



Cisco IronPort “for beginners”



Sébastien Commérot

Manager, Security Marketing
Emerging Markets

Agenda

- Cisco IronPort
- The latest Internet Threats
- E-Mail Security
- Web Security Solutions
- Why push IronPort?
- Questions & answers



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

Cisco Ironport CEE & Russia Sales Team

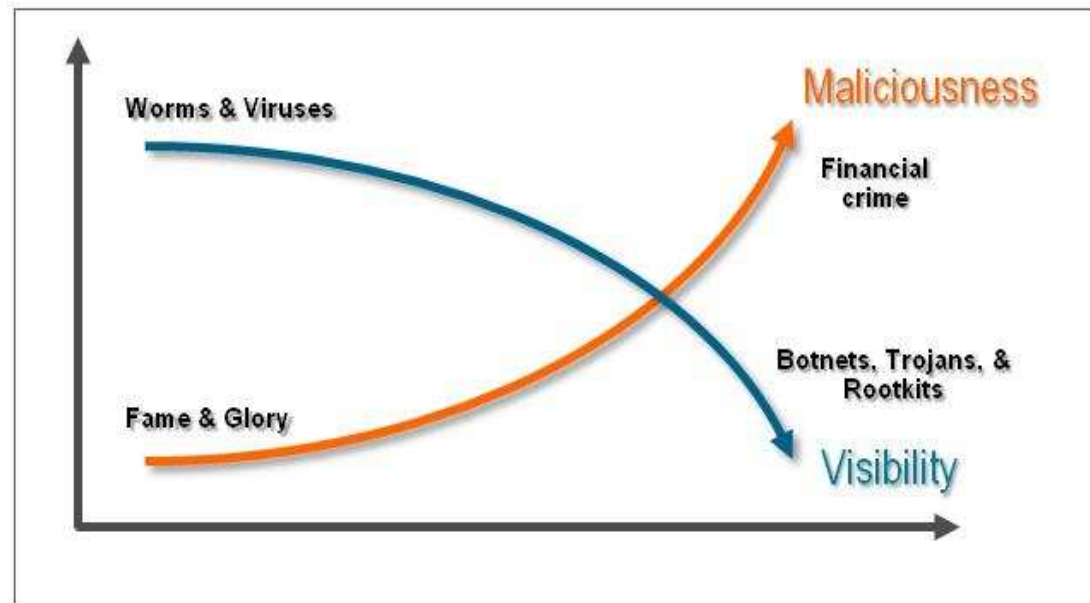


Internet Threats

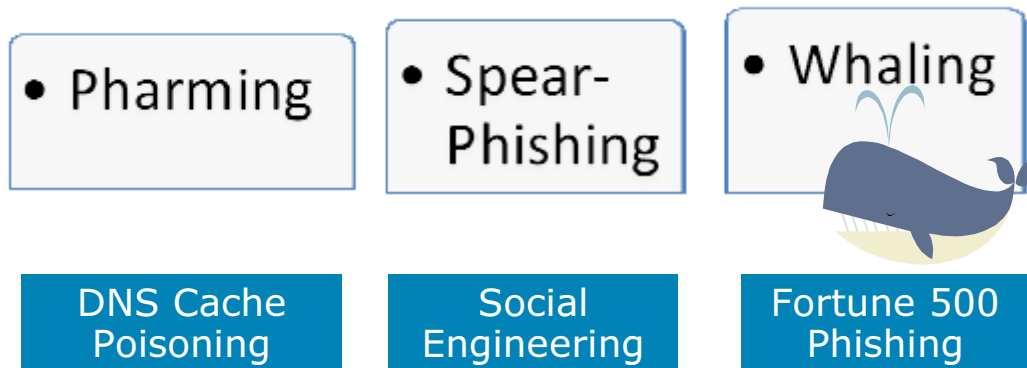


The new landscape

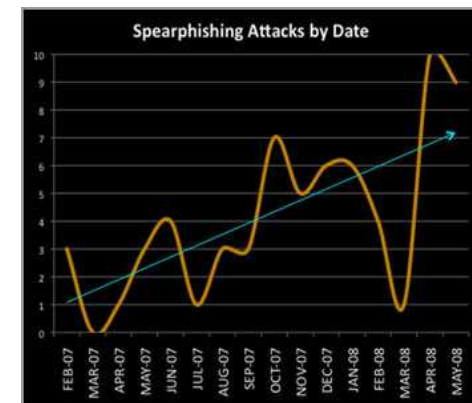
New motivations generate new threats



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~~tion of 1 letter
 - Name variant
(micr~~p~~soft)
 - Orthogra~~f~~ic Mistake
- Creation of a similar site, downloading malware on computers

www.google.com

www.mcrosoft.com

www.hotmial.com

www.wikipefia.org

Zombies are changing

The Storm network

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

1000 contaminated PCs rented \$220 in Germany

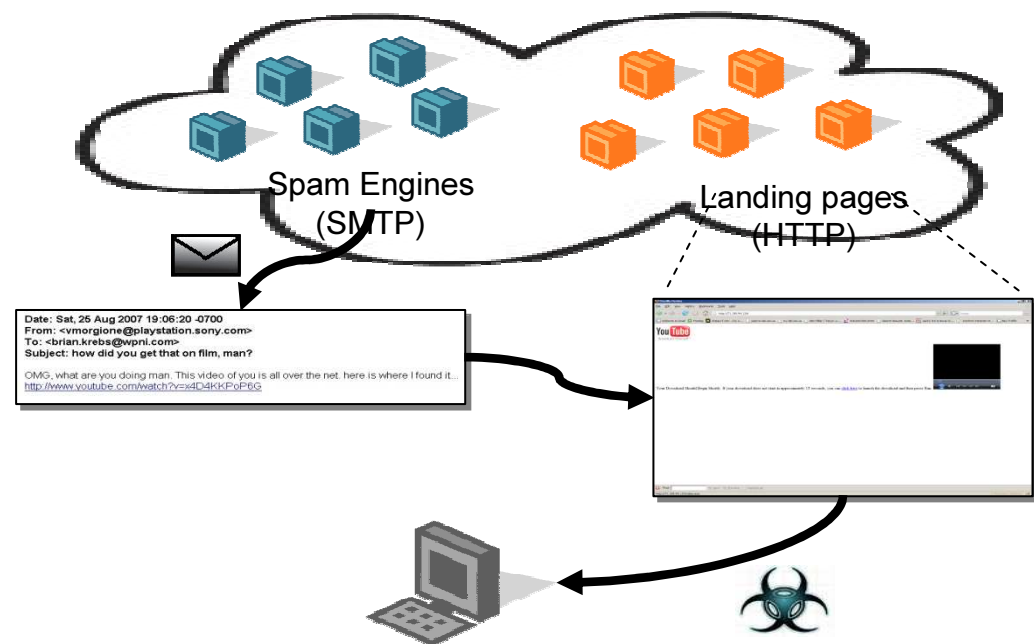
1000 contaminated PC in the USA \$110

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

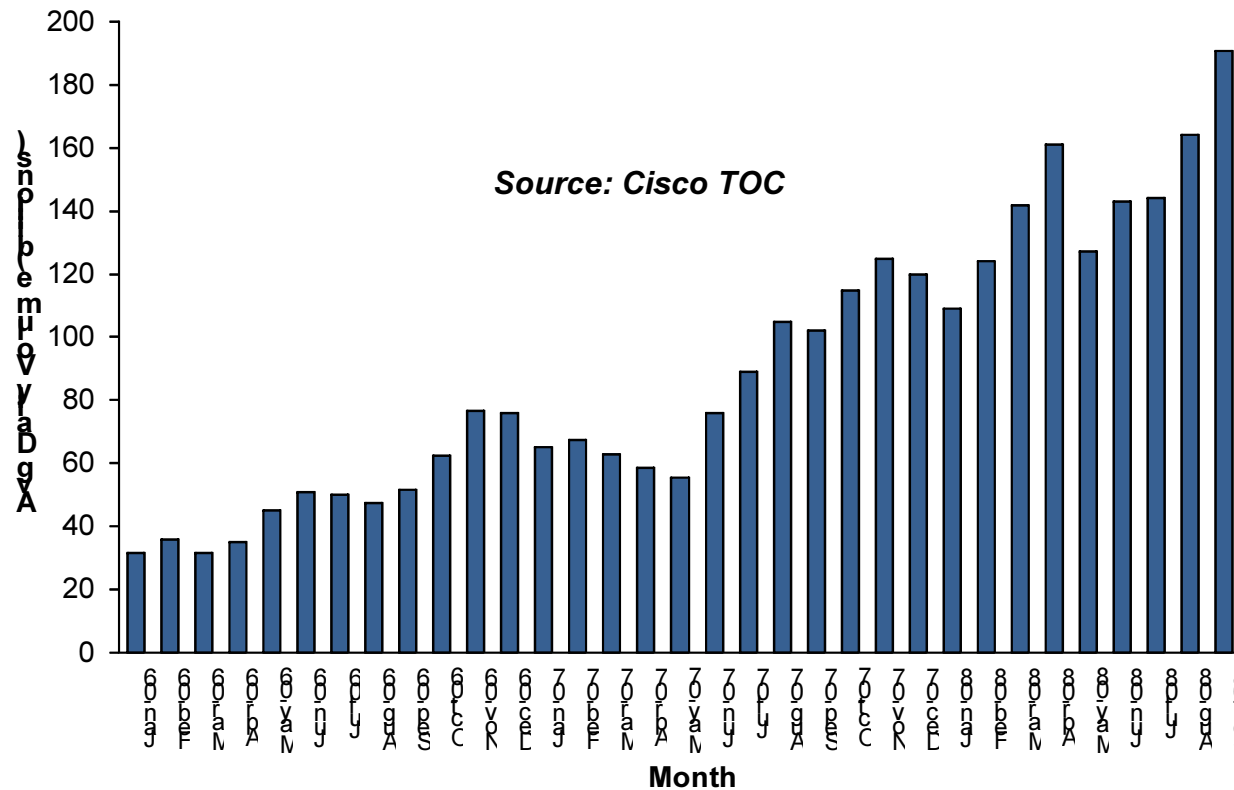


2007 : Storm is born

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

Spam keeps growing...

And will keep on growing!

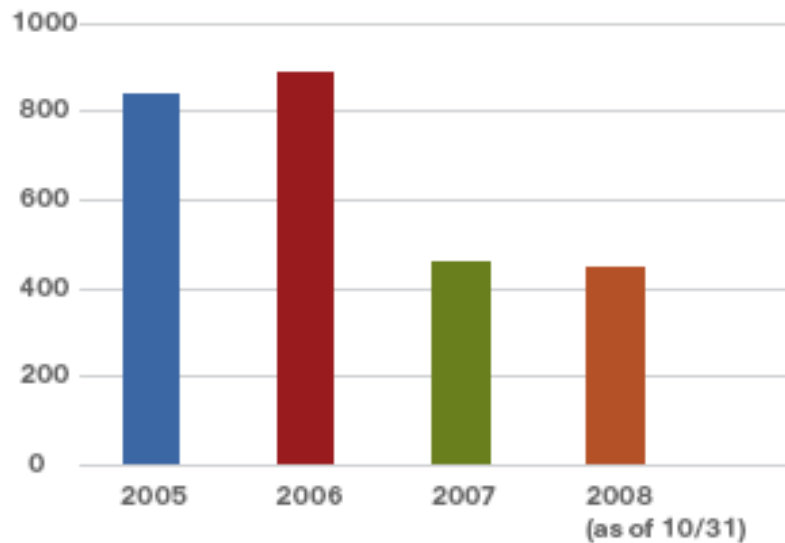


x6 in last 3 years!

