panda
MalwareRadar

Solution d’audits préventifs et curatifs

Agenda

Qui est Panda Software?

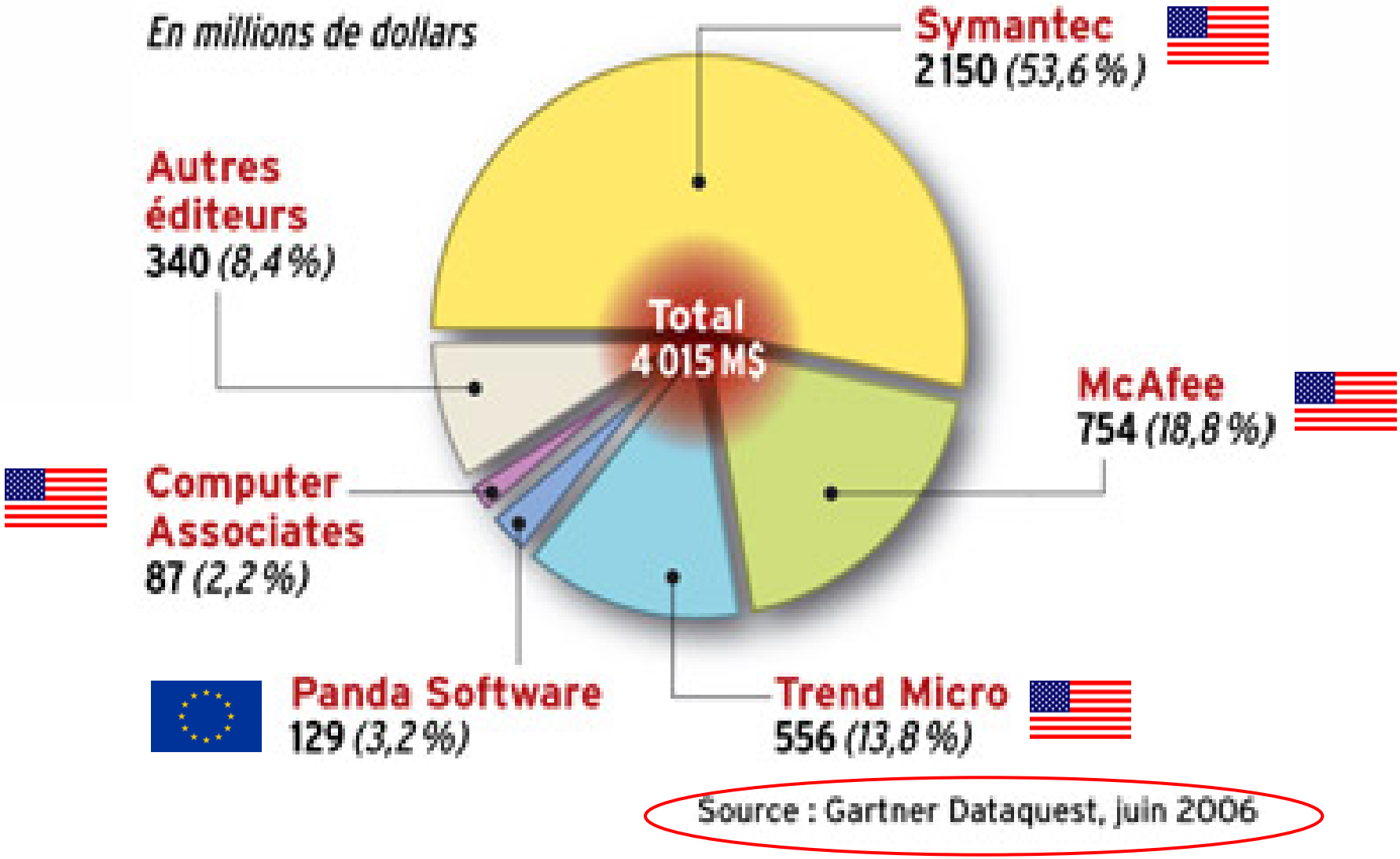
Un nouveau modèle de sécurité

Malware Radar

- Définition & caractéristiques
- Résultats obtenus dans les compagnies pilotes
- Fonctionnement
- Bénéfices clients

Final release versions of Malware Radar

Qui est Panda Software?



