IRONPORT®

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.

CISCO

Agenda

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

IRONPORT®

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**
  - 1er à développer un MTA hautes performances
  - *SenderBase: la plus grande base de monitoring*
  - 1er avec *Reputation Filtering*
  - 1er avec *Virus Outbreak Filters*

Menaces liées à Internet : les tendances

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 3,6 jours

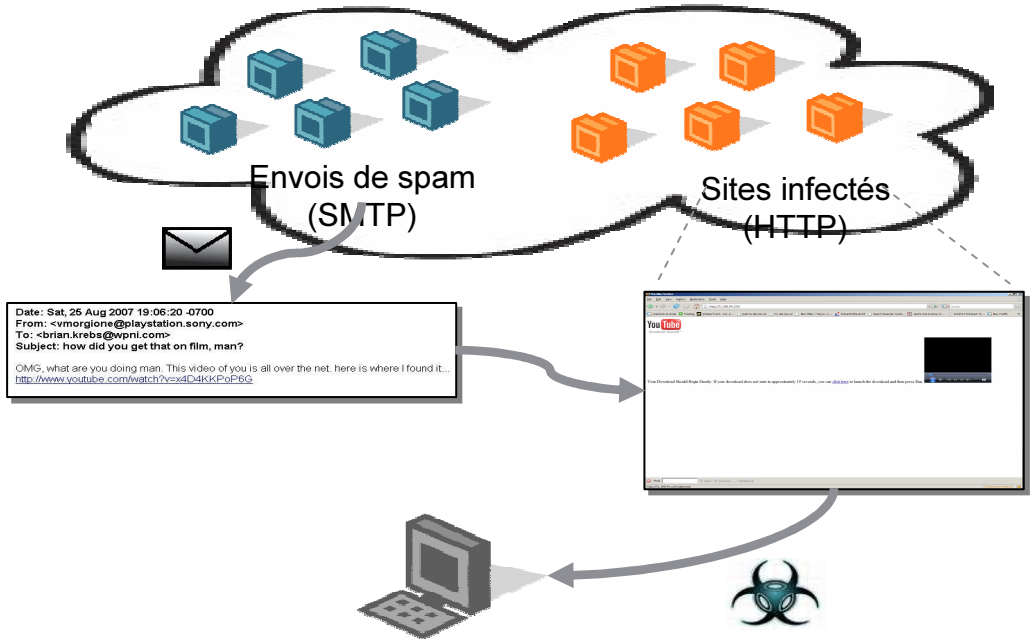
Source : Anti-Phishing Working Group

IRONPORT®

Les zombies changent

Le réseau Storm

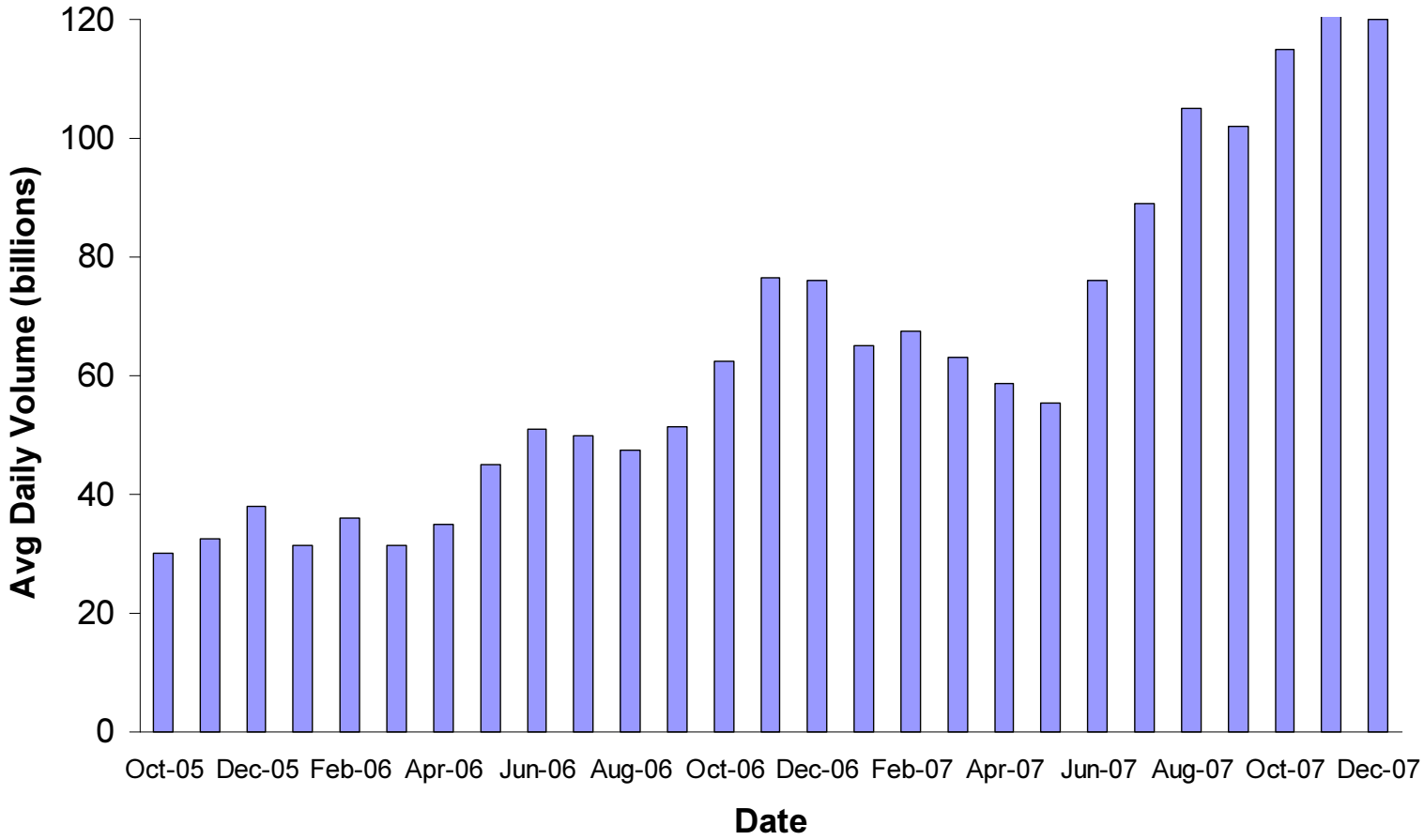
- **Le plus important réseau de zombies sur Internet**
  - 1000 PC infectés loués $220 en Allemagne
  - 1000 PC infectés aux USA proposés à $110
  - Accès loués à l'heure, support téléphonique disponible
- **Se reproduit** : envoie du spam de recrutement de zombies
- **Coordonné** : synchronise des envoi 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



IRONPORT

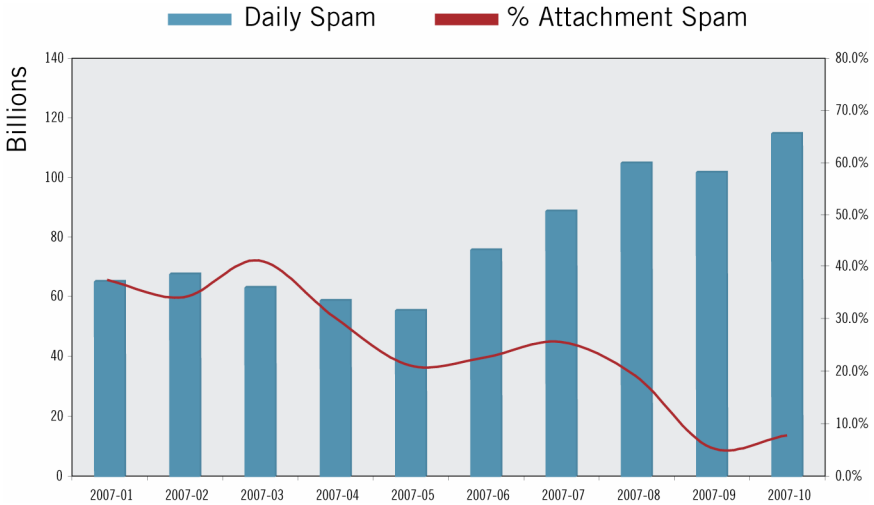
Le Spam continue à croître

x4 en 2 ans !



Les techniques de spam changent

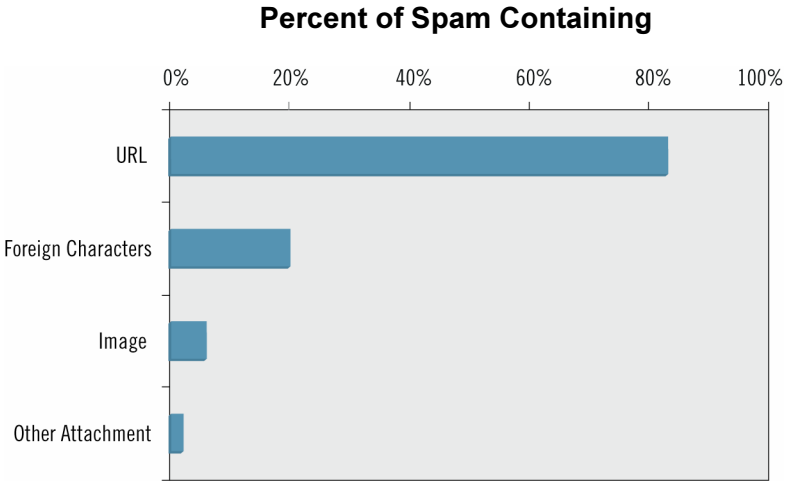
Des images aux liens Web



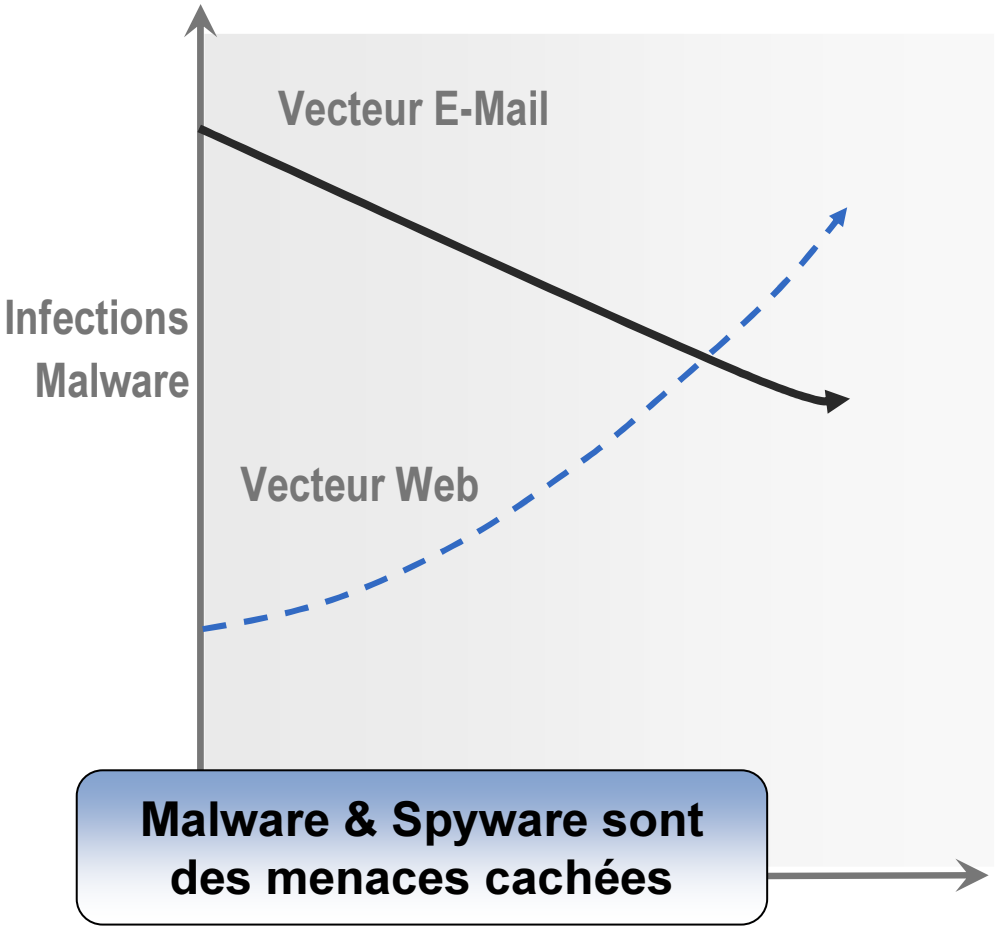
Le spam croît,
mais la part des fichiers attachés diminuent

