Sponzor komunikacijskih tehnologija

Hrvatski Telekom

Sponzori konferencije

SG Equipment Finance

SG Leasing d.o.o.

SOGELEASE

HRVATSKA UDRUGA POSLODAVACA

Komunikacijski partner

spona
Integrirane komunikacije

Partner digitalnog oglašavanja i video nadzora

RECRO net
We know IT

Partneri konferencije

COMPUTECH

computer systems

IBM

KING ICT

RECRO net

s&t

Sedam IT
Primjena informatičkih tehnologija

STORM

verso

Tehnološki sponzor

ComTel Corp.

EMC²

Novi Forum

SAP

Medijski pokrovitelji

vecernji.hr

ADRIA

MREŽA

racunalo.com

Večernji list

infoTrend

PC chip

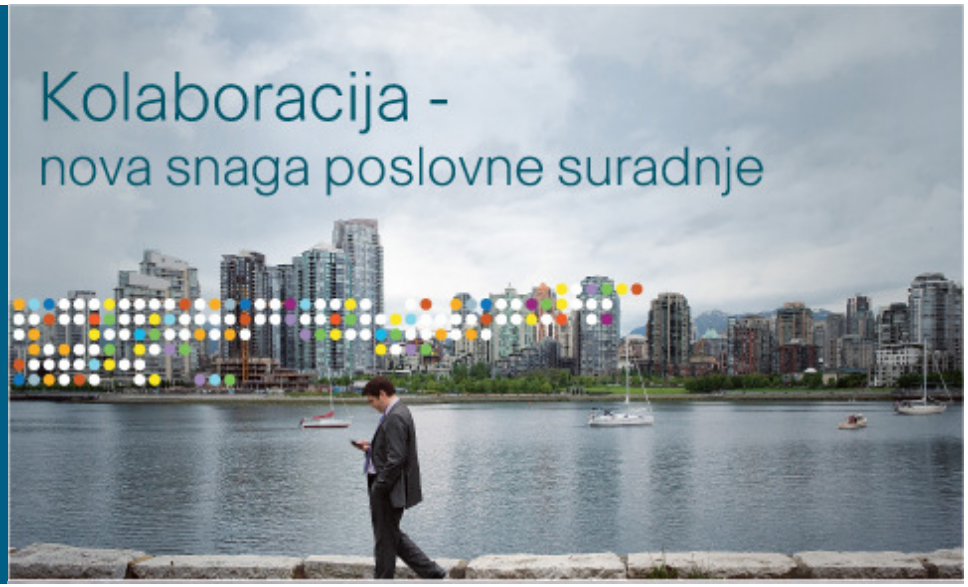
Cisco Expo 2010

24.–26. ožujka 2010.
Hotel Le Méridien Lav
Split

Kolaboracija -
nova snaga poslovne suradnje

Cisco Expo 2010

Cisco IronPort E-mail Security Solution

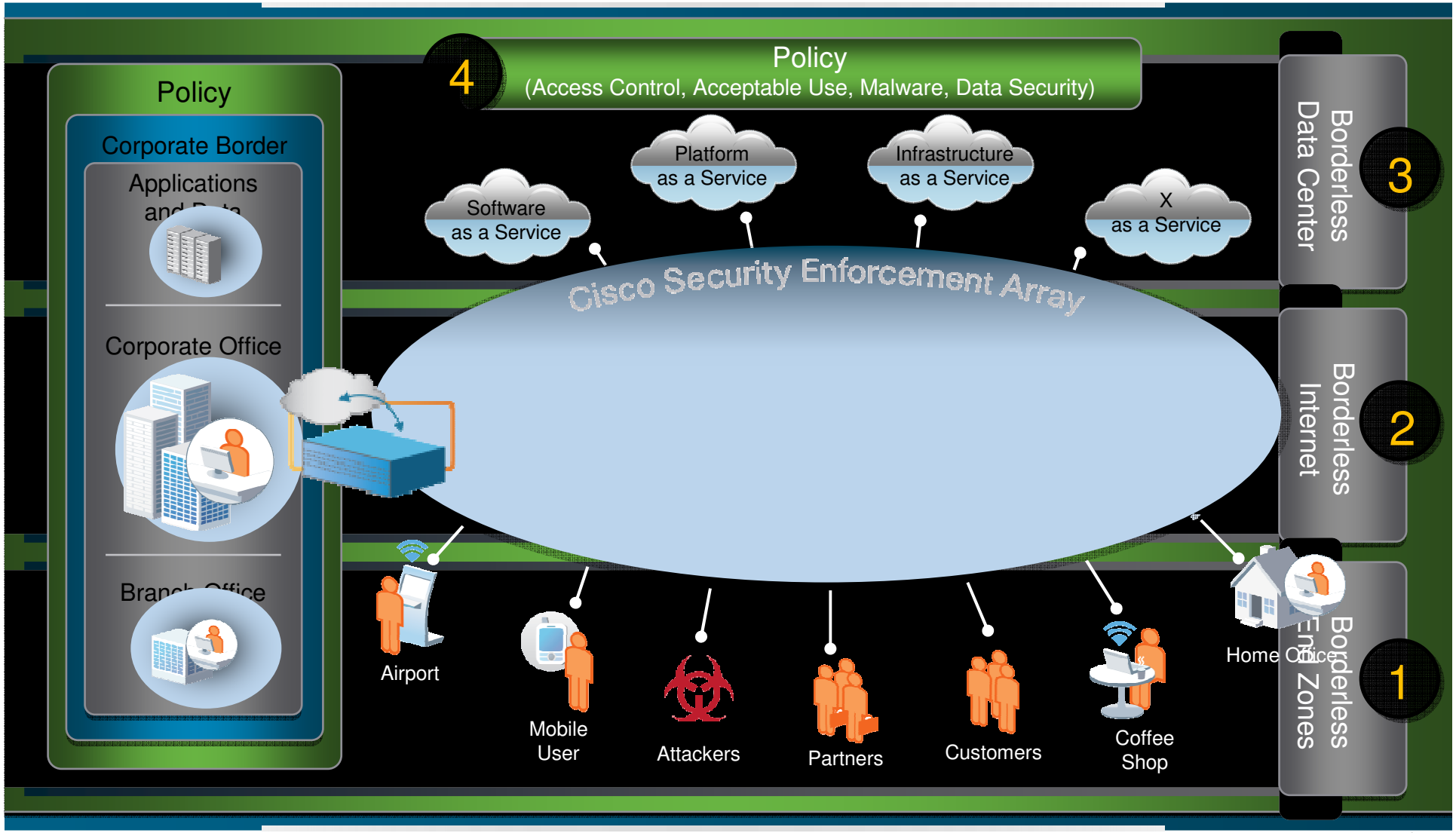


Borderless Advanced Protection - Hrvoje Dogan

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!

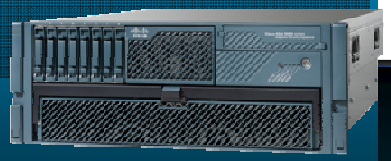
Cisco's Architecture for Borderless Network Security



Pillar 2: Borderless Security Array

Advanced Scanning and Enforcement Capabilities

Cisco Adaptive Security Appliance



Cisco Integrated Services Routers

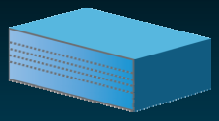
Cisco IronPort Web Security Appliance

Cisco IronPort Email Security Appliance

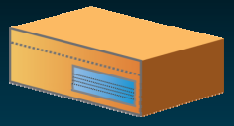
Access Control | Acceptable Use | Data Security |Threat Protection

Integrated into the Fabric of the Network

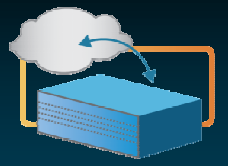
VM Software



Appliance



Security Module

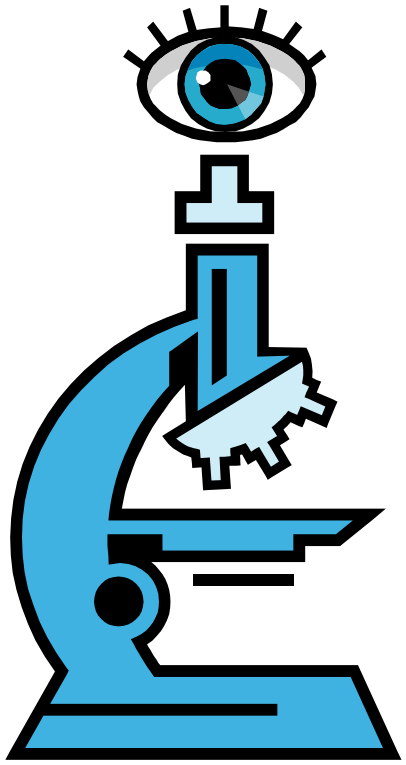


Hybrid Hosted

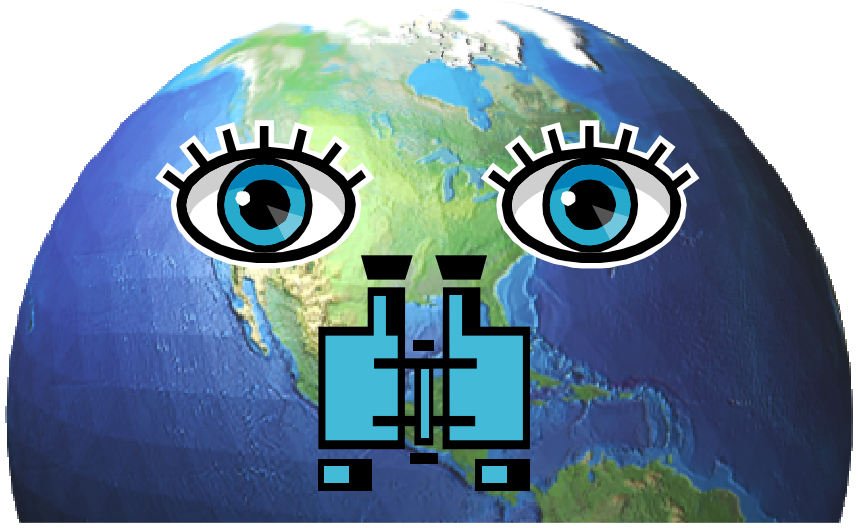
The Power for Advanced Protection

A Seismic Shift

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



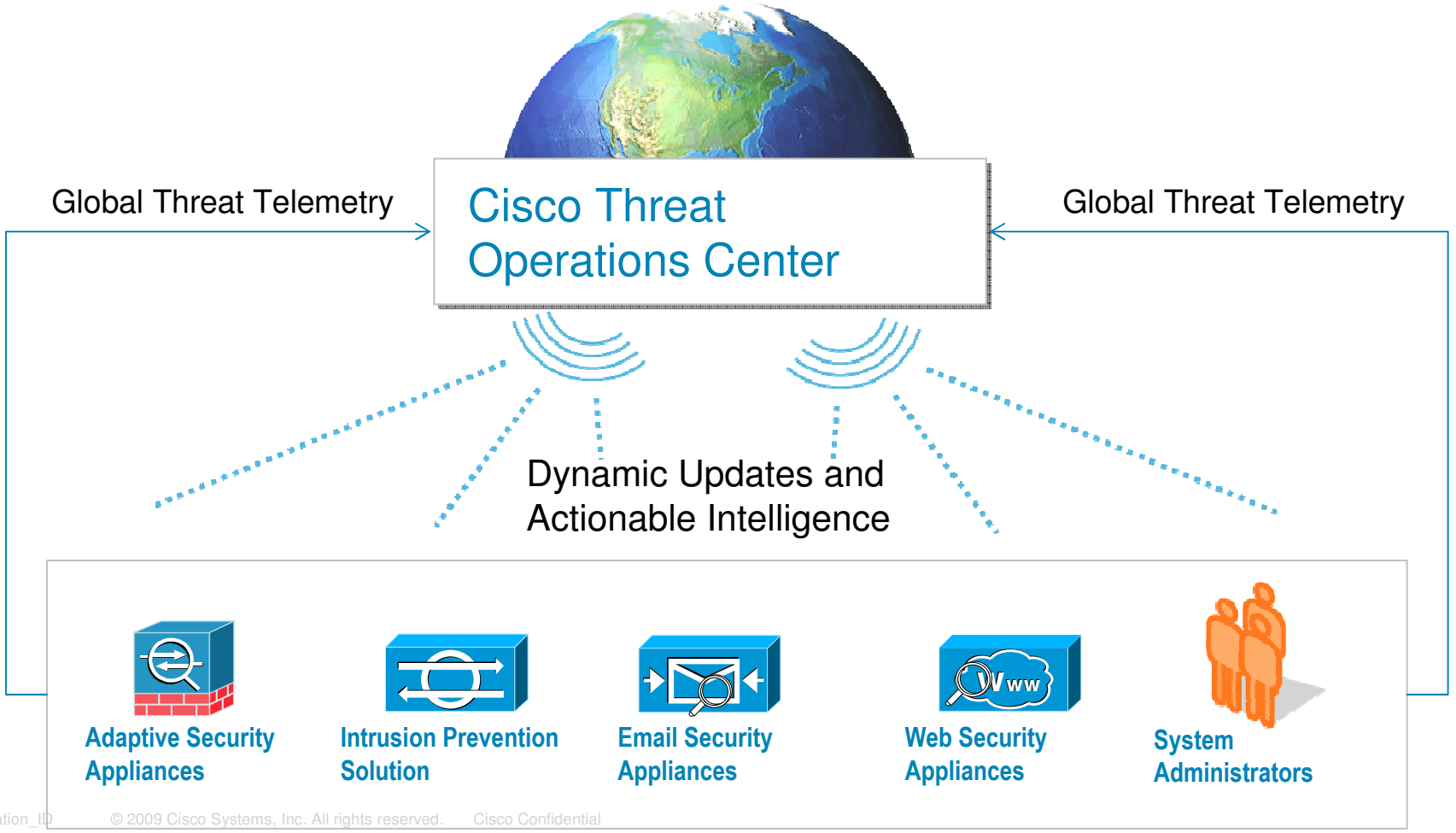
- **2009:** Cisco Security products look around, respond faster



Cisco Security Intelligence Operations (SIO)