4ème Éditeur mondial d'antivirus

Qui est Panda Software?

Une croissance 2x plus rapide que celle du marché

Table 1
Worldwide 2005 Total Antivirus Software Revenue for All Software Segment Types
(Millions of Dollars)

Company	2005	2005 Market Share (%)	2004	2004 Market Share (%)	2004-2005 Growth (%)
Symantec	2,150.4	53.6	1,915.3	54.2	12.3
McAfee	753.9	18.8	666.5	18.9	13.1
Trend Micro	555.7	13.8	509.3	14.4	9.1
Panda Software	128.6	3.2	103.9	2.9	23.8
CA	86.5	2.2	75.3	2.1	14.9
Other Vendors	340.2	8.5	263.0	7.5	29.4
Total	4,015.4	100.0	3,533.2	100.0	13.6

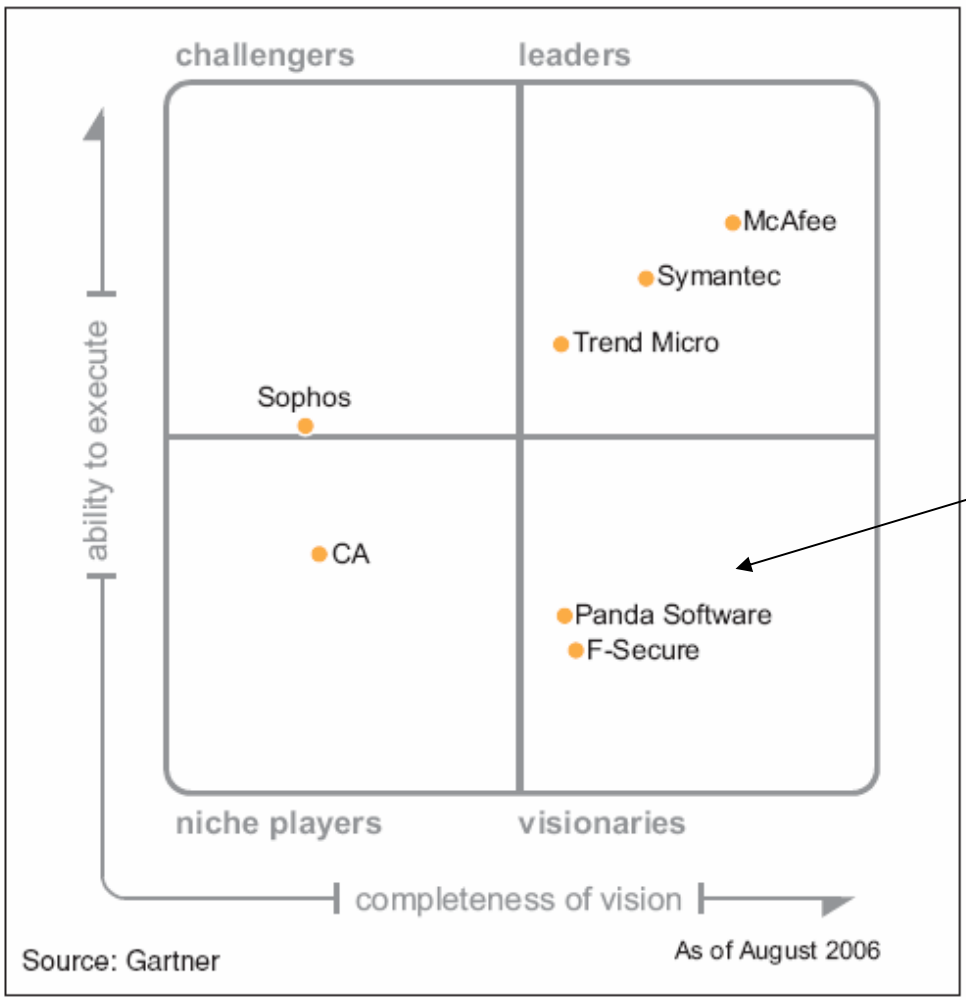
Source: Gartner Dataquest (June 2006)

Qui est Panda Software?

