Overview IronPort

Séminaire CBI/Cisco
Palace d'Anfa
Le 22 Janvier 2009

Denis Gadonnet
Territory Manager, Med Area
IronPort, a Cisco Business Unit

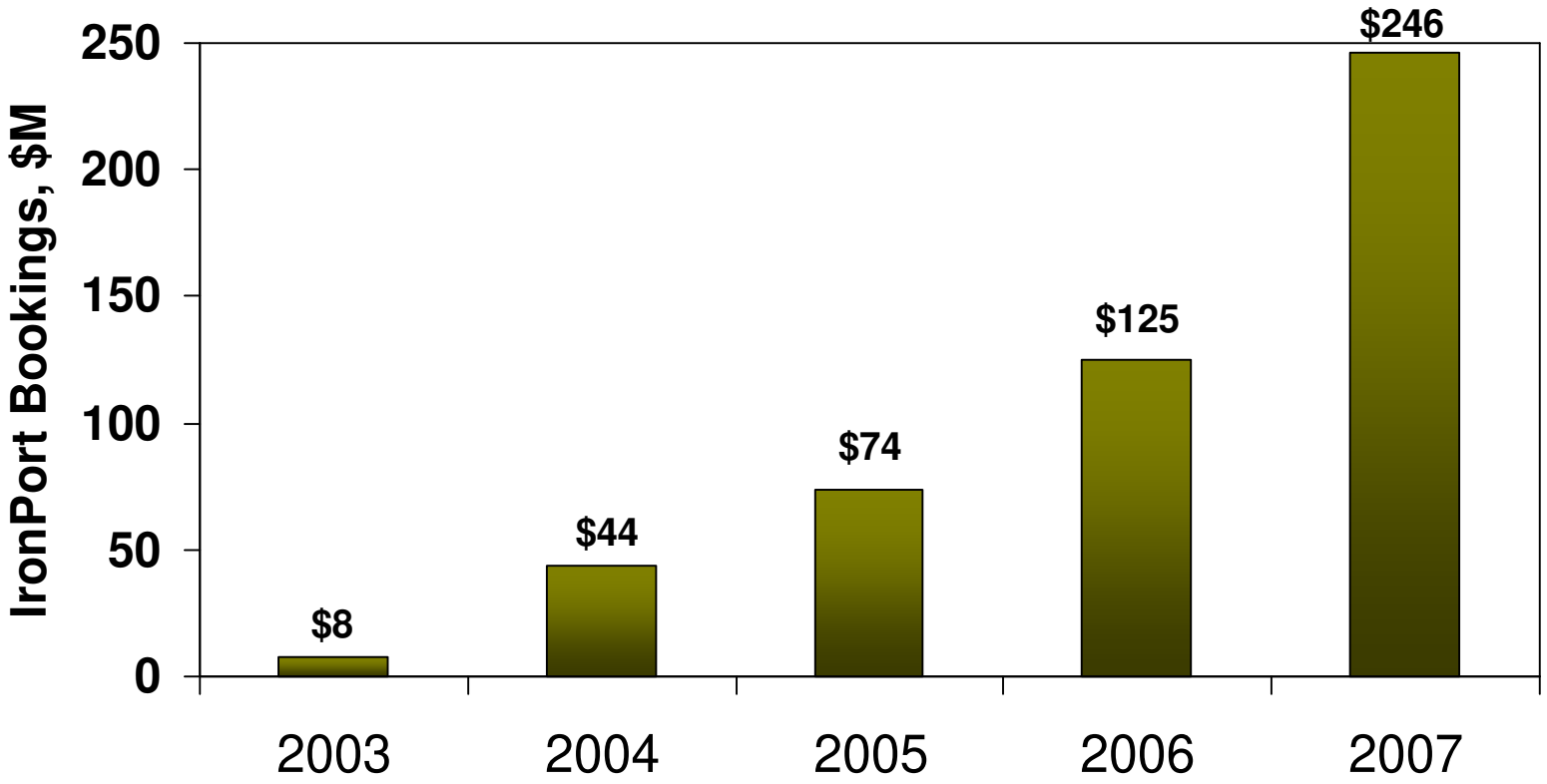
Agenda

- Overview Business Unit
- Overview Technologie / Produits
- Pourquoi pousser IronPort ?

La Business Unit IronPort

- 645 personnes (~100 en EMEA)
- Opérations dans 35 pays, 45 villes
- + de 7000 clients dans 85 pays
- Business Unit de Cisco rattaché au STG

IronPort Worldwide



Leadership / clients

- 54% des 100 plus grandes entreprises mondiales
- 12 des 15 plus grands ISPs
- 7 des 10 plus grandes banques mondiales
- 325 millions de boîtes aux lettres protégées
- 99% des clients renouvellent
- 90% des évaluations sont transformées en commandes

Leadership / Analystes

Gartner

*IronPort positionné dans le **"Leaders"** **Quadrant** du Magic Quadrant Report*

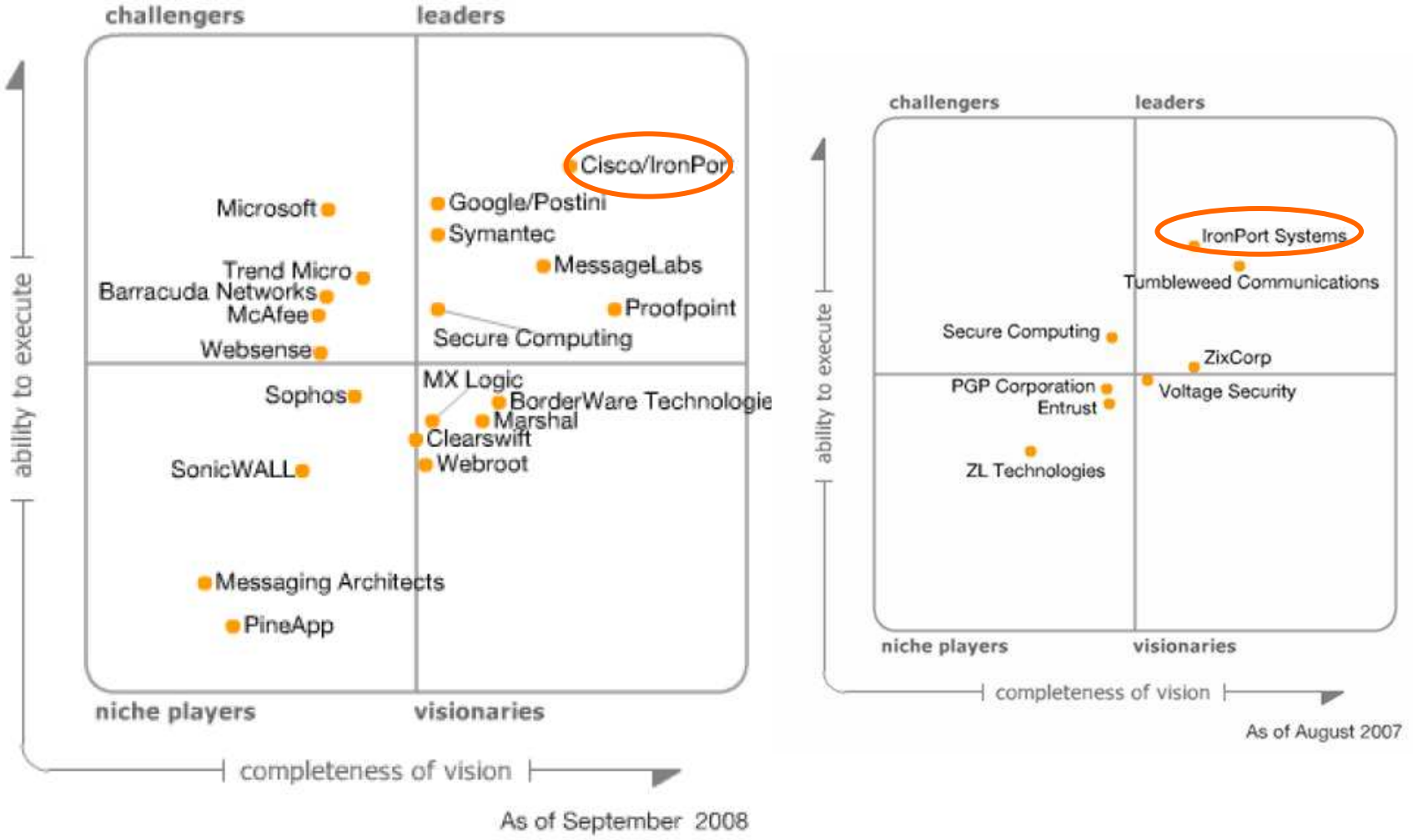
IDC
Analyze the Future

IronPort positionné comme le leader du marché des appliances de sécurité e-mail

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

Confirme IronPort comme le leader en parts de marché du marché des appliances de sécurité e-mail