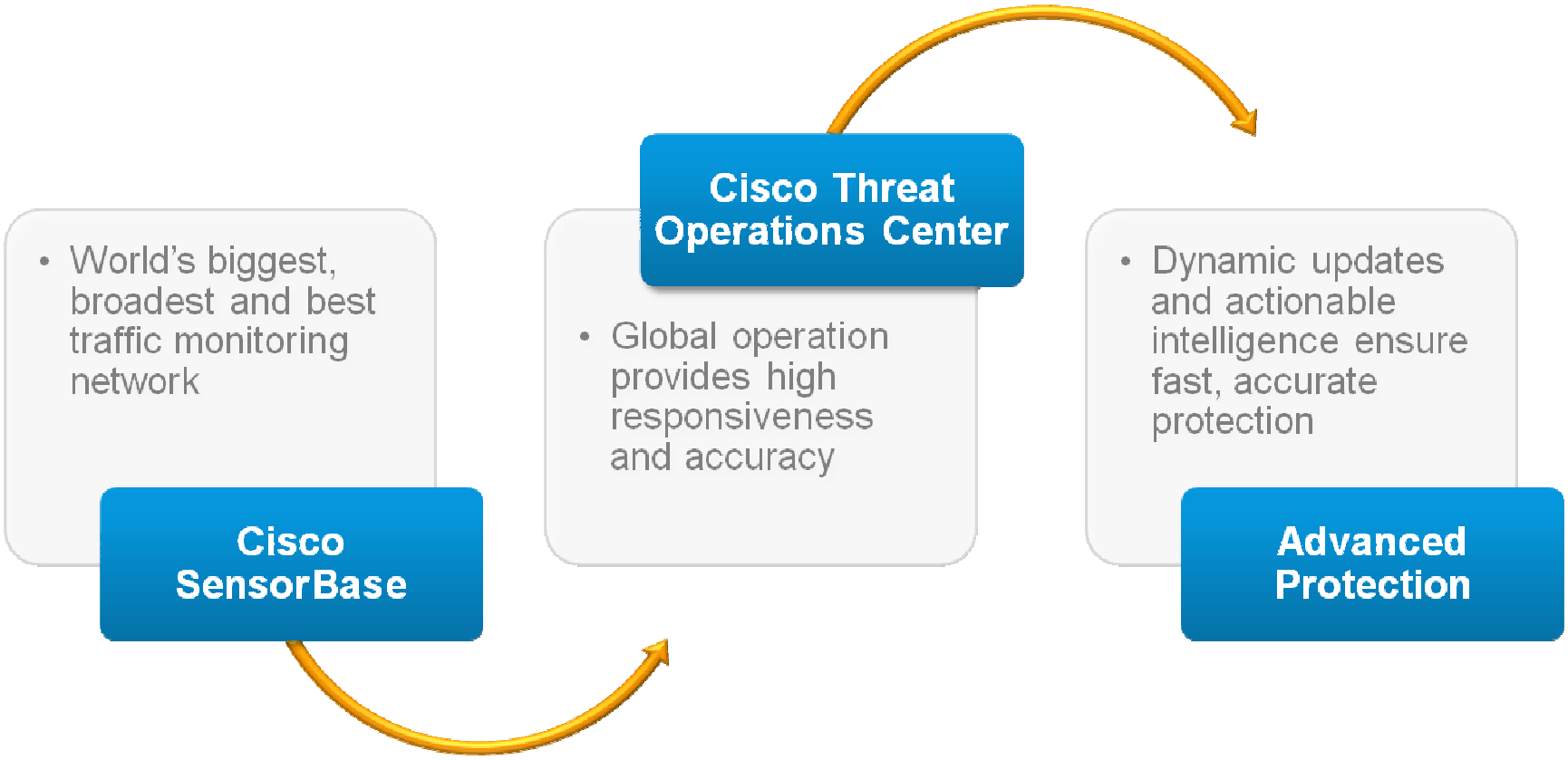
Overview

Most Accurate Protection Against a Broad Range of Threats



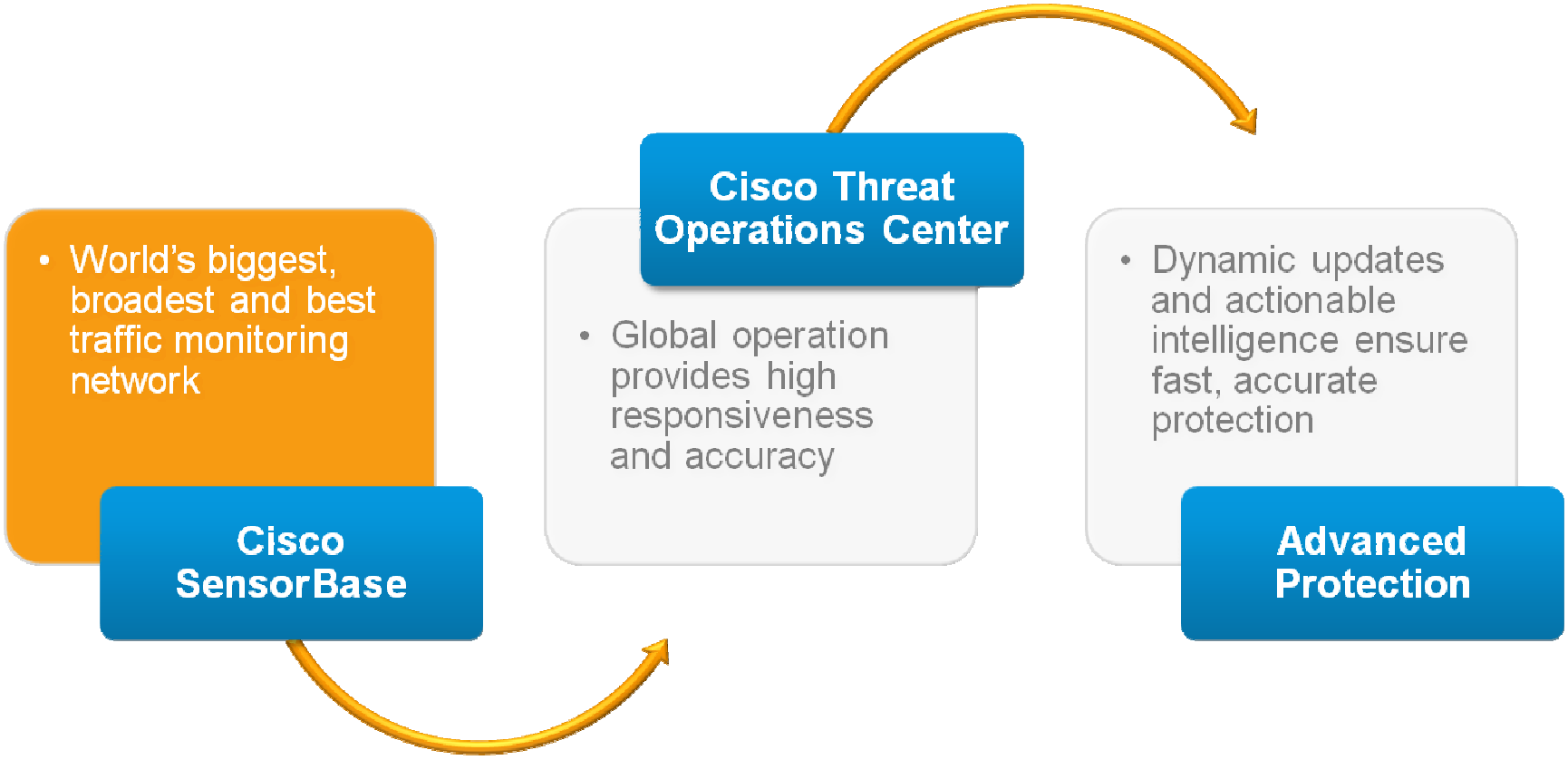
Cisco SIO
Key Components

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

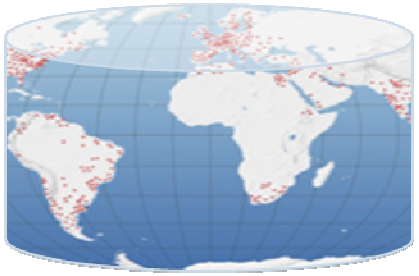
Fortune 500, Global 2000, universities, SMBs

152 third-party feeds

First to Combine Network and Application Layer Data

Cisco SensorBase Network

Unmatched Breadth



SensorBase Network

Email

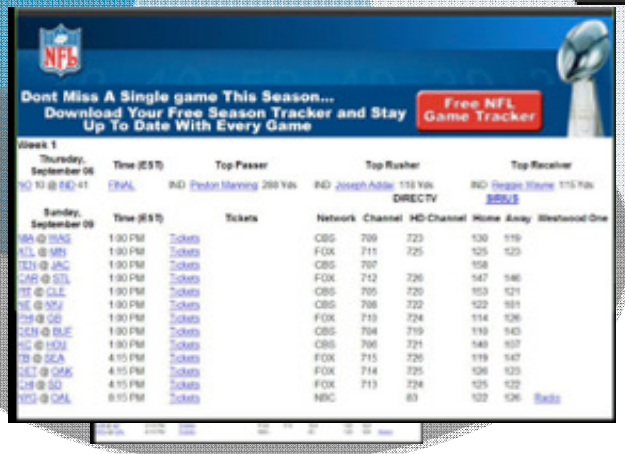
From: Bill Gates
To: John Chambers
Cc:
Subject: Free NFL Game[IronPort SUSPECTED SPAM]

Football is back, life may resume again!
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

Directed Attack

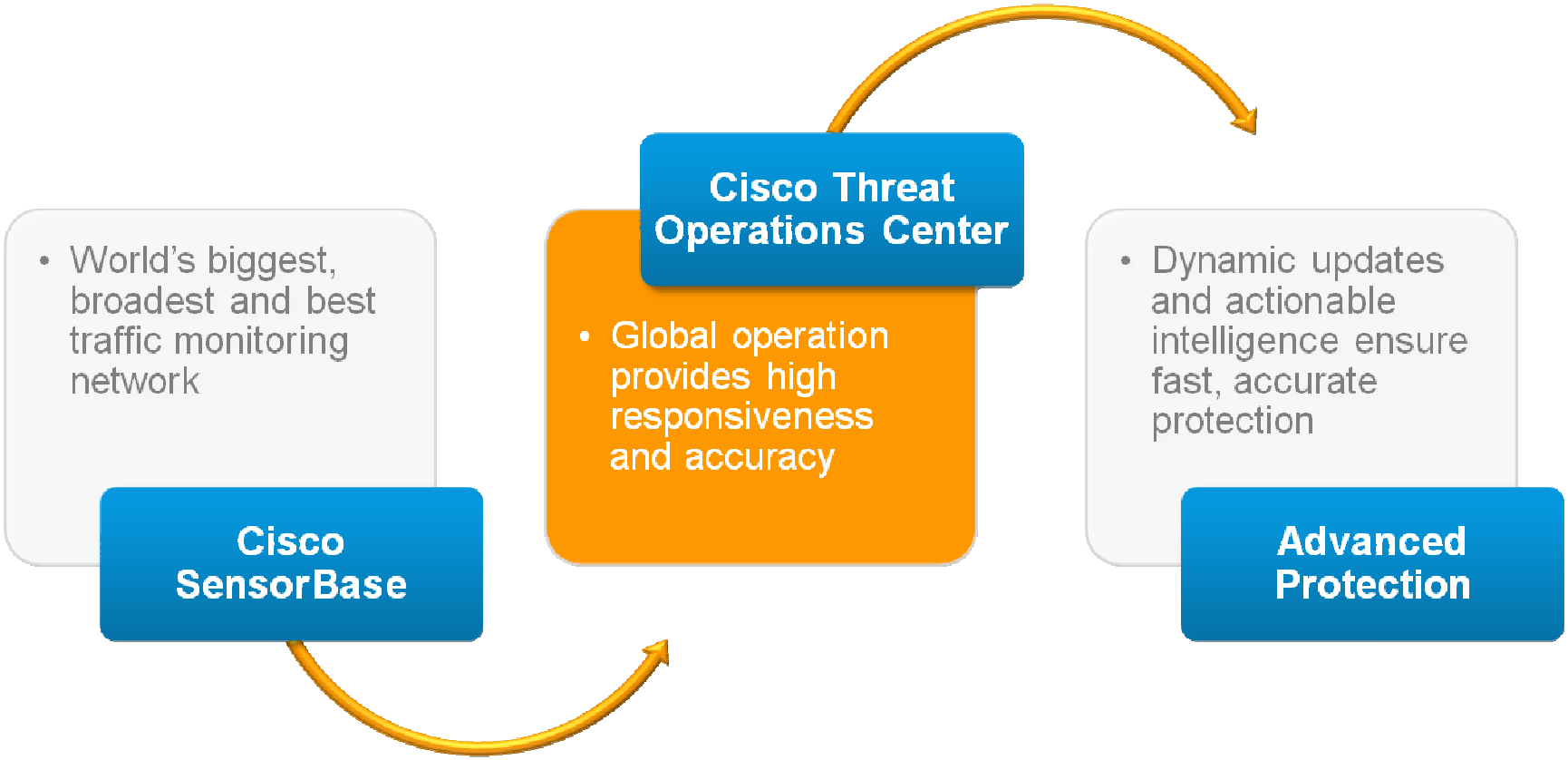


Malware Distributing Site

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

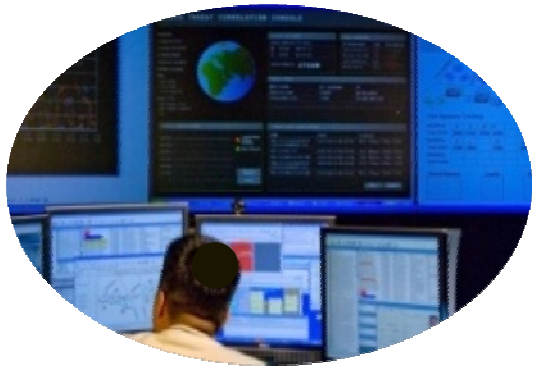
   ASA Botnet Traffic Filters

   Virus Outbreak Filters

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

Cisco Threat Operations Center

Ensuring Accuracy and Responsiveness



Experienced Analysts

500 analysts

European and Asian languages

1 Cisco Fellow

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

24x7x365 Operations

5 threat operations center locations around the globe

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

Powerful Tools

Dynamic updates

Correlation and data mining

Advanced rule approval, creation and publishing applications

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

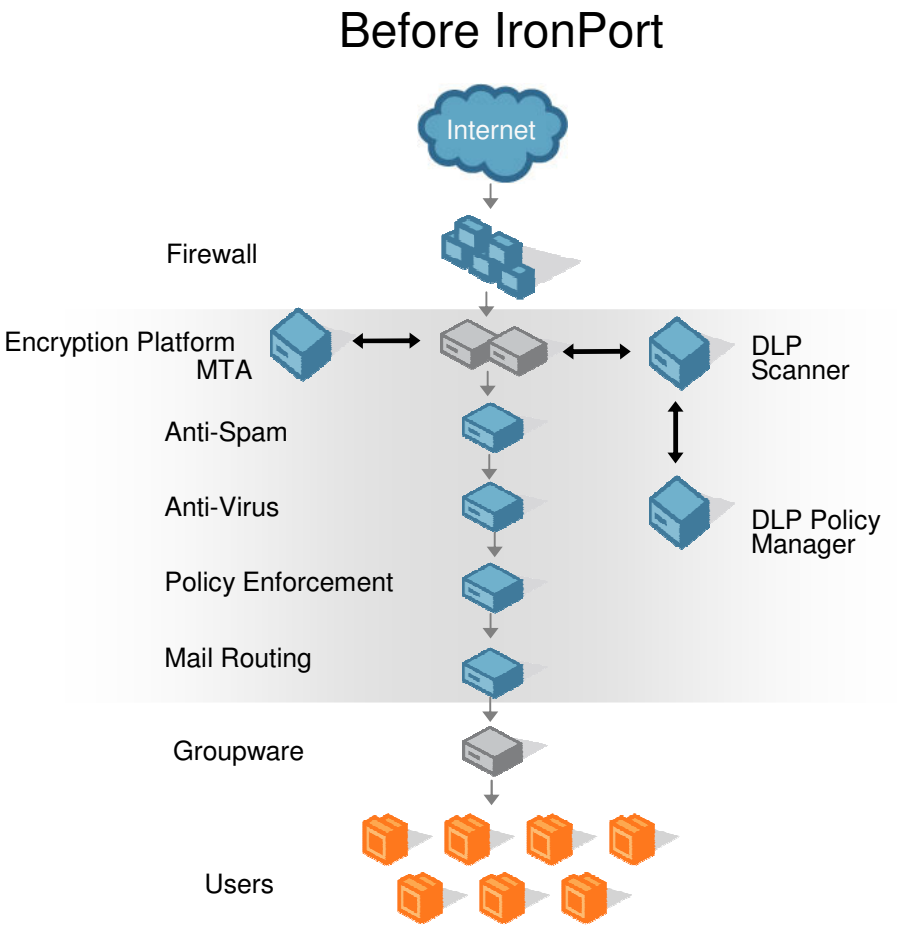
Cisco SIO: Cloud-based intelligence to power Cisco security services

