



**Contrer les menaces  
Internet  
*E-Mail & Web***

*Cisco Expo  
Alger le 27 Mai 2008*



**Denis Gadonnet**

***Territory Manager – Mediterranean Area***

**IronPort Systems, A Cisco Business Unit**

IronPort is now  
part of Cisco.



---

# Agenda

- Menaces Internet : les tendances
- Sécurité E-Mail : IronPort Série C
- Sécurité Web : IronPort Série S

# IronPort

## Qui sommes-nous?



- **Présence mondiale**
  - Société créée en 2000, désormais BU de Cisco
  - Siège mondial près de San Francisco
  - 45 bureaux répartis dans 35 pays
  - 645 personnes
- **Leadership / analystes**
  - Reconnu comme leader par Gartner, Radicati, IDC, etc.
- **Leadership / marché**
  - 325 millions de boîtes aux lettres protégées
  - Plus de 7000 clients dans 85 pays, dont: -
  - 54 des 100 plus grandes sociétés mondiales
  - 12 des 15 plus grands ISP mondiaux
  - 7 des 10 plus grandes banques mondiales
- **Leadership technologique**
  - 1<sup>er</sup> à développer un MTA hautes performances
  - SenderBase: la plus grande base de monitoring*
  - 1<sup>er</sup> avec *Reputation Filtering*
  - 1<sup>er</sup> avec *Virus Outbreak Filters*

# Menaces liées à Internet : les tendances

# Le phishing change

- Nouvelles tendances
  - Pharming
  - Spear phishing : social engineering
  - Attaques dites d'erreur typographique : [www.google.com](http://www.google.com)
- 1/3 des sites phishing hostent désormais du malware
- Les sites de phishing restent en ligne en moyenne 3,6 jours



Source : Anti-Phishing Working Group

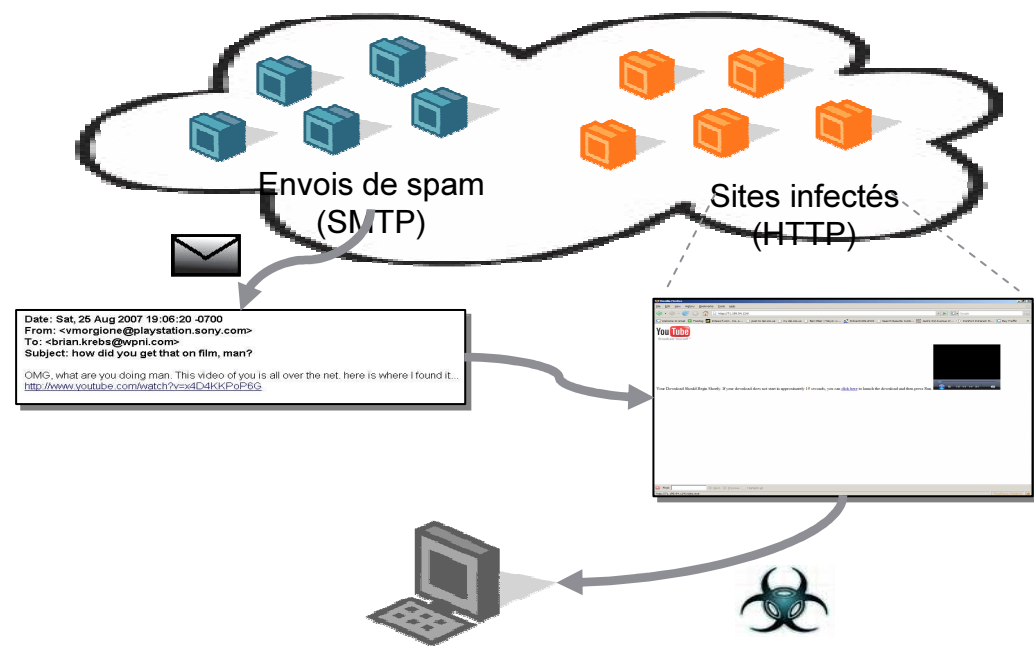
# Les zombies changent

## Le réseau Storm

- **Le plus important réseau de zombies sur Internet**

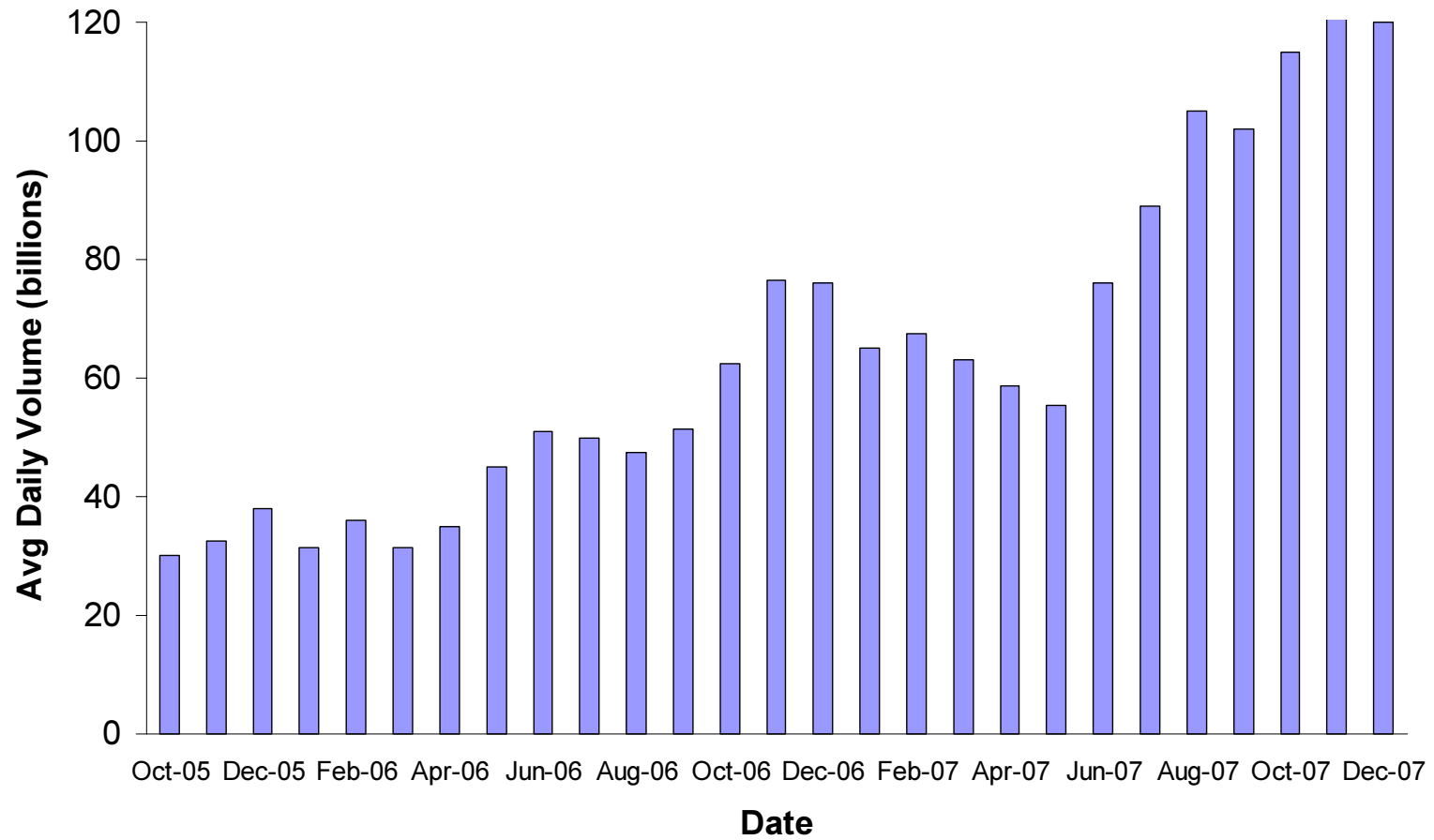
1000 PC infectés loués \$220 en Allemagne  
1000 PC infectés aux USA proposés à \$110  
Accès loués à l'heure, support téléphonique disponible

- **Se reproduit** : envoi de spam de recrutement de zombies
- **Coordonné** : synchronise des envoi de spams par certains zombies avec des sites infectés sur d'autres zombies
- **Peer-to-Peer** : utilise le peer-to-peer pour communiquer (plus de serveurs de contrôle)
- **Réutilisable** : Spam, phishing, dénis de service, etc.
- **Se défend** : par des attaques de déni de service contre ceux qui l'étudient de trop près