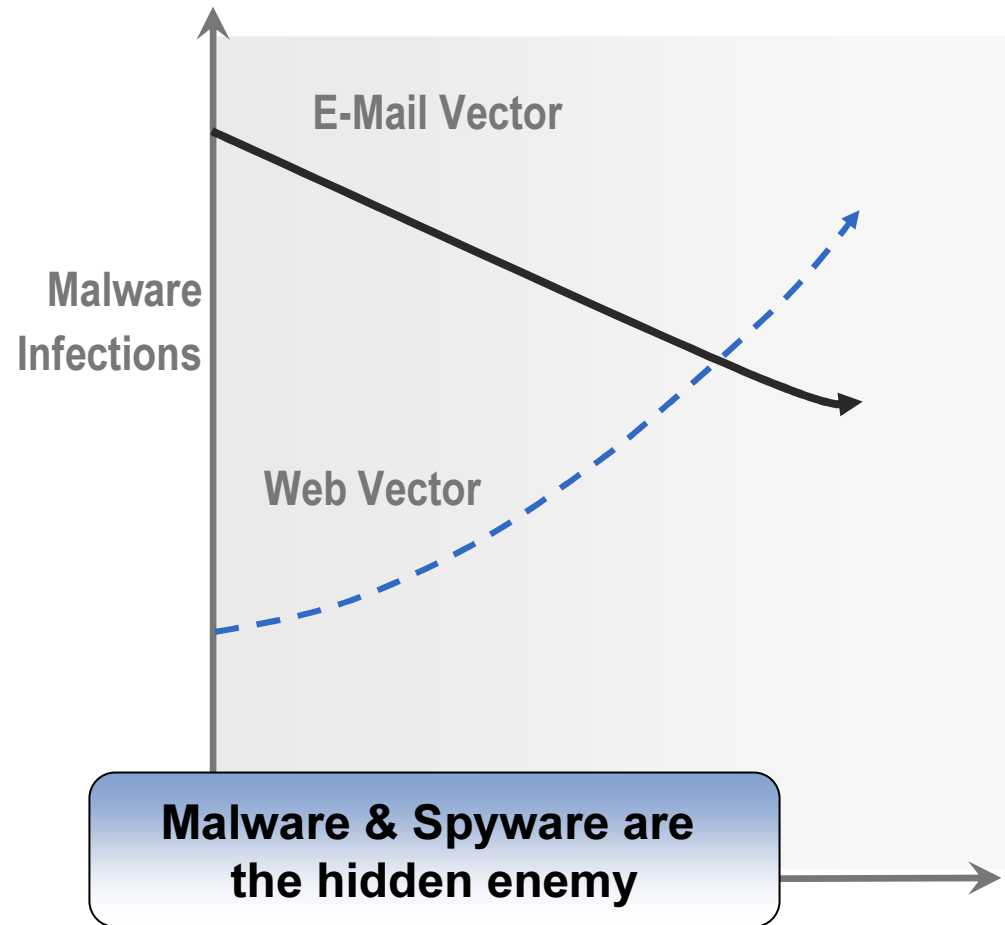
x2 in next 4 years!

	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%

Threat vectors are changing

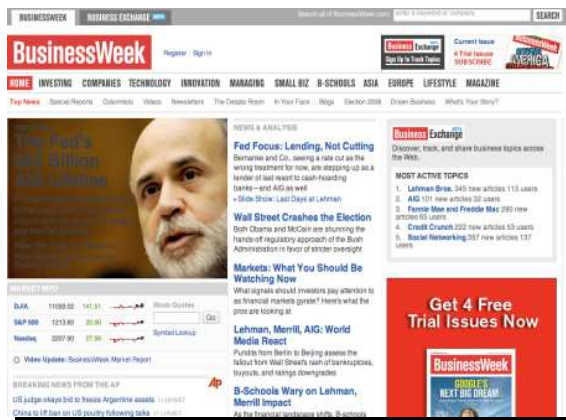


Volume of Malware Successfully Propagated via Email Attachments



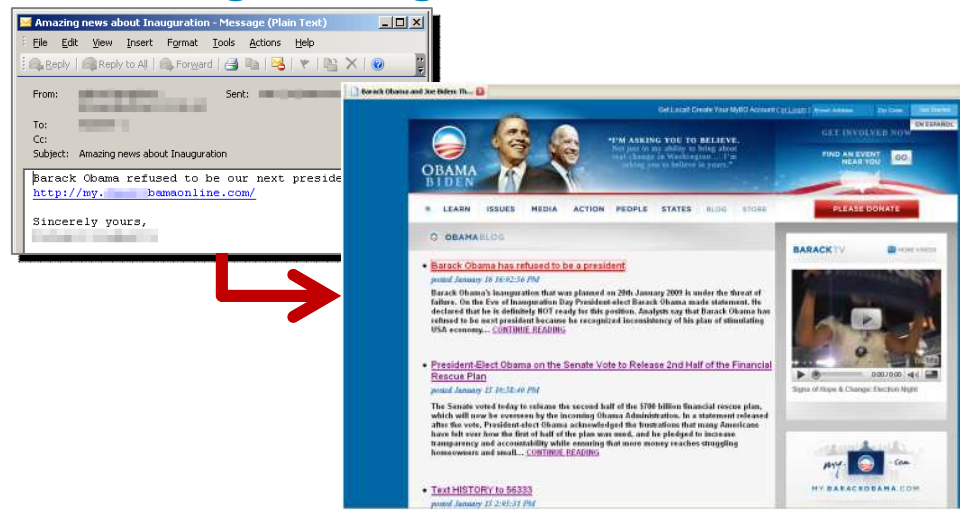
Two trendy techniques to spread threats

Exploited Websites



- Simply visiting a legitimate site can infect a user
- iFrame attacks convert websites in malware distribution platforms
- Accounts for 87 percent of all web-based threats today*

Social Engineering



- Current content with broad public interest
- Email sent to users with a link to a malicious web-site
- Web-site is downloading a malware on the user's computer

* Source: Cisco Threat Operations Center

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*

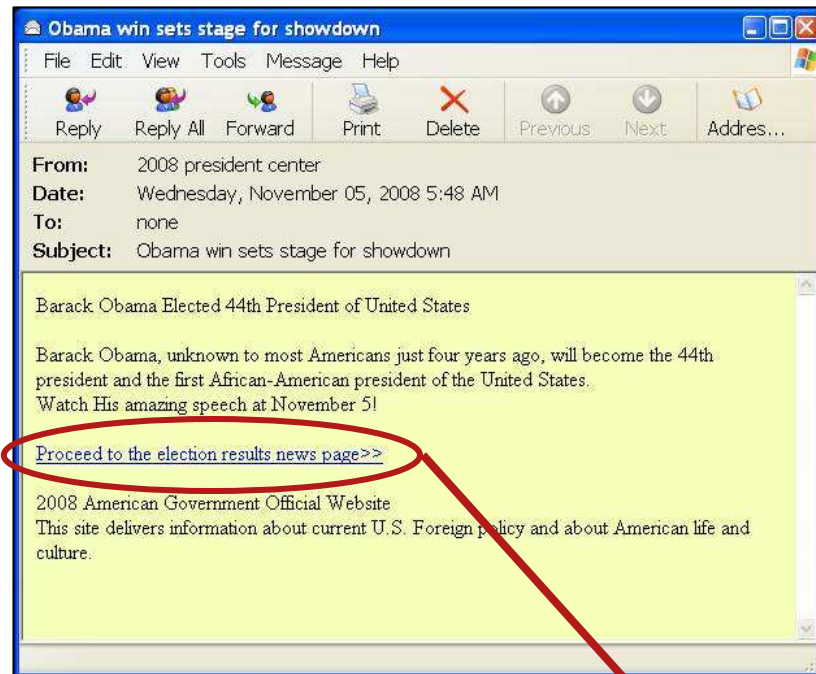
Exploited Website Example

- 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)



Social Engineering Example

Malware campaign using Obama's victory



- Users receive an email inviting them to watch President-elect Barack Obama's victory speech
- Links users to a government themed botsite
- Subject Line Examples:
 - Election Results Winner
 - The New President's Cabinet?

<http://slapiservlet.encrypted.viewcontent.XXXXXXXXXXXXXXXXXX.wconlinenrue.com/president.htm?/slapiservlet/slapiservlet/OSL.htm?LOGIN=BfQd3Zno5H&VERIFY=0AHBgl9ixN7rvXm>

<http://portalserver.viewcontent.memberverify.EwTLOC5Rc.XXXXXXXXXXXXXXXXXX.bfiinwach.com/president.htm?/verifyonenet/certificateupdate/OSL.htm?LOGIN=ZeuroEwTLO&VERIFY=C5Rcwjj7qjsuVeb>

<http://actionvalidate.linkbrowse.servletdologin.QdfFSKkiw.XXXXXXXXXXXXXXXXXX/president.htm?/exacttrget/memberverify/OSL.htm?LOGIN=Tch0JQdfFS&VERIFY=KkiwFDDIWZhVvVNJ>