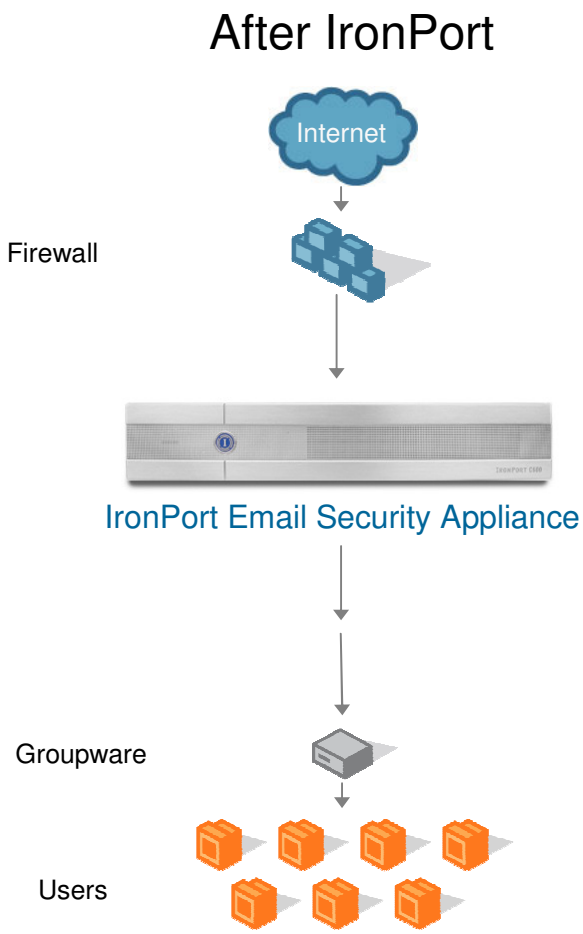
- Live Reputation Scores
- New and Updated Signatures
- Authored Rule Sets
- Dynamic Rule Sets
- Auto-Updates Every 5 minutes

Cisco IronPort
E-mail Security Appliances

Cisco IronPort Consolidates the Network Perimeter

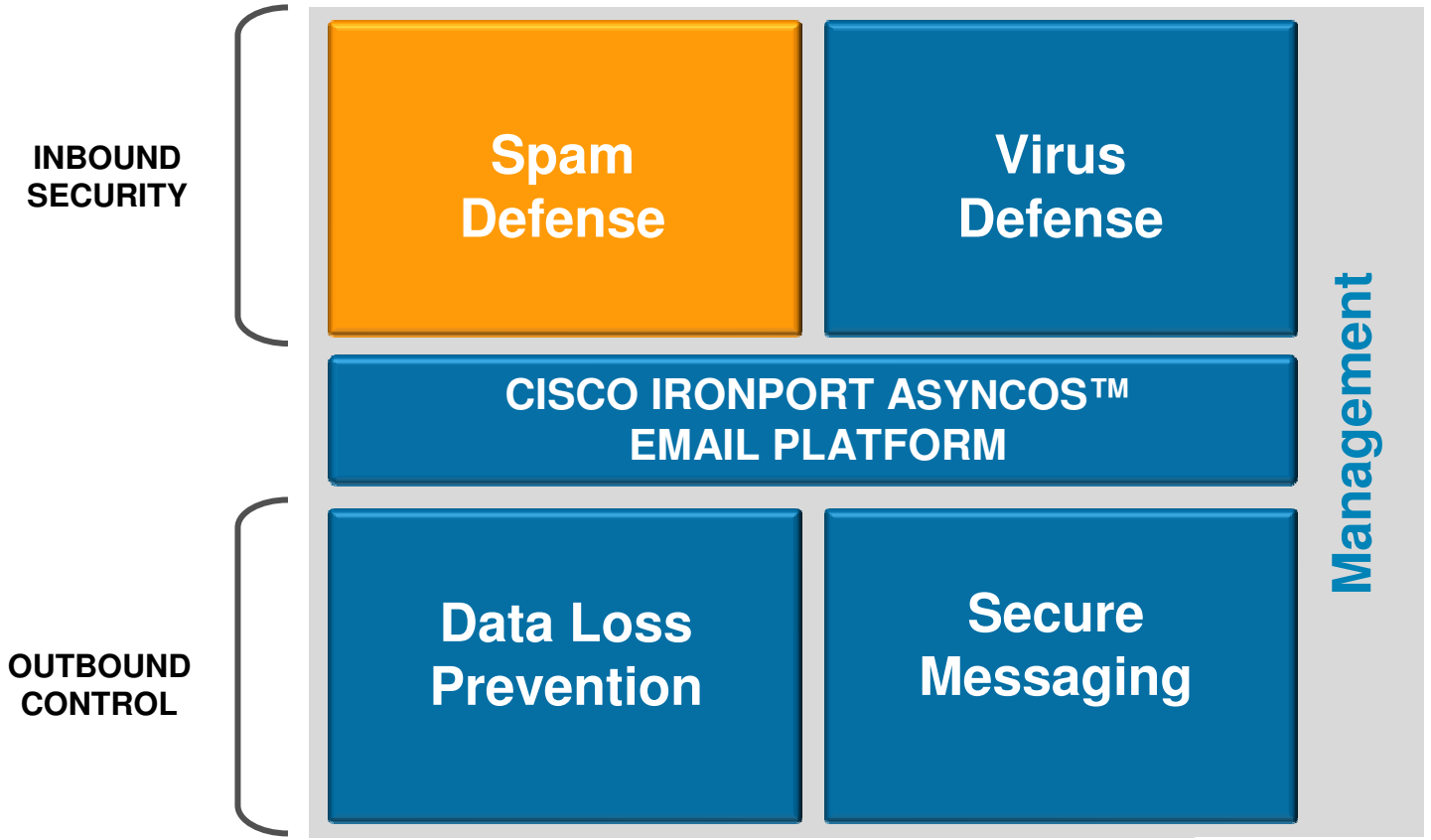
For Security, Reliability and Lower Maintenance





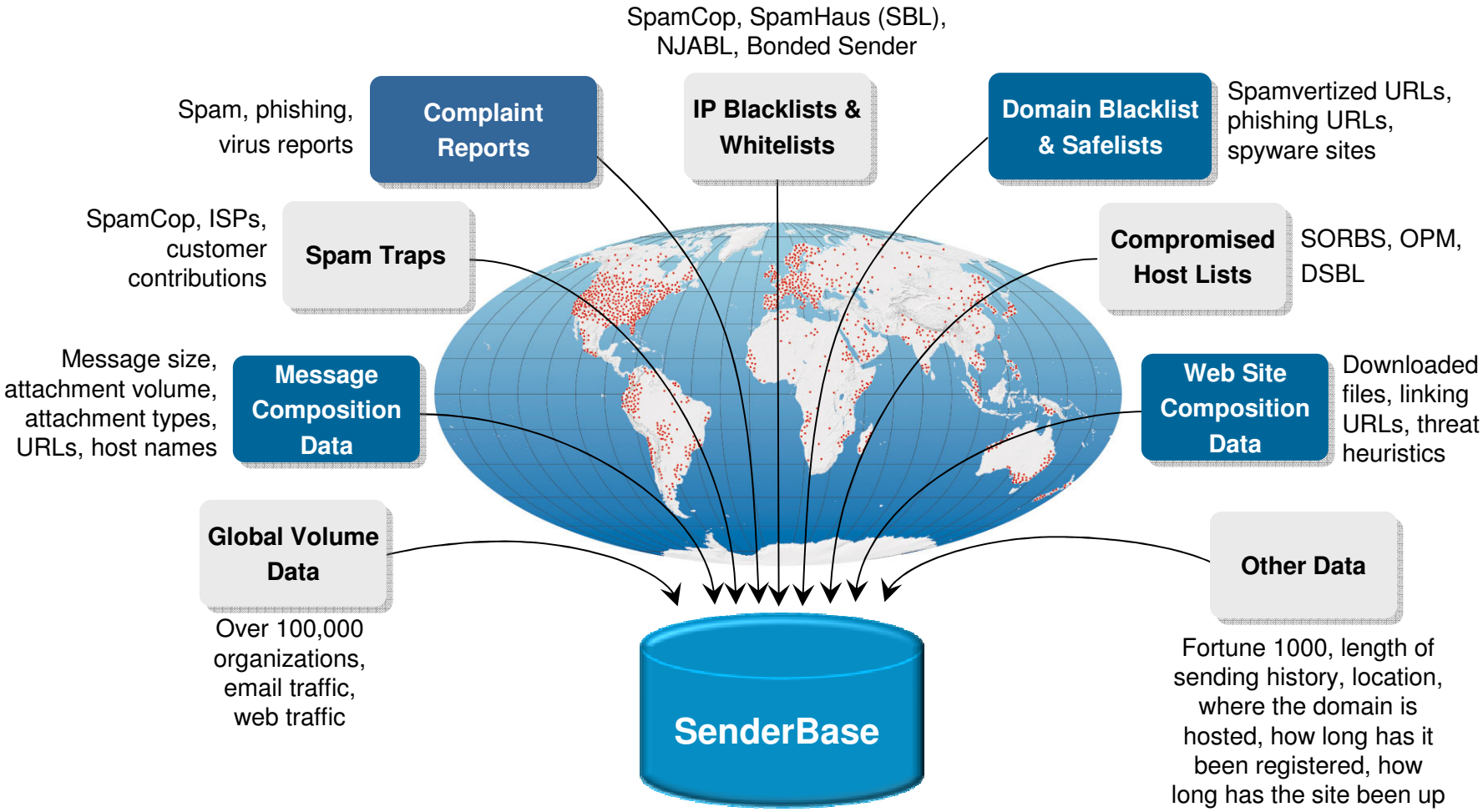
Email Security Architecture

Inbound Security, Outbound Control

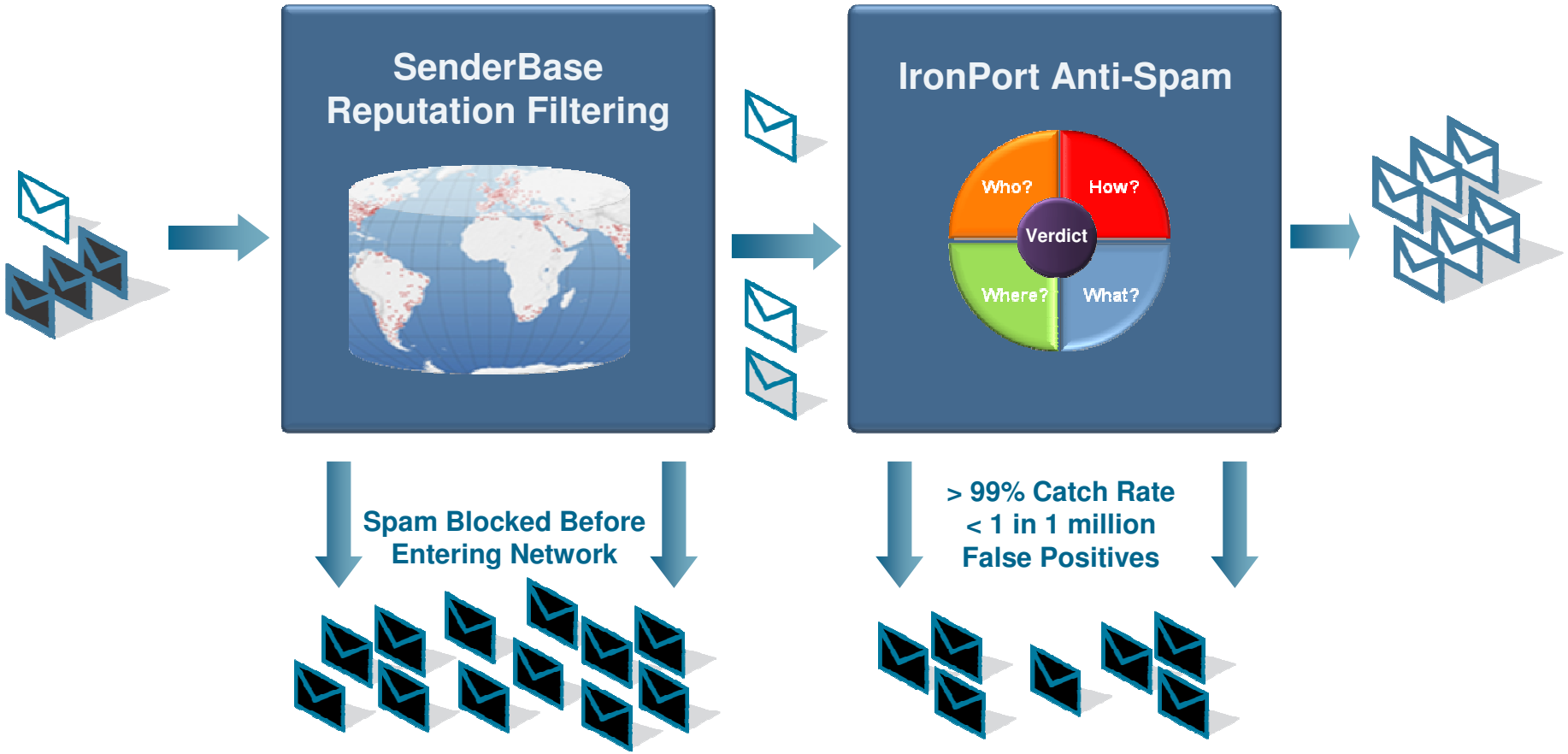


Cisco IronPort SenderBase

Breadth and Quality of Data Makes the Difference

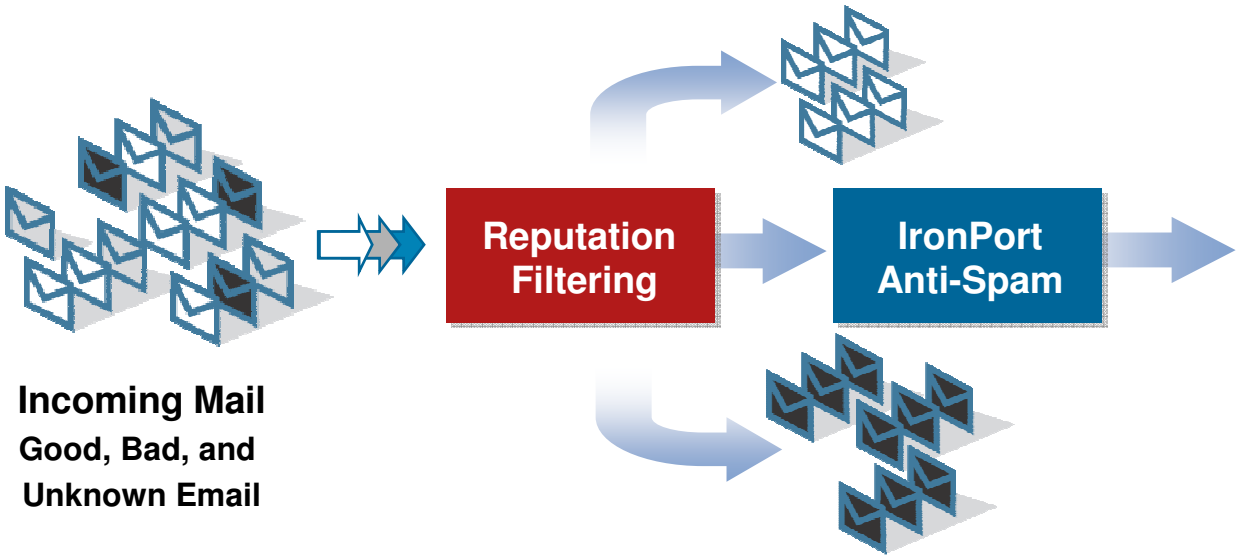


Anti-Spam Defense in Depth



SenderBase Reputation Filtering

Real Time Threat Prevention



- **Known good is delivered**
- **Suspicious is rate limited and spam filtered**
- **Known bad is blocked**