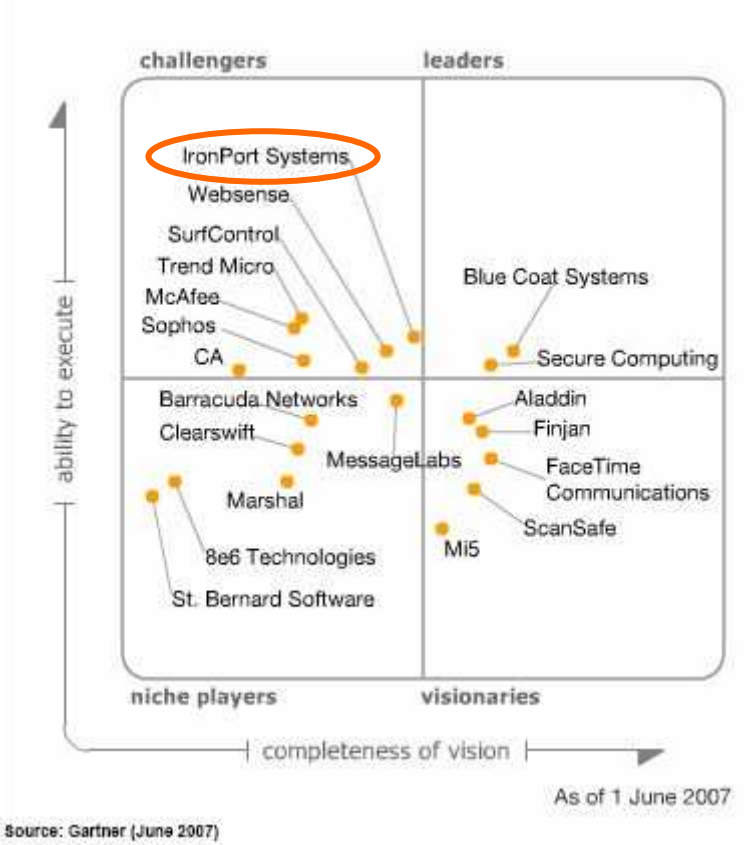
La reconnaissance des analystes : Sécurité e-mail, chiffrement



Source: Gartner (September 2008)

La reconnaissance des anaystes Sécurité Web

Figure 1. Magic Quadrant for Secure Web Gateway, 2007



Source: Gartner (June 2007)

"Compte tenu des ressources de Cisco, nous nous attendons à ce qu'IronPort devienne un leader sur la sécurité Web en 2008, et une menace très importante pour BlueCoat."

Quelques clients IronPort au Maroc

Les Domaines

Agenda

- Overview Business Unit
- Overview Technologies/Produits
- Pourquoi pousser IronPort ?

Le phishing change

- Nouvelles tendances

  Pharming

  Spear phishing : social engineering

  Attaques dites d'erreur typographique : www.googkle.com

- 1/3 des sites phishing hostent désormais du malware

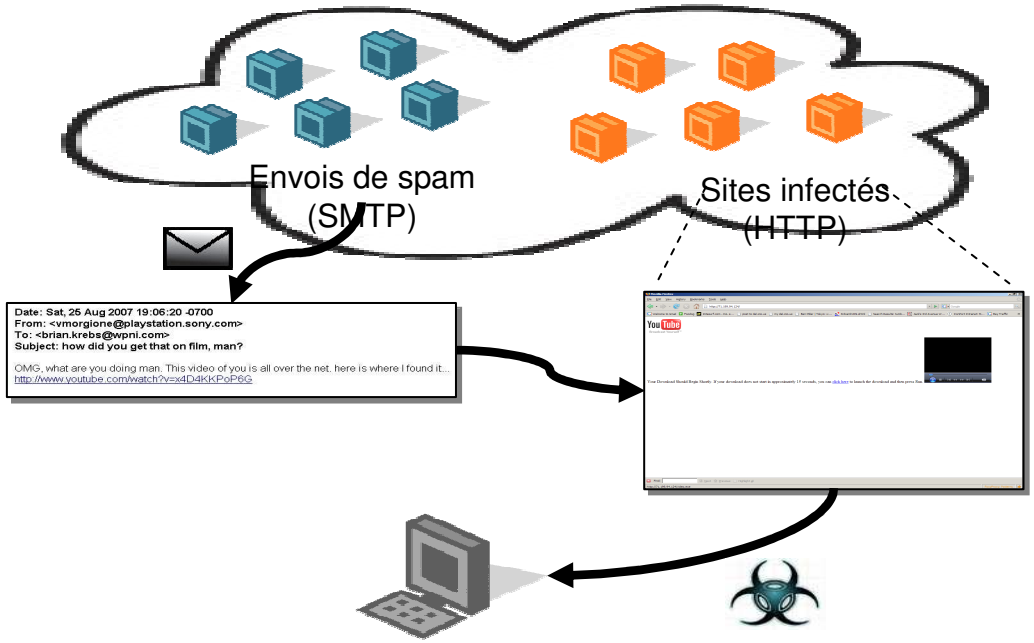
- Les sites de phishing restent en ligne en moyenne 3 jours

Source : Anti-Phishing Working Group

Les zombies changent

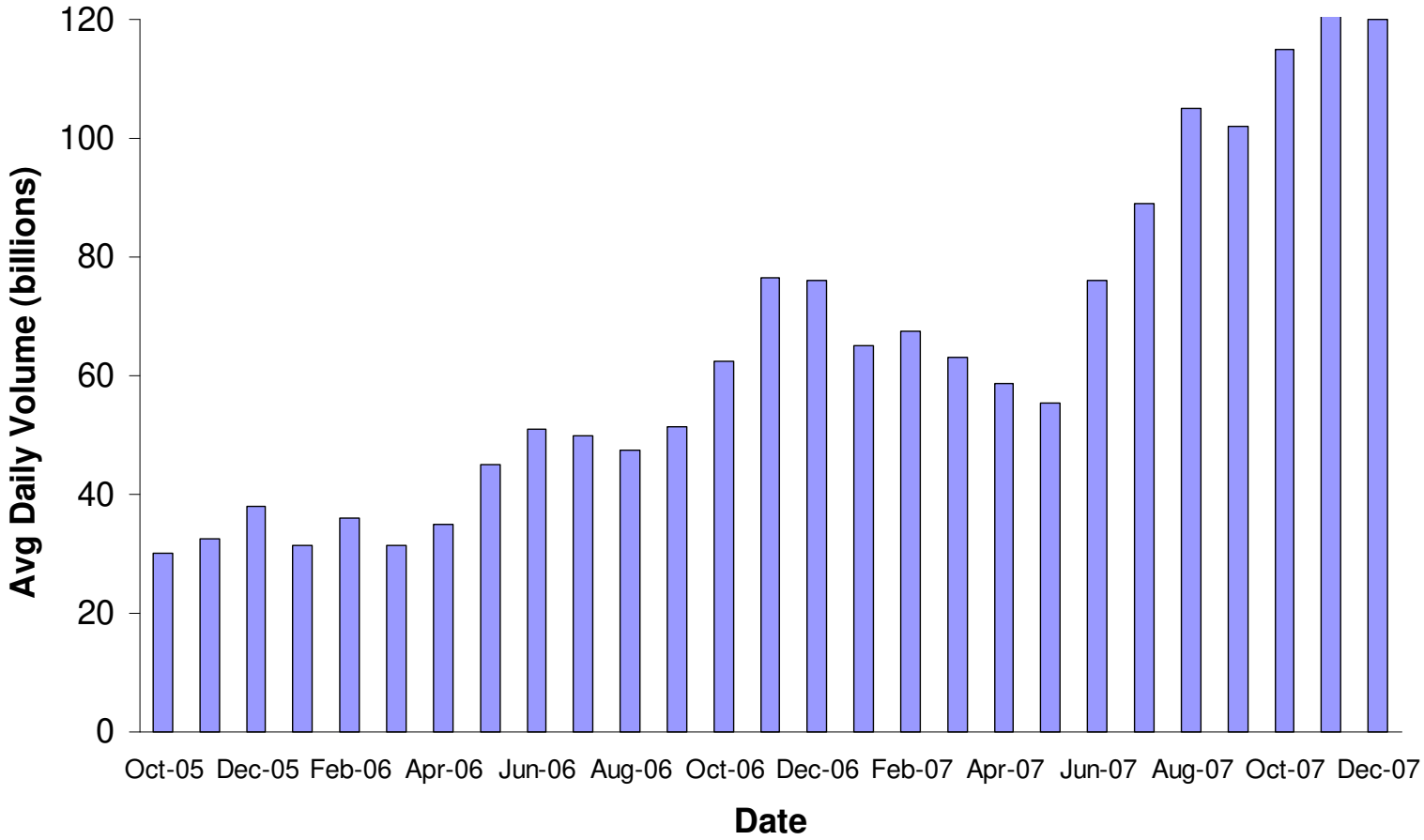
Le réseau Storm

- **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** : envoie du 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



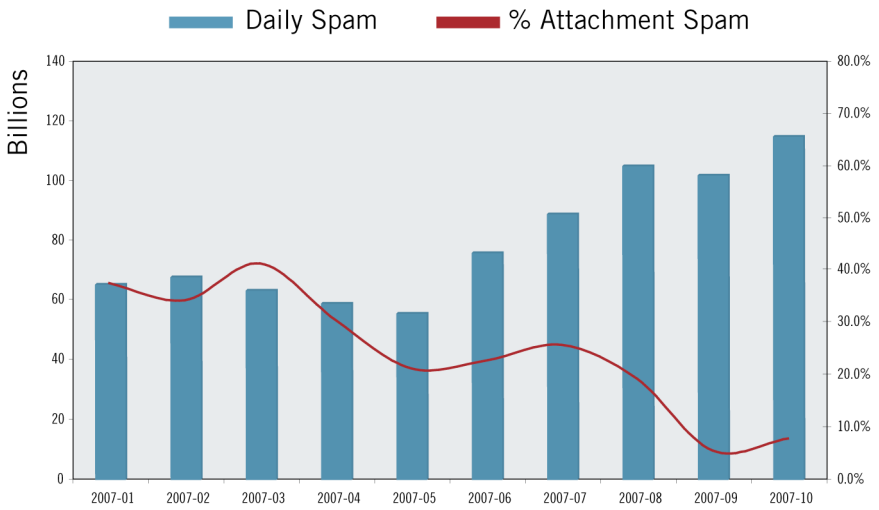
Le Spam continue à croître

x4 en 2 ans !