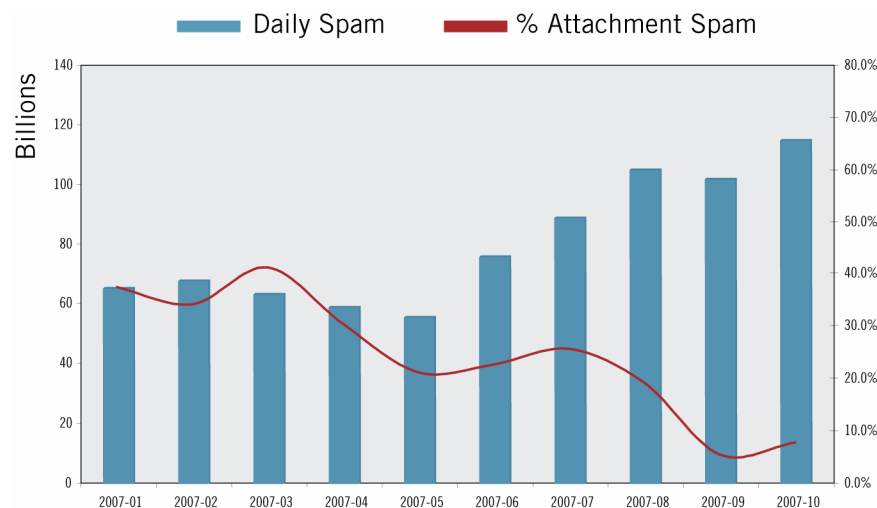
# Le Spam continue à croître

*x4 en 2 ans !*



# Les techniques de spam changent

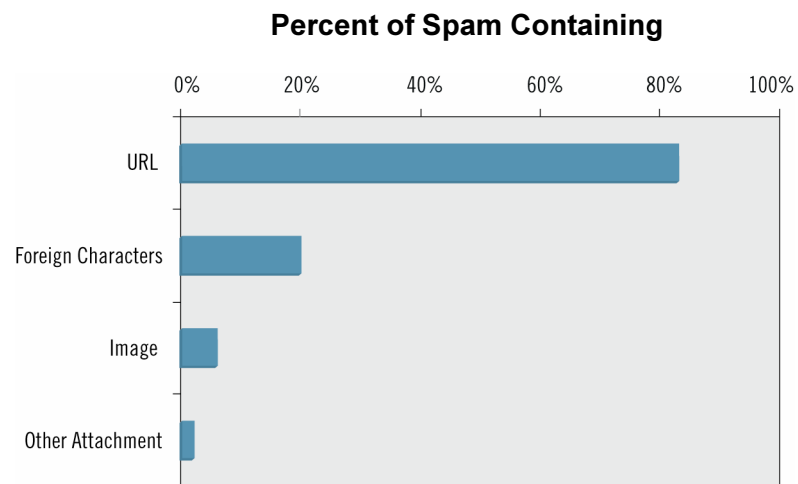
Des images aux liens Web



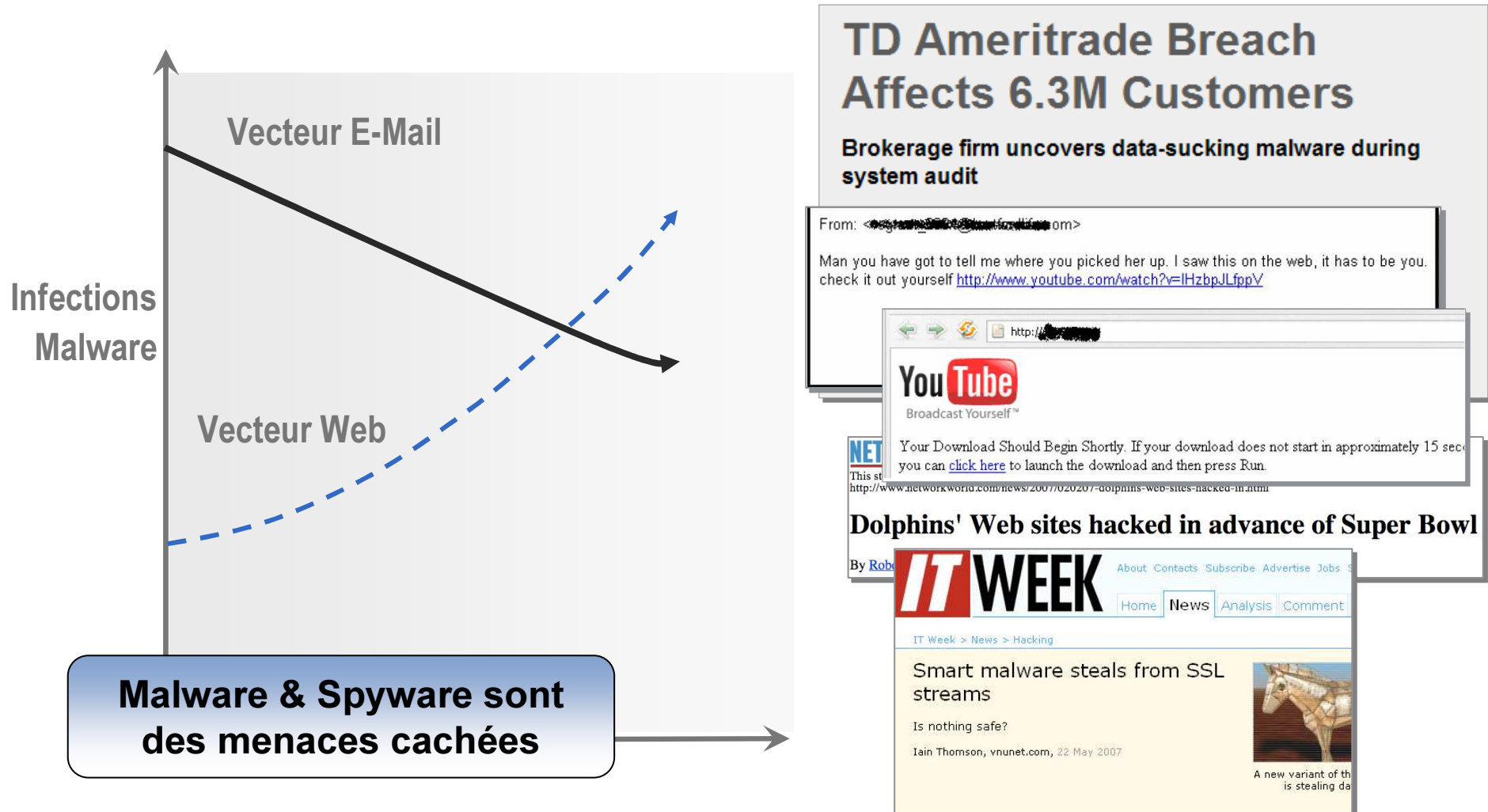
Le spam croît,  
mais la part des fichiers  
attachés diminuent

Le spam contenant des URL  
continue à croître

(+ 253% en 2007 vs 2006)



# Les vecteurs de menaces changent



# Les sites légitiment distribuent le malware

- 70% des infections Web viennent de sites 'légitimes' (étude Google Mai 2007)
- Attaques iFrame
  1. Un site légitime est compromis (ajout d'1 iFrame sur une page)
  2. L'utilisateur est redirigé par l'iFrame vers un site infecté
  3. Un malware se télécharge automatiquement sur le poste en exploitant une vulnérabilité du navigateur web
- Sites Web 2.0
  1. Le pirate modifie la page avec un code HTML malicieux
  2. Les utilisateurs sont touchés par ce code qui les redirige potentiellement vers un site malicieux

A screenshot of the MPAck v0.90 stats interface. It displays various statistics including attacked hosts, traffic, browser stats, and modules state. The interface is dark-themed with blue and white text.

| Attacked hosts (total - uniq) |             | Traffic (total - uniq) |             |
|-------------------------------|-------------|------------------------|-------------|
| IE XP ALL                     | 1321 - 1289 | Total traff            | 1848 - 1785 |
| QuickTime                     | 564 - 488   | Exploited              | 754 - 311   |
| Win2000                       | 57 - 56     | Loads count            | -           |
| Firefox                       | 293 - 291   | Loader's response      | 0% - 0%     |
| Opera7                        | 7 - 4       | Efficiency             | 0% - 0%     |

| Browser stats (total) |             | Modules state |    |
|-----------------------|-------------|---------------|----|
| Statistic type        | MySQL-based | User blocking | ON |
| Country blocking      | OFF         |               |    |

| Country                 | Traff       | Loads   | Efficiency |
|-------------------------|-------------|---------|------------|
| US - United states      | 1368<br>74% | 0<br>0% | 0%         |
| RU - Russian Federation | 150<br>8.1% | 0<br>0% | 0%         |
| DE - Germany            | 72<br>3.9%  | 0<br>0% | 0%         |

# Comment contrôler les données ?

## *L'e-mail : un vecteur majeur de fuites*

- Protection des données sensibles

  - Données personnelles ou financières

  - Propriété intellectuelle

  - Sécuriser les échanges avec les partenaires commerciaux ou les clients

  - Bloquer les communications avec des destinataires sensibles (concurrents, etc.)



- Politique d'utilisation acceptable de l'e-mail

  - Bloquer selon la taille, le type ou le contenu des fichiers attachés

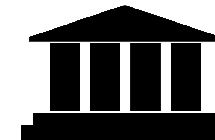
  - Bloquer les contenus inappropriés

  - Ajouter des bas de page ou des mentions légales aux messages sortants



- Conformité aux règlements

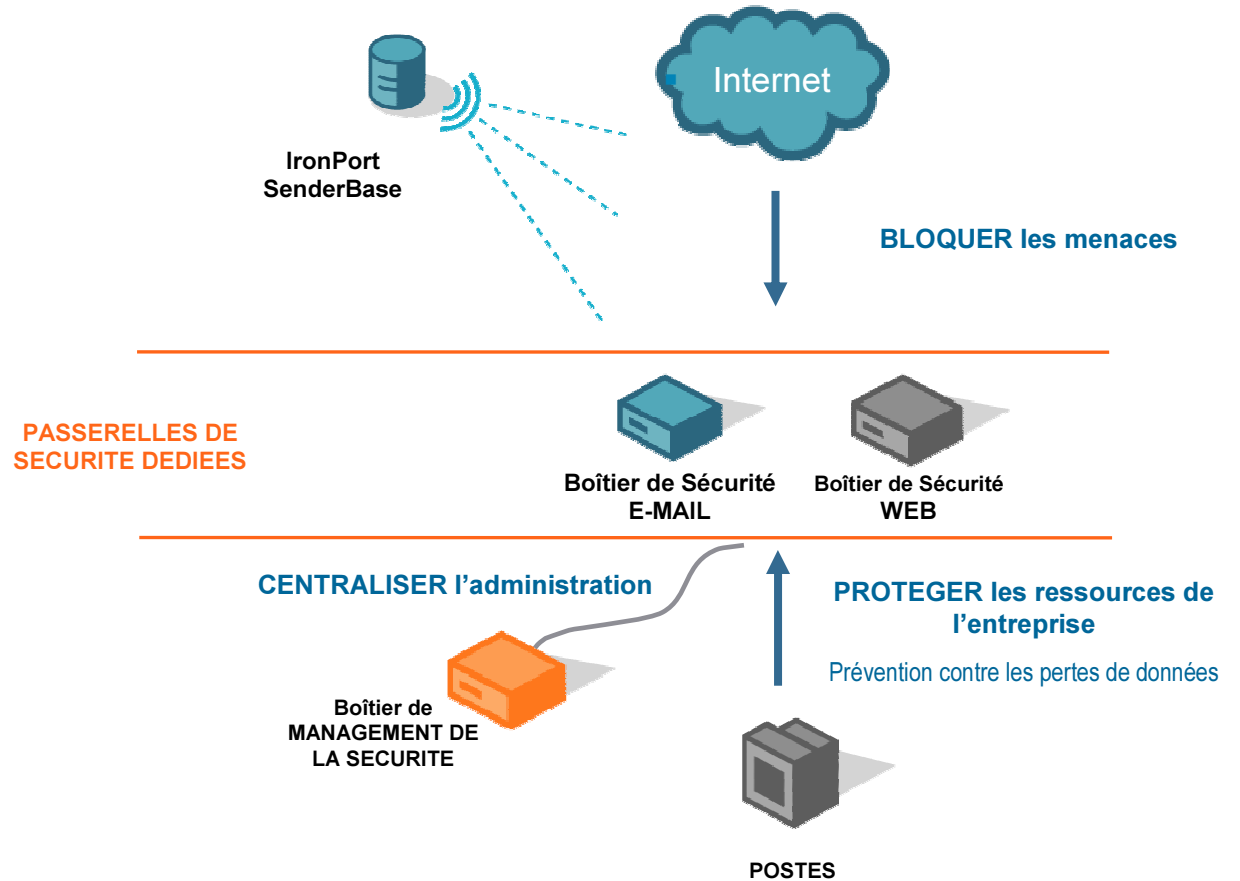
  - SOX, HIPAA, GLBA, PCI, etc.



*“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*

# La vision IronPort



# IronPort SenderBase®

Détection des alertes et création de scores de réputation



- **Statistiques sur plus de 25%** du trafic E-Mail mondial
- Remontée d'informations des routeurs Cisco
- Détection des nouvelles alertes





