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*
  - 1str with *Reputation Filtering*
  - 1st with *Virus Outbreak Filters*

Internet Threats
Latest trends

Phishing is changing

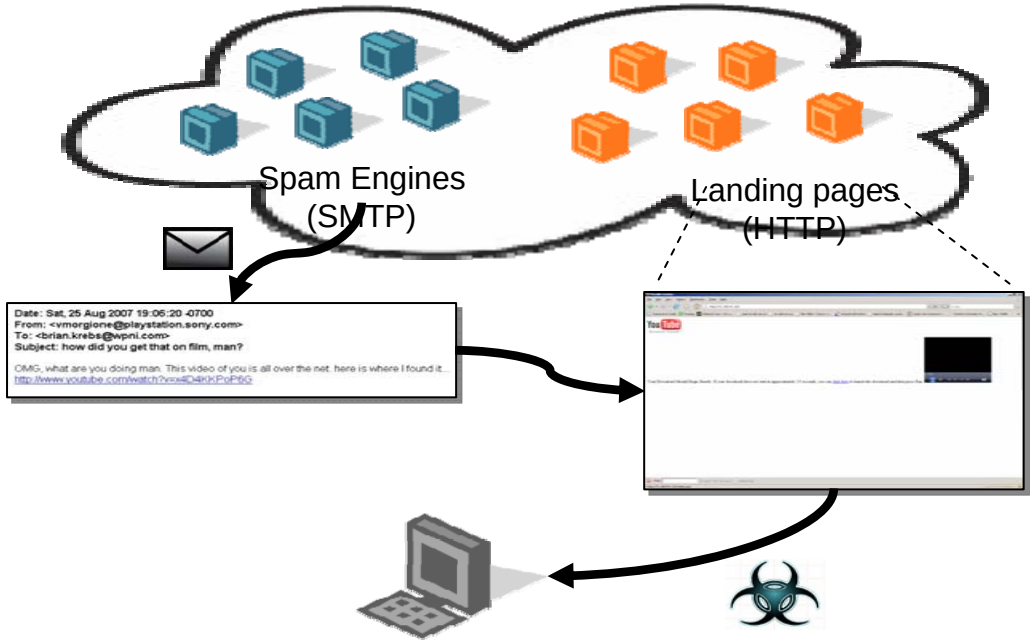
- New trends
  - Pharming
  - Spear phishing : social engineering
  - Typo attacks: www.googkle.com
- 1/3 of phishing sites host malware
- Average on-line time for a phishing site : 3.6 days

Source : Anti-Phishing Working Group

Zombies are changing

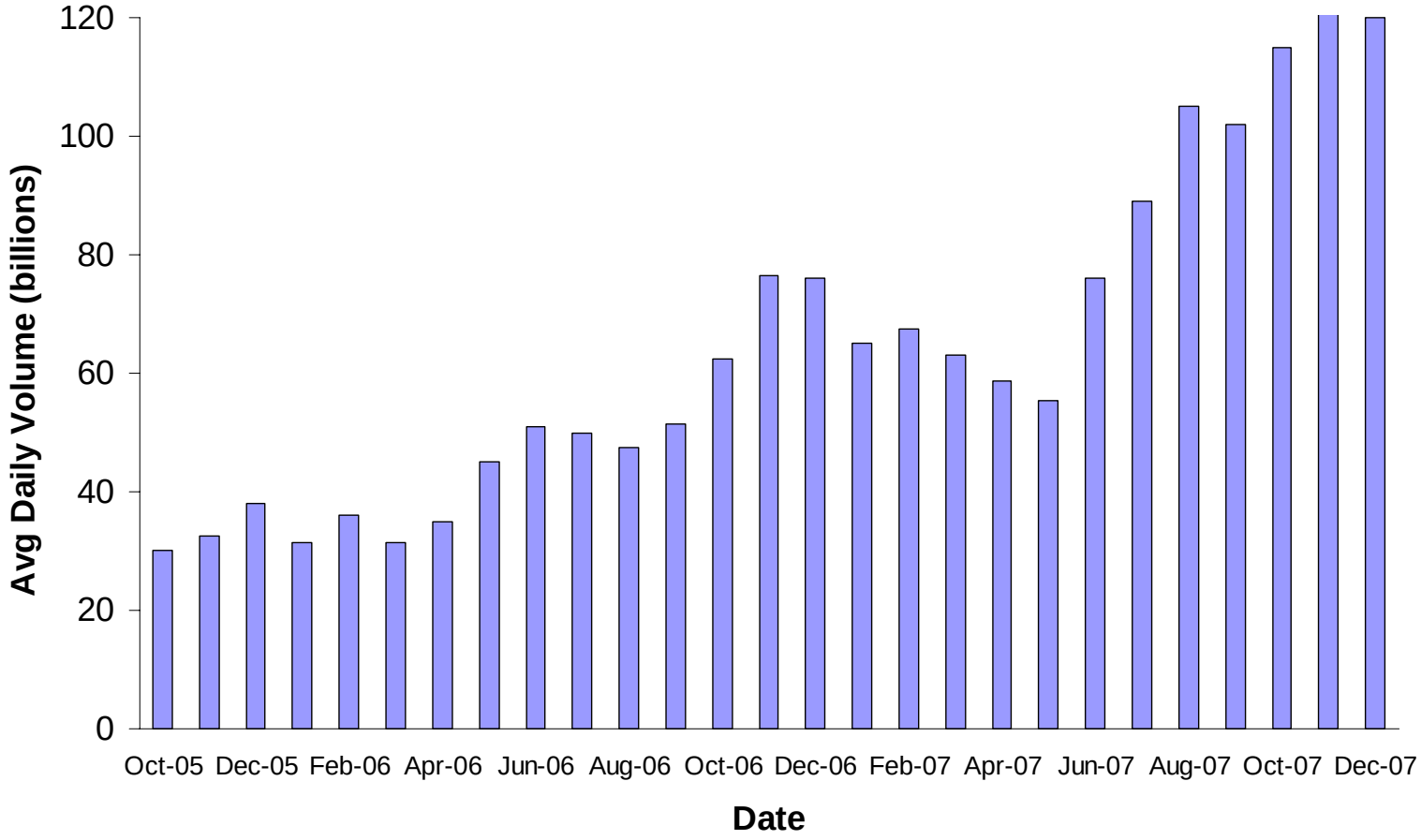
The Storm network

- **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



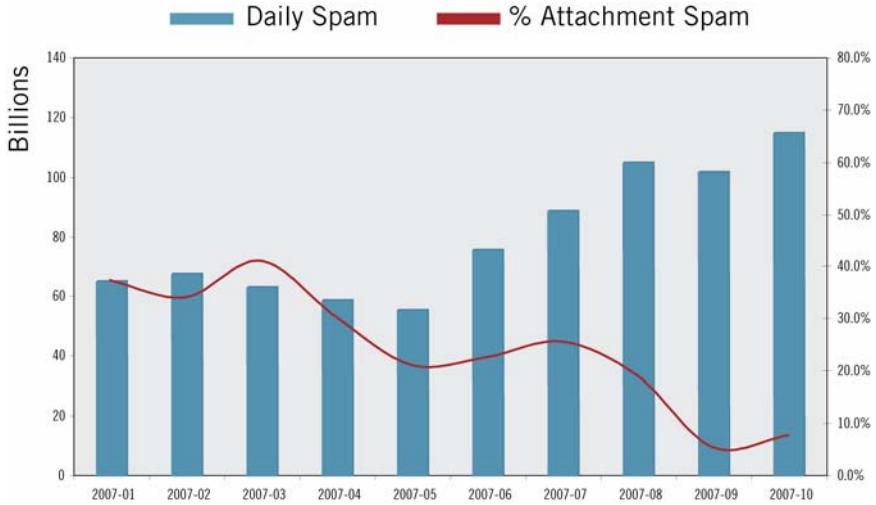
Spam keeps growing!

x4 in 2 years!