Les techniques de spam changent

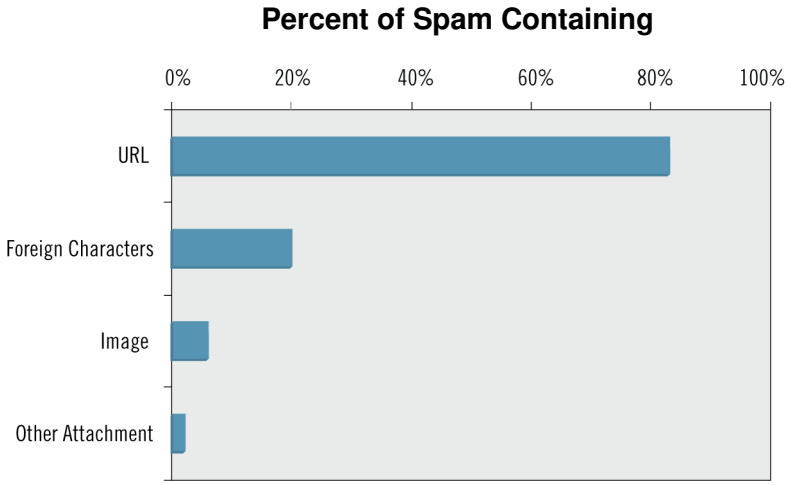
Des images aux liens Web



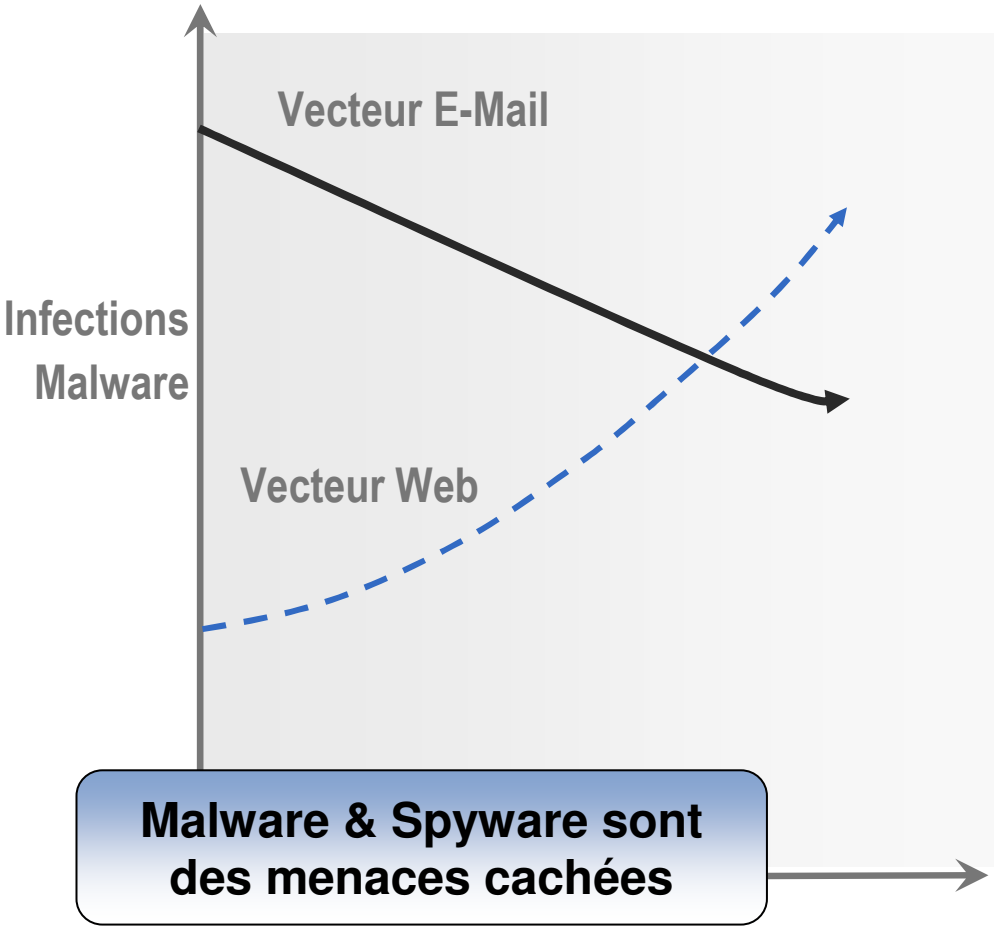
Le spam croît,
mais la part des fichiers attachés diminuent

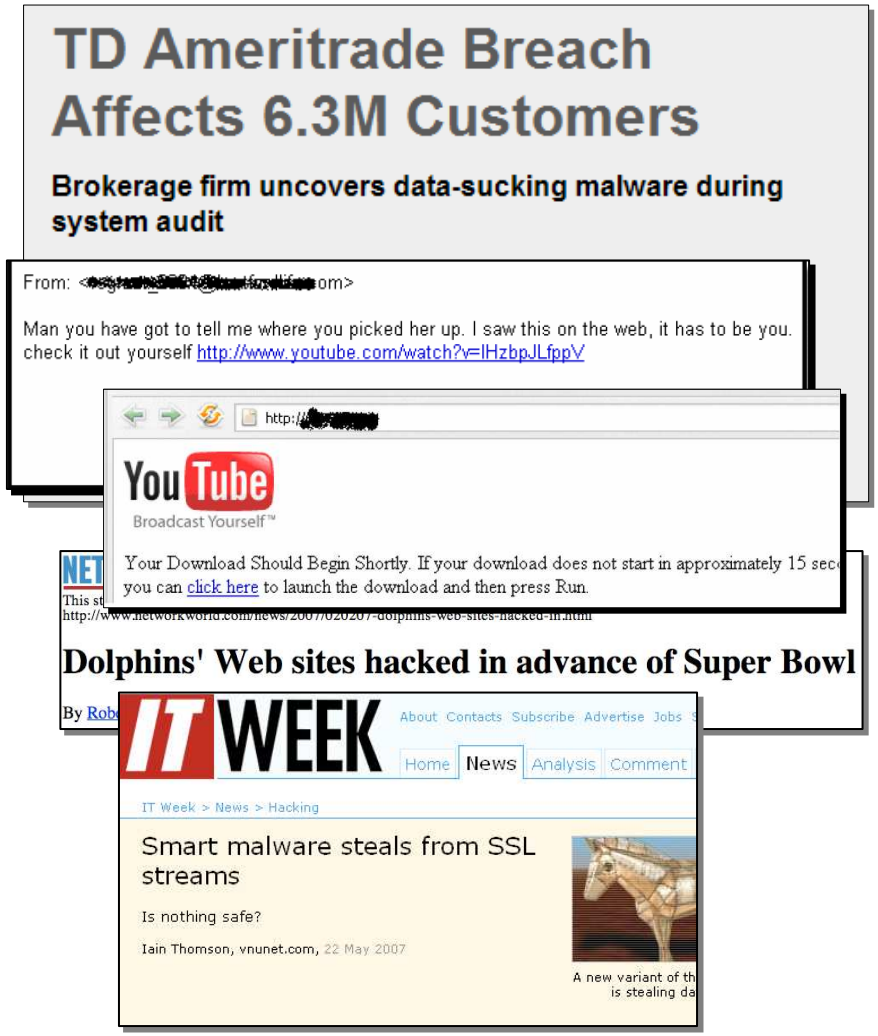
Le spam contenant des URL continue à croître

(+ 253% en 2007 vs 2006)



