Malware Protection

Data Security

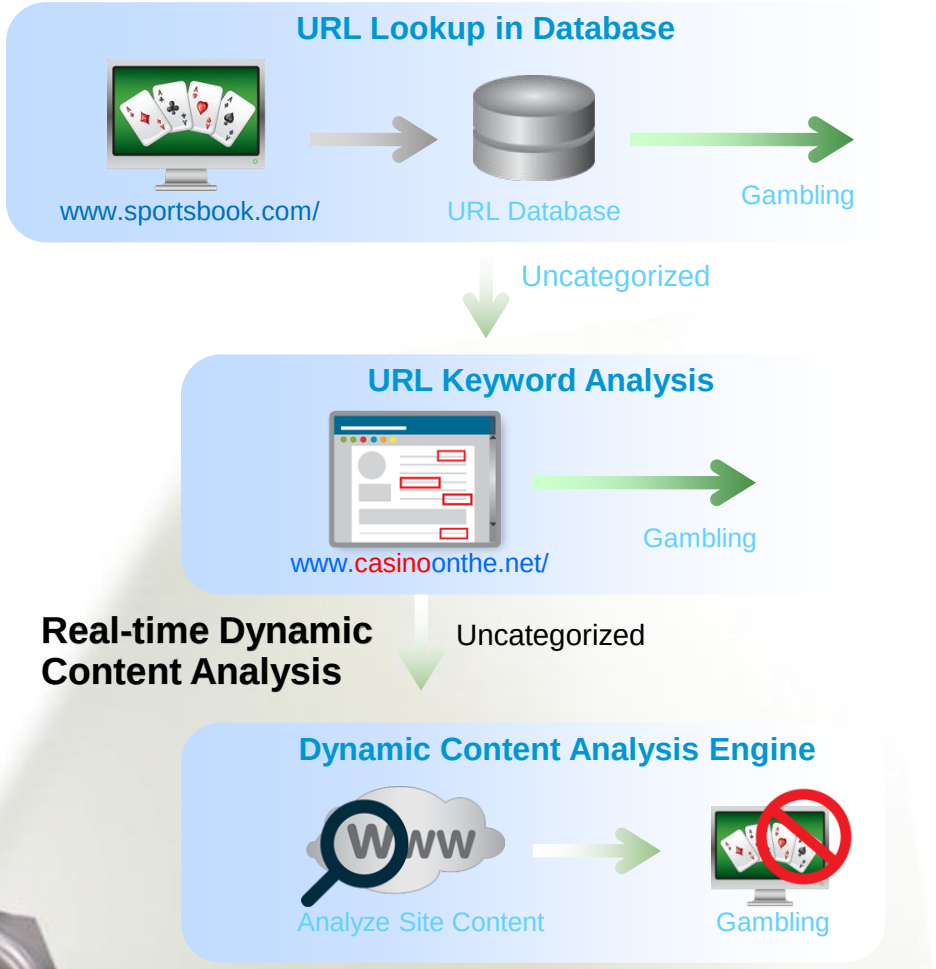
Danger

Acceptable Use Controls

SaaS Access Controls

© 2010 Cisco and/or its affiliates. All rights reserved.

The answer: Dynamic Categorization



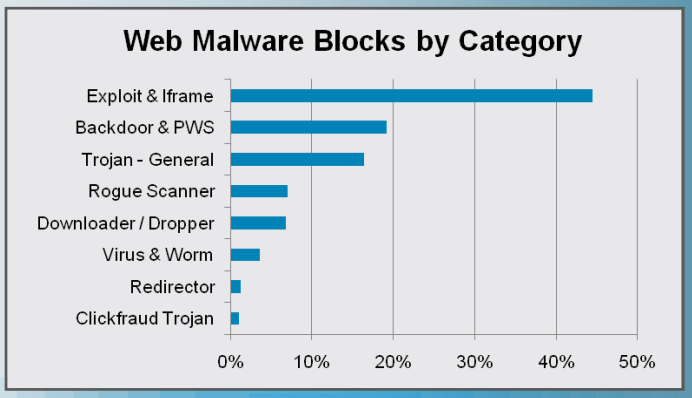
- Industry-leading URL database efficacy
  - 65 categories
  - Updated every 5 minutes
- Dynamic categorization identifies more than 90% of Dark Web content in commonly blocked categories

Cisco IronPort Web Security Appliance

Industry Leading Secure Web Gateway

© 2010 Cisco and/or its affiliates. All rights reserved.

Malware Threats Continue to Rise



- 237% volume increase in ‘09
- Over 70% of compromised web sites are legitimate
- Vulnerabilities in Adobe PDF emerged as the main target, followed by Flash

- 54% of malware encounters due to iframes and exploits
- Cross-Site Scripting and SQL Injection are top attack methods
- 83% of websites have at least 1 serious vulnerability

© 2010 Cisco and/or its affiliates. All rights reserved.

Why web exploits can be difficult to detect:

BoingBoing.net: A Popular Blog

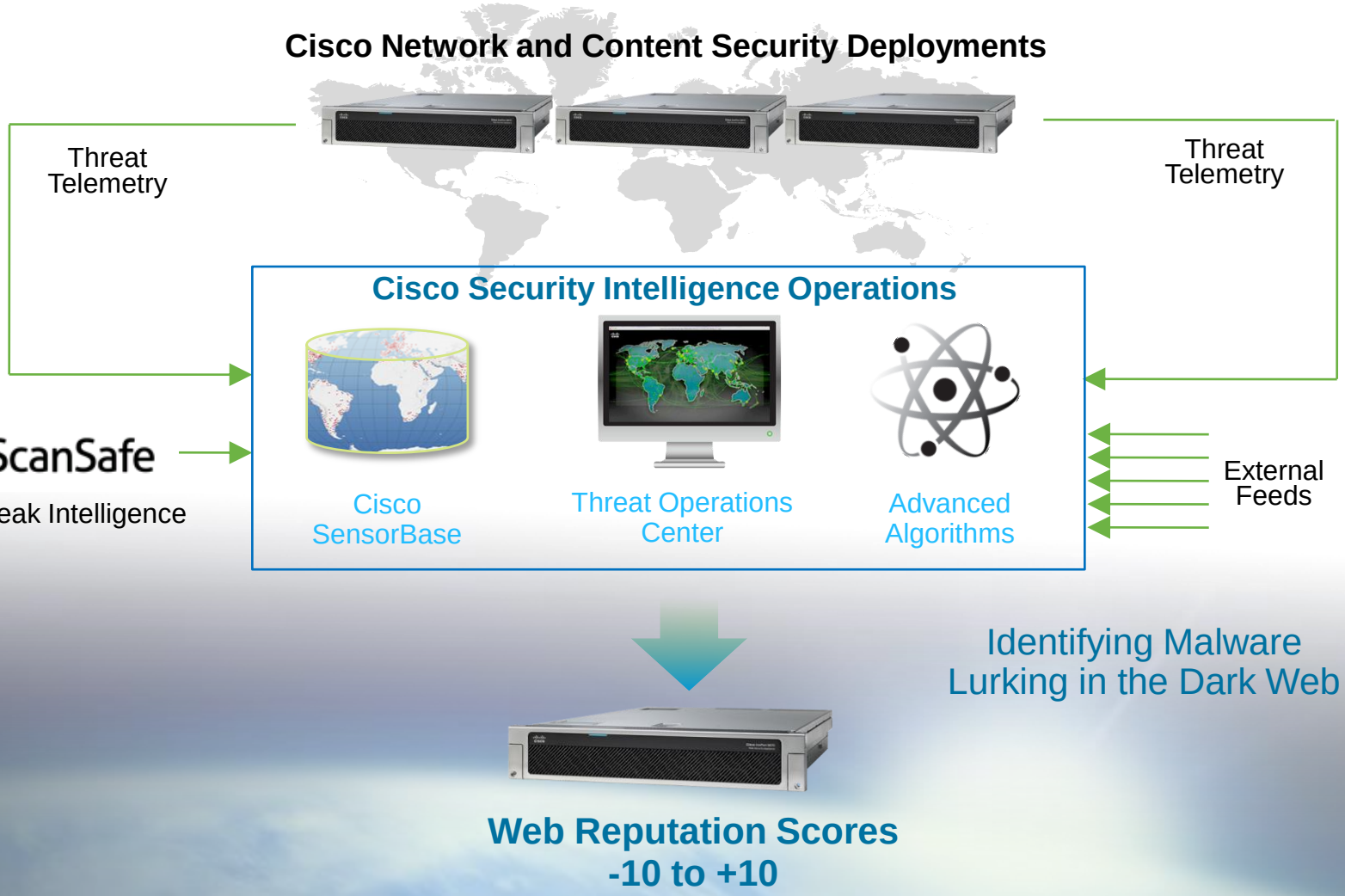
- URLs in browser: **1**
- HTTP Gets: **162**
- Images: **66**
  from **18** domains including **5** separate 1x1 pixel invisible tracking images
- Scripts: **87** from **7** domains
- Cookies: **118** from **15** domains
- **8** Flash objects from **4** domains

Why web exploits can be difficult to detect:

BoingBoing.net: A Popular Blog

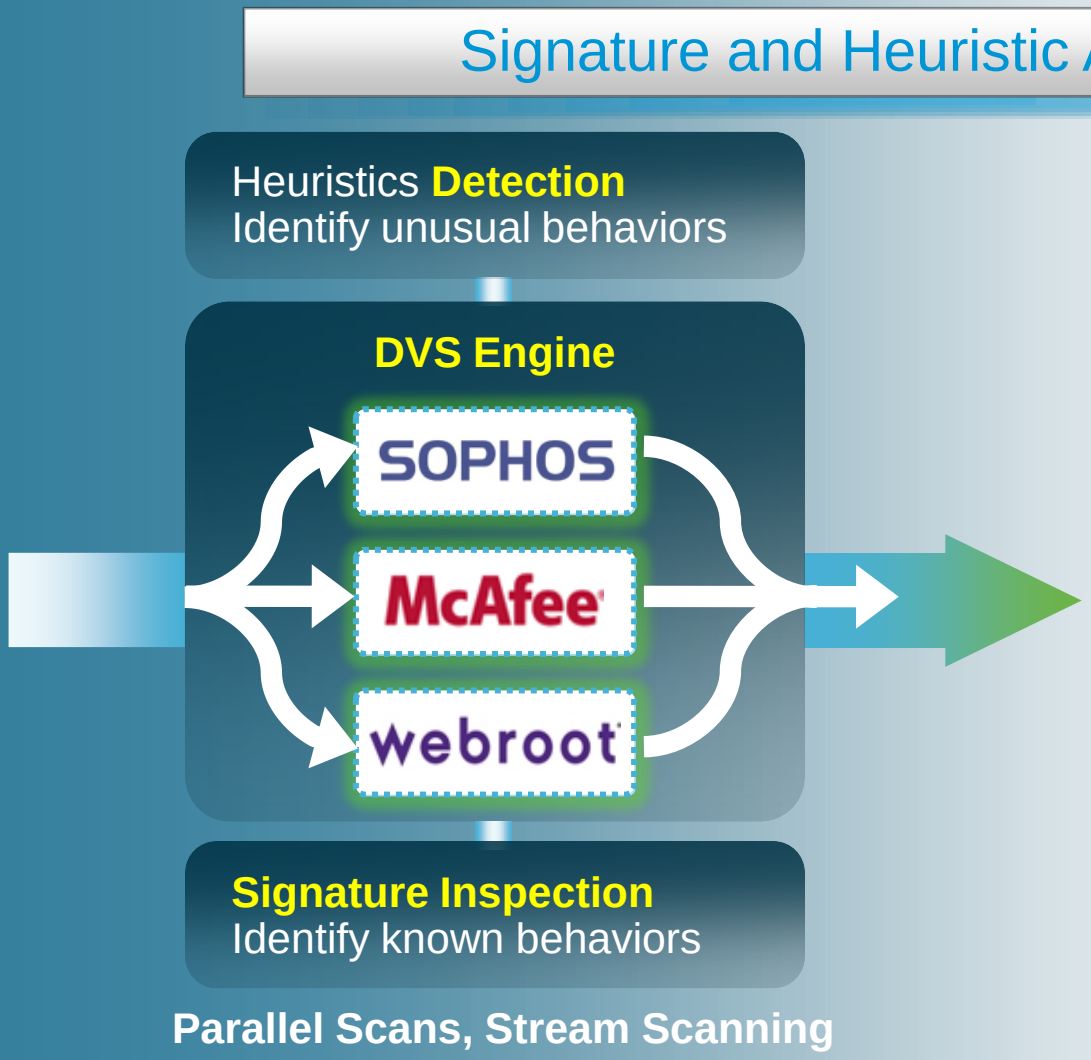
Reputation and Behavioral Analysis

Predictive, Zero-day Protection



Cisco IronPort DVS Engine

Dynamic Vectoring and Streaming

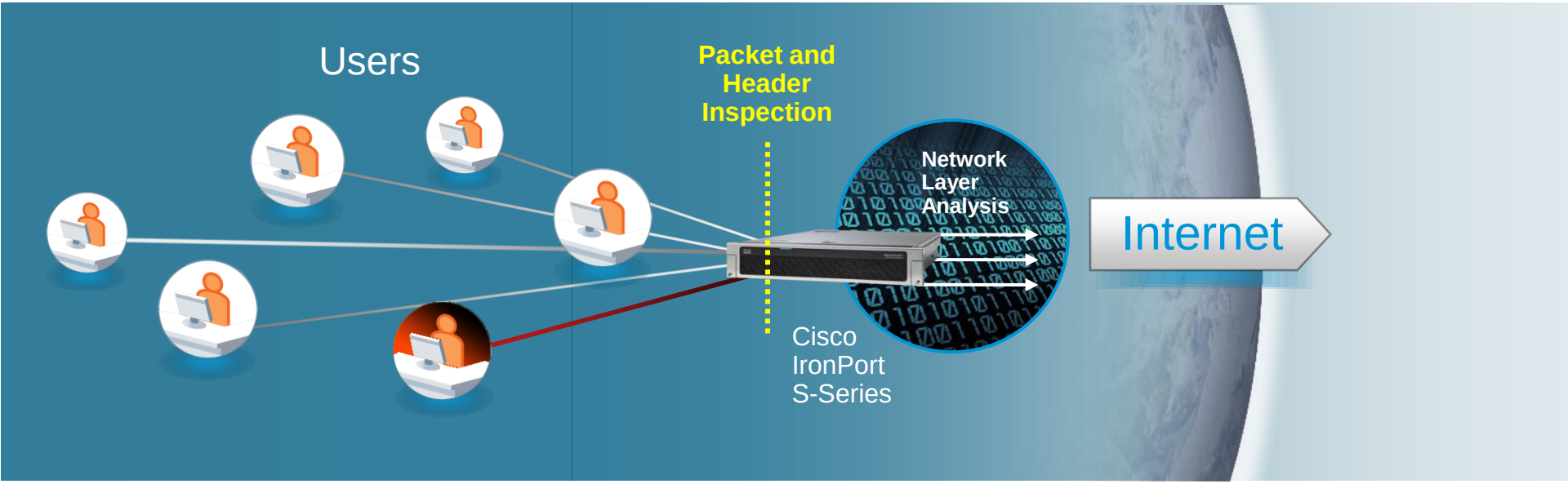


- Wide coverage with multiple signature scanning engines
- Identify encrypted malicious traffic by decrypting and scanning SSL traffic
- Seamless user experience with parallel scanning
- Latest coverage with automated updates

© 2010 Cisco and/or its affiliates. All rights reserved.

Infected Endpoint Detection

Layer 4 Traffic Monitor



Preventing "Phone-Home" Traffic

- Scans all traffic, all ports, all protocols
- Detects malware bypassing Port 80
- Prevents Botnet traffic

Powerful Anti-Malware Data

- Automatically updated rules
- Real-time rule generation using, "Dynamic Discovery"

Also available on the ASA as Botnet Traffic Filter

© 2010 Cisco and/or its affiliates. All rights reserved.

Cisco IronPort Web Security Appliance

Industry Leading Secure Web Gateway

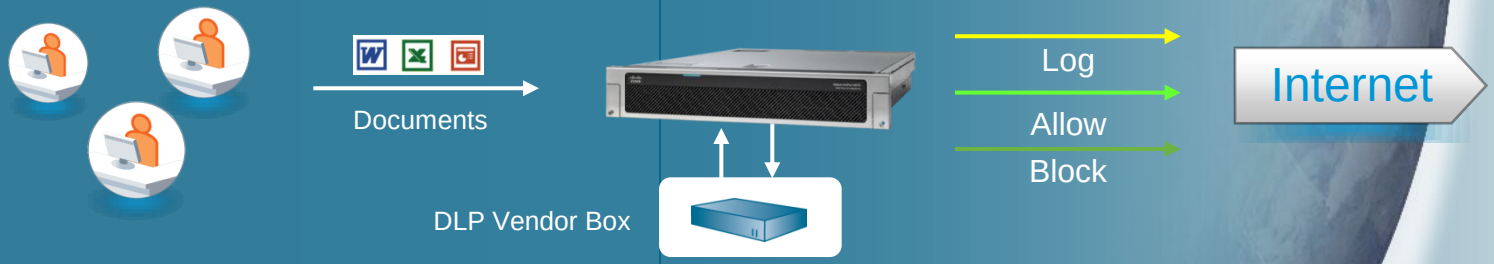
© 2010 Cisco and/or its affiliates. All rights reserved.