Malicious URLs

Social Engineering Example

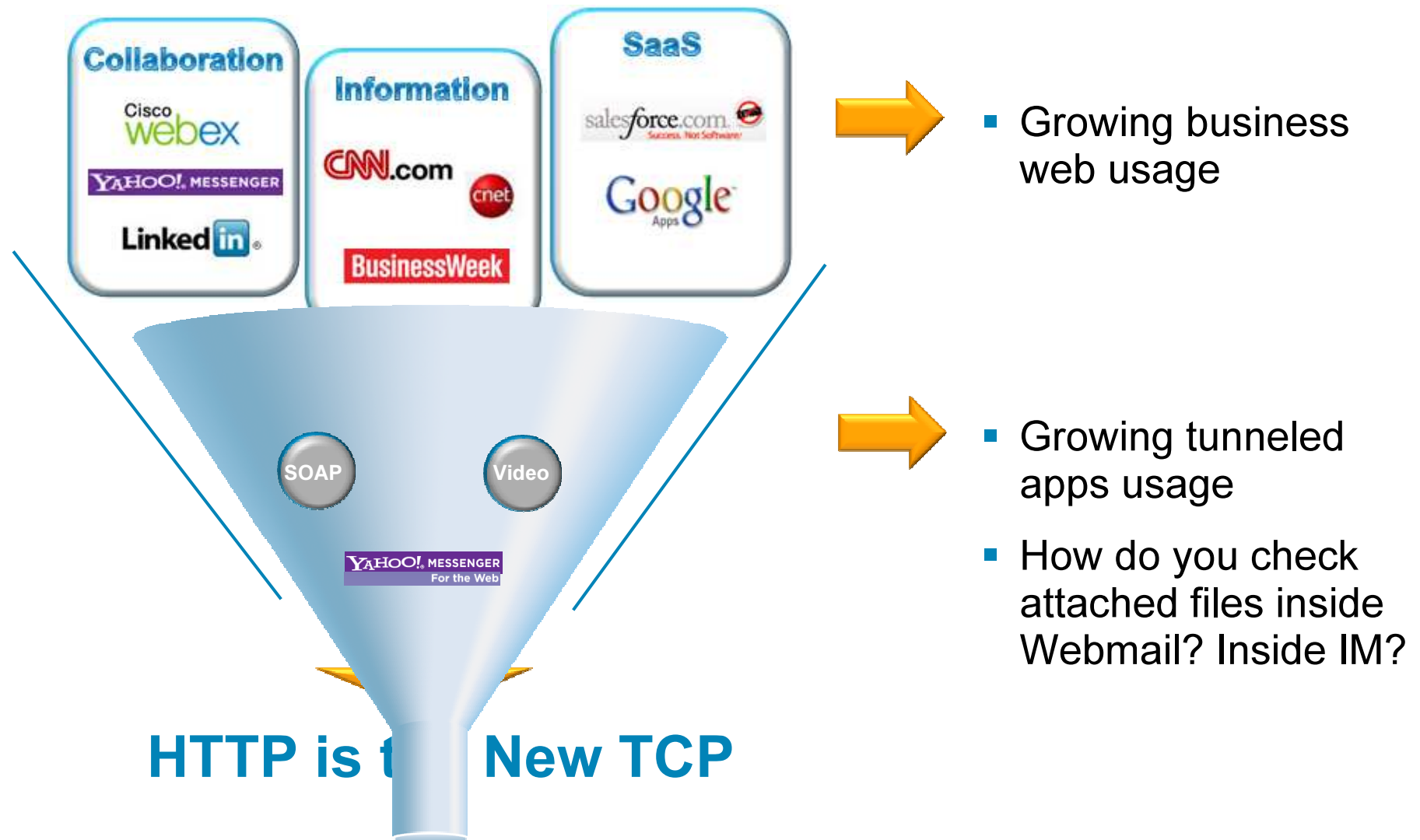
Malware campaign using Obama's victory



- Users prompted to install an Adobe Flash Player update, which is actually **data-stealing malware**
- Steals **screen shots, passwords** and sends to a web server located in Kiev, Ukraine
- Not stopped by traditional URL filtering (Category : government)

