



# Cisco IronPort Email & Web Security Solutions



**Sébastien Commérot**

Marketing Manager, Southern Europe, Middle-East & Africa

Cisco IronPort

# Cisco IronPort: Unparalleled Market Leadership

## Gartner

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



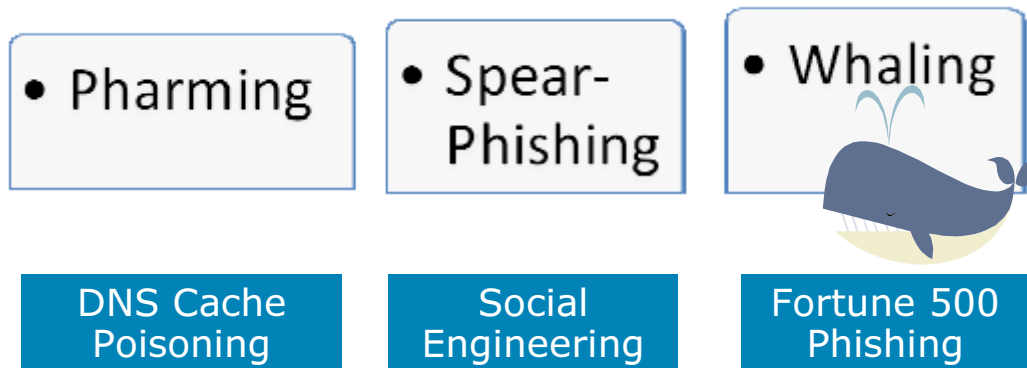
*IronPort is positioned as a leading  
player in the messaging security  
appliance market*

**THE RADICATI GROUP, INC.**  
A TECHNOLOGY MARKET RESEARCH FIRM

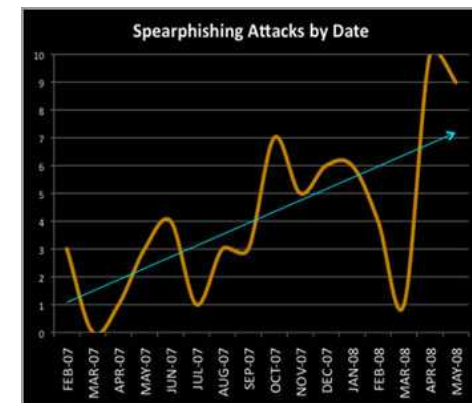
*Named IronPort the market share  
leader in the email security appliance  
market*

- IronPort funded in 2000, acquired by Cisco in 2007
- 20,000+ customers globally
- 400 million users protected
- 40% of Fortune 100 companies
- 8 of the 10 largest service providers
- 99%+ customer renewal rates

# Phishing is changing



- 1/3 of phishing sites host malware
- Average on-line time for a phishing site: 3 days



Source : Anti-Phishing Working Group

# What about TypoSquatting?

- Focus on heavy traffic sites
- Hackers register names close to famous brands or sites
  - Inve~~s~~rion of 1 letter
  - Name variant  
(micr~~p~~soft)
  - Orthog~~r~~afic Mistake
- Creation of a similar site, downloading malware on computers

[www.google.com](http://www.google.com)

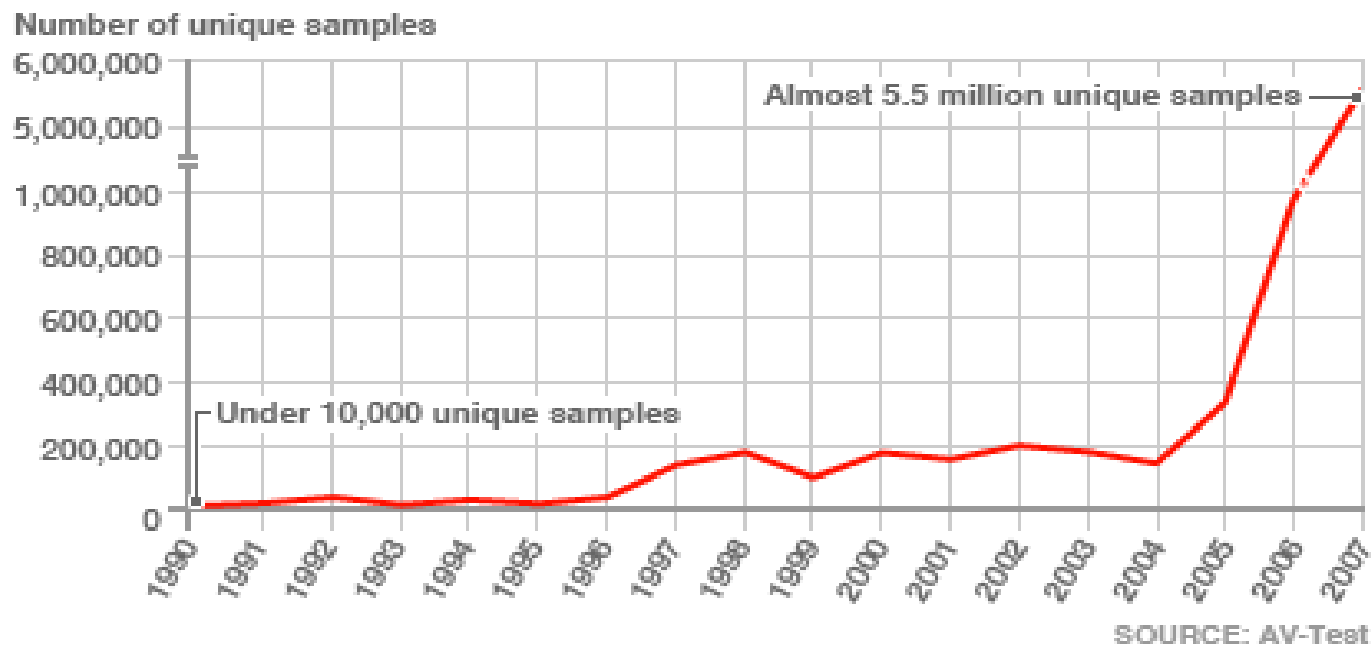
[www.mcrosoft.com](http://www.mcrosoft.com)

[www.hotmial.com](http://www.hotmial.com)

[www.wikipefia.org](http://www.wikipefia.org)

# Malware is on the rise

## Unique samples of malicious codes

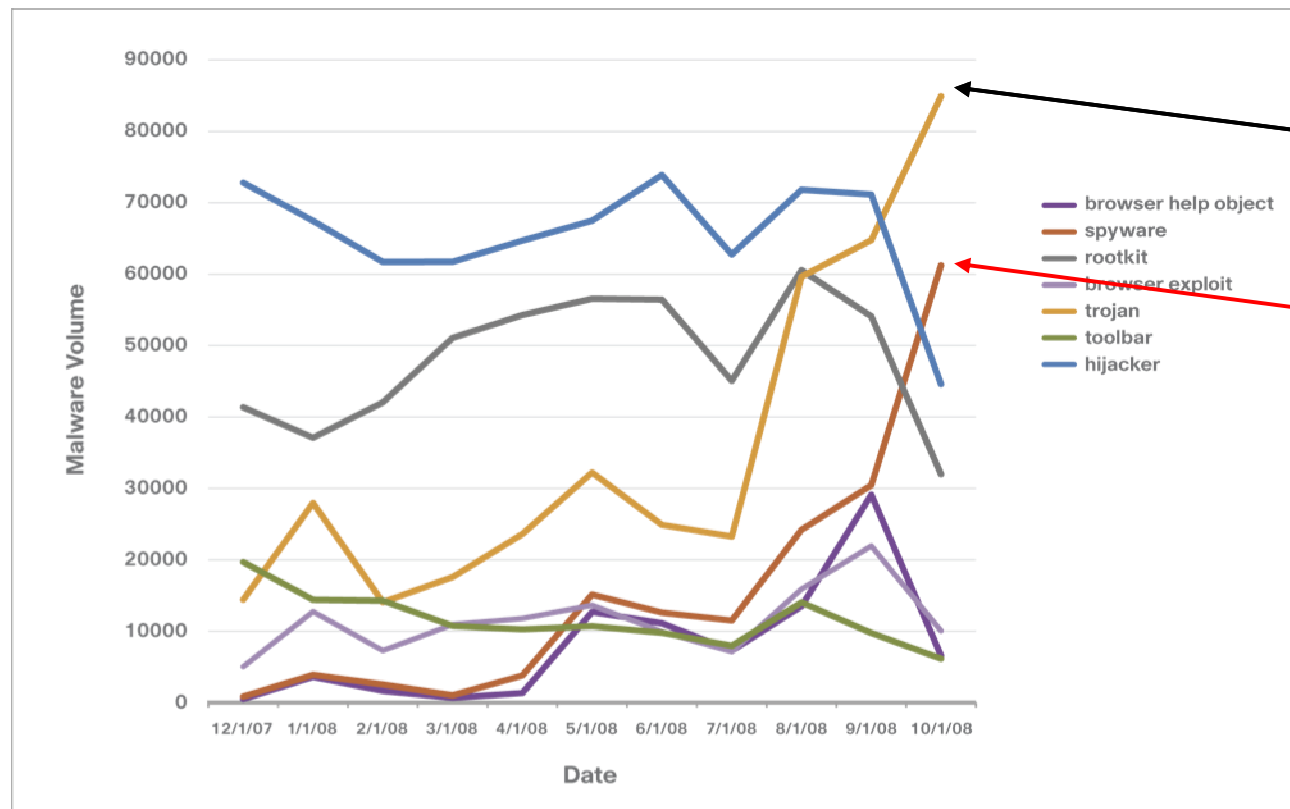


Unique malware samples in 2006: 972 000  
Unique malware samples in 2007: 5,5 M

+ 500% in 12 months!