Une entreprise visionnaire

MAGIC QUADRANT

Figure 1. Magic Quadrant for Enterprise Antivirus, 2006



panda software

Ruptures technologiques

2004: HIPS introduction: TruPrevent Technologies

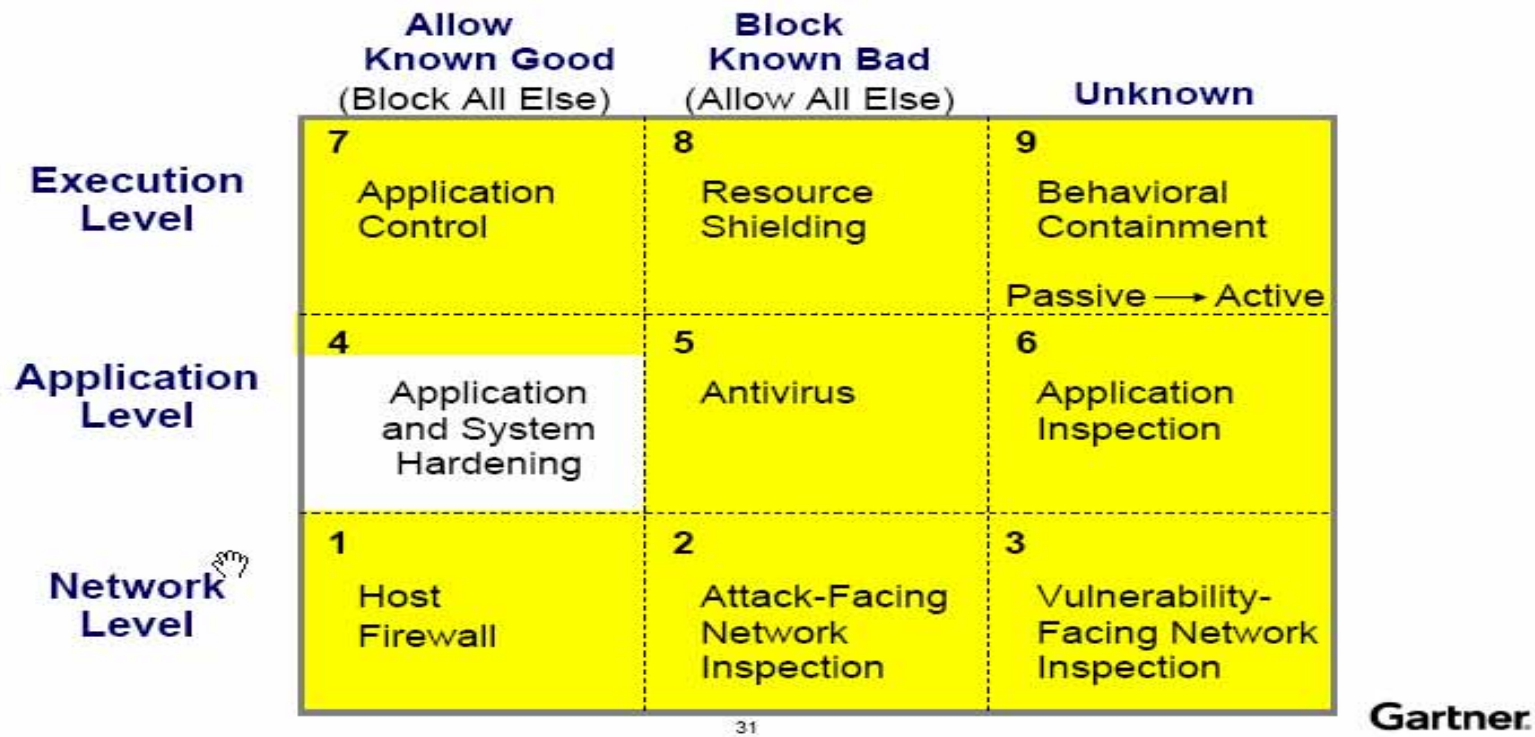
2007: Panda Collective Intelligence. (PCI)
(Production automatisée de signatures)