Sécurité E-Mail



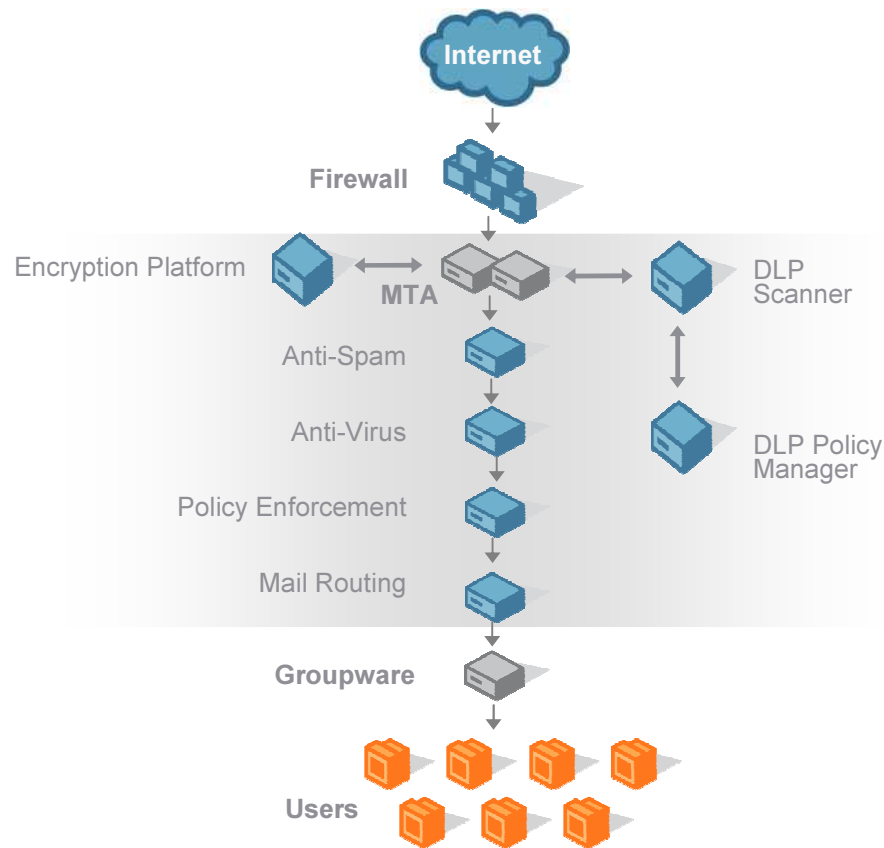
IronPort Série C



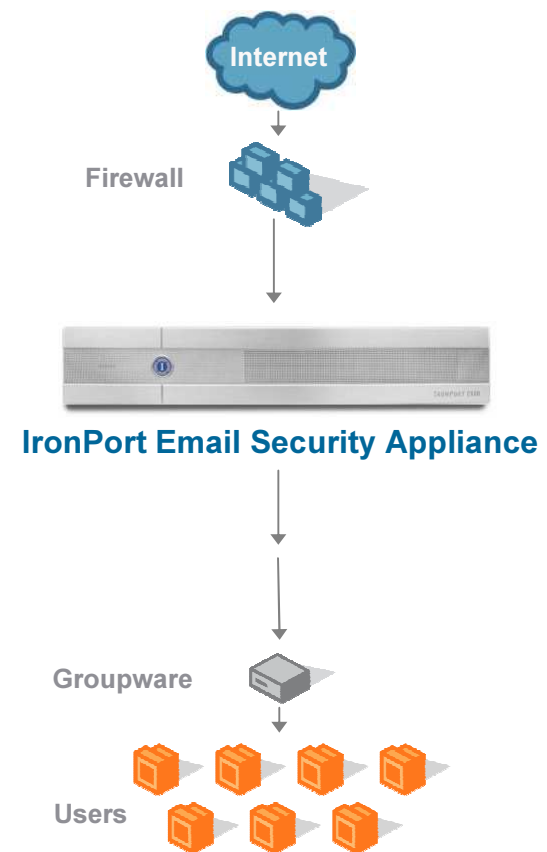
# IronPort Consolidates the Network Perimeter

*For Security, Reliability and Lower Maintenance*

## Before IronPort



## After IronPort



# IronPort SenderBase®

Détection des alertes et création de scores de réputation



- **Statistiques sur plus de 30%** du trafic E-Mail mondial
- Détection des nouvelles alertes
- Plus de **150 paramètres E-Mail & Web** pris en compte pour établir les scores de réputation

- *Volume de données*
- *Composition du message*
  - *Plaintes*
- *Blacklists, whitelists*
- *Données hors-ligne*

• **E-Mail Reputation Filters** •••▶

**Score de réputation**

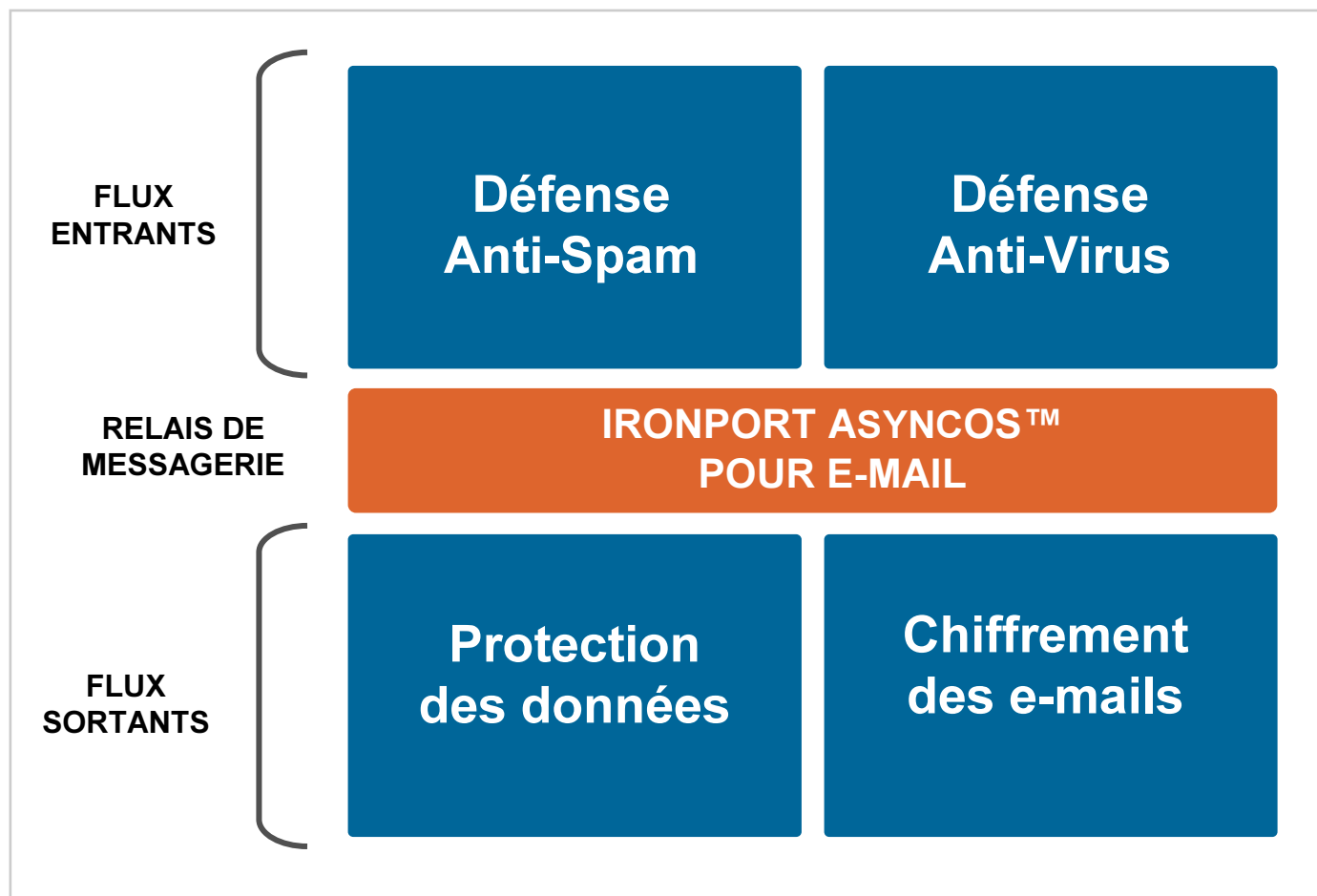
- *blacklists et whitelists d'URL*
  - *Contenu HTML*
  - *Infos sur le domaine*
- *URL à problèmes "connues"*
- *Histoire du site Web...*

• **Web Reputation Filters** •••▶

**Score de réputation**

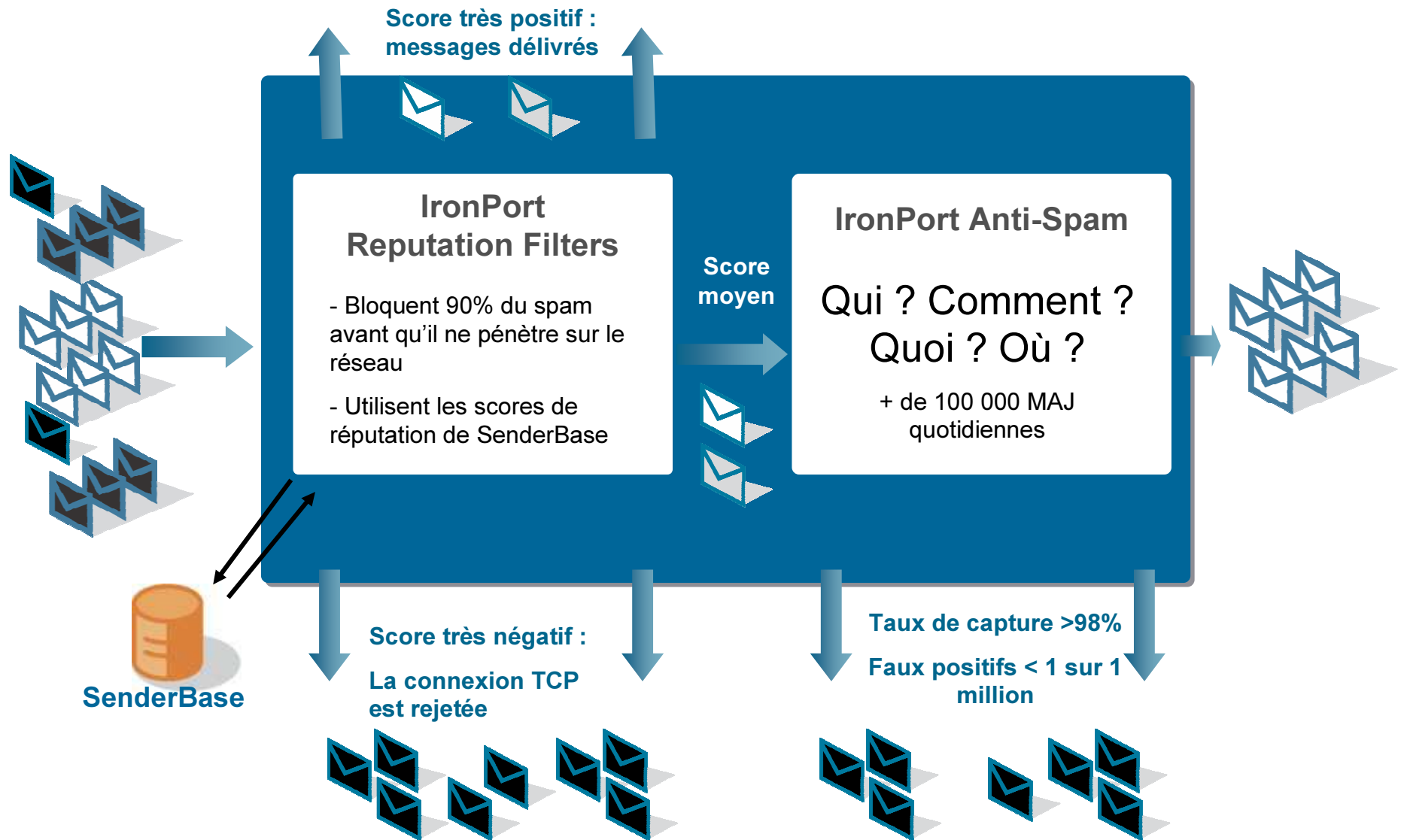
# Architecture Série C IronPort

*Sécurité des flux entrants et sortants*

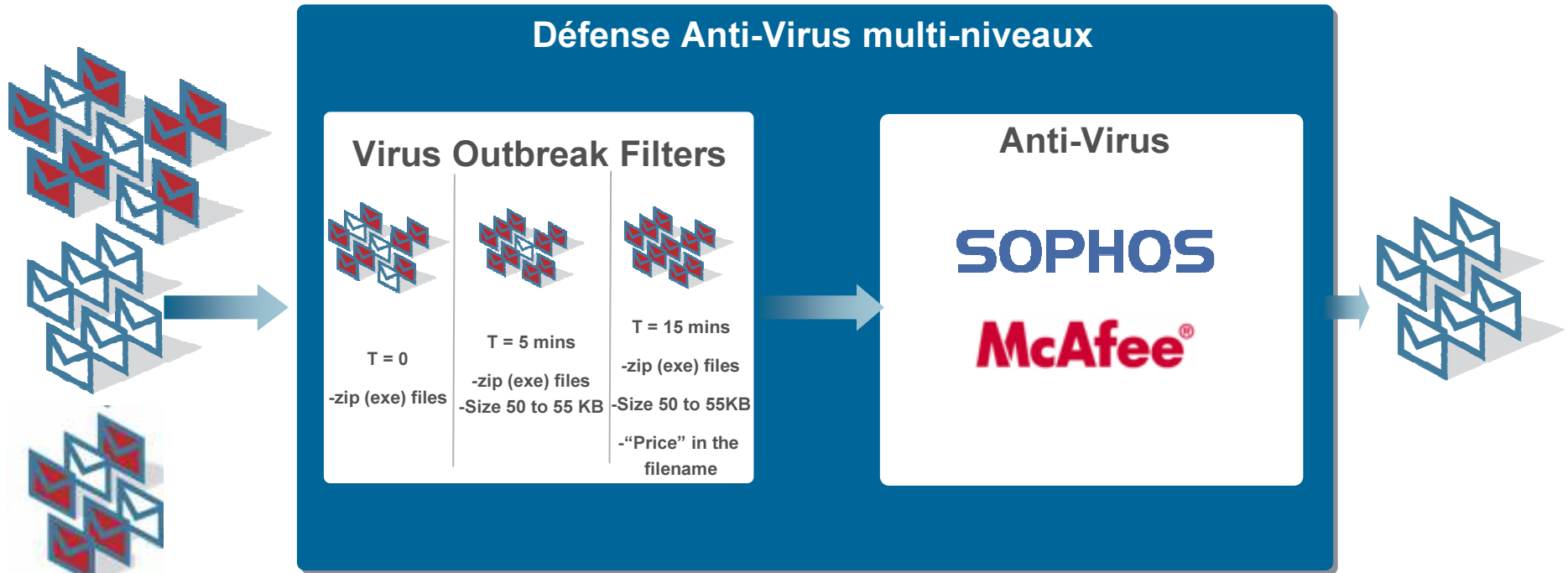


# La défense Anti-Spam IronPort

*Une protection multi-niveaux*



# La défense Anti-Virus IronPort



## L'avantage Virus Outbreak Filters

[www.ironport.com/toc](http://www.ironport.com/toc)

