



Cisco Expo
2008

E-Mail & Web Security



Sébastien Commérot
Marketing Manager, Southern Europe, Middle-East & Africa
IronPort, a Cisco Business Unit

Agenda

- Internet Threats : latest trends
- E-Mail Security : IronPort C-Series
- Web Security : IronPort S-Series

IronPort : who are we?



- Global Operations

- Funded in 2000, now a Cisco Business Unit

- Worldwide HQ near San Francisco

- 45 offices in 35 countries

- 645 people

- Analyst Leadership

- Recognized as the leader of e-mail security appliances by Gartner, IDC, Radicati, etc.

- Customer Leadership

- 325 million mail boxes secured

- More than 7000 customers in 85 countries, including:

- 54% of the world's Top 100 companies

- 12 of the 15 biggest ISP's worldwide

- 7 of the 10 biggest banks worldwide

- Technology Leadership

- 1st to develop a high-performance MTA

- SenderBase: first & largest monitoring database*

- 1st with *Reputation Filtering*

- 1st with *Virus Outbreak Filters*

Internet Threats

Latest trends



Phishing is changing

- New trends
 - Pharming
 - Spear phishing : social engineering
 - Typo attacks: www.google.com
- 1/3 of phishing sites host malware
- Average on-line time for a phishing site : 3.6 days

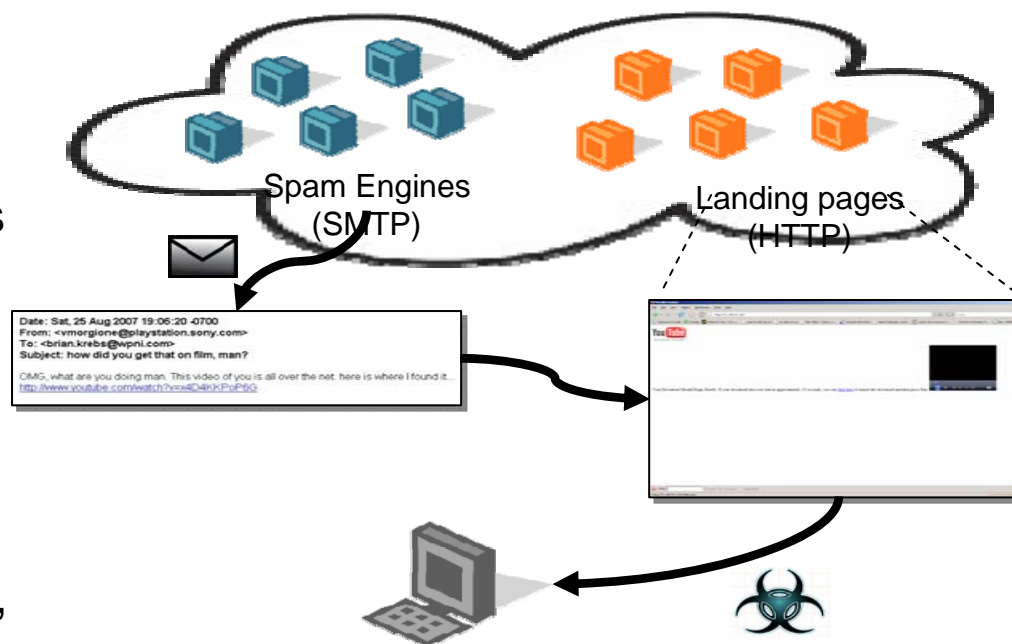


Source : Anti-Phishing Working Group

Zombies are changing

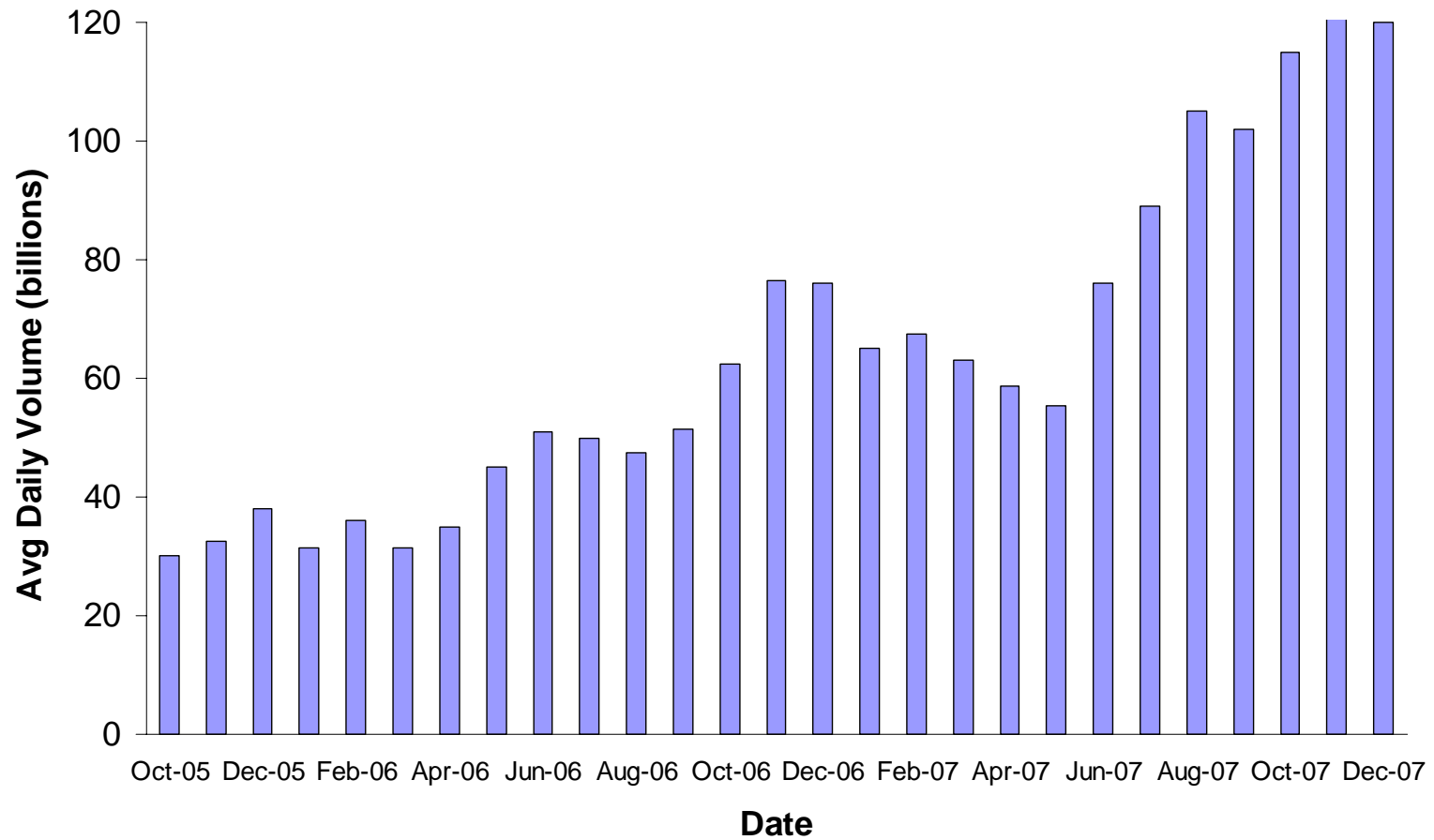
The Storm network

- **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 fast-flux and P2P network
- **Reusable:** Spam, Phishing, DDoS, Blog Spam
- **Self-Defending:** Will DDoS those to poke it



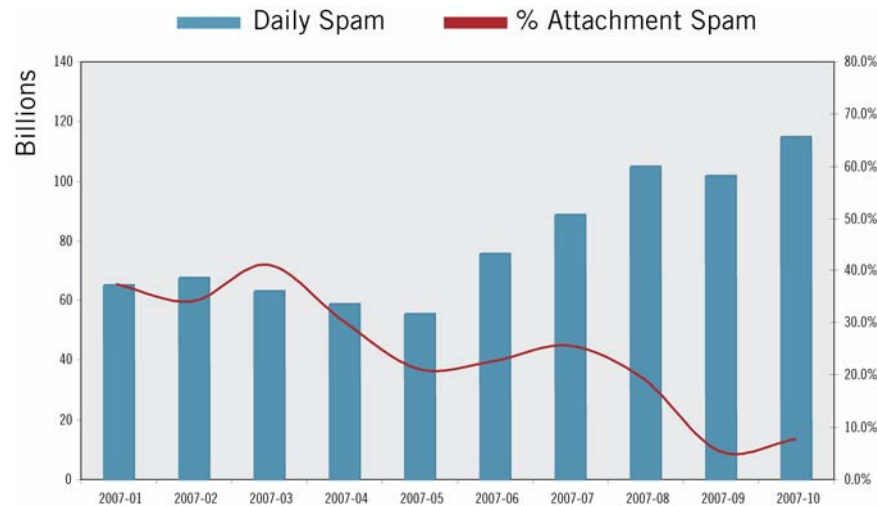
Spam keeps growing!

x4 in 2 years!