# More and more Trojan Horses

*Converting computers into zombies*



*Trojan horses  
x6 in 1 year!*

*Spyware  
x12 in 1 year!*

# Zombies are changing

## The Storm network

- **The world's most important botnet**

1000 contaminated PCs rented \$220 in Germany

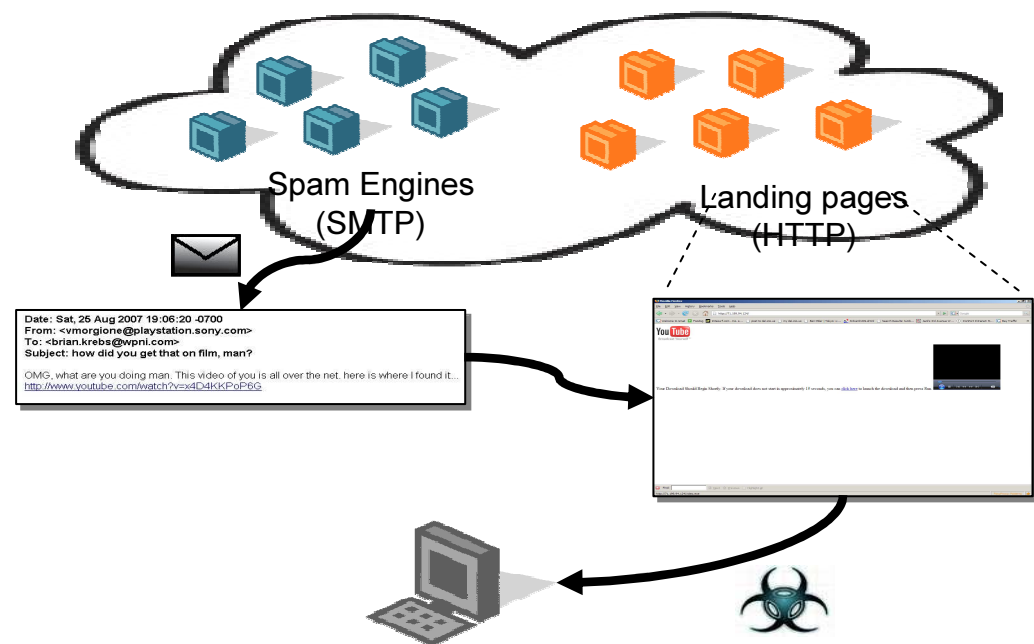
1000 contaminated PC in the USA \$110

Rented per hour, with phone support available

- **Self-expanding:** Recruiting emails & Spam

- **Coordinated:** Synchronizes email spam with web landing pages

- **Peer-to-Peer:** Uses P2P network to communicate

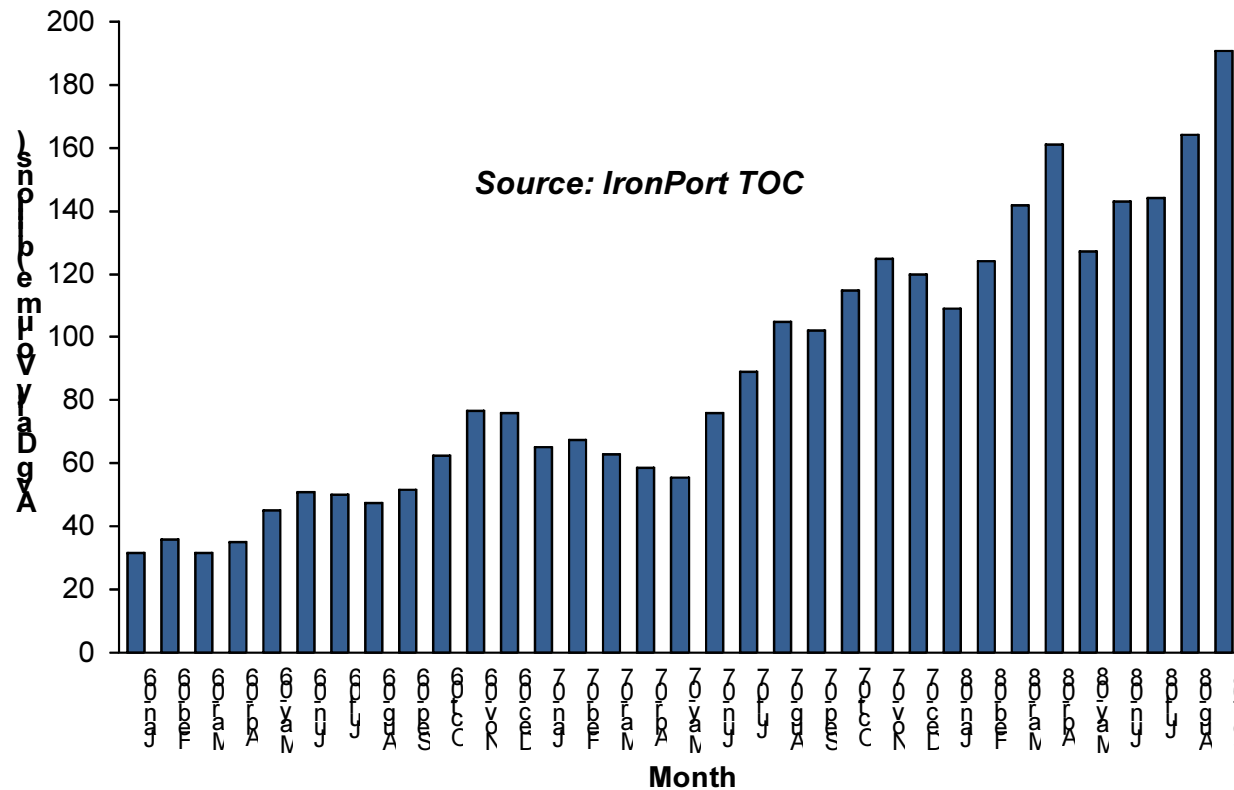


**2007** : Storm is born

**2008** : Storm still active, joined by Kraken/Bobax & Asprox

# Spam keeps growing...

*And will keep on growing!*



*x6 in last 3 years!*

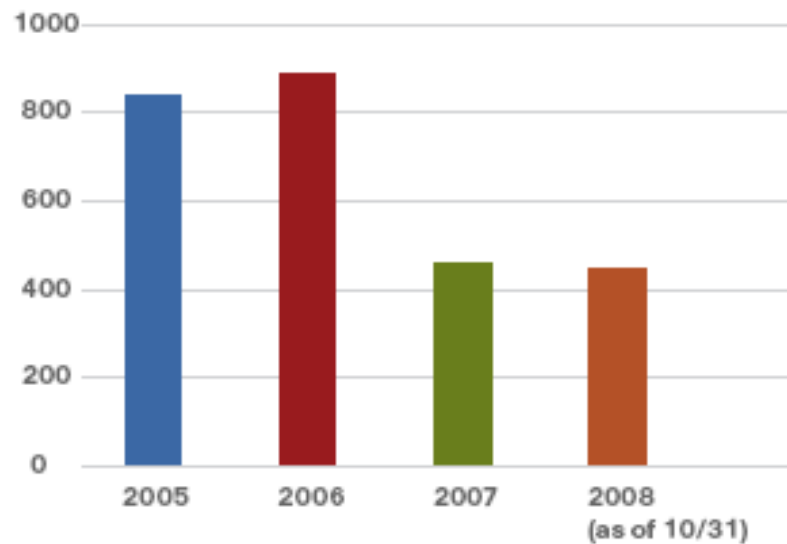
*x2 in next 4 years!*

	2008	2009	2010	2011	2012
Worldwide Messages/Day (B)	210	247	294	349	419
Worldwide Spam Traffic/Day (B)	164	199	238	286	347
Total Spam %	78%	80%	81%	82%	83%