Spam techniques are changing

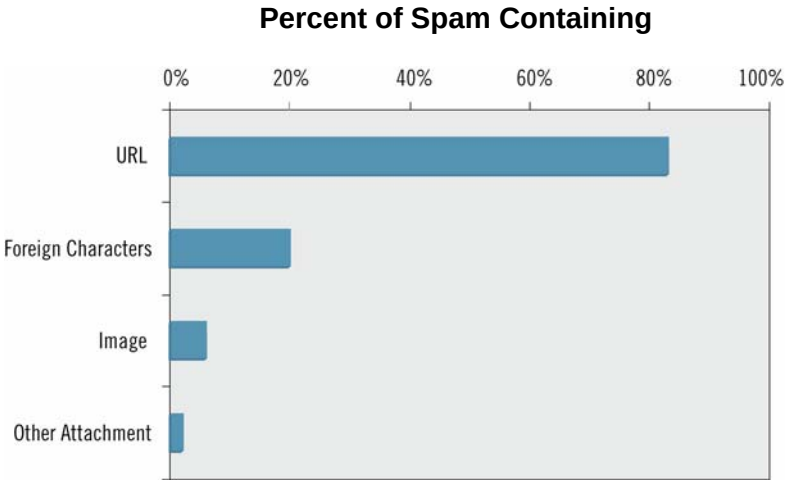
From images to web links



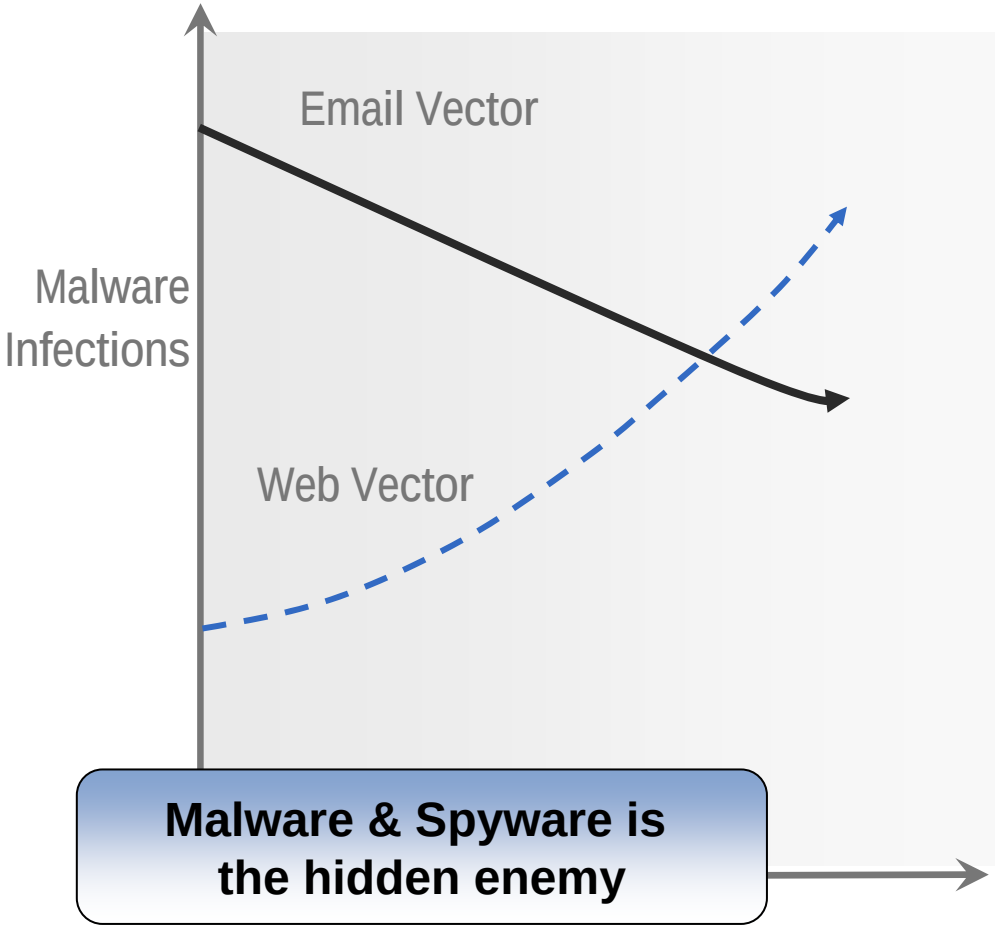
Spam keeps growing, but attachment spam reduces

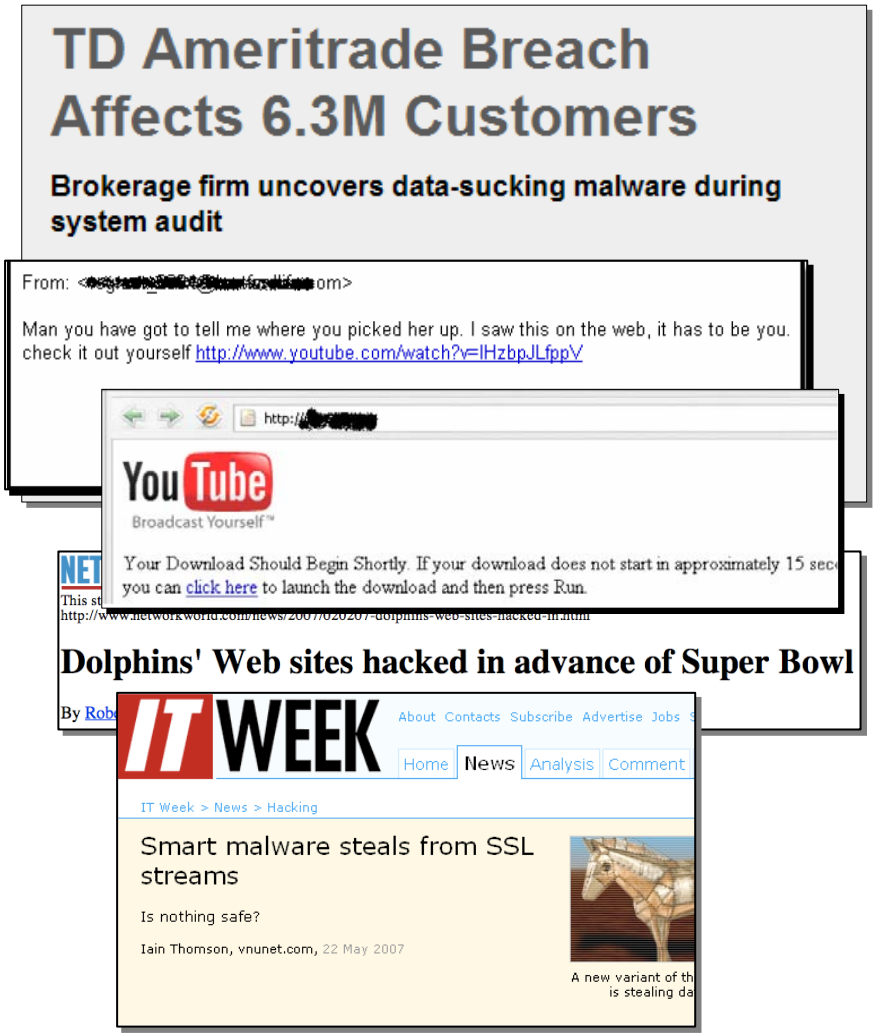
URL spam keeps growing

(+ 253% in 2007 vs 2006)



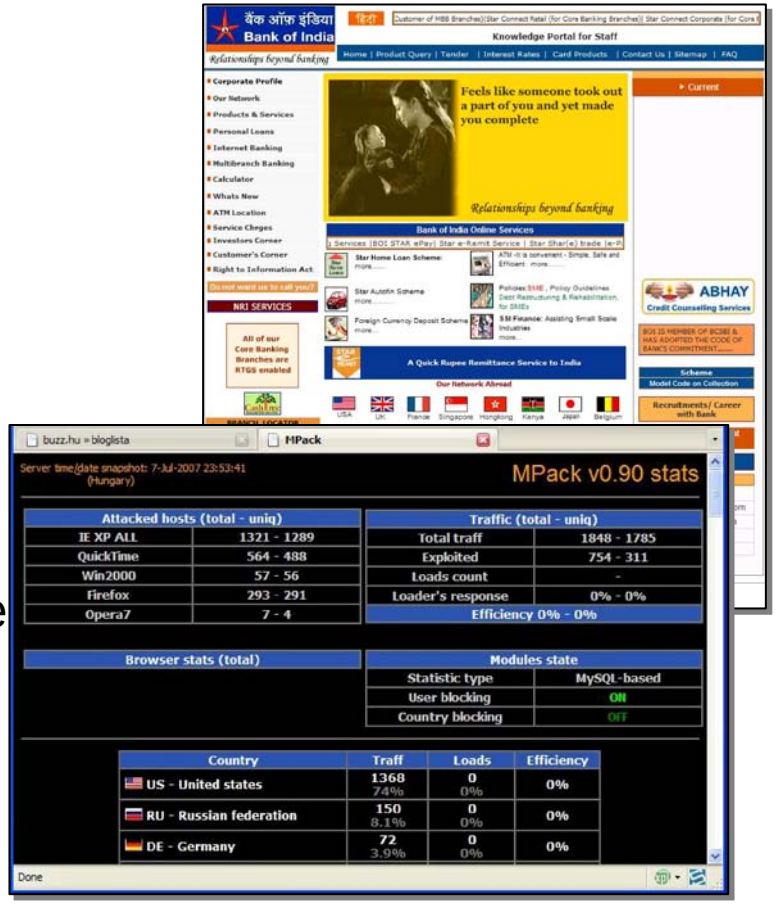
Threat vectors are changing





Legitimate Sites Hacked

- 70% of Web-based infections were found on ‘legitimate’ websites (Google survey, May 2007)
- 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 sur le poste en exploitant une vulnérabilité du navigateur web
- Web 2.0 Sites
  1. The hacker modifies the page with a malicious code la page avec un code
  2. 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

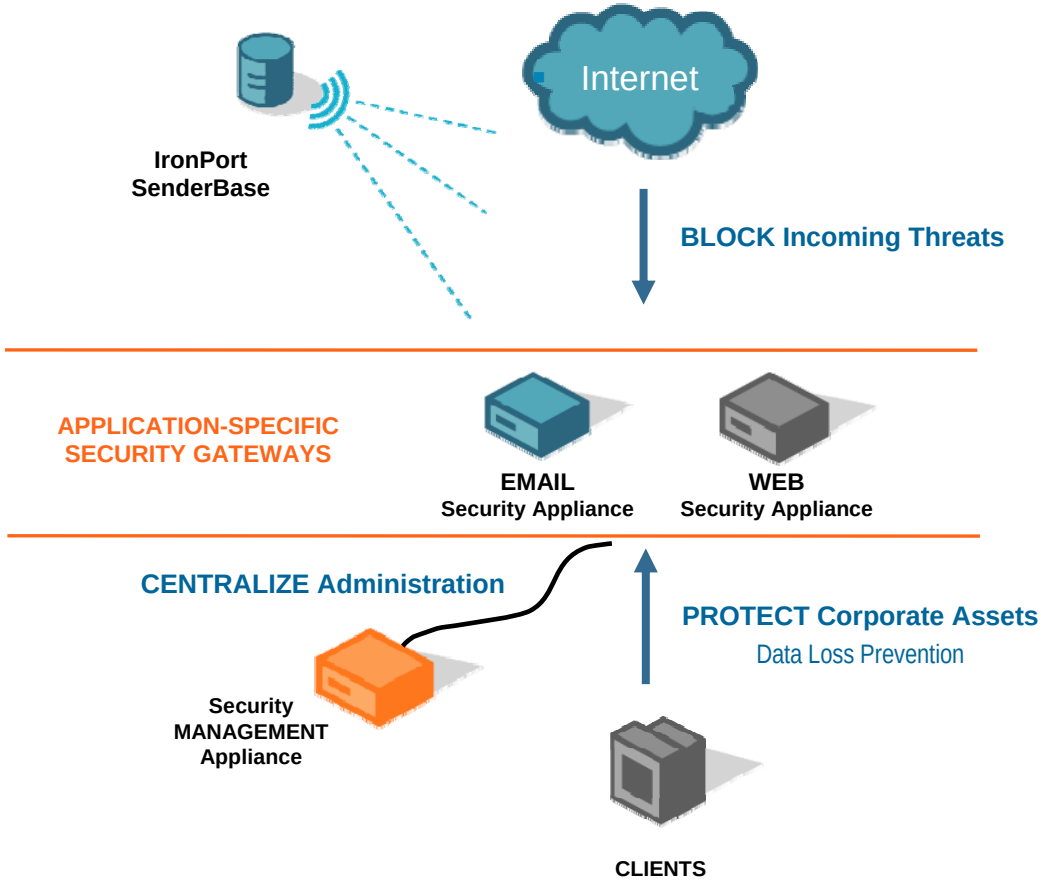
- Regulatory Compliance
  - SOX, HIPAA, GLBA, PCI, etc.