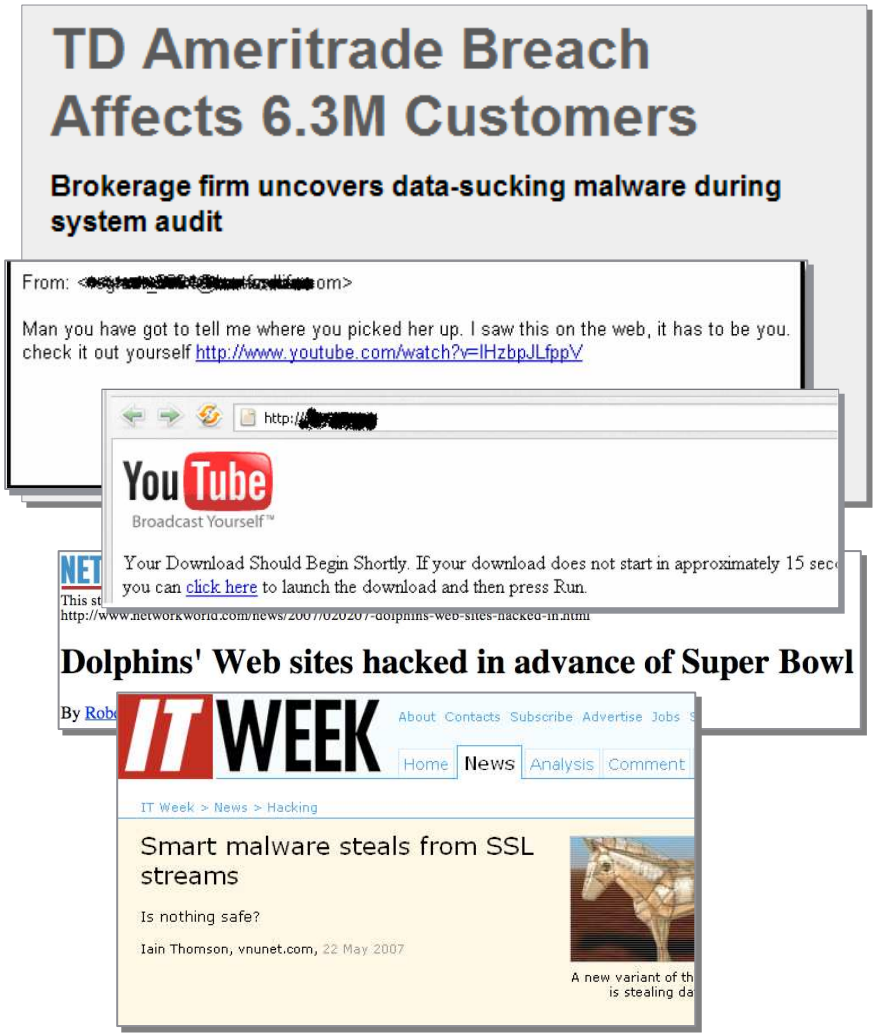
Le spam contenant des URL continue à croître

(+ 253% en 2007 vs 2006)



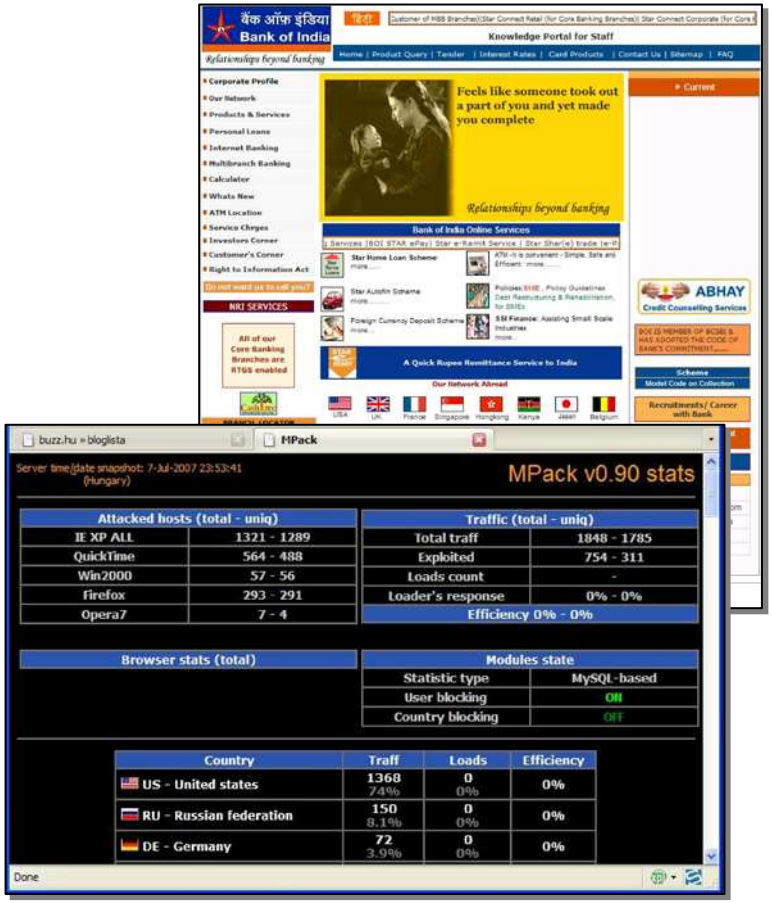
Les vecteurs de menaces changent





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

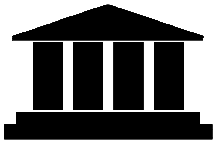


IRONPORT®

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.

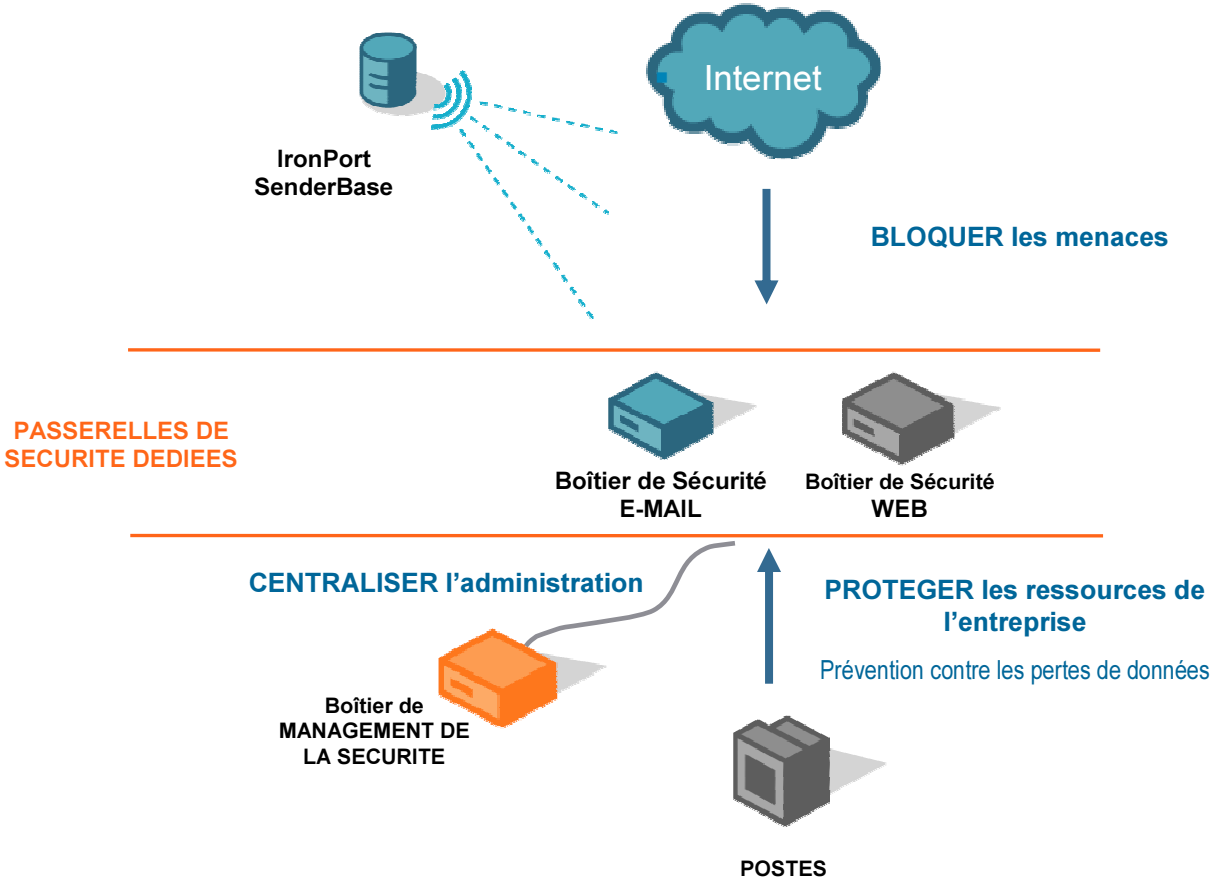


IDC Analyze the Future

"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



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

+ de 90 paramètres

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

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

+ de 50 paramètres

- *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**

IRONPORT®

Sécurité E-Mail

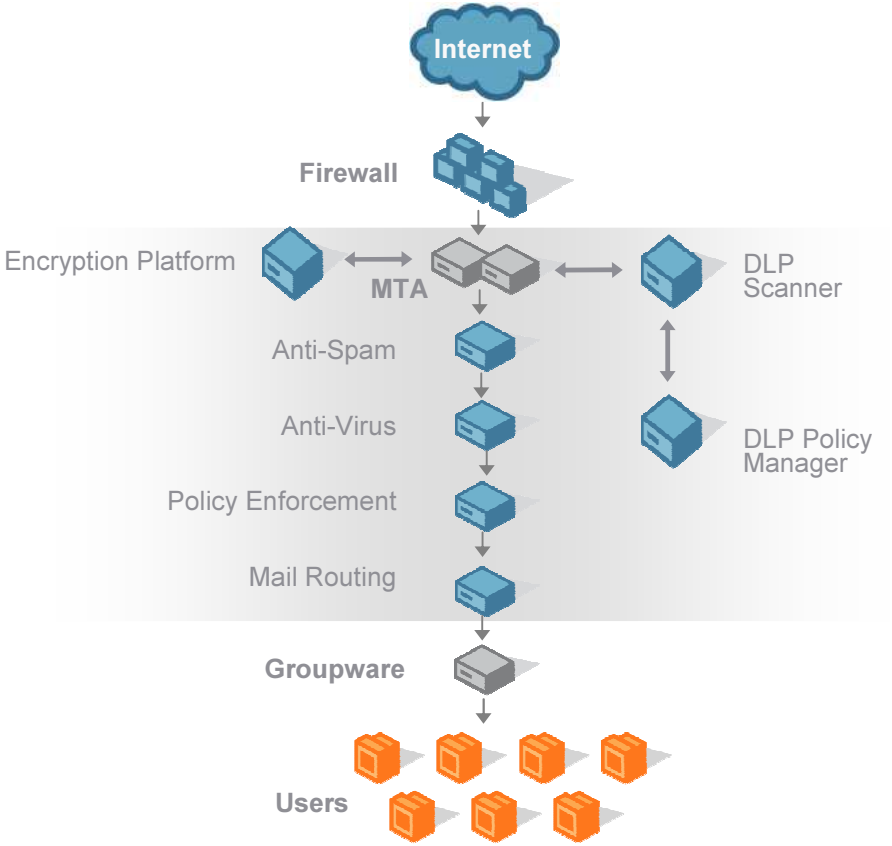
IronPort Série C

IRONPORT™

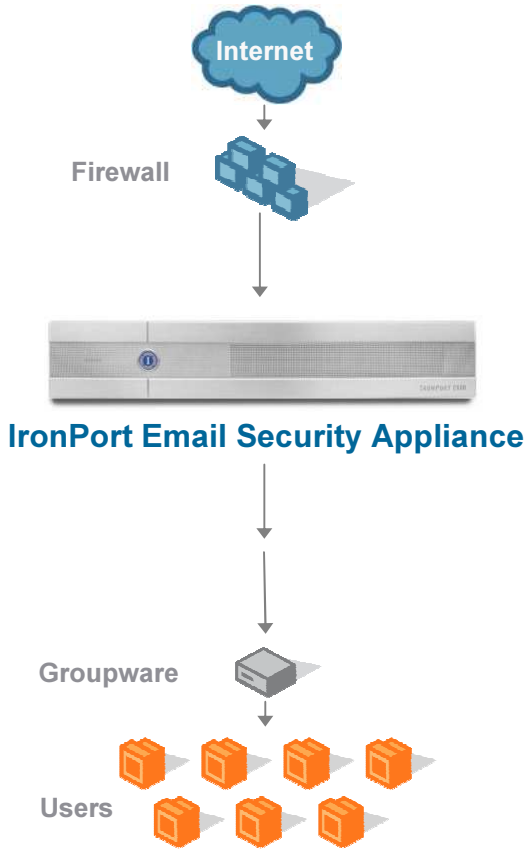
IronPort Consolidates the Network Perimeter