**Temps moyen de protection additionnelle \* ..... + de 13 heures**

**Sur un total d'attaques bloquées de \* ..... 248 alertes**

**Protection totale incrémentale \* ..... + de 134 jours**

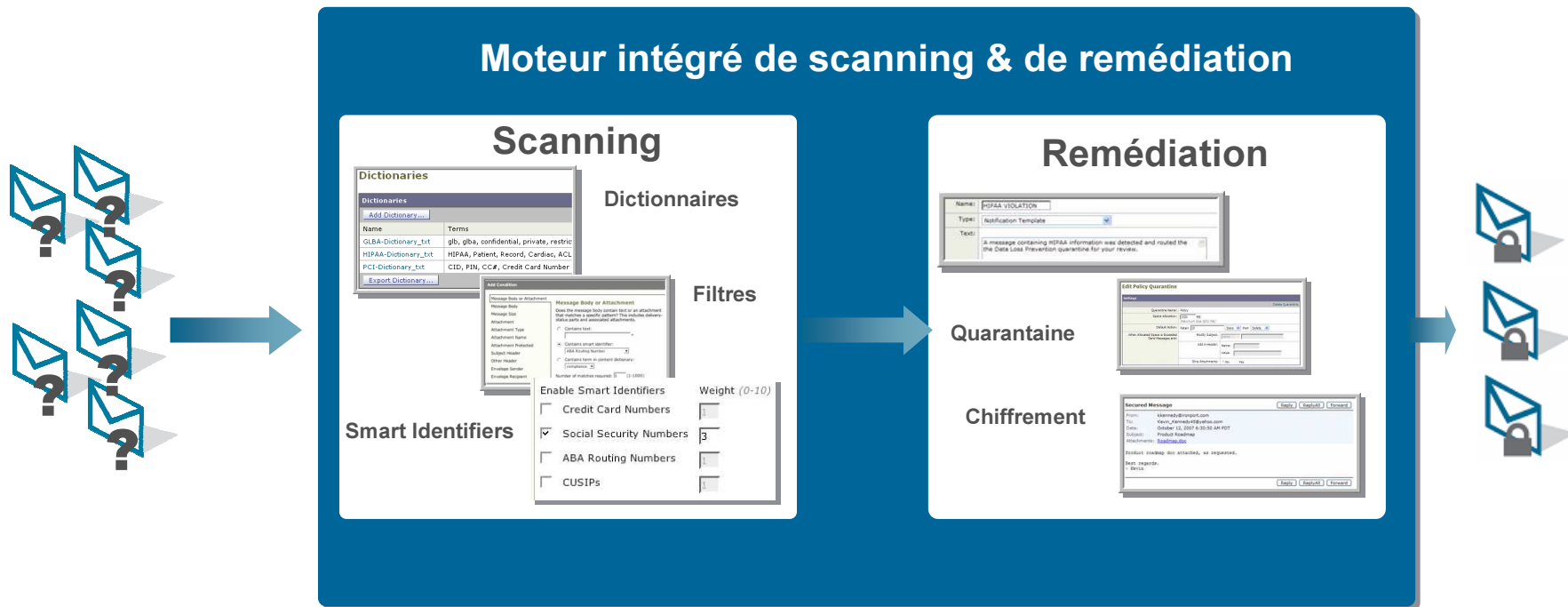


\* Entre Oct 2006 et Sept 2007.

Calculé en fonction des dates officielles de publication des signatures des éditeurs suivants : Sophos, Trend Micro, Computer Associates, F-Secure, Symantec et McAfee.

# Protection des données

## *IronPort Data Loss Prevention*



**Scanning** : Filtres pré-définis (SOX, HIPAA, etc.), Dictionnaires de conformité, Reconnaissance automatique des n° de cartes bleues, etc.

**Remédiation** : Alerte de l'administrateur, reporting, mise en quarantaine, chiffrement...

# Chiffrement: la vision IronPort

*Appréciée par les analystes...*

- IronPort permet aux entreprises de communiquer des informations sensibles cruciales pour leur activité commerciale et les relations avec leurs clients
1. Sans besoin d'un logiciel client sur le poste du destinataire
  2. Quelle que soit sa plateforme de messagerie et son système d'exploitation

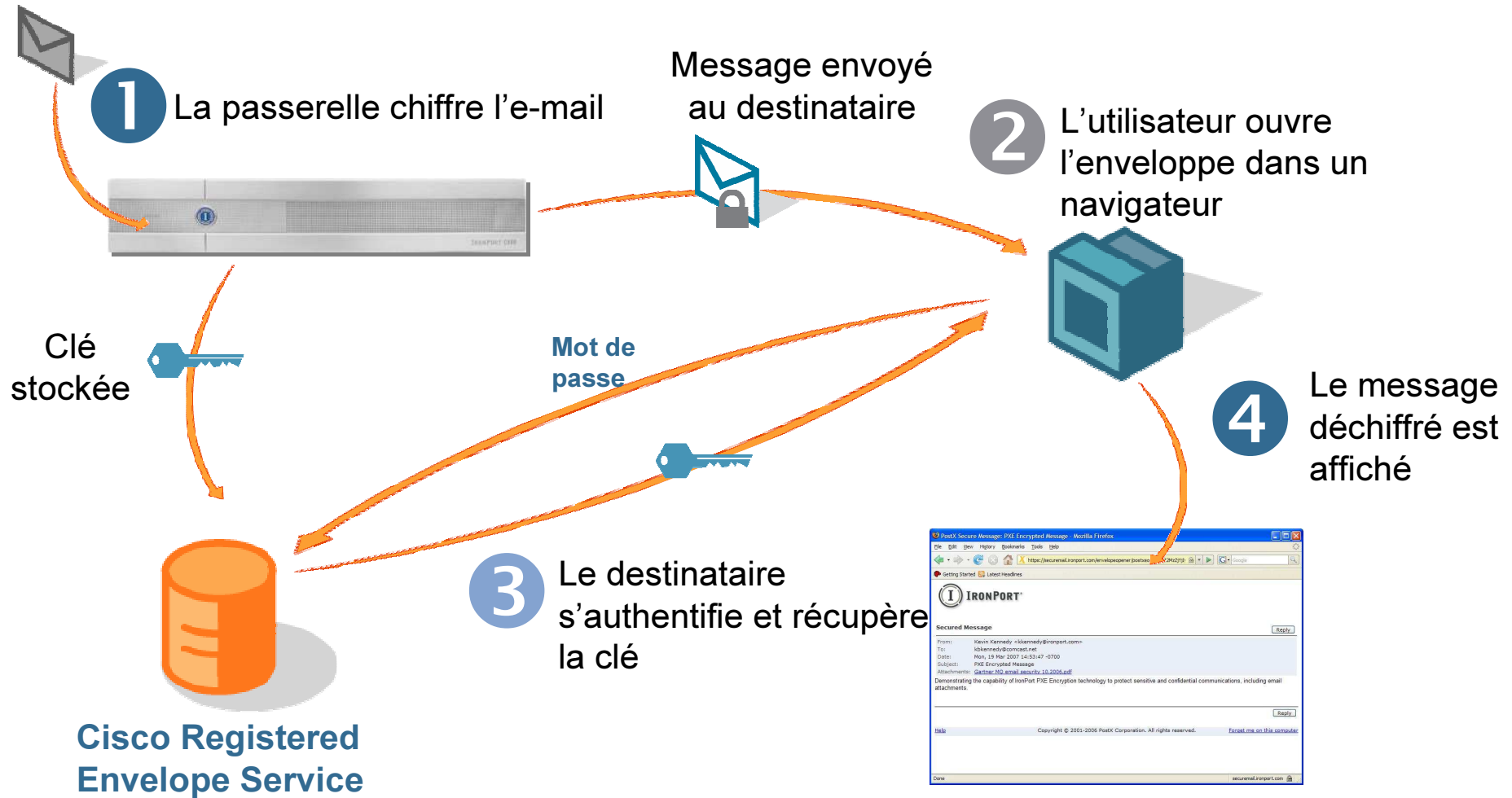


As of August 2007

Source: "Magic Quadrant" Gartner  
Chiffrement E-Mail



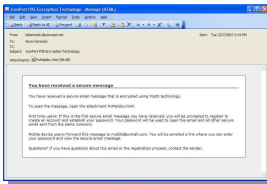
# IronPort PXE: Comment ça marche?