Complete Data Security

On-Box Common Sense Security

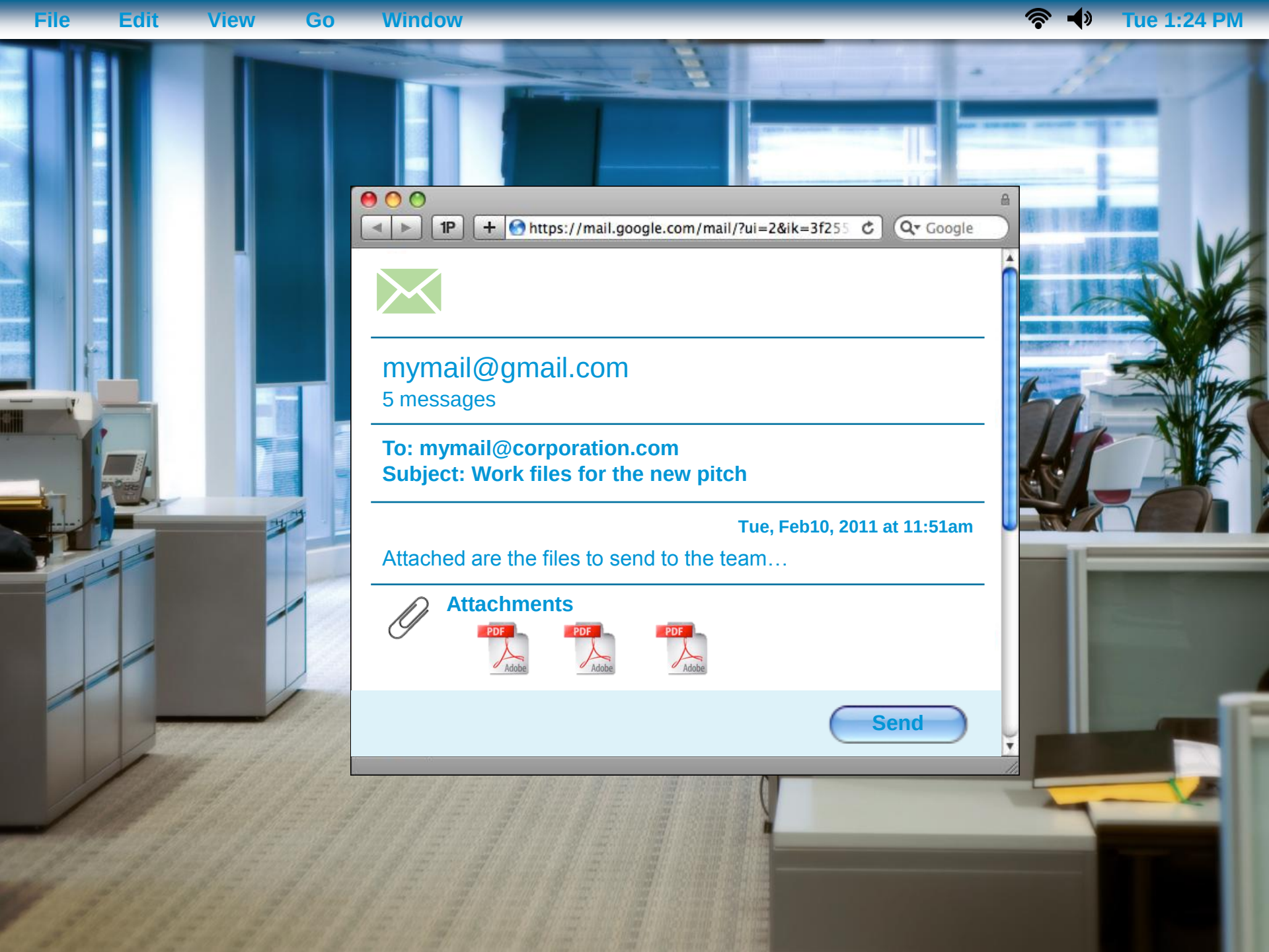
- Allow, block, log based on file metadata, URL category, user and web reputation
- Multi-protocol: HTTP(s), FTP, HTTP tunneled

Off-Box Advanced Data Security



- Deep content inspection: Structured and unstructured data matching
- Performance optimized: Works in tandem with accelerated on-box policies

© 2010 Cisco and/or its affiliates. All rights reserved.


File
Edit
View
Go
Window
Tue 1:24 PM
https://mail.google.com/mail/?ui=2&ik=3f25
Google
mymail@gmail.com
5 messages
To: mymail@corporation.com
Subject: Work files for the new pitch
Tue, Feb10, 2011 at 11:51am
Attached are the files to send to the team…
Attachments
PDF
Adobe
PDF
Adobe
PDF
Adobe
Send

Cisco IronPort Web Security Appliance

Industry Leading Secure Web Gateway

© 2010 Cisco and/or its affiliates. All rights reserved.

Full Context Awareness

Identity

Time

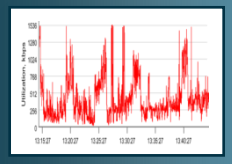
Object

Job Sites	✓	Human Resource
Instant Message	✓	No File Transfer
Facebook	?	Lunch hour
Streaming Media	✓	100 kbps/User
P2P	–	All

Application

Location

Priority



© 2010 Cisco and/or its affiliates. All rights reserved.

