

Sponzor komunikacijskih tehnologija



Sponzori konferencije



SG Leasing d.o.o.



Komunikacijski partner



Partner digitalnog oglašavanja i video nadzora



Partneri konferencije



COMPUTECH



Tehnološki sponzor



Medijski pokrovitelji

vecernji.hr



MREŽA

racunalo.com



Cisco Expo 2010

24.-26. ožujka 2010.

Hotel Le Méridien Lav
Split

Kolaboracija - nova snaga poslovne suradnje



welcome to the human network.





Cisco Expo
2010

Cisco IronPort E-mail Security Solution

Kolaboracija -
nova snaga poslovne suradnje

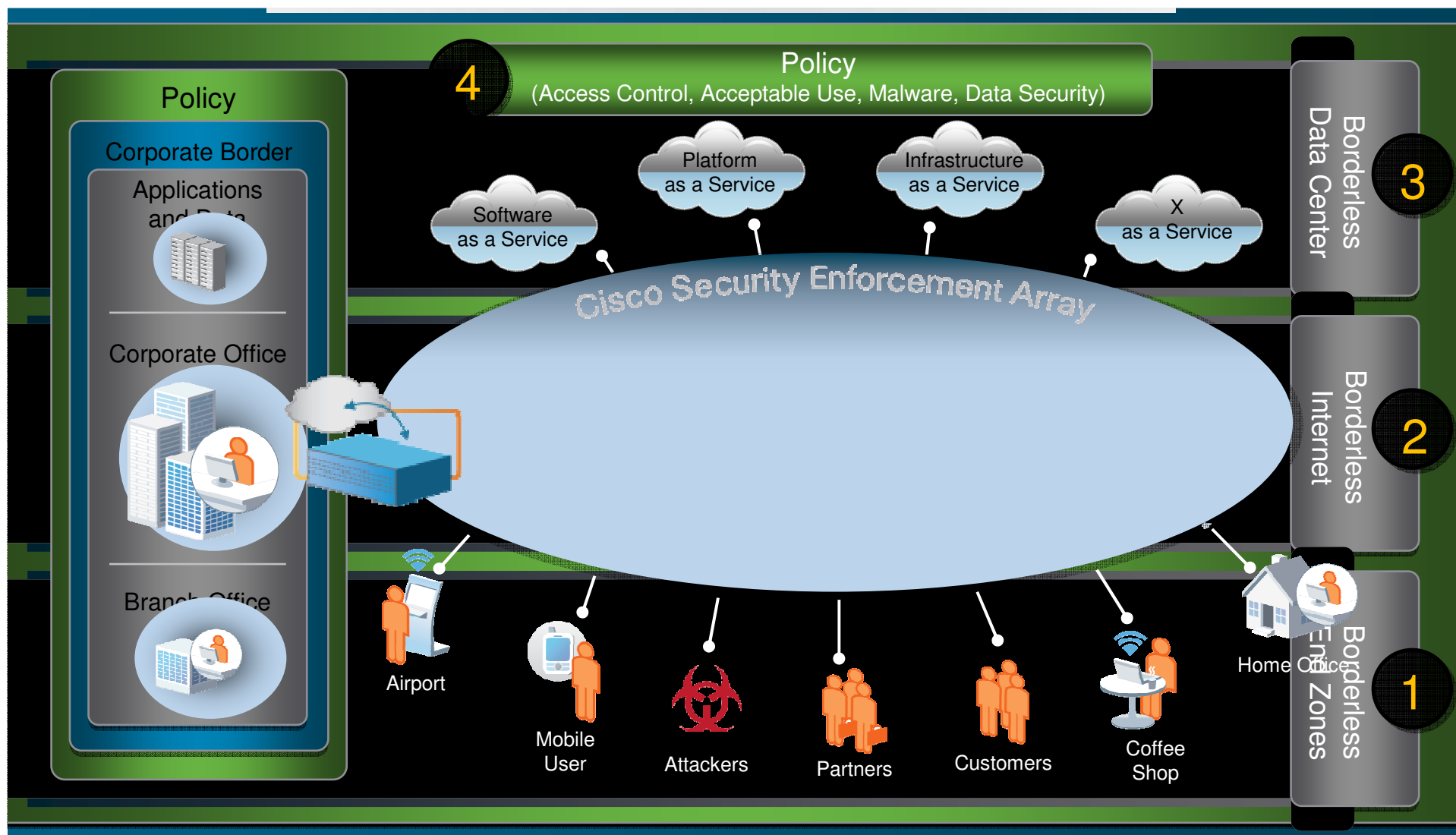


Borderless Advanced Protection - Hrvoje Dogan

Agenda

1. About Cisco IronPort and Cisco Security
2. The Power for Advanced Protection
3. Cisco IronPort E-mail Security Appliances
4. Don't Believe What We Say – Try It Out!

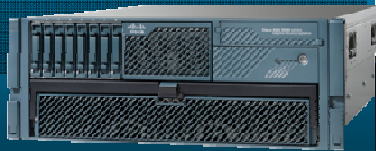
Cisco's Architecture for Borderless Network Security



Pillar 2: Borderless Security Array

Advanced Scanning and Enforcement Capabilities

Cisco Adaptive
Security Appliance



Cisco Integrated
Services Routers



Cisco IronPort
Web Security
Appliance



Cisco IronPort
Email Security
Appliance

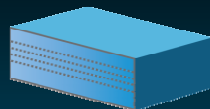


Access Control | Acceptable Use | Data Security | Threat Protection

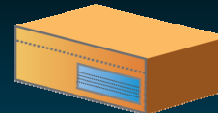
Integrated into the Fabric of the Network



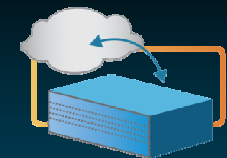
VM Software



Appliance



Security Module



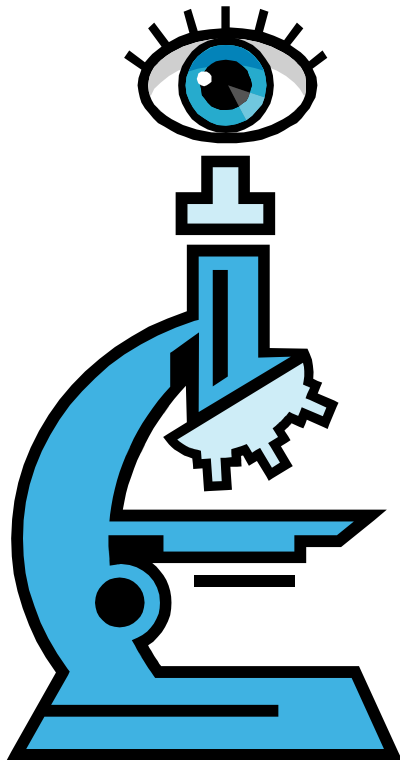
Hybrid Hosted

The Power for Advanced Protection



A Seismic Shift

1. **2000-2008:** IT security products look deeper



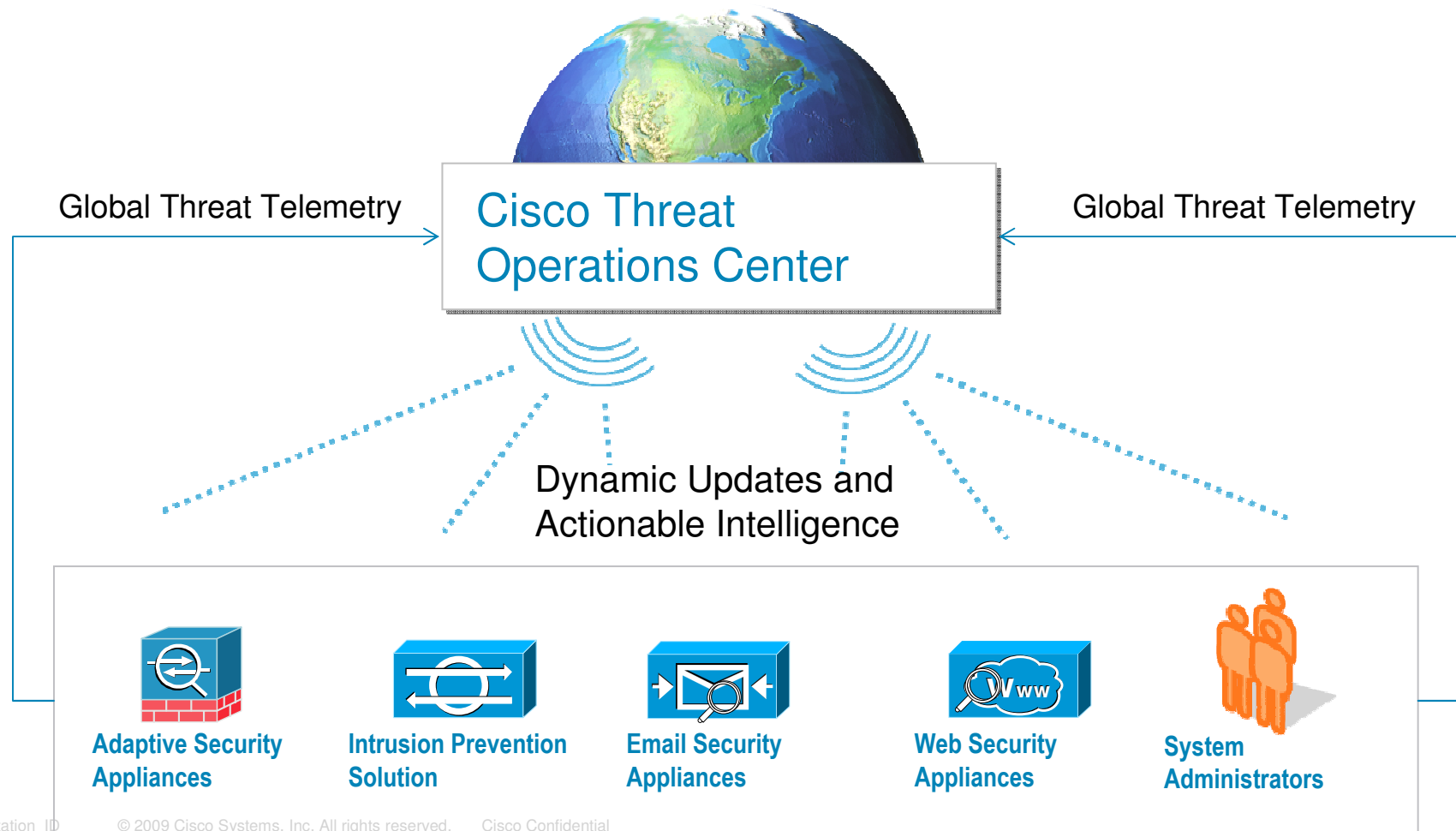
- **2009:** Cisco Security products look around, respond faster



Cisco Security Intelligence Operations (SIO)

Overview

Most Accurate Protection Against a Broad Range of Threats



Cisco SIO

Key Components

Powerful Ecosystem Enables Fast, Accurate Protection



Cisco SIO

Cisco SensorBase

Largest Network, Highest Data Quality, Unmatched Breadth



Cisco SensorBase Network

Unmatched Visibility Into Global Threats

Most Devices

1M security devices, 10M
clients shipped per year

Core Internet routers

Cloud-based services

Largest Footprint

30% of the world's
email traffic

200+ parameters

368GB per day sensor
feeds

Diverse Sources

Eight of the top ten ISPs

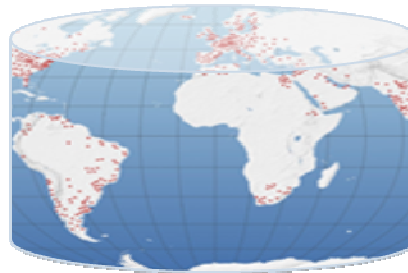
Fortune 500, Global 2000,
universities, SMBs

152 third-party feeds

First to Combine Network and Application Layer Data

Cisco SensorBase Network

Unmatched Breadth



SensorBase Network

Email

From: Bill Gates
To: John Chambers
Cc:
Subject: Free NFL Game[IronPort SUSPECTED SPAM]

Football is back, life may resume again!
...channel and
...with our f

From: Bill Gates
To: John Chambers
Cc:
Subject: Free NFL Game[IronPort SUSPECTED SPAM]

Football is back, life may resume again!
Know all the games, what time what channel and
have all the details for every game with our f
<http://69.247.209.124>

Spam with Malicious
Attachment



Firewall / IPS



Dir



Directed Attack

Don't Miss A Single game This Season...
Download Your Free Season Tracker and Stay Up To Date With Every Game

Free NFL Game Tracker

Week 1

Thursday, September 06

Time (EST)	Top Passer	Top Rusher	Top Receiver
10:10 @ KC-41	IND Peyton Manning 288 Yds	IND Joseph Addai 115 Yds	IND Reggie Wayne 115 Yds