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**

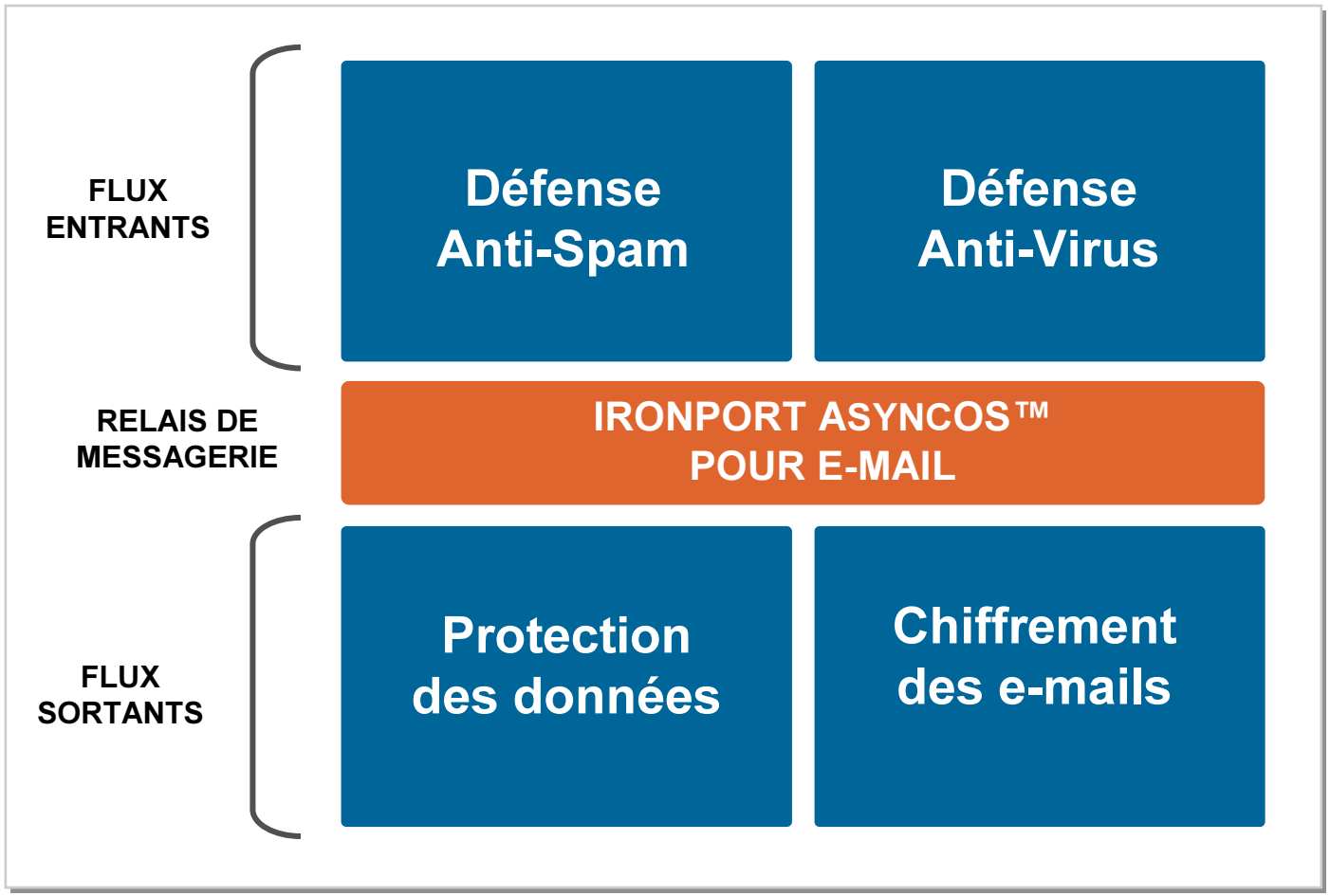
- *blacklists et whitelists d'URL*
- *Contenu HTML*
- *Infos sur le domaine*
- *URL à problèmes "connues"*
- *Histoire du site Web…*