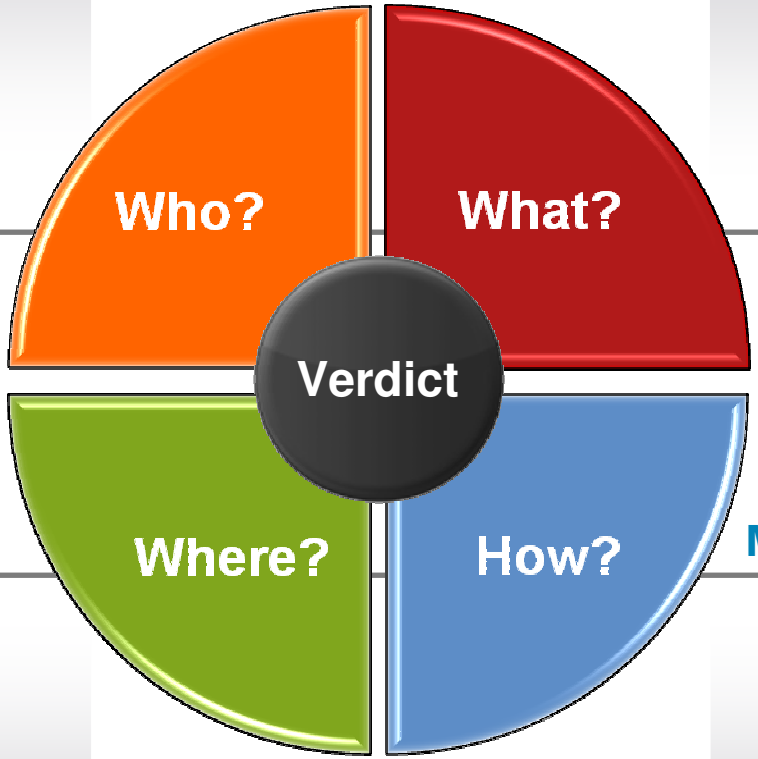
Cisco on Cisco

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



EMAIL REPUTATION

- ✓ Spam Botnets
- ✓ Spammer Networks

MESSAGE CONTENT

- ✓ SMS Spam
- ✓ Attachment-based Spam

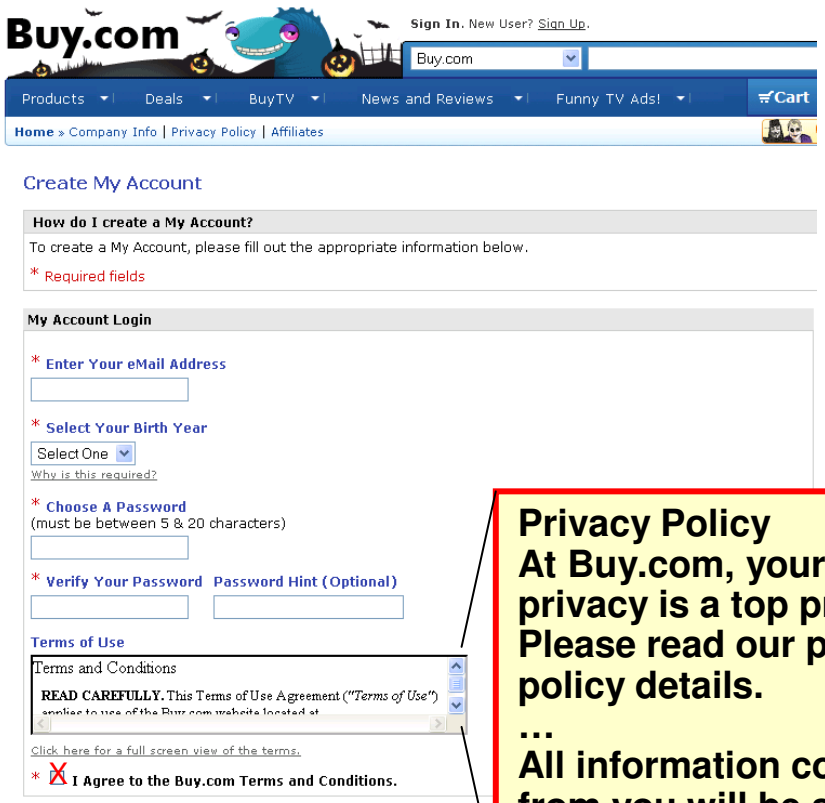
WEB REPUTATION

- ✓ Malware/Phishes
- ✓ Short-Texted Spam with URLs

MESSAGE CONSTRUCTION

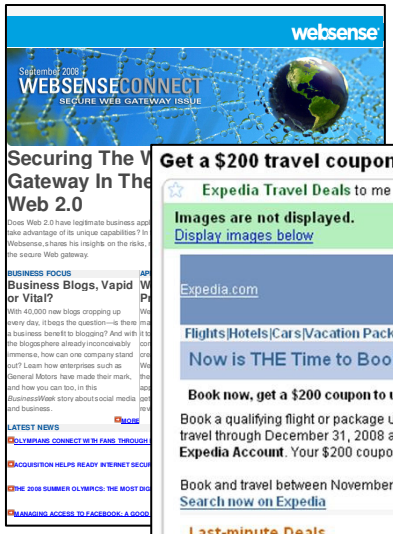
- ✓ Image Spam
- ✓ Spam created using Automation Tools

Marketing Message Detection –
The Problem



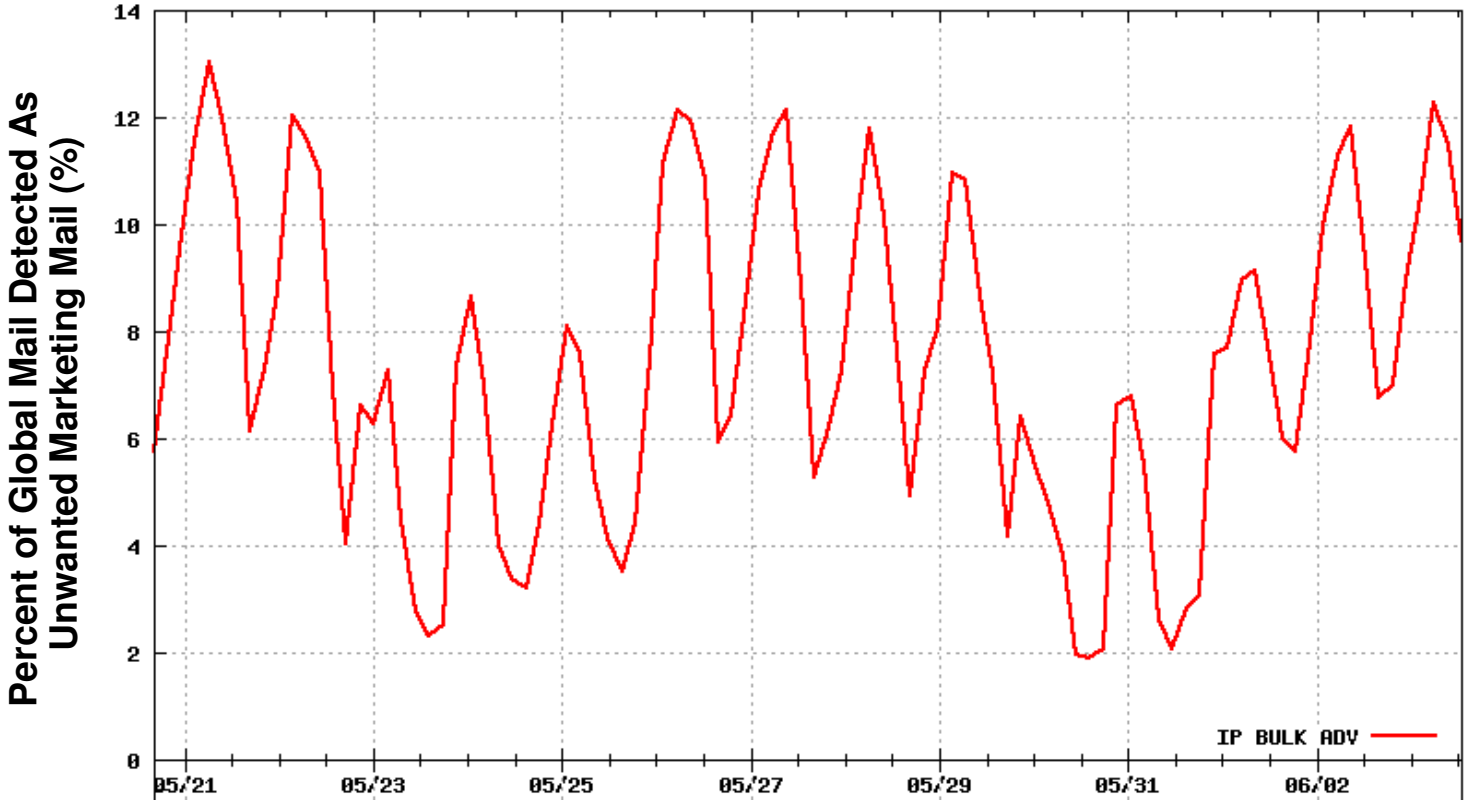
Privacy Policy
At Buy.com, your privacy is a top priority. Please read our privacy policy details.
...
All information collected from you will be shared with Buy.com and its affiliate companies.

ot-in an



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

Marketing Messages Settings

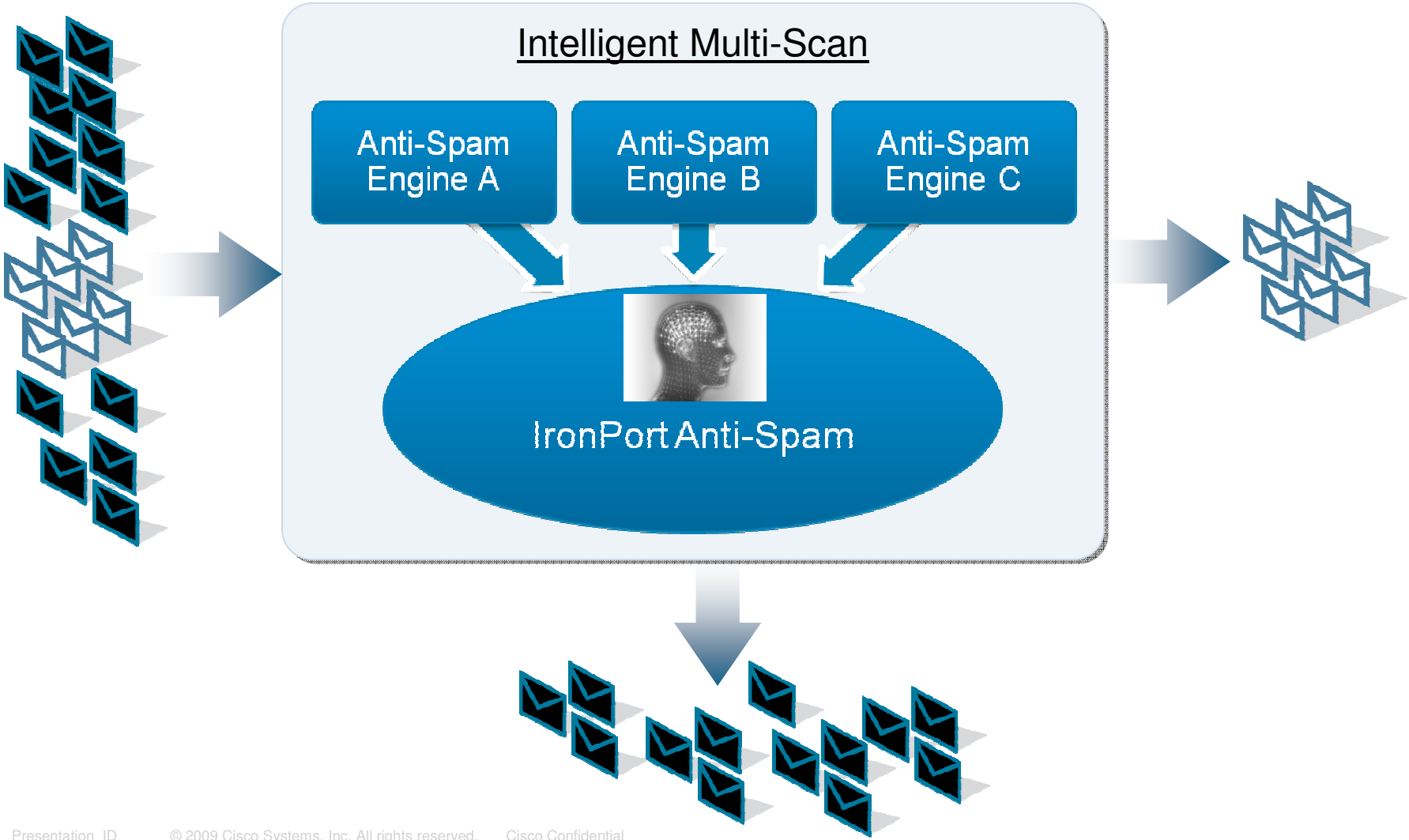
Enable Marketing Message Scanning:	○ No ◉ Yes	
Apply This Action to Message:	Deliver Send to Alternate Host (optional):	
Add Text to Subject:	Prepend [MARKETING]	
▽ Advanced	Add Custom Header (optional):	Header: Value:
	Send to an Alternate Envelope Recipient (optional):	Email Address: *(e.g. employee@company.com)*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