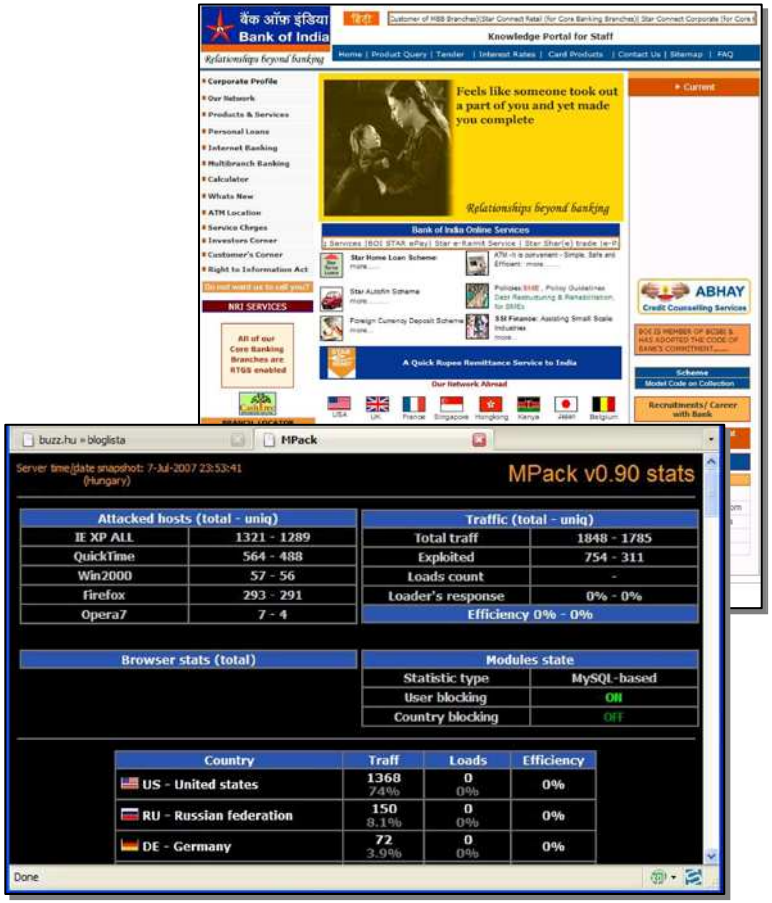
Les vecteurs de menaces changent





Les sites légitimes distribuent le malware

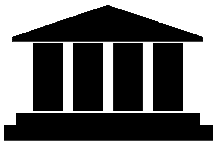
- 70% des infections Web viennent de sites ‘légitimes’ (étude Google Mai 2007)
- Attaques iFrame
  1. Un site légitime est compromis (ajout d’1 iFrame sur une page)
  2. L’utilisateur est redirigé par l’iFrame vers un site infecté
  3. Un malware se télécharge automatiquement sur le poste en exploitant 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



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 réglements
  - SOX, HIPAA, GLBA, PCI, etc.

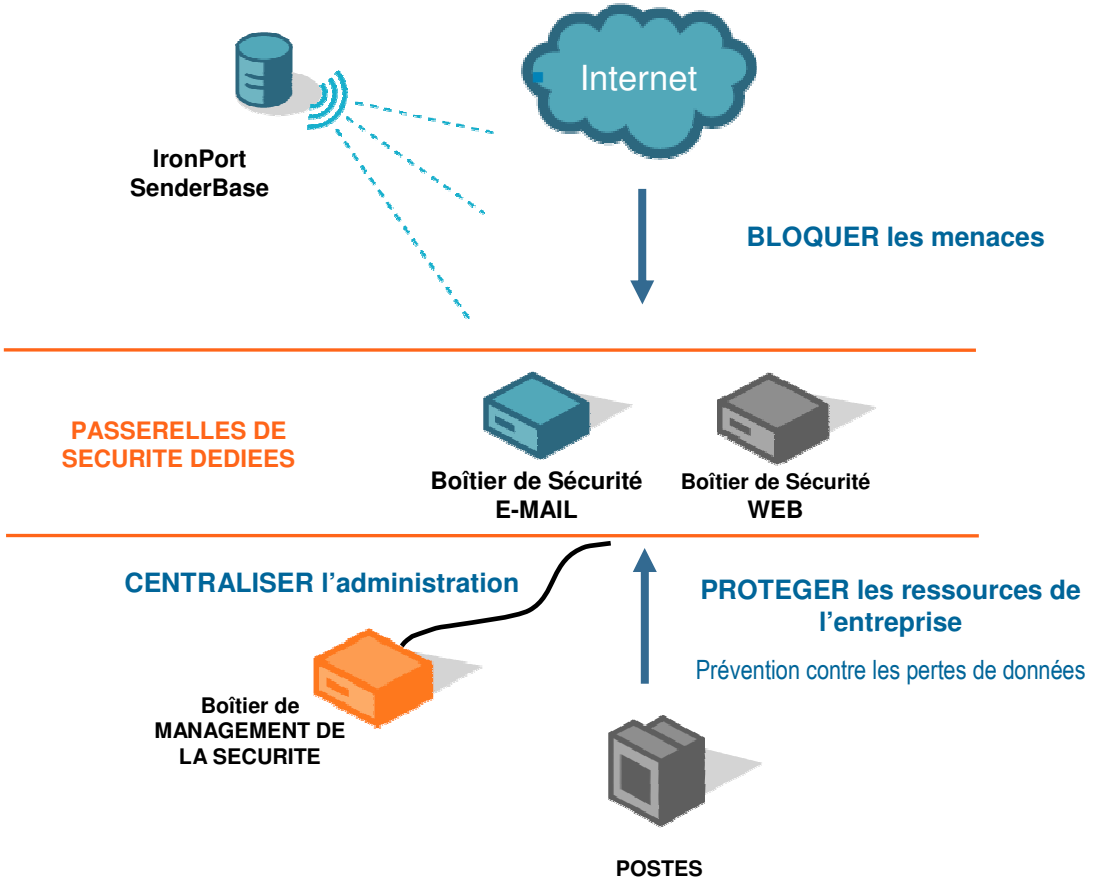


IDC Analyze the Future

"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

La vision IronPort



Sécurité Web | Sécurité E-Mail | Gestion de la Sécurité

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*

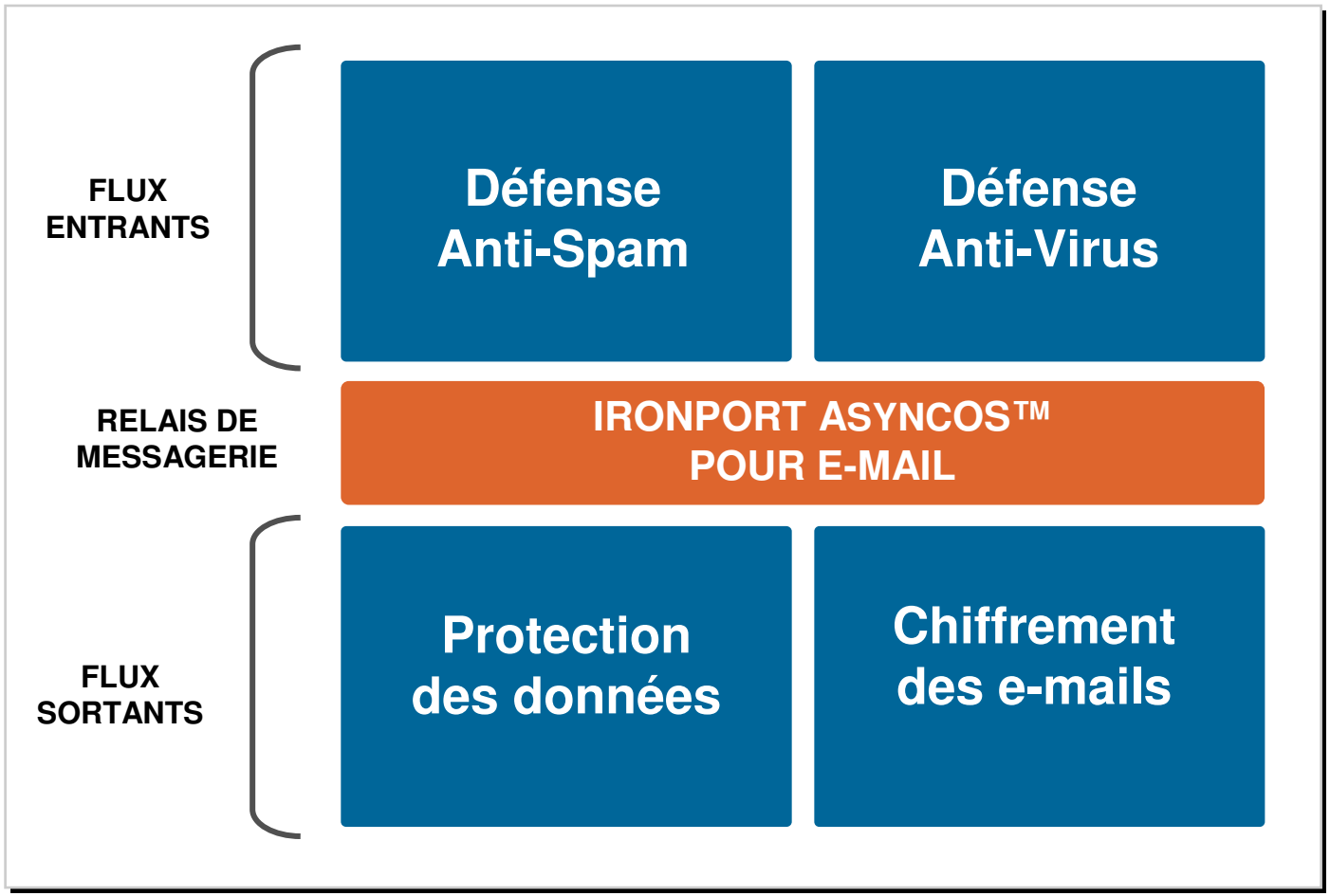
E-Mail Reputation Filters → **Score de réputation**