IDC
Analyze the Future

"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

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

E-Mail Reputation Filters → **Reputation Score**

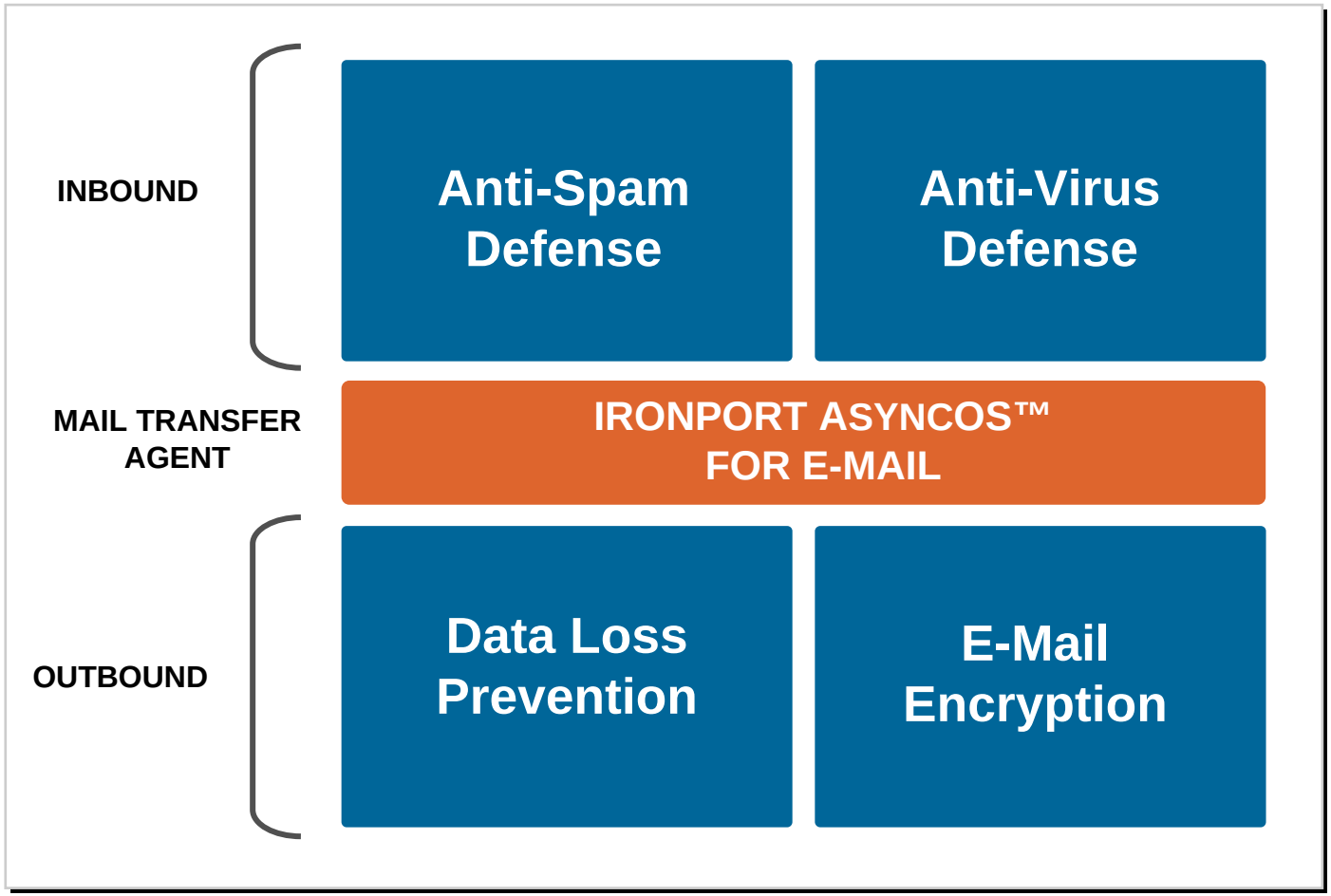
- *URL blacklists & whitelists*
- *HTML Content*
- *Domain Info*
- *Known "bad" URLs*
- *Website history…*