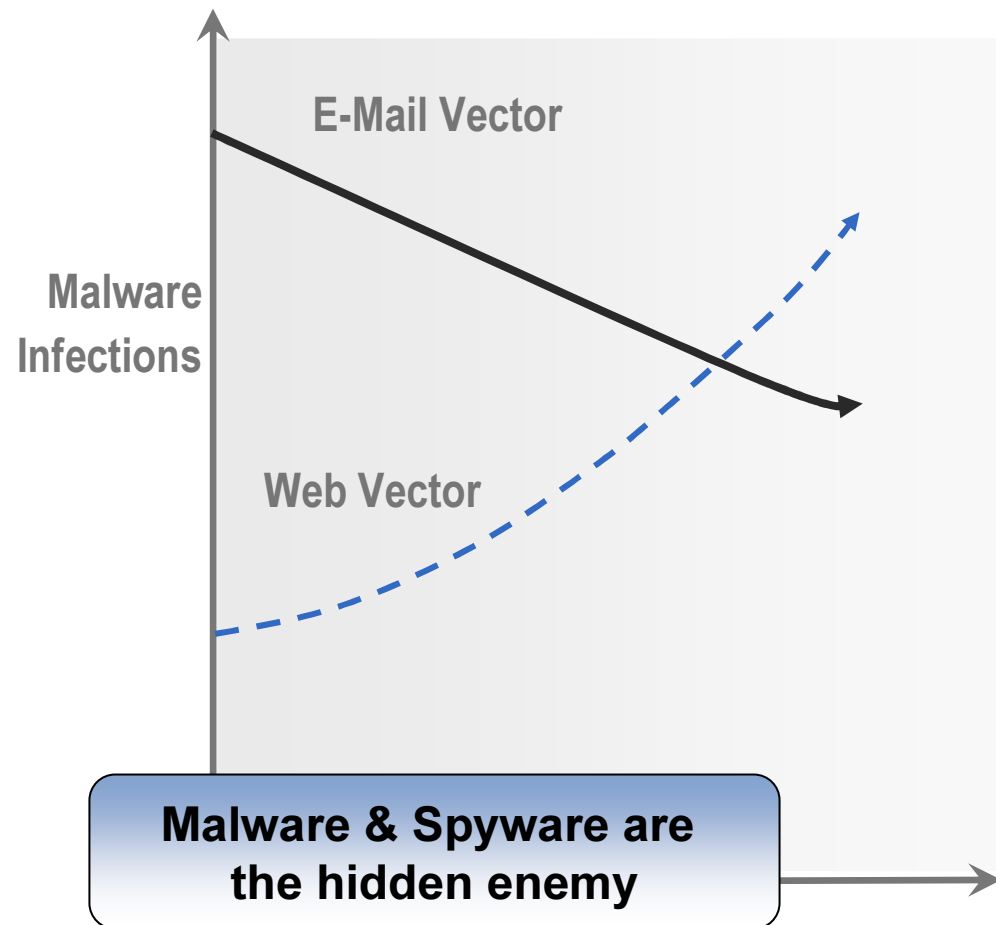
Source: Radicati E-Mail Security Market 2008-2012



# Threat vectors are changing



Volume of Malware Successfully Propagated via Email Attachments



# Legitimate Sites Hacked

- Over **87%** of all Web-based **threats today** are using **exploited web sites\***
- **9 out of 10** web sites vulnerable to attack\*\*
- A commonly used technique today: iFrame attacks
  1. A legitimate site is hacked (iFrame added on a page)
  2. The user is re-directed by the iFrame towards an infected website
  3. A malware is automatically downloaded on the desktop by exploiting a vulnerability of the web browser
- **Cannot be secured with legacy URL filtering solutions**



**\*Source: Cisco TOC**

**\*\*Source: White Hat Security, Website Sec Statistics Report 10/2007**

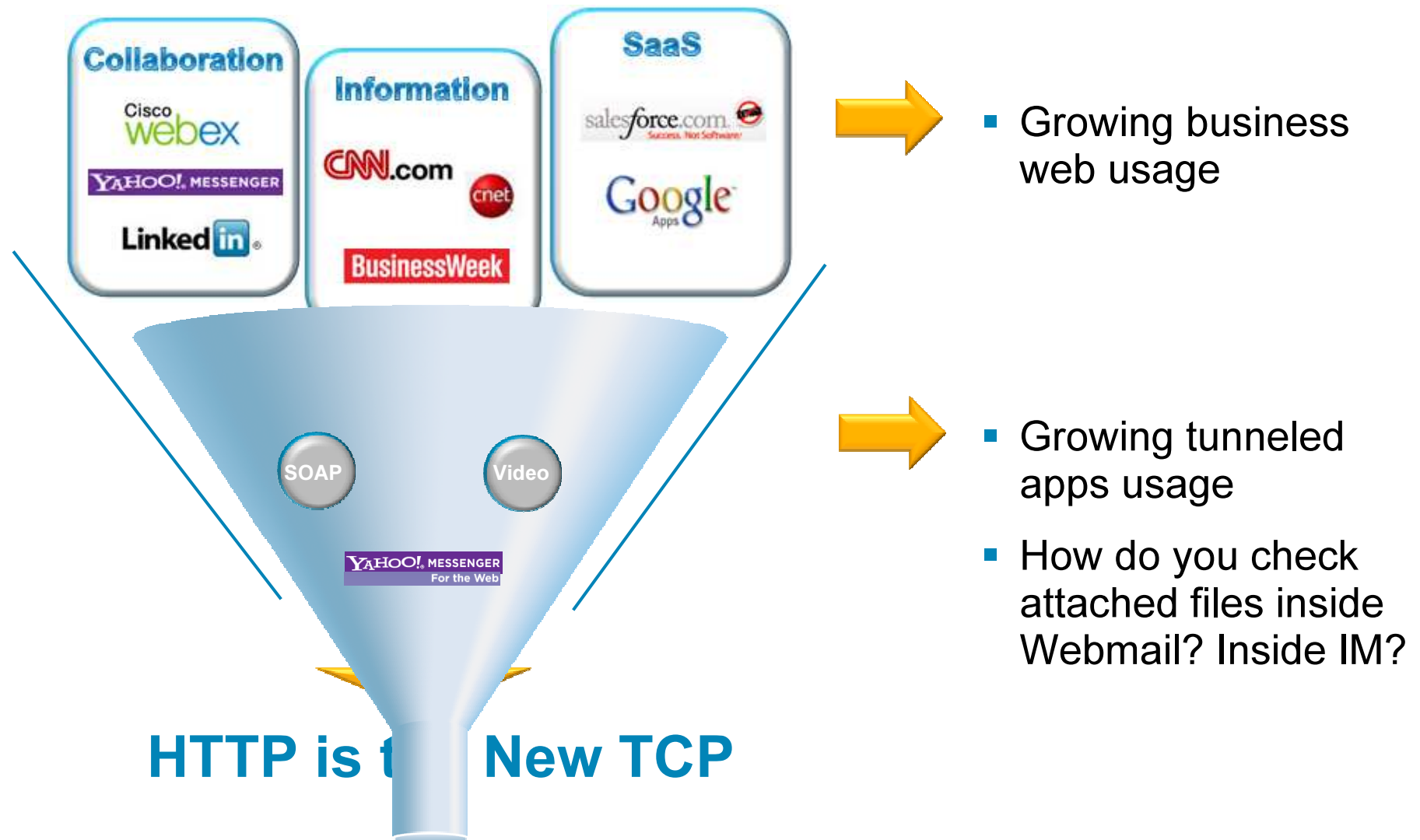
# Exploited Website Example

- The user simply connects to the “Business Week” homepage
- He can look at the page, but at the same time he is redirected towards a malicious website
- A malware is downloaded from the malicious site
- Not stopped by traditional URL filtering solutions (category : news)