Sunday, September 09

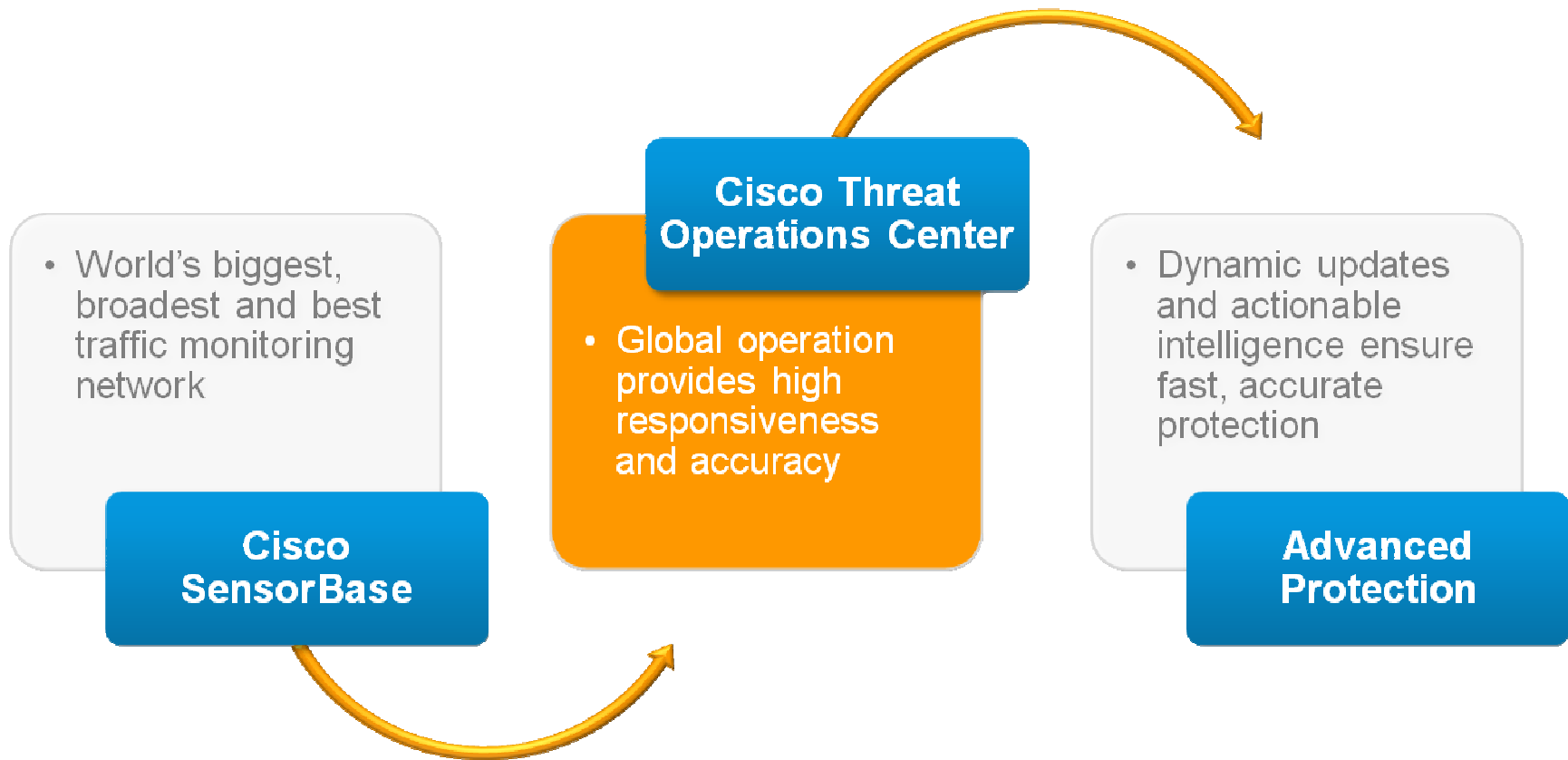
Time (EST)	Tickets	Network	Channel	HD-Channel	Home	Away	Weekend One
1:00 PM	Tickets	CBS	709	723	130	119	
1:00 PM	Tickets	FOX	711	725	125	123	
1:00 PM	Tickets	CBS	707		108		
1:00 PM	Tickets	FOX	712	726	147	146	
1:00 PM	Tickets	CBS	705	720	103	121	
1:00 PM	Tickets	CBS	708	722	122	101	
1:00 PM	Tickets	FOX	713	724	114	126	
1:00 PM	Tickets	CBS	704	719	119	143	
1:00 PM	Tickets	CBS	706	721	140	107	
4:15 PM	Tickets	FOX	715	726	119	147	
4:15 PM	Tickets	FOX	714	725	106	123	
4:15 PM	Tickets	FOX	713	724	125	132	
8:15 PM	Tickets	NBC	83		127	126	Radio

Malware Distributing Site

Cisco SIO

Cisco Threat Operations Center (TOC)

**Advanced Research and Development, Security Modeling,
Experienced Analysts**



Cisco Threat Operation Center

Advanced Research and Development

1. Millions in R&D investment

Threat experts and statisticians

Equipment and infrastructure

Thought leadership, prevention
and best practices expertise

76 patents

2. Innovative services

IPS Global Correlation

ASA Botnet Traffic Filters

Virus Outbreak Filters

Reputation Filters (IPS, email,
web, etc.)

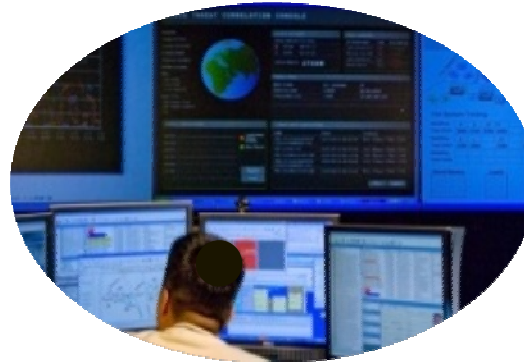


Cisco Threat Operations Center

Ensuring Accuracy and Responsiveness



Parameters Under Management		
IP Address Reputation	19,111,326	36.4% corporate
URL Reputation	160,003,098	99.9% of all Servers C...
Product Vulnerability	39,983	
Protocol Signatures	3,261	25.1% Vul...



Outdated Security Rules	Deployment Interval	Last D...
Email: IronPort Anti-Spam	5 minutes	2009-01-
Email: VOF	5 minutes	2009-01-
Firewall: Protocol Violation	1 week	2009-01-
Anomaly Detection	1 week	2009-
...	15 minutes	
...	5 minutes	

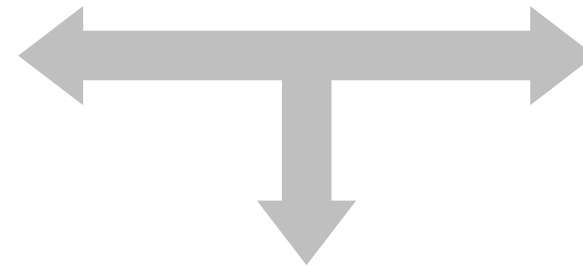
Experienced Analysts

500 analysts

European and Asian languages

1 Cisco Fellow

80+ Ph.D.s, CCIEs, CISSPs, MSCEs



Powerful Tools

Dynamic updates

Correlation and data mining

Advanced rule approval, creation and publishing applications

24x7x365 Operations

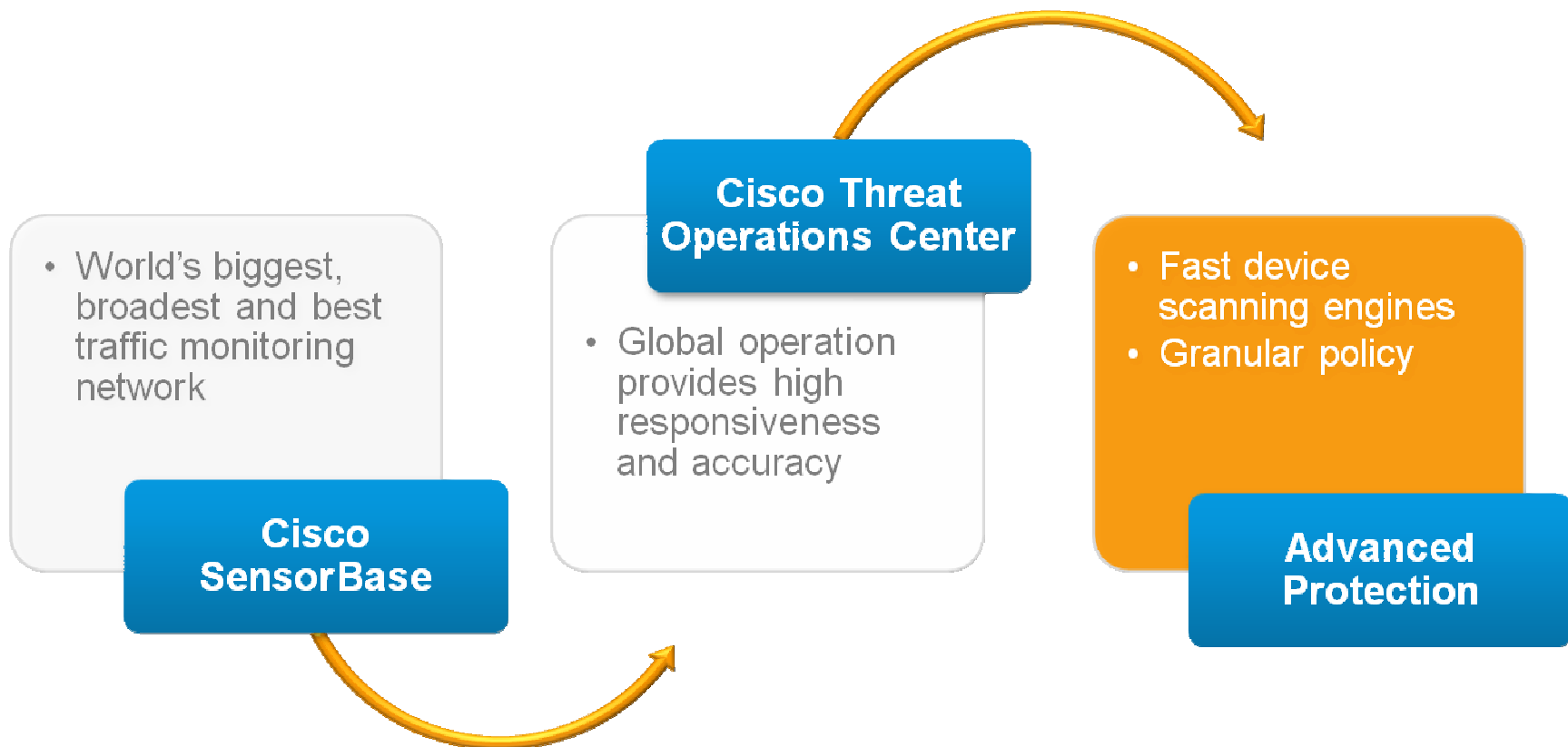
5 threat operations center locations around the globe

San Jose, San Bruno, Austin, North Carolina, Shanghai

Cisco SIO

Broadest Enforcement Capabilities

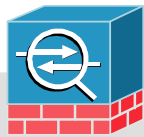
Fast Device Scanning Engines and Granular Policy



Advanced Protection

Putting It All Together

Cisco Products and Services: High-performance, flexible enforcement points



**Adaptive Security
Appliances**



**Intrusion Prevention
Solution**



**Web Security
Appliances**



**Email Security
Appliances**



**Hosted Email
Services**

Security Filters: Industry's most effective security features

**Virus
Outbreak
Filters**

Anti-Spam

**Email
Reputation
Filters**

**Web
Reputation
Filters**

**IPS Reputation
and Signature
Filters**

**Firewall Botnet
Traffic Filters**

Cisco SIO: Cloud-based intelligence to power Cisco security services

**Live
Reputation
Scores**

**New and
Updated
Signatures**

**Authored
Rule Sets**

**Dynamic
Rule Sets**

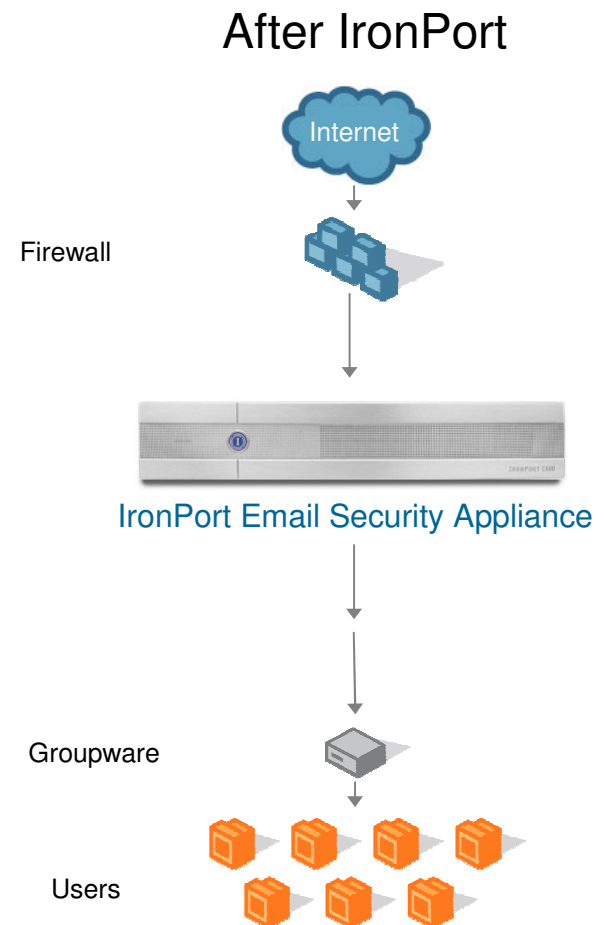
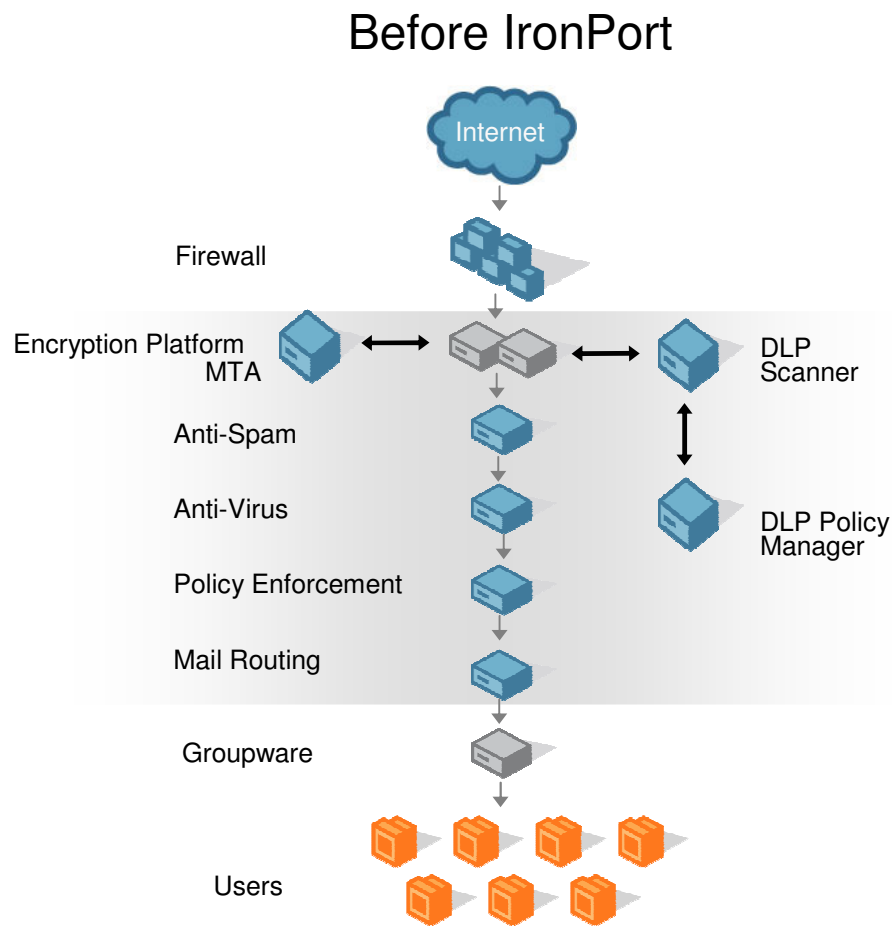
**Auto-Updates
Every 5 minutes**