- *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**

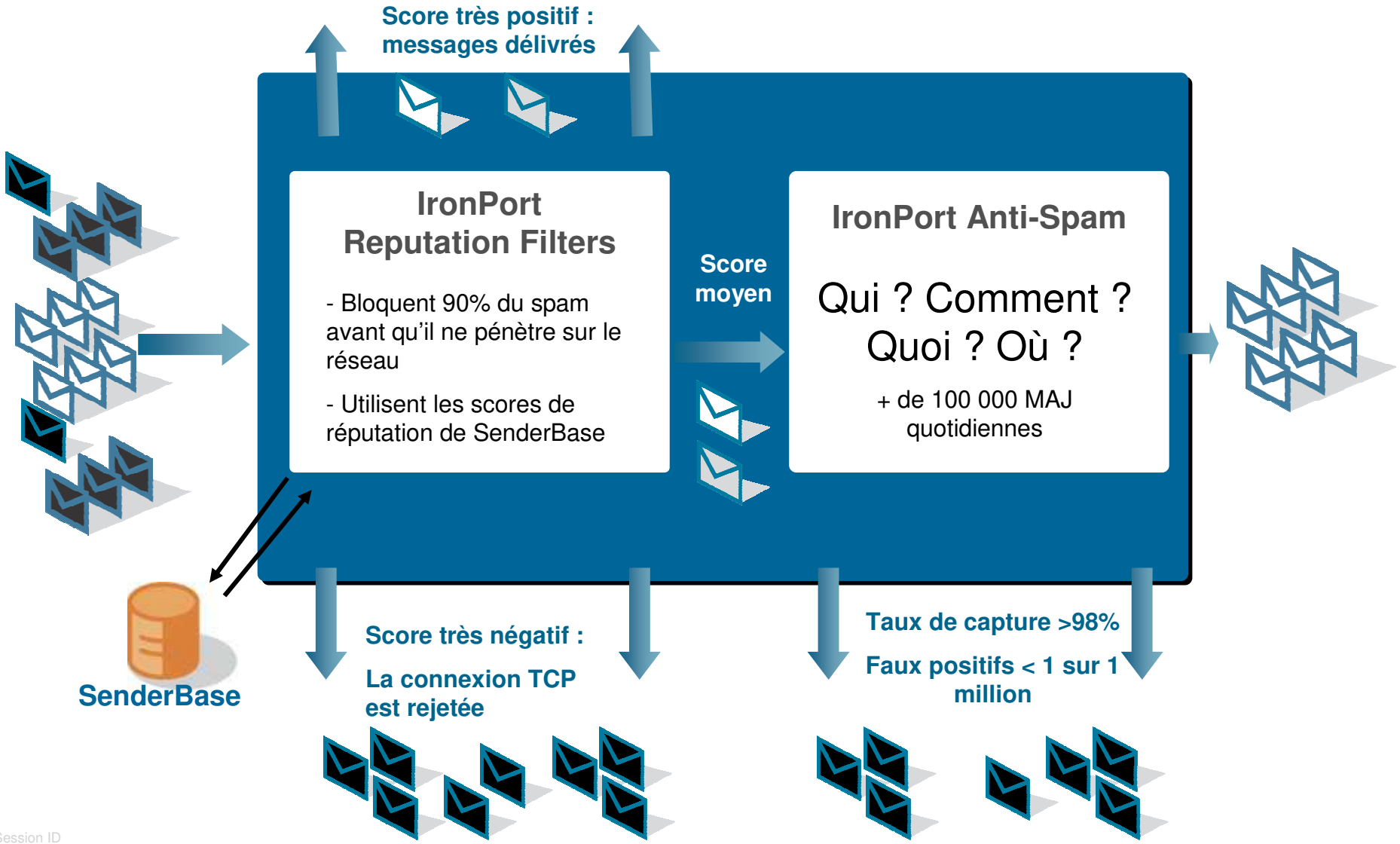
Architecture Série C IronPort

Sécurité des flux entrants et sortants

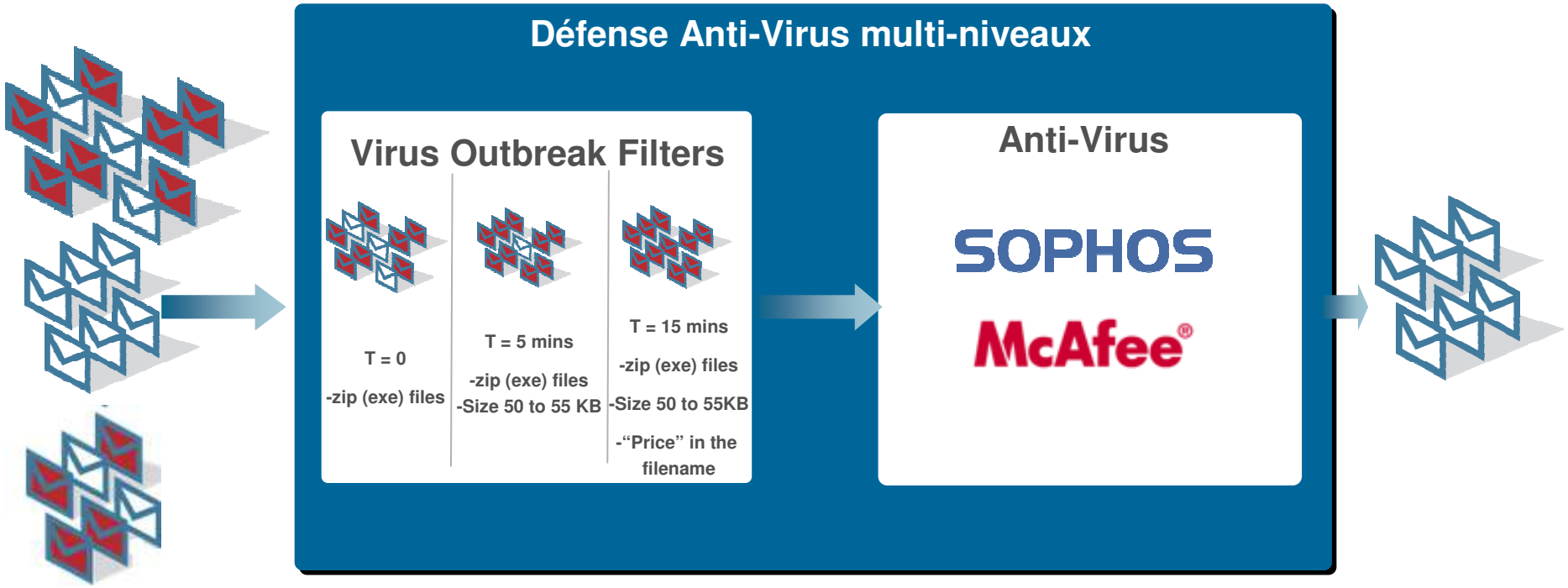


La défense Anti-Spam IronPort

Une protection multi-niveaux



La défense Anti-Virus IronPort



L'avantage Virus Outbreak Filters

www.ironport.com/toc

Temps moyen de protection additionnelle *…… + de 13 heures

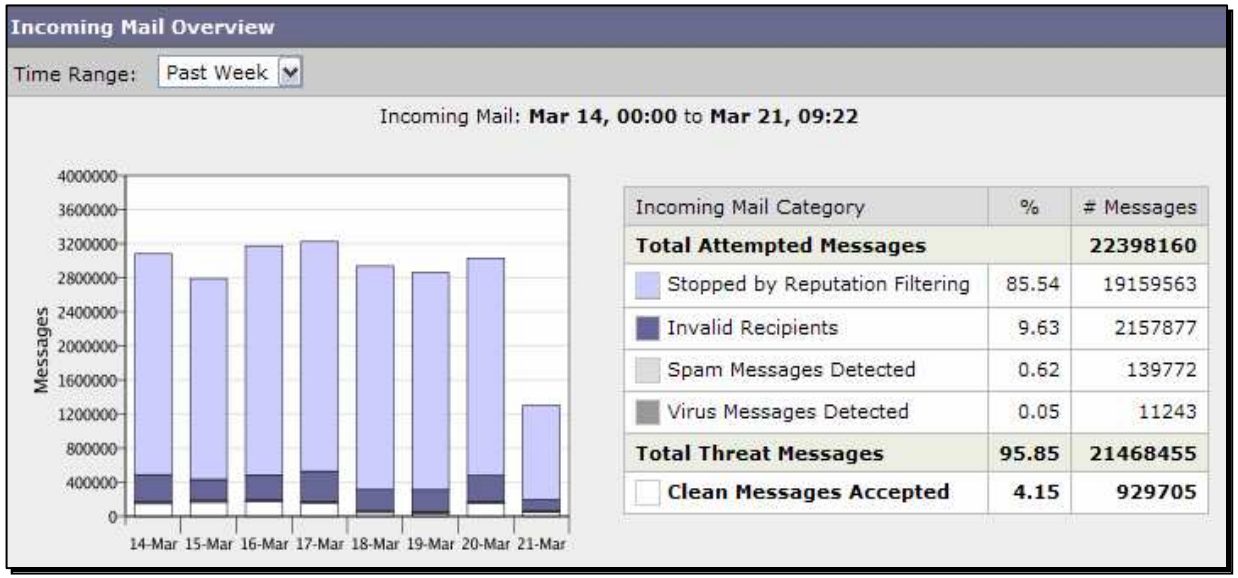
Sur un total d'attaques bloquées de * …….. 248 alertes

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.