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**

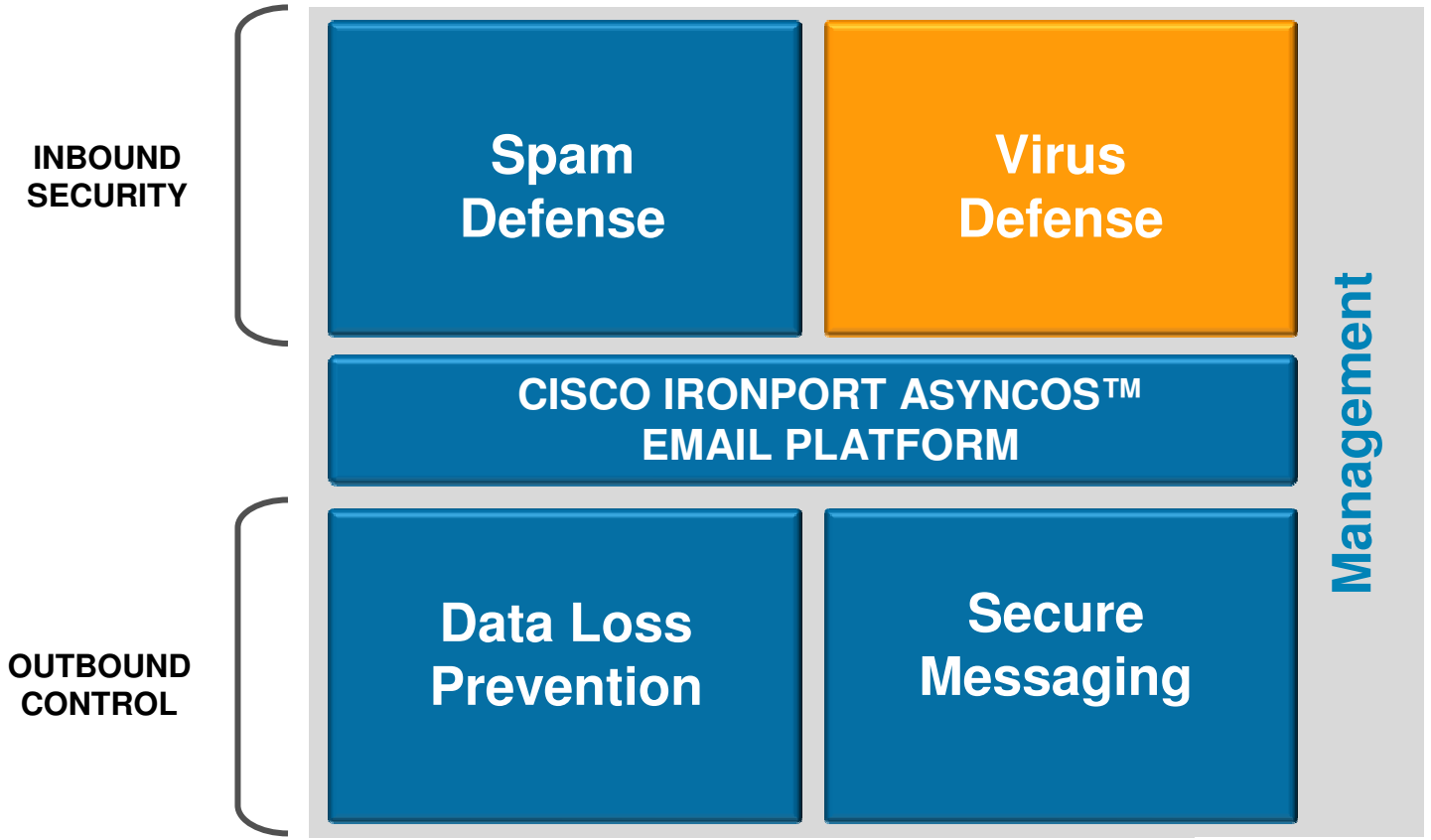
Intelligent Multi-Scan

Best of Both Worlds: Higher Detection with Low FPs

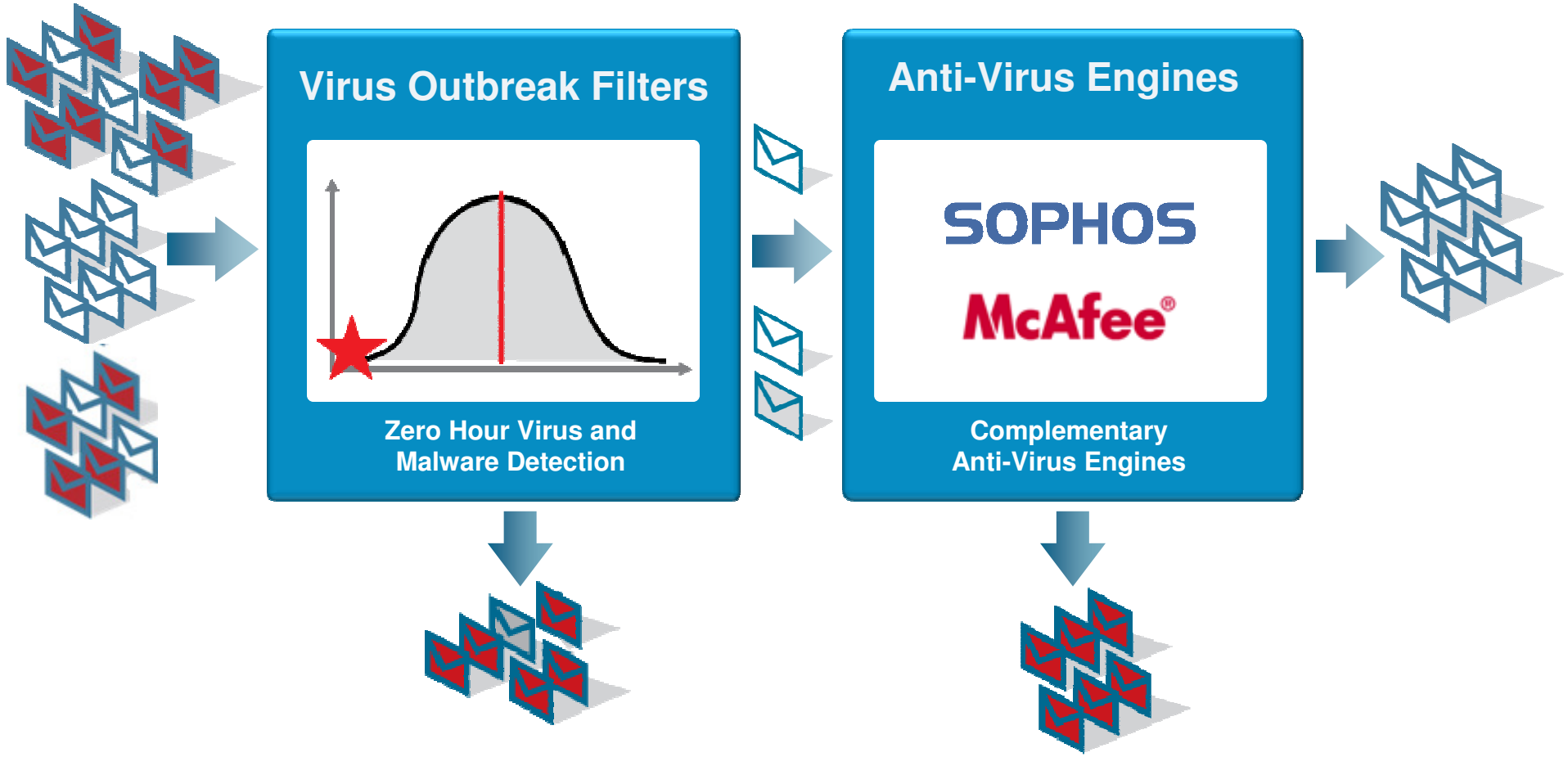


Email Security Architecture

Inbound Security, Outbound Control



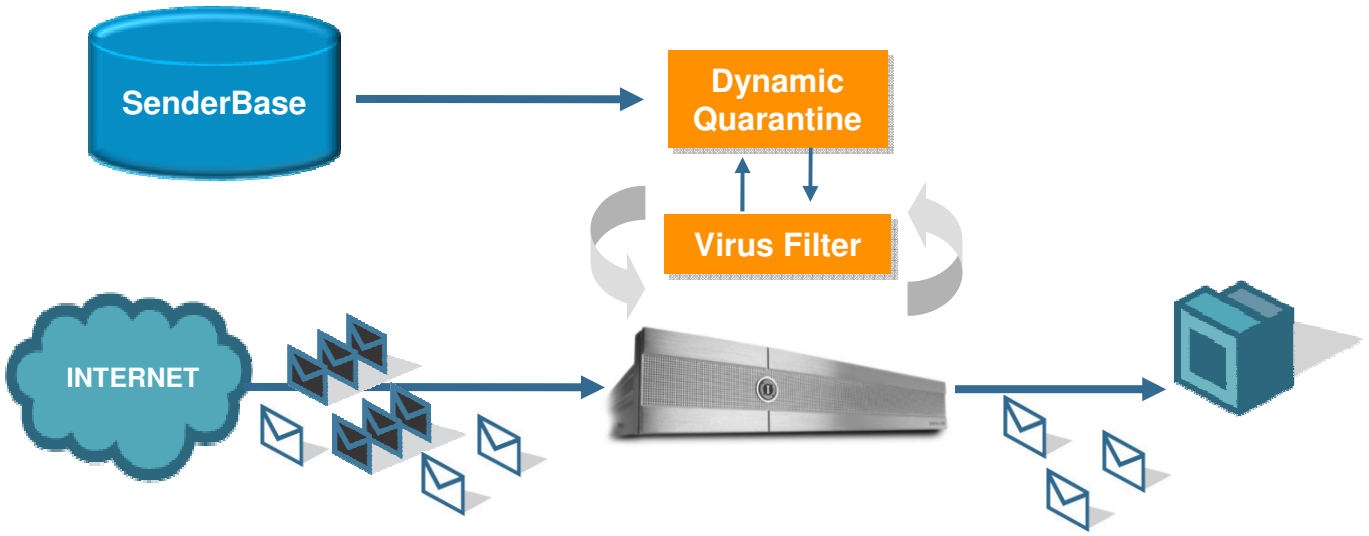
Anti-Virus Defense in Depth



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!"