Cisco IronPort E-mail Security Appliances



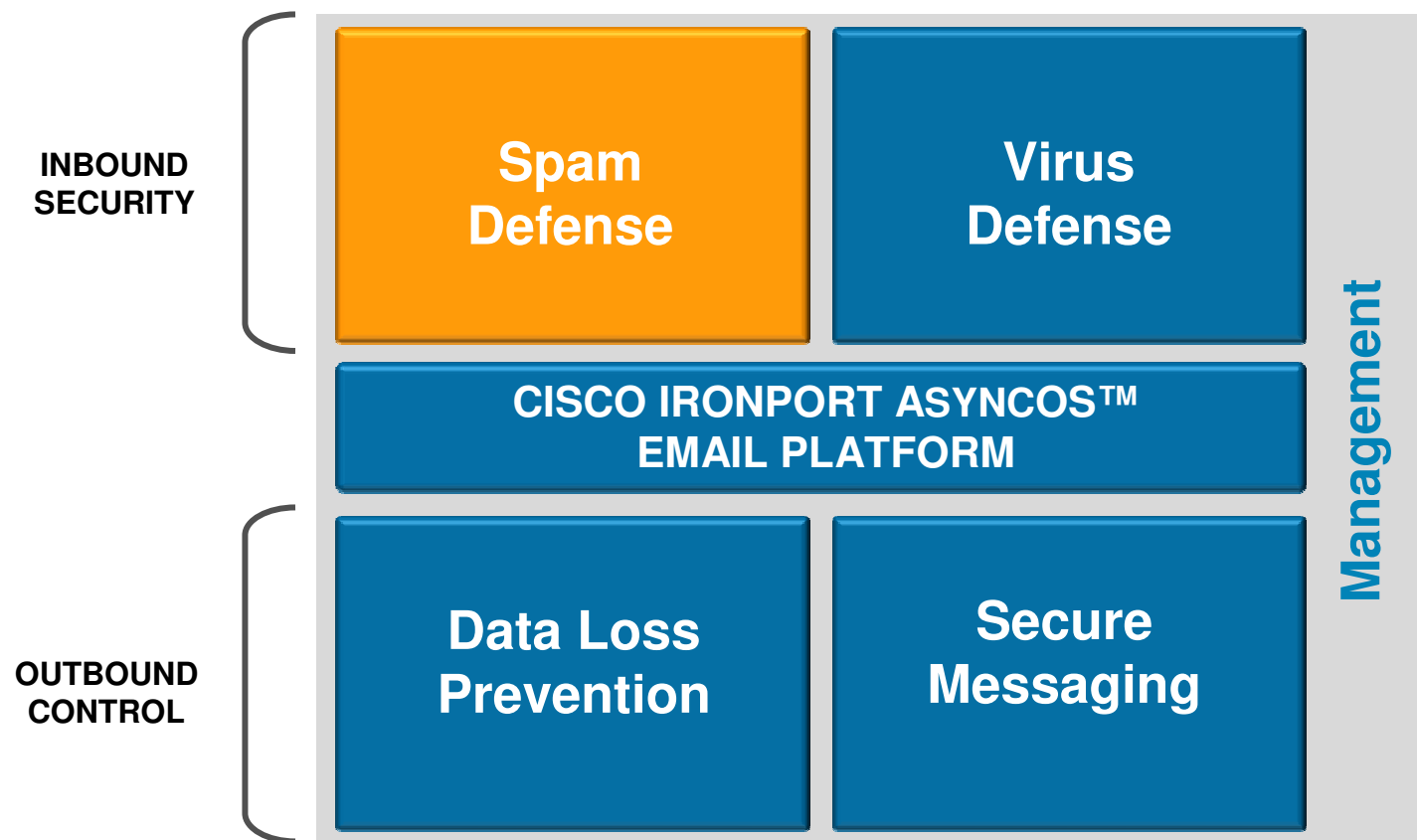
Cisco IronPort Consolidates the Network Perimeter