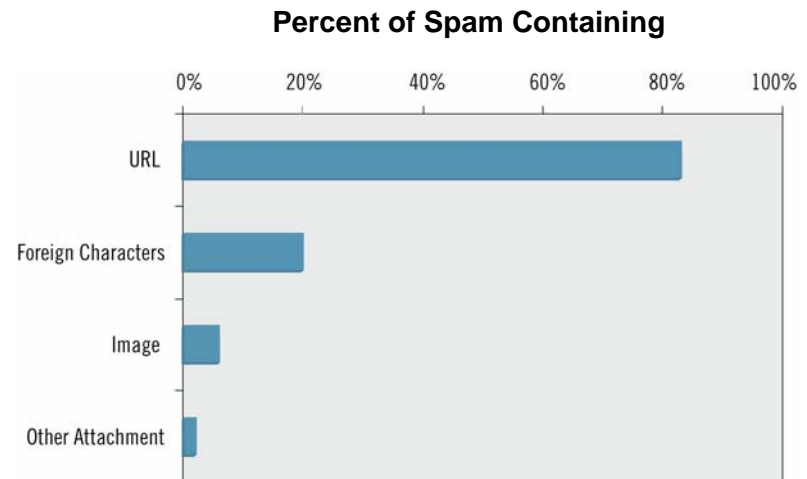
Spam techniques are changing

From images to web links

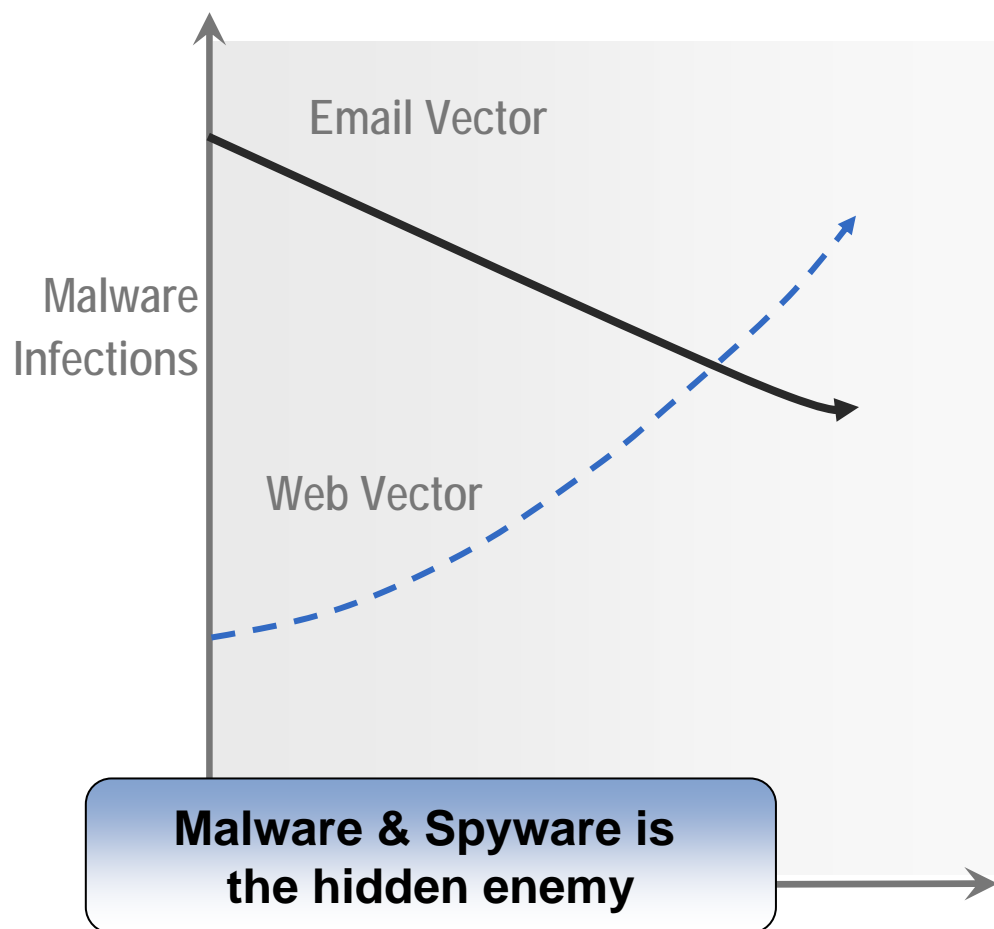


Spam keeps growing, but attachment spam reduces

URL spam keeps growing
(+ 253% in 2007 vs 2006)



Threat vectors are changing



TD Ameritrade Breach Affects 6.3M Customers

Brokerage firm uncovers data-sucking malware during system audit

From: <[redacted]@tdameritrade.com>

Man you have got to tell me where you picked her up. I saw this on the web, it has to be you. check it out yourself <http://www.youtube.com/watch?v=IHZbpJLfpV>



Dolphins' Web sites hacked in advance of Super Bowl

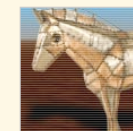
By Rob [redacted]



Smart malware steals from SSL streams

Is nothing safe?

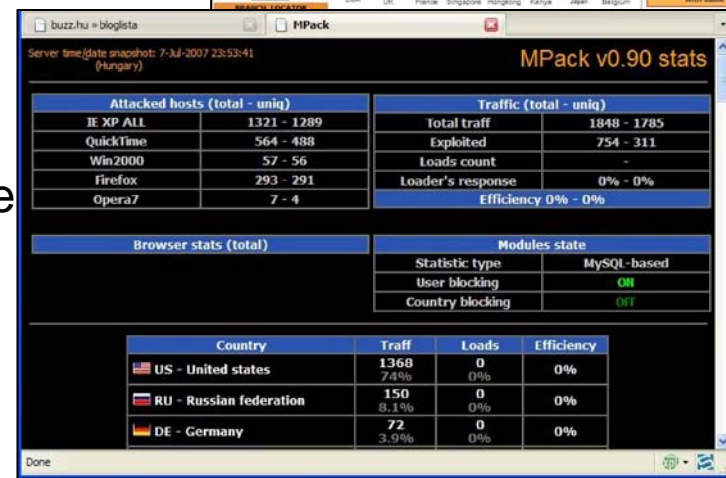
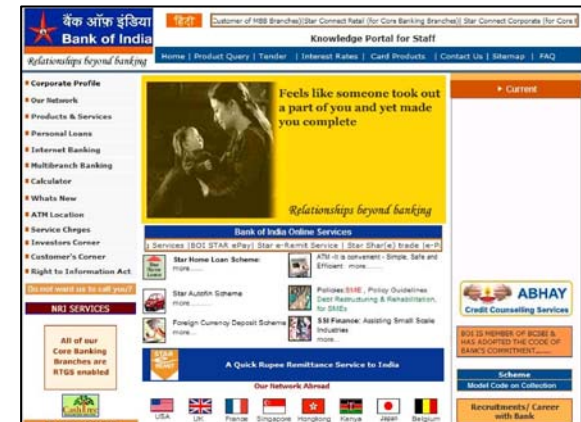
Iain Thomson, vnunet.com, 22 May 2007



A new variant of the [redacted] is stealing data

Legitimate Sites Hacked

- 70% of Web-based infections were found on 'legitimate' websites (Google survey, May 2007)
- iFrame attacks
 - A legitimate site is hacked (iFrame added on a page)
 - The user is re-directed by the iFrame towards an infected website
 - A malware is automatically downloaded on the desktop by exploiting a vulnerability of the web browser sur le poste en exploitant une vulnérabilité du navigateur web
- Web 2.0 Sites
 - The hacker modifies the page with a malicious code la page avec un code
 - The code potentially redirects the users towards a malicious site.



Data Loss Prevention

E-Mail is a major leak vector

- Intellectual Property Protection

 - Personal / Financial Data

 - Intellectual Property

 - Secure communications with partners or customers

 - Control communications with specific domains (competitors, etc.)



- Acceptable Use

 - Enforce messaging policy (size, type, content of attachments)

 - Control offensive content

 - Add legal disclaimers to outgoing mails



- Regulatory Compliance

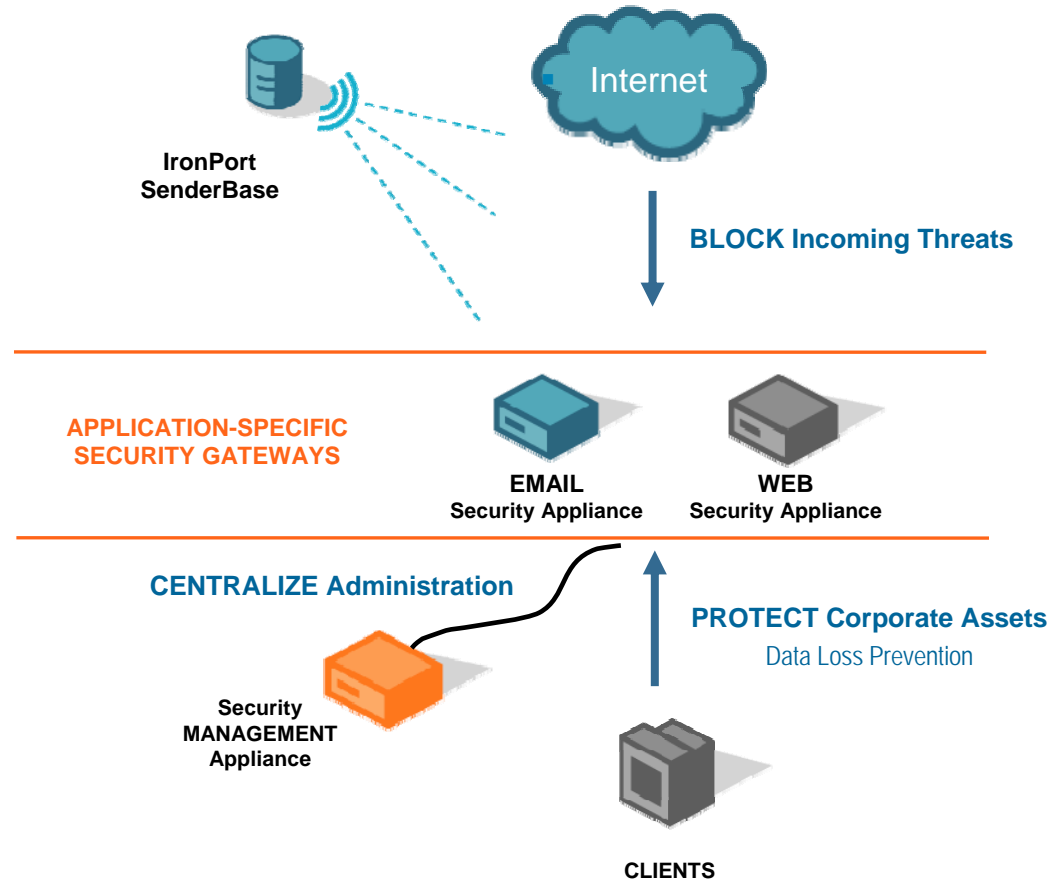
 - SOX, HIPAA, GLBA, PCI, etc.