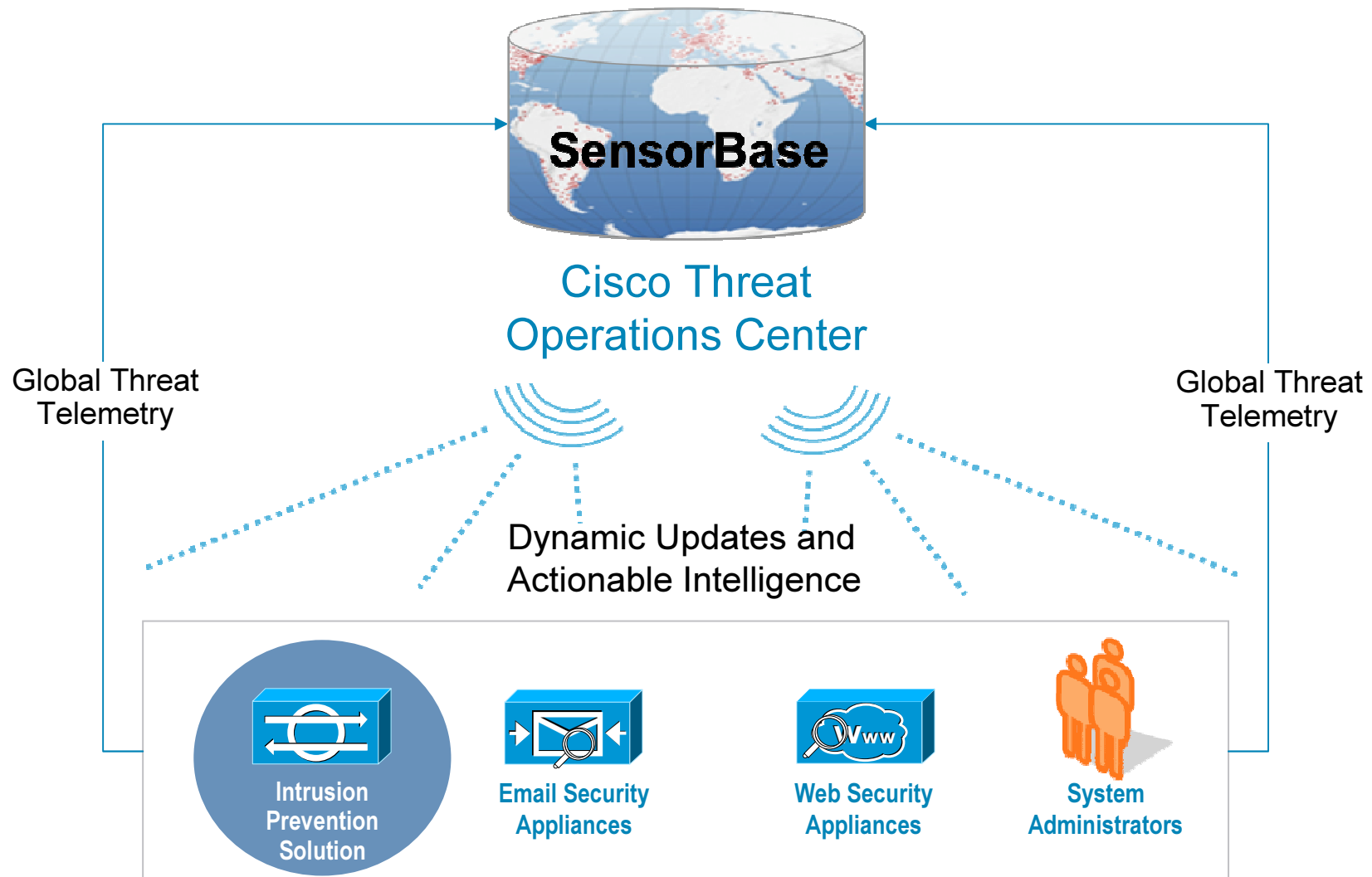


# Increasing Enterprise Web Traffic

Port 80 & 443 usage has changed



# Cisco Global Threat Correlation



# Cisco IronPort SensorBase®



- Statistics on more than 30% of the world's e-mail traffic
- New threats & alerts detection
- More than **150 parameters** to build reputation scores

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

## E-Mail Reputation Filters

.....► Reputation Score

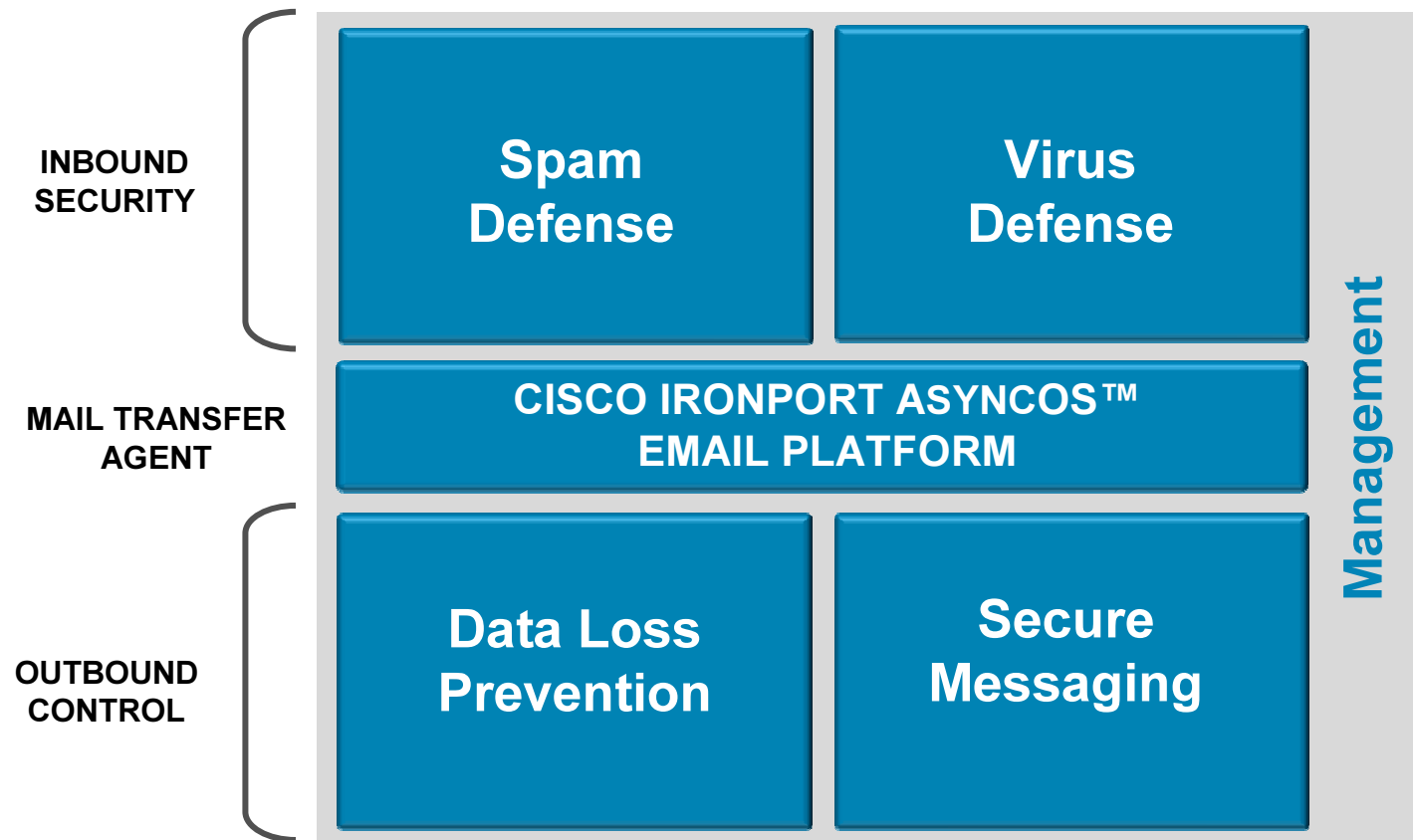
- URL blacklists & whitelists
- HTML Content
- Domain Info
- Known "bad" URLs
- Website history...