AIR FRANCE

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

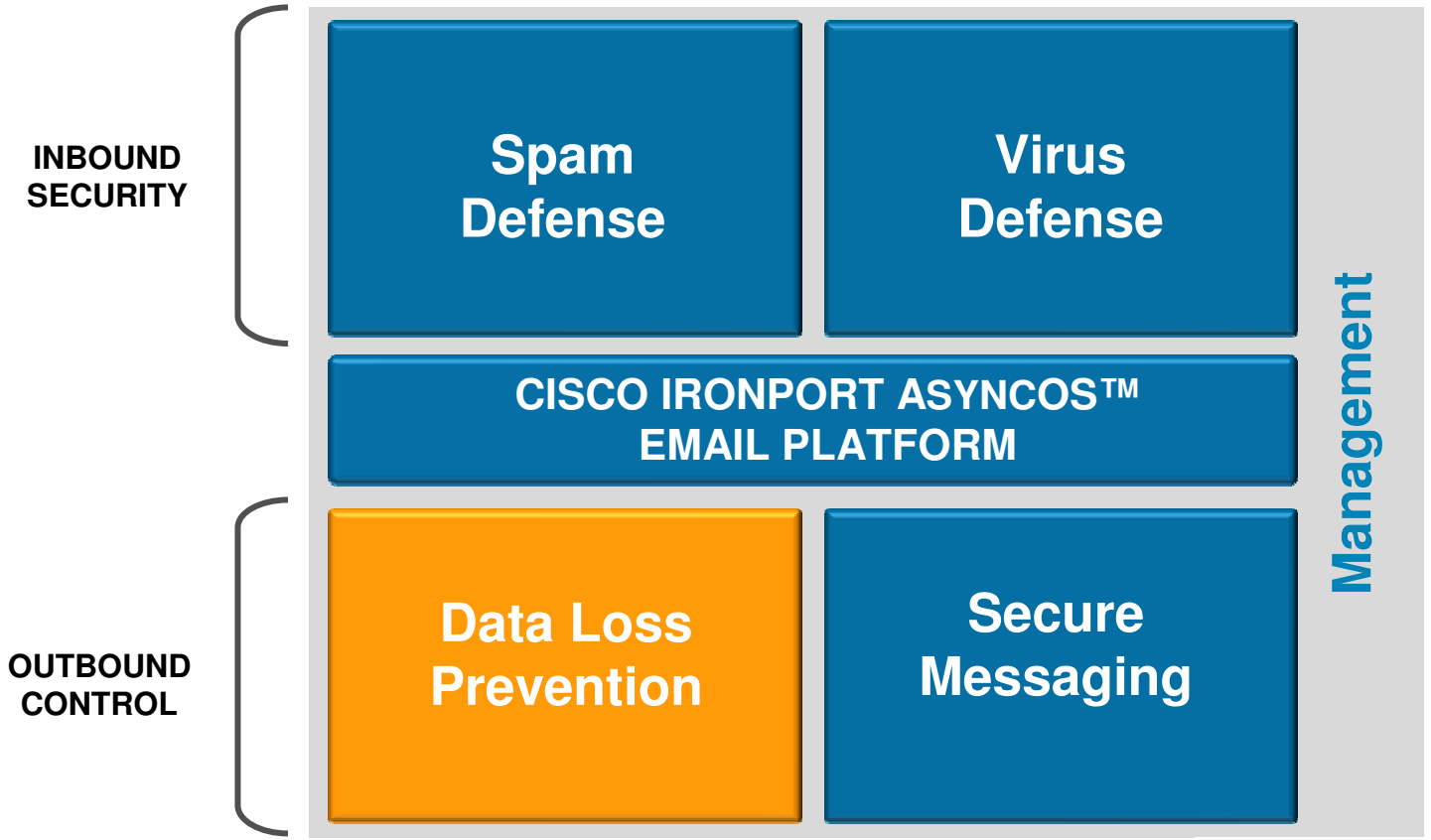
JOHNS HOPKINS UNIVERSITY

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

ACS

Email Security Architecture

Inbound Security, Outbound Control



IronPort DLP: Comprehensive, Accurate, Easy

Comprehensive

Worldwide regulatory compliance coverage, numerous remediation options

Accurate

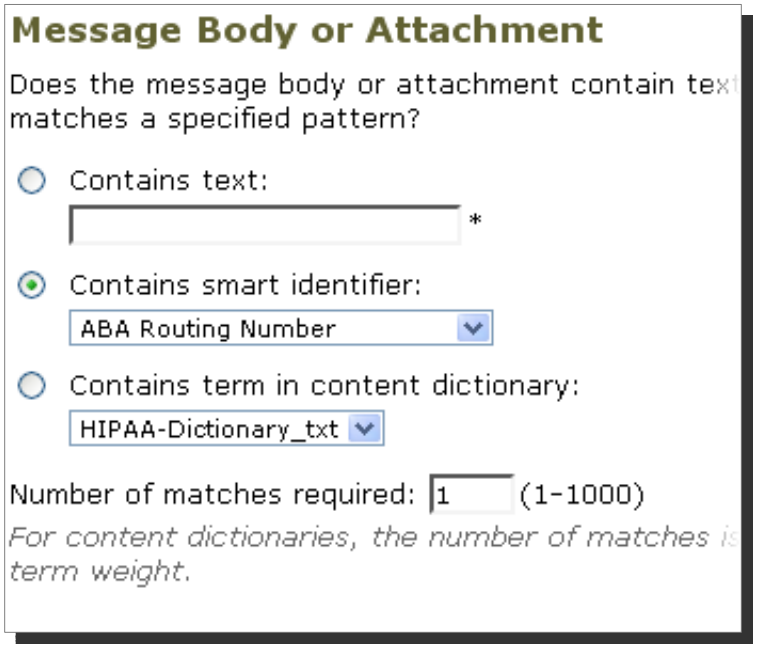
No managing false positives

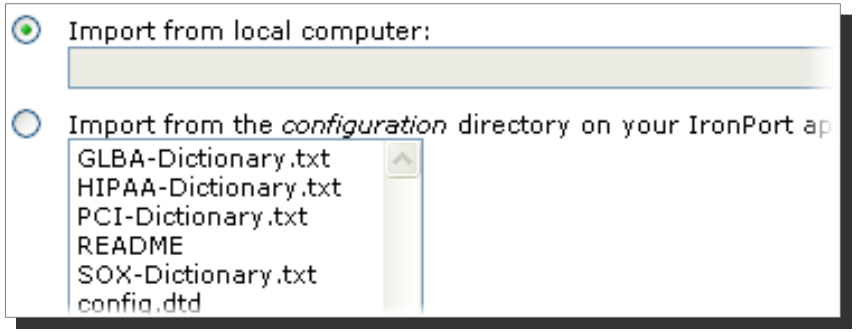
Easy

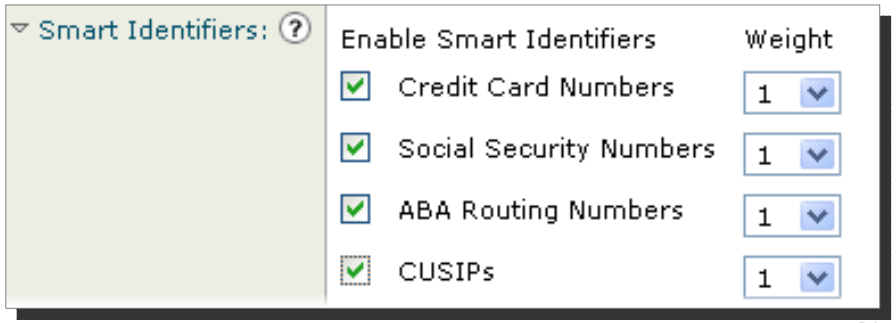
Quickly deploy and manage

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



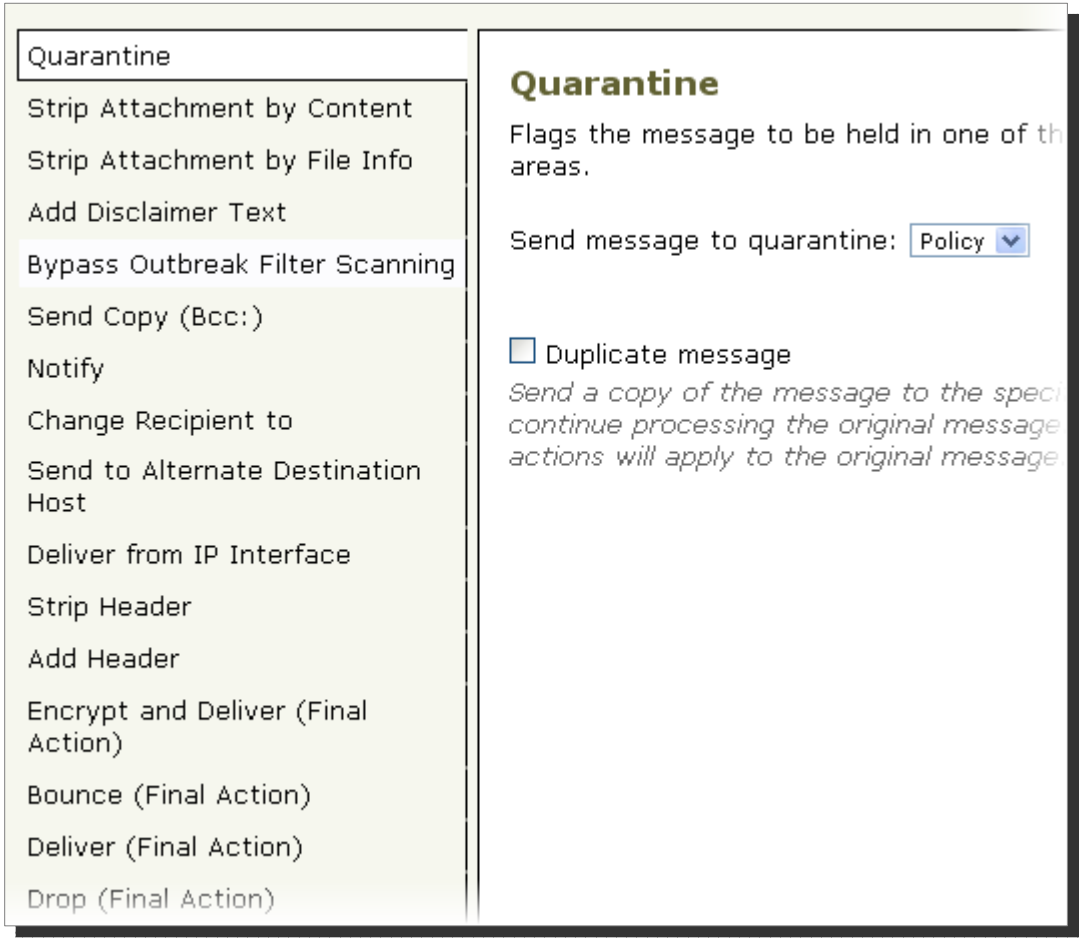




Data Loss Prevention

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



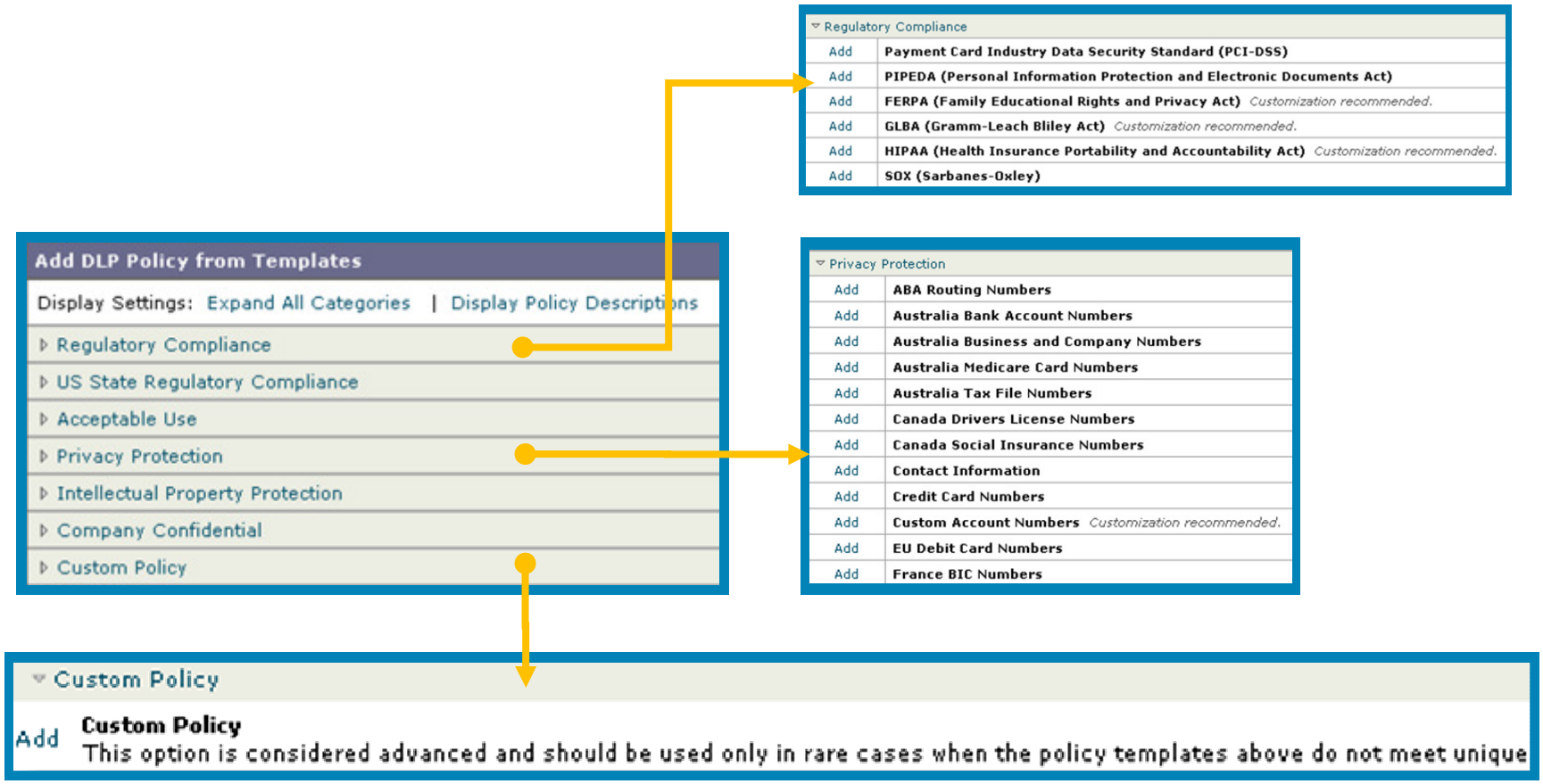
RSA – Market & Technology Leader

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

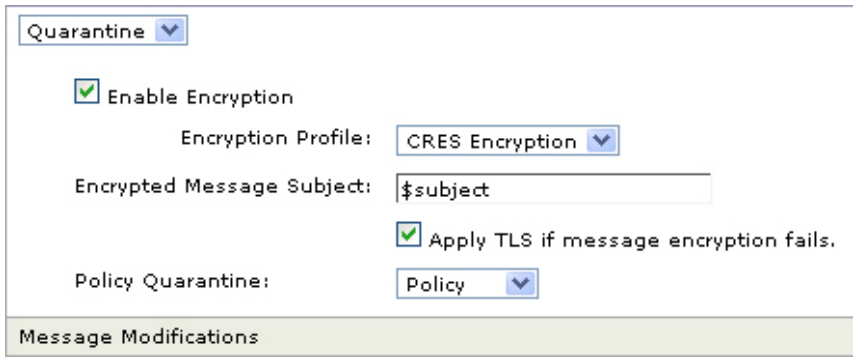
“RSA has strong described content capabilities enabled by a formal knowledge-engineering process” - Gartner

Comprehensive Policy Coverage

100+ Predefined Policies for Comprehensive Coverage



Comprehensive Remediation Options



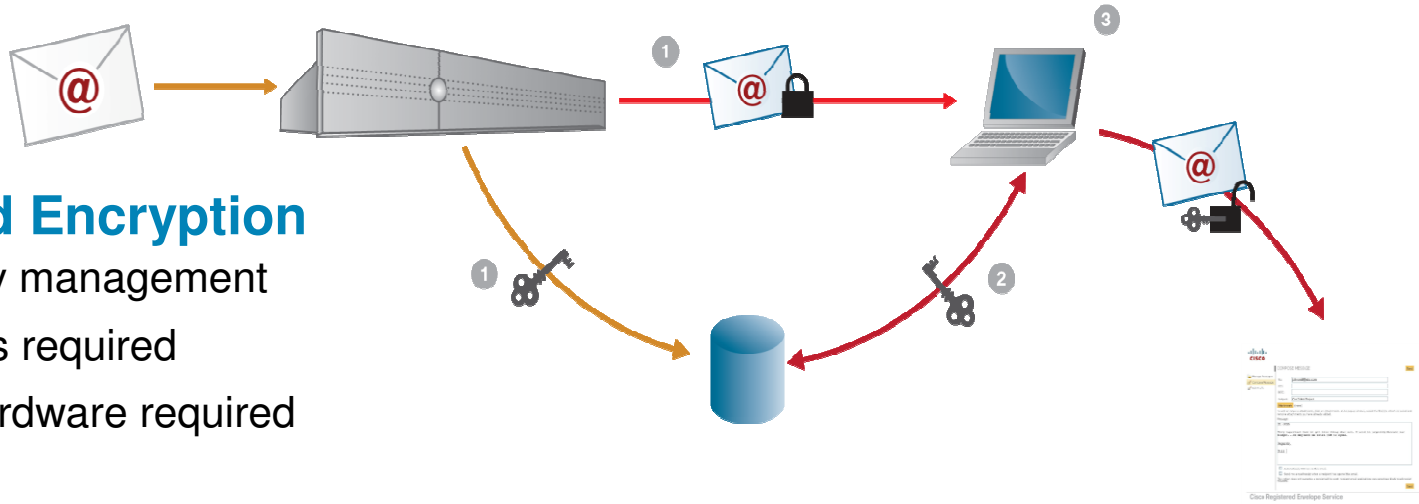
Automated Remediation

Encrypt, quarantine, deliver, or drop

Add disclaimer, modify subject

Copy or notify

Guaranteed secure delivery



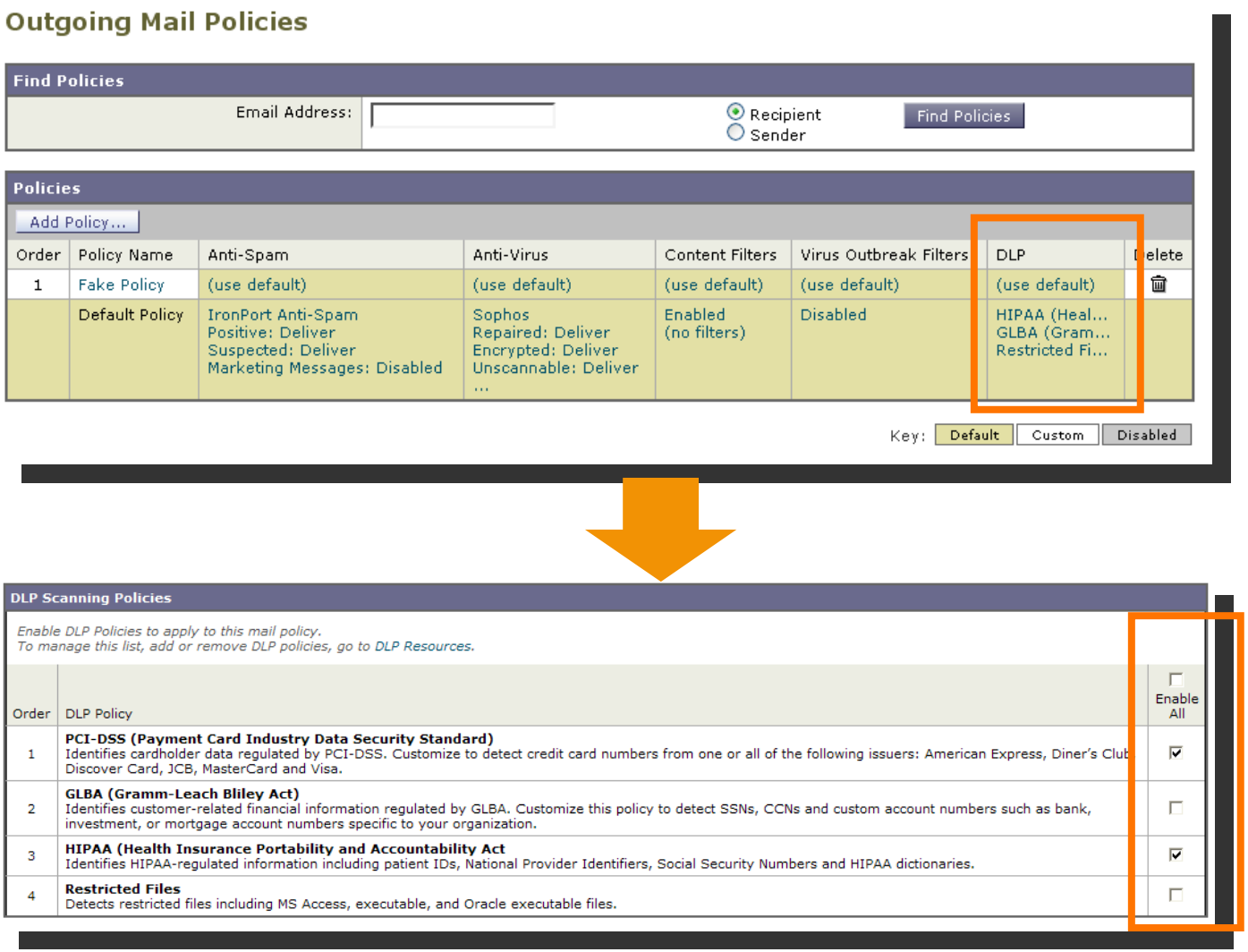
Integrated Encryption

Hosted key management

No plug-ins required

No new hardware required

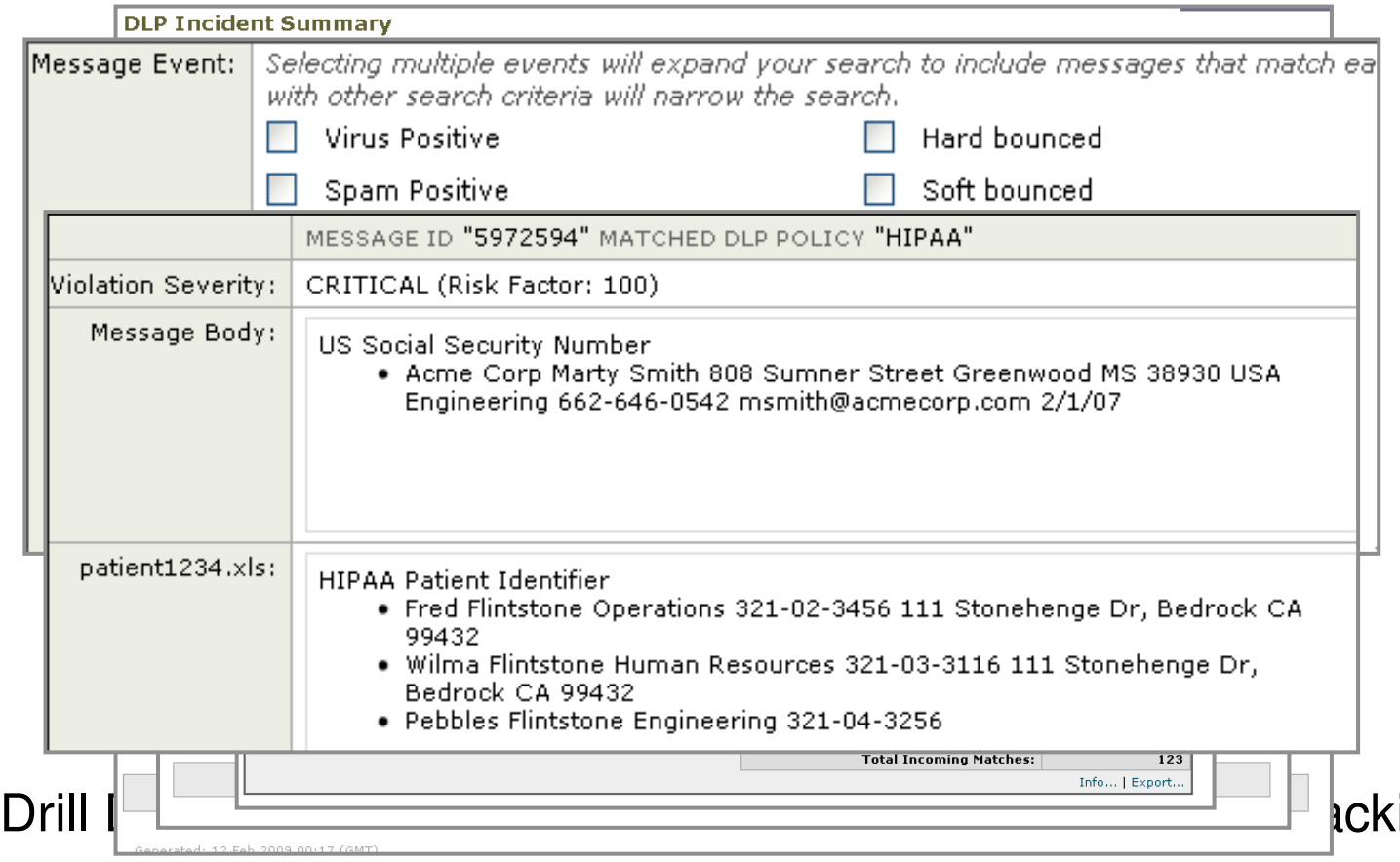
Easy to Set Up
Stop Sensitive Content in Minutes