Increasing Enterprise Web Traffic

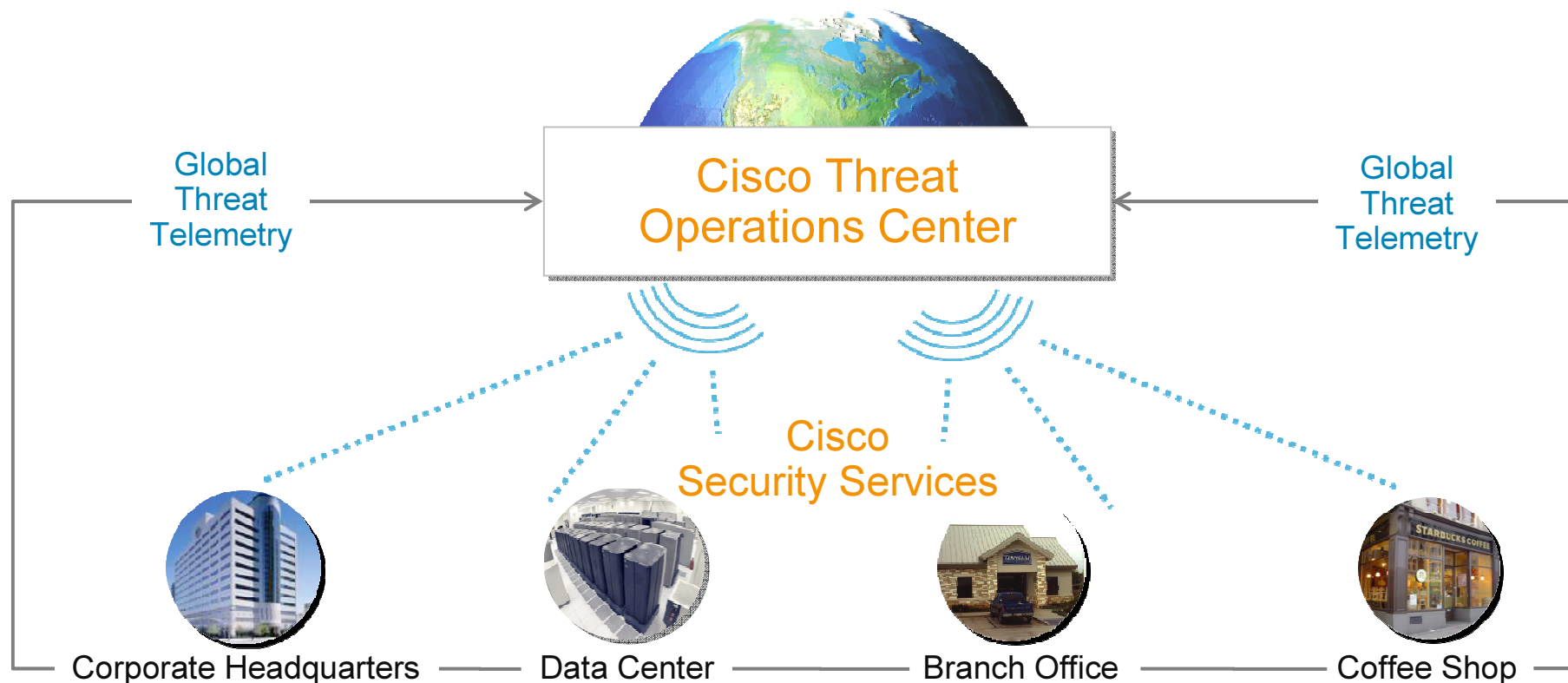
Port 80 & 443 usage has changed



Cisco Security : Securing the Borderless Networks



Cisco Security Intelligence Operations



Security in every location
Security in every form factor



Appliance



Security Module

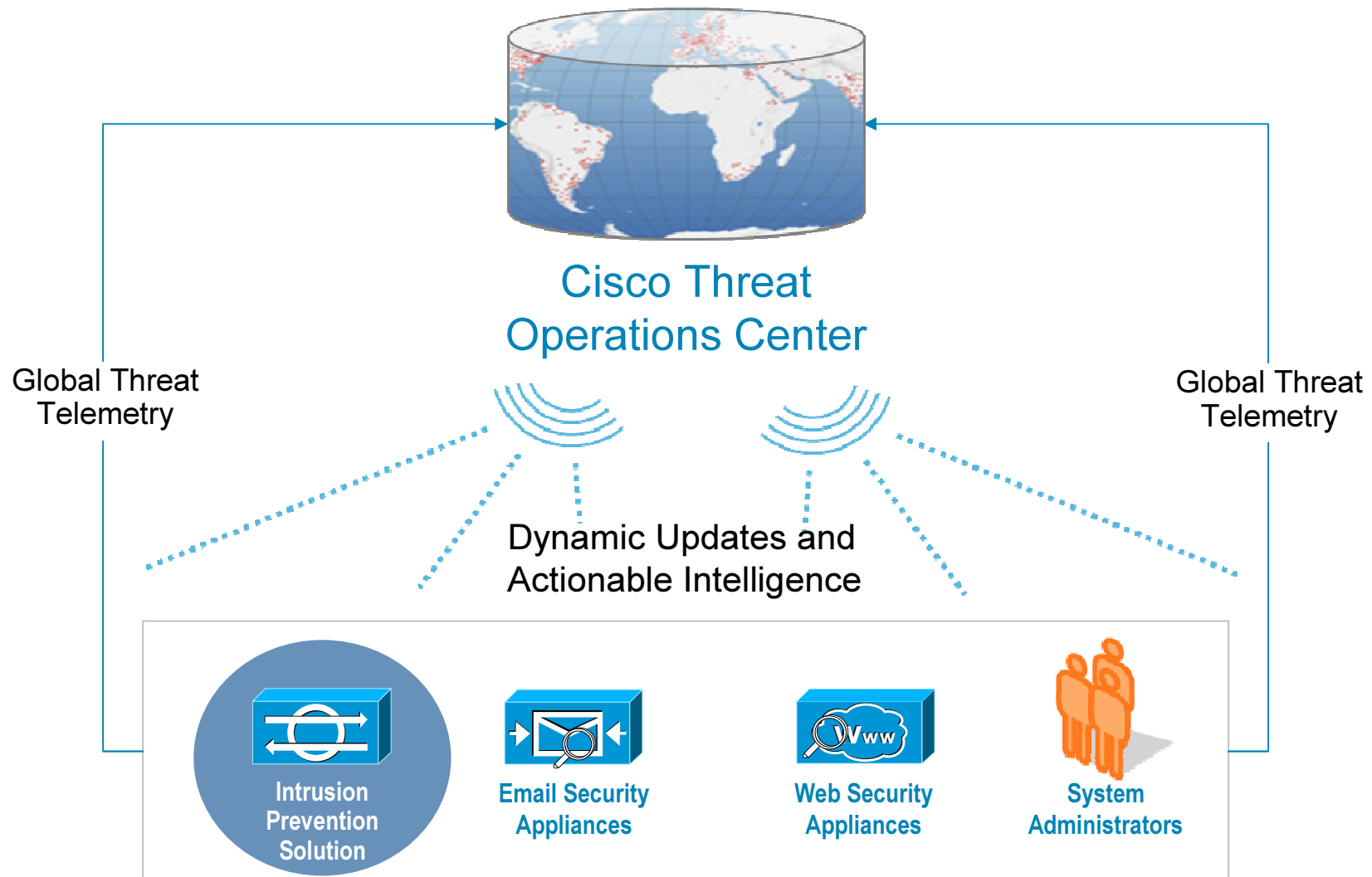


Hybrid Hosted



Security Software

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

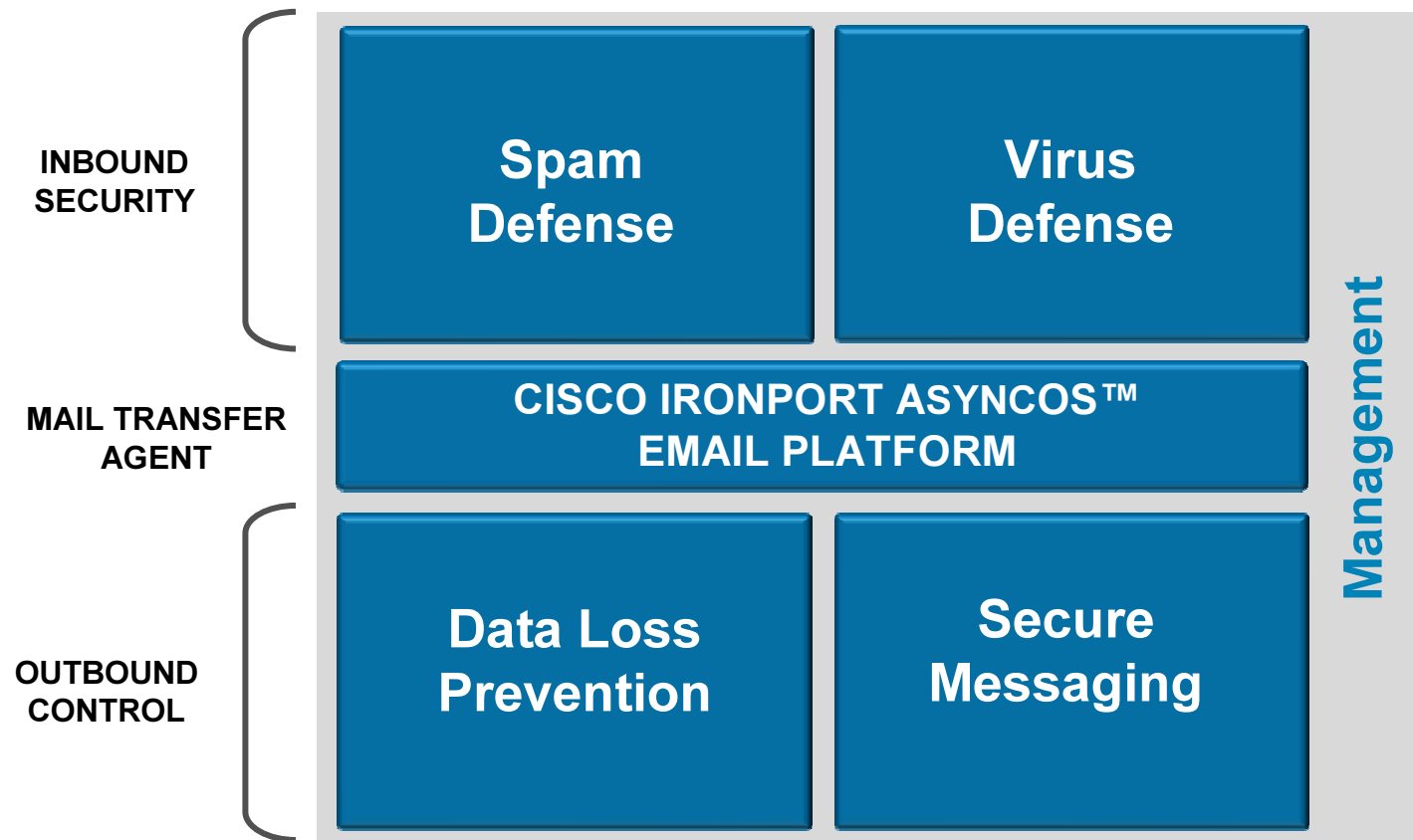
.....► **Reputation Score**

Email Security



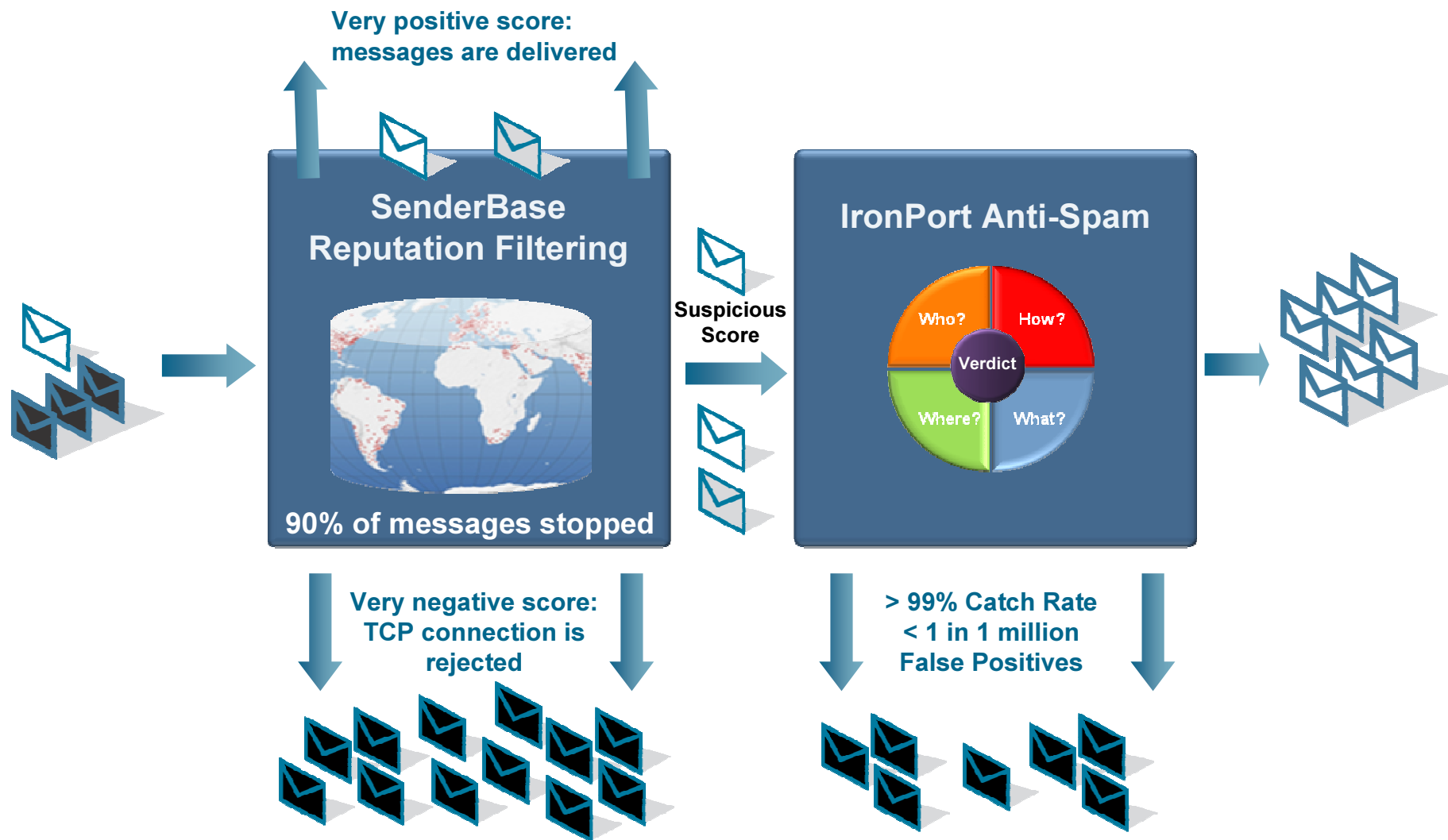
Email Security Architecture

Cisco IronPort C-Series



Anti-Spam Defense

Multi-layer architecture



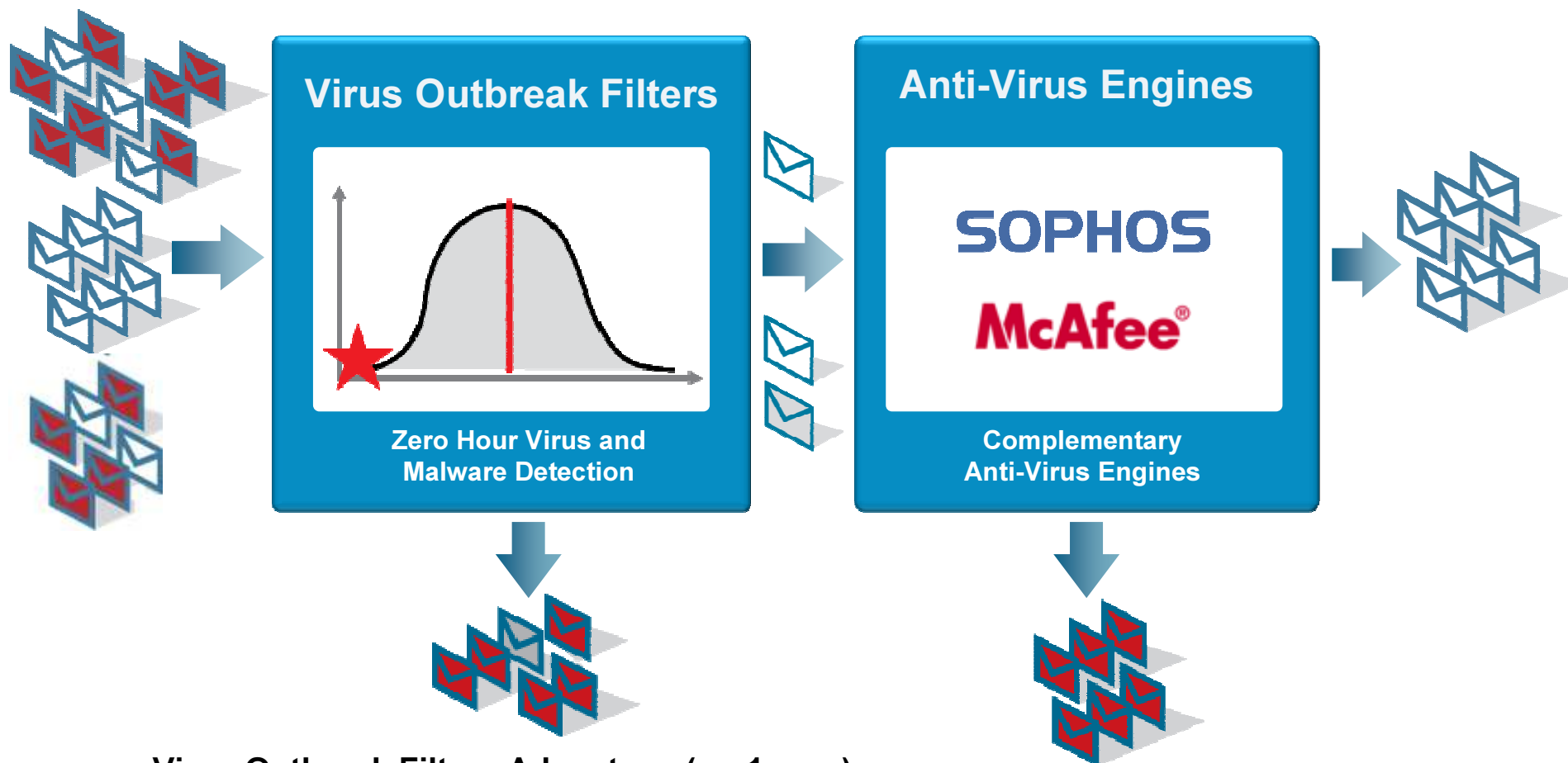
SenderBase Reputation Filtering

The Cisco Example

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

Anti-Virus Defense

Multi-layer architecture



Virus Outbreak Filters Advantage (on 1 year)