## Web Reputation Filters

.....► Reputation Score

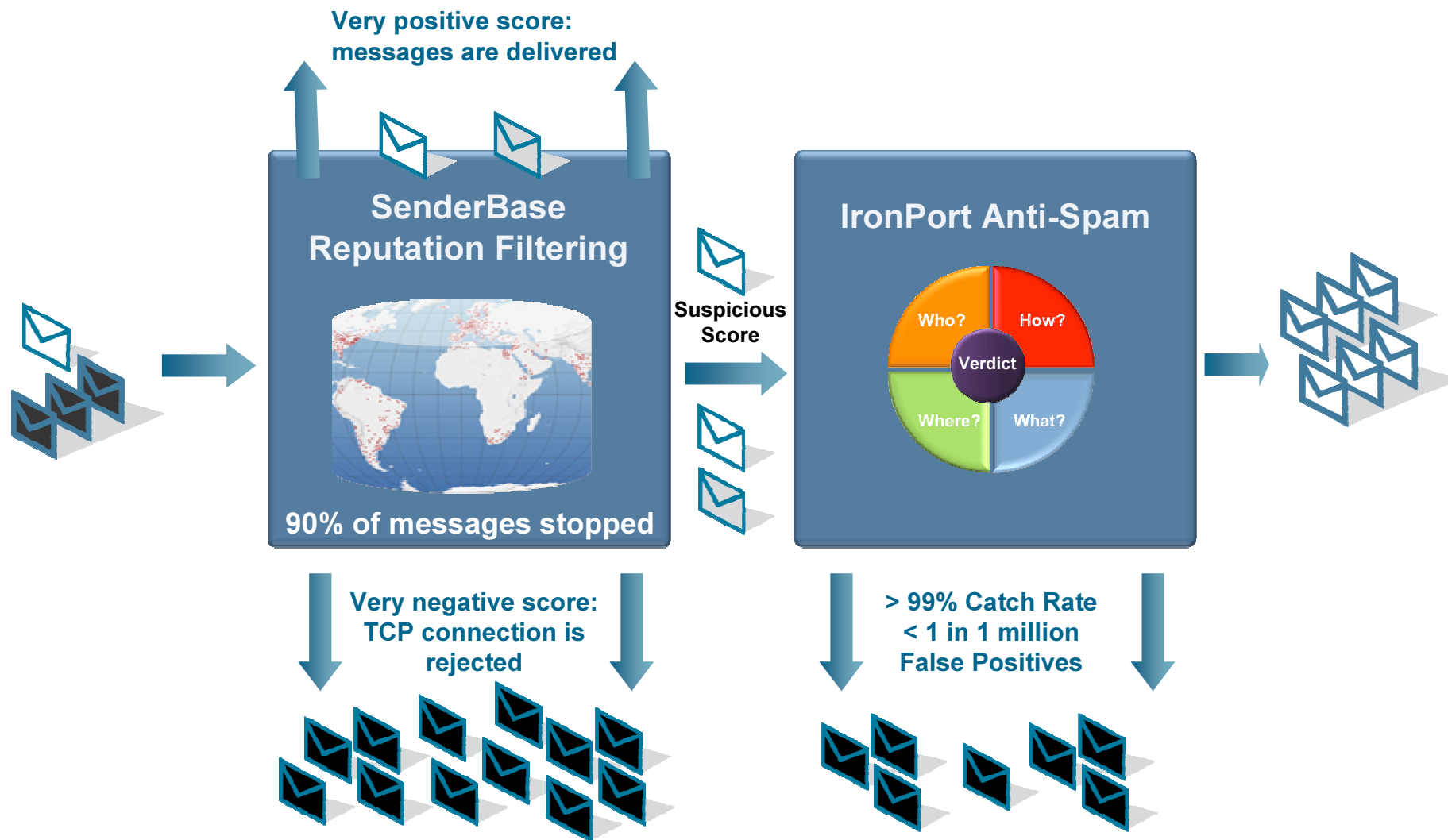
# Email Security Architecture

Cisco IronPort C-Series



# Anti-Spam Defense

## *Multi-layer architecture*





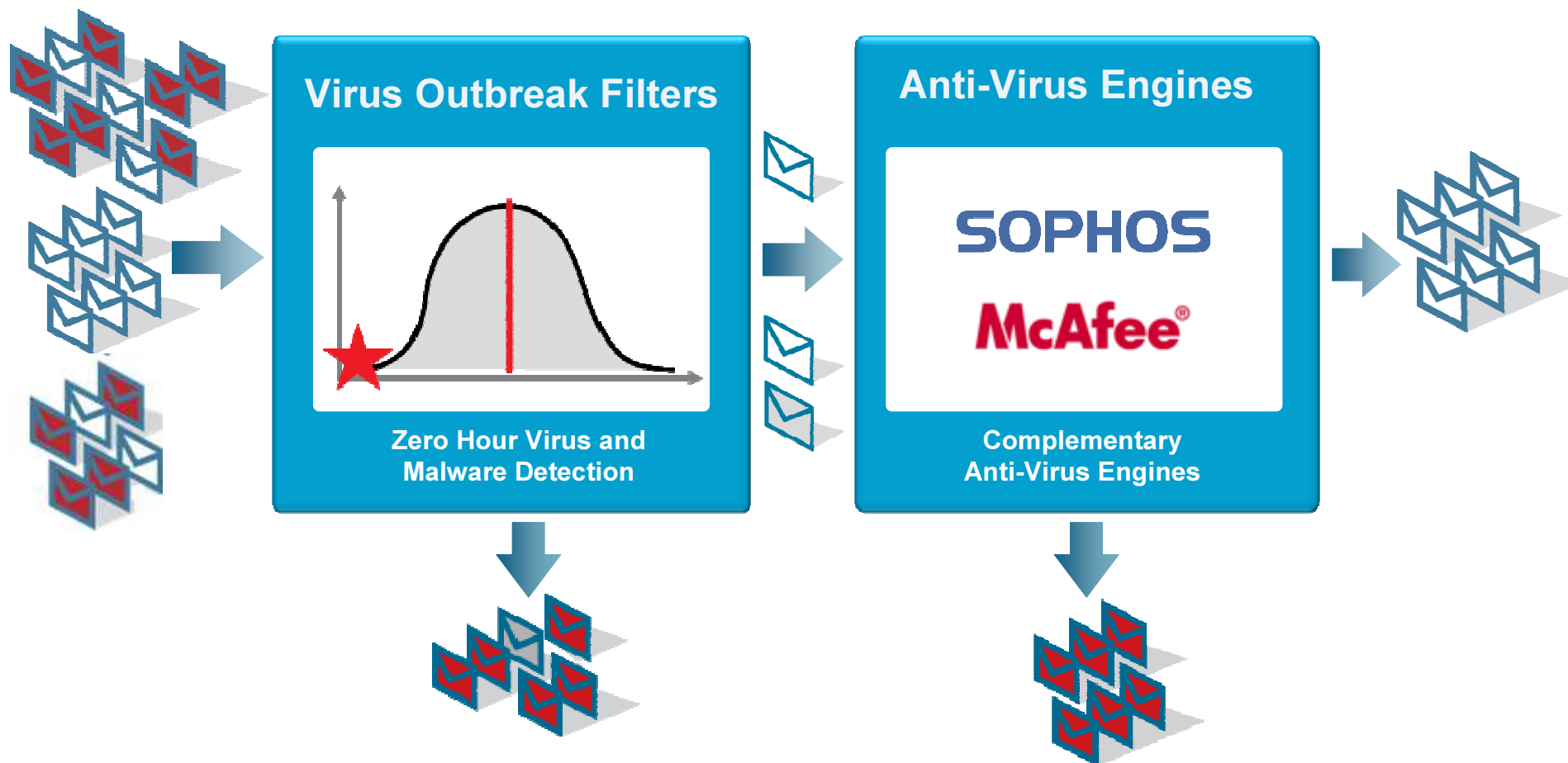
# SenderBase Reputation Filtering

## The Cisco Example

Message Category	%	Messages
<b>Stopped by Reputation Filtering</b>	<b>93.1%</b>	<b>700,876,217</b>
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
<b>Total Threat Messages:</b>	<b>96.8%</b>	<b>728,797,126</b>
Clean Messages	3.2%	24,102,874
<b>Total Attempted Messages:</b>		<b>752,900,000</b>