Integrated into Policy Manager

One click activation of pre-loaded policies

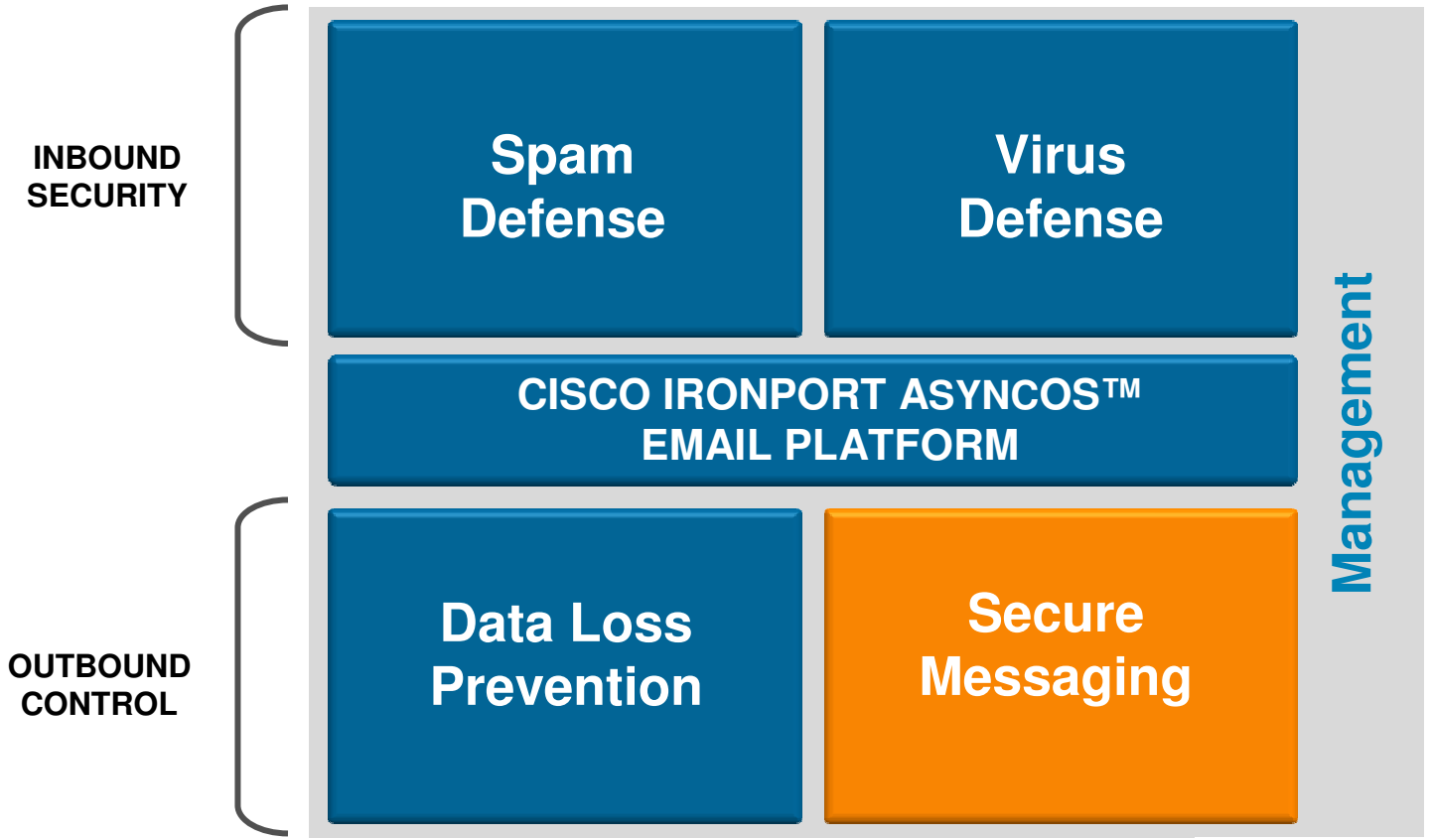
Easy Reporting & Monitoring



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

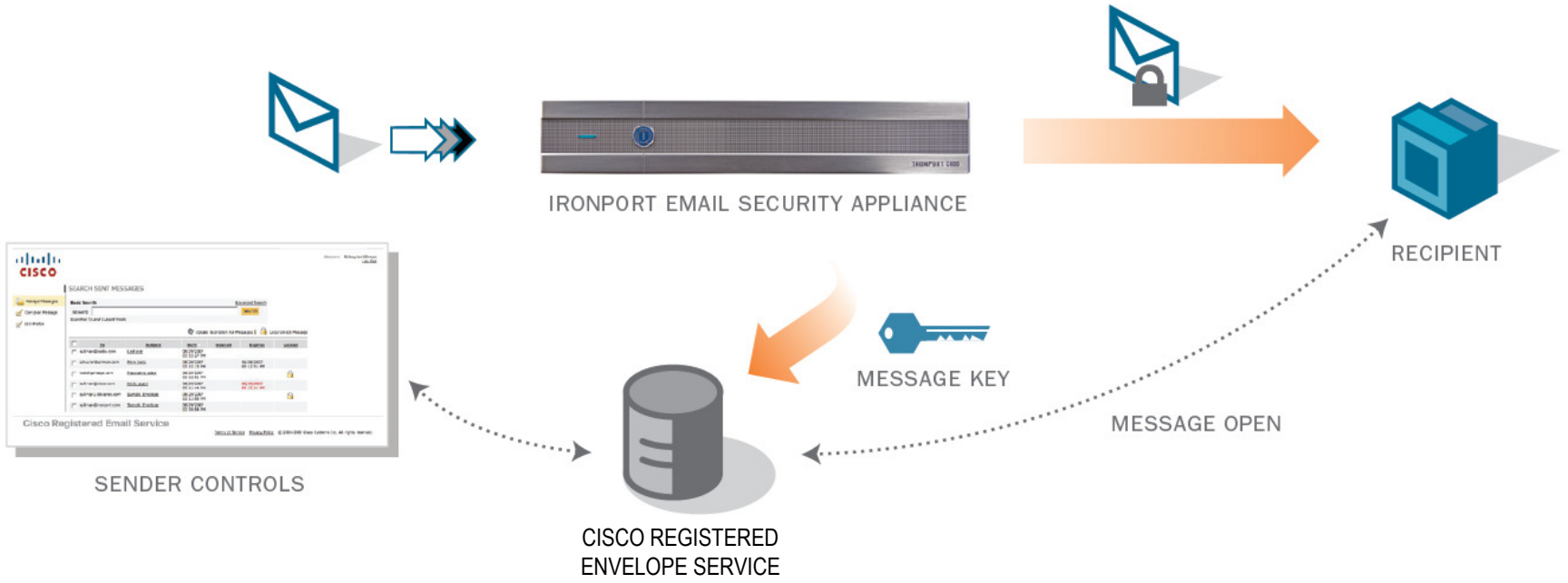
- Client plug-in support
- Public Key and Identity Management Infrastructure

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. . .

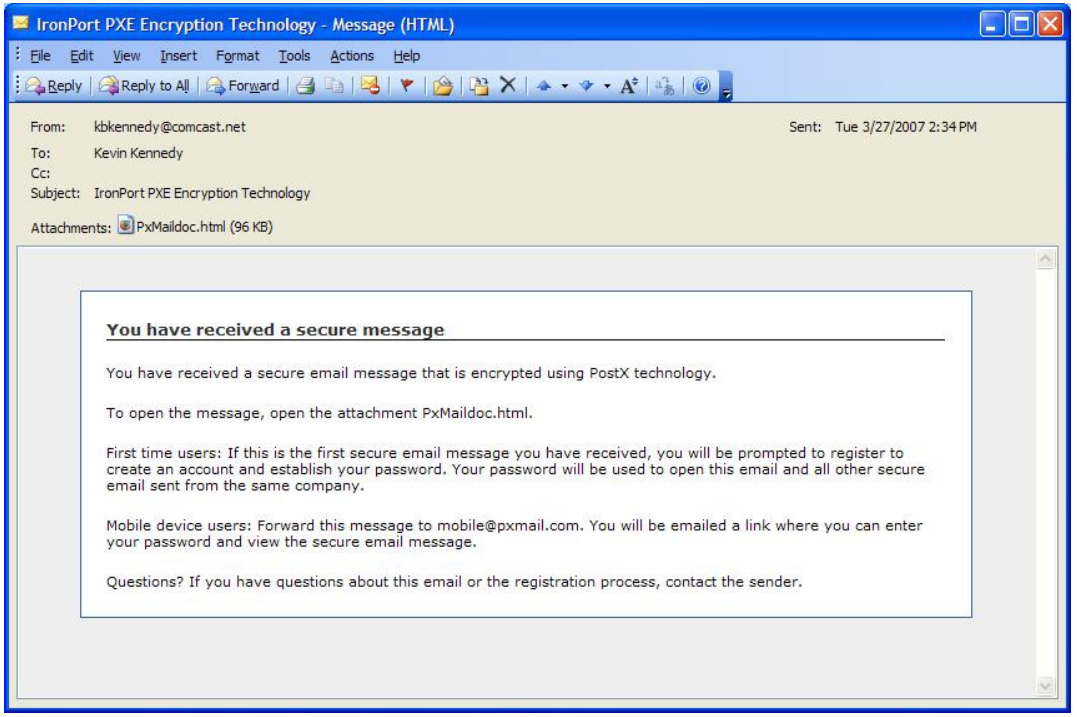


- Automated key management
- No desktop software requirements
- Send to any email address seamlessly

Cisco IronPort Email Encryption

Receiving a message

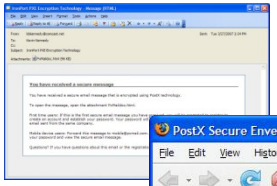
1. Receive email, click to open attachment



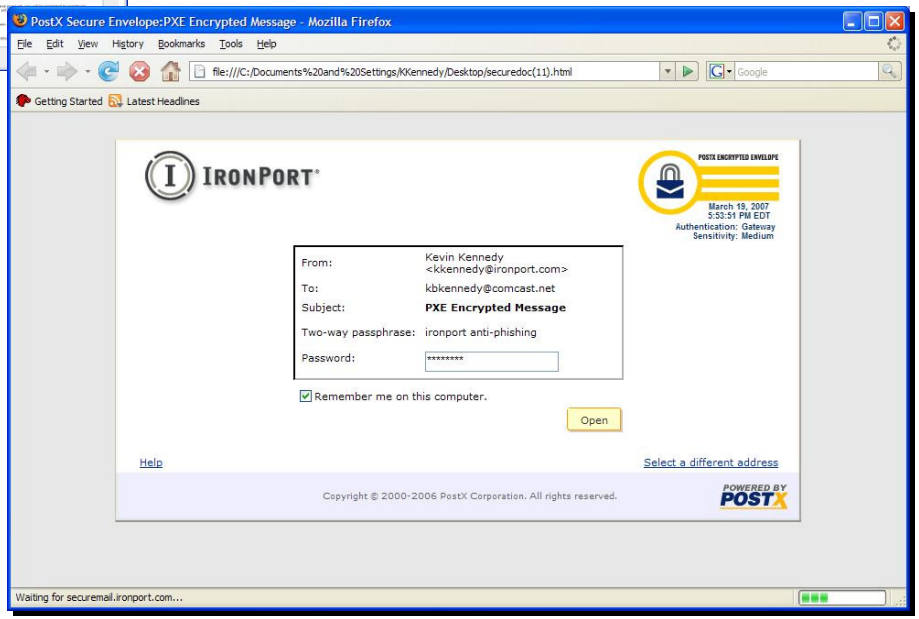
Cisco IronPort Email Encryption

Receiving a message

1 Receive email



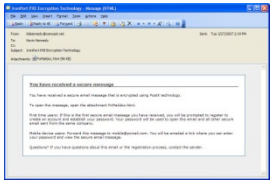
2 Enter password



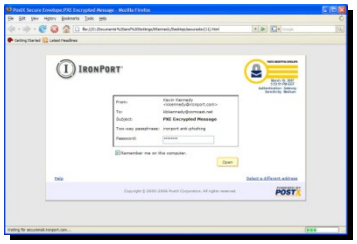
Cisco IronPort Email Encryption

Receiving a message

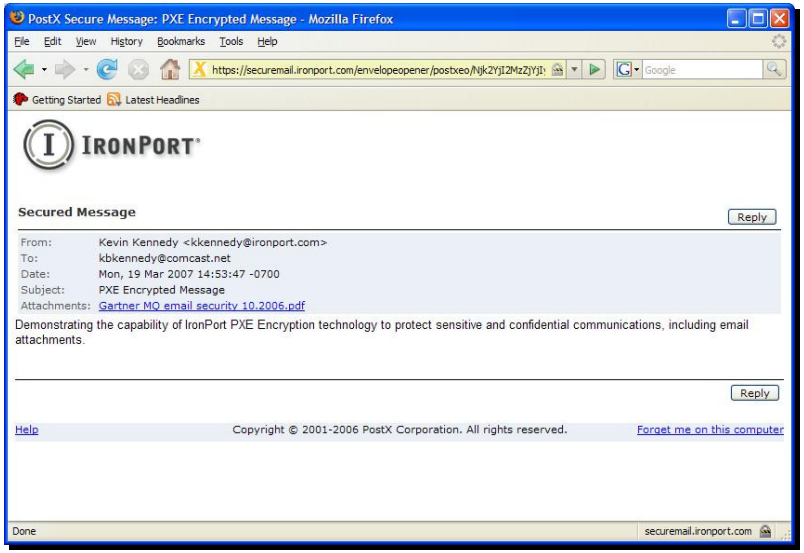
1 Receive email



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**

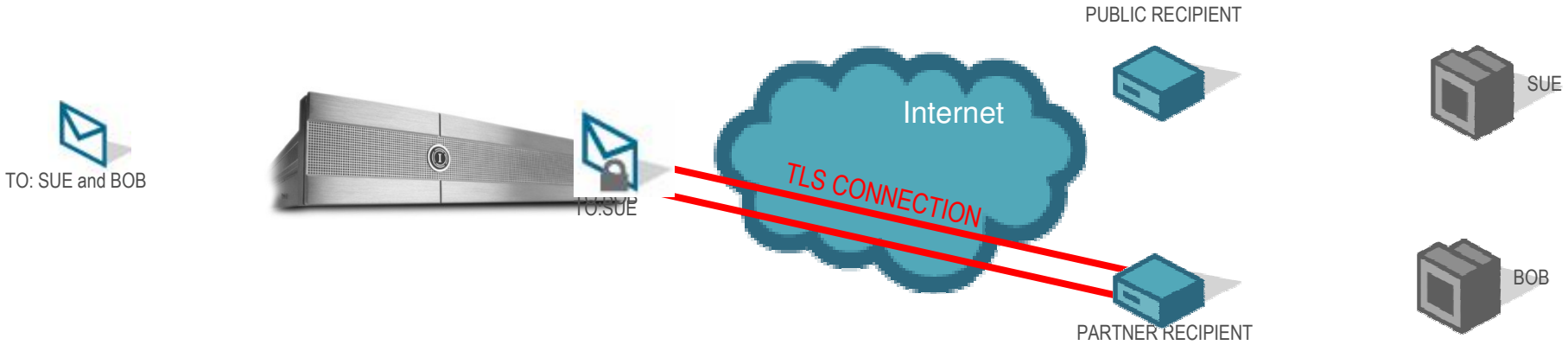
2. **Ease-of-Deployment - Solved**
   - Client plug-in support
   - Public Key and Identity Management Infrastructure
   - **IronPort Hosted Keys service**