3 Solutions Panda en bénéficient

- Malware Radar **(Audit préventif et curatif en ligne)**
- TrustLayer **(Analyse mail en ligne antispam, garantie 100% sans virus)**
- NanoScan – TotalScan **(analyse gratuite en ligne)**

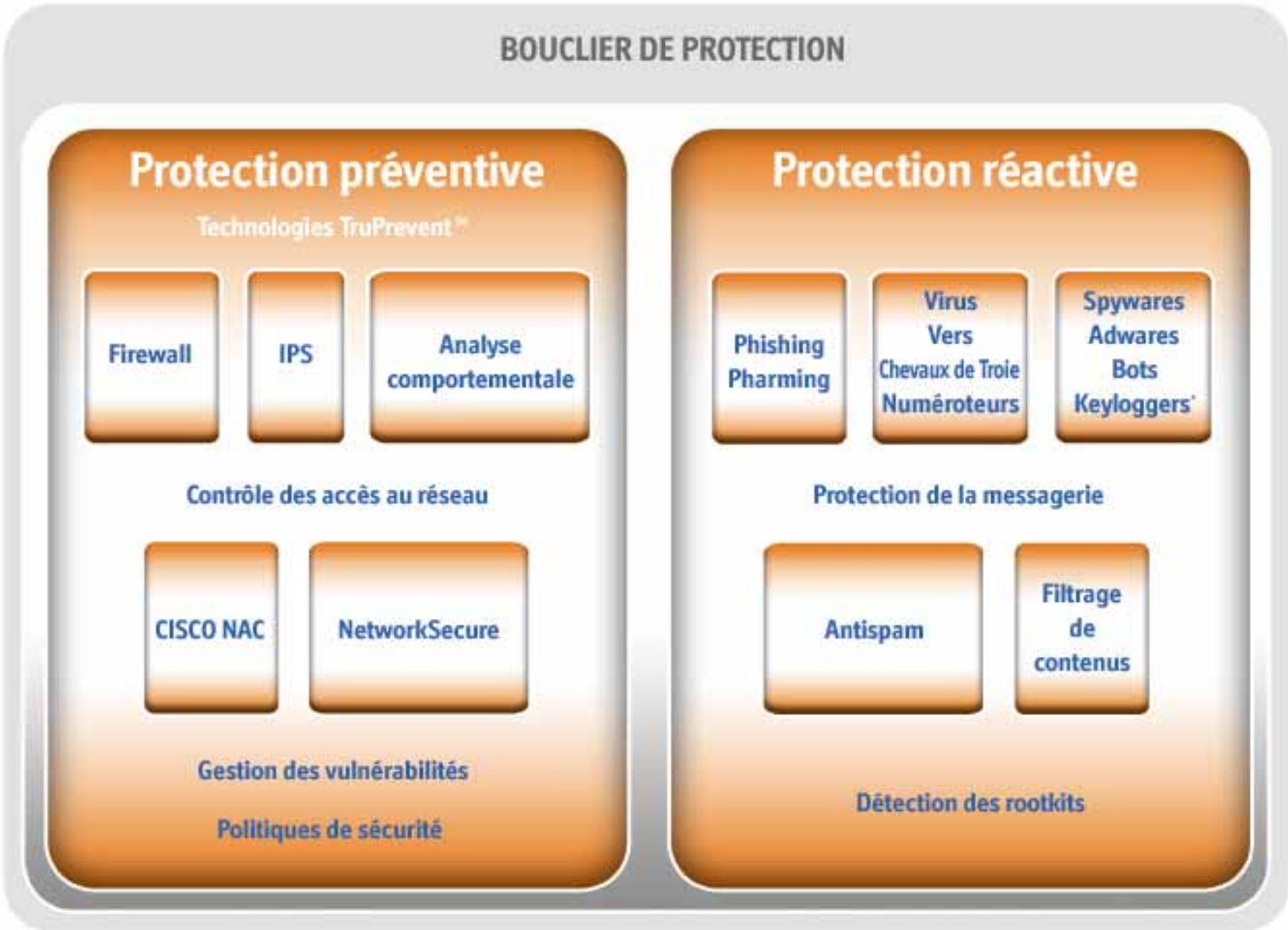
Les 9 protections d'un HIPS vu par le Gartner