For Security, Reliability and Lower Maintenance



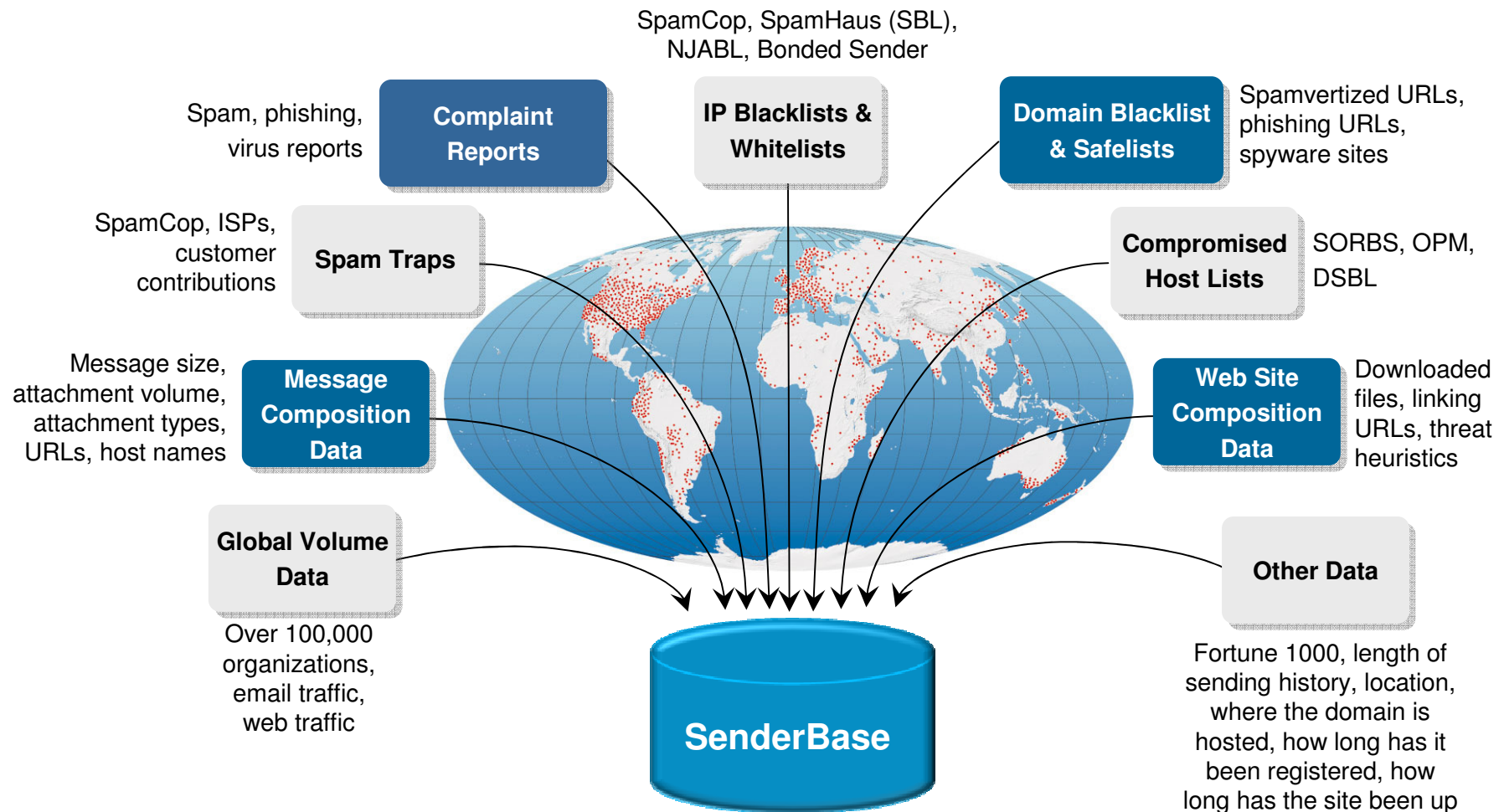
Email Security Architecture

Inbound Security, Outbound Control

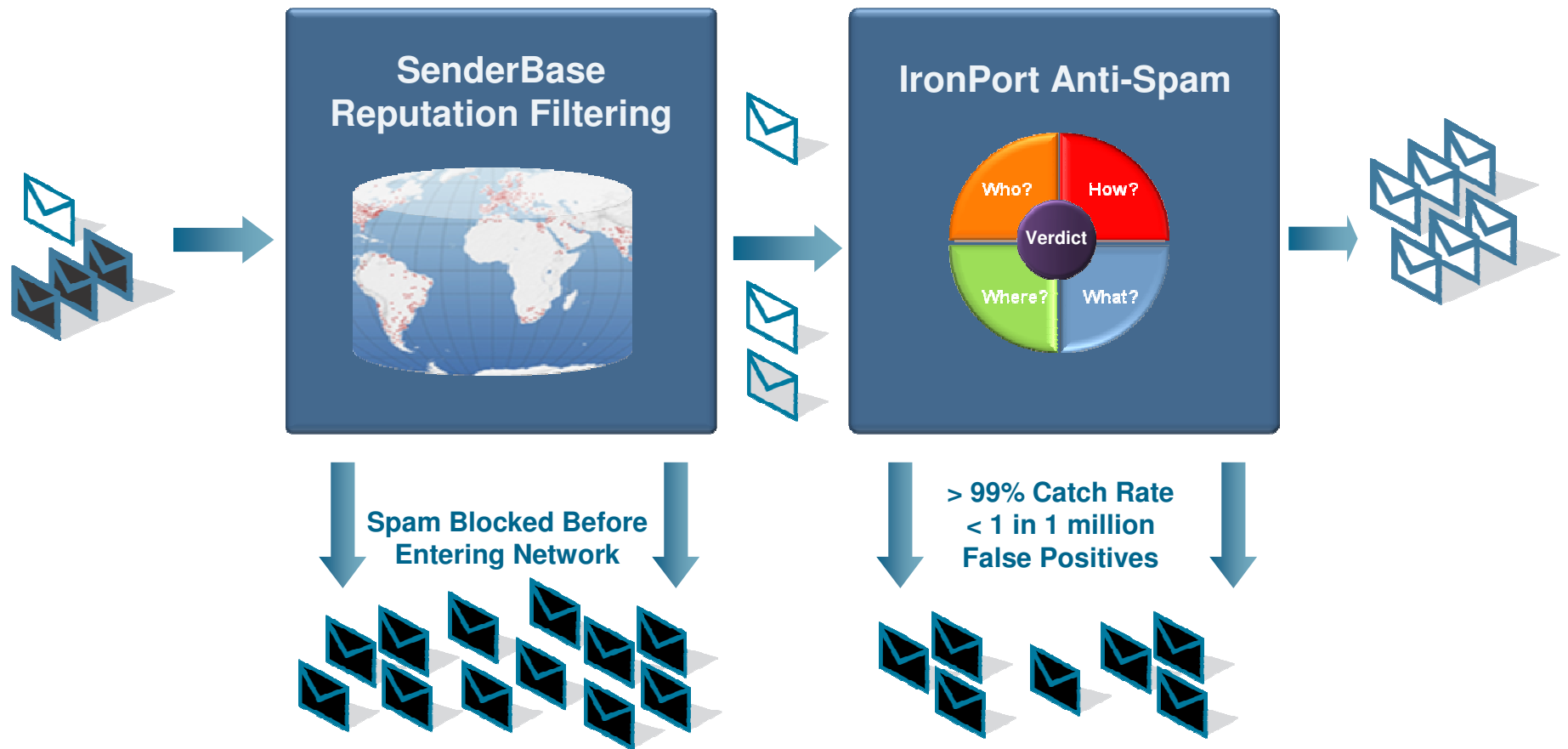


Cisco IronPort SenderBase

Breadth and Quality of Data Makes the Difference

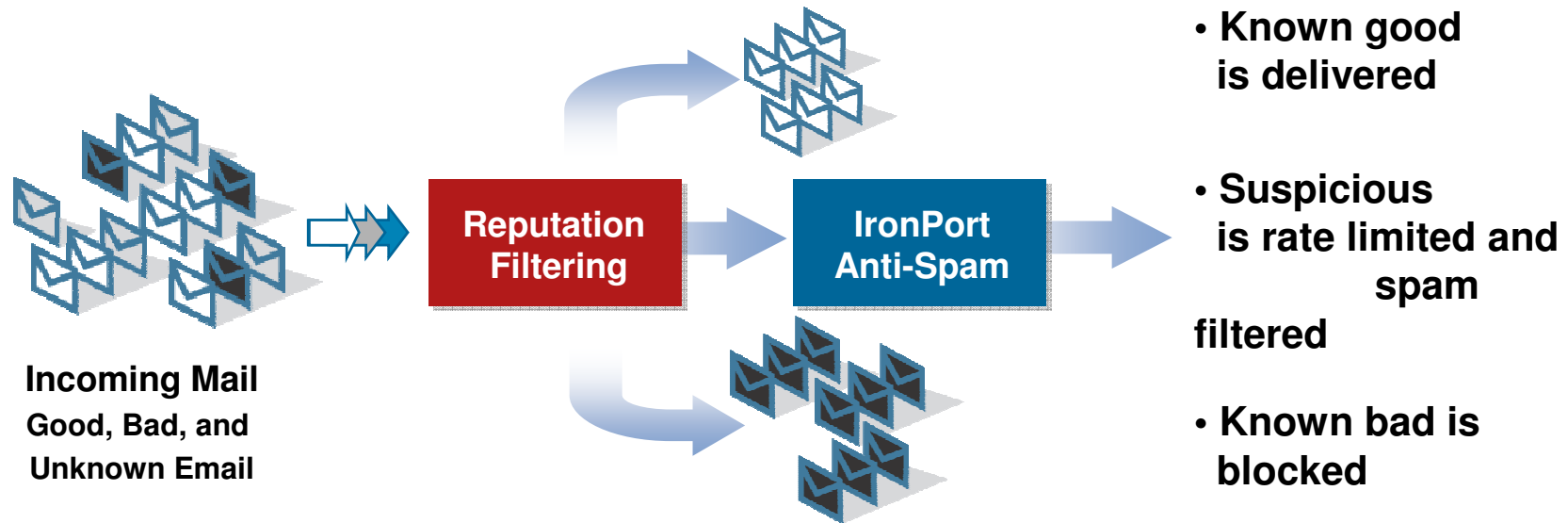


Anti-Spam Defense in Depth



SenderBase Reputation Filtering

Real Time Threat Prevention



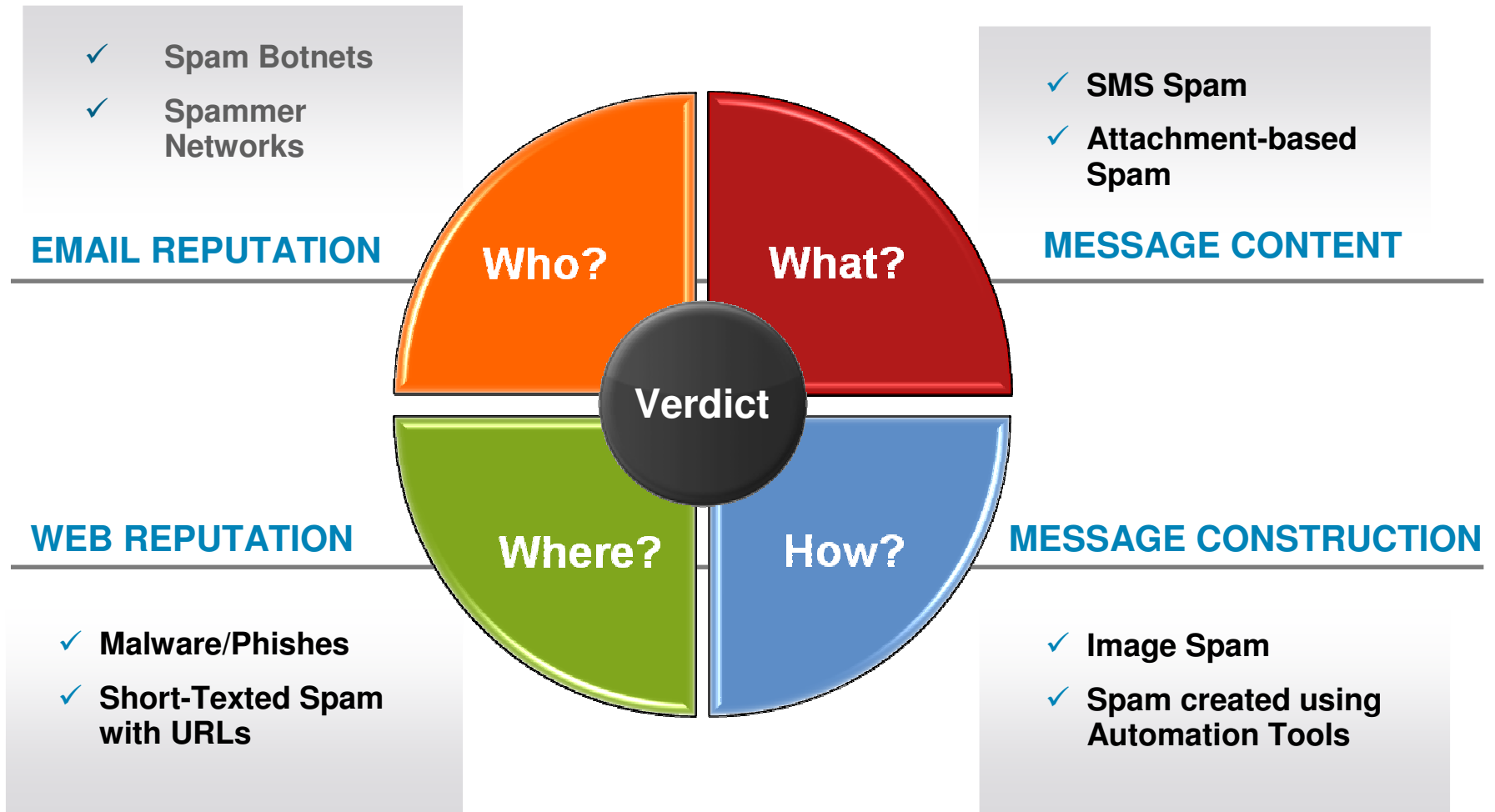
Cisco on Cisco

Our Corporate Email Experience

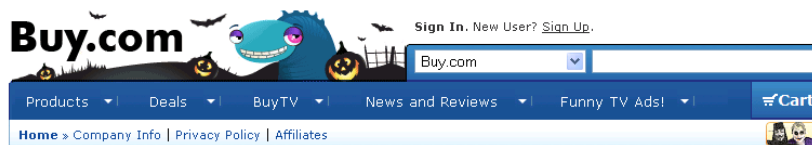
Message Category	%	Messages
Stopped by Reputation Filtering	93.1%	700,876,217
Stopped as Invalid recipients	0.3%	2,280,104
Spam Detected	2.5%	18,617,700
Virus Detected	0.3%	2,144,793
Stopped by Content Filter	0.6%	4,878,312
Total Threat Messages:	96.8%	728,797,126
Clean Messages	3.2%	24,102,874
Total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

Cisco IronPort Anti-Spam

Defense in Depth Spam Protection



Marketing Message Detection – The Problem



Buy.com Sign In. New User? Sign Up.

Products Deals BuyTV News and Reviews Funny TV Ads! Cart

Home » Company Info | Privacy Policy | Affiliates

Create My Account

How do I create a My Account?

To create a My Account, please fill out the appropriate information below.

* Required fields

My Account Login

* Enter Your eMail Address

* Select Your Birth Year

Select One

[Why is this required?](#)

* Choose A Password

(must be between 5 & 20 characters)

* Verify Your Password Password Hint (Optional)

Terms of Use

Terms and Conditions

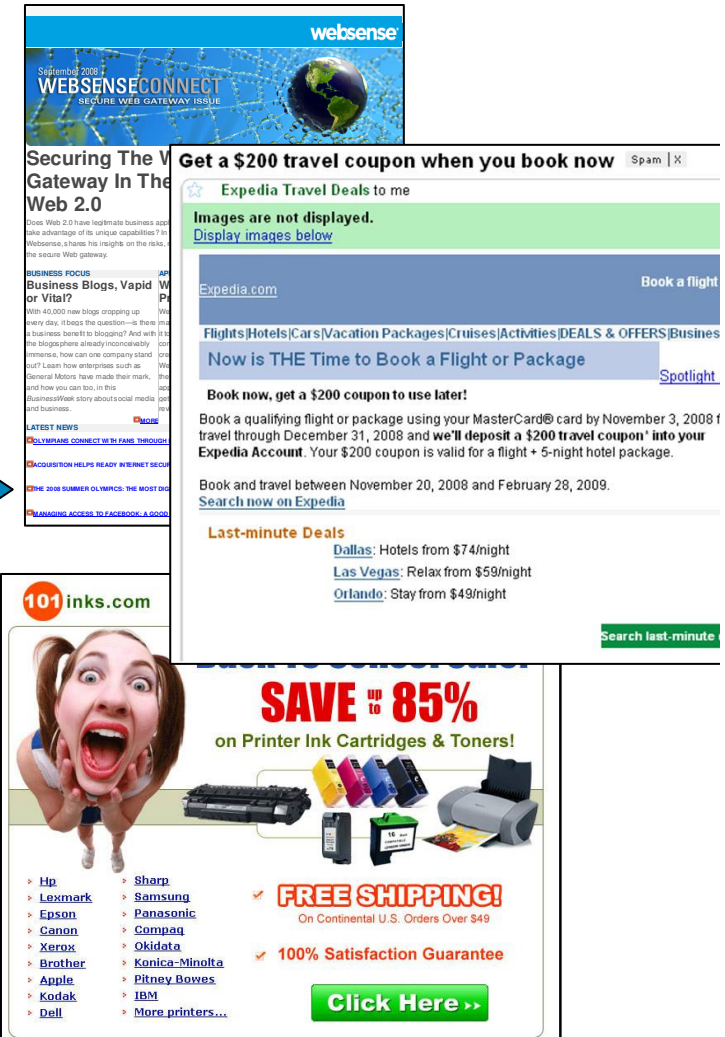
READ CAREFULLY. This Terms of Use Agreement ("Terms of Use") applies to use of the Buy.com website located at

[Click here for a full screen view of the terms.](#)

* ☒ I Agree to the Buy.com Terms and Conditions.

Privacy Policy
At Buy.com, your privacy is a top priority. Please read our privacy policy details.

...
All information collected from you will be shared with Buy.com and its affiliate companies.



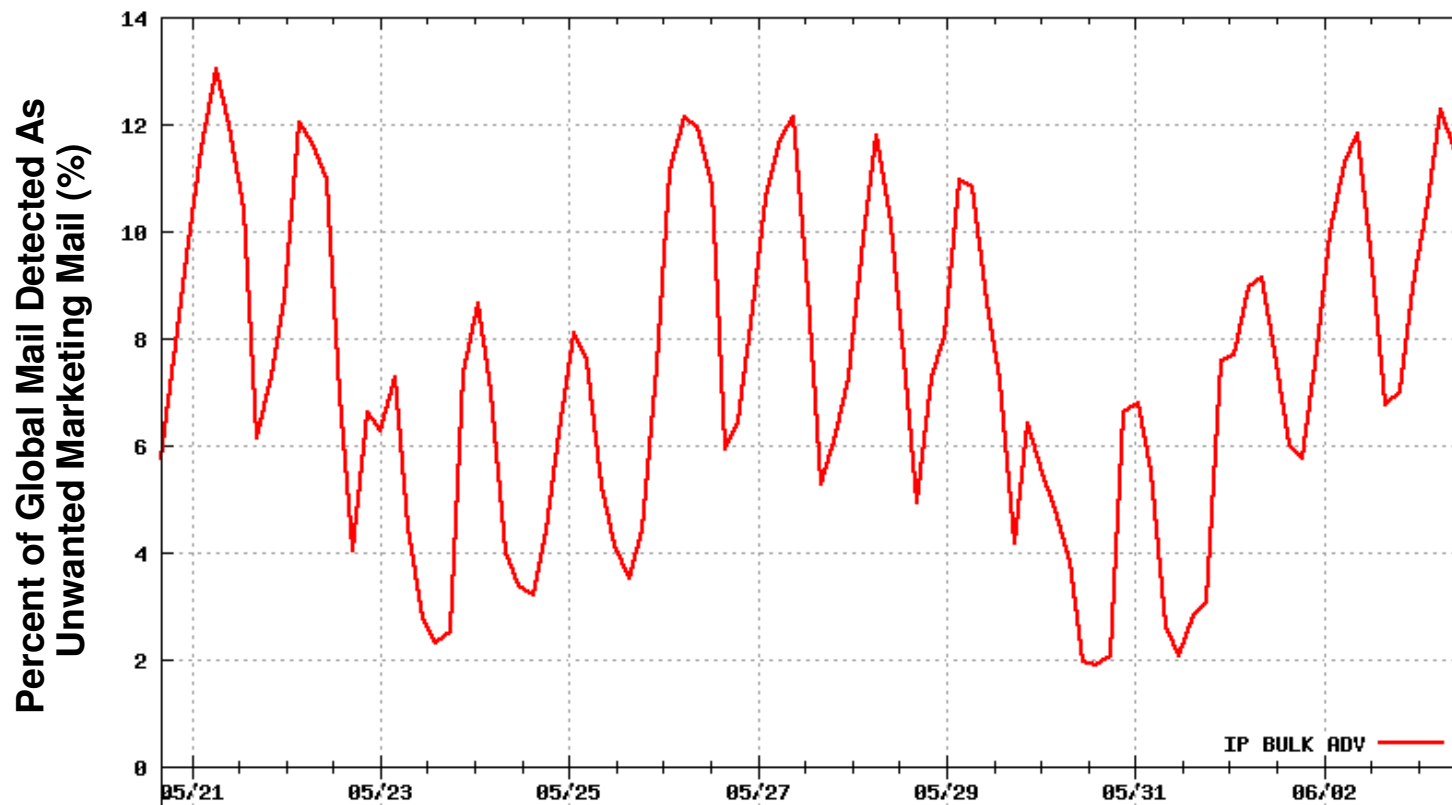
The collage includes several promotional banners and advertisements:

- websense**: "September 2008 WEBSENSECONNECT SECURE WEB GATEWAY ISSUE".
- Securing The Web Gateway In The Web 2.0**: Article snippet about business blogs and Web 2.0 security.
- Expedia Travel Deals**: "Get a \$200 travel coupon when you book now". Includes links for flights, hotels, cars, etc.
- 101 inks.com**: "SAVE up to 85% on Printer Ink Cartridges & Toner!". Lists various printer brands like HP, Lexmark, Epson, etc.
- FREE SHIPPING**: "On Continental U.S. Orders Over \$49".
- 100% Satisfaction Guarantee**.
- Click Here >>** button.