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

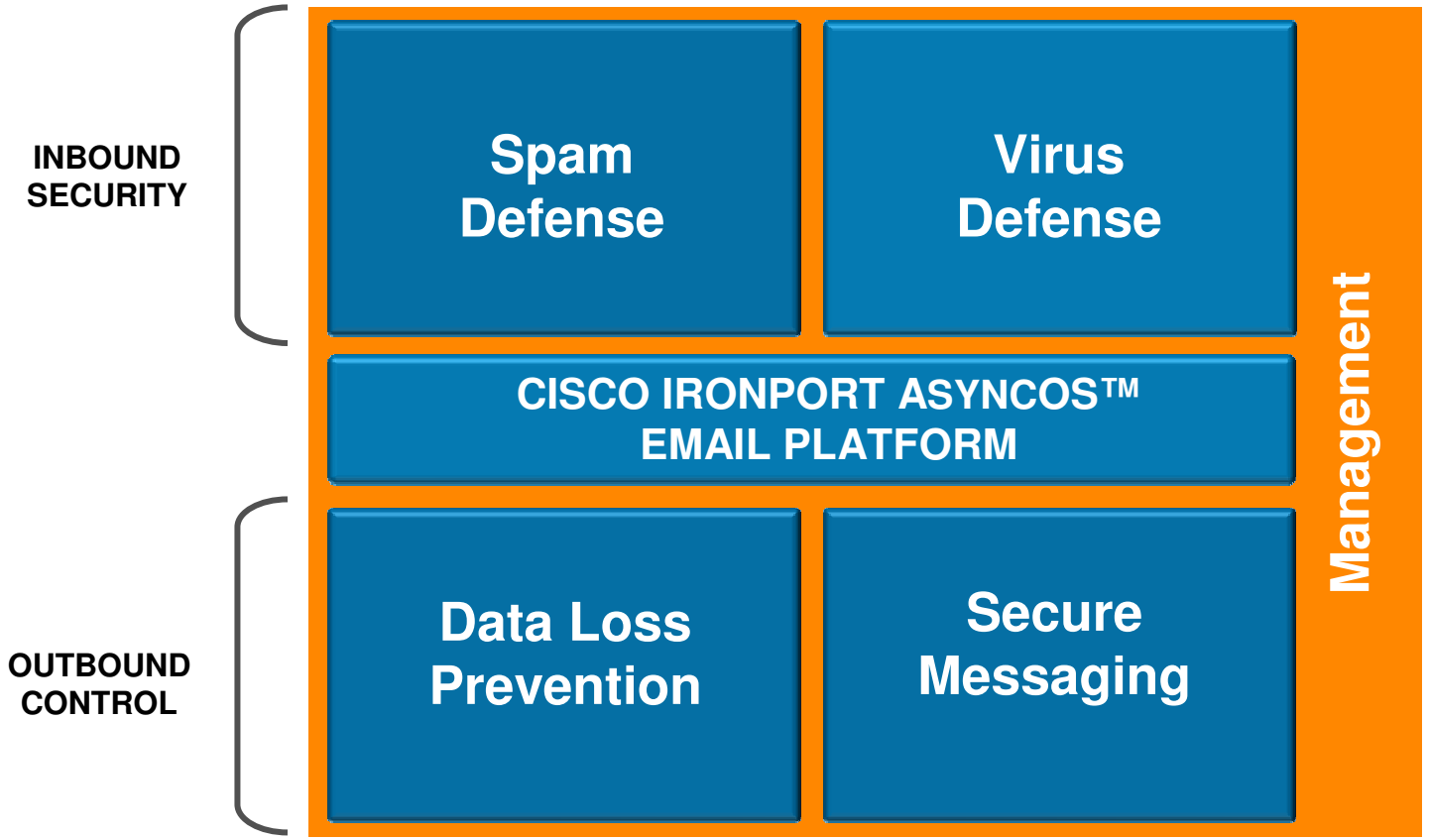
Destination-Sensitive Email Encryption

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



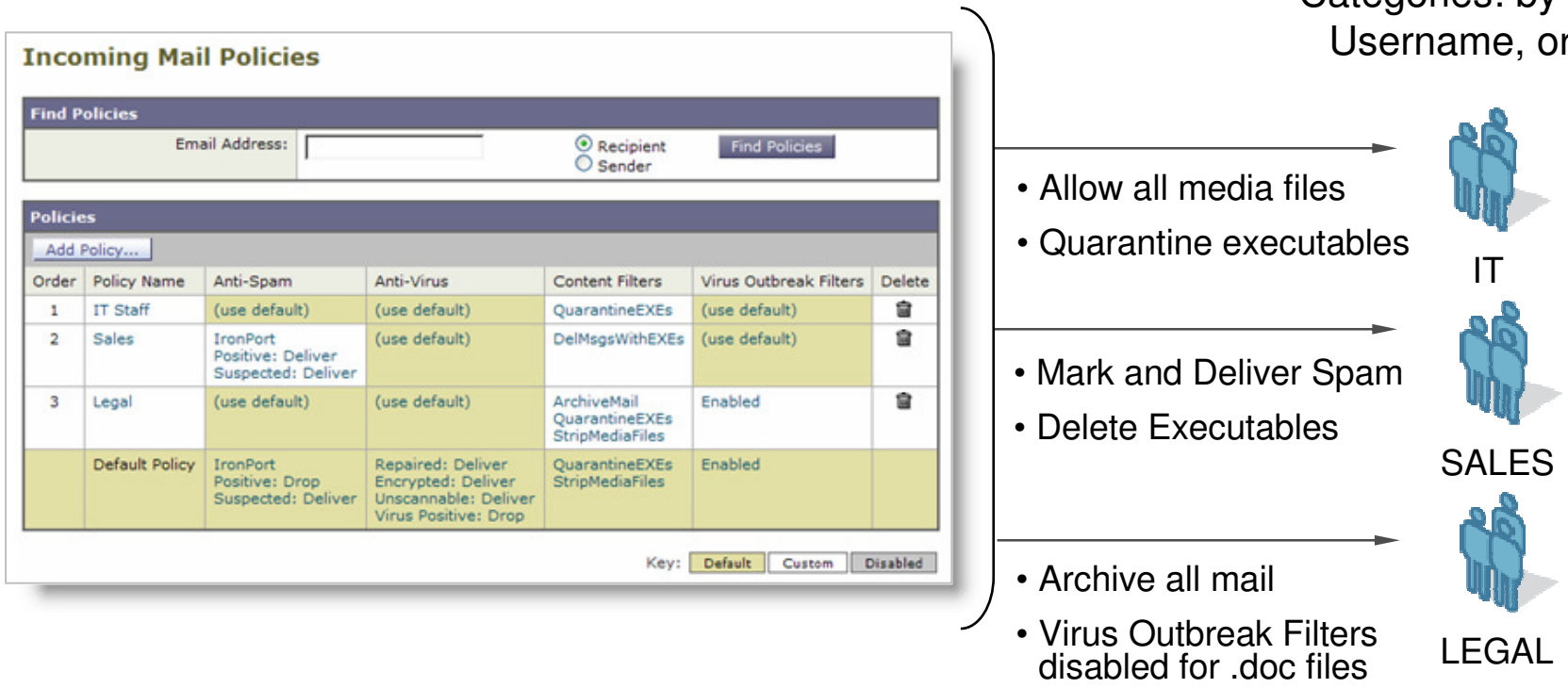
Email Security Architecture

Inbound Security, Outbound Control



Cisco IronPort Email Security Manager

Single view of policies for the entire organization



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

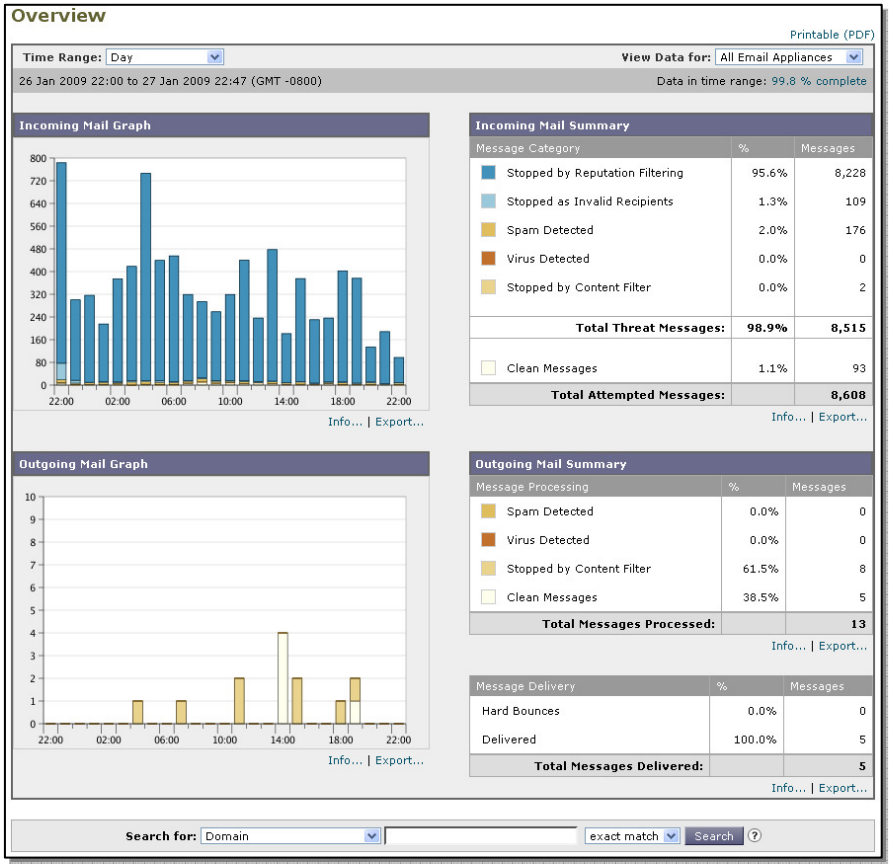
"IronPort Email Security Manager serves as a single, versatile dashboard to manage all the services on the appliance." – PC Magazine

Comprehensive Insight

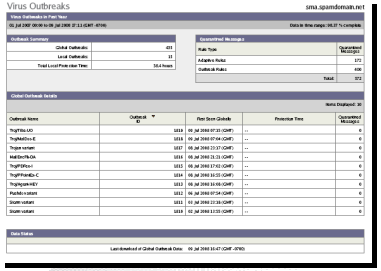
Unified Business Reporting

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

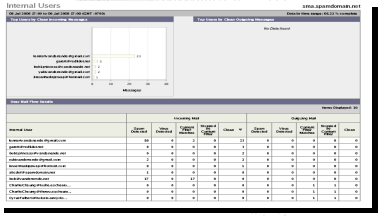
Consolidated Reports



Multiple data points



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



Visibility Into Email Messages

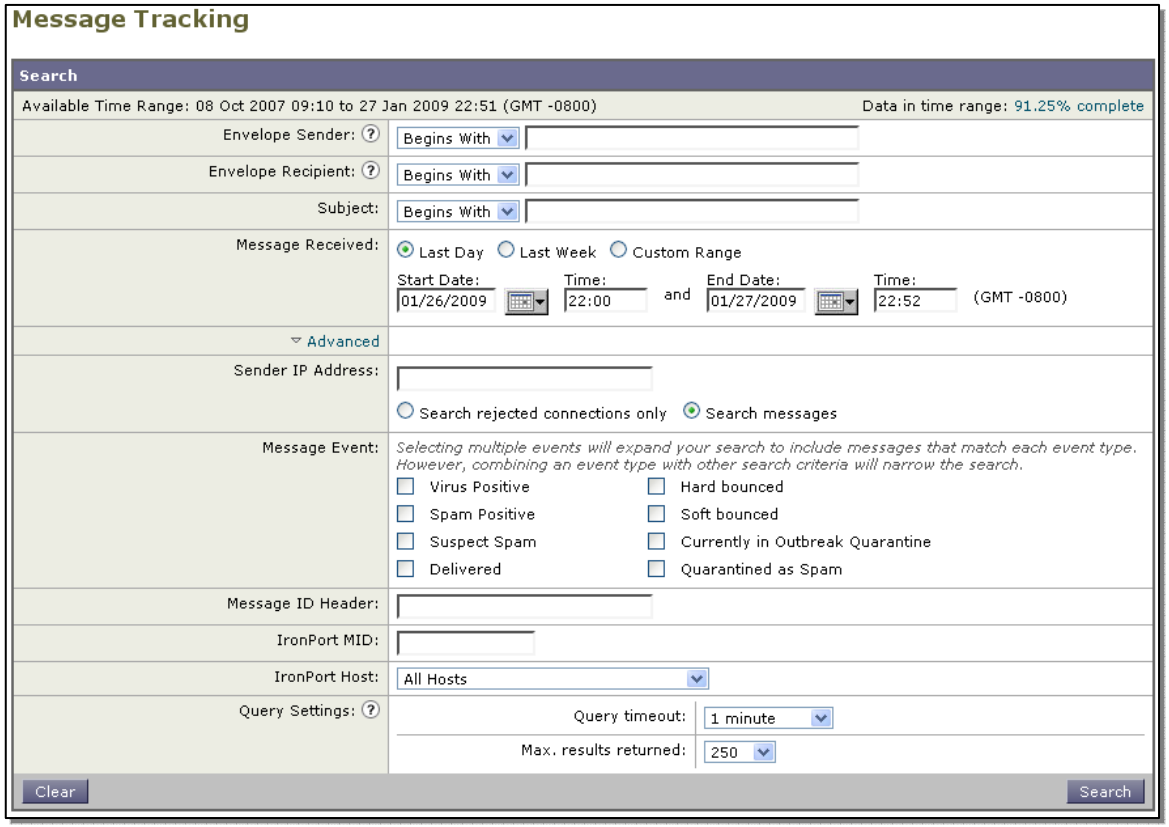
Message Tracking

What happened to the email I sent 2 hours ago?

- ✓ Track Individual Email Messages

Who else received similar emails?

- ✓ Forensics to Ensure Compliance



Unparalleled Market Leadership

Gartner

IronPort Positioned in the "Leaders" Quadrant in Magic Quadrant Report

IDC
Analyze the Future

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