Défense Anti-Spam & Anti-Virus

Exemple Dell



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**

Efficacité anti-spam x**10**
68 serveurs avec Spam Assassin remplacés par 8 boîtiers Série C
Coûts réduits de **75%**

"IronPort a augmenté la qualité et la fiabilitié de nos opérations IT, tout en réduisant nos coûts."

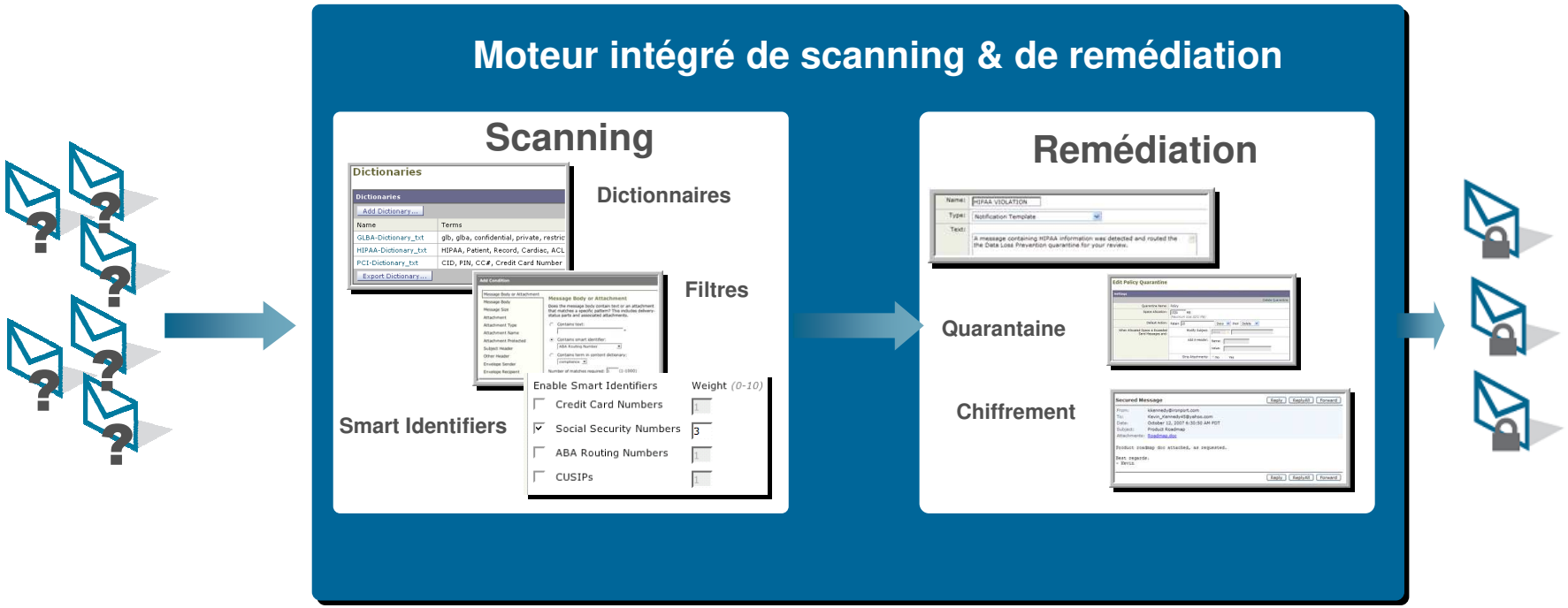
— Tim Helmsetetter
Manager, Global Collaborative Systems Engineering and Service Management,

DELL CORPORATION

BOITES AUX LETTRES	100,000

Protection des données

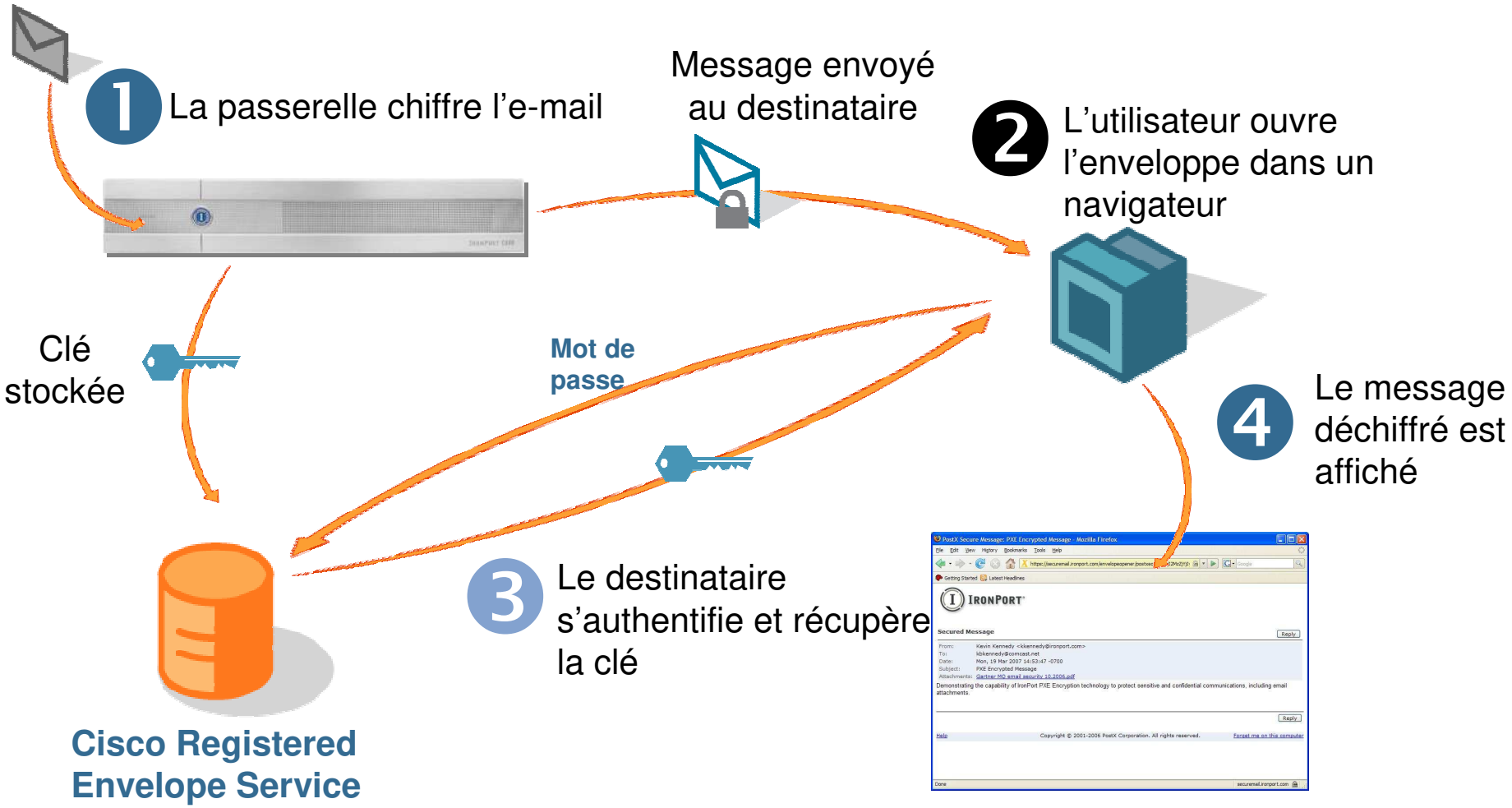
IronPort Data Loss Prevention



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…

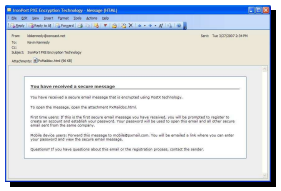
IronPort PXE: Comment ça marche?