Marketing Message Detection –

The Solution: AsyncOS 7.0

- **Blocks messages from major bulk mailers** (i.e. Constant Contact, Vertical Response)
- **Determination based on user voting** (i.e. Apple iTunes, Dell, United Airlines are legitimate)



Marketing Message Detection

- Stops aggressive bulk mailers
- Can be applied on user-by-user basis
- Flexible actions: tag, drop, quarantine
- Separate reporting for visibility

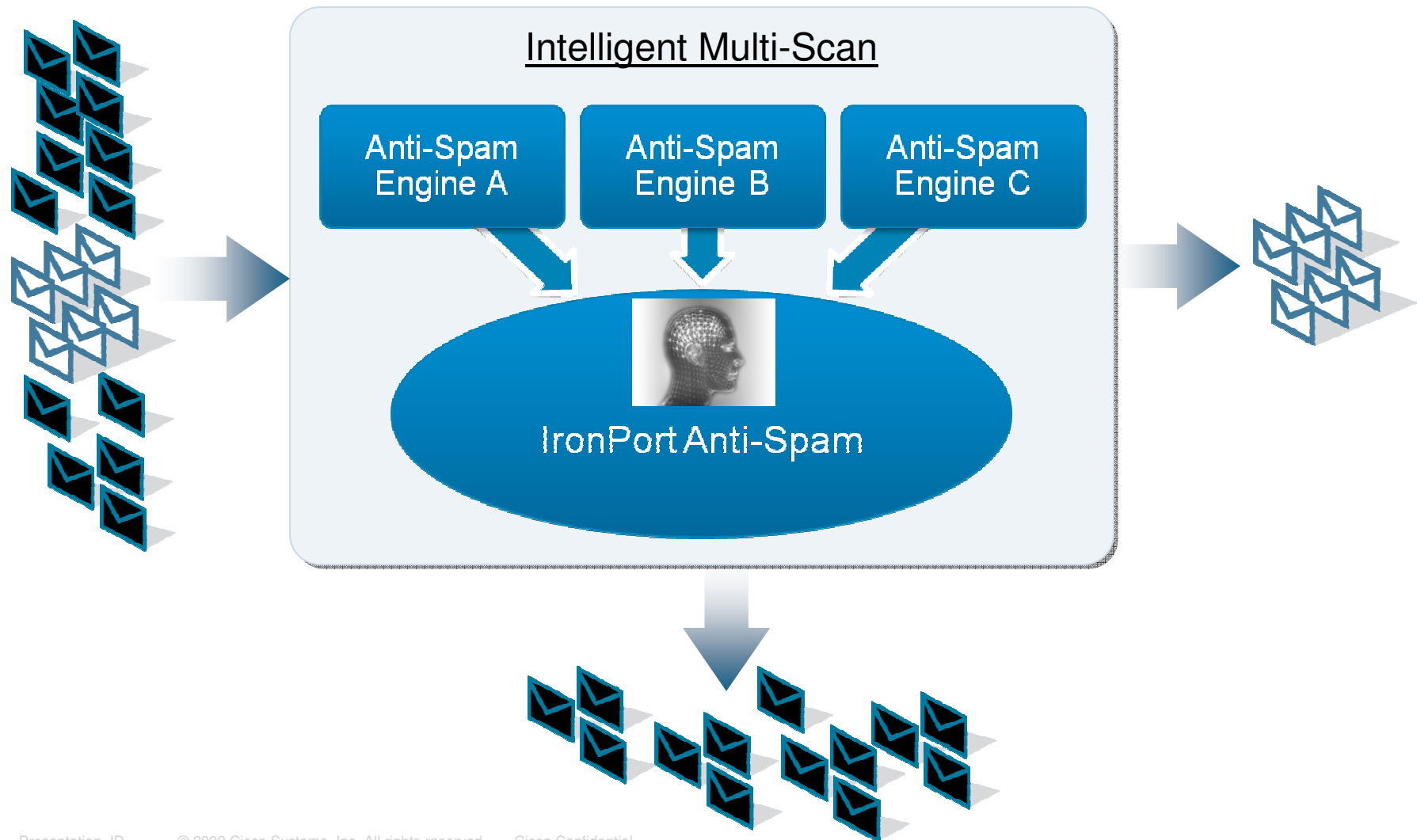


Incoming Mail Summary		
Message Category	%	Messages
Stopped by Reputation Filtering	33.5%	98.1k
Stopped as Invalid Recipients	11.5%	33.6k
Spam Detected	15.3%	44.8k
Additional Spam Detected by Intelligent Multi-Scan	15.3%	44.8k
Virus Detected	4.4%	13.1k
Stopped by Content Filter	20.0%	58.6k
Total Threat Messages:	75.0%	293k
Marketing Messages	15.8%	44.8k
Clean Messages	10.2%	70.8k
Total Attempted Messages:	100.0%	415.6k

Marketing Messages Settings	
Enable Marketing Message Scanning:	☐ No ☒ Yes
Apply This Action to Message:	Deliver v Send to Alternate Host (optional):
Add Text to Subject:	Prepend v [MARKETING]
Advanced	Add Custom Header (optional): Header: Value: Send to an Alternate Envelope Recipient (optional): Email Address: (e.g., employee@company.com) Archive Message: ☒ No ☐ Yes

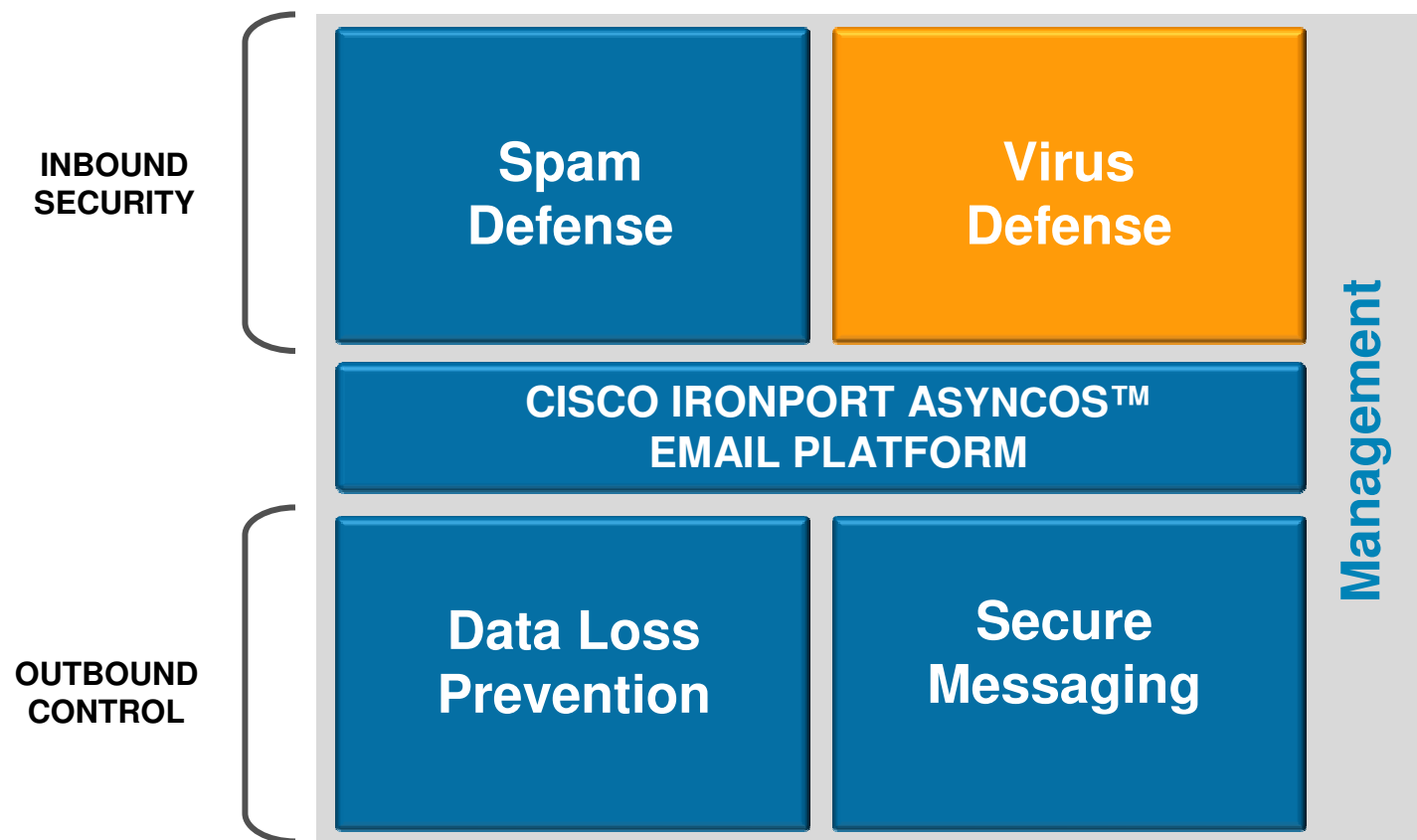
Intelligent Multi-Scan

Best of Both Worlds: Higher Detection with Low FPs

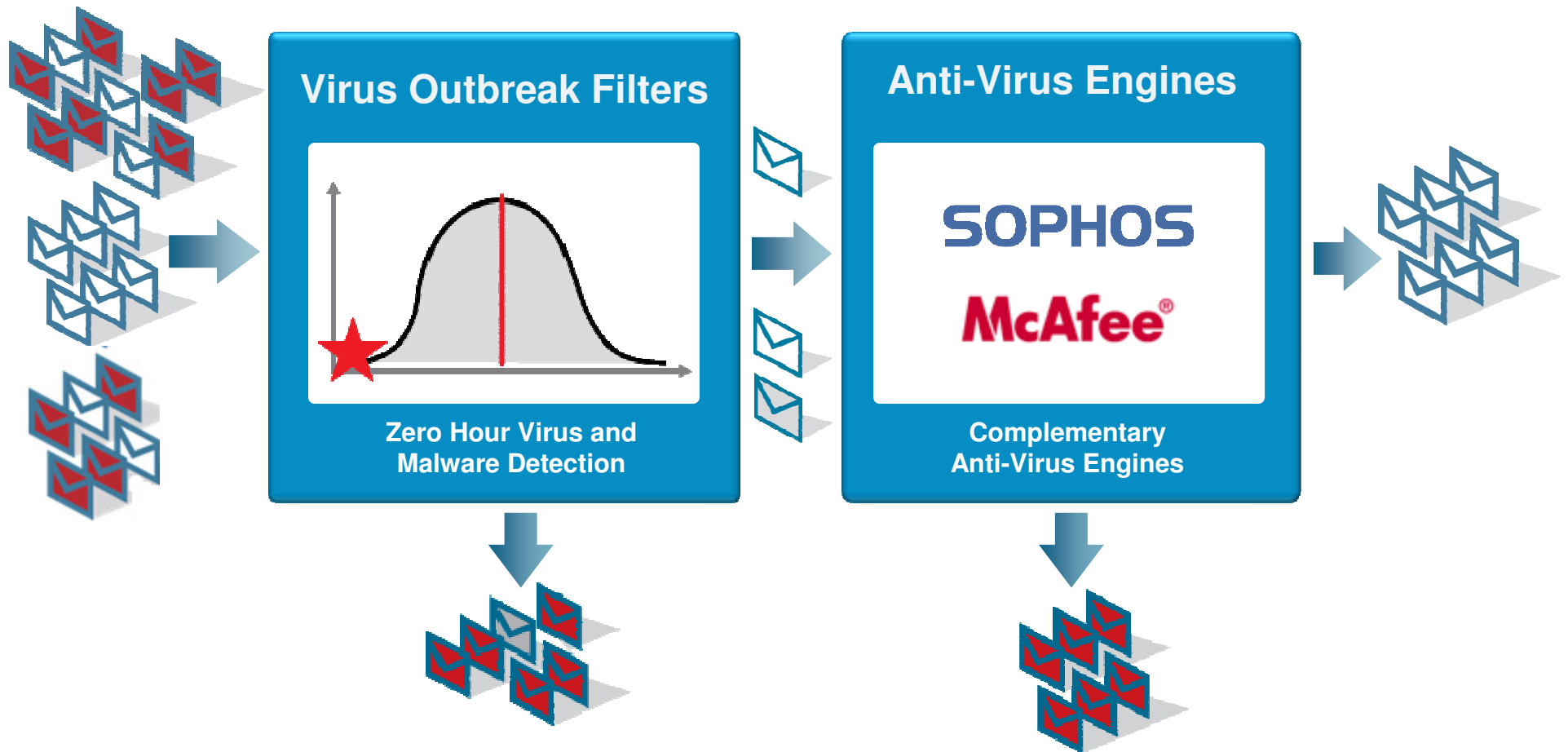


Email Security Architecture

Inbound Security, Outbound Control



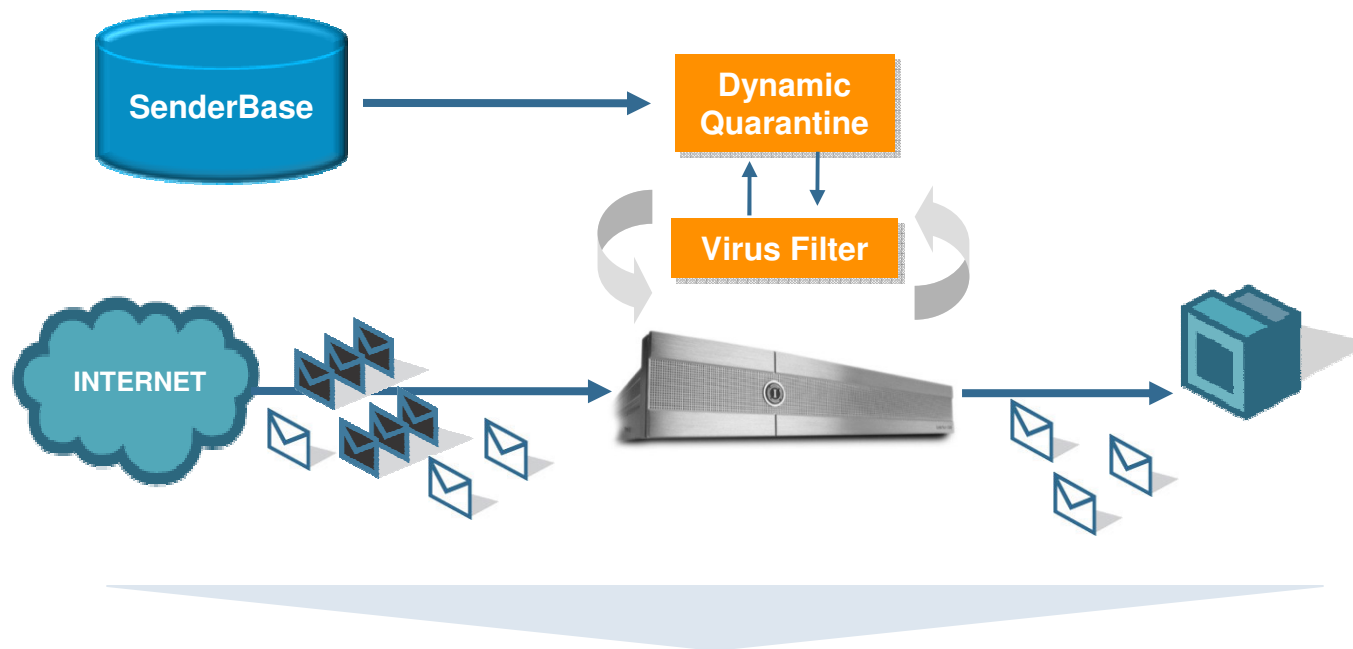
Anti-Virus Defense in Depth



Cisco IronPort Virus Outbreak Filters

Zero Hour Malware Prevention

Virus Outbreak Filters In Action



Virus Outbreak Filters Advantage

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

"Since VOF we have not had a single virus outbreak!"