# Anti-Virus Defense

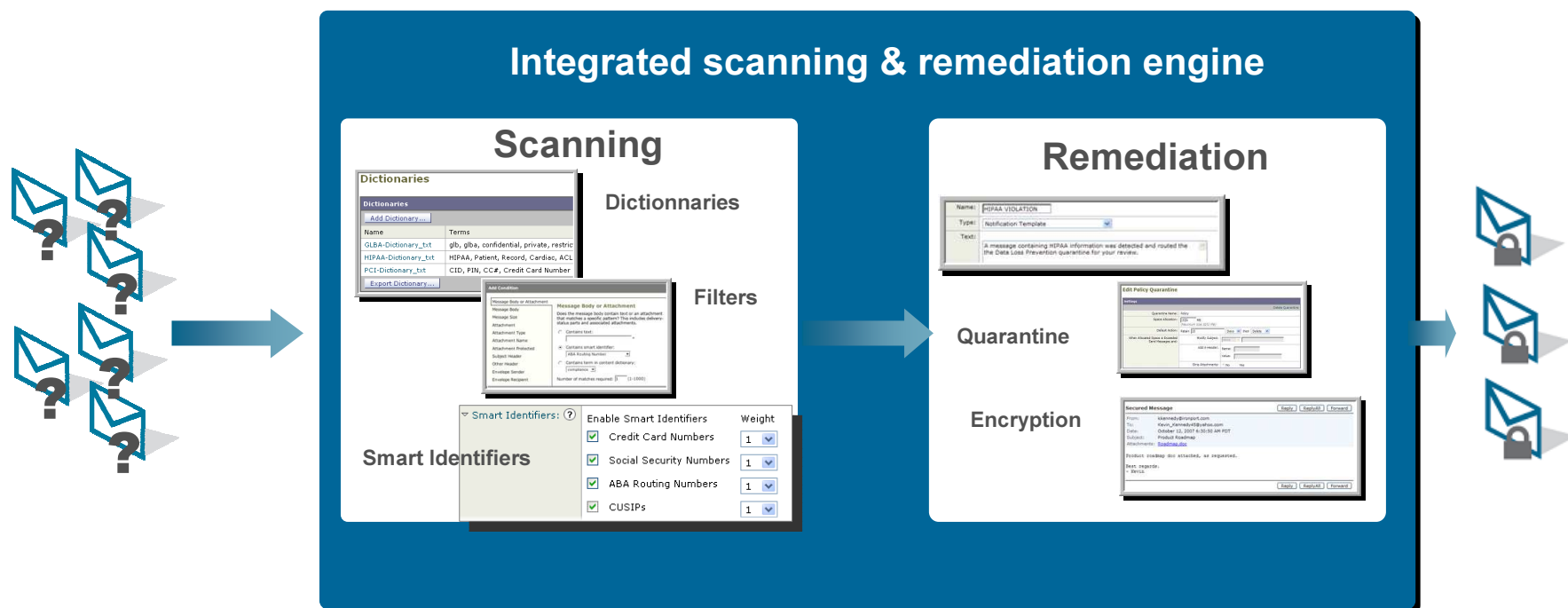
## *Multi-layer architecture*



**Virus Outbreak Filters  
Advantage  
(on 1 year)**

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

# Data Loss Prevention

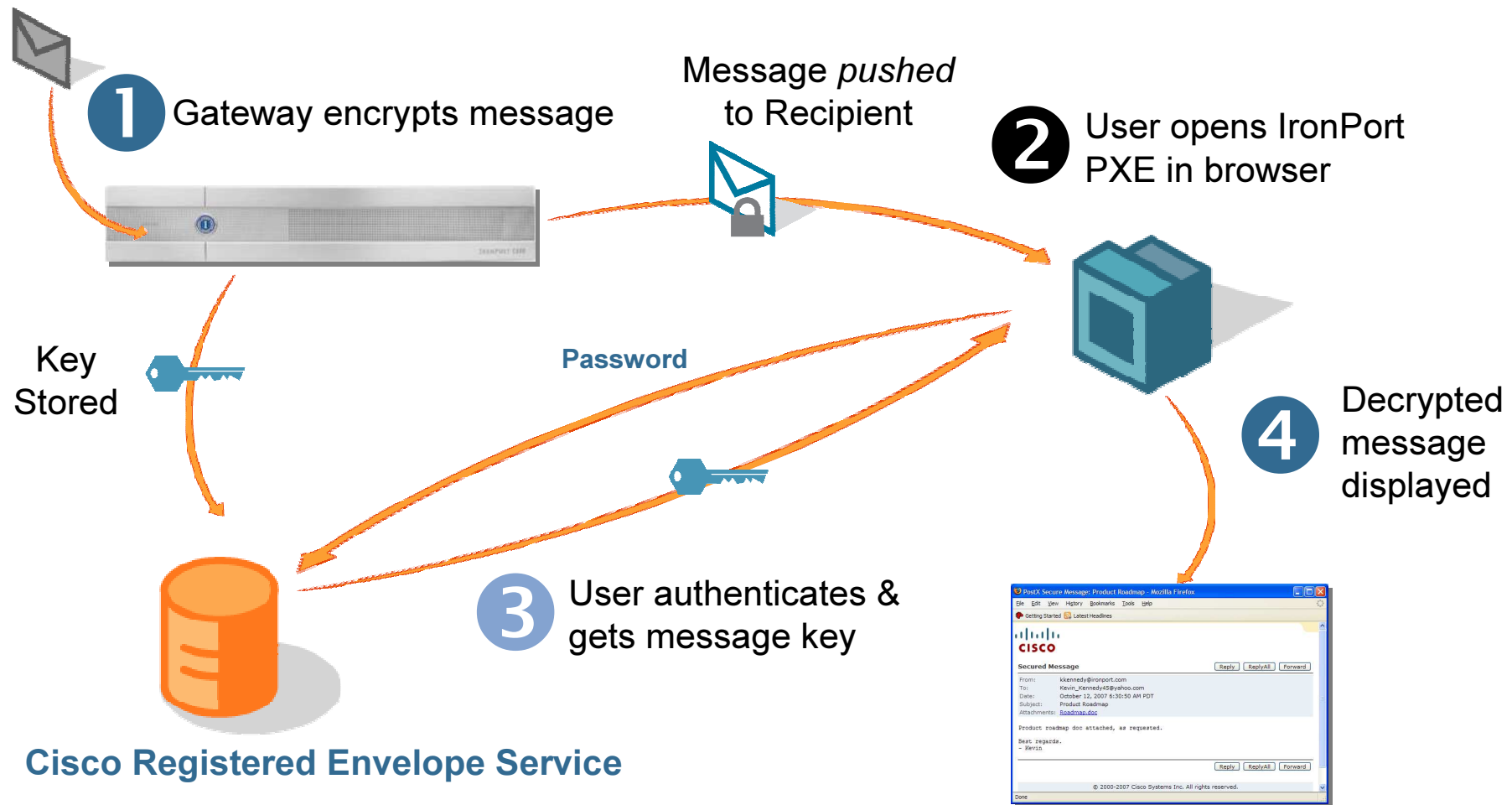


**Scanning** : pre-defined filters (SOX, HIPAA, etc.), compliance dictionaries, automatic tracking of credit card numbers, etc.

**Multiple remediation actions**: quarantine, drop, bounce, BCC, strip content, encrypt

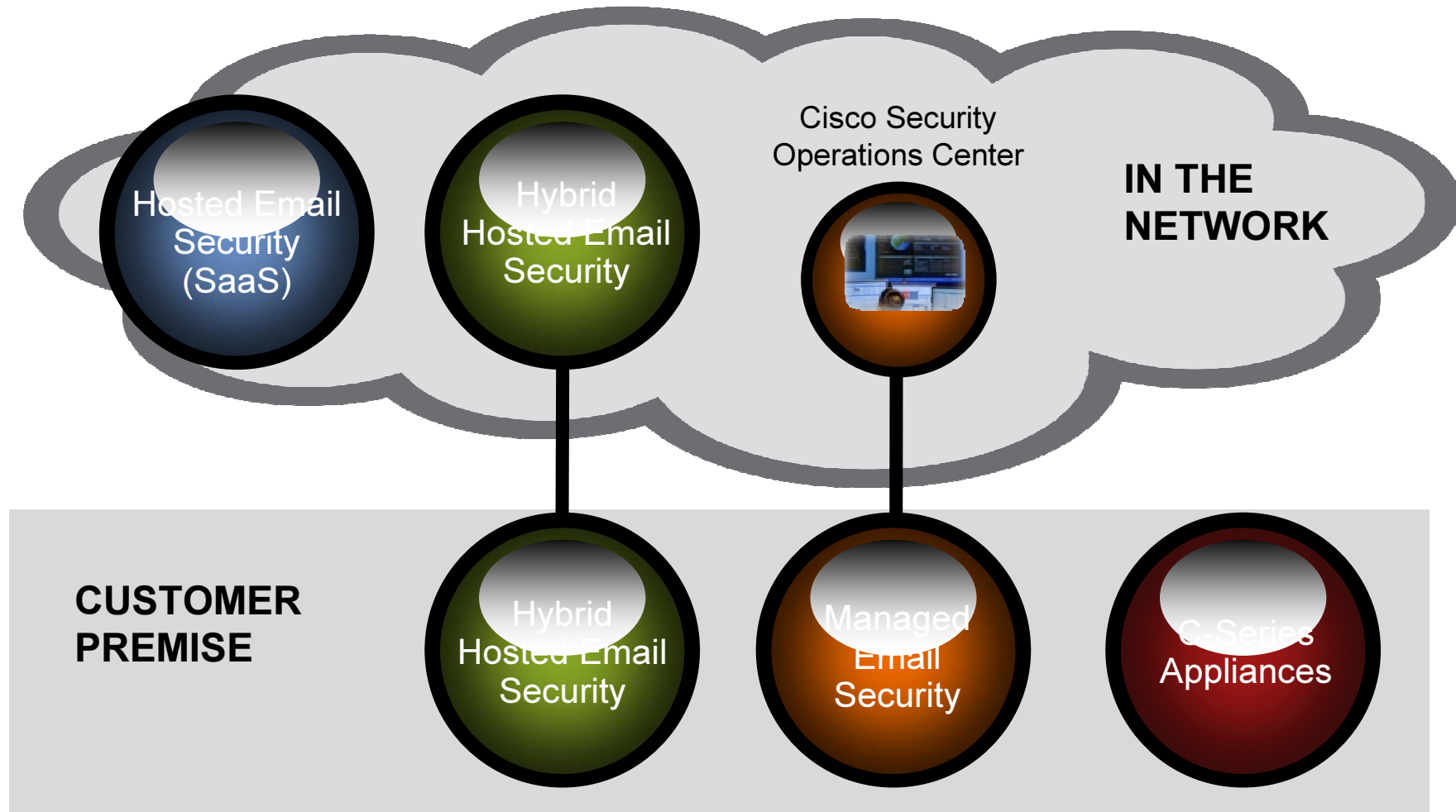
# Cisco IronPort E-Mail Encryption

Easy for the sender...