Average lead time.....over 13 hours

Outbreaks blocked291 outbreaks

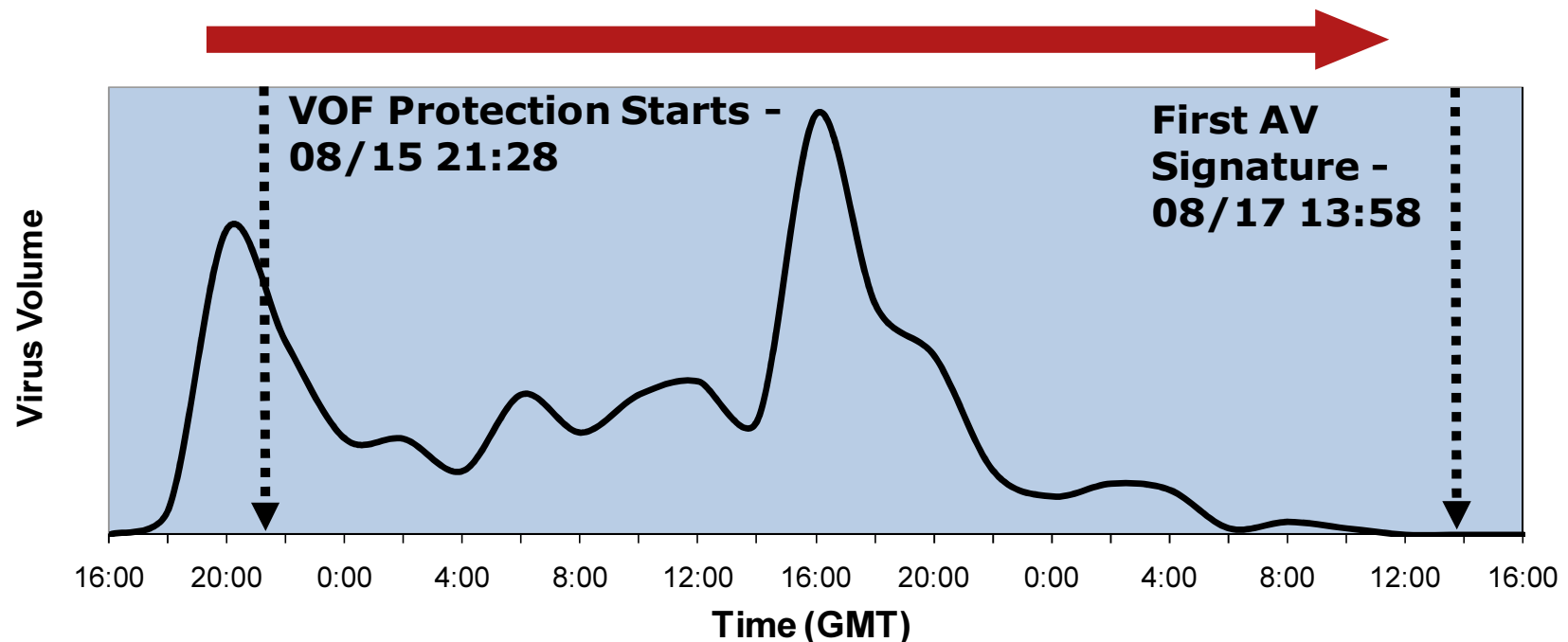
Total incremental protection..... over 157 days

Virus Outbreak Filters

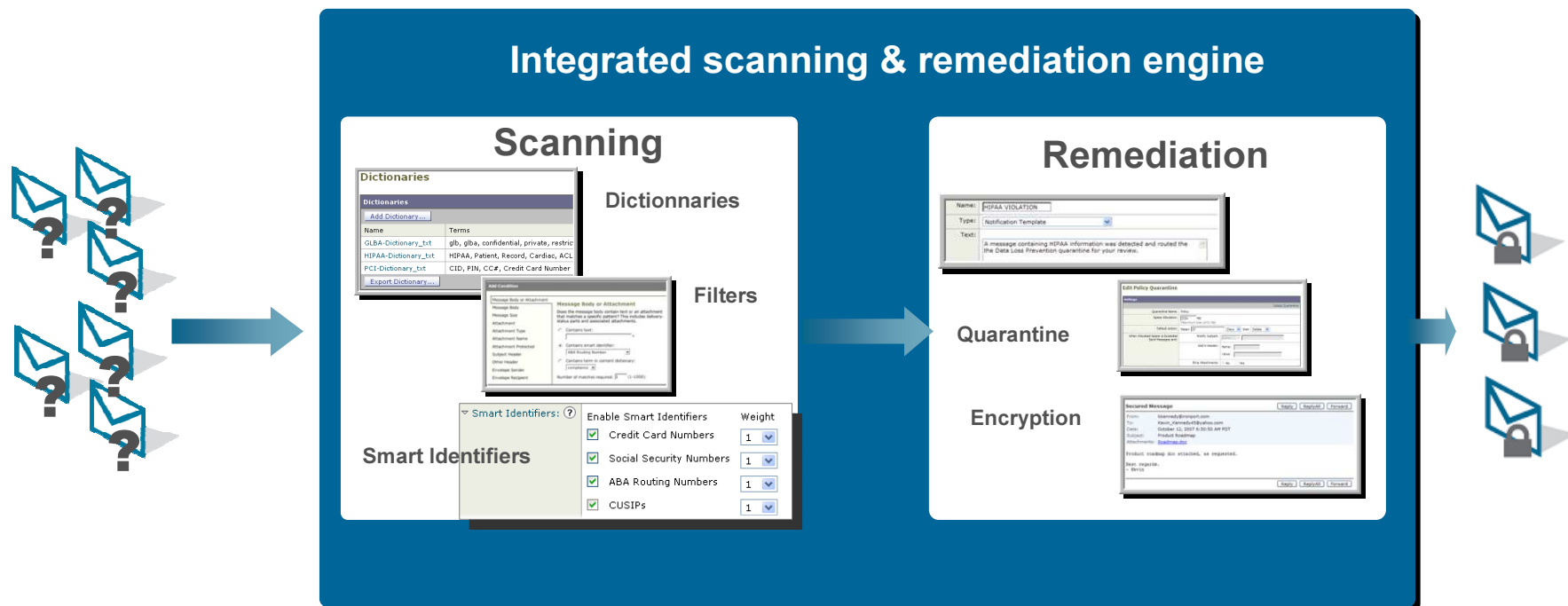
Targeted FedEx Delivery Trojan (August 15, 2008)

- Email subject: "FedEx Postal Service [tracking#]"
- Numerous mutations, similar to UPS attacks in previous month
- Attachment installed Trojan letting remote hackers control infected PC

Protection Time: 40 hours 29 minutes



Data Loss Prevention

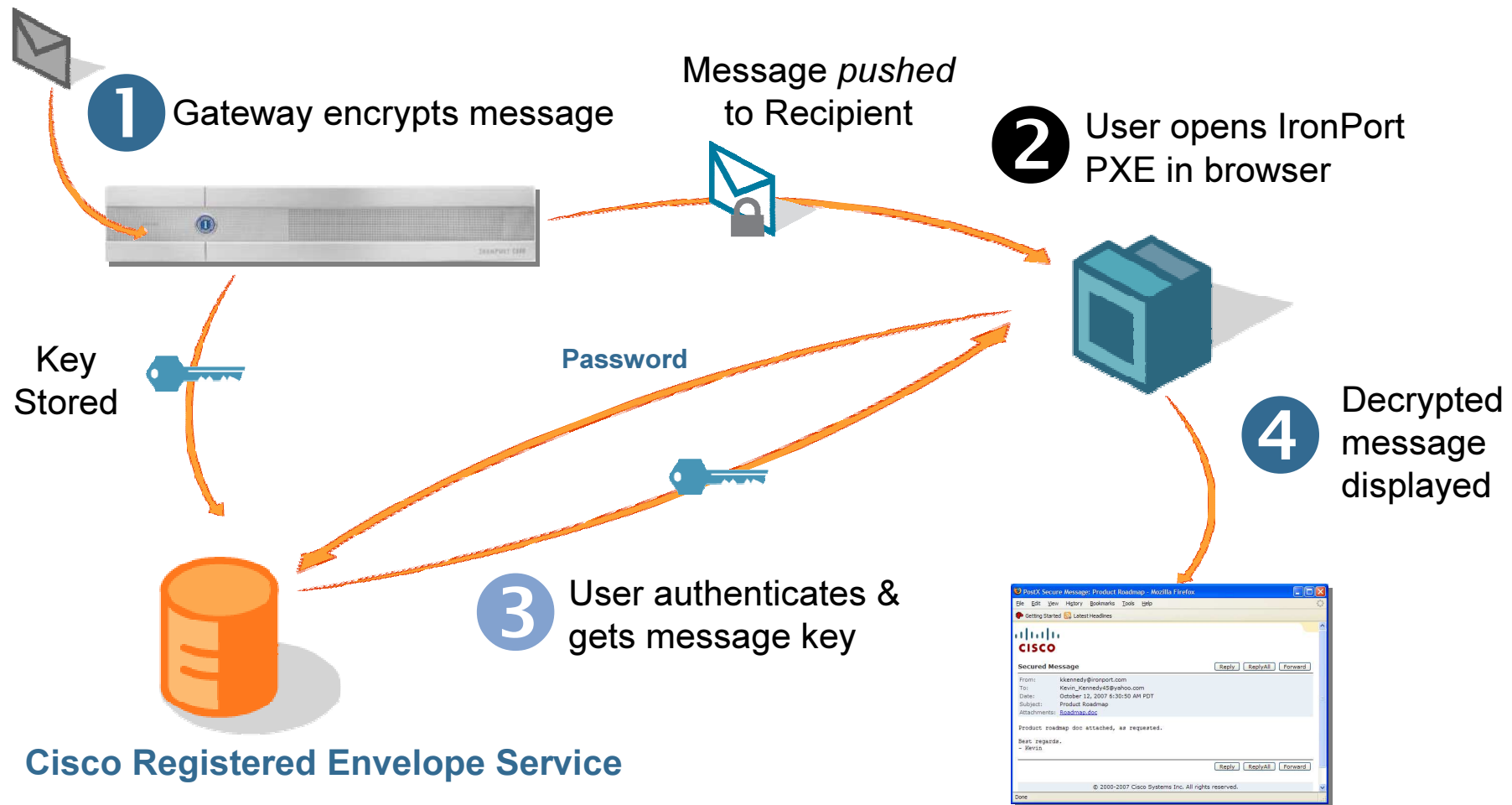


Scanning : pre-defined filters (SOX, HIPAA, etc.), compliance dictionaries, automatic tracking of credit card numbers, etc.