# IronPort PXE

## *Vu par le destinataire du message*

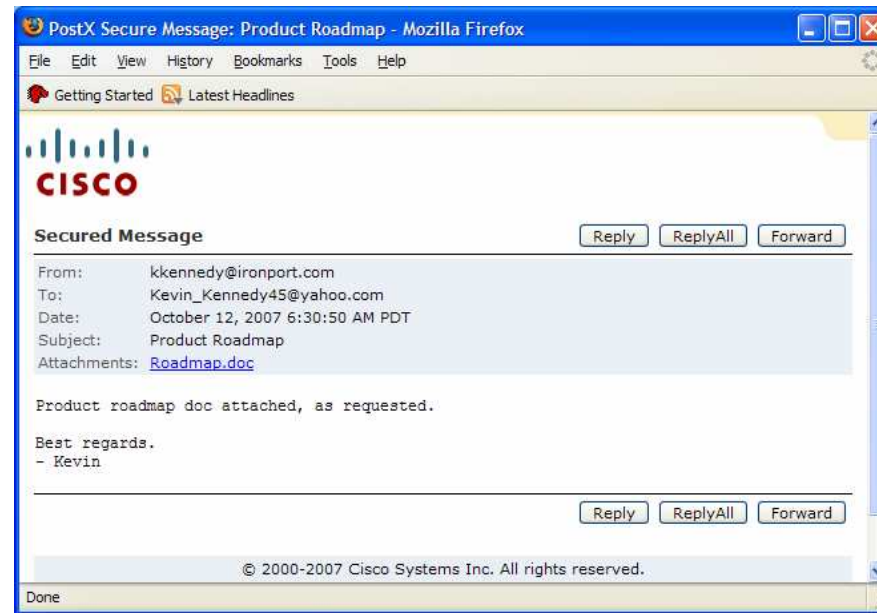
### 1. Ouvre l'attachement



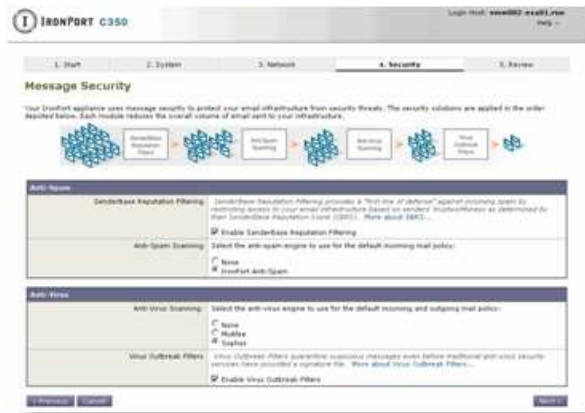
### 2. Entre son mot de passe



### 3. Lit le message



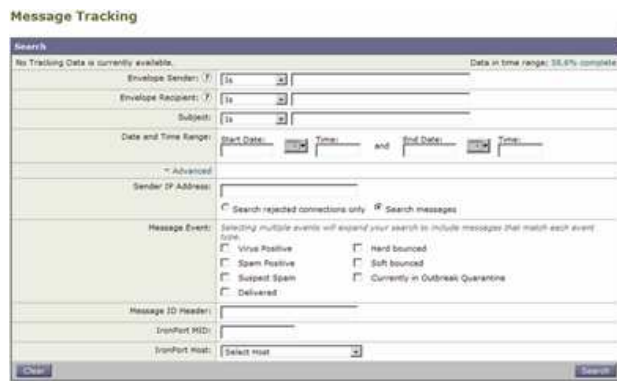
# Une administration simplifiée



Installation en 5 étapes



Email Security Manager  
Configuration des politiques par groupes



Tracking des messages



E-Mail Security Monitor  
Reporting en temps réel

# IronPort Email Security Manager™

## Définir ses politiques de sécurité par groupes

### Incoming Mail Policies

| Find Policies                                |                |   |   |  |  |        |
|--|----------------|---|---|--|--|--------|
| Email Address:                               |                | <input type="text"/>                                |   | <input checked="" type="radio"/> Recipient<br><input type="radio"/> Sender | <input type="button" value="Find Policies"/> |        |
| Policies                                     |                |   |   |  |  |        |
| <input type="button" value="Add Policy..."/> |                |   |   |  |  |        |
| Order  | Policy Name    | Anti-Spam   | Anti-Virus  | Content Filters  | Virus Outbreak Filters                       | Delete |
| 1  | IT Staff       | (use default)                                       | (use default)   | QuarantineEXEs   | (use default)                                |        |
| 2  | Sales          | IronPort<br>Positive: Deliver<br>Suspected: Deliver | (use default)   | DelMsgsWithEXEs  | (use default)                                |        |
| 3  | Legal          | (use default)                                       | (use default)   | ArchiveMail<br>QuarantineEXEs<br>StripMediaFiles                           | Enabled                                      |        |
|  | Default Policy | IronPort<br>Positive: Drop<br>Suspected: Deliver    | Repaired: Deliver<br>Encrypted: Deliver<br>Unscannable: Deliver<br>Virus Positive: Drop | QuarantineEXEs<br>StripMediaFiles  | Enabled                                      |        |

Key:  Default  Custom  Disabled

Catégories: par domaine,  
utilisateur, ou groupe LDAP

- Autoriser les fichiers audio
- Mettre en quarantaine les .exe
- Marquer et distribuer le spam
- Effacer les exécutables
- Archiver les messages
- Virus Outbreak Filters désactivé pour les .doc



IT



SALES



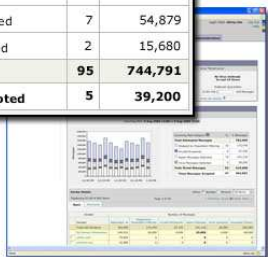
LEGAL

# IronPort Email Security Monitor™

## Systeme de reporting avancé

Rapports graphiques en temps réel

| Incoming Mail Category ?                                 | %         | # Messages     |
|--|-----------|----------------|
| <b>Total Attempted Messages</b>                          |           | <b>783,990</b> |
| <input type="checkbox"/> Stopped by Reputation Filtering | 85        | 666,392        |
| <input checked="" type="checkbox"/> Invalid Recipients   | 1         | 7,840          |
| <input type="checkbox"/> Spam Messages Detected          | 7         | 54,879         |
| <input type="checkbox"/> Virus Messages Detected         | 2         | 15,680         |
| <b>Total Threat Messages</b>                             | <b>95</b> | <b>744,791</b> |
| <input type="checkbox"/> Clean Messages Accepted         | 5         | 39,200         |



Exporter en CSV

Envois programmés

**Add Scheduled Report**

Report Settings

Report Type:

Title:

Time Range To Include:

Report Options

Number of Rows:

Scheduling and Delivery

Schedule:  Daily  Weekly on   Monthly (on first day of month)

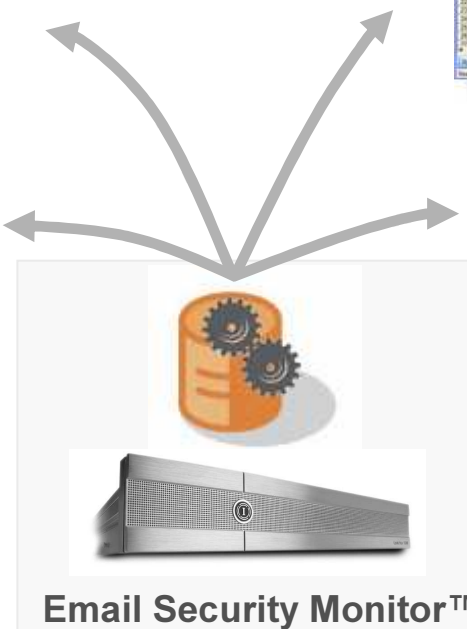
At time:

Email to:

Separate multiple addresses with commas. Leave blank for archive only.



Recherches par domaine



Email Security Monitor™



# Tracking on-box des messages

- Aide les administrateurs à **retrouver rapidement un e-mail**
- Permet de traiter des appels Helpd-Desk ou de support de façon plus rapide
- **Disponible on-box (C150 et supérieurs), et centralisé sur les M-Series**

The screenshot displays the 'Message Tracking' web interface. At the top, it shows the available data range: 'Available Data: 05 Jun 2007 14:00 to 06 Jun 2007 14:12 (GMT -0700)'. Below this is a search form with the following fields:

- Envelope Sender or Sender IP:** Contains [tacoma]
- Envelope Recipient:** Contains [ironport.com]
- Subject:** Begins with [ ]
- Date and Time Range:** Start Date: [mm/dd/yyyy] Time: [hh:mm:ss] End Date: [mm/dd/yyyy] Time: [hh:mm:ss]

There are 'Clear' and 'Submit' buttons. Below the search form, it indicates 'Generated: 05 Jun 2007 14:00 (GMT -0700)'. The 'Results' section shows 'Items per page: 10' and 'Displaying 1 - 4 of 4 items.' The results are as follows:

| Item | Date and Time                     | MID       | Host               | Sender                     | Recipient            | Subject      | Last State                     | Action       |
|------|-----------------------------------|-----------|--------------------|----------------------------|----------------------|--------------|--------------------------------|--------------|
| 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 | Show Details |
| 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 | Show Details |
| 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 | Show Details |
| 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 | Show Details |

At the bottom, it shows 'Displaying 1 - 4 of 4 items.'

# IronPort M-Series

## Quarantaine de Spam, Reporting et Tracking Centralisés

- Rapports d'IronPort Email Security Monitor disponibles de façon centralisée sur la Série M IronPort
- Rapports sur les appliances C gérées (capacité système, fonctionnement, etc.)
- Stocke plus d'un an de données
- Tracking centralisé facilitant la recherche de messages pour les administrateurs
- Quarantaine centralisée de spam

The screenshot displays the IronPort Message Tracking interface, which is used for monitoring and managing email messages. It is divided into several sections:

- Message Tracking (Top):** A search interface with filters for Envelope Sender, Envelope Recipient, Subject, Date and Time Range, and Sender IP Address. It includes a 'Search rejected' checkbox and a 'Clear' button.
- Message Tracking (Middle):** A search interface with filters for Envelope Sender or Sender IP, Envelope Recipient, Subject, and Date and Time Range. It includes a 'Search messages using advanced criteria' link and a 'Submit' button.
- Message Details (Bottom Left):** A detailed view of a message with the following information:
  - 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: 5b4b55a9f@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:** A log of events including message enqueue, processing by Anti-spam (Verdict: Negative), processing by Sophos Anti-Virus (Verdict: Negative), and successful delivery to brightmail@d1.qa41.qa.
- Results (Bottom Right):** A list of search results showing 4 items. Each item includes the date and time (Thu Jul 22 2005 16:37 (GMT-0700)), MID (988809854), HOST (mailman.domain.com), and details for the sender (normal\_sender@29801.tacoma) and recipient (janedoe@ironport.com). The last state for all items is 'Message successfully delivered'.

# IronPort Série C

## Exemple Dell



Efficacité anti-spam x10

68 serveurs avec Spam Assassin remplacés par 8 boîtiers Série C

Coûts réduits de **75%**



*“IronPort a augmenté la qualité et la fiabilité de nos opérations IT, tout en réduisant nos coûts.”*

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

DELL CORPORATION

BOITES AUX  
LETTRES

**100,000**

# Les Séries C/X/M

**IronPort X1050** – boîtier haute performance pour les plus grandes entreprises et les fournisseurs d'accès Internet.

**IronPort C650** – pour les réseaux des grandes entreprises.

**IronPort C350** - pour les entreprises de taille moyenne et les filiales des grandes entreprises.

**IronPort C150** – pour les PME.

**IronPort C350D** - version optimisée pour les besoins spécifiques d'émissions d'e-mails (confirmations de transactions, cotations boursières, lettres d'information).