→ **Web Reputation Filters** → **Score de réputation**

IRONPORT®

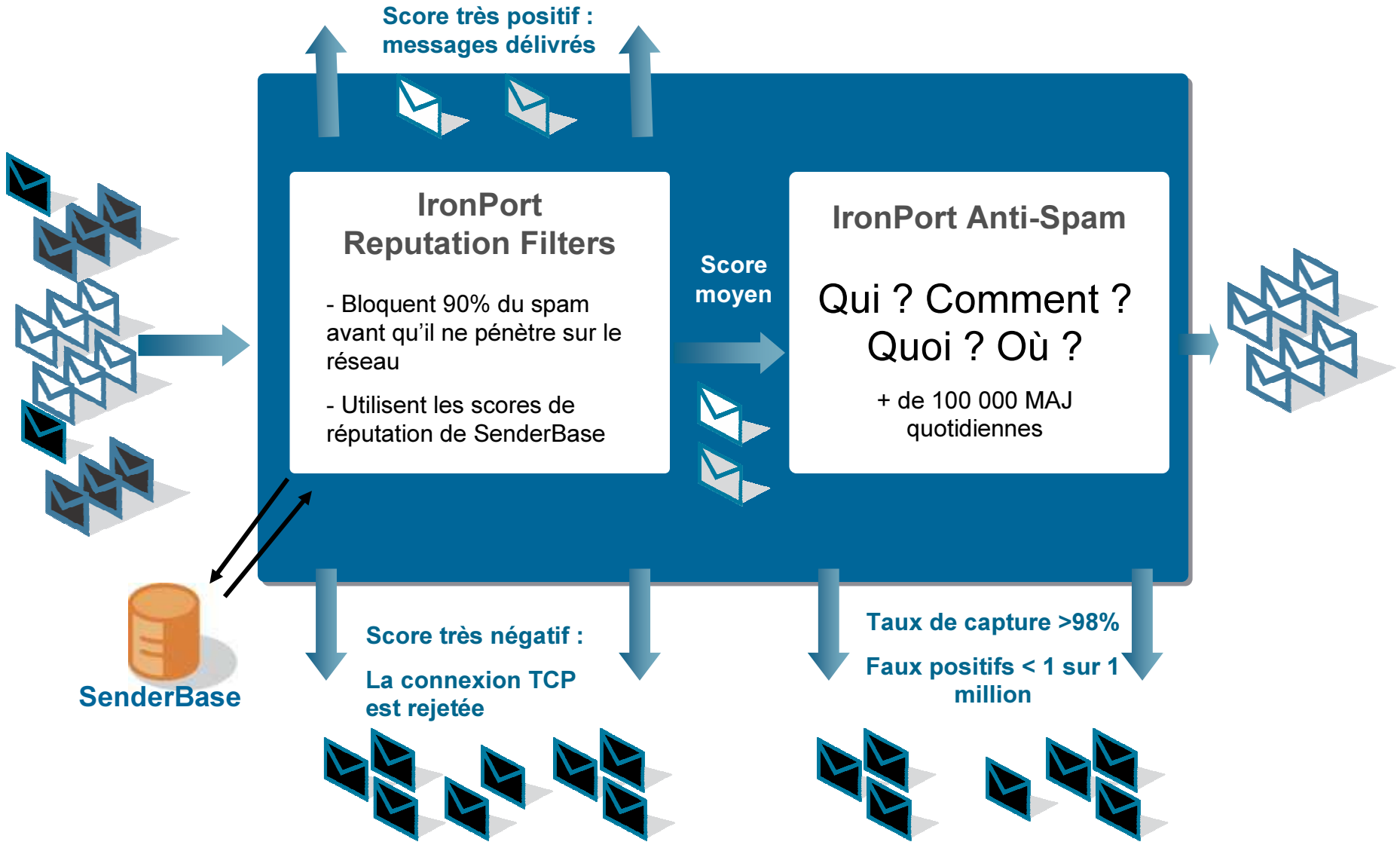
Architecture Série C IronPort

Sécurité des flux entrants et sortants

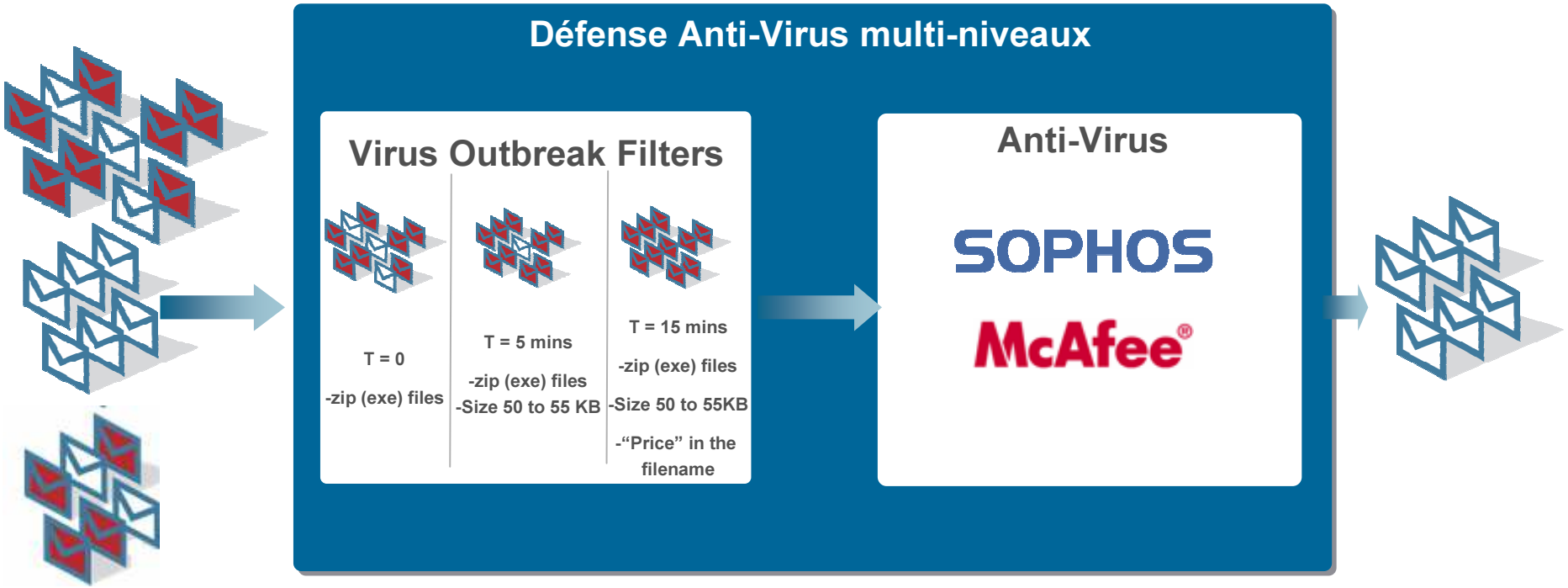


La défense Anti-Spam IronPort

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

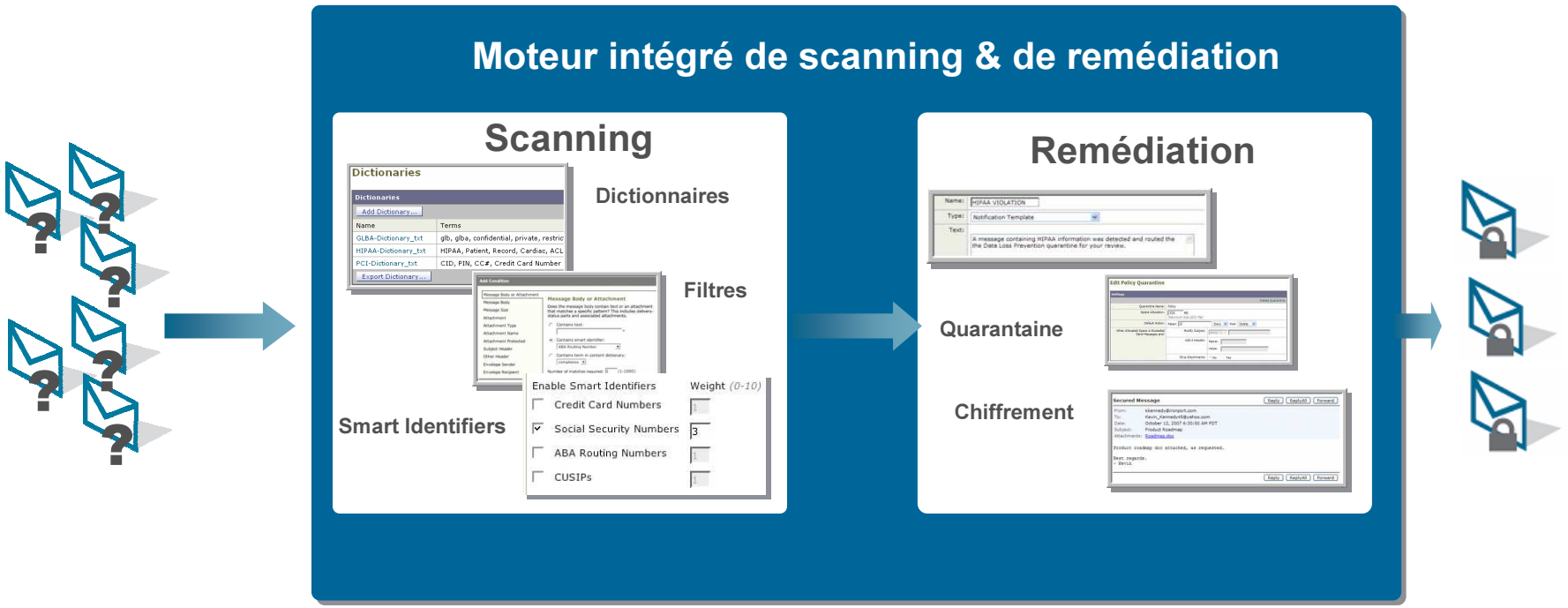
Protection totale incrémentale * …… + de 134 jours

IRONPORT®

** 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.

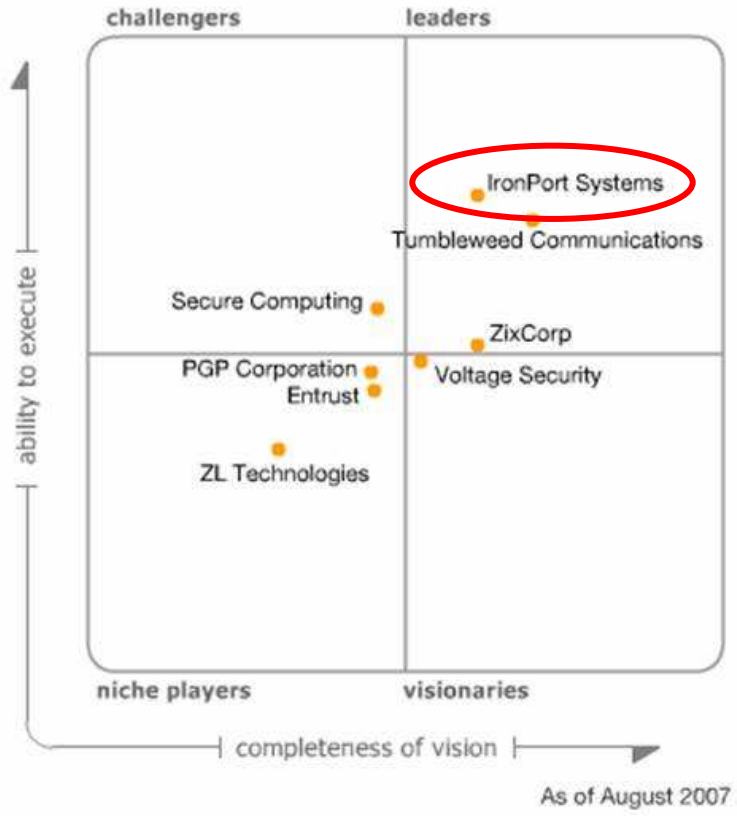
Remédiation : Alerte de l'administrateur, reporting, mise en quarantaine, chiffrement…

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

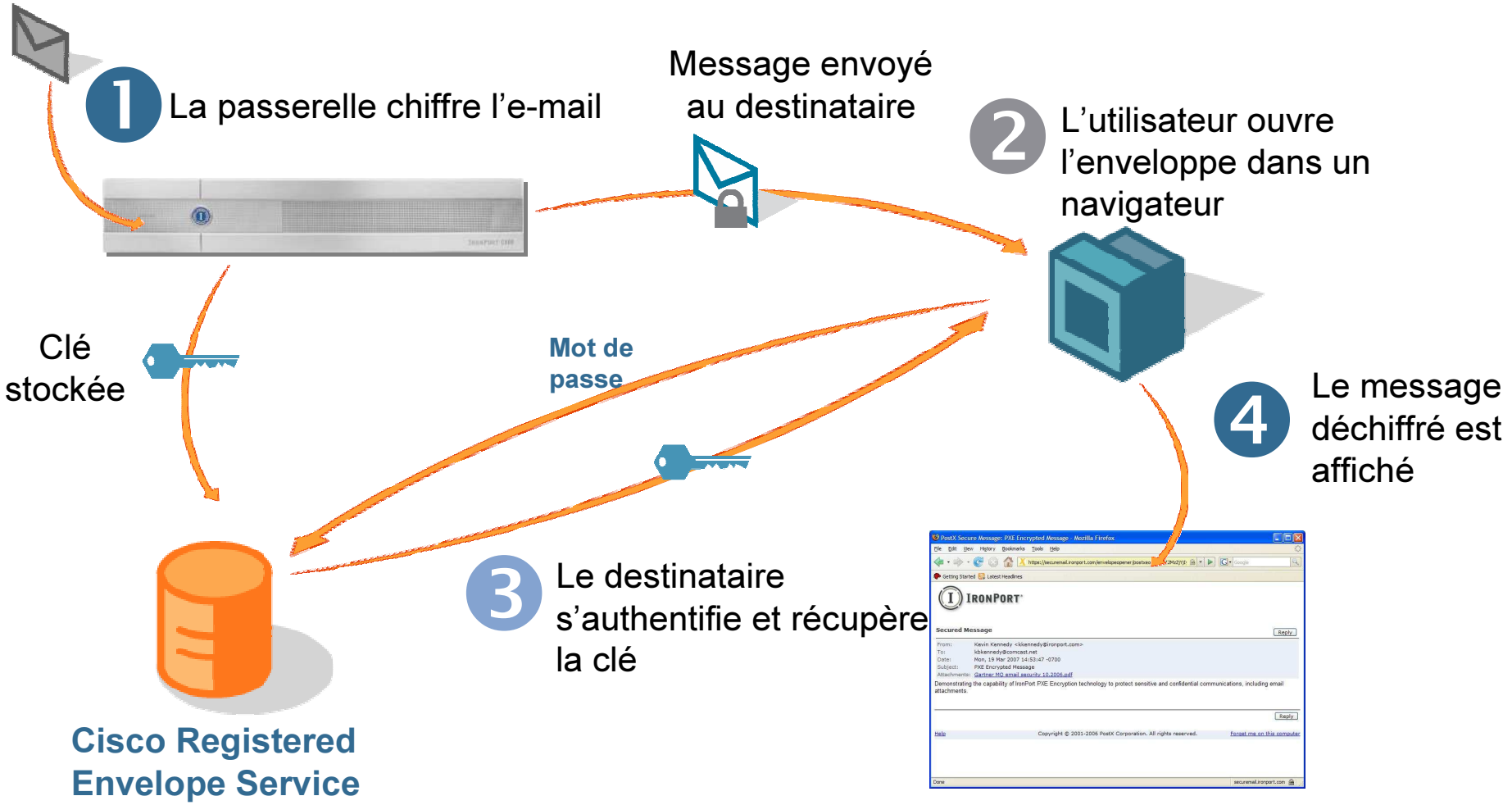
1. Sans besoin d'un logiciel client sur le poste du destinataire
2. Quelle que soit sa plate-forme de messagerie et son système d'exploitation



Source: "Magic Quadrant" Gartner
Chiffrement E-Mail

IRONPORT

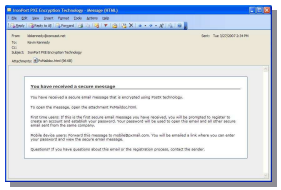
IronPort PXE: Comment ça marche?