Acceptable Use Controls for Web 2.0

Cisco IronPort Web Usage Controls

Enforce Acceptable Use Policies

- Reduce productivity loss
- Reduce risk of legal liabilities
- Control Web 2.0 traffic and web applications
- Control bandwidth intensive streaming media traffic

URL Filtering

- URL database covering over 50M sites worldwide
- Real-time on-box dynamic categorization for unknown URLs
- Auto update every five minutes

Application Visibility and Control

- Deep application control, e.g., IM, Facebook, WebEx
- Bandwidth control for streaming media
- Site content ratings

© 2010 Cisco and/or its affiliates. All rights reserved.

Web Application Controls

Access Control Policy

Instant Messaging
Facebook: Limited Apps
Video: 512 kbps max

Access Control Violation

File Transfer over IM
Facebook Chat, Email
P2P

- Granular control over HTTP, HTTP(s), FTP applications
- Dynamic signature updates maintained by Cisco SIO

Employee in Finance

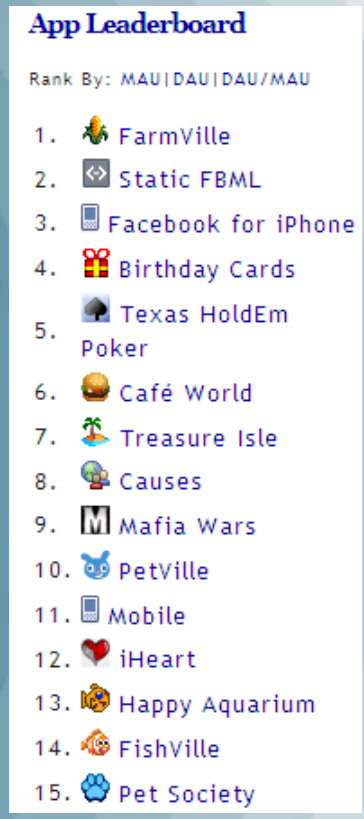
Granular Control over Application Usage

© 2010 Cisco and/or its affiliates. All rights reserved.

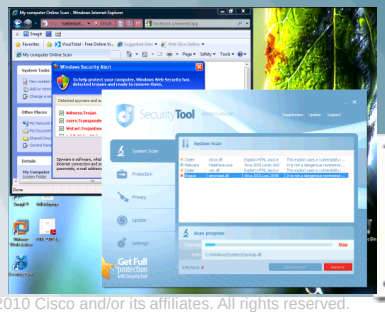
Social Networking Controls

Allow/Block features like Chat, Messaging, Video & audio bandwidth

Allow/Block thousands of Facebook Apps



Block Malware like 'Farm Town' app ad that redirects users to fake antivirus software



© 2010 Cisco and/or its affiliates. All rights reserved.

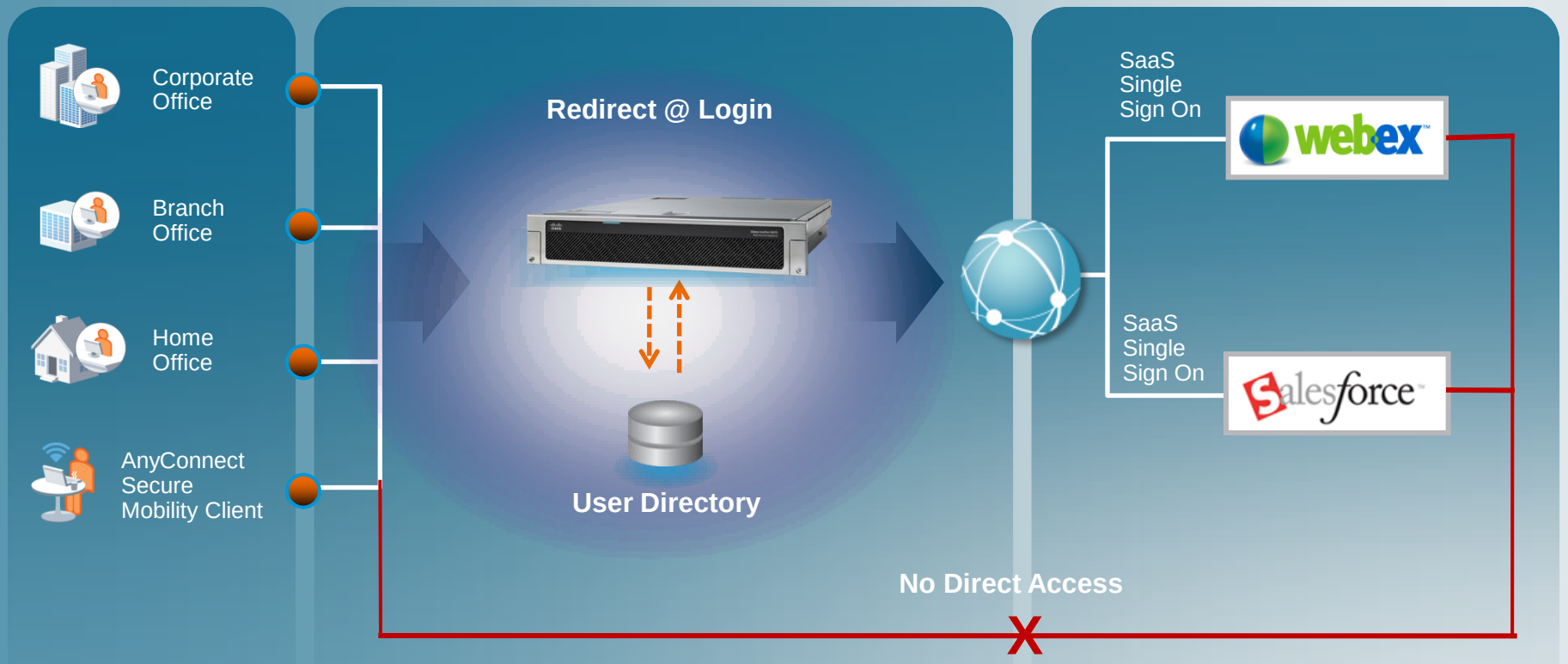
Cisco IronPort Web Security Appliance

Industry Leading Secure Web Gateway

© 2010 Cisco and/or its affiliates. All rights reserved.