“Email has become the de facto filing system for nearly all corporate information, making it even more critical to protect the outbound flow of messages.”

- Brian Burke, Security Products Research Manager, IDC

The IronPort® Vision



Web Security | **Email Security** | **Security Management**

IronPort SenderBase®



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

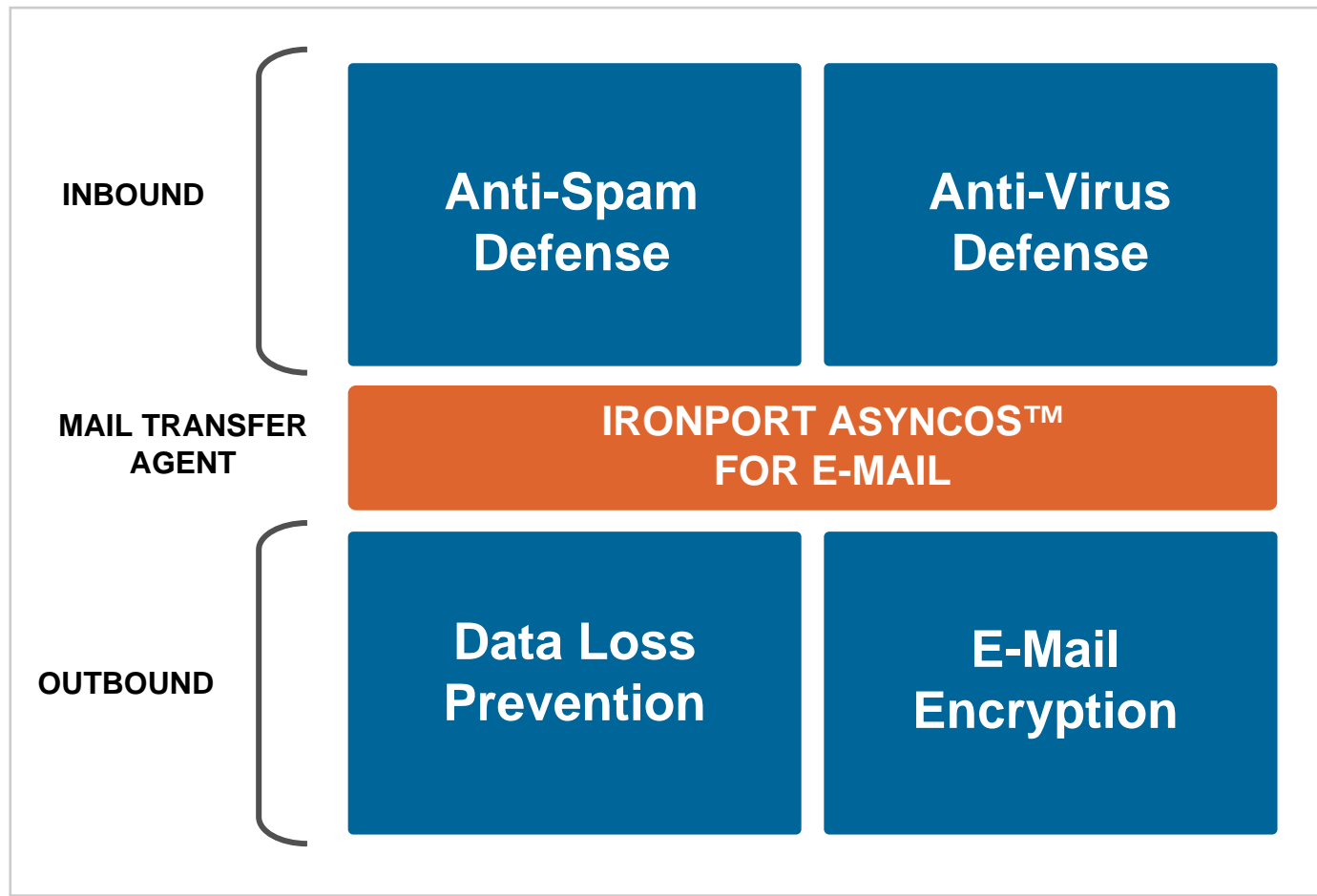


E-Mail Security IronPort C-Series



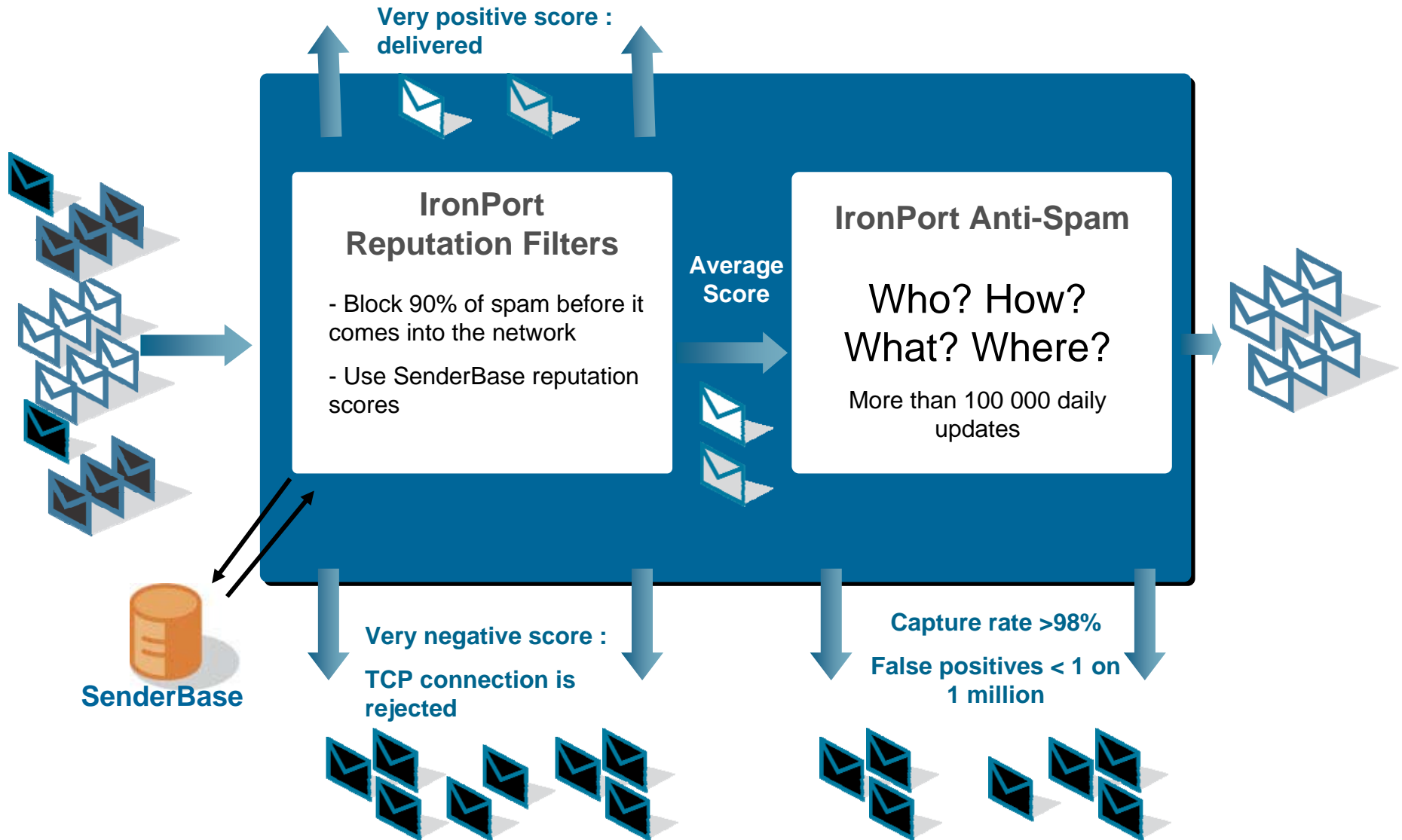
IronPort C-Series

Inbound & Outbound Security



IronPort Spam Defense

Multi-Layer Protection



IronPort Stops Phishing

- Web Reputation: IronPort exclusive technology assigns reputation score to URLs in emails based on likelihood to host phishy / spammy content
- Stops over 97% of phishing attacks

From: Barclays Bank PLC
Date: Sunday, July 15, 2007 9:23 PM
To: X
Subject: [SPAM] [SPAM] Barclays Bank Secur



Dear Sir/Madam,

Barclays Bank PLC. always look forward for the h
account maintenance and verification procedures
might be due to either of the following reasons:

1. A recent change in your personal information.
2. Submitting invalid information during the initial

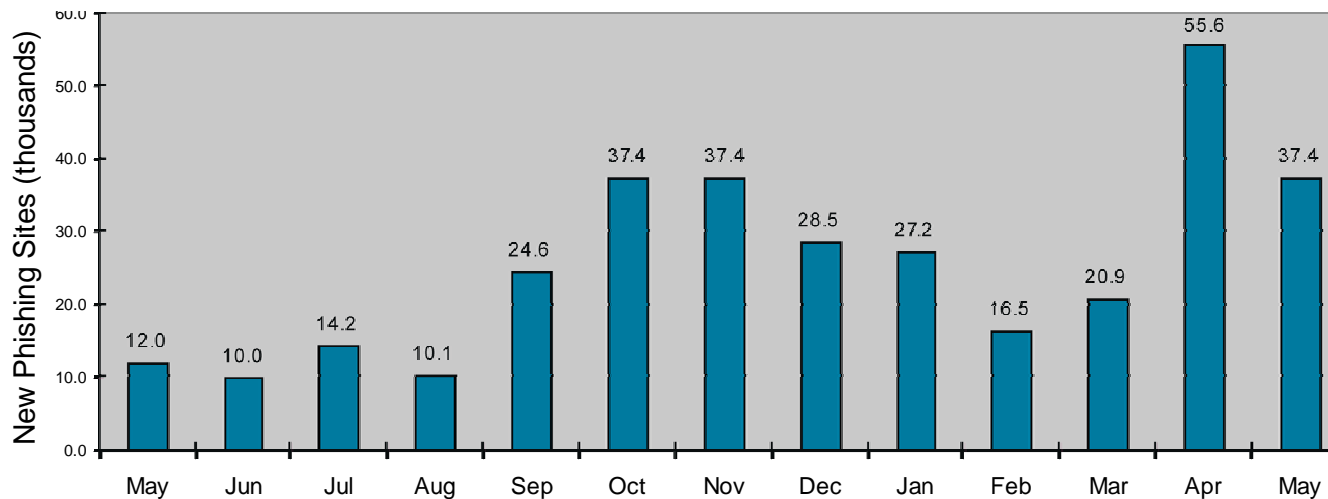
Due to this, you are requested to please update and verify your information by clicking the link below:

<https://ibank.barclays.co.uk/olb/x/LoginMember.do>

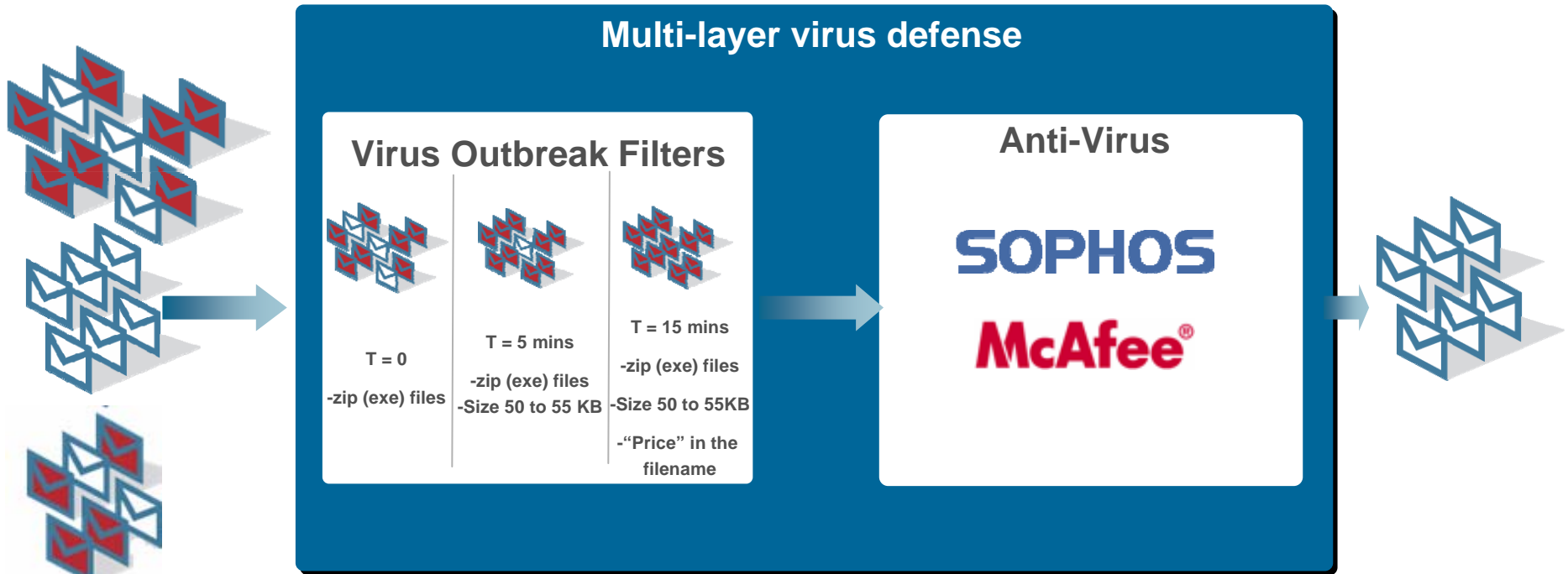
– URL registered to ISP in Mauritius, not Barclays

– domain on several blacklists

– abnormally high volume traffic to domain



IronPort Virus Defense



Virus Outbreak Filters Advantage

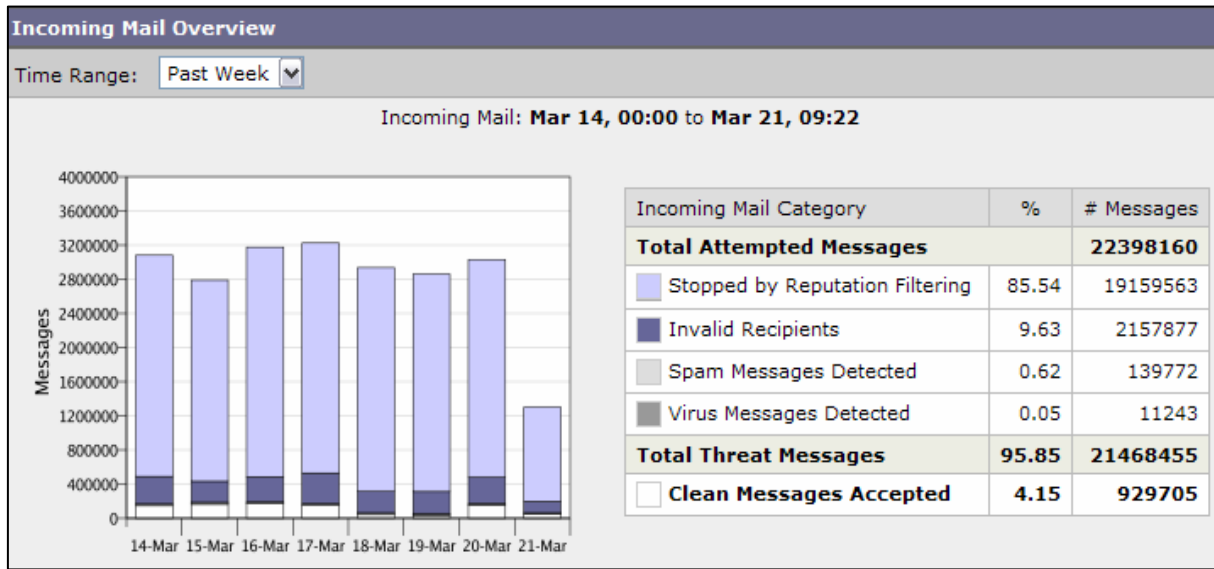
www.ironport.com/toc

Average lead time on protection * over 13 hours
On a total of major outbreaks of * 248 outbreaks
Total incremental protection * over 134 days

* Between Oct 2006 et Sept 2007.

Calculated From official release data from the following vendors : Sophos, Trend Micro, Computer Associates, F-Secure, Symantec et McAfee.

IronPort Spam & Virus Defense Dell Case Study



Accuracy of spam filtering increased **10x**
 68 servers running Spam Assassin replaced by 8
 IronPort C-Series (70% consolidation)
 Operating costs reduced by **75%**



“IronPort has increased the quality and reliability of our network operations, while reducing our costs.”

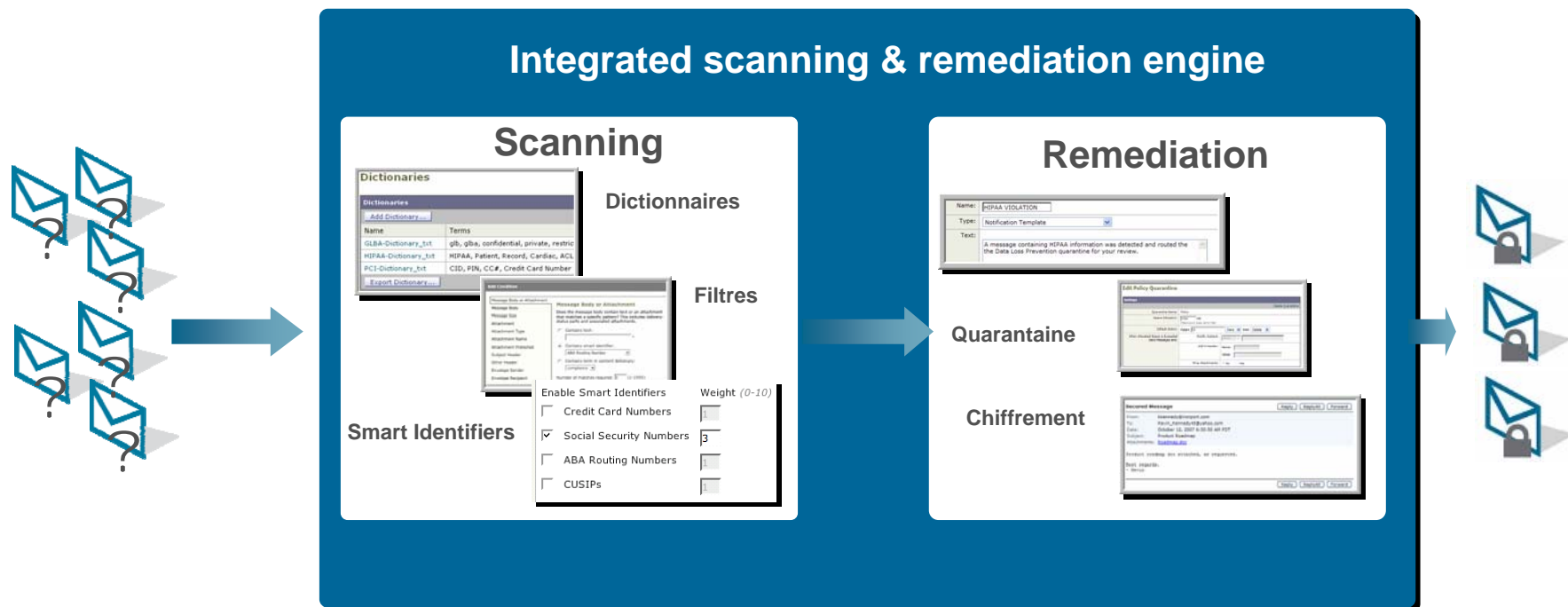
— Tim Helmsetter
 Manager, Global Collaborative
 Systems Engineering and
 Service Management,