IronPort PXE

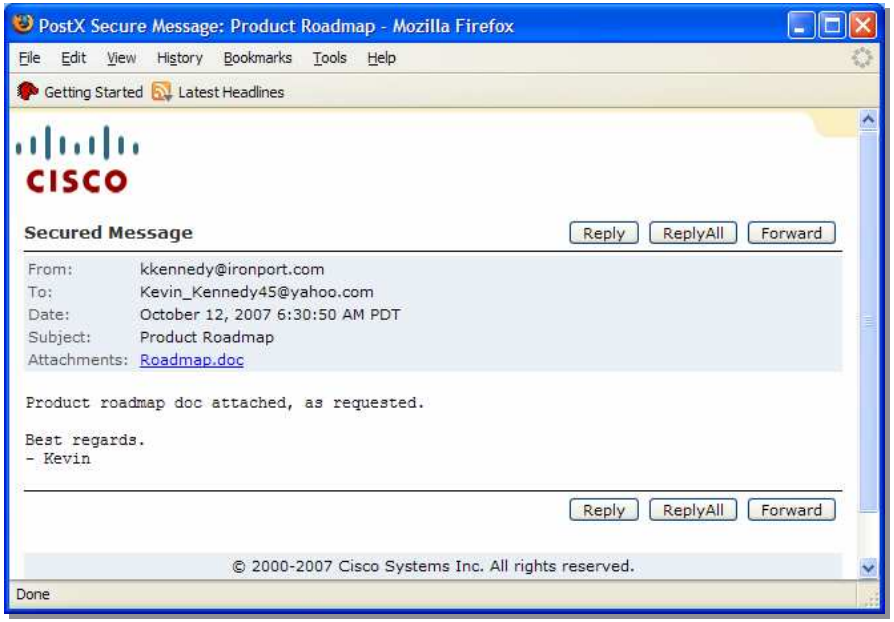
Vu par le destinataire du message

1. Ouvre l'attachement

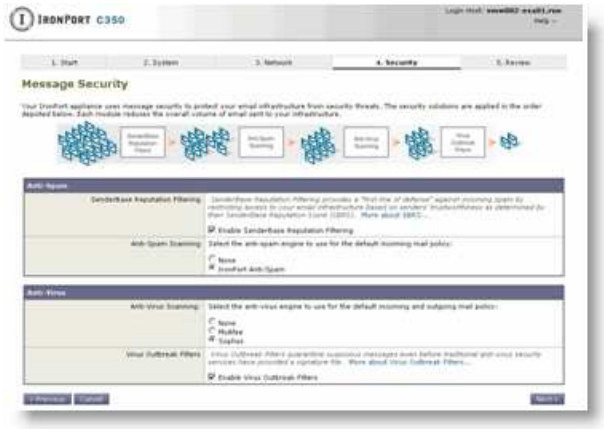


2. Entre son mot de passe

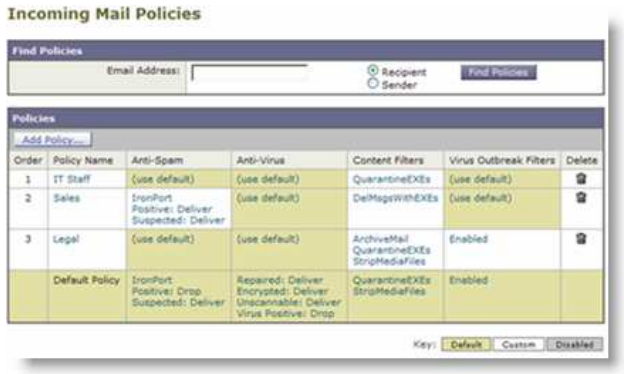
3. Lit le message



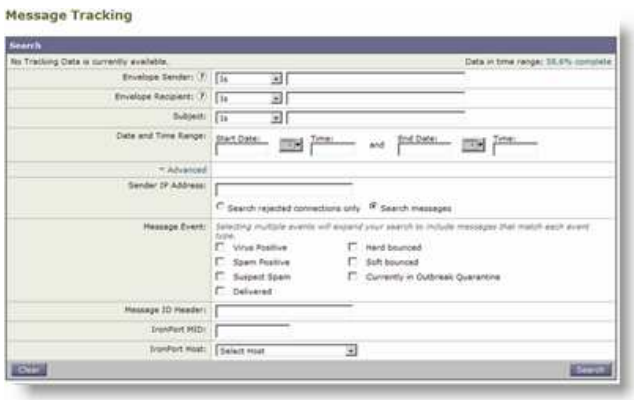
Une administration simplifiée



Installation en 5 étapes



Email Security Manager
Configuration des politiques par groupes

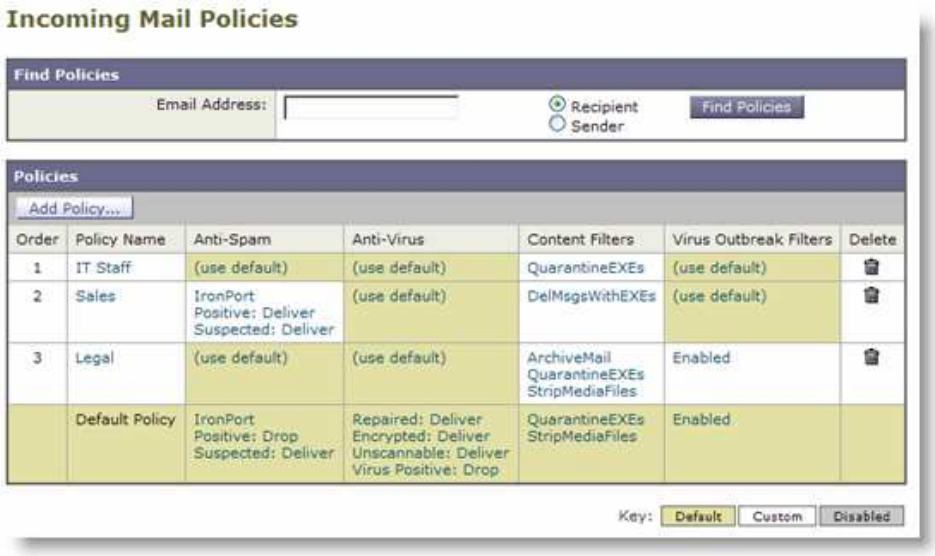


Tracking des messages

E-Mail Security Monitor
Reporting en temps réel

IronPort Email Security Manager™

Définir ses politiques de sécurité par groupes



Catégories: par domaine, utilisateur, ou groupe LDAP

- Autoriser les fichiers audio
- Mettre en quarantaine les .exe

IT

- Marquer et distribuer le spam

SALES

- Effacer les exécutables

LEGAL

- Archiver les messages
- Virus Outbreak Filters désacrivé pour les .doc

IRONPORT®

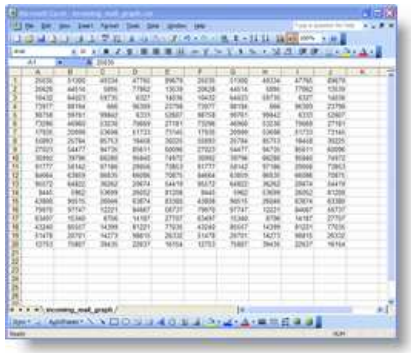
IronPort Email Security Monitor™

Système de reporting avancé

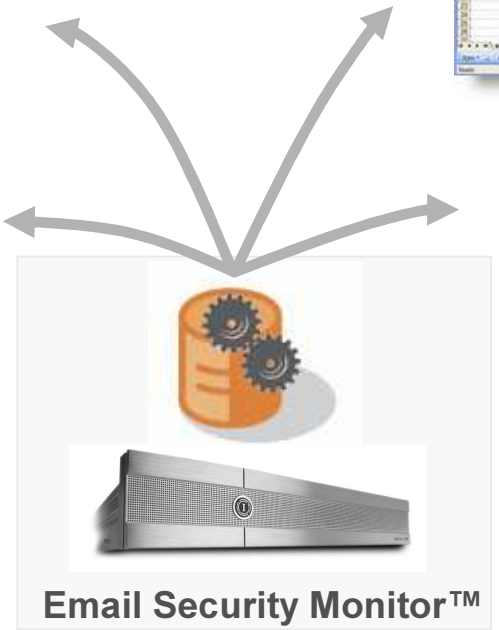
Rapports graphiques en temps réel

Incoming Mail Category	%	# Messages
Total Attempted Messages		**783,990**
Stopped by Reputation Filtering	85	666,392
Invalid Recipients	1	7,840
Spam Messages Detected	7	54,879
Virus Messages Detected	2	15,680
Total Threat Messages	**95**	**744,791**
Clean Messages Accepted	**5**	**39,200**