Web Reputation Filters → **Reputation Score**

E-Mail Security
IronPort C-Series

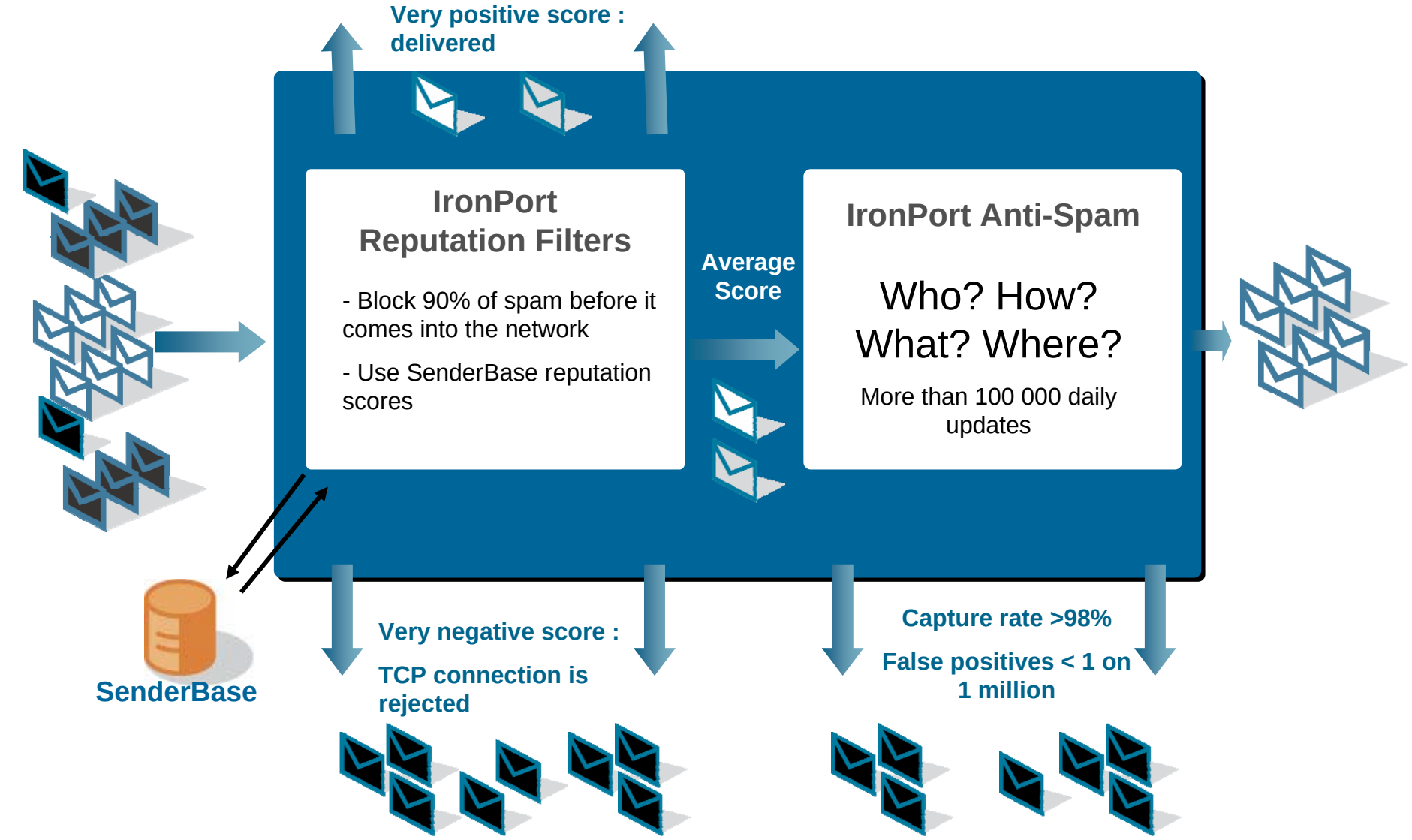
IronPort C-Series

Inbound & Outbound Security



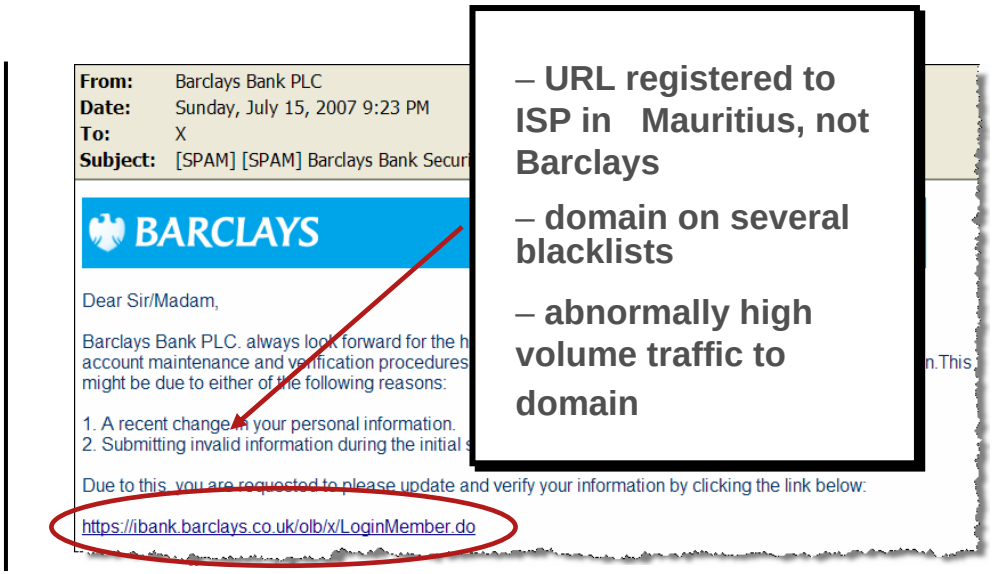
IronPort Spam Defense

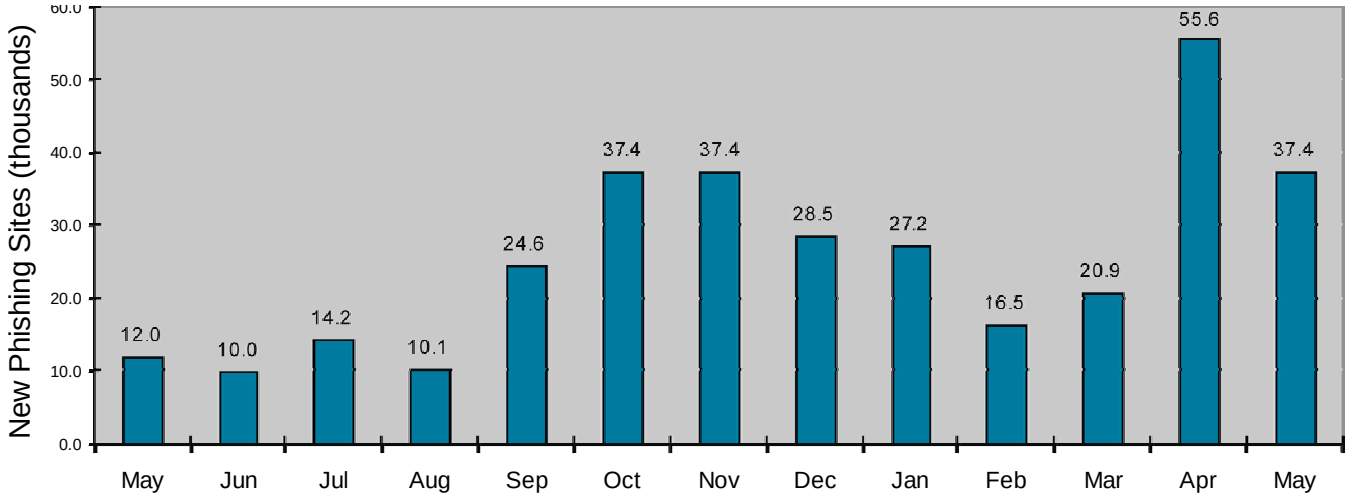
Multi-Layer Protection



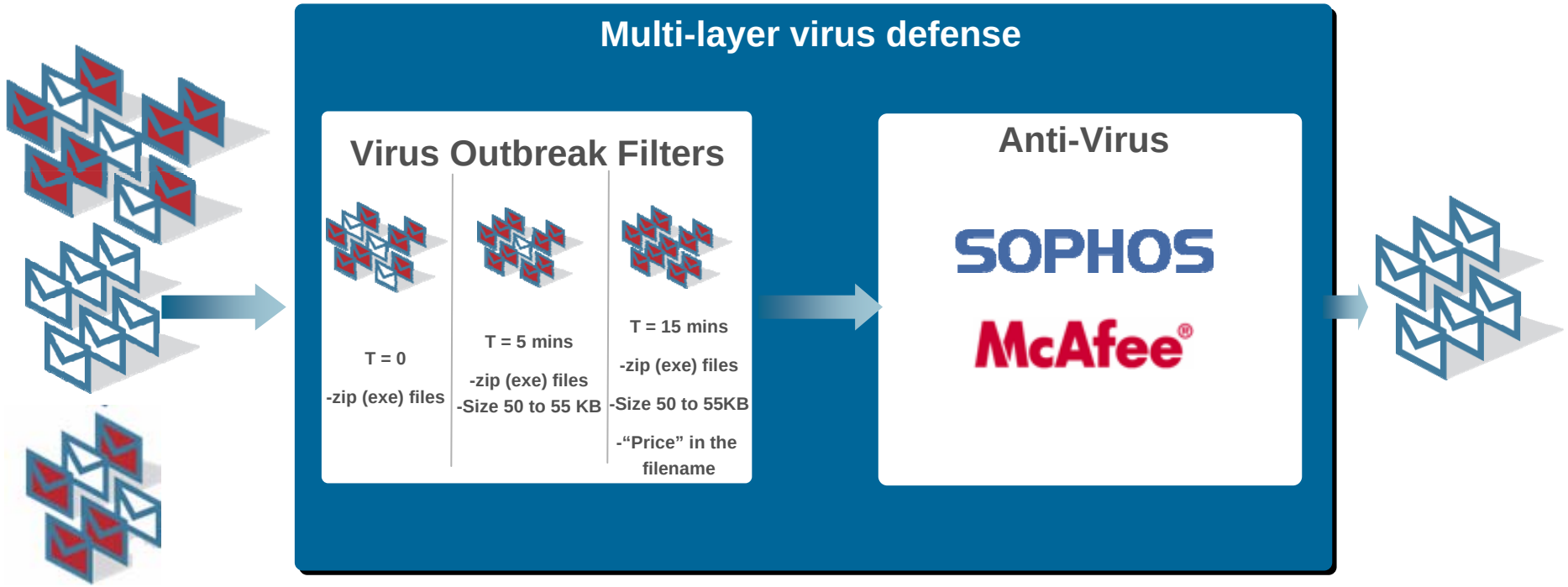
IronPort Stops Phishing

- 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





IronPort Virus Defense



Virus Outbreak Filters Advantage

www.ironport.com/toc

Average lead time on protection *……. over 13 hours

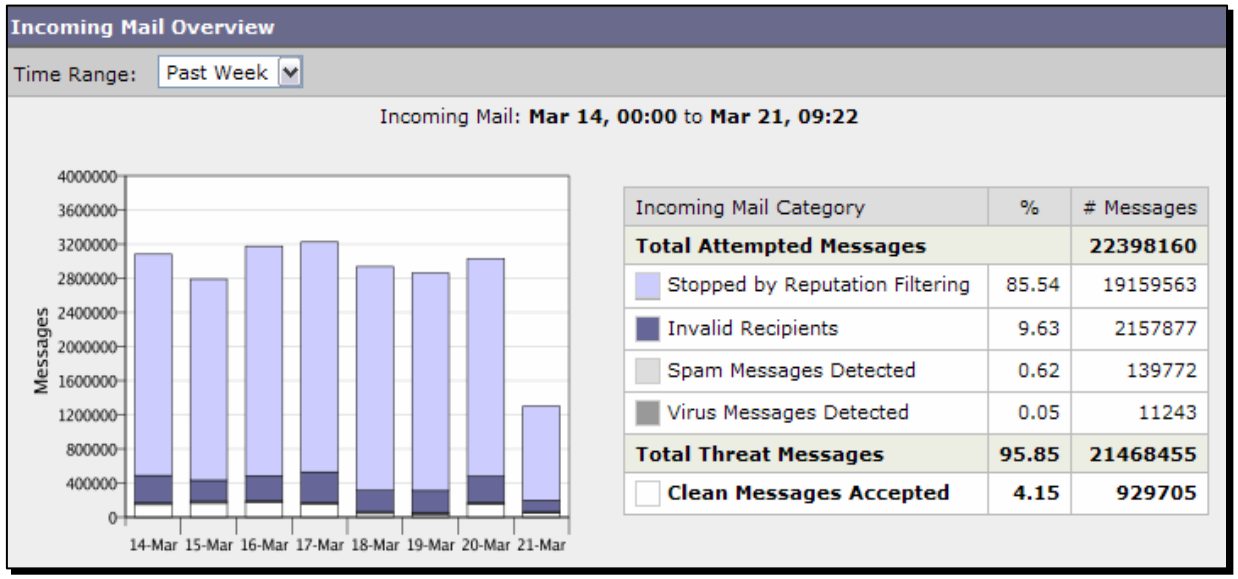
On a total of major outbreaks of * …….. 248 outbreaks

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



Incoming Mail Category	%	# Messages
Total Attempted Messages		**22398160**
Stopped by Reputation Filtering	85.54	19159563
Invalid Recipients	9.63	2157877
Spam Messages Detected	0.62	139772
Virus Messages Detected	0.05	11243
Total Threat Messages	**95.85**	**21468455**
Clean Messages Accepted	**4.15**	**929705**