DELL CORPORATION

MAILBOXES
 PROTECTED

100,000+

IronPort Data Loss Prevention



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

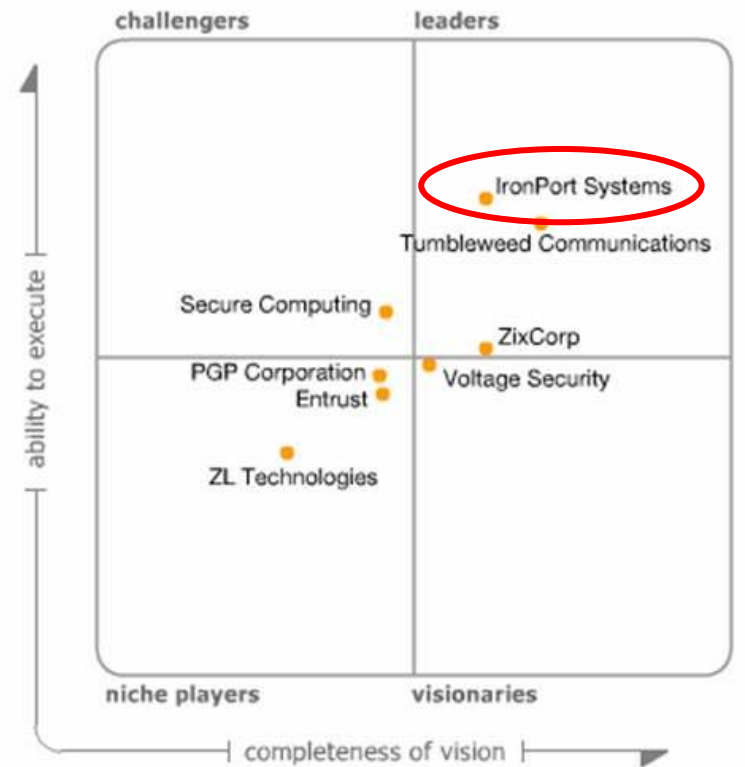
Remediation : alerts, reporting, quarantine, encryption...

IronPort Encryption Overview

Approved by the analysts...

IronPort enables enterprises to communicate sensitive information vital to business and customer relationships

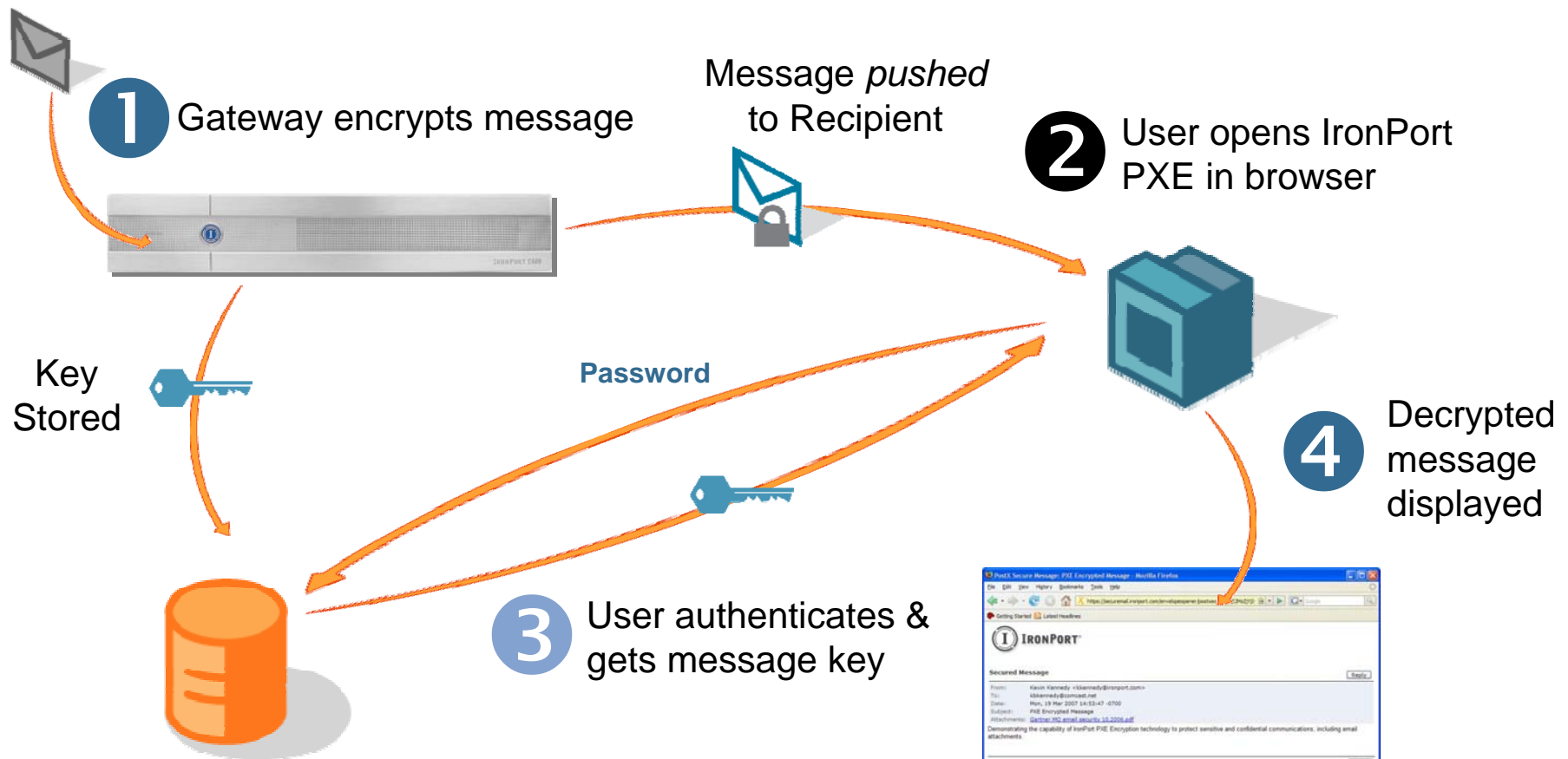
1. Without the need for the recipient to install software
2. Regardless of the e-mail platform & OS used by the recipient



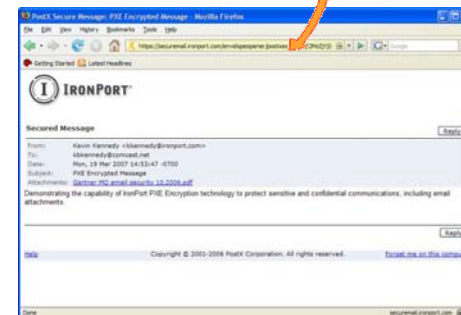
As of August 2007
Source: Gartner "Magic Quadrant"
E-Mail Encryption

IronPort E-Mail Encryption

How does it work?



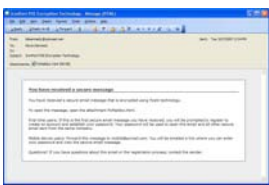
Cisco Registered Envelope Service



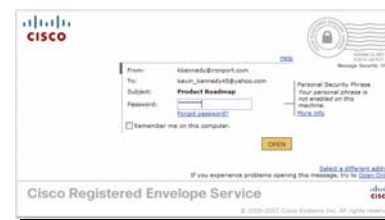
IronPort PXE: Receiving a Message

Seamless End-User Experience

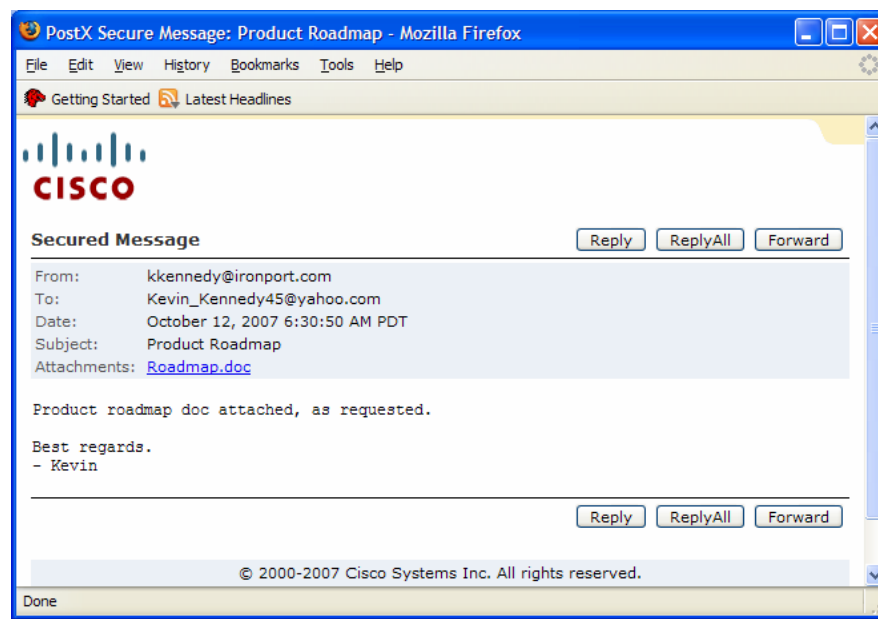
1. Open Attachment



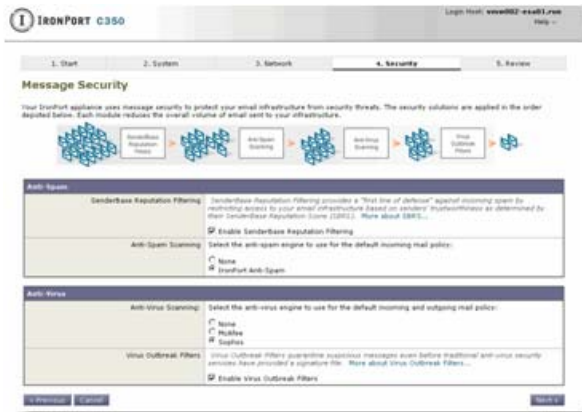
2. Enter password



3. View message



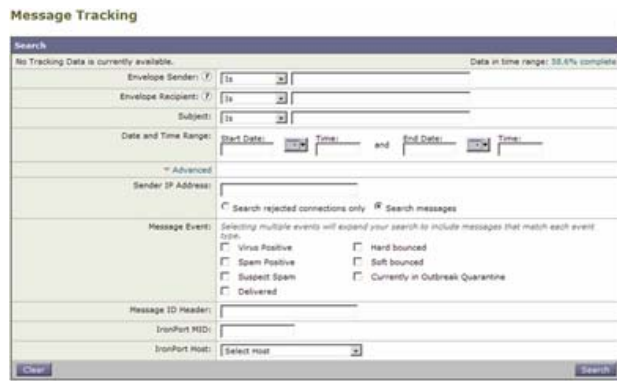
Ease of administration



5-Step installation



Email Security Manager
Configuration of policies pergroups, users, etc.