**IronPort M1050** – boîtier de gestion à haute capacité de stockage

**IronPort M650** – boîtier de gestion à capacité intermédiaire de stockage





Sécurité Web

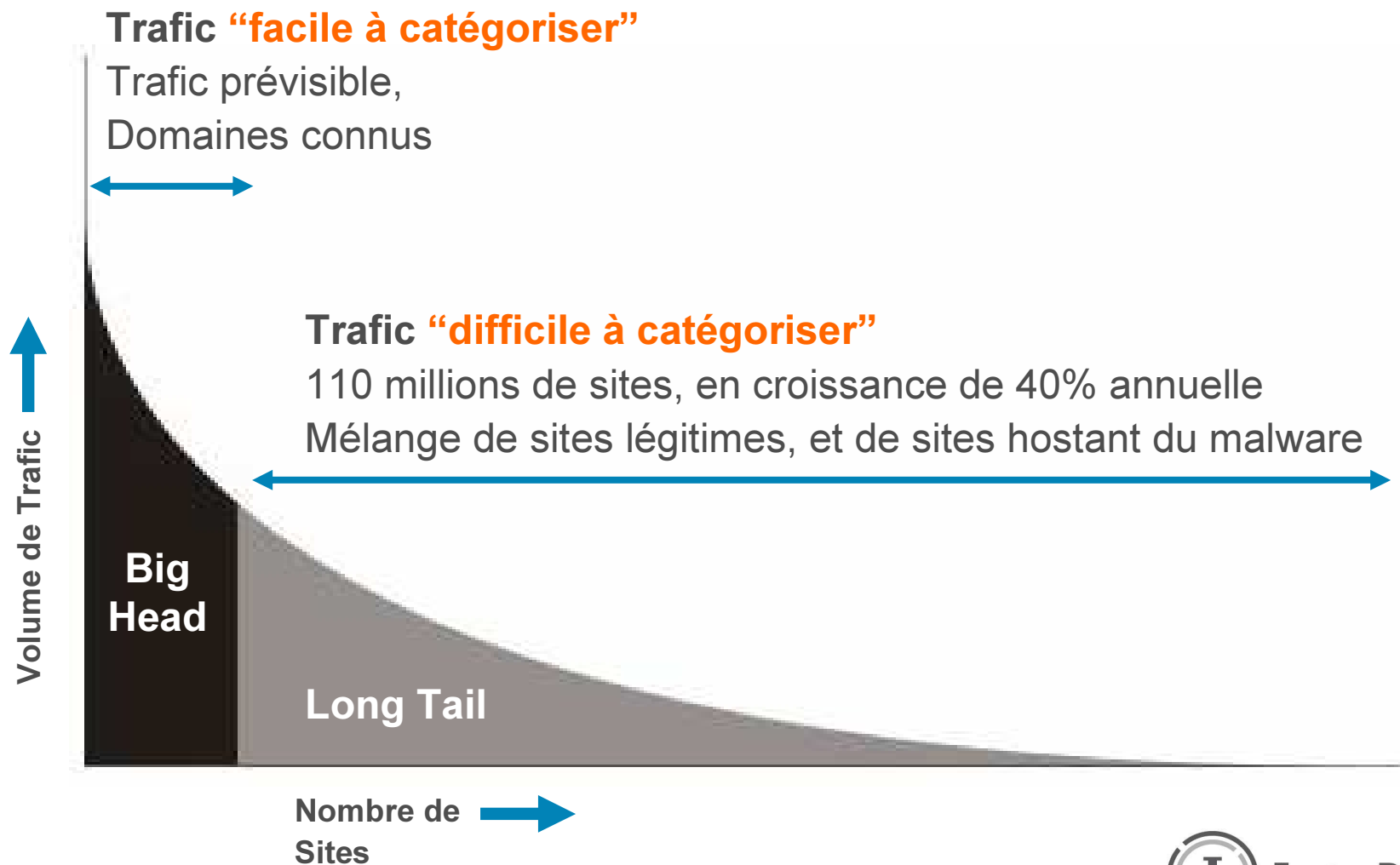


IronPort Série S



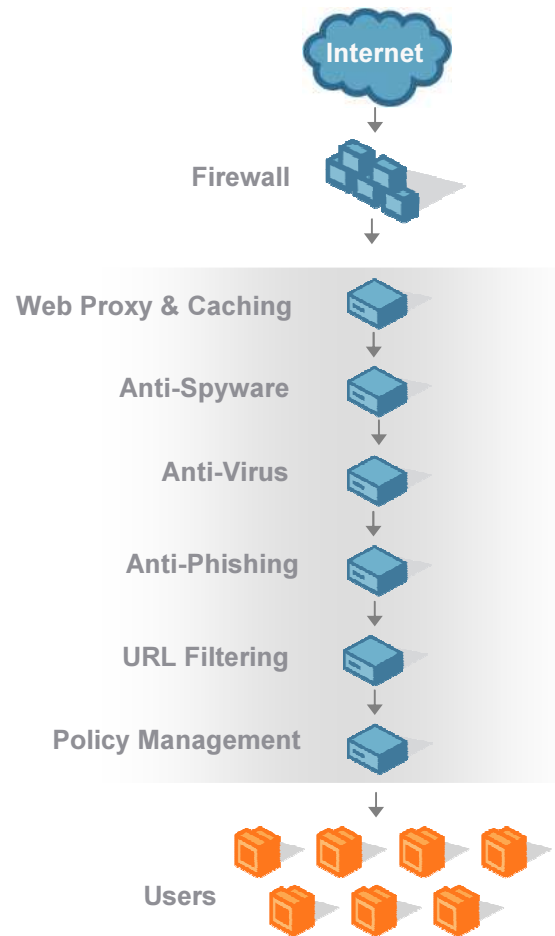
# Le Trafic Web

*De plus en plus de sites inconnus*

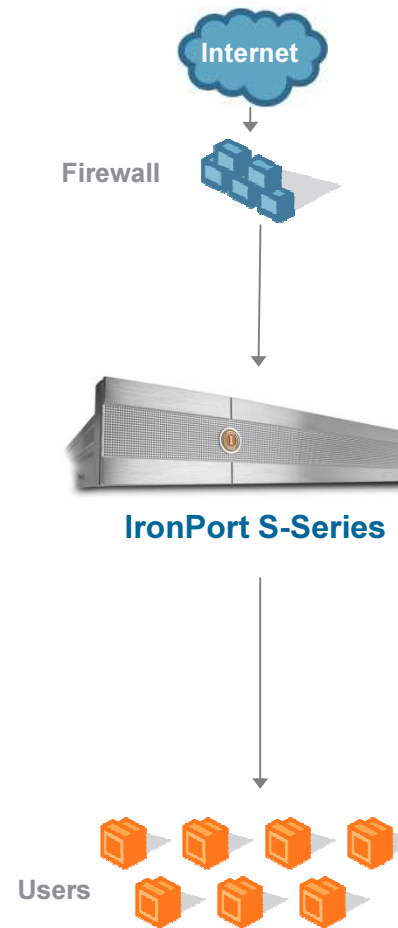


# Next Generation Secure Web Gateway

Before IronPort

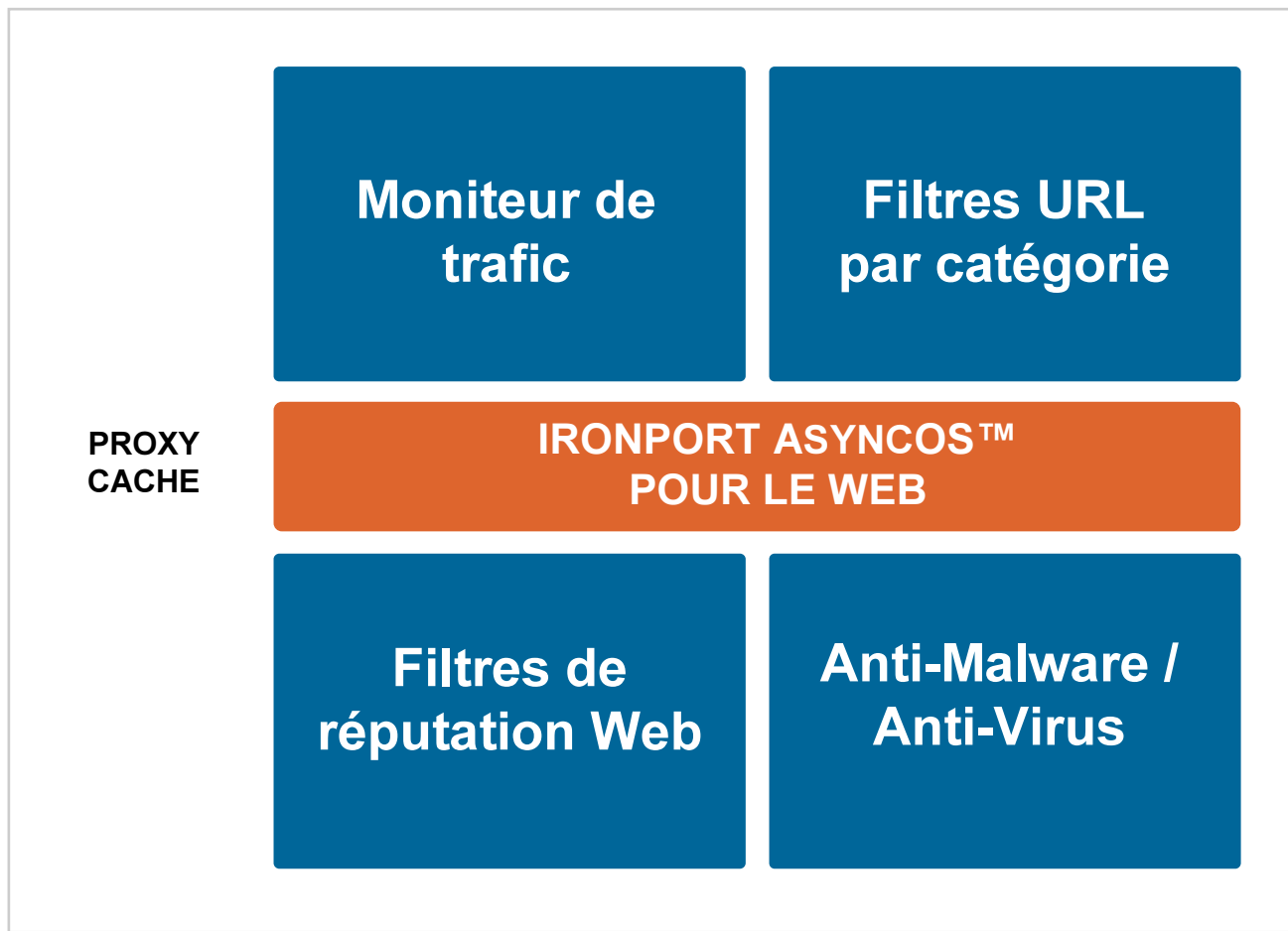


After IronPort



# Architecture Série S IronPort

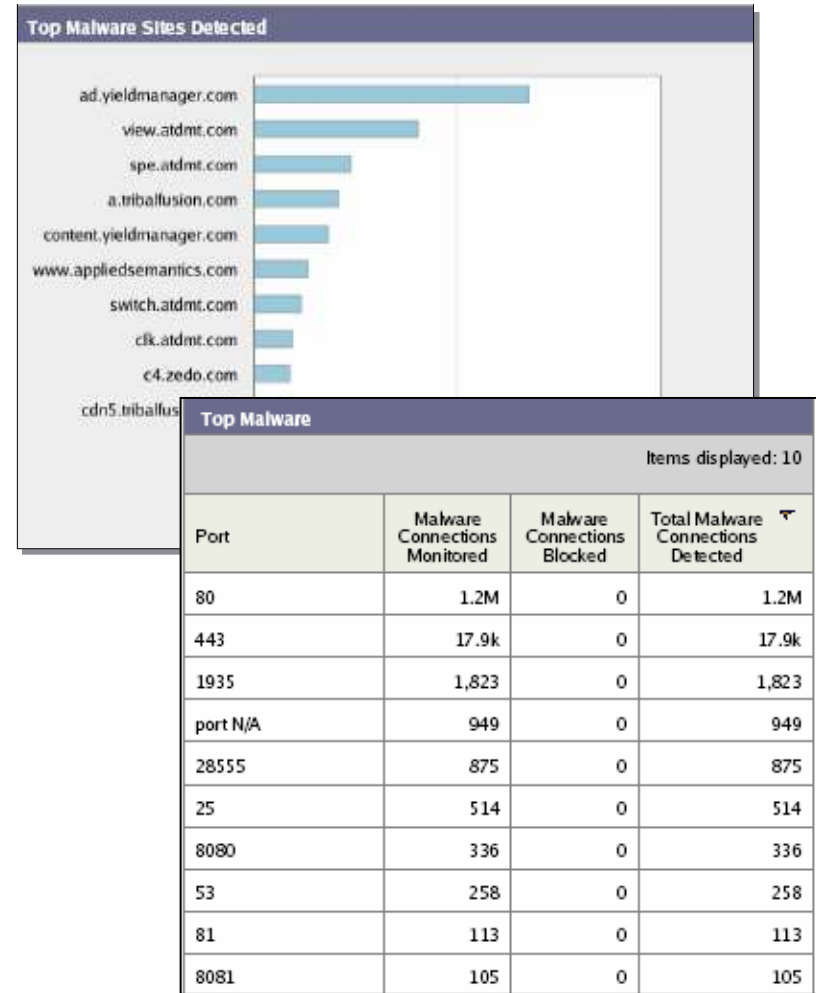
## *Sécurité des flux entrants et sortants*



# Détecter les postes déjà infectés

## Contrôler le trafic malicieux

- Détecte toute communication de spyware ou de cheval de Troie avec un serveur externe
  - Scanne tous les ports et protocoles
- Compare les adresses IP extérieures contactées à une liste connue de serveurs de contrôles de zombies
- Règles anti-malware automatiques distribuées sur les boîtiers
- Mode “monitor” ou mode “monitor & block”