"Over 24,000 virus positive messages stopped in 9 months"

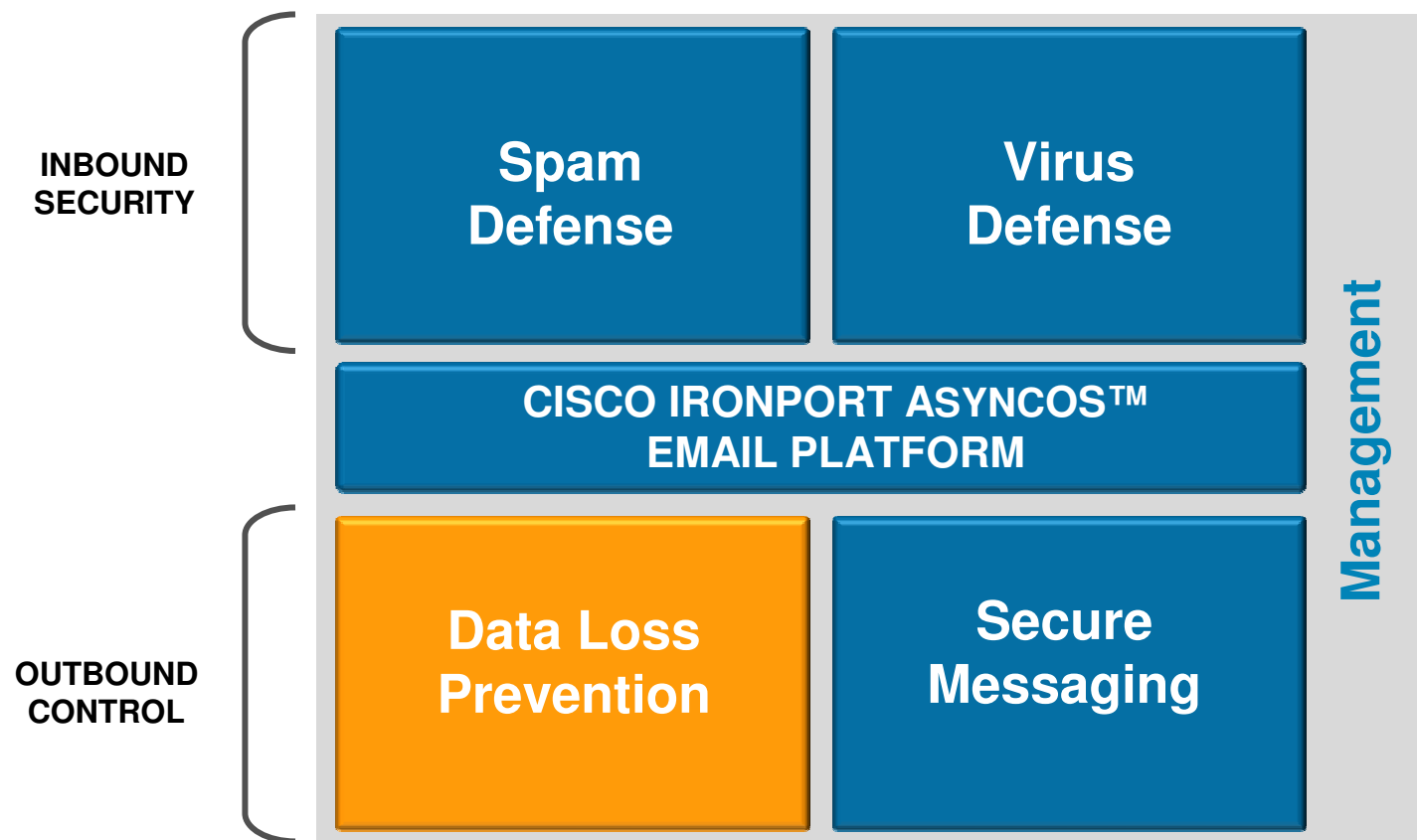


"VOF has stopped more than 12,000 separate viral messages in the last year"



Email Security Architecture

Inbound Security, Outbound Control



IronPort DLP: Comprehensive, Accurate, Easy

Comprehensive



Worldwide regulatory compliance coverage, numerous remediation options

Accurate



No managing false positives

Easy



Quickly deploy and manage

Data Loss Prevention

Simple Set Up

- Easy “3 click” set-up using content filters
- Use pre-defined content categories or create / customize your own
- Can be applied to specific users under specific conditions

Message Body or Attachment

Does the message body or attachment contain text that matches a specified pattern?

- ☐ Contains text:
 *
- ☒ Contains smart identifier:
ABA Routing Number ▼
- ☐ Contains term in content dictionary:
HIPAA-Dictionary_txt ▼

Number of matches required: 1 (1-1000)

For content dictionaries, the number of matches is term weight.

☒ Import from local computer:

☐ Import from the *configuration* directory on your IronPort appliance

- GLBA-Dictionary.txt
- HIPAA-Dictionary.txt
- PCI-Dictionary.txt
- README
- SOX-Dictionary.txt
- config.dtd

▼ Smart Identifiers: ?

Enable Smart Identifiers	Weight
☒ Credit Card Numbers	1 ▼
☒ Social Security Numbers	1 ▼
☒ ABA Routing Numbers	1 ▼
☒ CUSIPs	1 ▼

Data Loss Prevention

Comprehensive Remediation & Reporting

- Multiple remediation actions
 - encrypt, quarantine, drop, bounce, BCC, strip content
- Offending content highlighted in quarantine for easy analysis
- Reporting on a per policy and per user basis

Quarantine
Strip Attachment by Content
Strip Attachment by File Info
Add Disclaimer Text
Bypass Outbreak Filter Scanning
Send Copy (Bcc:)
Notify
Change Recipient to
Send to Alternate Destination Host
Deliver from IP Interface
Strip Header
Add Header
Encrypt and Deliver (Final Action)
Bounce (Final Action)
Deliver (Final Action)
Drop (Final Action)

Quarantine

Flags the message to be held in one of the areas.

Send message to quarantine: Policy ▼

☐ Duplicate message

Send a copy of the message to the specified area. The original message will continue processing the original message actions will apply to the original message.

RSA – Market & Technology Leader



at&t



Microsoft®

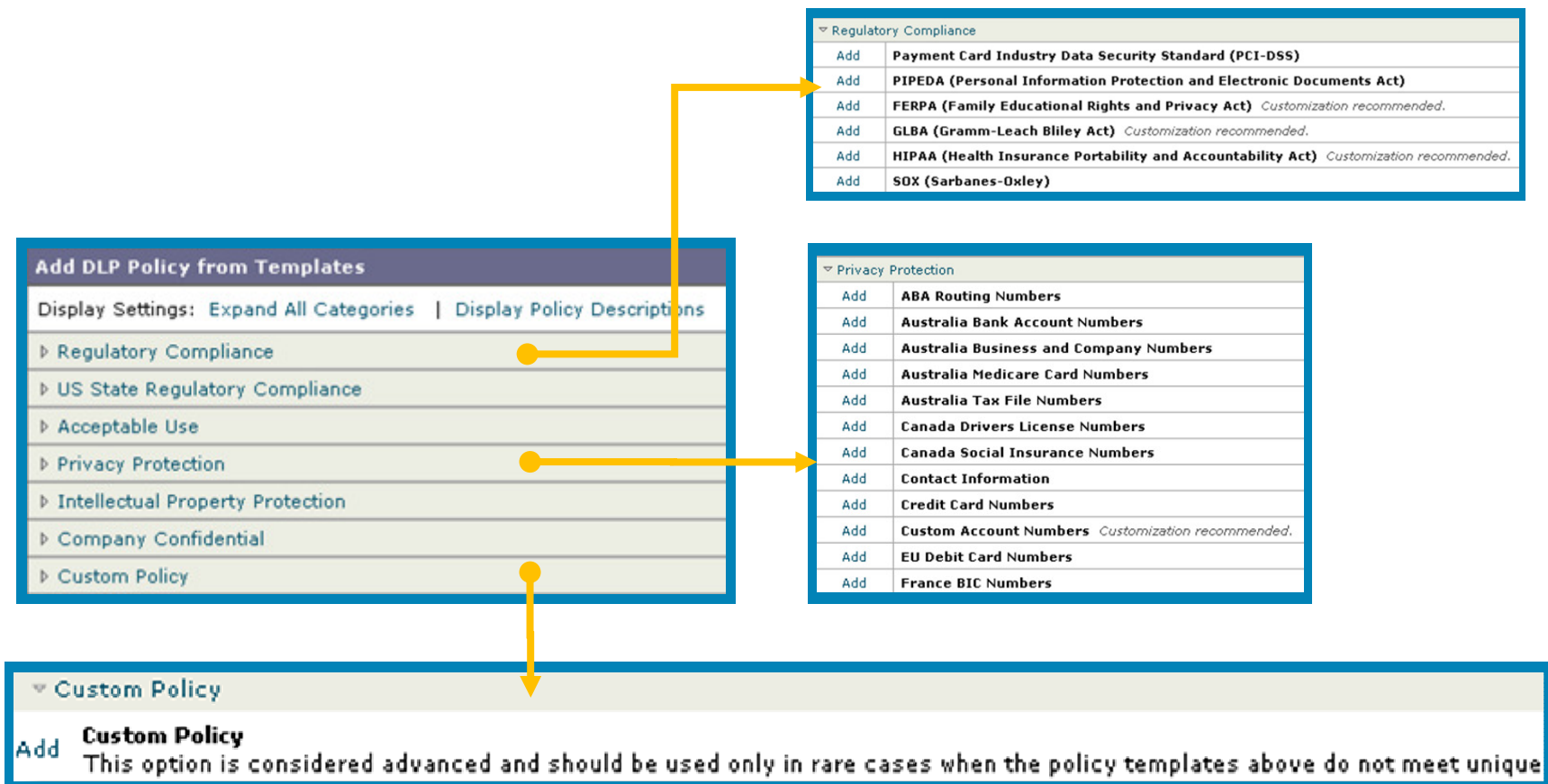


- Ranked as “Leader” in Gartner Magic Quadrant
- Focus on accuracy:
large research team staffed specifically to write and refine content policies

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

Comprehensive Policy Coverage

100+ Predefined Policies for Comprehensive Coverage



Comprehensive Remediation Options

Quarantine ▾

☒ Enable Encryption

Encryption Profile: CRES Encryption ▾

Encrypted Message Subject: \$subject

☒ Apply TLS if message encryption fails.

Policy Quarantine: Policy ▾

Message Modifications

Automated Remediation

Encrypt, quarantine, deliver, or drop

Add disclaimer, modify subject

Copy or notify

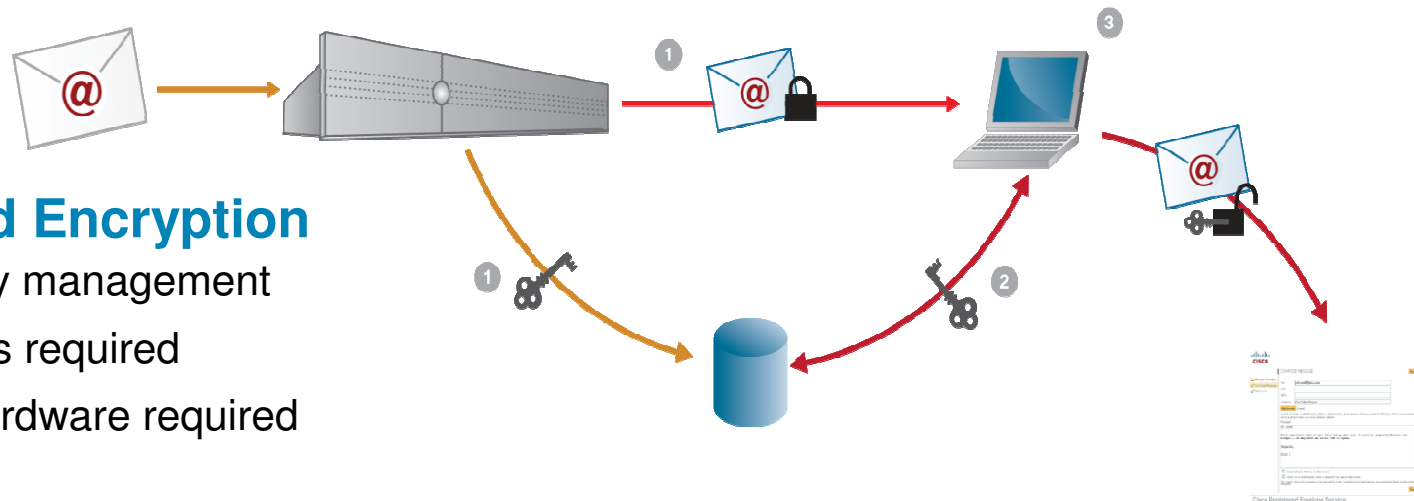
Guaranteed secure delivery

Integrated Encryption

Hosted key management

No plug-ins required

No new hardware required



Easy to Set Up

Stop Sensitive Content in Minutes

Outgoing 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	DLP	Delete
1	Fake Policy	(use default)	(use default)	(use default)	(use default)	(use default)	
	Default Policy	IronPort Anti-Spam Positive: Deliver Suspected: Deliver Marketing Messages: Disabled	Sophos Repaired: Deliver Encrypted: Deliver Unscannable: Deliver ...	Enabled (no filters)	Disabled	HIPAA (Heal... GLBA (Gram... Restricted Fi...	