SaaS Access Control

Regaining Visibility and Control Through Identity



Visibility | Centralized Enforcement | Single Source Revocation

© 2010 Cisco and/or its affiliates. All rights reserved.

The Mobility Problem Is Getting Harder

The World as We Knew It → **The World Today** → **Un-Managed Devices**

Managed Devices

Un-Managed Devices

© 2010 Cisco and/or its affiliates. All rights reserved.

The Mobile Data Security Challenge

© 2010 Cisco and/

Cisco AnyConnect Secure Mobility

Web Security with Next Generation Remote Access

Choice

Diverse Endpoint Support for Greater Flexibility

Security

Rich, Granular Security Integrated into the network

Experience

Always-on Intelligent Connection for Seamless Experience and Performance

AnyConnect Secure Mobility Client

Network and Security Follows User—It Just Works

Broad Mobile Support

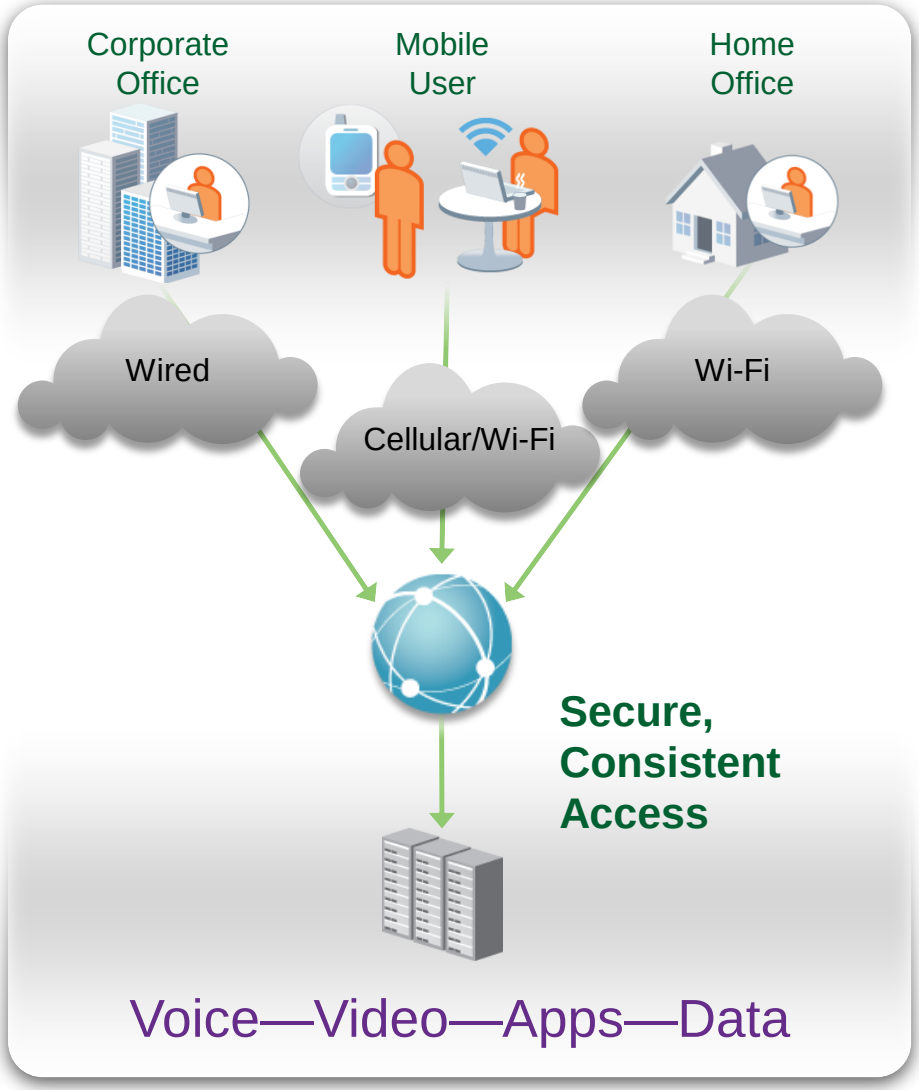
- Fixed and semi-fixed platforms
- Mobile platforms

Persistent Connectivity

- Always-on connectivity
- Optimal gateway selection
- Automatic hotspot negotiation
- Seamless connection hand-offs

Next-Gen Unified Security

- User/device identity
- Posture validation
- Integrated web security for always-on security (hybrid)
- Clientless and desktop virtualization