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

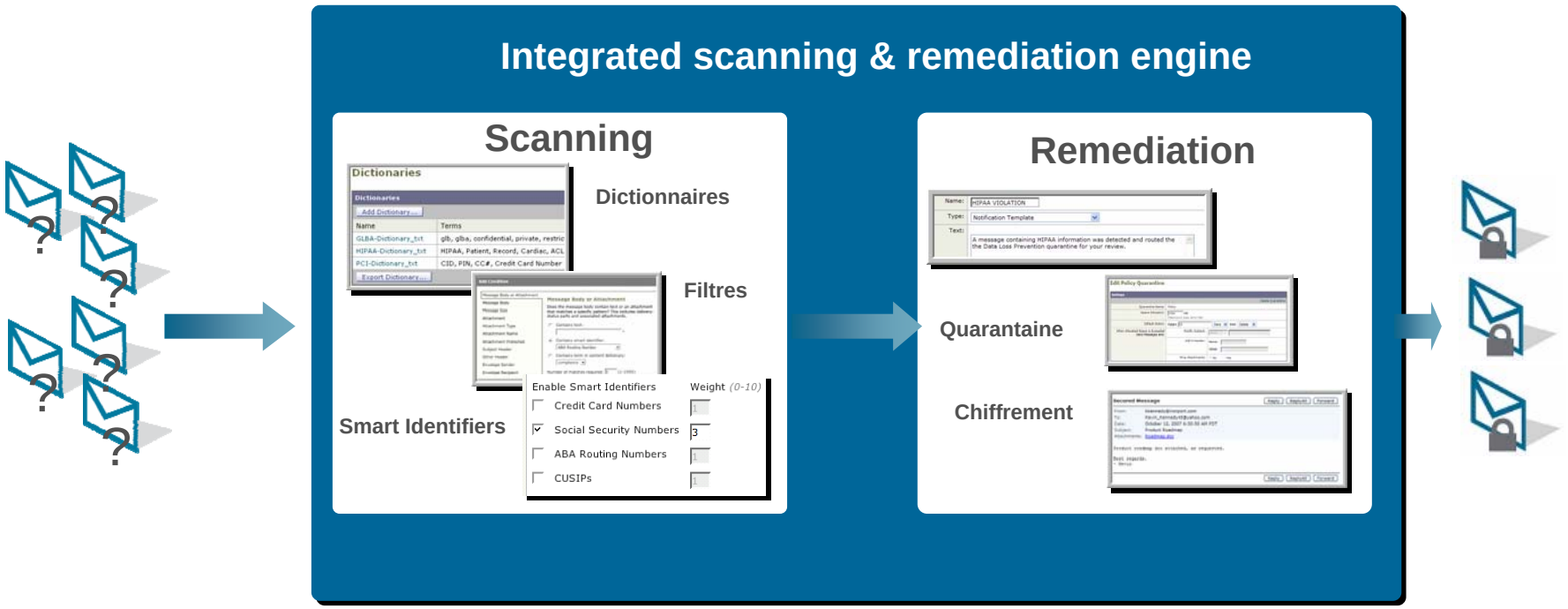
"IronPort has increased the quality and reliability of our network operations, while reducing our costs."

— Tim Helmsetetter
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.

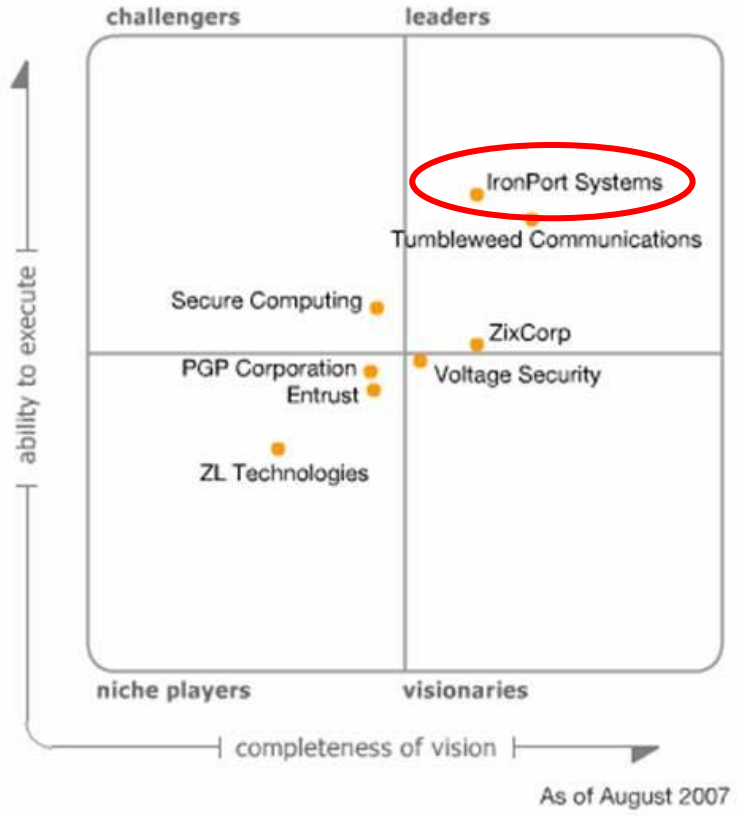
Remediation : alerts, reporting, quarantine, encryption…

IronPort Encryption Overview

Approved by the analysts…

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

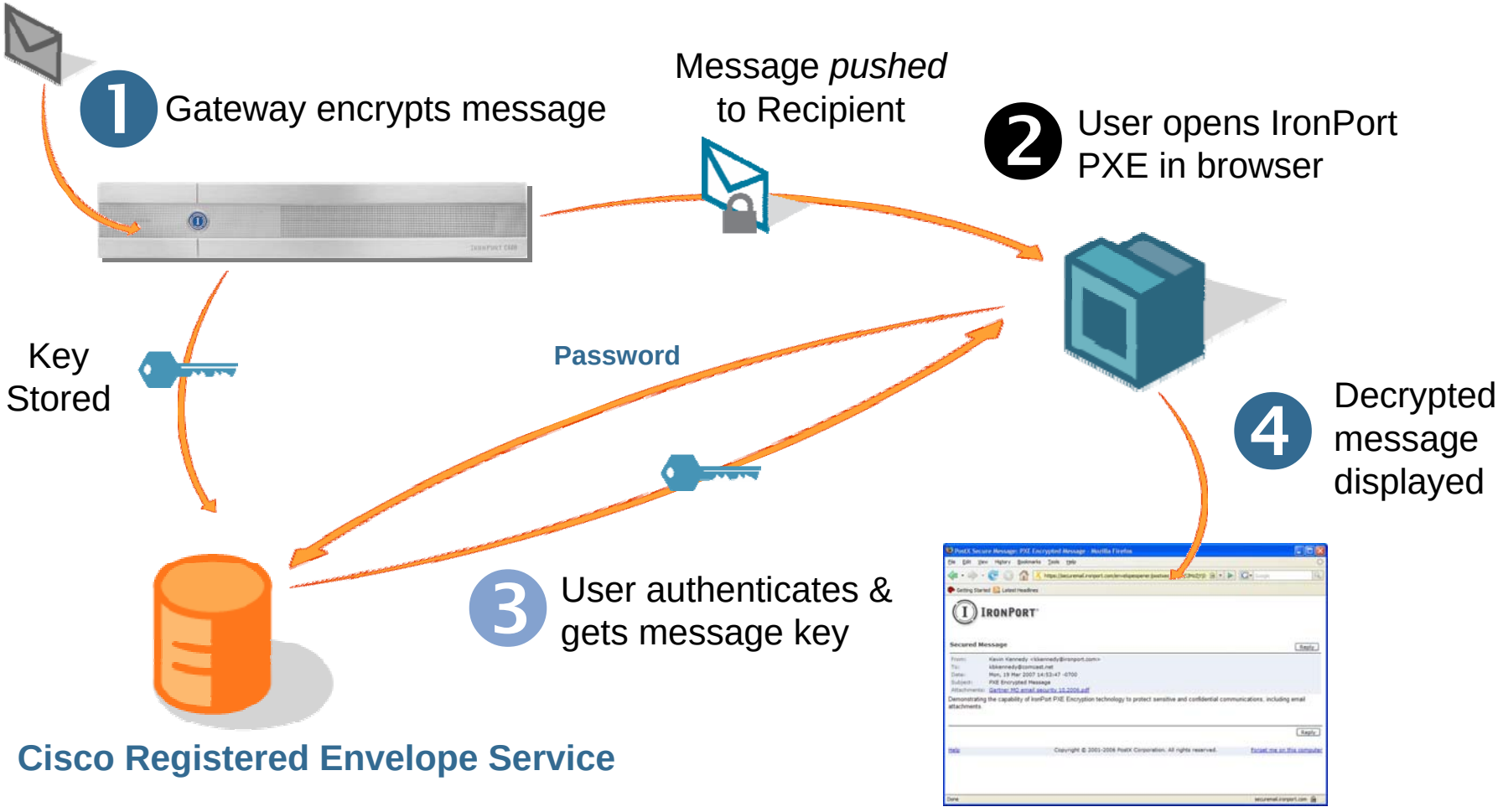
1. Without the need for the recipient to install software
2. Regardless of the e-mail platform & OS used by the recipient



Source: Gartner "Magic Quadrant" E-Mail Encryption

IronPort E-Mail Encryption

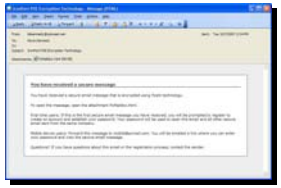
How does it work?