Key: Default Custom Disabled

Integrated into
Policy
Manager



DLP Scanning Policies

Enable DLP Policies to apply to this mail policy.
To manage this list, add or remove DLP policies, go to DLP Resources.

Order	DLP Policy	
1	PCI-DSS (Payment Card Industry Data Security Standard) Identifies cardholder data regulated by PCI-DSS. Customize to detect credit card numbers from one or all of the following issuers: American Express, Diner's Club, Discover Card, JCB, MasterCard and Visa.	☒
2	GLBA (Gramm-Leach Bliley Act) Identifies customer-related financial information regulated by GLBA. Customize this policy to detect SSNs, CCNs and custom account numbers such as bank, investment, or mortgage account numbers specific to your organization.	☐
3	HIPAA (Health Insurance Portability and Accountability Act) Identifies HIPAA-regulated information including patient IDs, National Provider Identifiers, Social Security Numbers and HIPAA dictionaries.	☒
4	Restricted Files Detects restricted files including MS Access, executable, and Oracle executable files.	☐

[Enable All](#)

One click activation
of pre-loaded
policies

Easy Reporting & Monitoring

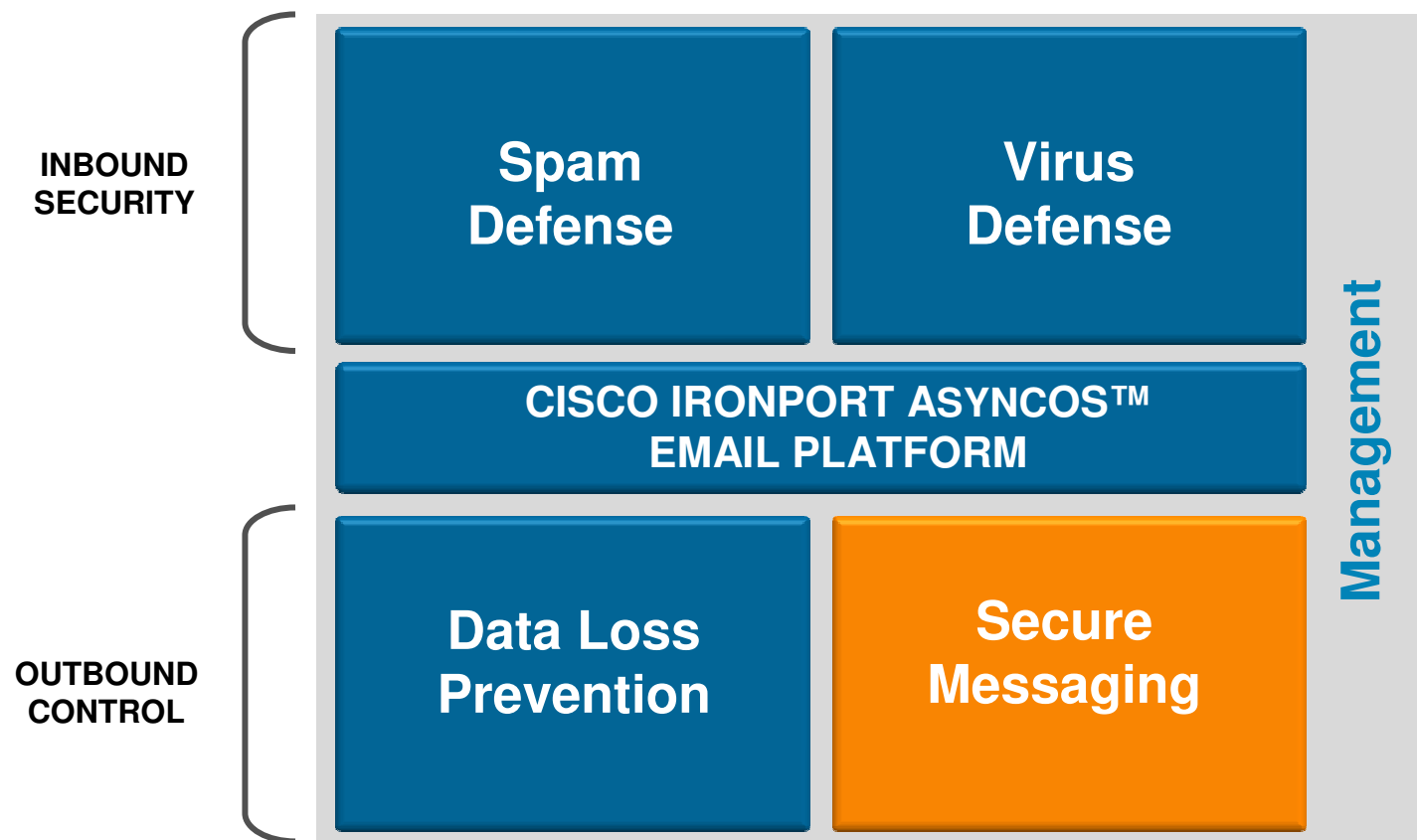
DLP Incident Summary	
Message Event:	Selecting multiple events will expand your search to include messages that match ea with other search criteria will narrow the search. ☐ Virus Positive☐ Hard bounced ☐ Spam Positive☐ Soft bounced
MESSAGE ID "5972594" MATCHED DLP POLICY "HIPAA"	
Violation Severity:	CRITICAL (Risk Factor: 100)
Message Body:	US Social Security Number Acme Corp Marty Smith 808 Sumner Street Greenwood MS 38930 USA Engineering 662-646-0542 msmith@acmecorp.com 2/1/07
patient1234.xls:	HIPAA Patient Identifier - Fred Flintstone Operations 321-02-3456 111 Stonehenge Dr, Bedrock CA 99432 - Wilma Flintstone Human Resources 321-03-3116 111 Stonehenge Dr, Bedrock CA 99432 - Pebbles Flintstone Engineering 321-04-3256
Total Incoming Matches: 123	
Info... Export...	
Generated: 12-Feb-2009 00:17 (GMT)	

Drill I

acking

Email Security Architecture

Inbound Security, Outbound Control



Barriers to Adoption

Why Email Encryption Isn't Everywhere... Yet

1. Ease-Of-Use

- Client plug-ins and confusing end-user intervention
- Public Key and Identity Management

2. Ease-of-Deployment

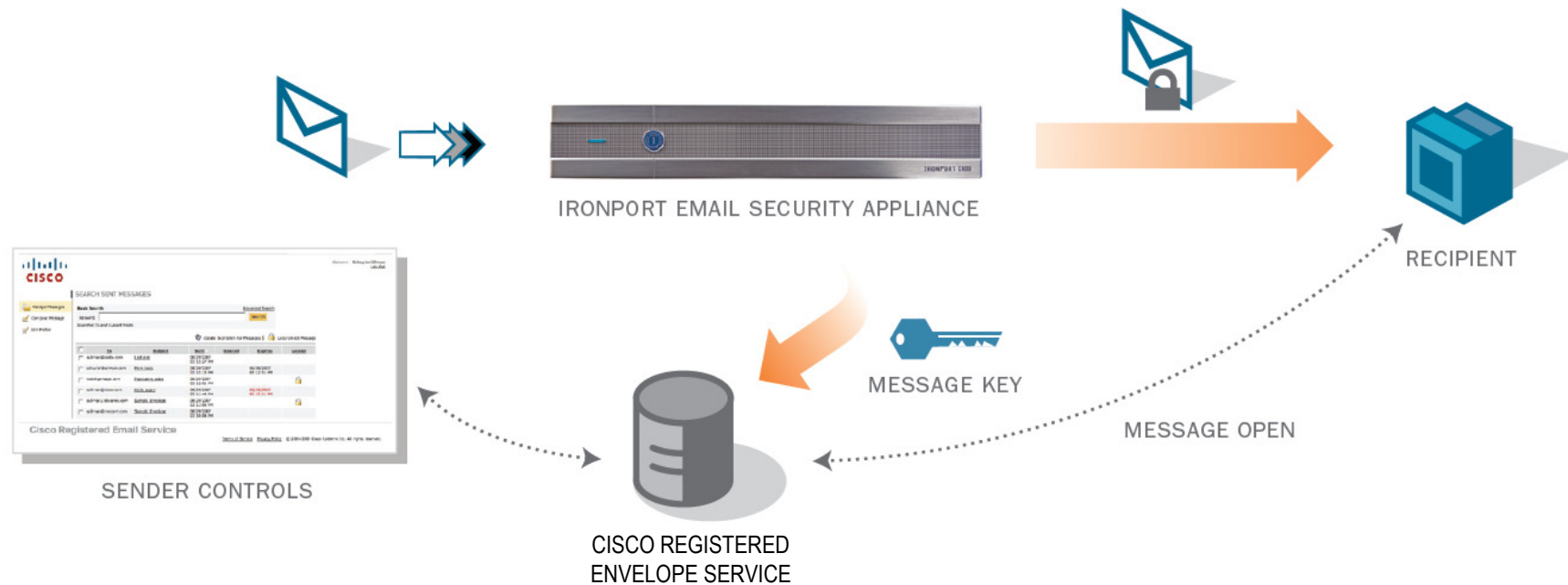
- Client plug-in support
- Public Key and Identity Management Infrastructure

3. Universal Reach

- Require pre-existing cryptographic relationship
- Send / receive on limited set of email clients with plug-in

Cisco IronPort Email Encryption

Easy for the Sender. . .

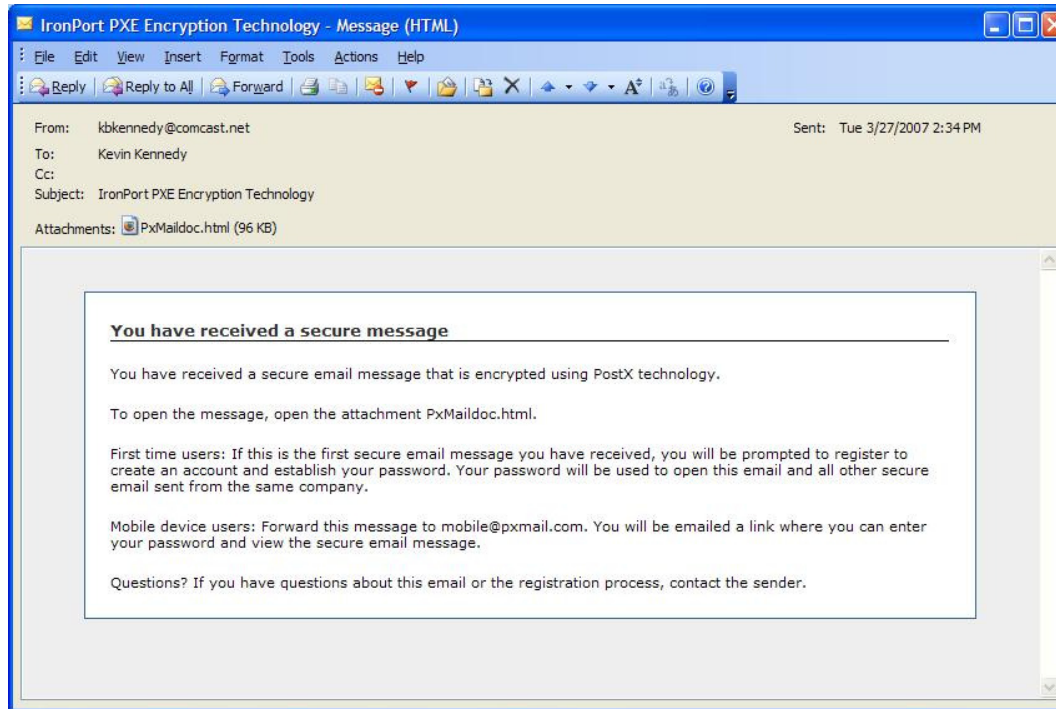


- Automated key management
- No desktop software requirements
- Send to any email address seamlessly

Cisco IronPort Email Encryption

Receiving a message

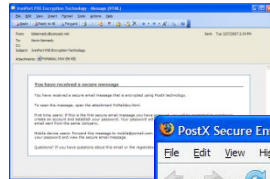
- 1 Receive email, click to open attachment