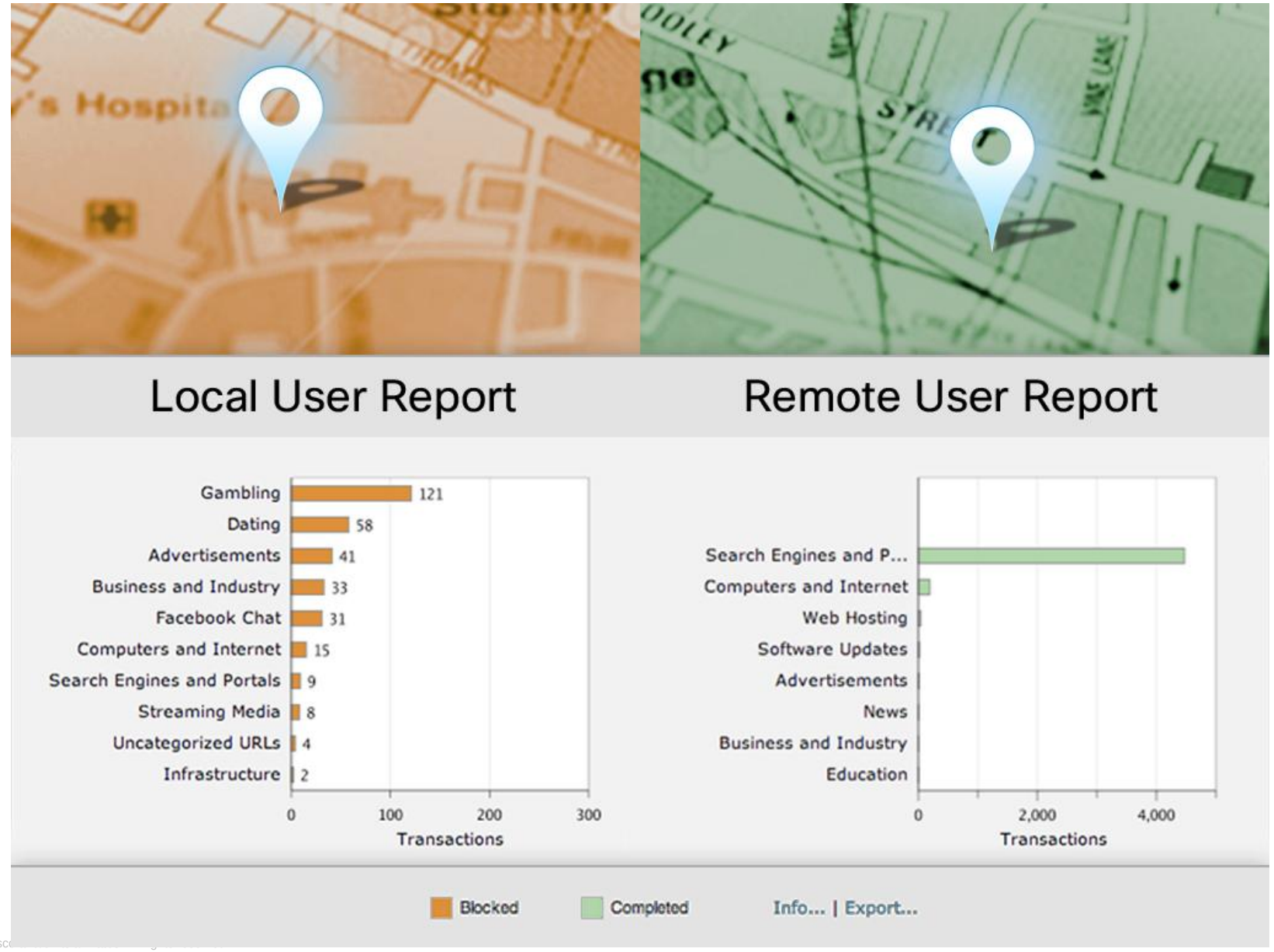
© 2010 Cisco and/or its affiliates. All rights reserved.

AnyConnect 3.0

- "Always On" VPN
- Trusted Network Detection
- Session Mobility
- Optimal Gateway Selection
- Broad protocol support
  - IPsec IKE v2, SSL and DTLS
- Unification of 4 Cisco clients
- Enhanced Security and Mobility
  - Integrated connection management (L2 supplicant)
  - Integrated posture assessment (HostScan)
  - Wired network identity/security (802.1x & MACsec)
  - Support for ScanSafe cloud security
  - Endpoint telemetry feeds

© 2010 Cisco and/or its affiliates. All rights reserved.

Mobile User Reports



© 2010 Cisco

Cisco IronPort Web Security Appliance

Industry Leading Secure Web Gateway

© 2010 Cisco and/or its affiliates. All rights reserved.

Web Security Management

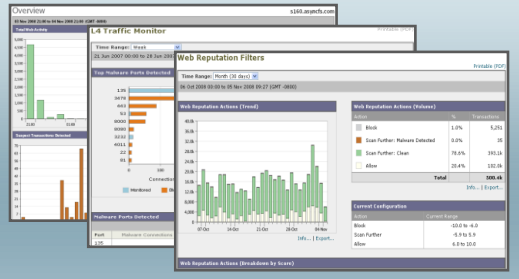
Security Management Appliance

Centralized Management

Centralized Policy Management

Delegated Administration

Centralized Reporting



In-Depth Threat Visibility

Extensive Forensic Capabilities

Insight
Across Threats, Data and Applications

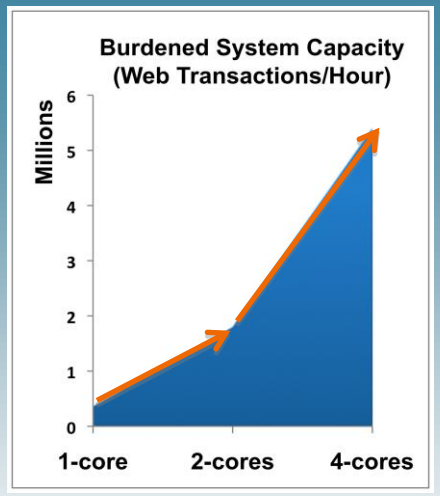
Control
Consistent Policy Across Offices and for Remote Users

Visibility
Visibility Across Different Devices, Services, and Network Layers

© 2010 Cisco and/or its affiliates. All rights reserved.