Panda TruPrevent



*"The best example of a **vendor that has taken the visionary step** of delivering a single client with a full complement of host-based intrusion prevention technologies is **Panda Software**, with its **ClientShield** product, which is priced as a single solution and provides protection across eight of the nine protection styles outlined in our HIPS research" **Gartner.***

PIPS PANDA



* Enregistreurs de frappes

Reconnaissance marché

Panda Software : un leader technologique reconnu

TruPrevent™ - “Meilleur logiciel 2006”

CeBIT
HANNOVER · GERMANY
9 – 15 MARCH 2006

A l’occasion de l’édition 2006 du salon international **CeBIT**, les Technologies **TruPrevent™** ont obtenu le prix du **“Meilleur Software”.**

TRUPREVENT HONEYNET

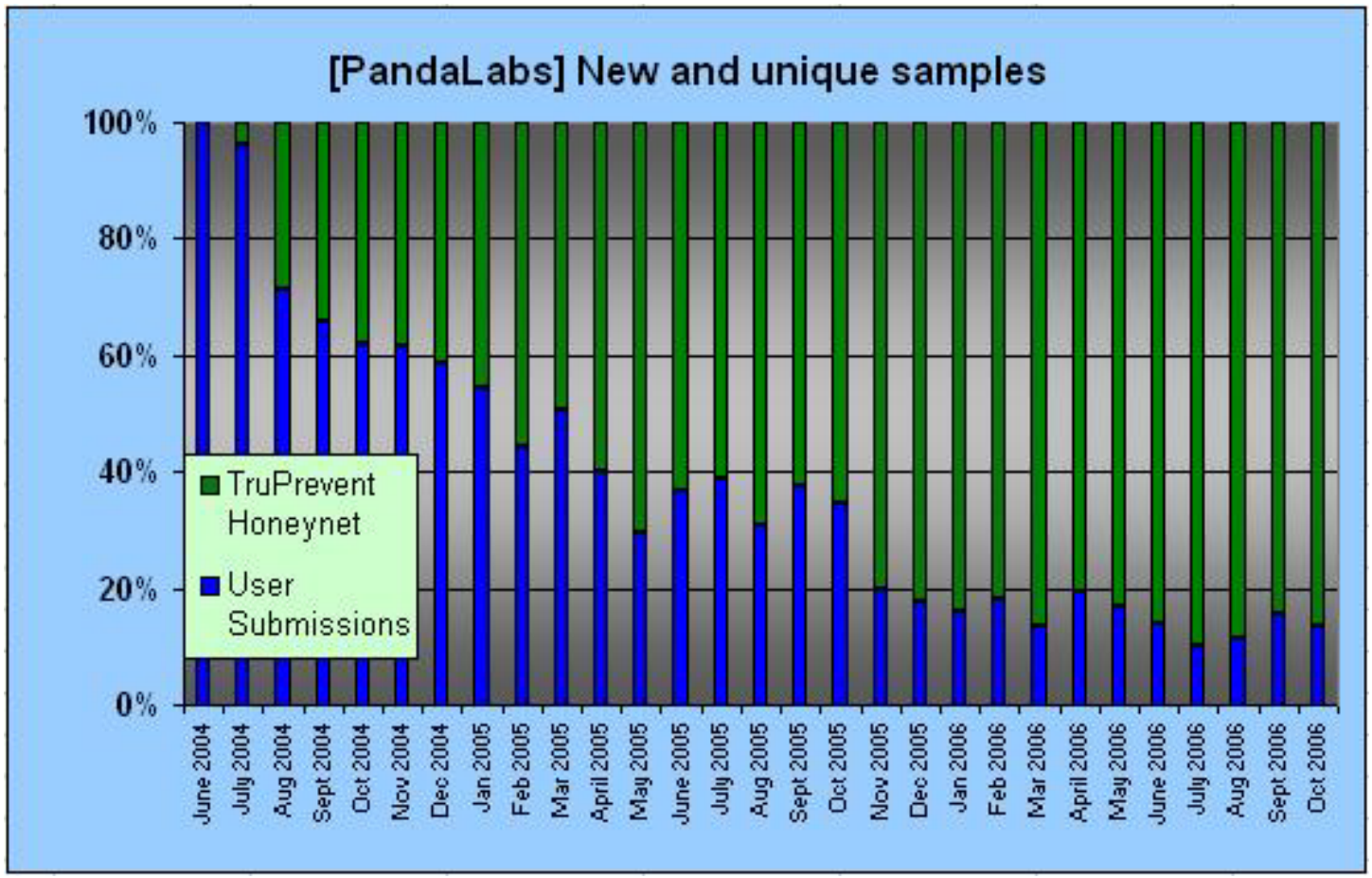
- **A very large malware honeyNet**
- As of today approximately **4.5 million PCs** are running a malware honeypot on their machines with Panda's behavioural-based Host Intrusion Prevention System (aka TruPrevent). All these high-interaction malware honeypot nodes report to PandaLabs any new malware sample that TruPrevent© flags as malware and which is not detected by regular AV signatures.