Tracking of the messages



E-Mail Security Monitor
Real-time reporting

IronPort M-Series

Centralized Spam Quarantine, Reporting & Tracking

- IronPort Email Security Monitor reports centrally available on IronPort M-Series
- Reports on C-Series appliances managed (system capacity, functioning, etc.)
- Stores more than 1 year of data
- Centralized tracking of messages
- Centralized Spam Quarantine

The image displays three overlapping screenshots of the IronPort Message Tracking interface. The top-left screenshot shows the search criteria page with fields for Envelope Sender, Envelope Recipient, Subject, Date and Time Range, and Message ID Header. The top-right screenshot shows the search results page with a table of messages and a 'Results' section. The bottom-left screenshot shows the 'Message Details' page for a specific message, including envelope and header summary, sending host information, and processing details.

Item	Date	Time	MID	Host	Sender	Recipient	Subject	Last State
1	Thu Jul 22 2005	16:37 (GMT -0700)	988809854	mailman.domain.com	normal_sender@29801.tacoma	janedoe@ironport.com	(no subject)	Message successfully delivered
2	Thu Jul 22 2005	16:37 (GMT -0700)	988809854	mailman.domain.com	normal_sender@29801.tacoma	janedoe@ironport.com	(no subject)	Message successfully delivered
3	Thu Jul 22 2005	16:37 (GMT -0700)	988809854	mailman.domain.com	normal_sender@29801.tacoma	janedoe@ironport.com	(no subject)	Message successfully delivered
4	Thu Jul 22 2005	16:37 (GMT -0700)	988809854	mailman.domain.com	normal_sender@29801.tacoma	janedoe@ironport.com	(no subject)	Message successfully delivered

Message Details

Envelope and Header Summary

Received Time: 05 Jun 2007 14:00 (GMT -0700)
MID: 167660
Message Size: 905 Bytes
Subject: (no subject)
Sender: tacozilla@tacomateritory.com
Recipients: brightmail@d1.qa41.qa, brightmail@d1.qa41.qa
Message ID Header: sb4b553a9f@a020.d2.clayton.qa
Receiving Host: ironport.qa
Receiving IP: 172.22.141.2
SMTP Auth User ID: N/A

Sending Host

Reverse DNS Hostname: ironport.qa (verified)
IP Address: 172.22.141.2
SBRs Score: N/A

Processing Details

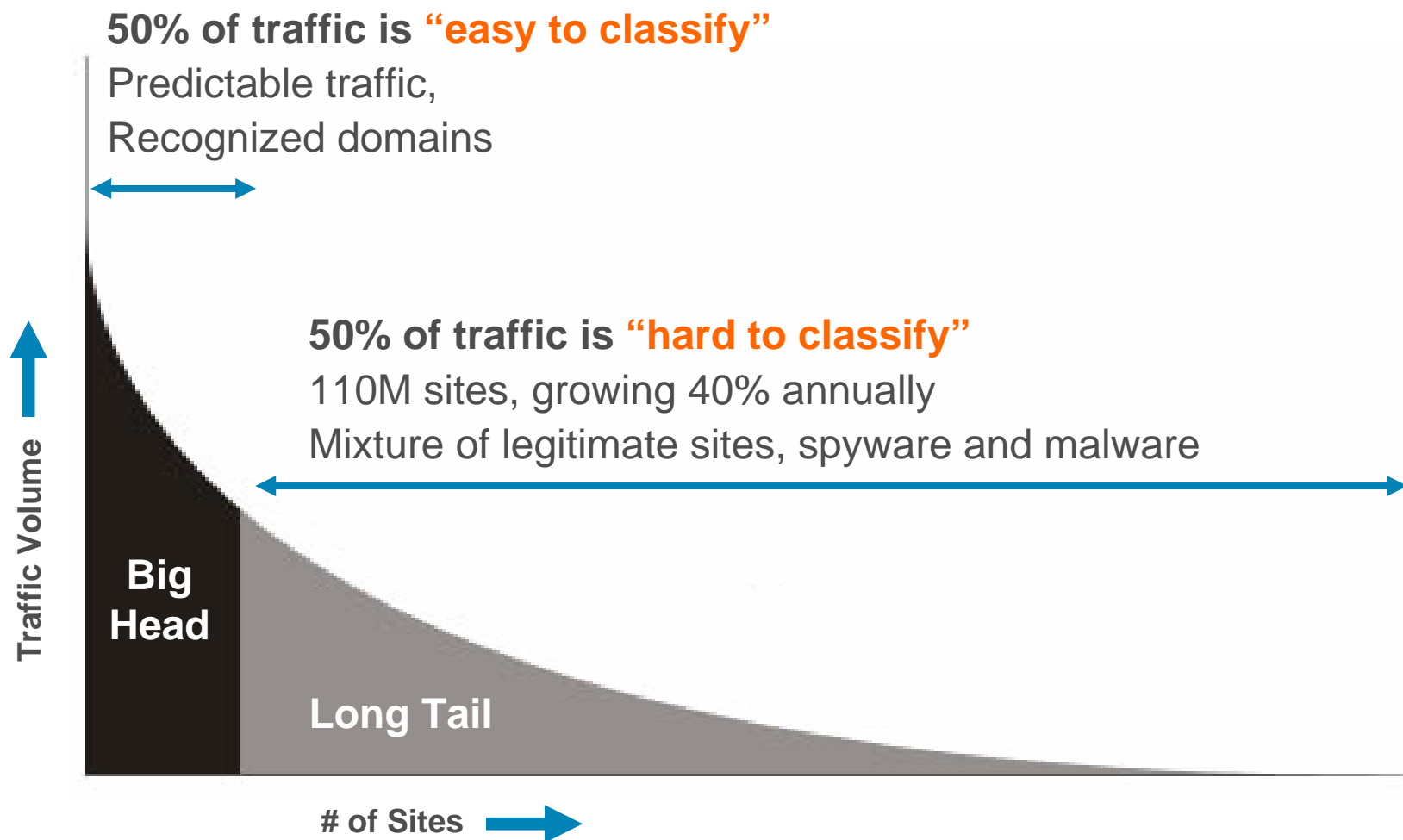
Sep 18, 2006 12:11:40 -0800 Message enqueued
Sep 18, 2006 12:11:40 -0800 Message enqueued
MAIL POLICY "DEFAULT" PROCESSING brightmail@d1.qa41.qa
Sep 18, 2006 12:11:40 -0800 Message processed by Anti-spam. Verdict: Negative
Sep 18, 2006 12:11:40 -0800 Message processed by Sophos Anti-Virus. Verdict: Negative
Sep 18, 2006 12:11:40 -0800 Message queued for delivery
Sep 18, 2006 12:11:40 -0800 Message successfully delivered to brightmail@d1.qa41.qa at '172.21.141.1'. Response: "sent"
MAIL POLICY "DEFAULT" PROCESSING brightmail@d1.qa41.qa
Sep 18, 2006 12:11:40 -0800 Message processed by Anti-spam. Verdict: Negative
Sep 18, 2006 12:11:40 -0800 Message processed by Sophos Anti-Virus. Verdict: Negative
Sep 18, 2006 12:11:40 -0800 Message queued for delivery
Sep 18, 2006 12:11:40 -0800 Message successfully delivered to brightmail@d1.qa41.qa at '172.21.141.1'. Response: "sent"
MAIL POLICY "ipas_drop" PROCESSING ipas_drop@d1.qa41.qa
Sep 18, 2006 12:11:40 -0800 Message processed by Anti-Spam. Verdict: Suspected spam
MAIL POLICY "ipas_drop" PROCESSING ipas_drop@d1.qa41.qa
Sep 18, 2006 12:11:40 -0800 Message processed by Anti-Spam. Verdict: Suspected spam