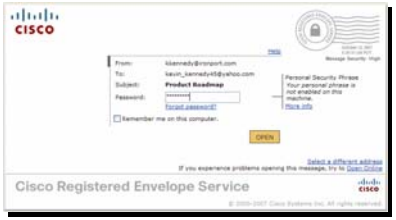
IronPort PXE: Receiving a Message

Seamless End-User Experience

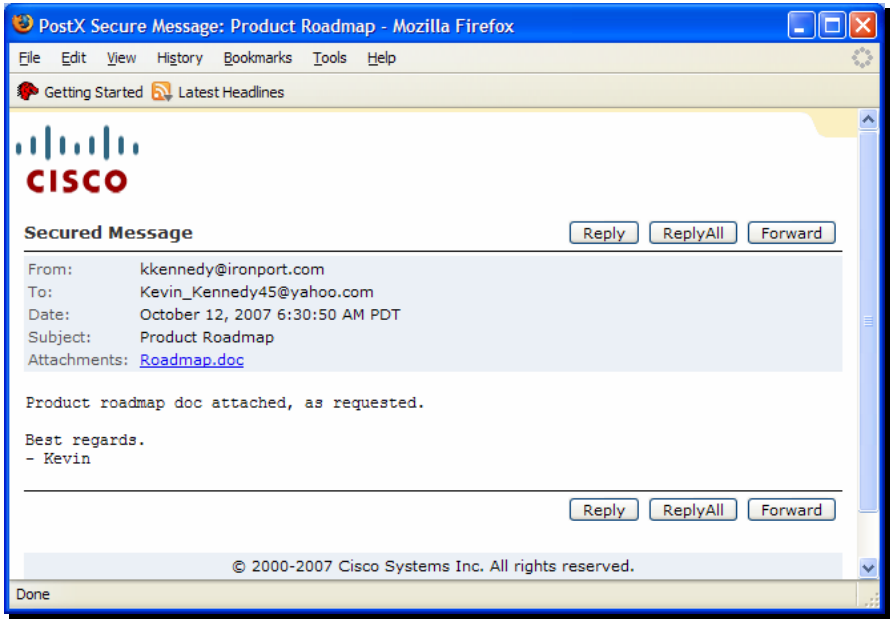
1. Open Attachment



2. Enter password

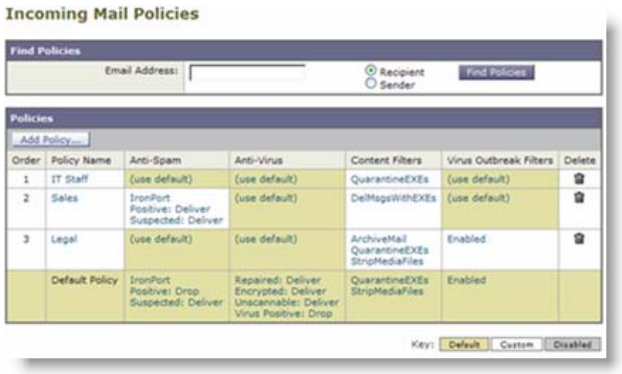


3. View message



Ease of administration

5-Step installation



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

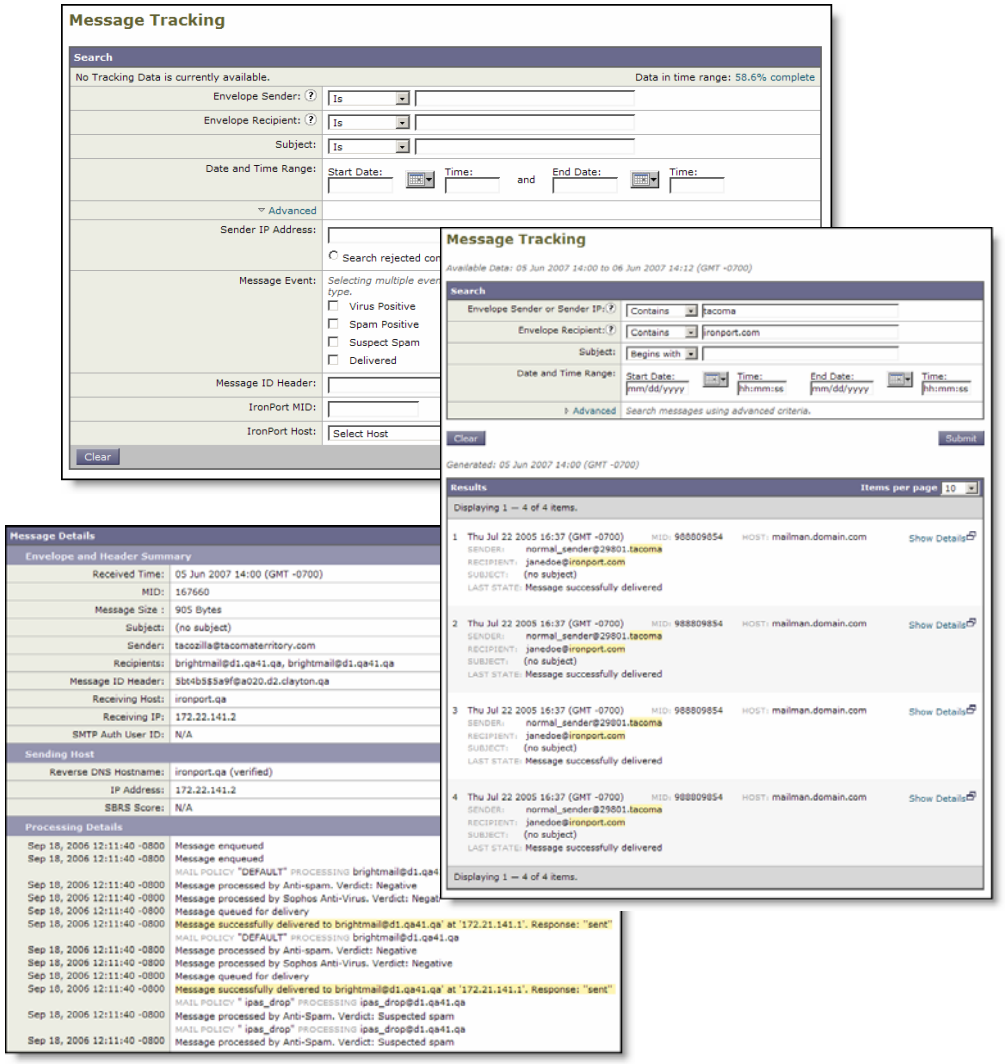
Tracking of the messages

E-Mail Security Monitor
Real-time reporting

IronPort M-Series

Centralized Spam Quarantine, Reporting & Tracking

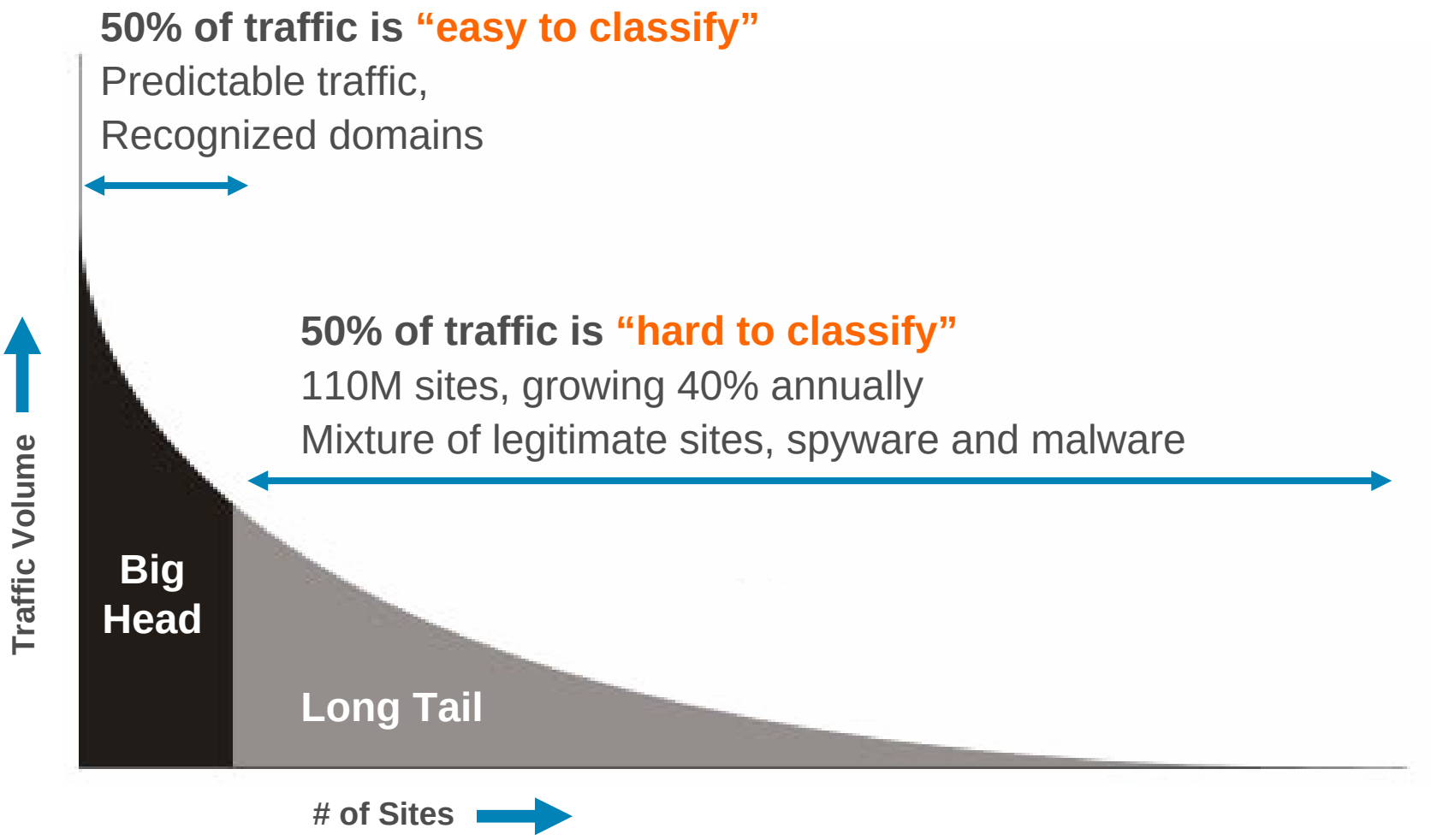
- IronPort Email Security Monitor reports centrally available on IronPort M-Series
- Reports on C-Series appliances managed (system capacity, functioning, etc.)
- Stores more than 1 year of data
- Centralized tracking of messages
- Centralized Spam Quarantine