Exporter en CSV



Envois programmés

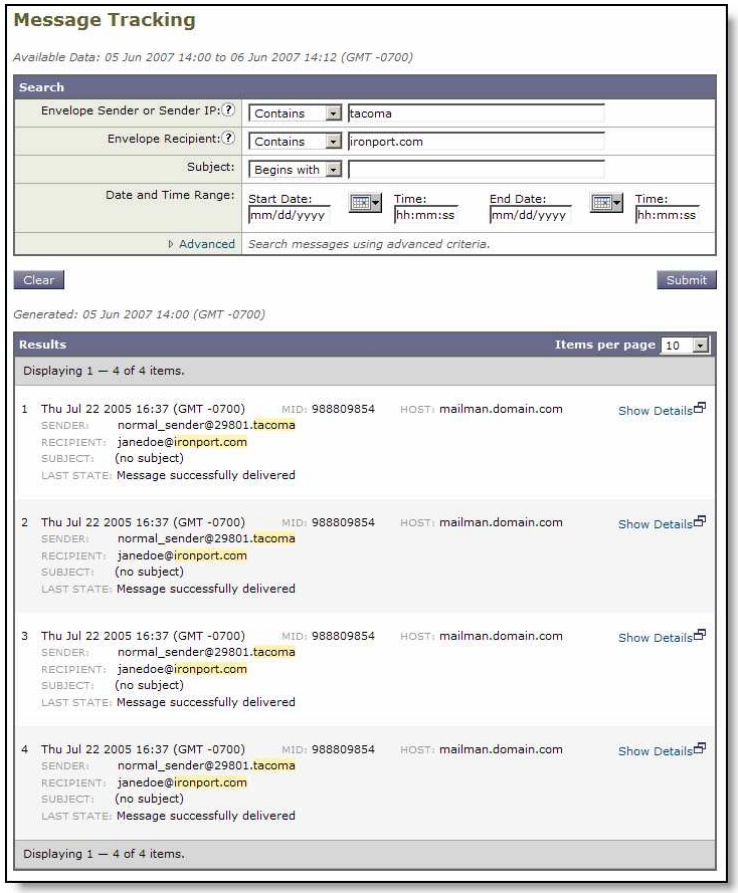


Recherches par domaine

IRONPORT®

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**

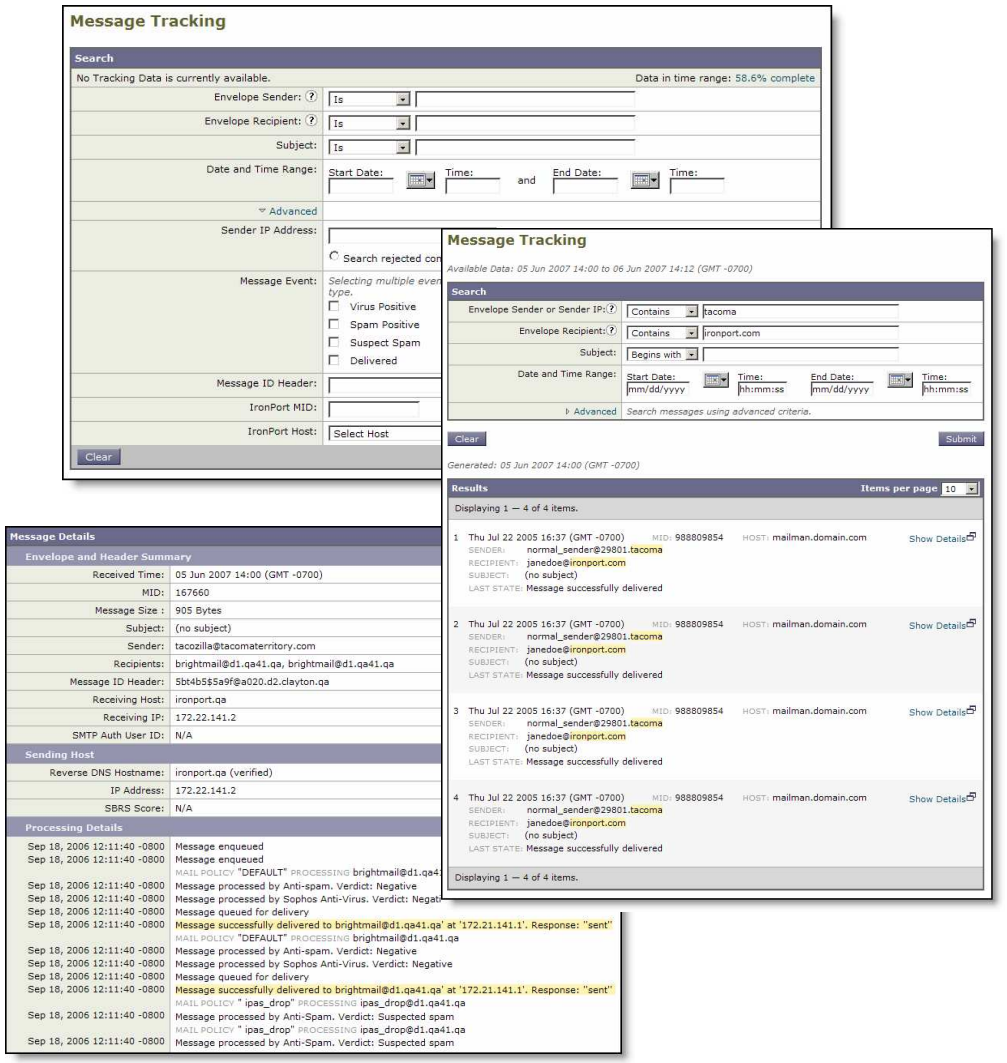


IRONPORT®

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



IronPort Série C

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

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

IRONPORT®

IRONPORT®

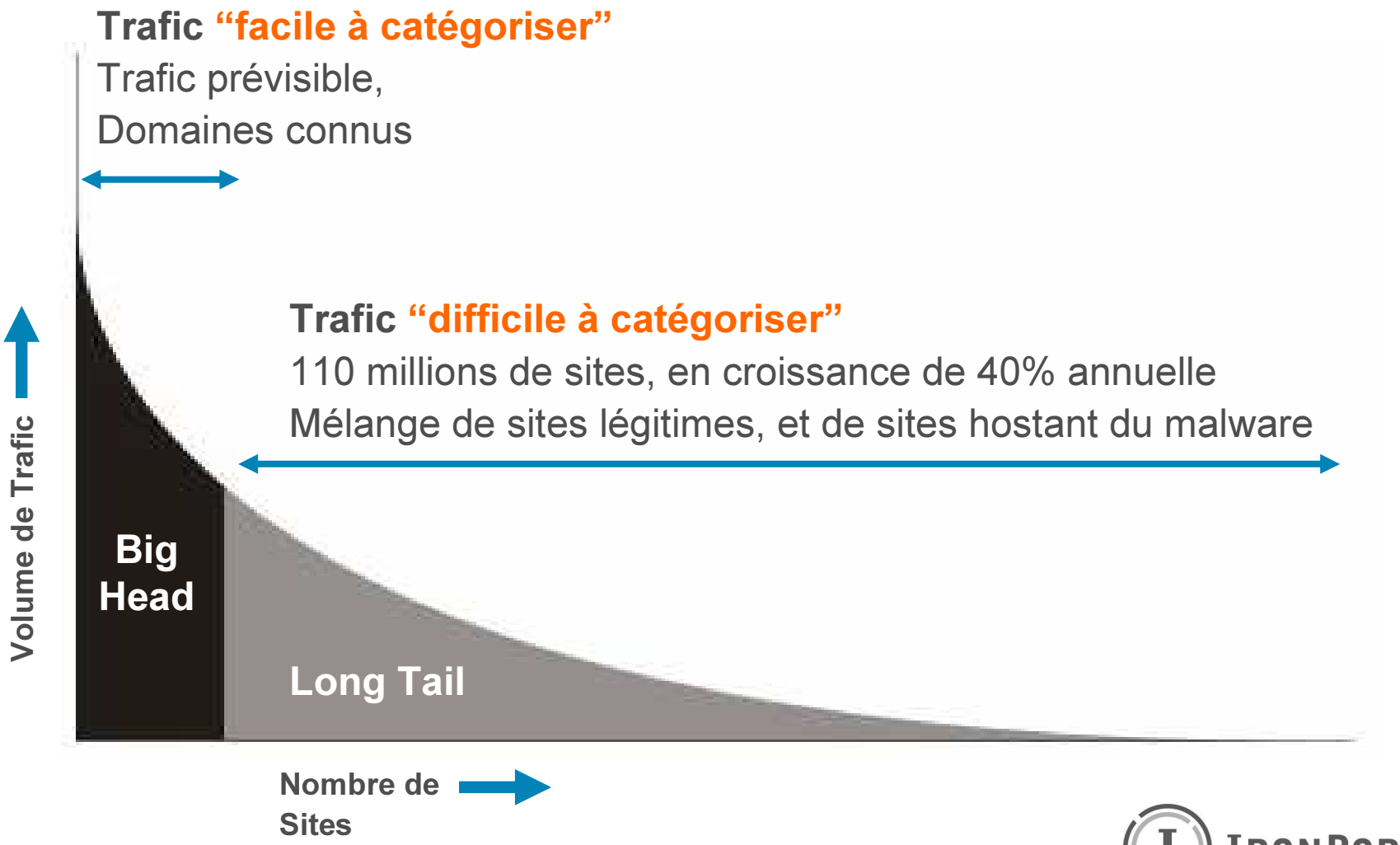
Sécurité Web

IronPort Série S

IRONPORT™

Le Trafic Web

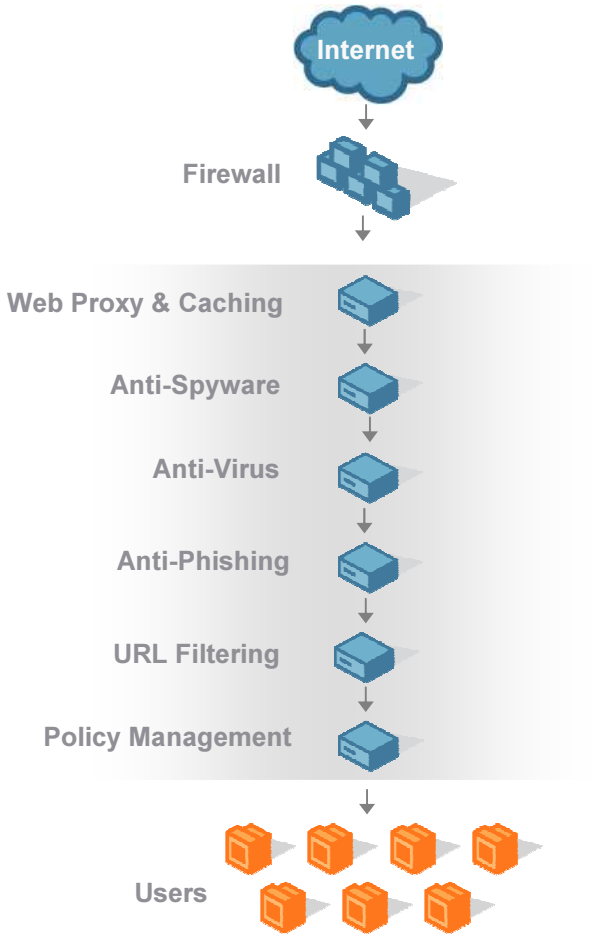
De plus en plus de sites inconnus



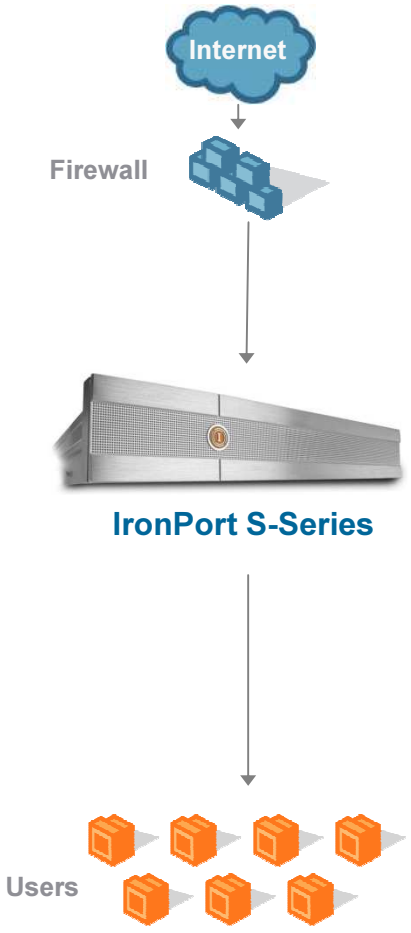
IRONPORT

Next Generation Secure Web Gateway

Before IronPort

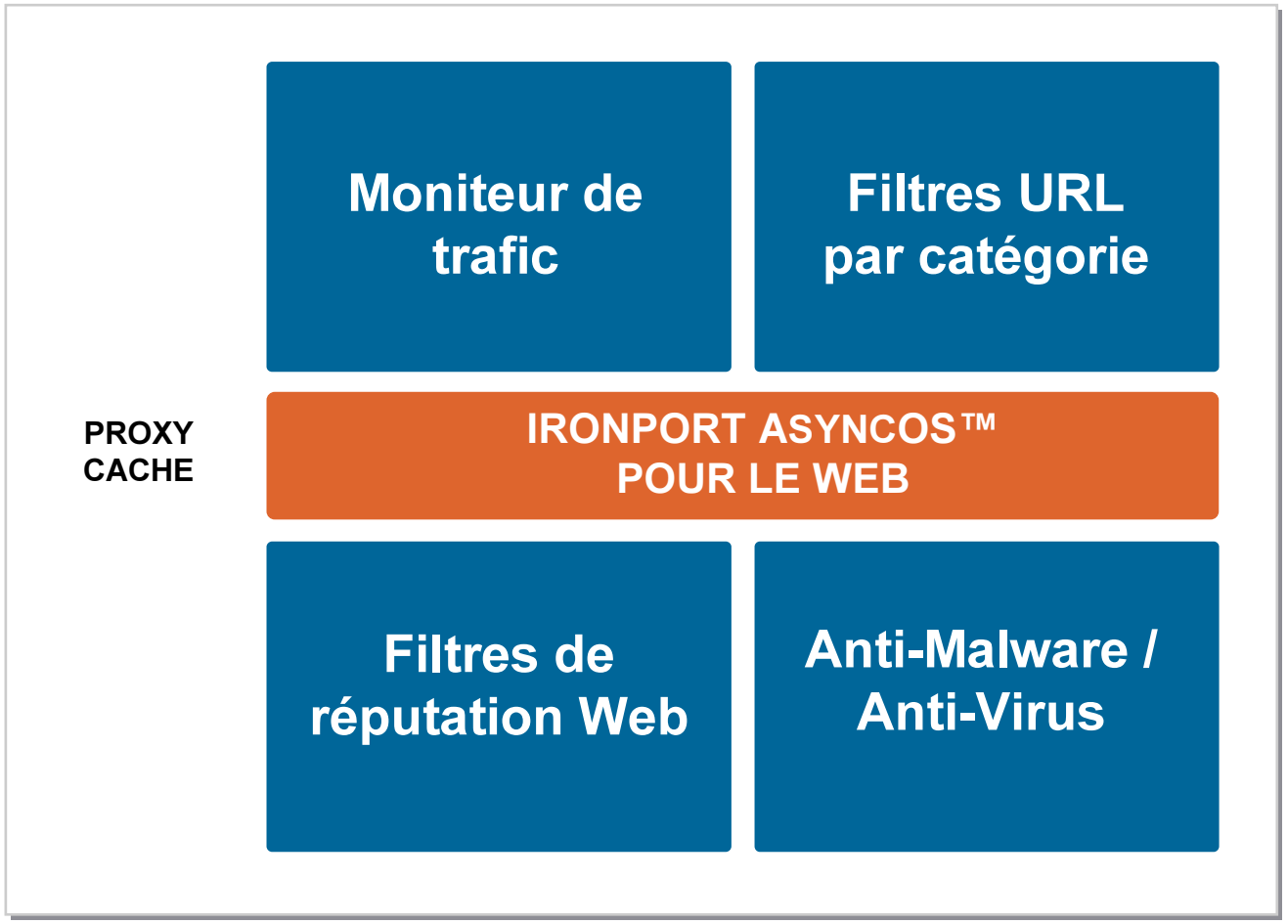


After IronPort



Architecture Série S IronPort

Sécurité des flux entrants et sortants

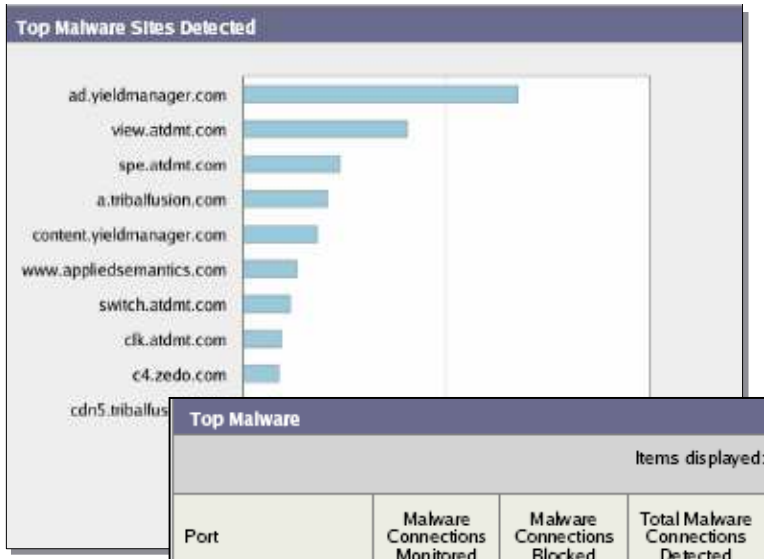


IRONPORT®

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”