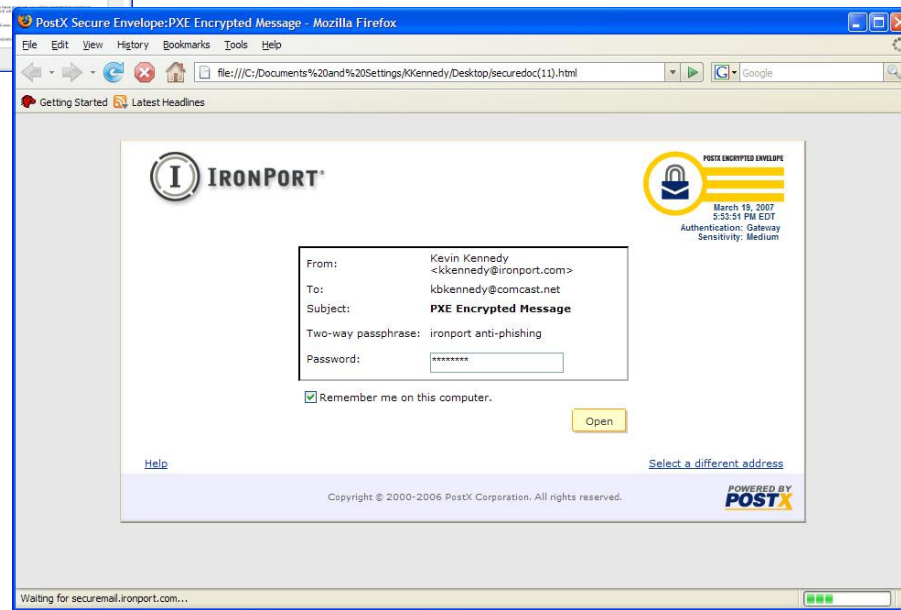
Cisco IronPort Email Encryption

Receiving a message

1 Receive email



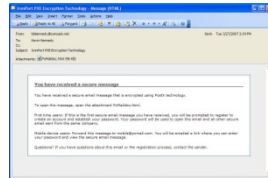
2 Enter password



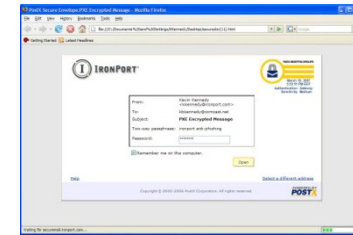
Cisco IronPort Email Encryption

Receiving a message

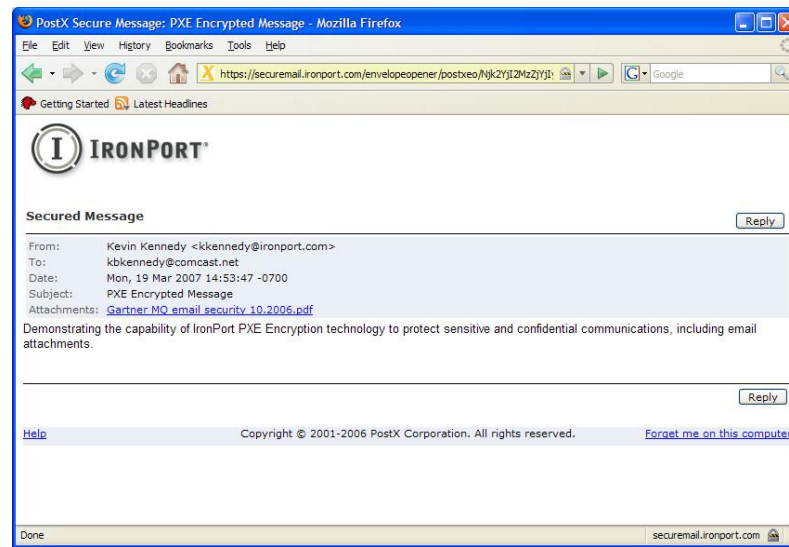
1 Receive email



2 Enter password



3 View secure message



Solving Limitations of Other Email Encryption Products

1. Ease-Of-Use - **Solved**

- Client plug-ins and confusing end-user intervention
- Public Key and Identity Management
- **No client software, no certificates**

2. Ease-of-Deployment - **Solved**

- Client plug-in support
- Public Key and Identity Management Infrastructure
- **IronPort Hosted Keys service**

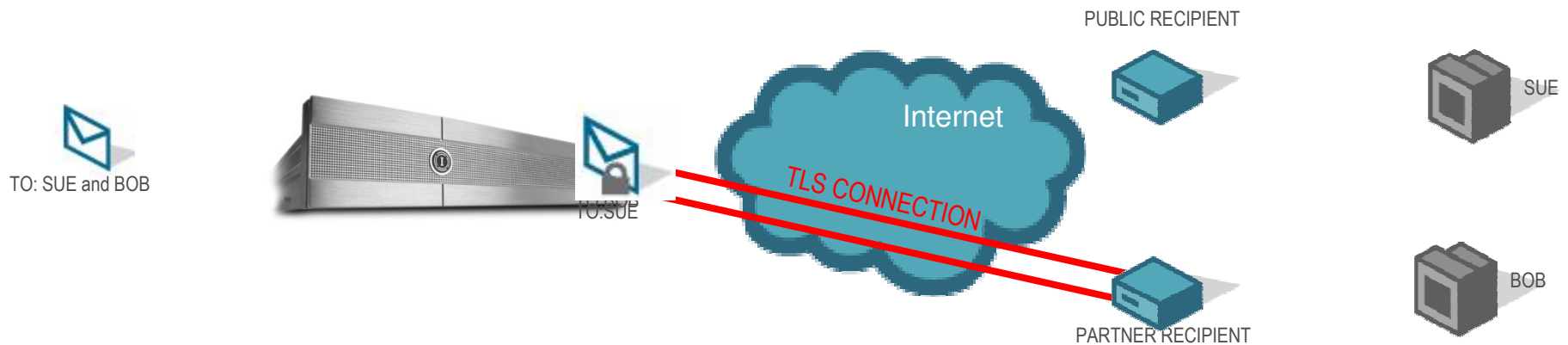
3. Universal Reach - **Solved**

- Require pre-existing cryptographic relationship
- Send / receive on limited set of email clients with plug-in
- **Send / receive from any email platform**

Guaranteed Secure Delivery

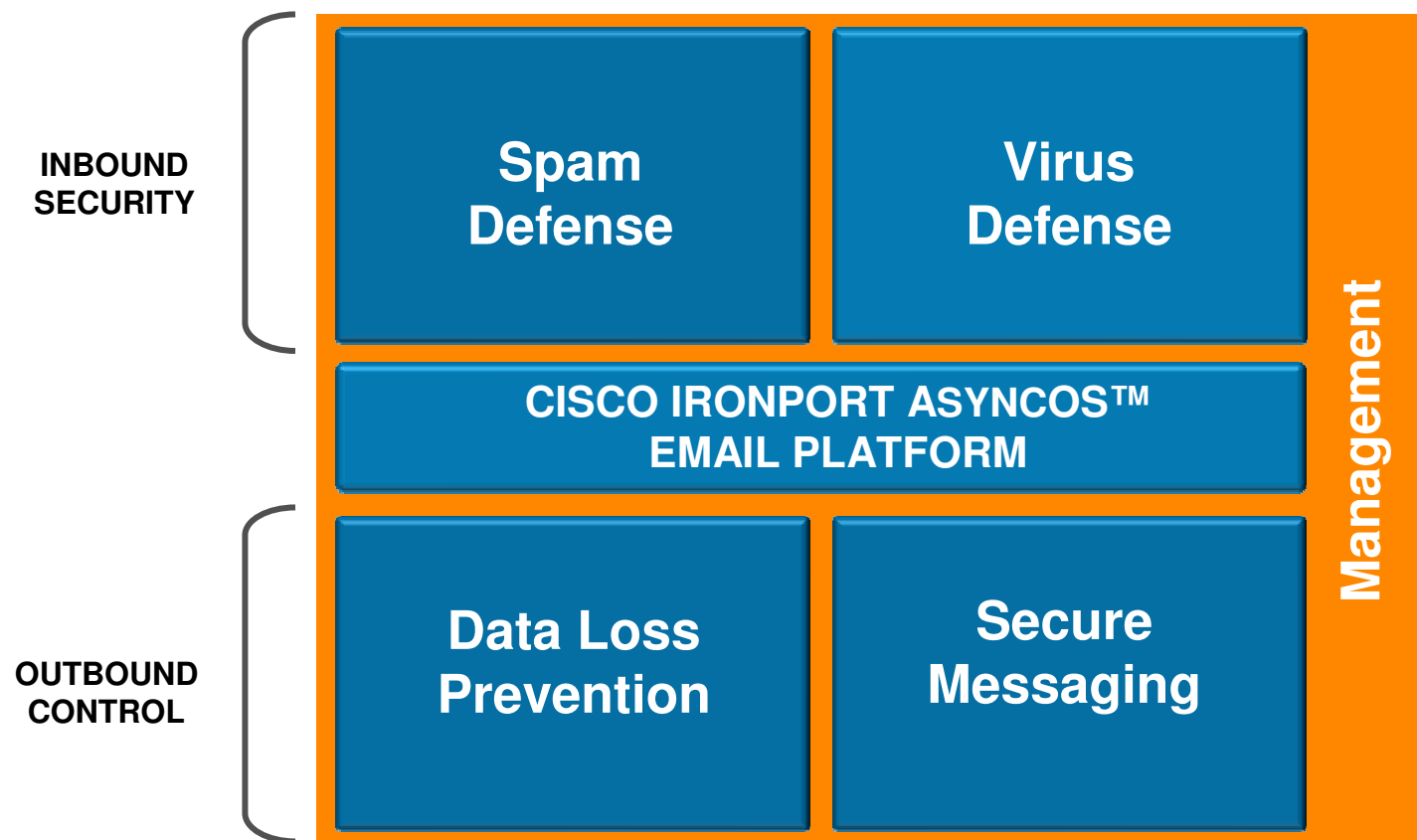
Destination-Sensitive Email Encryption

1. Use TLS if available
2. Encrypt using PXE Secure Envelope



Email Security Architecture

Inbound Security, Outbound Control



Cisco IronPort Email Security Manager

Single view of policies for the entire organization

Incoming Mail Policies

Find Policies

Email Address: ☒ Recipient ☐ Sender

Policies

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:

Categories: by Domain, Username, or LDAP

- Allow all media files
- Quarantine executables



IT

- Mark and Deliver Spam
- Delete Executables



SALES

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



LEGAL

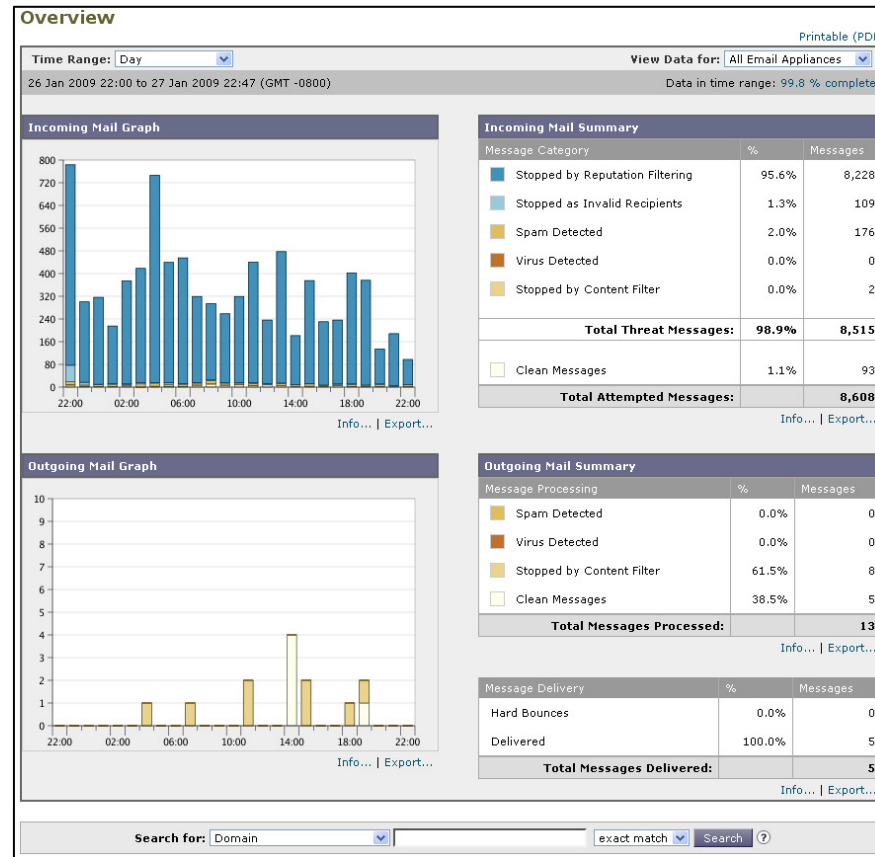
“IronPort Email Security Manager serves as a single, versatile dashboard to manage all the services on the appliance.” – PC Magazine

Comprehensive Insight

Unified Business Reporting

Consolidated Reports

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



Virus Outbreaks

26 Jan 2009 22:00 to 27 Jan 2009 22:47 (GMT -0800)

Outbreak Name	Outbreak Type	Outbreak Status	Outbreak Date	Outbreak Time	Outbreak Count
Outbreak 1	Spam	Active	26 Jan 2009	22:00	100
Outbreak 2	Virus	Resolved	27 Jan 2009	00:00	50
Outbreak 3	Spam	Active	27 Jan 2009	06:00	200

Multiple data points

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

Internal Users

26 Jan 2009 22:00 to 27 Jan 2009 22:47 (GMT -0800)

User Name	User Type	User Status	User Date	User Time	User Count
User 1	Internal	Active	26 Jan 2009	22:00	10
User 2	Internal	Resolved	27 Jan 2009	00:00	5
User 3	Internal	Active	27 Jan 2009	06:00	20

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

Message Tracking

Search

Available Time Range: 08 Oct 2007 09:10 to 27 Jan 2009 22:51 (GMT -0800) Data in time range: 91.25% complete

Envelope Sender: ? Begins With []

Envelope Recipient: ? Begins With []

Subject: Begins With []

Message Received: ☒ Last Day ☐ Last Week ☐ Custom Range

Start Date: 01/26/2009 Time: 22:00 and End Date: 01/27/2009 Time: 22:52 (GMT -0800)

Advanced

Sender IP Address: []

☐ Search rejected connections only ☒ Search messages

Message Event: *Selecting multiple events will expand your search to include messages that match each event type. However, combining an event type with other search criteria will narrow the search.*

☐ Virus Positive ☐ Hard bounced

☐ Spam Positive ☐ Soft bounced

☐ Suspect Spam ☐ Currently in Outbreak Quarantine

☐ Delivered ☐ Quarantined as Spam

Message ID Header: []

IronPort MID: []

IronPort Host: All Hosts []

Query Settings: ? Query timeout: 1 minute []

Max. results returned: 250 []

Clear Search

Unparalleled Market Leadership

Gartner

IronPort Positioned in the “Leaders” Quadrant in Magic Quadrant Report



IronPort is positioned as a leading player in the messaging security appliance market

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

Named IronPort the market share leader in the email security appliance market

- 20,000+ customers globally
- 300 million users protected
- 40% of Fortune 100 companies
- 8 of the 10 largest service providers
- 99%+ customer renewal rates



TRY
BEFORE YOU
BUY

NO RISK
30-DAY
FREE TRIAL