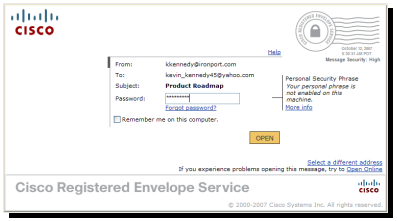
IronPort PXE

Vu par le destinataire du message

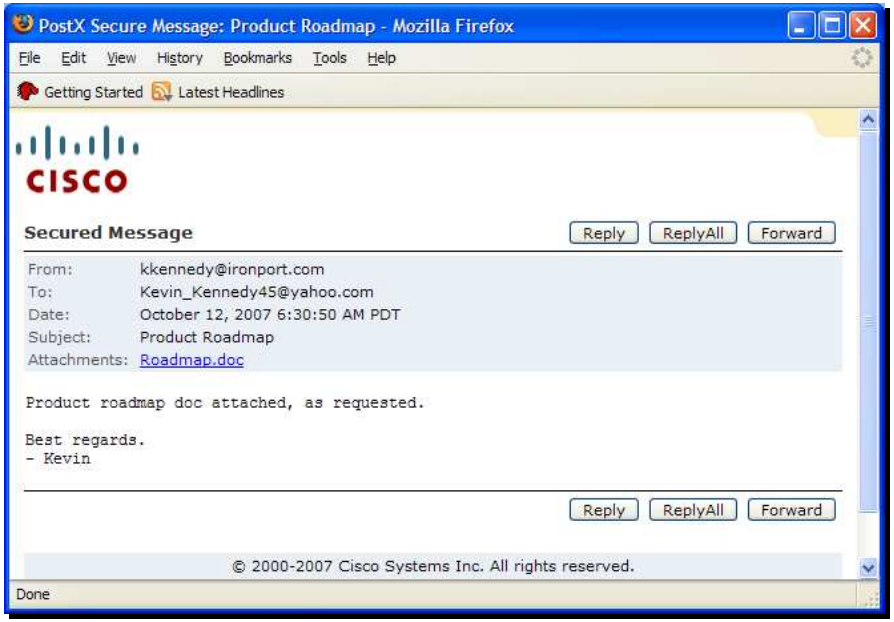
1. Ouvre l'attachement



2. Entre son mot de passe

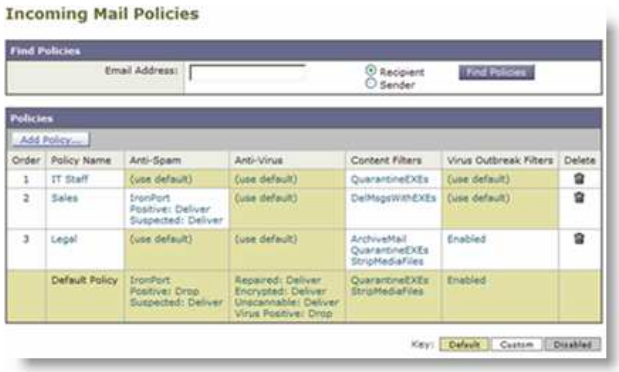


3. Lit le message



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

Le Trafic Web

De plus en plus de sites inconnus

Trafic “facile à catégoriser”

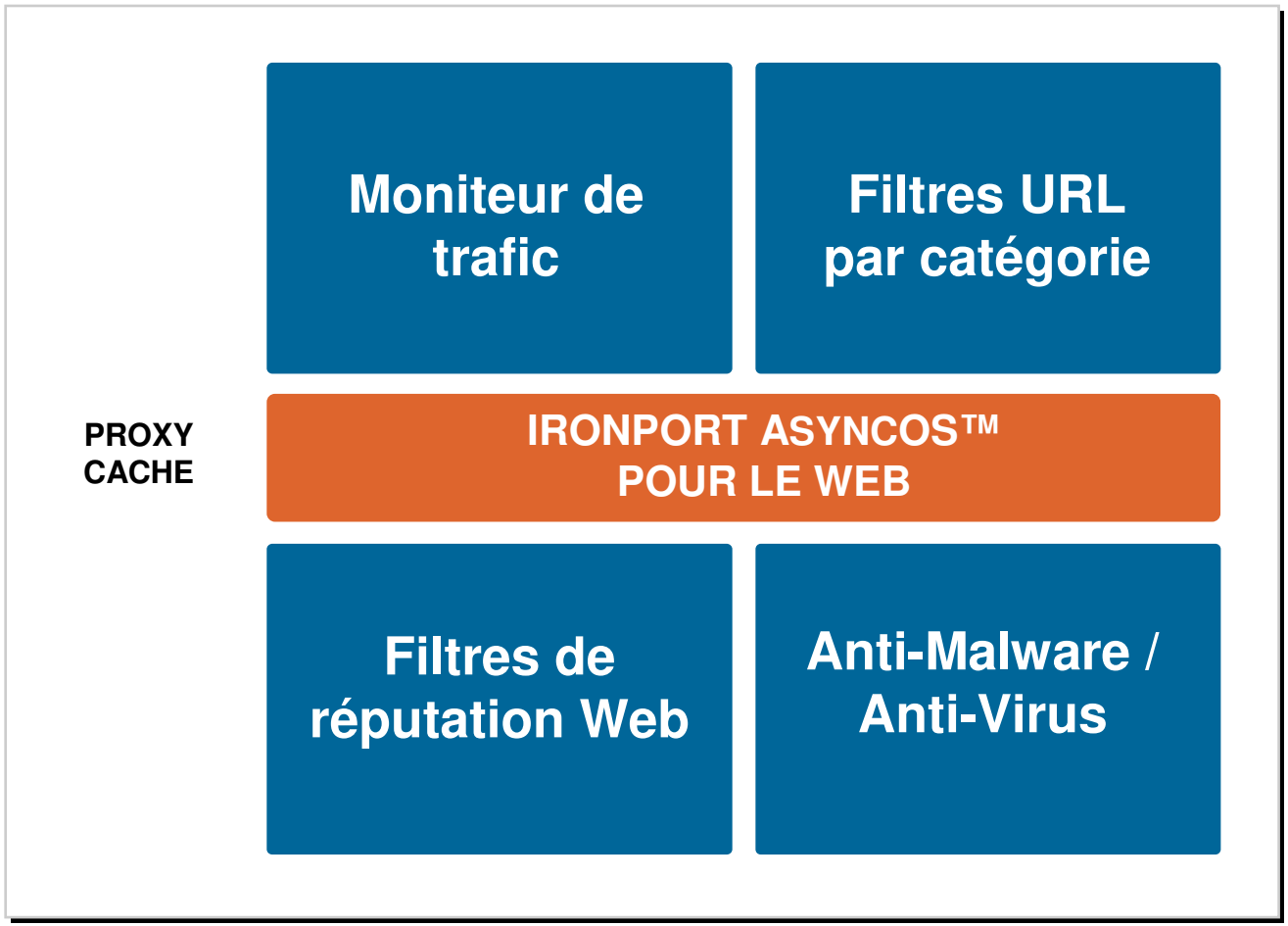
Trafic prévisible,
Domaines connus

Trafic “difficile à catégoriser”

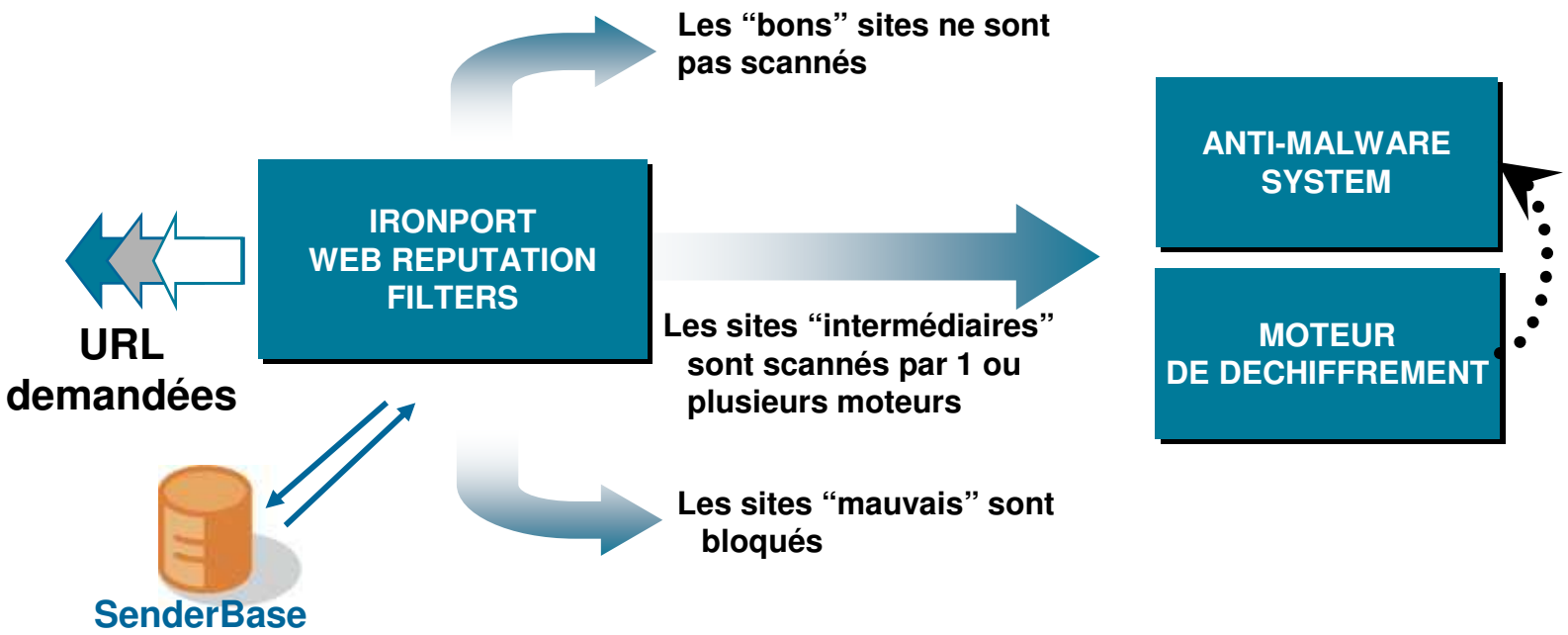
110 millions de sites, en croissance de 40% annuelle
Mélange de sites légitimes, et de sites hostant du malware