# Flexible Deployment Options

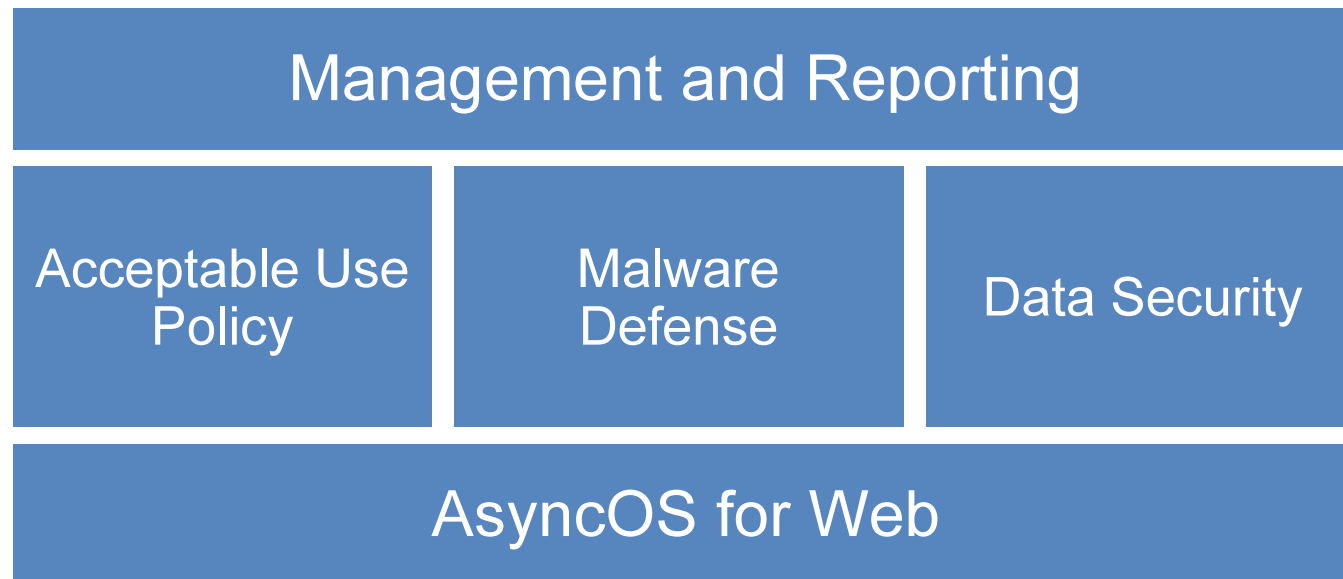
Same Market-Leading Email Security



Common Policy | Centralized Reporting | Consistent Protection

# Cisco IronPort S-Series

## Web Security Architecture



# IronPort URL Filters

## Comprehensive Management and Visibility

- Enterprise-class database
  - 52 categories
  - Over 21 million sites, ~3.5 billion webpages
- 24 x 7 monitoring, regular & automated updates
- Flexible policy management
  - Per user, per group policies
  - Multiple actions, including block, warn and monitor
  - Time-based policies
  - Custom categories and notifications
  - Guest Policies



# Web Application Control

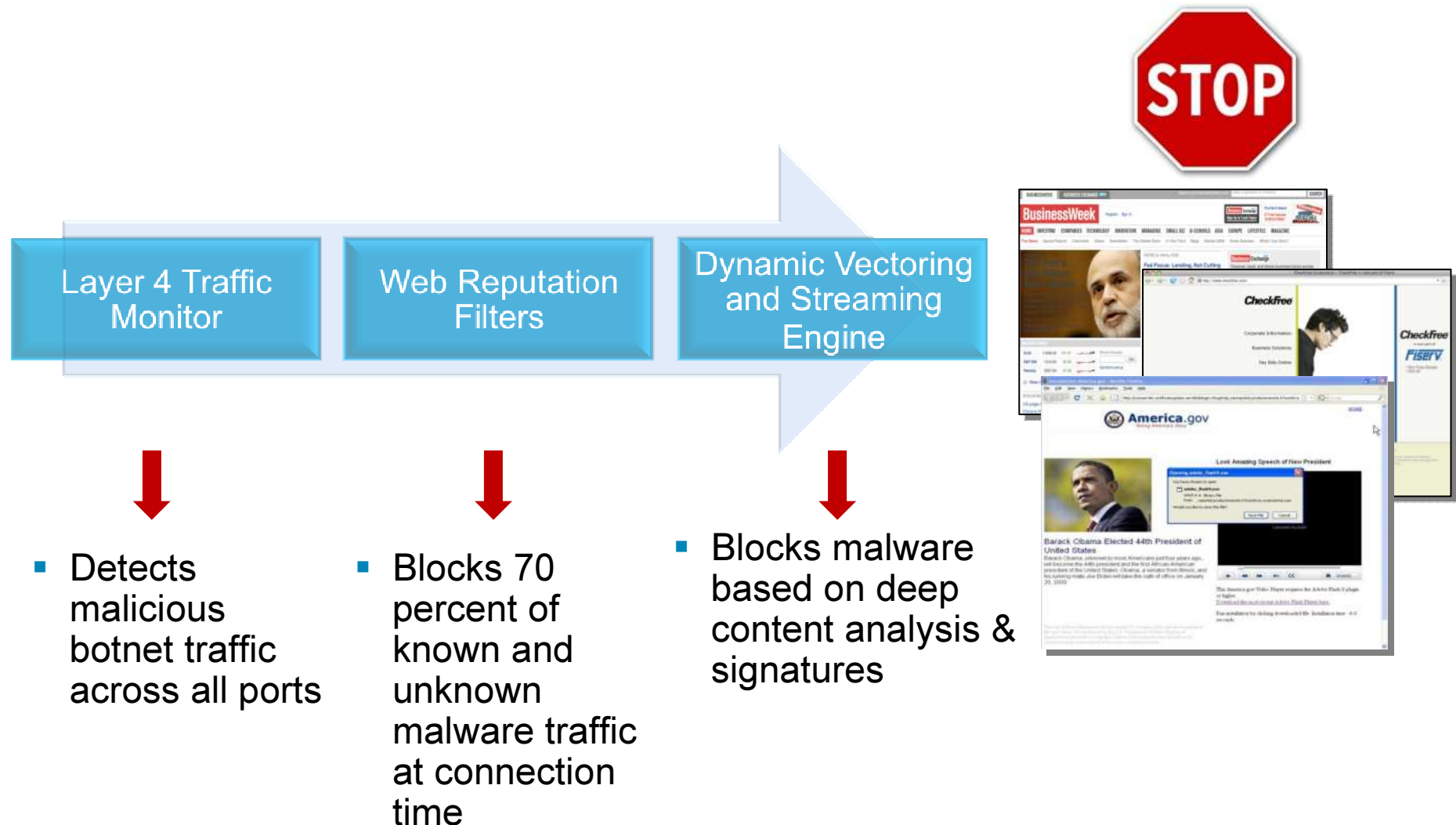
- Native control for HTTP, HTTP(s), FTP applications
- Selective decryption of SSL traffic for security and policy
- Policy enforcement for applications tunneled over HTTP—FTP, IM, video
- Web Objects filtering (by size or type)