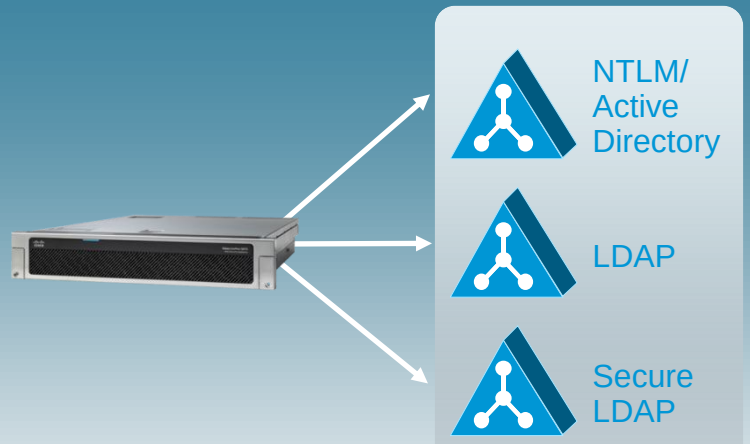
High-Performance Proxy Platform, Integrated Authentication

Multi-Core Optimization



- Addresses latency issues associated with anti-virus scanning
- Enables multi-scan features for improved security efficacy
- Optimized for rich web content

Integrated Identity and Authentication



- Identity Based Policies
- Transparent, single sign-on (SSO) authentication against Active Directory
- Guest Policies, Re-Auth

© 2010 Cisco and/or its affiliates. All rights reserved.

Appliance or Cloud ?

ScanSafe

- Pioneer in SaaS Web Security
- Over 34% market share in SaaS Web Security (IDC)
- Multi-award winning product portfolio
- Millions of users
- Billions of Web requests scanned every day
- 100% Availability

Customers

IKEA, Shell, Disney, Lilly, Louis Vuitton, AkzoNobel

Awards

SC Magazine Awards 2007, SC Magazine Awards 2008, SC Magazine Awards 2009, Network Products Guide Product Innovation 2010

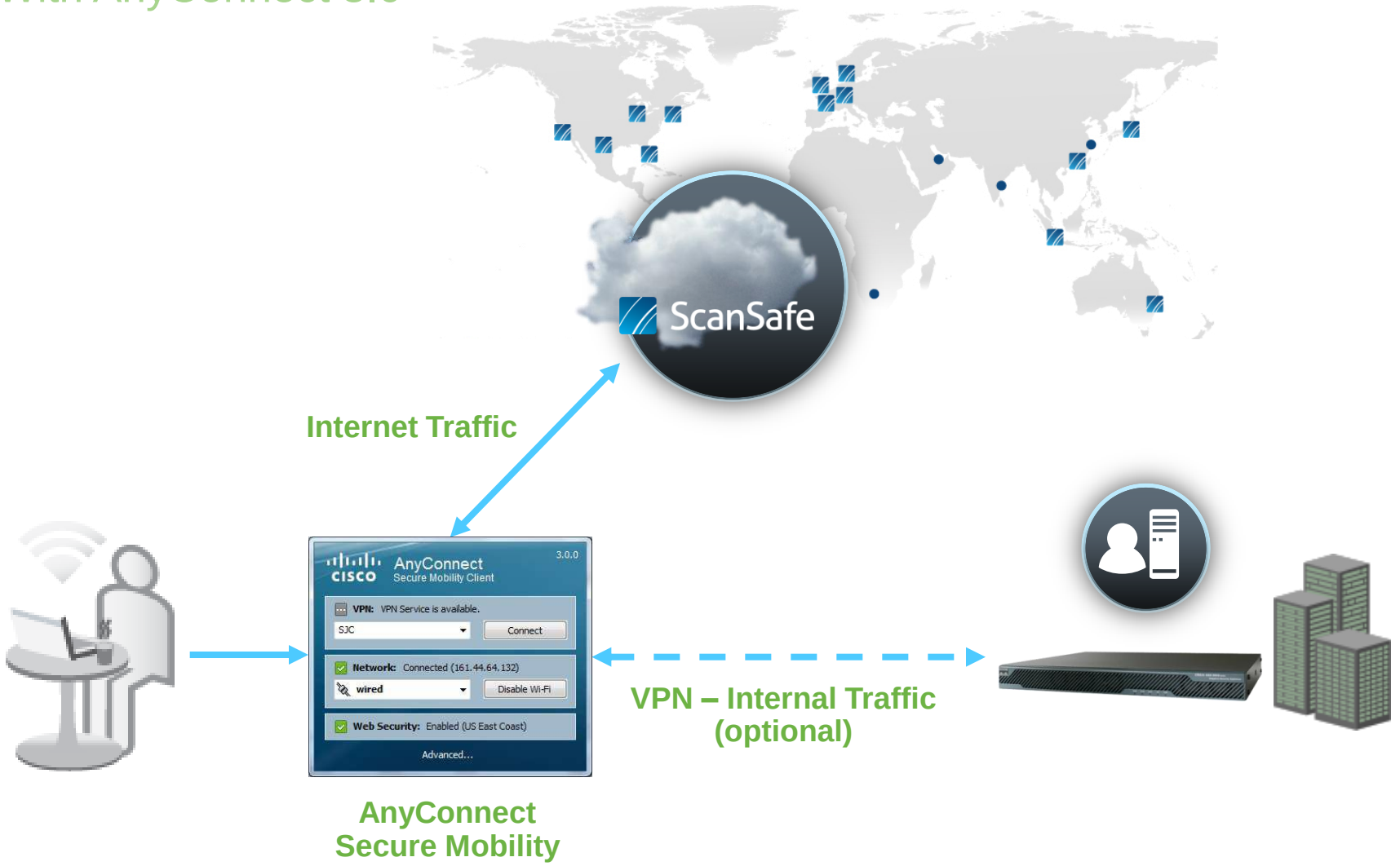
Partners

at&t, Sprint, orange, vodafone, TELUS

© 2010 Cisco and/or its affiliates. All rights reserved.

ScanSafe Secure Mobility

With AnyConnect 3.0



© 2010 Cisco and/or its affiliates. All rights reserved.

Thank you.