Web Security IronPort S-Series



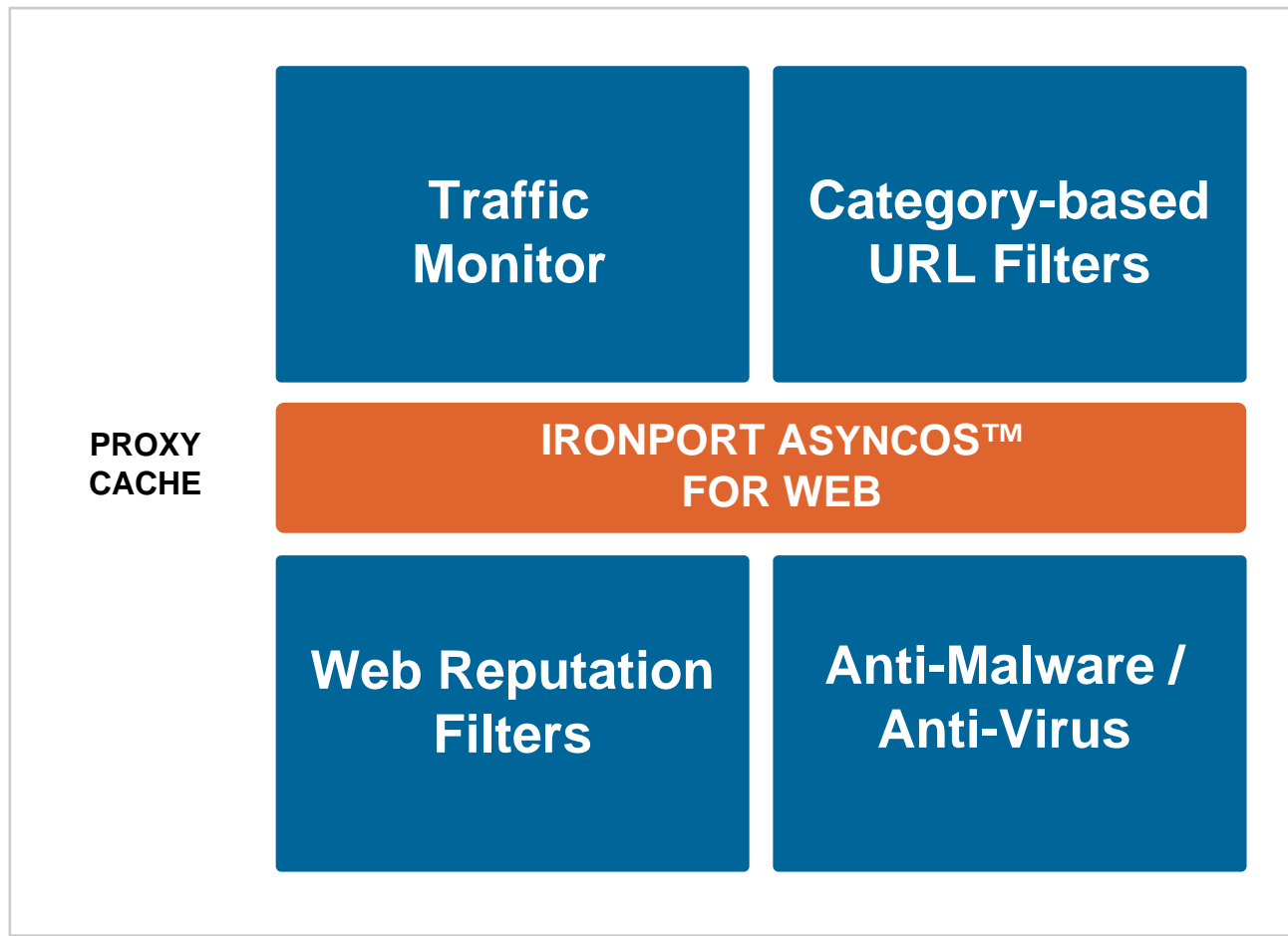
Web Traffic

How to protect according to its nature?



IronPort S-Series

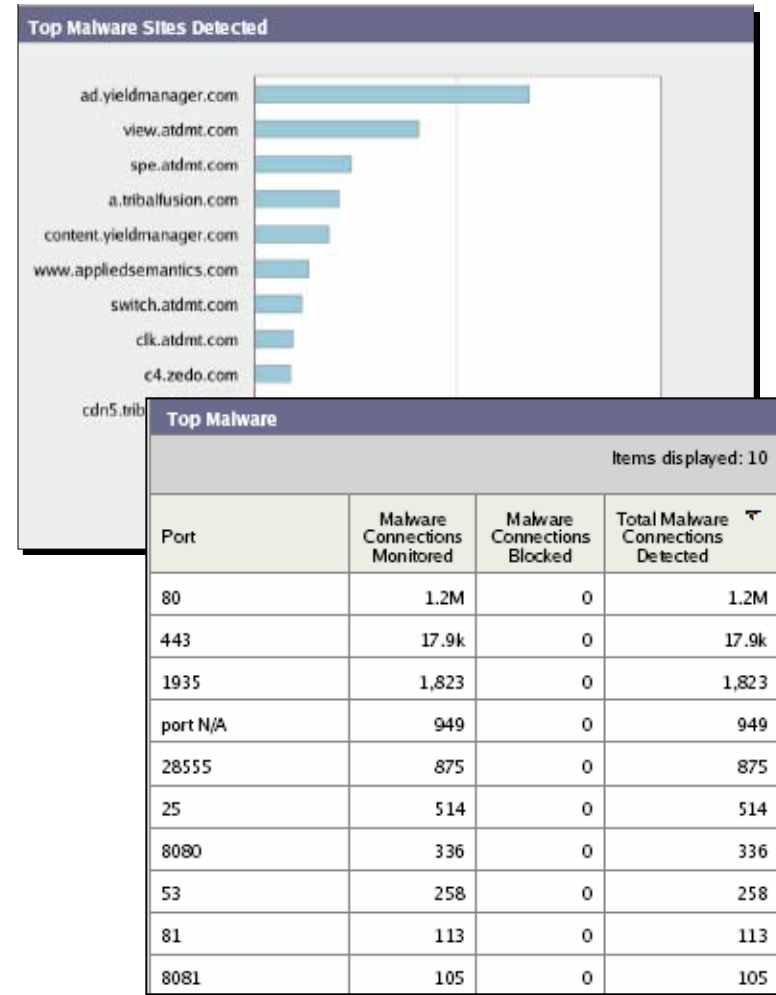
Architecture



Detecting Existing Client Infections

Monitoring “Phone Home” Traffic

- Detects all spyware/Trojan communication with an external server
 - Scans all traffic, all ports, all protocols
- Compare contacted external IP addresses with a “command & control servers” blacklist
- Automatically updated anti-malware rules
- « Monitor » or « Monitor & Block » modes



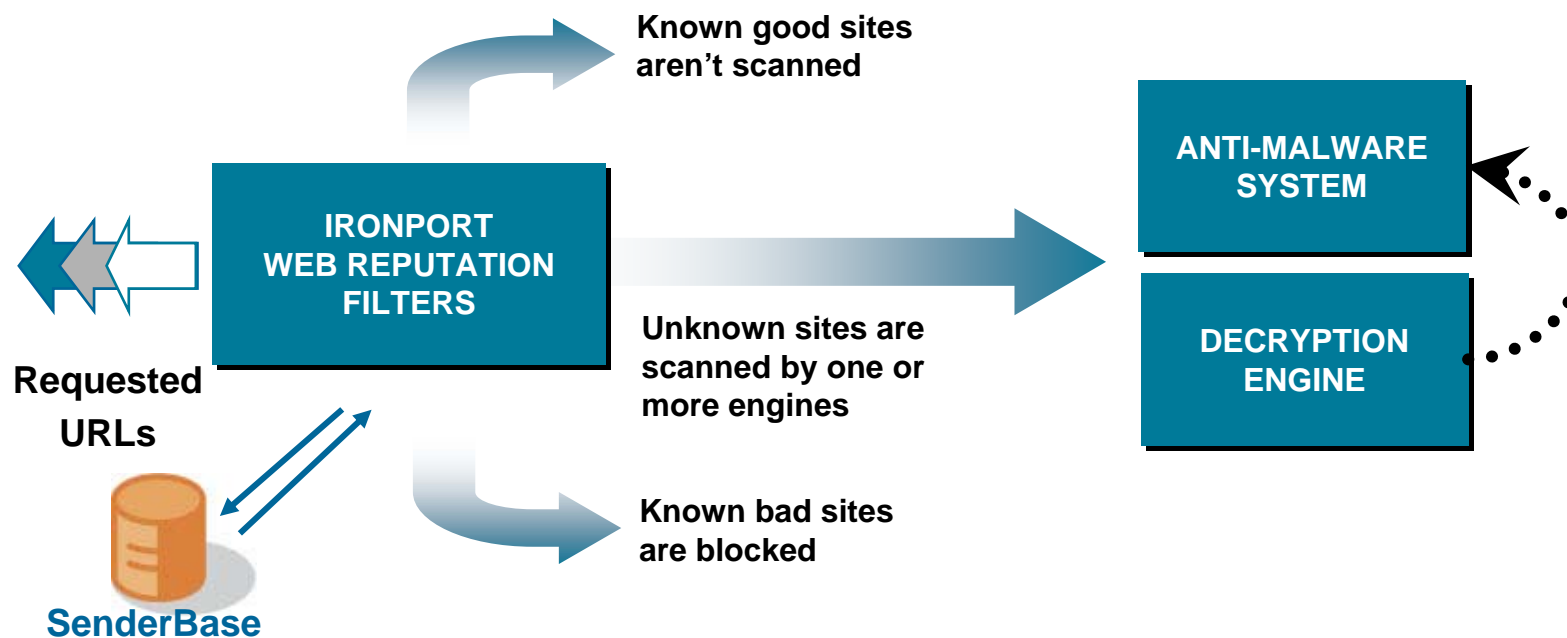
IronPort URL Filters

Leading Accuracy and Control

- Enterprise-class database
 - 52 categories, over 21 million sites, ~3.5 billion webpages
 - 1/3 of the database is international
- 24 x 7 monitoring
- Regular, automated updates
- Flexible policy management
 - Per user, per group policies
 - Monitor only mode