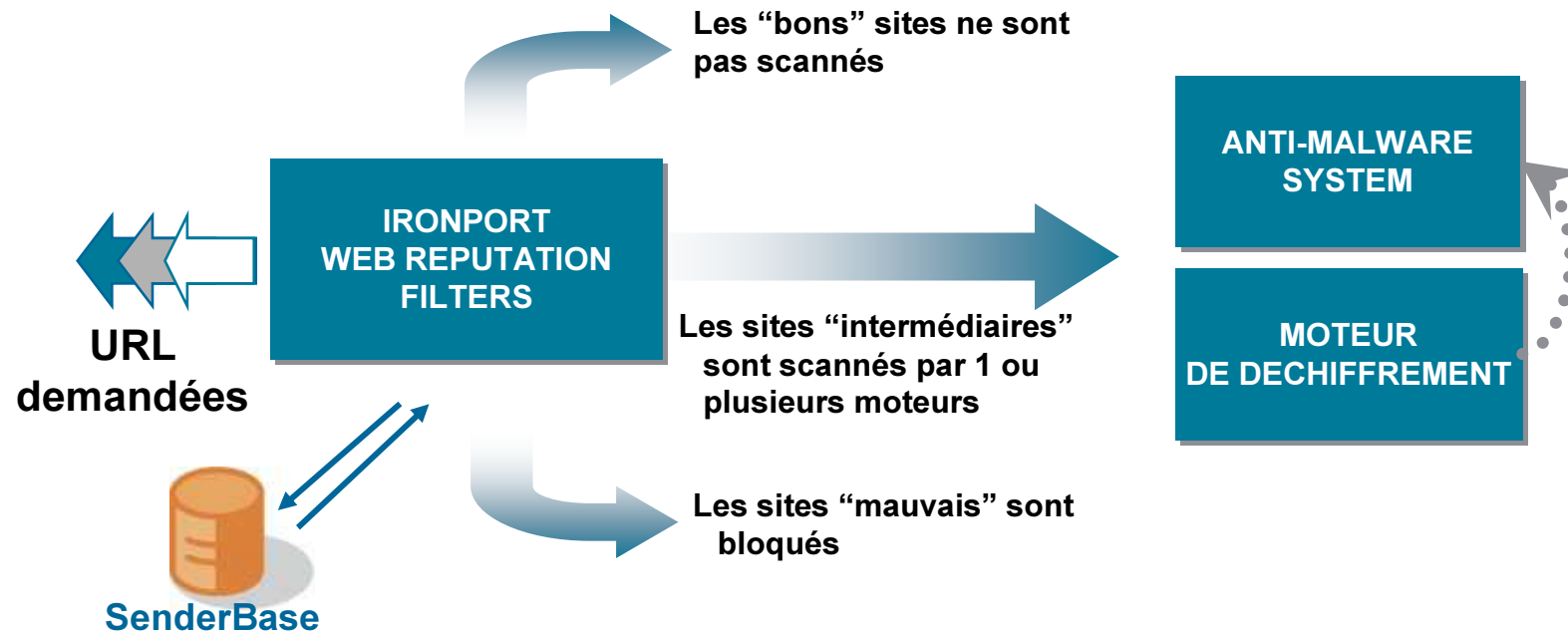


# IronPort URL Filters

- Une base de données complète
  - 52 catégories
  - + de 21 millions de sites
  - ~3,5 milliards de pages web
- Monitoring 24h/24, 7j/7
- Mise à jour régulières et automatiques
- Catégories personnalisables
- Gestion flexible des politiques
  - Par utilisateur, par groupe
  - Actions multiples, incluant le mode “**monitor only**”
  - Notifications personnalisables

| Catégories                         |  |
|------------------------------------|--|
| Advertisements & PopUps            |  |
| Arts                               |  |
| Blogs & Forums                     |  |
| Business                           |  |
| Chat                               |  |
| Computing                          |  |
| Downloads                          |  |
| Education                          |  |
| Entertainment                      |  |
| Fashion & Beauty                   |  |
| Finance & Business                 |  |
| Food & Dining                      |  |
| Games                              |  |
| Government                         |  |
| Health & Medical                   |  |
| Hobbies & Recreation               |  |
| Hosting Services                   |  |
| Infrastructure                     |  |
| Intimate Apparel & Swimwear        |  |
| Job Search & Career Development    |  |
| Kids Sites                         |  |
| Motor Vehicles                     |  |
| News                               |  |
| Peer-to-Peer                       |  |
| Personals & Dating                 |  |
| Philanthropic & Professional Orgs. |  |
| Photo Searches                     |  |
| Politics                           |  |
| Proxies & Translators              |  |
| Real Estate                        |  |
| Reference                          |  |

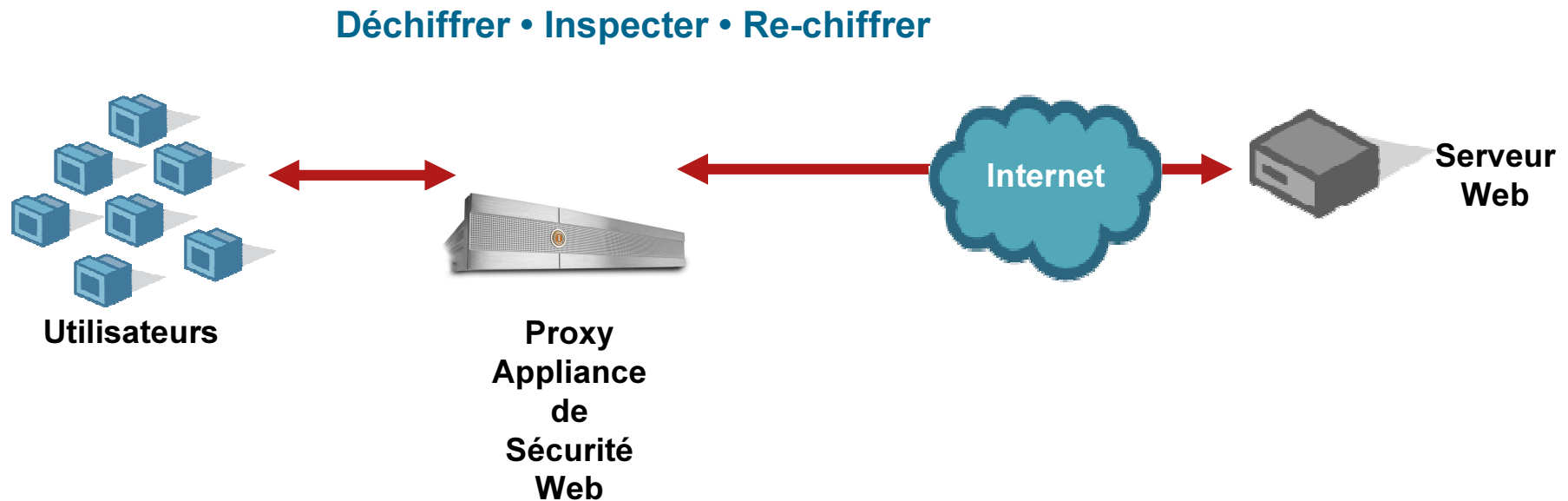
# La réputation Web : un filtrage intelligent



- **IronPort Web Reputation est le premier niveau de défense** qui détermine le besoin de scanner ensuite par:
  - Le moteur de déchiffrement HTTPS
  - IronPort Anti-Malware System™

# Scan HTTPS sélectif

*Basé sur la réputation*



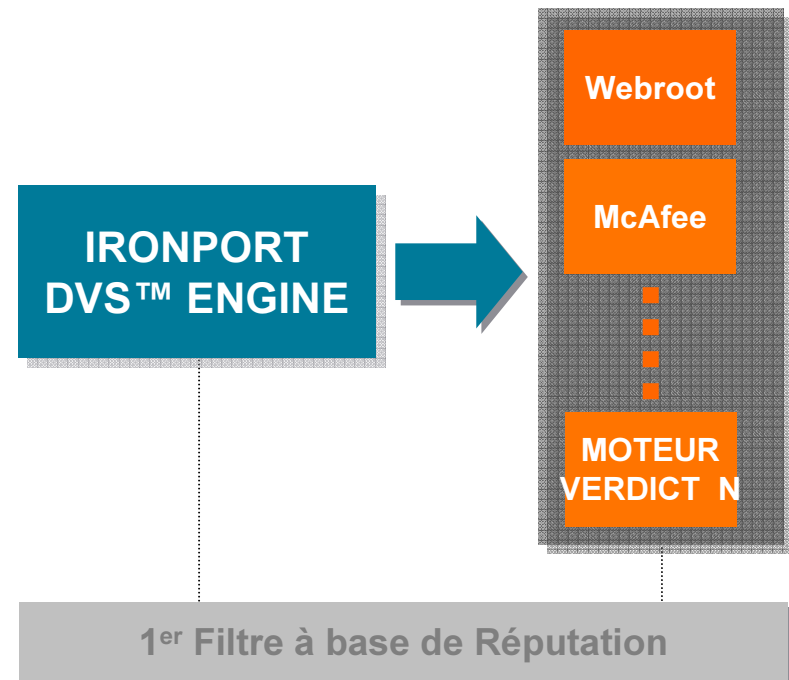
- **Le filtrage HTTPS sélectif :**

- Respecte la confidentialité des véritables sessions HTTPS légitimes (par exemple un utilisateur consultant son compte bancaire en ligne)
- Empêche le téléchargement de malware en toute impunité via des sites HTTPS frauduleux

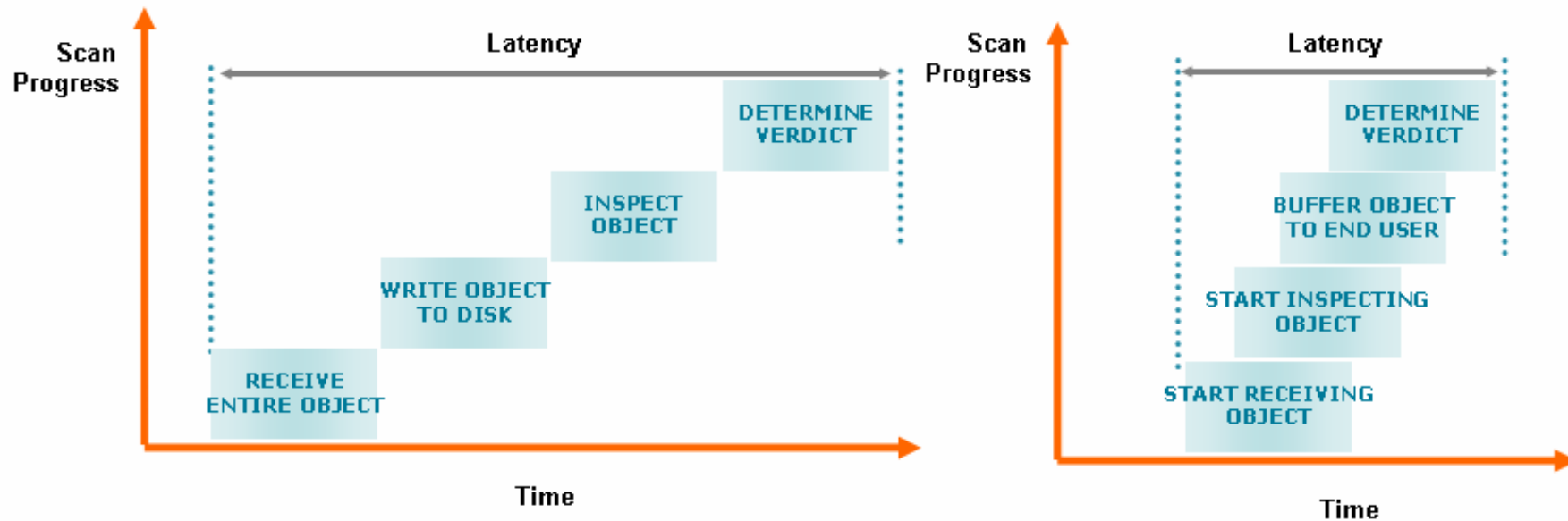
# IronPort DVS™ Engine

*Filtrage Anti-Malware à base de signatures*

- DVS Engine : moteur incluant plusieurs bases de signatures
  - Webroot (n°1 mondial de l'anti-spyware)
  - McAfee (n°1 sur l'anti-virus Web et n°2 sur l'anti-spyware)
  - Etc.
- Scanning en mode streaming  
Solution au problème de latence