Architecture Série S IronPort

Sécurité des flux entrants et sortants



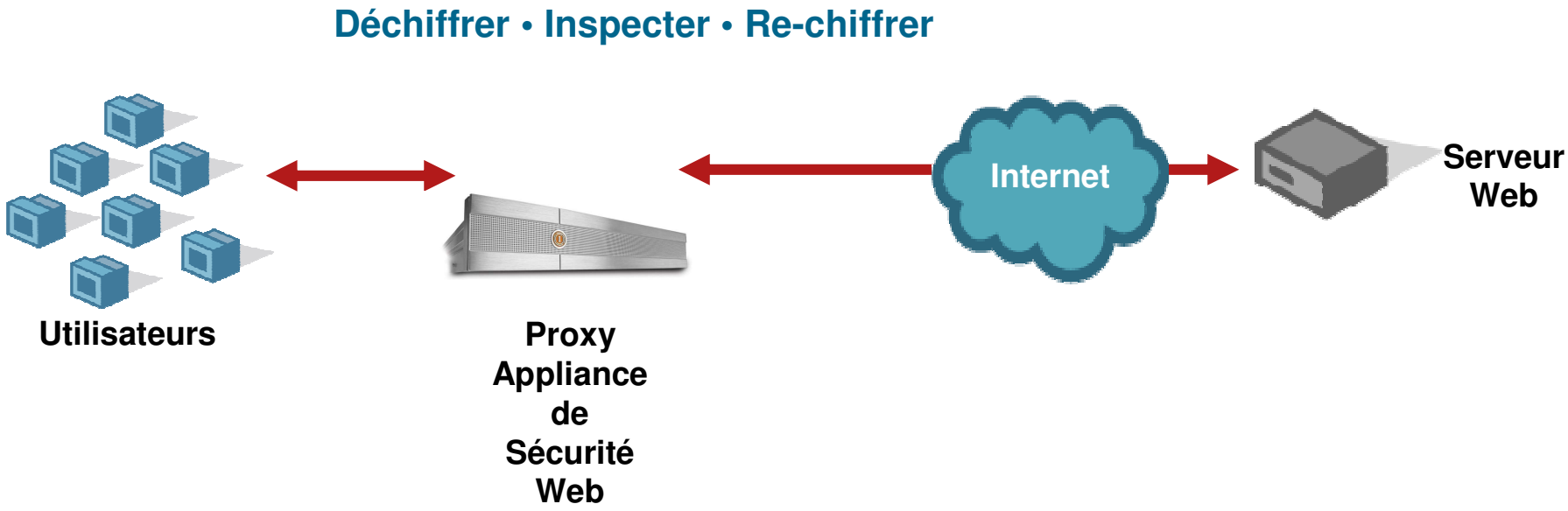
La réputation Web : un filtrage intelligent



- **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** :

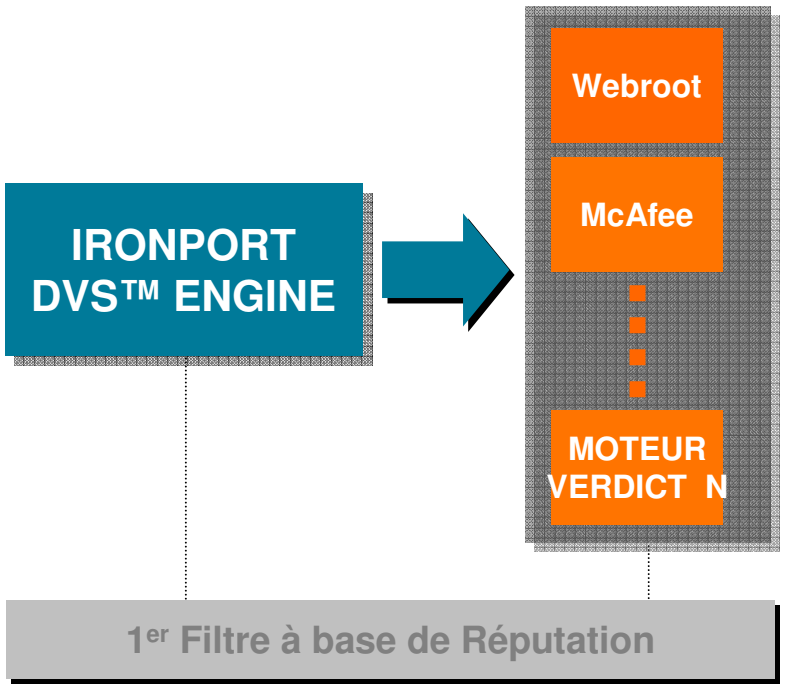
  - Respecte la confidentialité des véritables sessions HTTPS légitimes (par exemple un utilisateur consultant son compte bancaire en ligne)

  - Empêche le téléchargement de malware en toute impunité via des sites HTTPS frauduleux

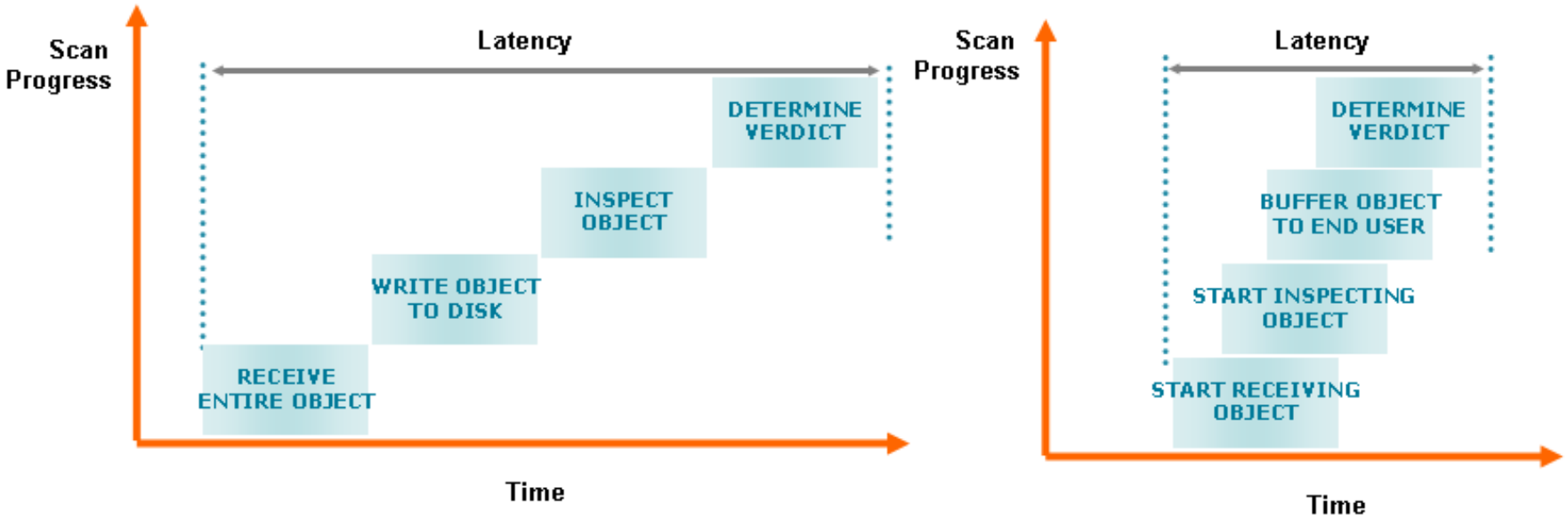
IronPort DVS™ Engine

Filtrage Anti-Malware à base de signatures

- DVS Engine : moteur incluant plusieurs bases de signatures
  - Webroot
  - McAfee
  - 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

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