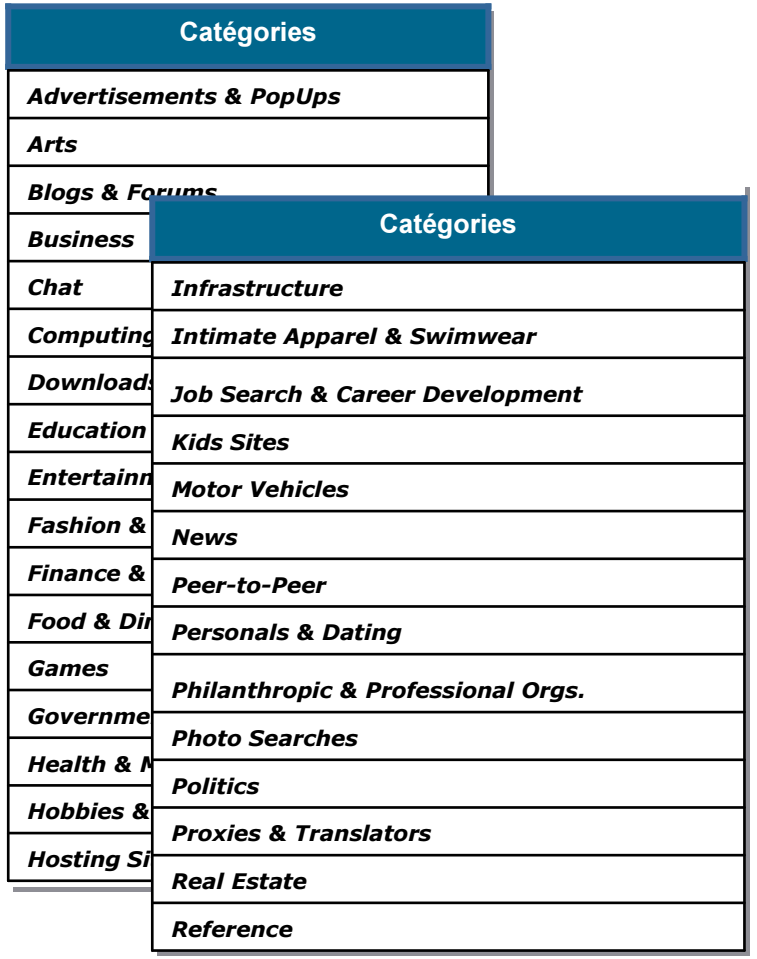
Top Malware

Items displayed: 10

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

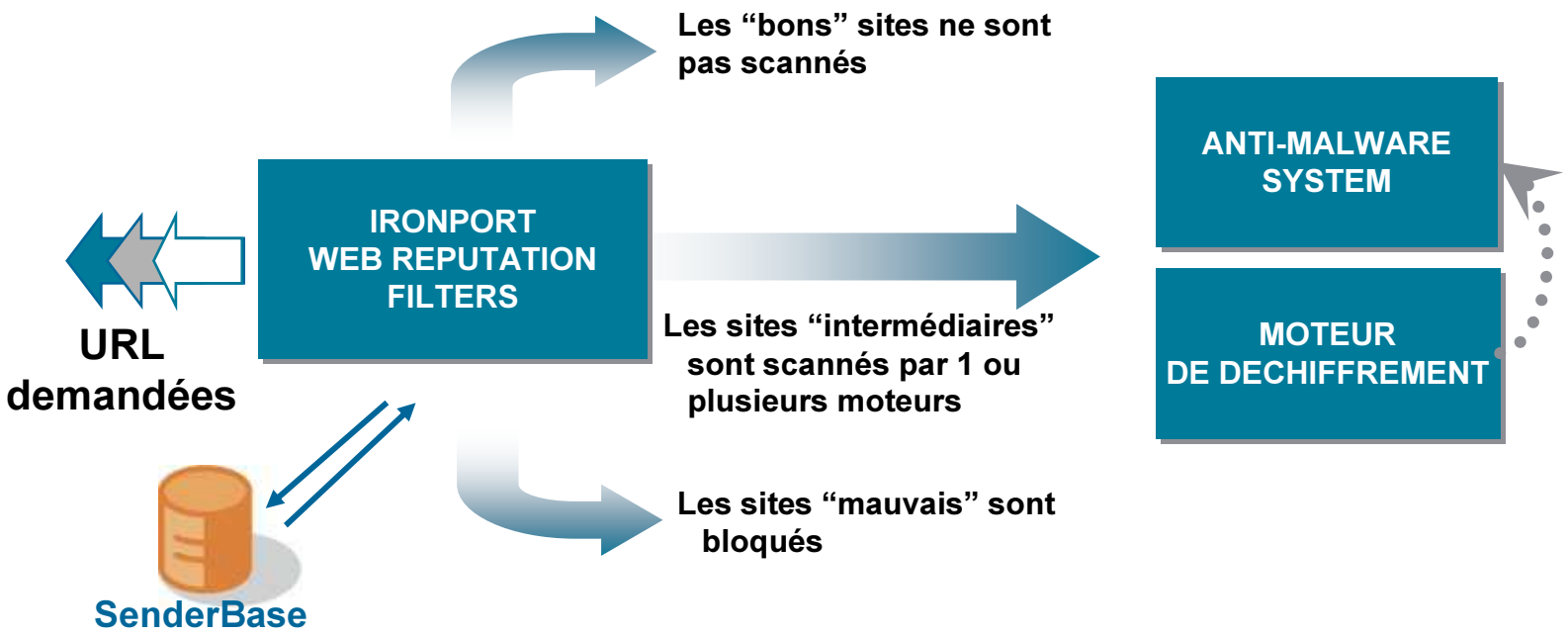
IronPort URL Filters

- 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



IRONPORT®

La réputation Web : un filtrage intelligent

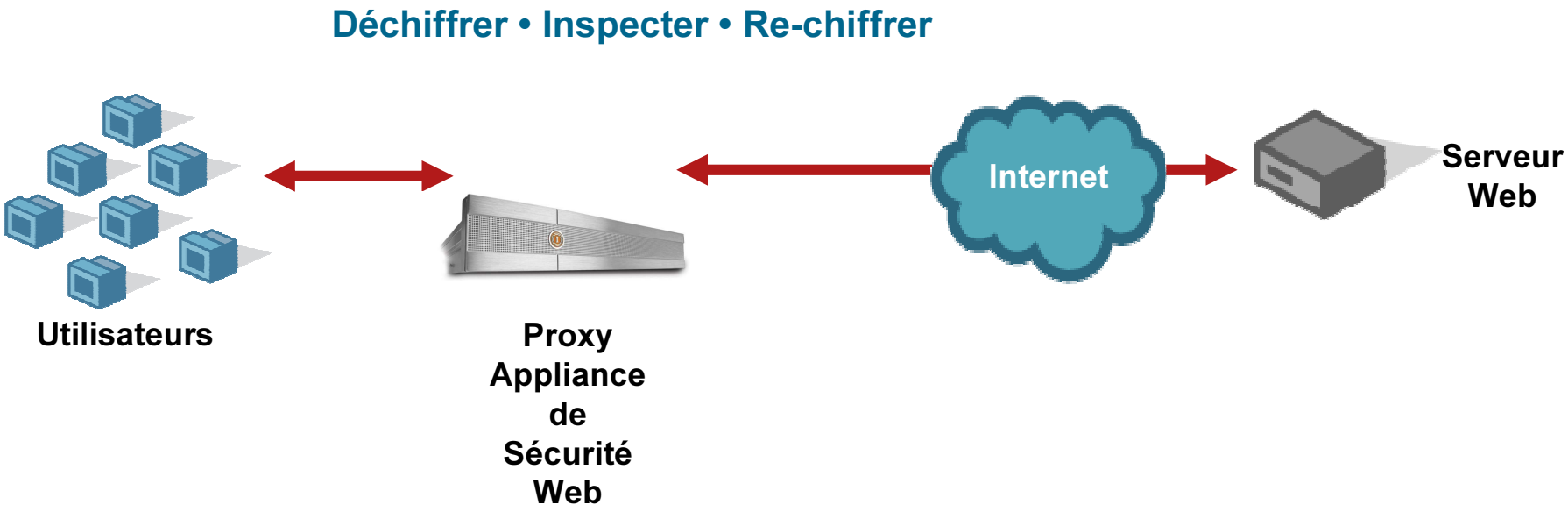


- **IronPort Web Reputation est le premier niveau de défense** qui détermine le besoin de scanner ensuite par:
  - Le moteur de déchiffrement HTTPS
  - IronPort Anti-Malware System™

IRONPORT®

Scan HTTPS sélectif

Basé sur la réputation



- **Le filtrage HTTPS sélectif** :

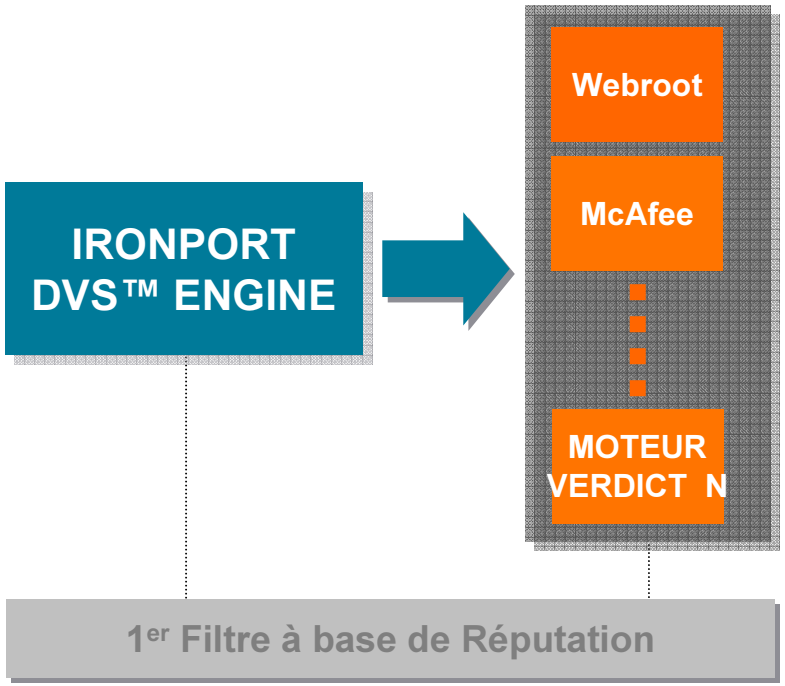
  - Respecte la confidentialité des véritables sessions HTTPS légitimes (par exemple un utilisateur consultant son compte bancaire en ligne)