# Scan en mode streaming



« En raison de la nature en temps réel des protocoles HTTP (...) et HTTPS et de leur flux de données, des fonctionnalités de scanning en temps réel (= en streaming) plus sophistiquées sont nécessaires pour s'assurer que le trafic Web reste sécurisé et à l'abri des attaques. »

IDC

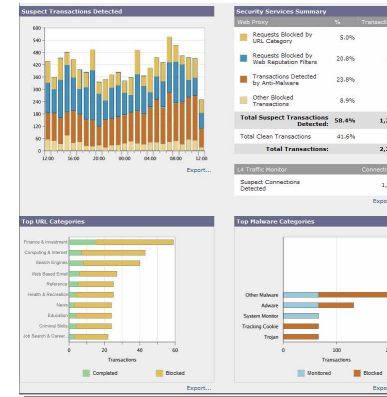
# Une administration simplifiée

**Web Filtering Policies**

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

Key:  Global  Disabled  
 Authentication

**Web Security Manager**  
Configuration des politiques par groupes



**Web Security Monitor**  
Reporting en temps réel

Calendar Date Range Filter Printer Friendly Update Database | Rebuild Database

**Overview**

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

|                   | All days | Average per day |
|-------------------|----------|-----------------|
| Requests          | 79,029   | 11,404.14       |
| Page views        | 71,628   | 10,232.57       |
| Unique source IPs | 7        | -               |
| Size              | 1.85 G   | 270.73 M        |

**Reporting centralisé**  
Sawmill



IRONPORT M-SERIES



CONFIGURATION PROFILES

**Gestion centralisée des configurations**  
IronPort Série M

# IronPort Web Security Manager™

*Définir ses politiques de sécurité, par groupes*

**Web Filtering Policies**

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

Key:  Global  Disabled  
? Authentication

## Groupes LDAP, AD, Réseau

- Bloque FTP
- Autorise les fichiers média
- Permet toutes les catégories d'URL



Marketing

- Bloque les exécutables
- Bloque les sites de jeu
- Bloque tous les malware



Sales

- Autorise Skype
- Monitore le trafic
- Autorise les exécutables
- Autorise toutes les applications
- Autorise tous les protocoles



IT



# IronPort Web Security Monitor™

- *Overview Système*
- *Tendances Trafic Web*
- *Activités / Site*
- *Détail des sites*
- *Activités / utilisateur*
- *Détails par utilisateur*
- *Détails des catégories*
- *Détails des malware*
- *Tendances Malware*
- *Moniteur de Trafic*
- *Réputation Web*



# Reporting Centralisé - Sawmill

*Vue consolidée de multiples boîtiers*

- Application leader de création de rapports Web – Sawmill

- Rapports complets

Vues détaillées des activités Web par site ou utilisateur

Personnalisables

- Centralisés & agrégés

Environnements cluster/équilibrage de charge via HTTP, FTP, Local File ou Command Line

Supporte des bases de données standard & MySQL database server™

Planifiables

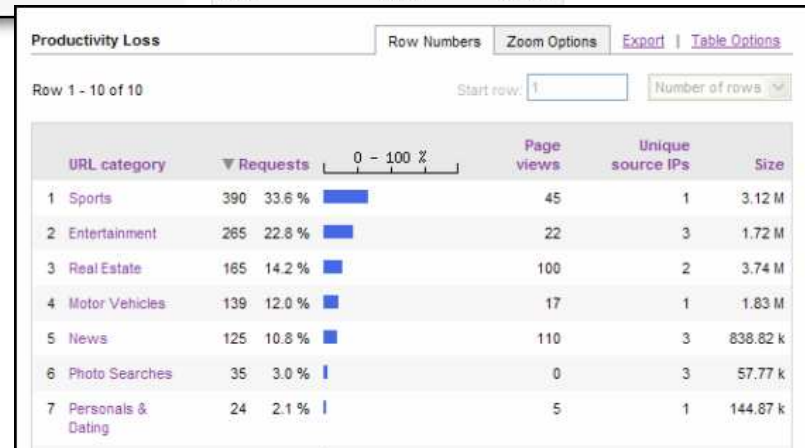


Calendar Date Range Filter Printer Friendly Update Database | Rebuild Database

### Overview

1 Statistics for 26/Jun/2007 - 02/Jul/2007, 7 days  Date Filter  Filter Refresh

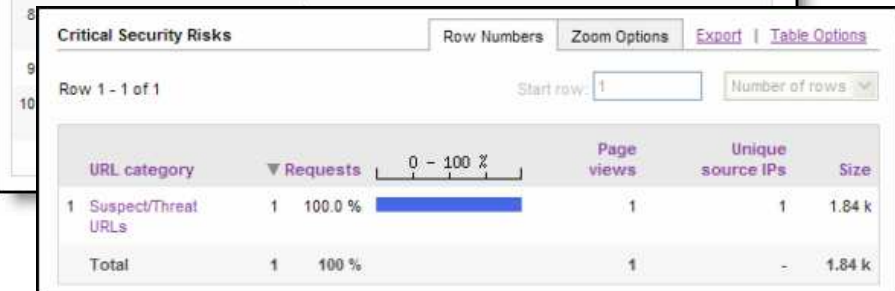
|                   | All days | Average per day |
|-------------------|----------|-----------------|
| Requests          | 79,829   | 11,404.14       |
| Page views        | 71,628   | 10,232.57       |
| Unique source IPs | 7        | -               |
| Size              | 1.85 G   | 270.73 M    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



Productivity Loss Row Numbers Zoom Options Export | Table Options

Row 1 - 10 of 10 Start row: 1 Number of rows

| URL category         | Requests | 0 - 100 % | Page views | Unique source IPs | Size     |
|----------------------|----------|-----------|------------|-------------------|----------|
| 1 Sports             | 390      | 33.6 %    | 45         | 1                 | 3.12 M   |
| 2 Entertainment      | 265      | 22.8 %    | 22         | 3                 | 1.72 M   |
| 3 Real Estate        | 165      | 14.2 %    | 100        | 2                 | 3.74 M   |
| 4 Motor Vehicles     | 139      | 12.0 %    | 17         | 1                 | 1.83 M   |
| 5 News               | 125      | 10.8 %    | 110        | 3                 | 838.82 k |
| 6 Photo Searches     | 35       | 3.0 %     | 0          | 3                 | 57.77 k  |
| 7 Personals & Dating | 24       | 2.1 %     | 5          | 1                 | 144.87 k |



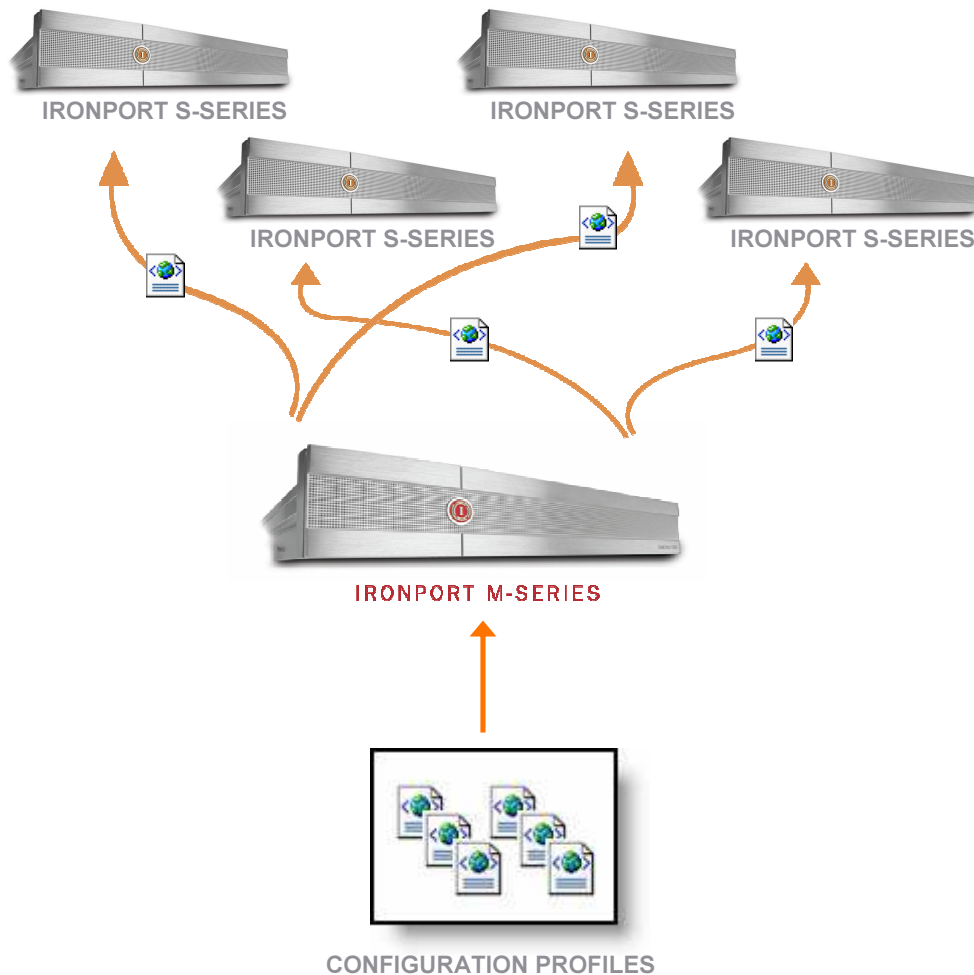
Critical Security Risks Row Numbers Zoom Options Export | Table Options

Row 1 - 1 of 1 Start row: 1 Number of rows

| URL category          | Requests | 0 - 100 % | Page views | Unique source IPs | Size   |
|-----------------------|----------|-----------|------------|-------------------|--------|
| 1 Suspect/Threat URLs | 1        | 100.0 %   | 1          | 1                 | 1.84 k |
| Total                 | 1        | 100 %     | 1          | -                 | 1.84 k |

# IronPort Centralized Configuration Manager

*Gestion centralisée des configurations sur la Série M*



- Créer et gérer de multiples profils de configuration de Série S
- Sauvegarder et restaurer rapidement des profils
- Large capacité  
Supporte plus de 100 boîtiers Série S

# IronPort S-Series

## Exemple Aurora Health Care



- **Le challenge Aurora Health Care:**
  - 13 Hôpitaux, 100 cliniques, plus de 30 000 utilisateurs
  - Infections régulières par du malware
  - Large infrastructure, 7 serveurs avec Websense
- **La solution IronPort :**
  - A bloqué **environ 2 millions** de transactions additionnelles par semaine
  - **3x plus de spyware a été bloqué**
  - Les **7** serveurs ont été remplacés par **2** boîtiers IronPort S-Series™



*“... nous avons été préoccupés par le niveau d’infection par du malware au sein de notre réseau. La Série S IronPort nous a permis de stopper le malware au niveau de la passerelle Web, tout en nous permettant également de déployer des politiques de filtrage des URL.”*

— Tim Sommers

AURORA HEALTH CARE

UTILISATEURS  
PROTEGES

**30 000**

# Questions - Réponses

**NE NOUS CROYEZ PAS SUR PAROLE...  
VERIFIEZ-LE !!**

- ⇒ prêt de l'équipement pour maquette en production
- ⇒ Recevez toutes les alertes virales en vous abonnant sur : <http://www.ironport.com/toc/>
- ⇒ Pour toute information: [fr-info@ironport.com](mailto:fr-info@ironport.com)