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

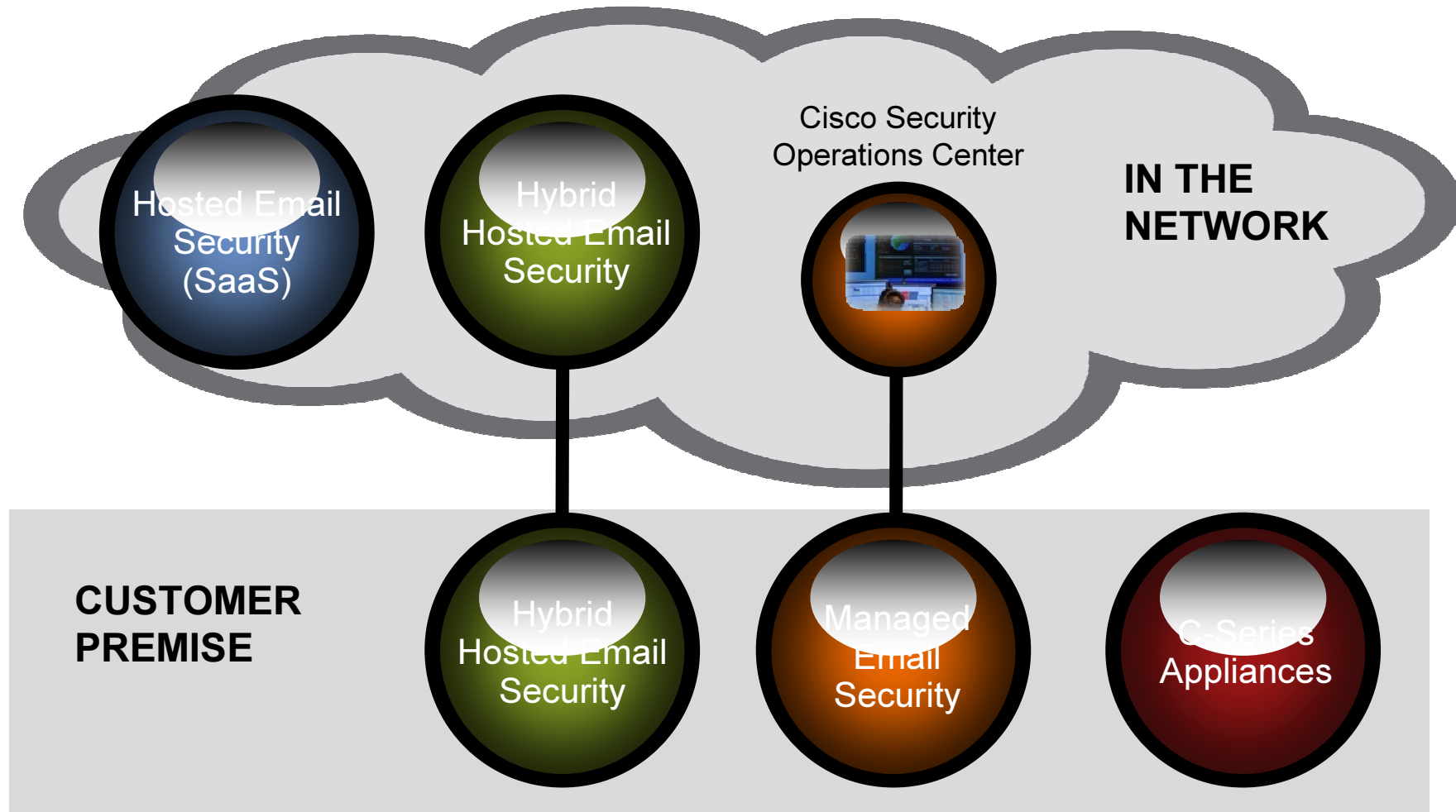
Cisco IronPort E-Mail Encryption

Easy for the sender...



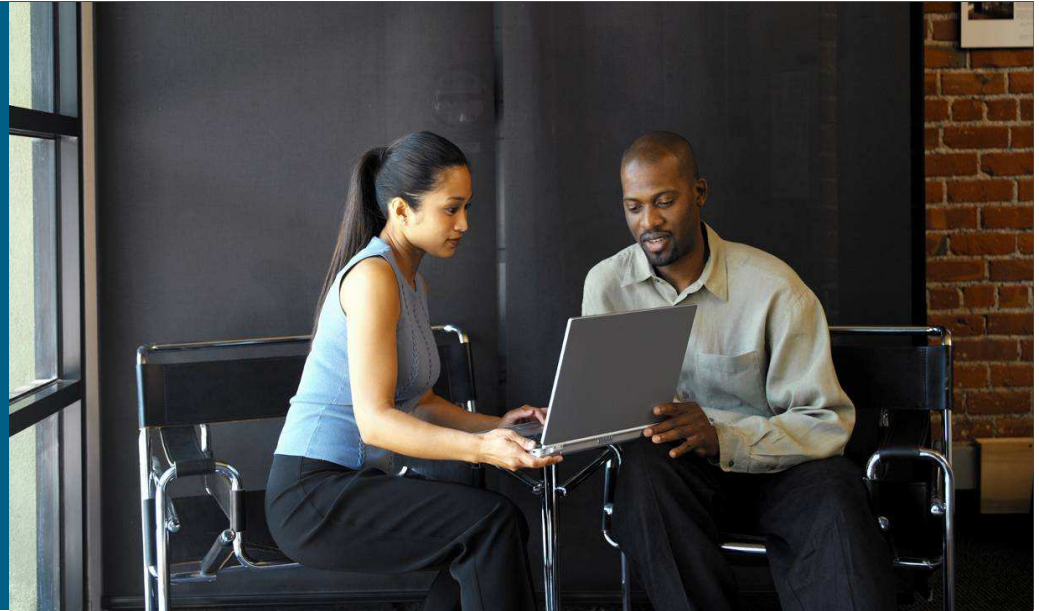
Flexible Deployment Options

Same Market-Leading Email Security



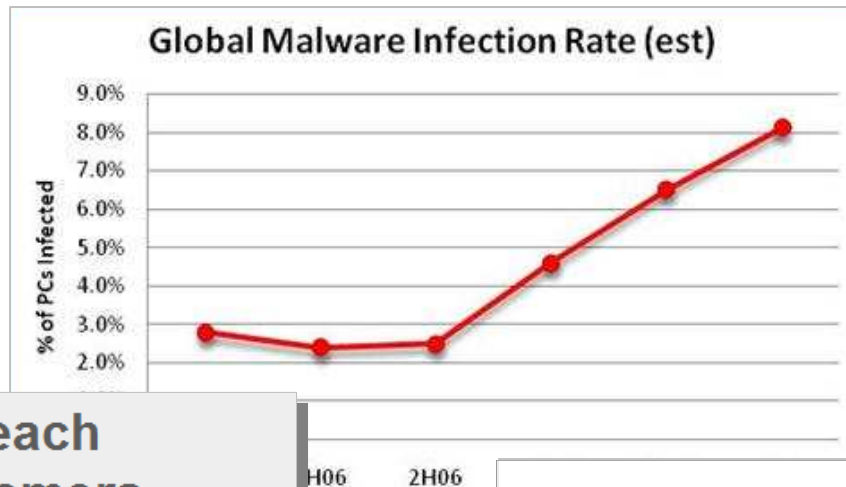
Common Policy | Centralized Reporting | Consistent Protection

Web Security



Web Business Challenges

Malware



Data Loss

TD Ameritrade Breach Affects 6.3M Customers

Brokerage firm uncovers data-sucking malware during system upgrade

IT WEEK

About Contacts Subscribe Advertise Jobs S

SEPTEMBER

By Tim
Site Editor

IT Week > News > Hacking

Malware
names
million

Smart malware steals from SSL streams

Is nothing safe?