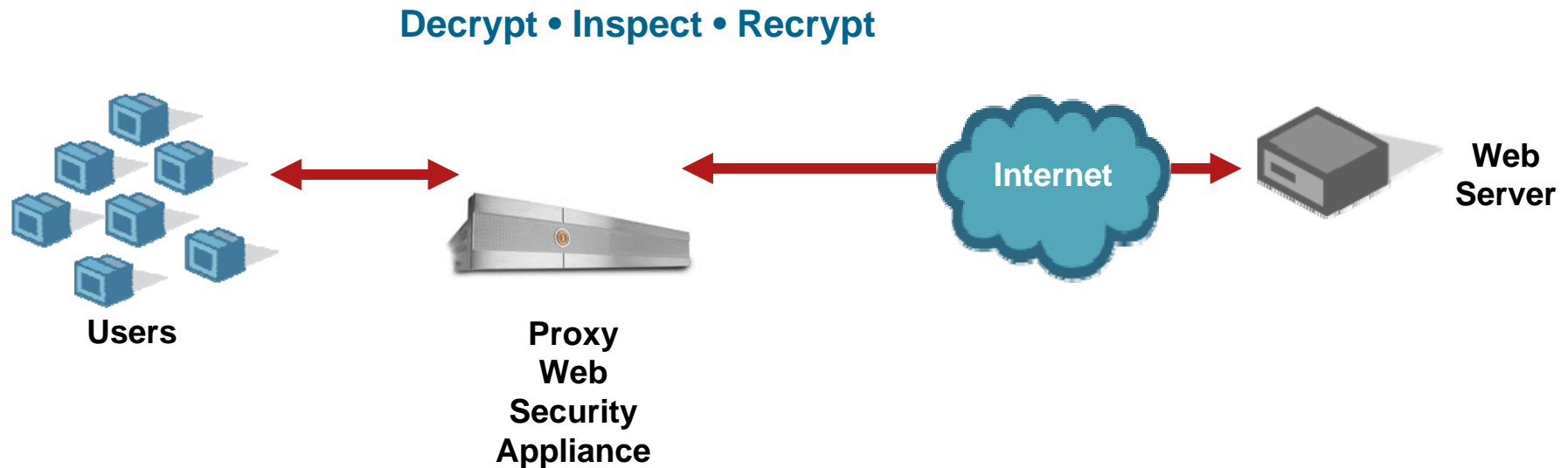
Web Reputation Filtering



- **IronPort Web Reputation** technology determines need for scanning by
 - Decryption Engine
 - IronPort Anti-Malware System™

Selective HTTPS scanning

Reputation-based



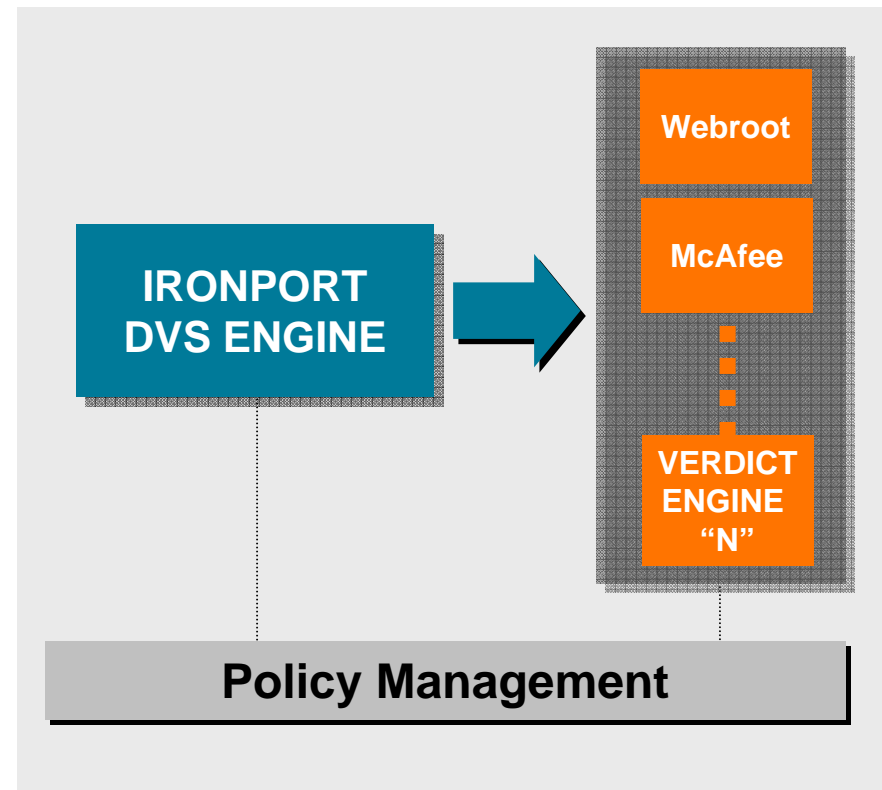
- **Selective HTTPS filtering :**

- Respects the confidentiality of legitimate HTTPS sessions (for example a user checking his bank account on-line)
- Prevents malware downloads using non-legitimate HTTPS traffic

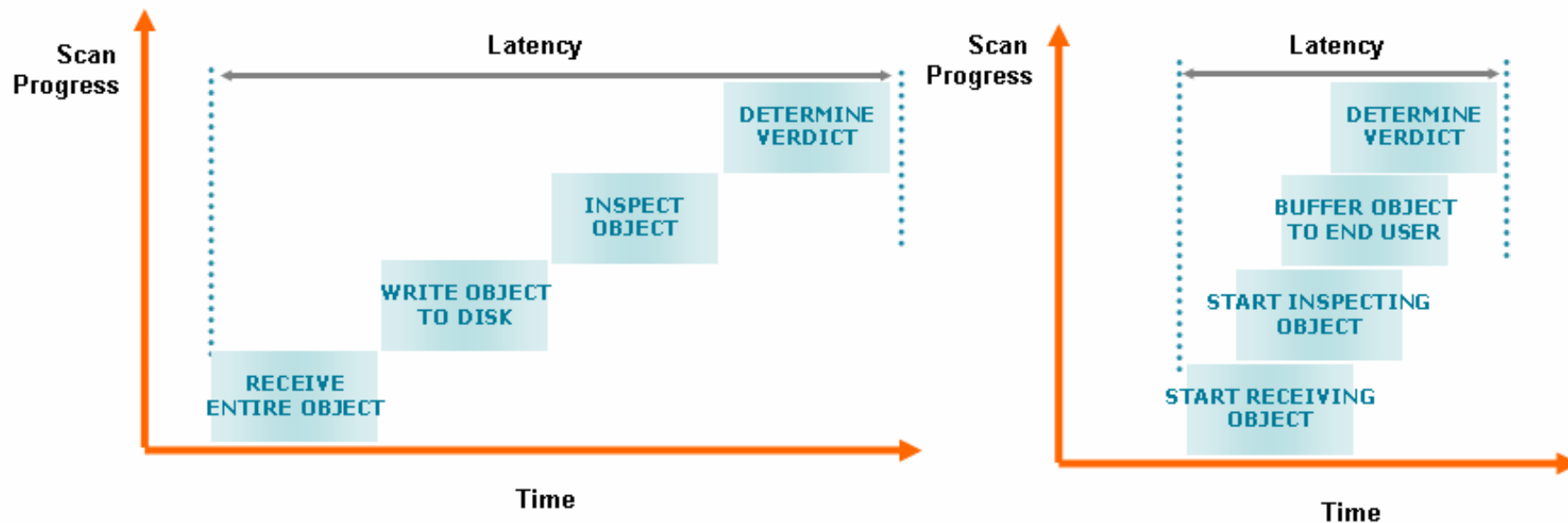
IronPort Anti-Malware System

Multi-Database & Stream Scanning

- DVS Engine : signature-based & multi-database engine including:
 - Webroot (N°1 in Anti-Spyware)
 - McAfee (N°1 in Anti-Virus & 2 in Anti-Spyware)
- High-performance 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

IronPort S-Series

Aurora Health Care Case Study



- **Aurora Health Care's challenge:**
 - 13 Hospitals, 100 clinics, over 30,000 users
 - Significant malware infections
 - Large infrastructure, ~7 servers running Websense
- **IronPort's solution:**
 - Blocked **~2 million** additional suspect transactions per week (downloads.hotbar.com, zedo.com)
 - Spyware filtering accuracy increased by **3x**
 - Replaced **7** servers with **2** IronPort S-Series™ appliances
 - Servers consolidated by **70%**



"... we have been very concerned about the level of malware infections in our network.

The fact that the IronPort S-Series enables us to stop malware at the network edge, while also allowing us to deploy URL filtering policies, is a big advantage for us."

— Tim Sommers

AURORA HEALTH CARE

USERS
PROTECTED

30,000+

Ease of Administration

Web Filtering Policies

Policies						
Order	Group	Applications	URL Categories	Objects	Anti-Malware	Delete
1	QA	Block: FTP Block: User Agents	Block: 52 Monitor: 2 Allow: 0	Block: 256 Mb	(global policy)	
2	Engineering	Block: User Agents	Block: 50 Monitor: 2 Allow: 2	Block: No Max Size Block: Object Types Block: File Types	(disabled)	
3	Marketing ?	(disabled)	Block: 50 Monitor: 2 Allow: 2	Block: No Max Size Block: Object Types	Block: 11 Monitor: 2	
4	Dev ?	(global policy)	Block: 50 Monitor: 2 Allow: 2	Block: No Max Size	(global policy)	
	Global Policy ?	Block: FTP, HTTPS Allow: HTTP Block: User Agents Allow: Ports 443, 21	Block: 46 Monitor: 8 Allow: 0	Block: 256 Mb Block: Object Types Block: File Types	Block: 13 Monitor: 0	

Key: Global Disabled
? Authentication

Web Security Manager
Configuration of policies per groups, users, etc.



Web Security Monitor
Real-time reporting

Centralized Reporting Sawmill

Overview

Statistics for 26/Jun/2007 - 02/Jul/2007, 7 days

	All days	Average per day
Requests	79,829	11,404.14
Page views	71,628	10,232.57
Unique source IPs	7	-
Size	1.85 G	270.73 M

Centralized Reporting
Sawmill



IRONPORT M-SERIES



CONFIGURATION PROFILES

Centralized Configuration Management
IronPort M-Series



DO NOT TRUST US...

TEST US !!

⇒ Free evaluation of the appliances & software

⇒ Subscription to viral alerts :

<http://www.ironport.com/toc/>

⇒ For more information:

fr-info@ironport.com