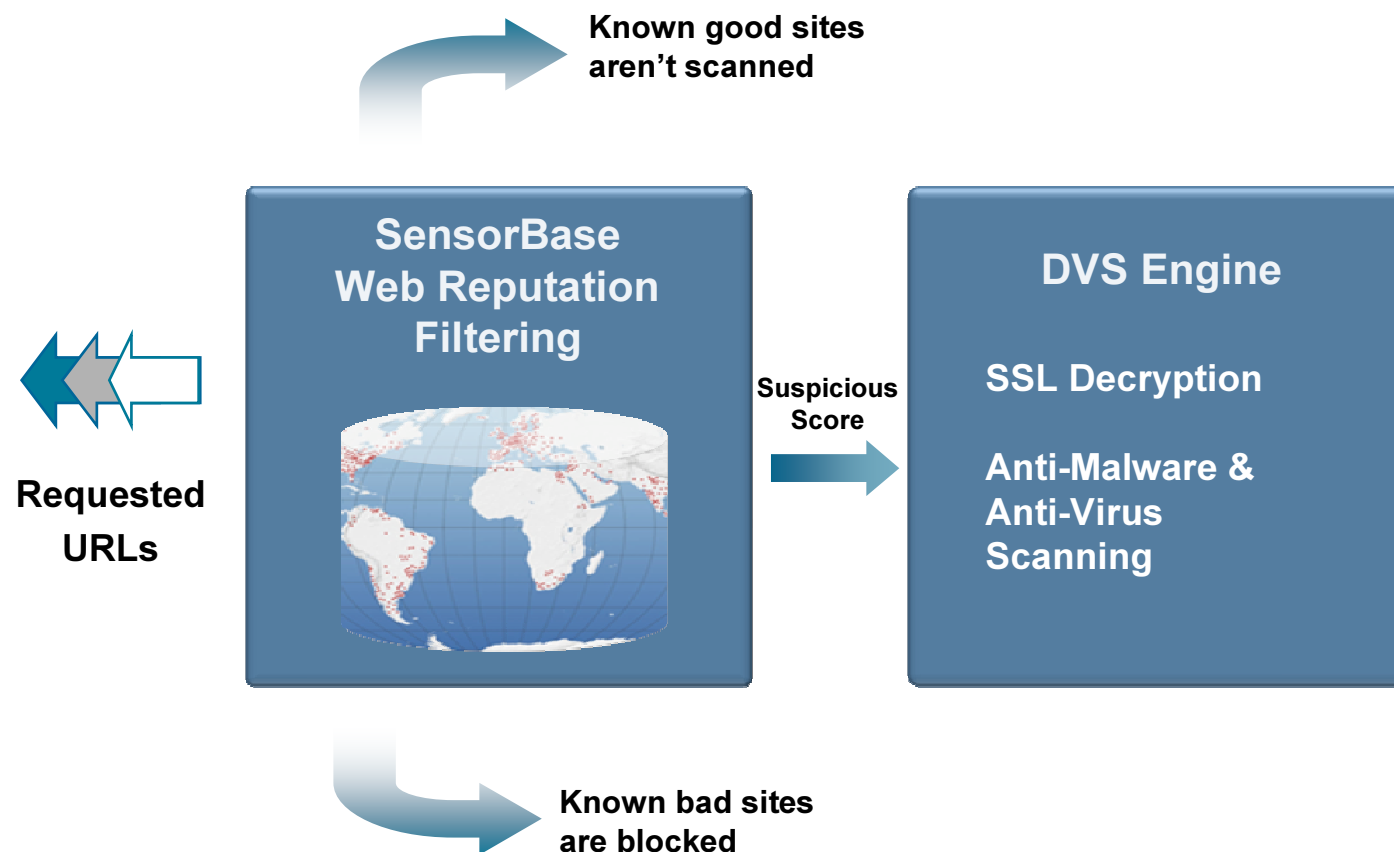


# Multi-Layered Malware Defense

## Protection Against Today's Threats



# Web Reputation Filtering

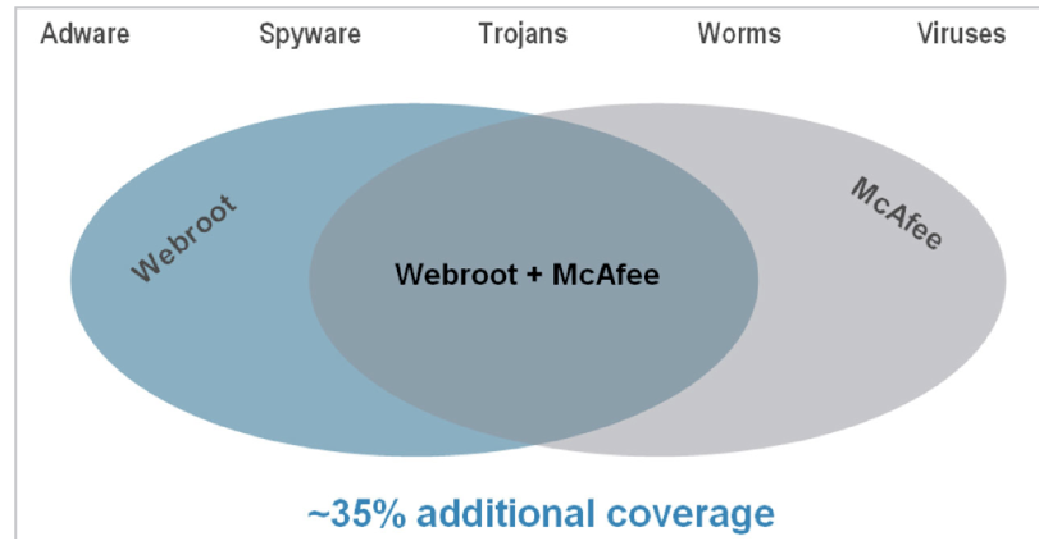


# Cisco IronPort DVS Engine

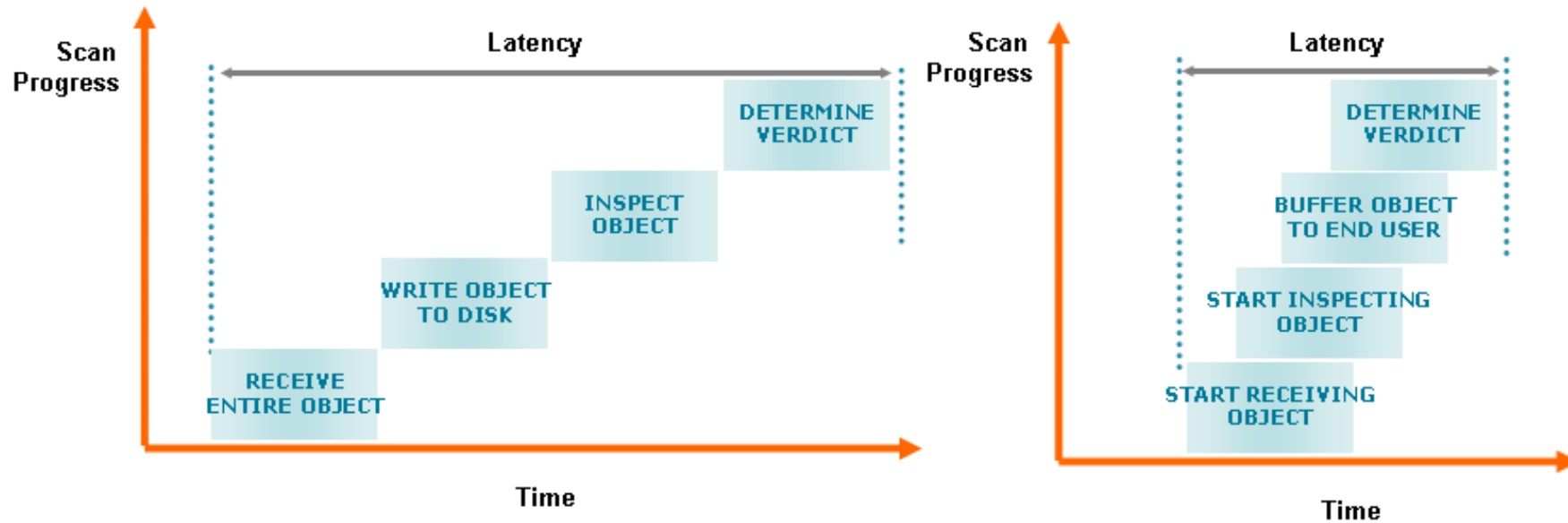
## Dynamic Vectoring and Streaming



- Decrypt and scan SSL traffic
  - Selectively, based on category and reputation
- Multiple integrated verdict engines
  - McAfee and Webroot
- Accelerated signature scanning
  - Parallel scans
  - Stream scanning



# Stream scanning



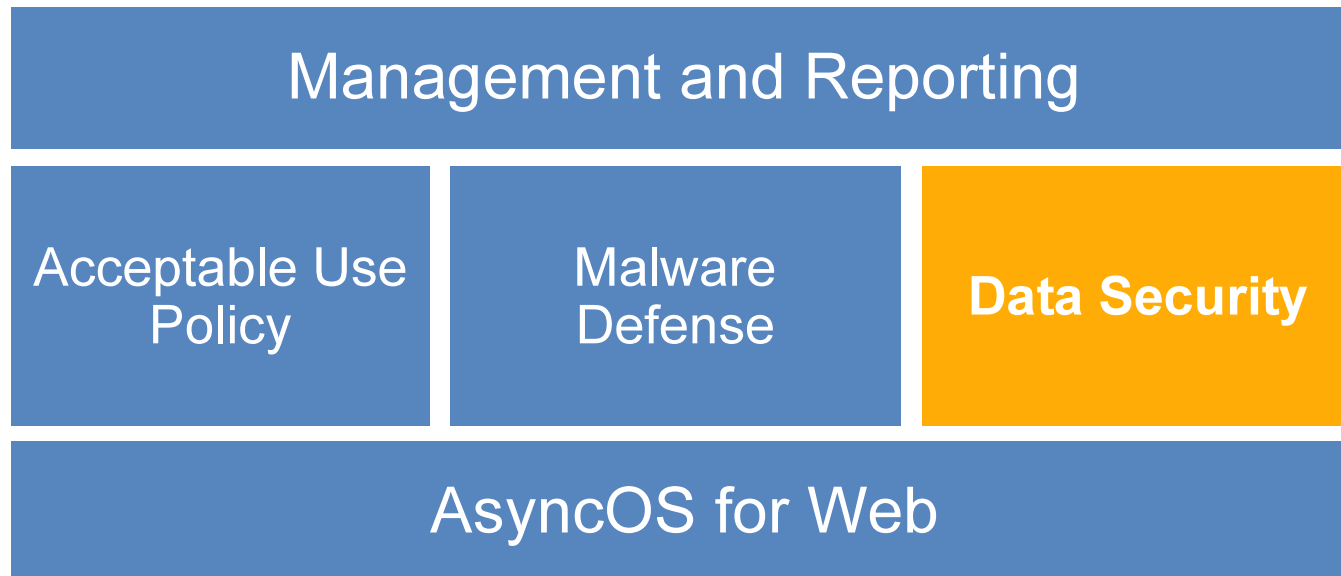
---

« Given the real-time nature of HTTP (...) & HTTPS protocols and their data streams, more sophisticated real-time scanning capabilities are needed to ensure that traffic within these Web-based paths remain free from successful attacks through these vectors » IDC

---

# Complete Data Security




Simplicity and Choice



- Simple on-box data security
- Advanced off-box data security

# Common Sense Policies

## Simple Approach for Avoiding Web Data Breaches

<b>Who?</b>	John Smith, Finance	John Smith, Finance	Jane Doe, Sales
<b>What?</b>	FiscalPlan.xls	FiscalPlan.xls	CustomerList.doc
<b>Where?</b>	Webmail.com	Taxfirm.com	Personal-site.com, -9 Reputation score
<b>How?</b>	HTTPS (Encrypted)	HTTPS (Encrypted)	FTP
<b>Verdict</b>			



95% of companies  
who try Cisco IronPort  
become customers.

*Contact:*

[scommero@cisco.com](mailto:scommero@cisco.com)