Iain Thomson, vnunet.com, 22 May 2007



A new variant of the

Acceptable Use Violations

40% Productivity Loss*

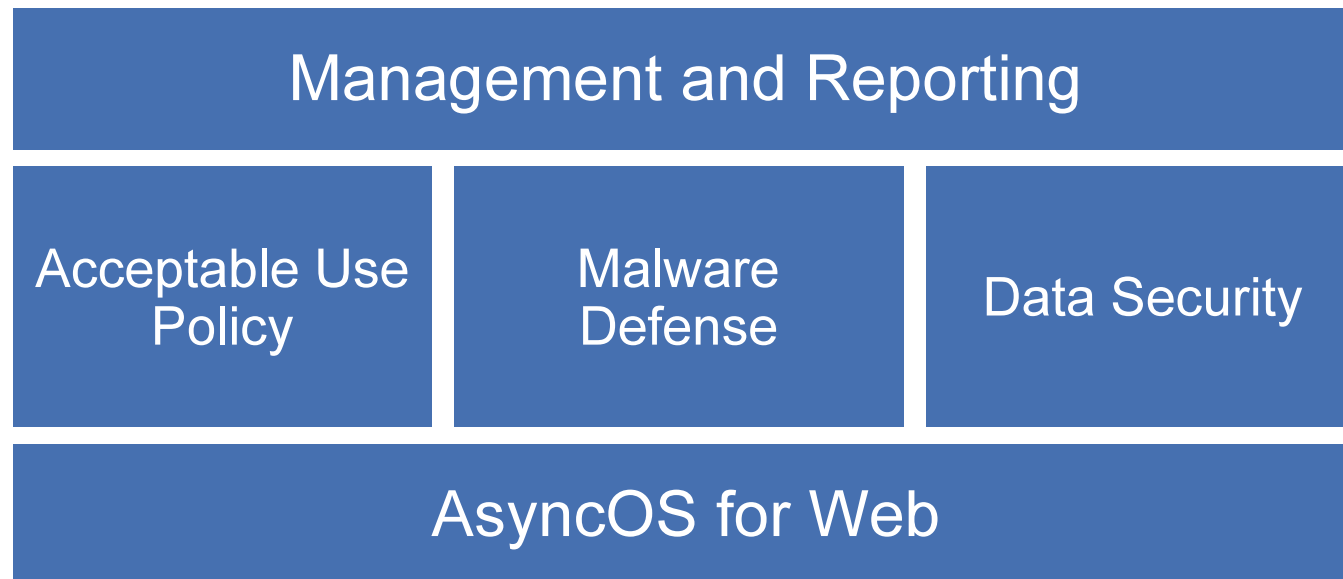
due to personal web use at work

Legal and Regulatory Risk

of offensive content brought into the workplace

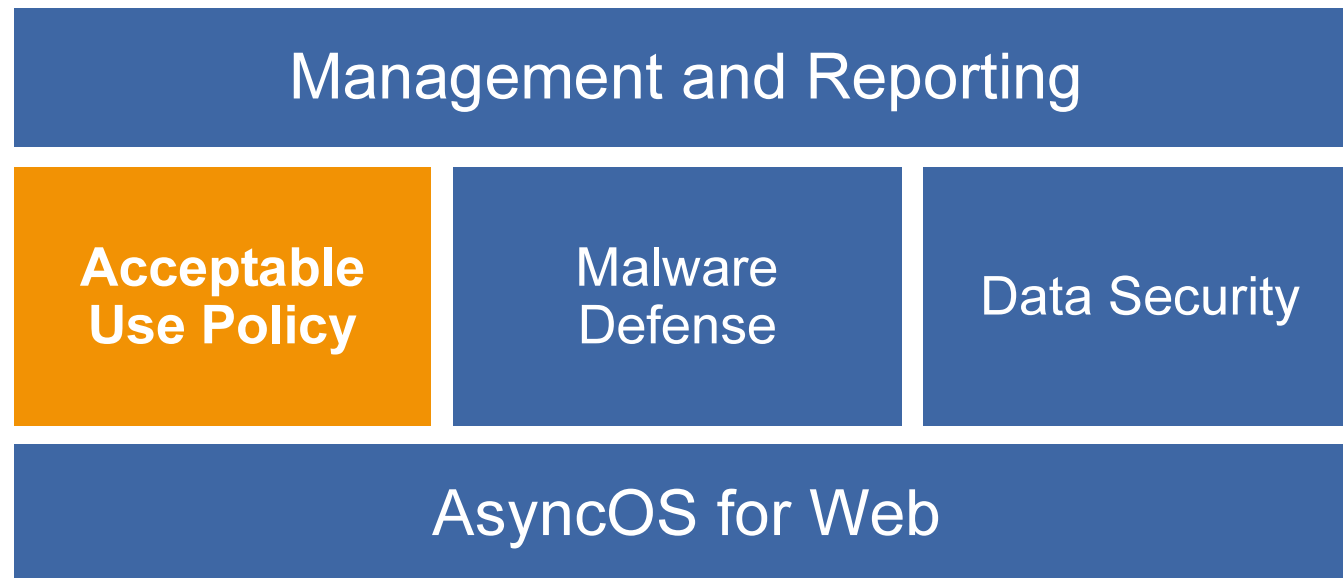
Cisco IronPort S-Series

A Powerful, Secure Web Gateway Solution



Acceptable Use Enforcement

Visibility and Control for the Web and Web Applications



- Enterprise-class URL filtering
- Applications and object filtering

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



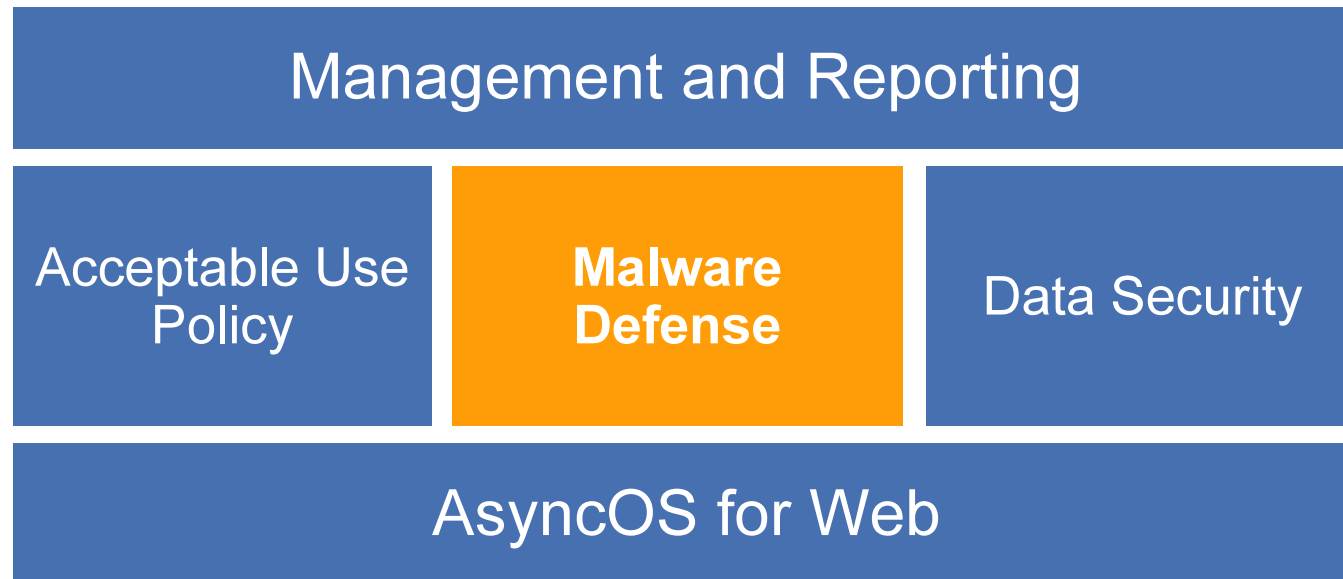
Web Application Control

- 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)



Malware Defense

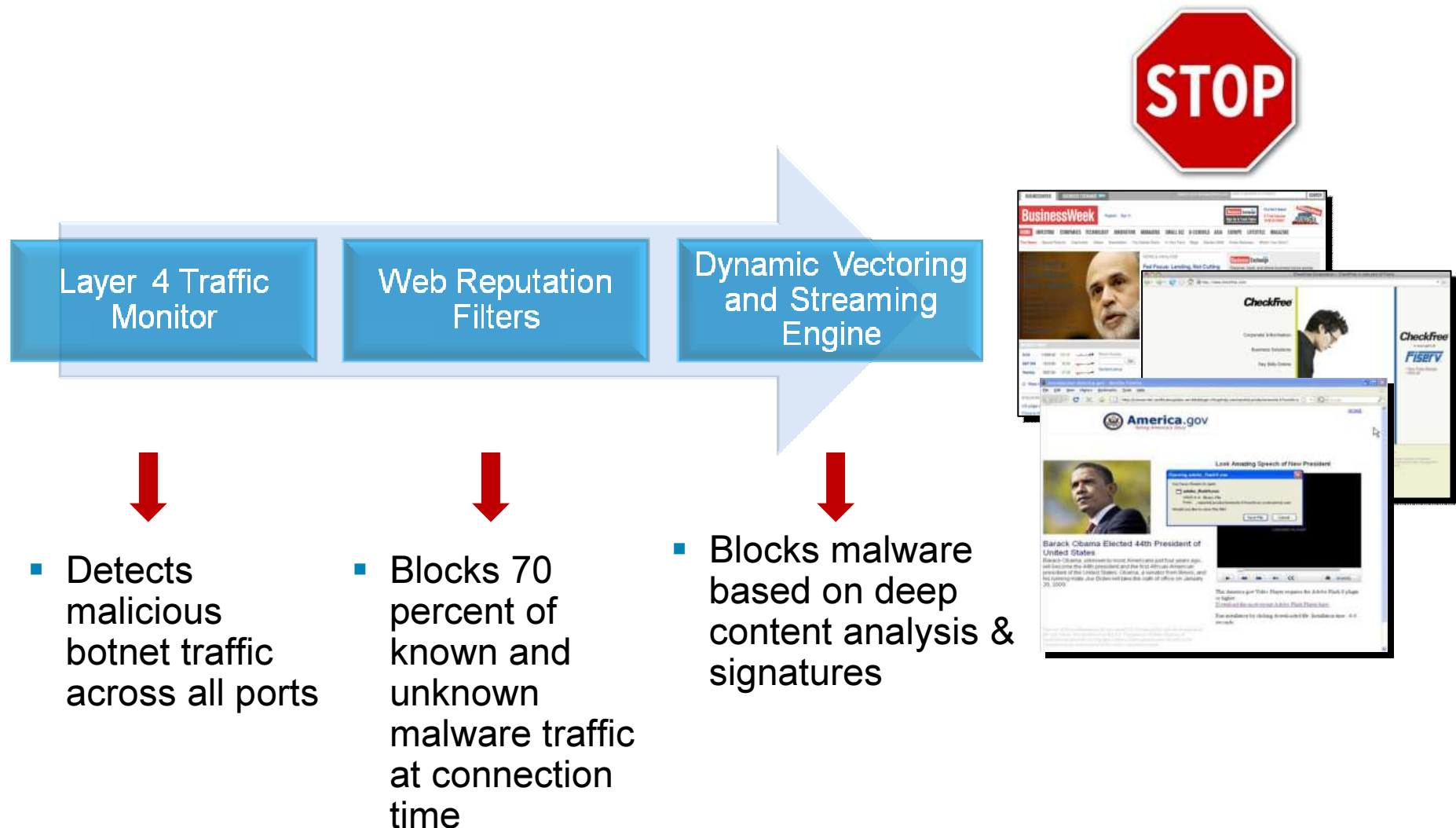
Multiple layers for Anti-Malware Protection



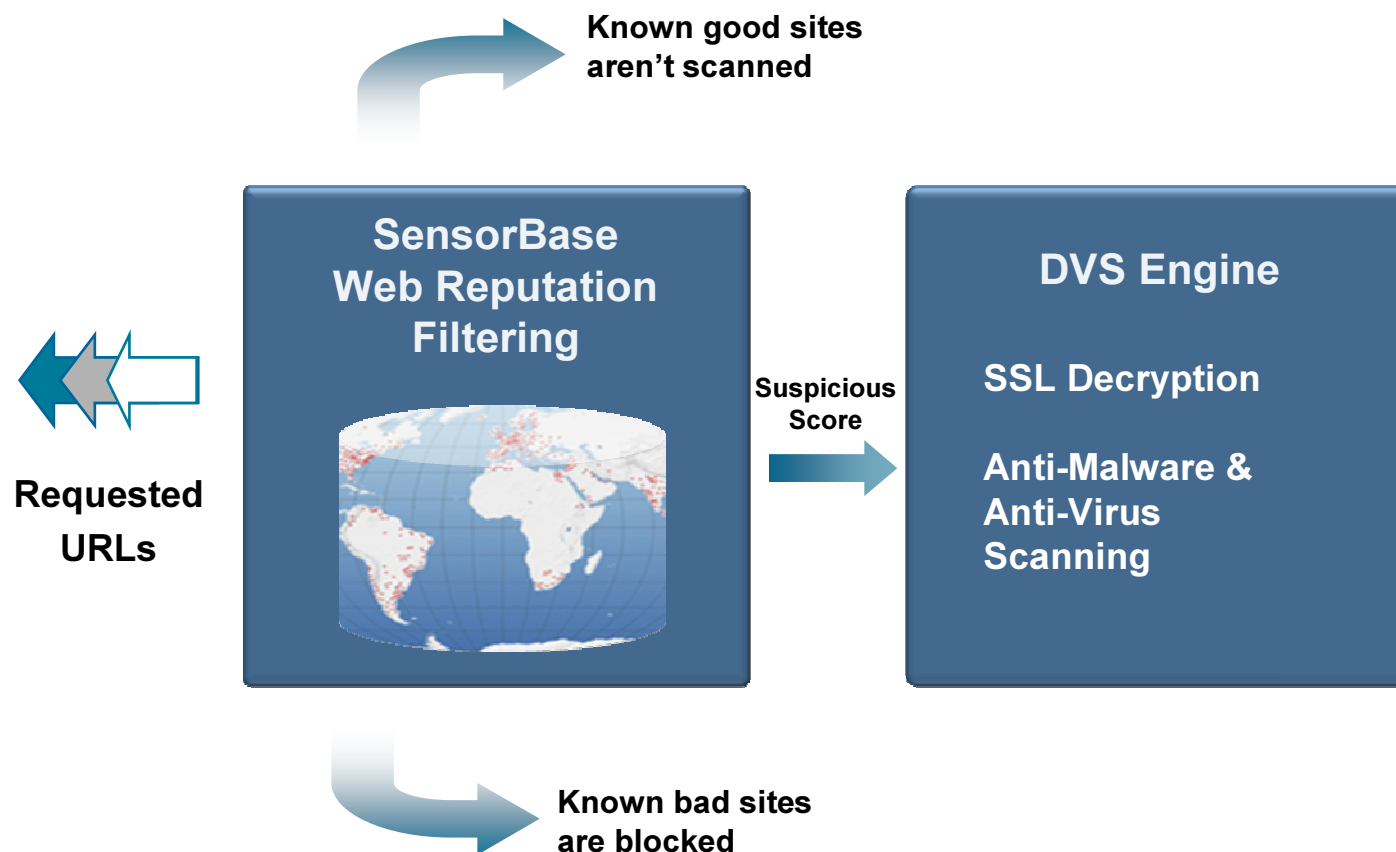
- Network layer Traffic Monitor
- Web Reputation Filters
- Signature-based scanning (DVS Engine)