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

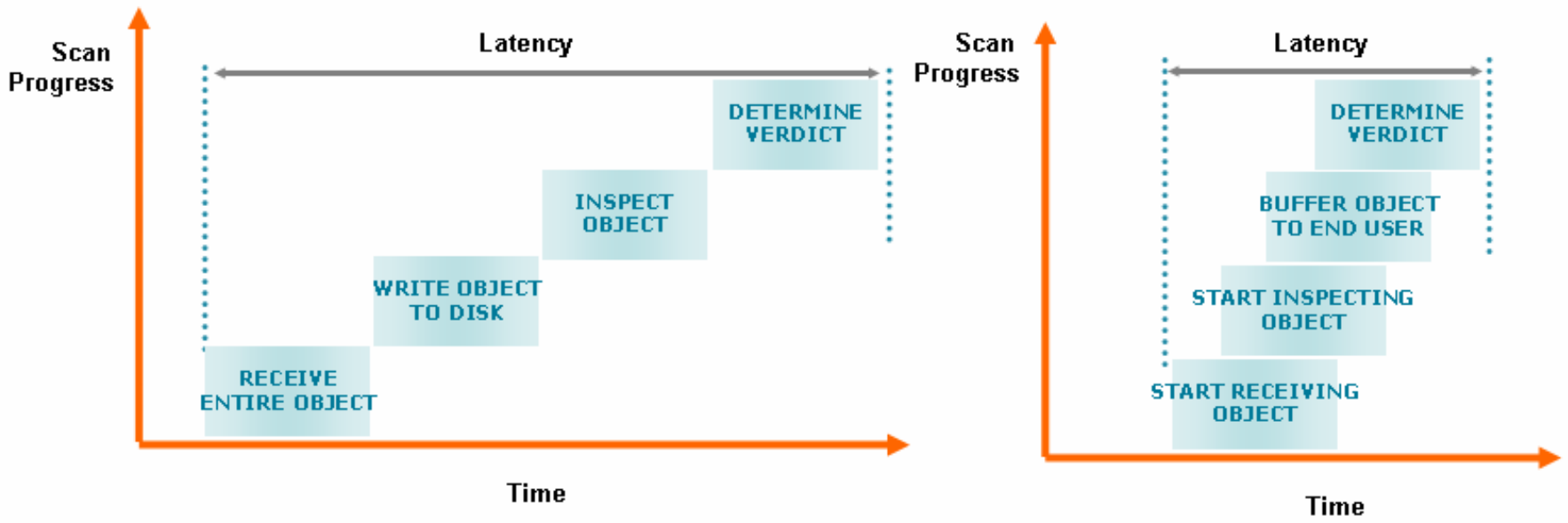
IronPort DVS™ Engine

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

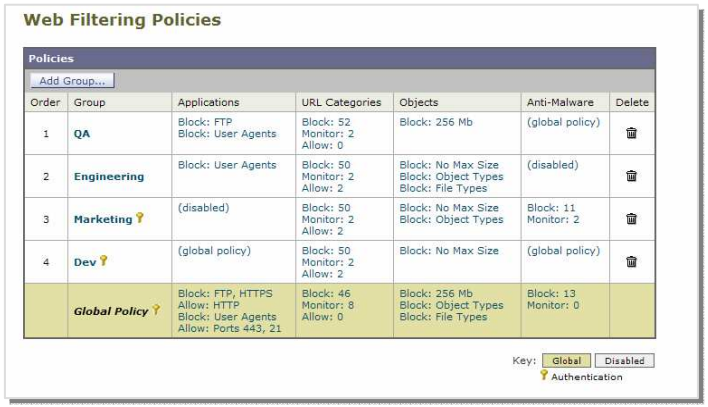


Scan en mode streaming

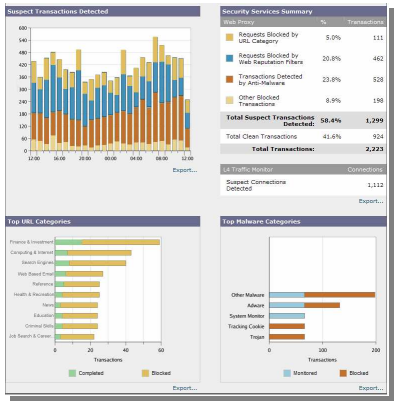


« En raison de la nature en temps réel des protocoles HTTP (…) et HTTPS et de leur flux de données, des fonctionnalités de scanning en temps réel (= en streaming) plus sophistiquées sont nécessaires pour s'assurer que le trafic Web reste sécurisé et à l'abri des attaques. »
IDC

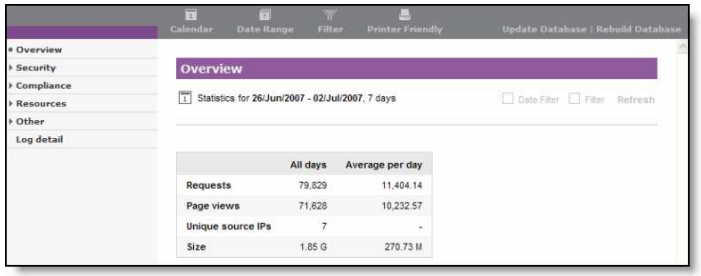
Une administration simplifiée



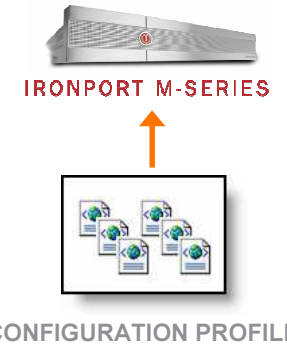
Web Security Manager
Configuration des politiques par groupes



Web Security Monitor
Reporting en temps réel



Reporting centralisé
Sawmill



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 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

Groupes LDAP, AD, Réseau

Marketing

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

Sales

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

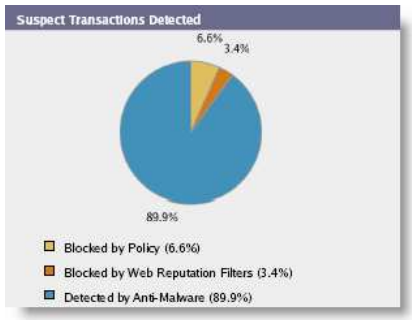
IT

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

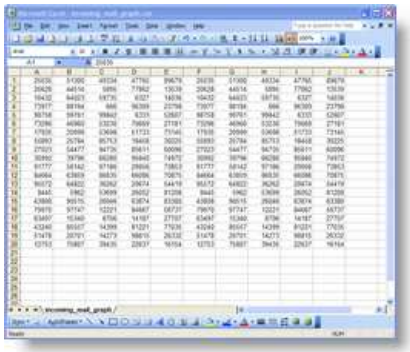
Web Security Monitor™

Extensible & Personnalisable

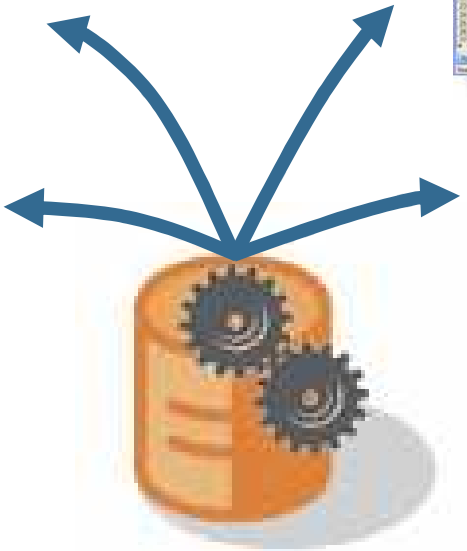
Rapports Graphiques en temps réel



Export en CSV



Envois programmés



Export en PDF®

Web Security Monitor™

IRONPORT®

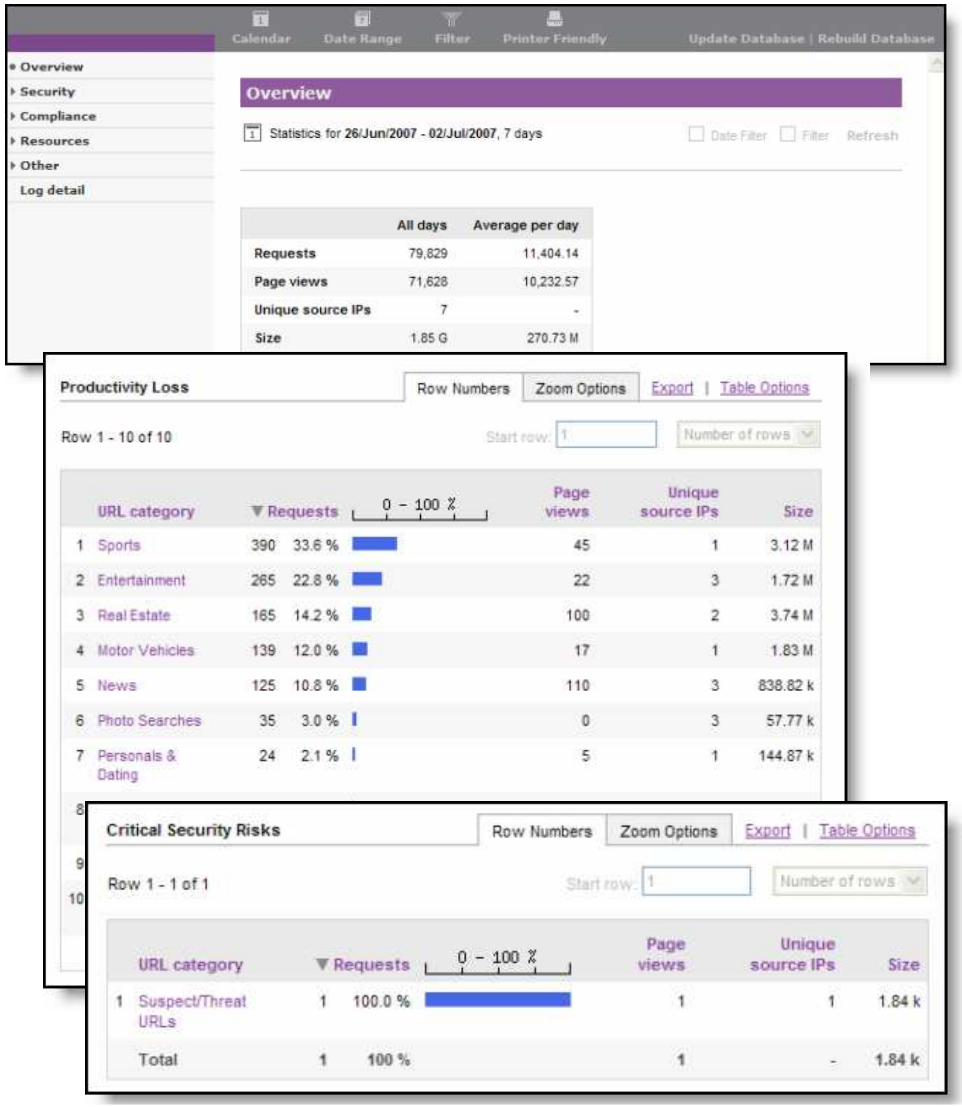
IronPort Web Security Monitor™

- *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

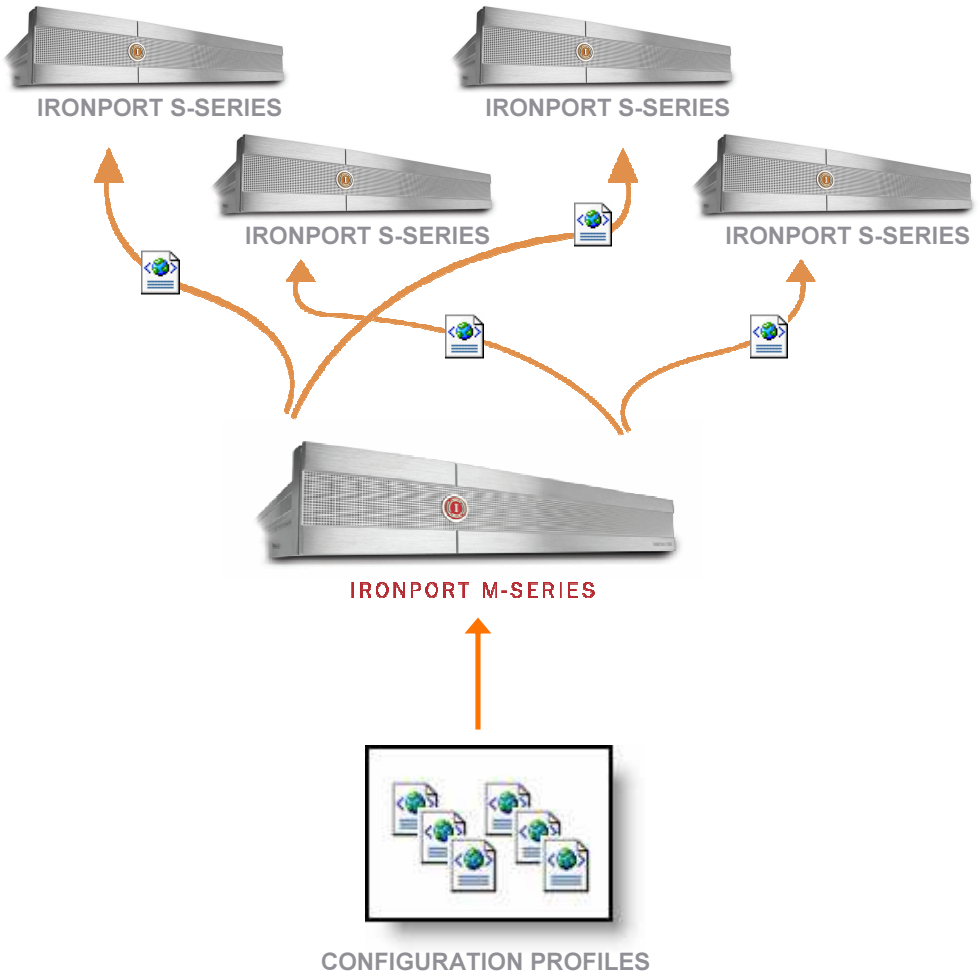
Vue consolidée de multiples boîtiers

- Application leader de création de rapports Web – Sawmill
- Rapports complets
  - Vues détaillées des activités Web par site ou utilisateur
  - Personnalisables
- Centralisés & aggrégés
  - Environnements cluster/équilibrage de charge via HTTP, FTP, Local File ou Command Line
  - Supporte des bases de données standard & MySQL database server™
  - Planifiables



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™

Aurora Health Care®

"… 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

IRONPORT®