Web Security
IronPort S-Series

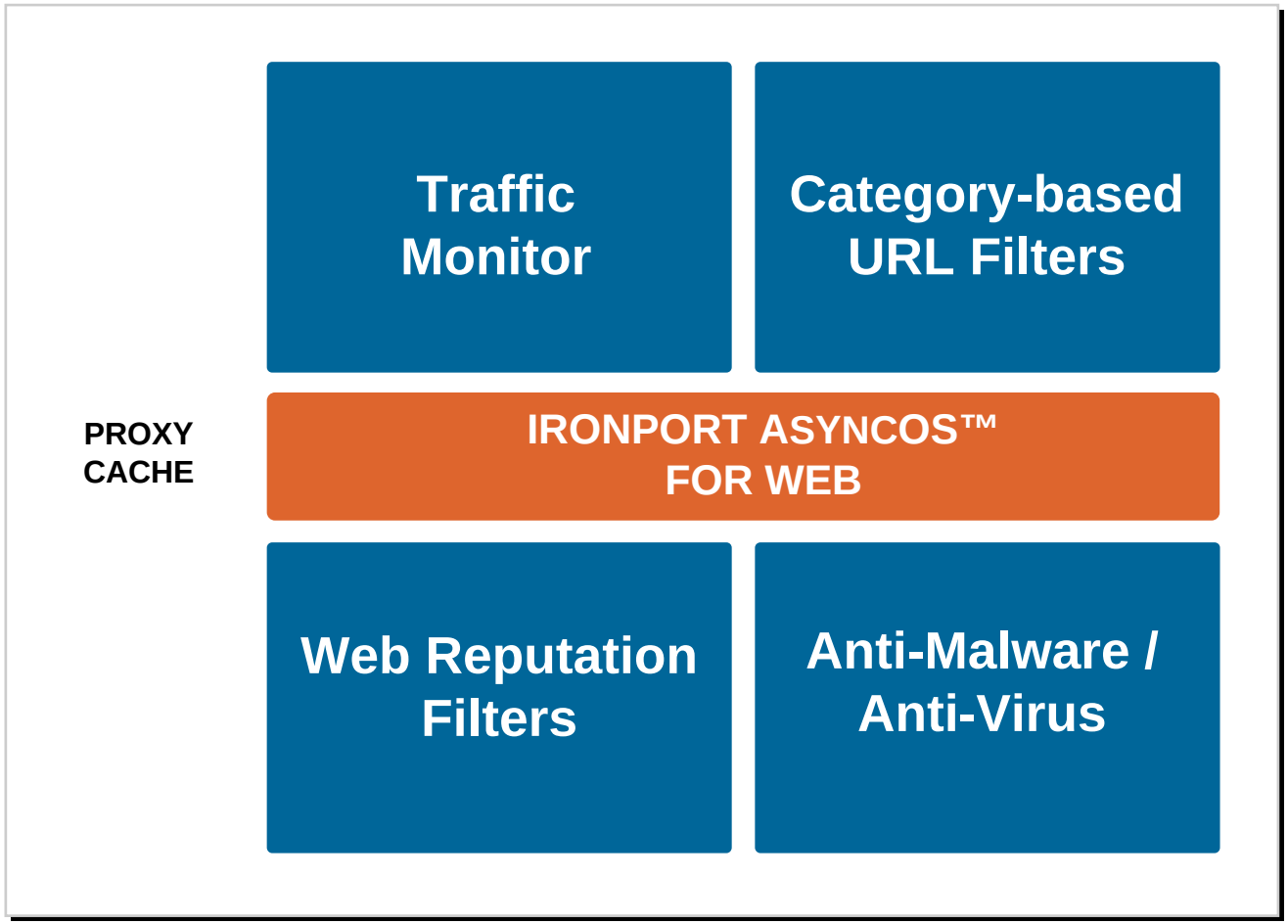
Web Traffic

How to protect according to its nature?



IronPort S-Series

Architecture



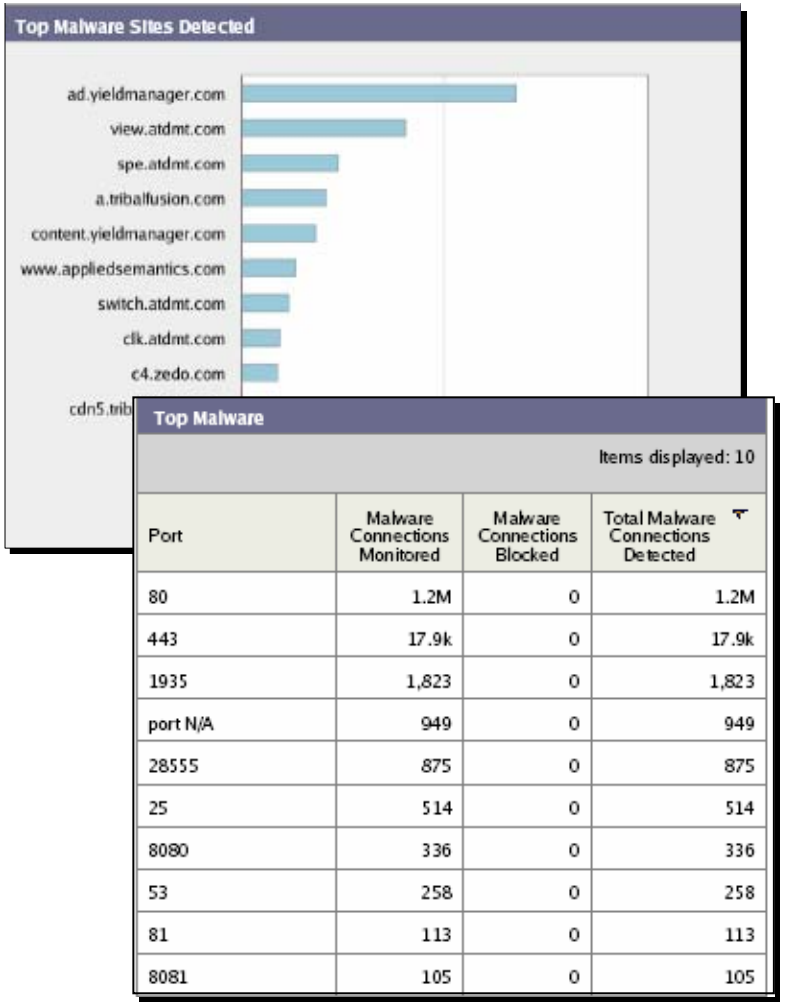
Detecting Existing Client Infections

Monitoring "Phone Home" Traffic

- Detects all spyware/Trojan communication with an external server

  Scans all traffic, all ports, all protocols

- Compare contacted external IP adresses with a "command & control servers" blacklist
- Automatically updated anti-malware rules
- « Monitor » or « Monitor & Block » modes



Port	Malware Connections Monitored	Malware Connections Blocked	Total Malware Connections Detected
80	1.2M	0	1.2M
443	17.9k	0	17.9k
1935	1,823	0	1,823
port N/A	949	0	949
28555	875	0	875
25	514	0	514
8080	336	0	336
53	258	0	258
81	113	0	113
8081	105	0	105