Multi-Layered Malware Defense

Protection Against Today's Threats



Web Reputation Filtering

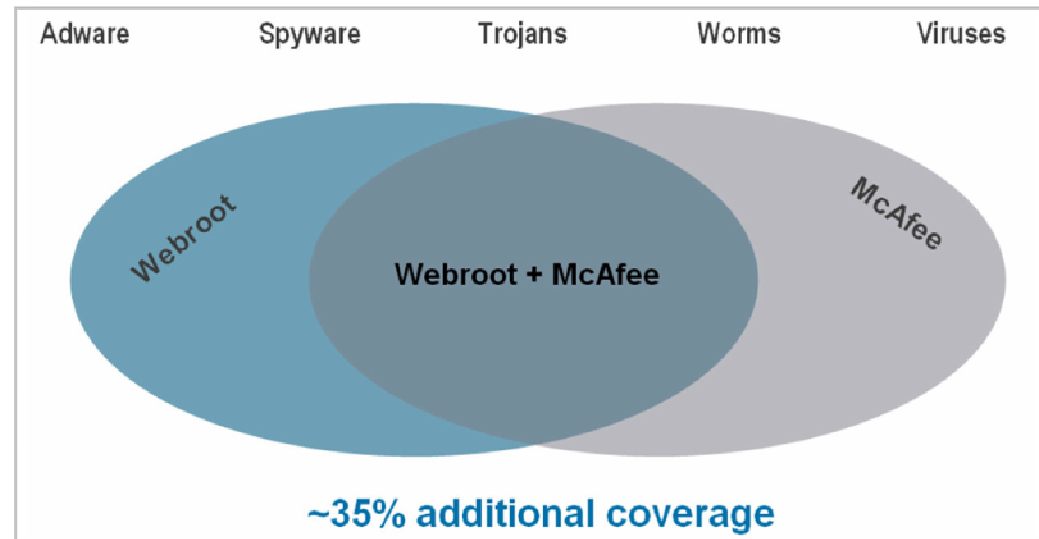


Cisco IronPort DVS Engine

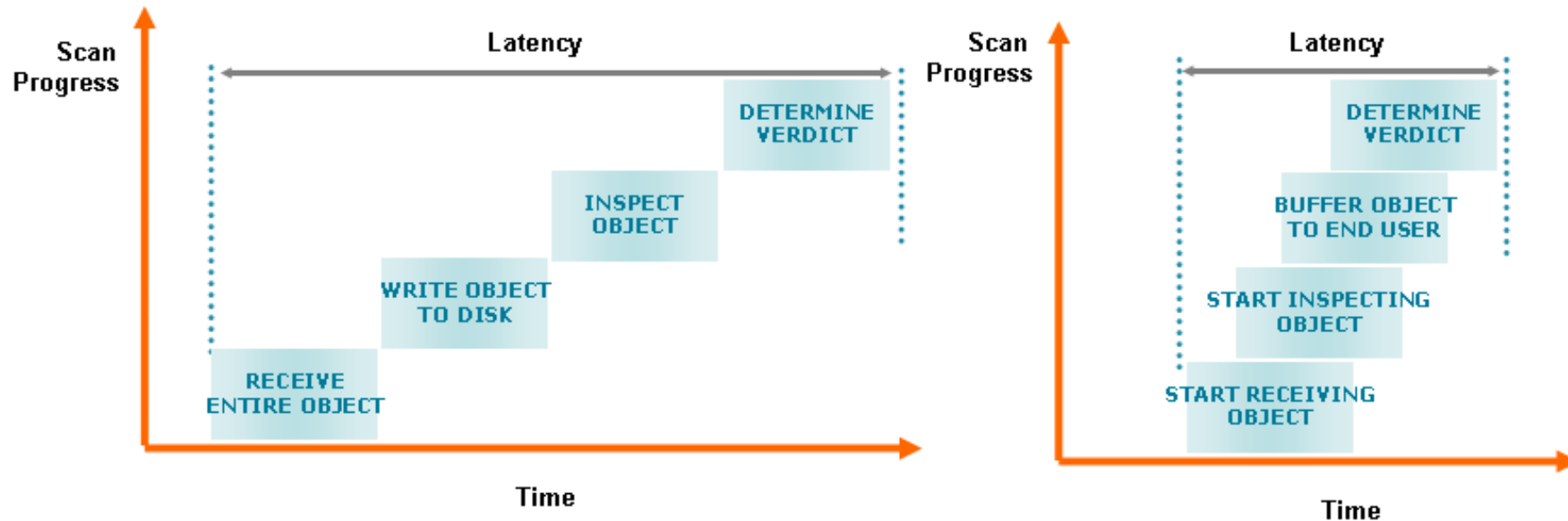
Dynamic Vectoring and Streaming



- 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



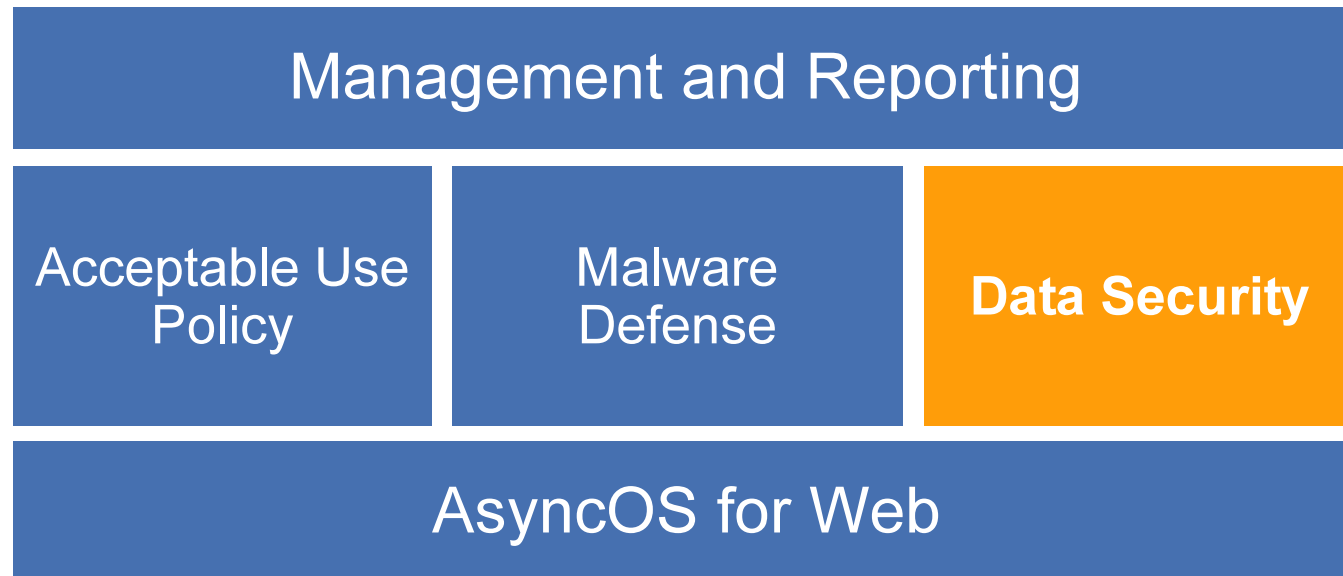
Stream scanning



« 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

Data Security




On-box Common Sense Security

- Metadata inspection
 - Including file type, size, name.
- Allow, block, log
 - Metadata combined with userID, category and reputation of the destination
- Multi-protocol
 - HTTP(s), FTP, HTTP tunneled



Common Sense Policies

Simple Approach for Avoiding Web Data Breaches

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

Quick Facts



3 questions & competitive advantages

Email

- Do you have problems with your current anti-spam solution?
 - False positives, capture rate, performance issues
- Are you protected against “zero-day” attacks (new viruses with no signatures known yet)?
- How do you secure your outbound messages?
 - Content scanning?
 - Encryption?
- High-Performance Mail Transfer Agent
 - More simultaneous connections managed
 - Advanced features included
- Sensorbase Email Rep filters
 - Best reputation database on the market. Stops 90% of messages at connection level
- High efficiency with no worries
 - High Capture Rate
 - Automatic, policy-based data security
 - Almost no administration needed

Competition / Email

Competitors

- Secure Computing (McAfee)
 - Low prices
- Proofpoint
 - Good technology with lower prices
- Barracuda
 - Extremely low prices
 - SMB target

Weaknesses

- Secure Computing
 - Weak Reputation catch rate, poor performance, poor support
- Proofpoint
 - Reputation database with no history
- Barracuda
 - Poor anti-spam catch rate
 - Poor performance & support

3 questions & competitive advantages

Web

- How do you prevent users to go to infected websites?
 - URL Filters not a secure solution against new threats
- How do you enforce Acceptable Use Policies for Internet access?
 - Site categories/Applications
- Do you have malware defense on the web gateway?
 - With no latency? Multi-protocols, including SSL?

- Integrated solution
 - 1 box for acceptable use policies, malware defense, and data security
- Sensorbase Web Rep filters
 - Best reputation database. Stop 70% of threats at connection level.
- Cisco IronPort's DVS Engine
 - Selective SSL decryption
 - Multi-database
 - Stream scanning technology

Competition / Web

Competitors

- BlueCoat
 - Large installed-base
 - High-level proxy
 - High number of security OEM partners
- Websense
 - Large installed-base
 - URL Filters
- Secure Computing (McAfee)
 - Low price
 - Multi-protocol scanning

Weaknesses

- Blue Coat
 - AV scanning needs a second box
 - Only 1 database can be used
 - Low-performance SSL decryption
- Websense
 - No Reputation (URL category Black list only)
 - No scanning engine/ advanced security features
- Secure Computing (McAfee)
 - Old e-mail centric reputation database
 - Poor performance & support