IronPort URL Filters

Leading Accuracy and Control

- Enterprise-class database

  52 categories, over 21 million sites, ~3.5 billion webpages

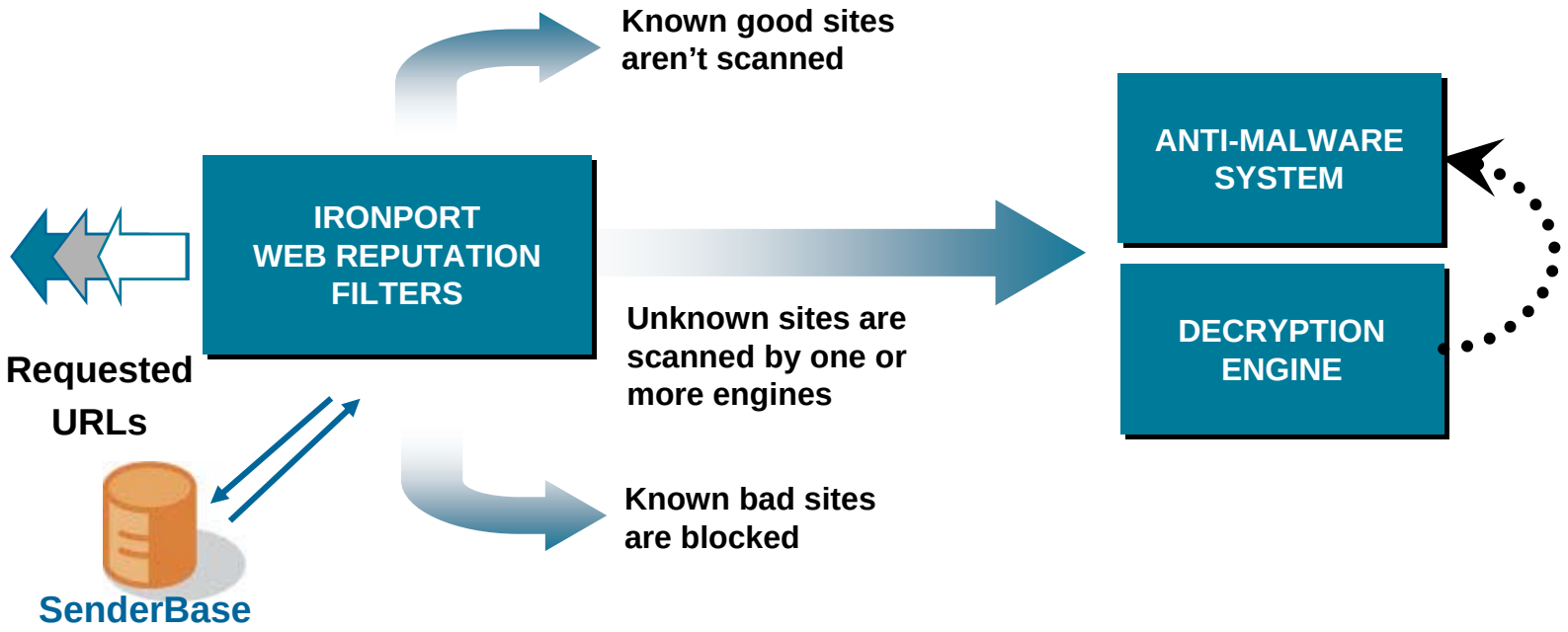
  1/3 of the database is international

- 24 x 7 monitoring
- Regular, automated updates
- Flexible policy management

  Per user, per group policies

  Monitor only mode

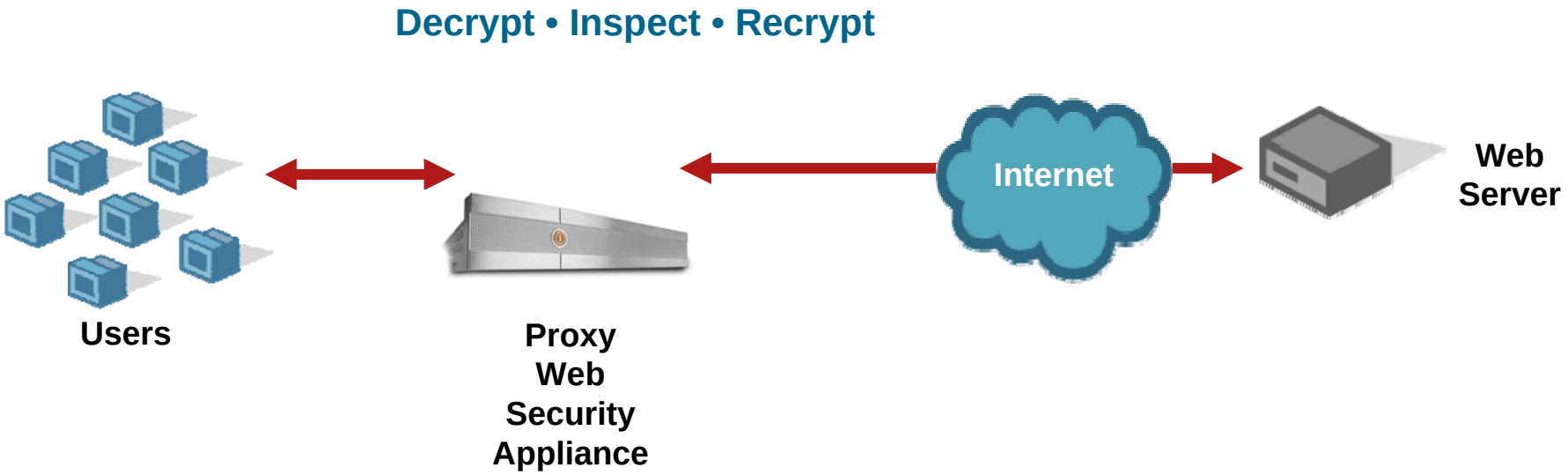
Web Reputation Filtering



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

Selective HTTPS scanning

Reputation-based



- **Selective HTTPS filtering** :

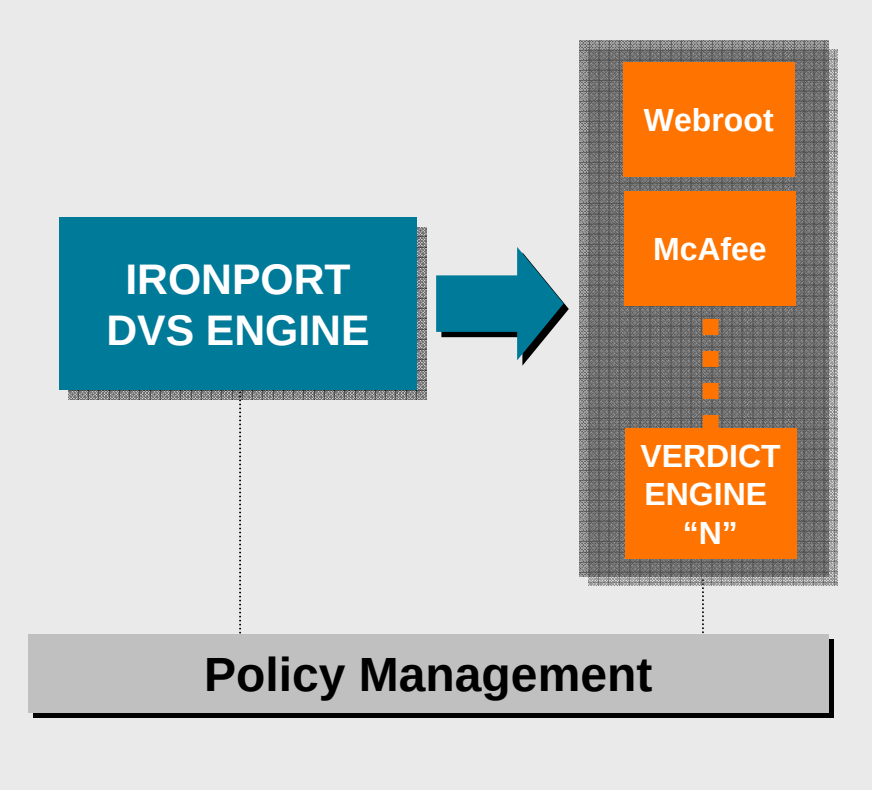
  - Respects the confidentiality of legitimate HTTPS sessions (for example a user checking his bank account on-line)

  - Prevents malware downloads using non-legitimate HTTPS traffic

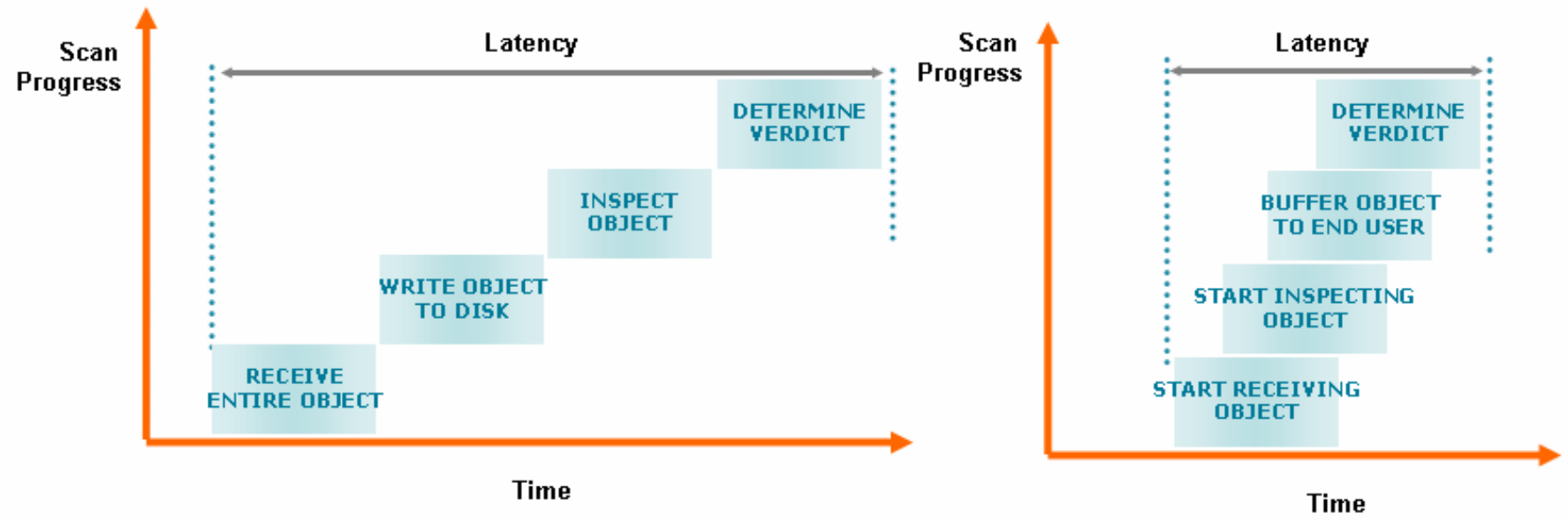
IronPort Anti-Malware System

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%**

Aurora Health Care®

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

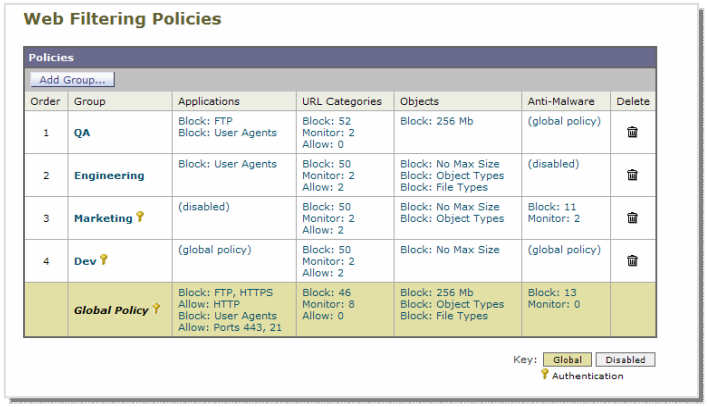
The fact that the IronPort S-Series enables us to stop malware at the network edge, while also allowing us to deploy URL filtering policies, is a big advantage for us."

— Tim Sommers

AURORA HEALTH CARE

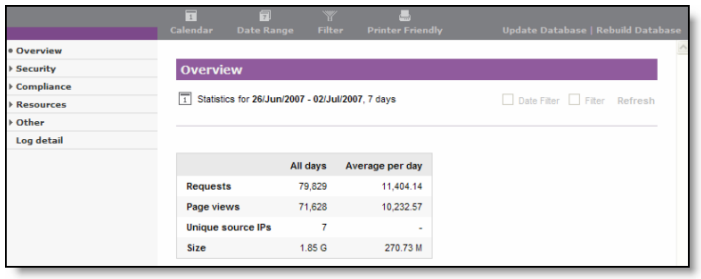
USERS PROTECTED	30,000+

Ease of Administration

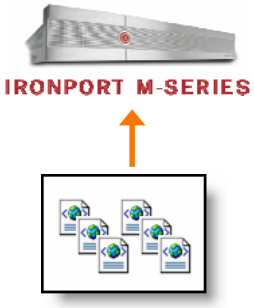


Web Security Manager
Configuration of policies per groups, users, etc.

Web Security Monitor
Real-time reporting



Centralized Reporting
Sawmill



CONFIGURATION PROFILES

Centralized Confirguration 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