  The results are pretty interesting. Over **80% of the malware samples** received at PandaLabs from our users are now coming from automated submissions from this honeynet. This also means that the number of unique samples received from users at PandaLabs has increased by about 700% over the last two years. It is interesting to note that these are the most interesting samples we are receiving in the Lab as they are real-life samples affecting real users, not private zoo collections that are not actively infecting users.

  The following graphs the evolution of how the samples are received at PandaLabs over time since we started deploying the HIPS honeynet to our users in mid-2004. Of course this graph excludes collections submitted by industry sharing and private researchers.

TRUPREVENT HONEYPOT NET

+ de 80% des nouvelles souches sont découvertes automatiquement par Truprevent



Agenda

Qui est Panda Software?

Un nouveau modèle de sécurité

Malware Radar

- Définition & caractéristiques
- Résultats obtenus dans les compagnies pilotes
- Fonctionnement
- Bénéfices clients

Final release versions of Malware Radar

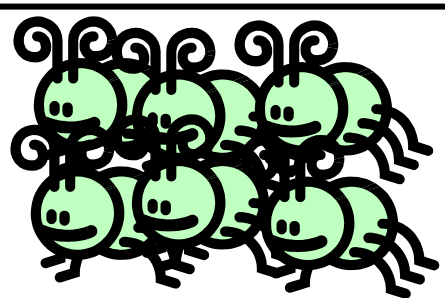
Que pouvons faire quand…?

Les pirates sont devenus professionnels

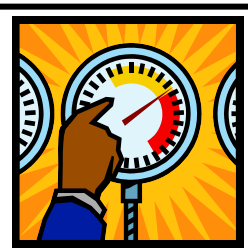
Les pirates ont créé un vrai modèle économique

Malwares sont plus nombreux, plus sophistiqués et de plus en plus difficiles à combattre.

Les pirates usent de stratagèmes pour rester le plus discret possible.



Les pirates créent de plus en plus de type de malwares



Tous les laboratoires sont saturés. Ils ne peuvent plus traiter tous les malwares reçus chaque jour

La stratégie des pirates

La double stratégies des pirates :

Intérêts financiers
$$$ €€€

Création importante de malwares

Laboratoires AV dépassés

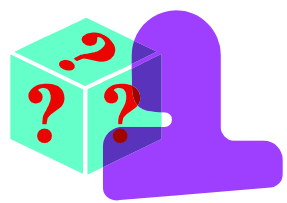
Les utilisateurs ne sont plus correctement protégés

Les pirates ont atteint leurs objectifs

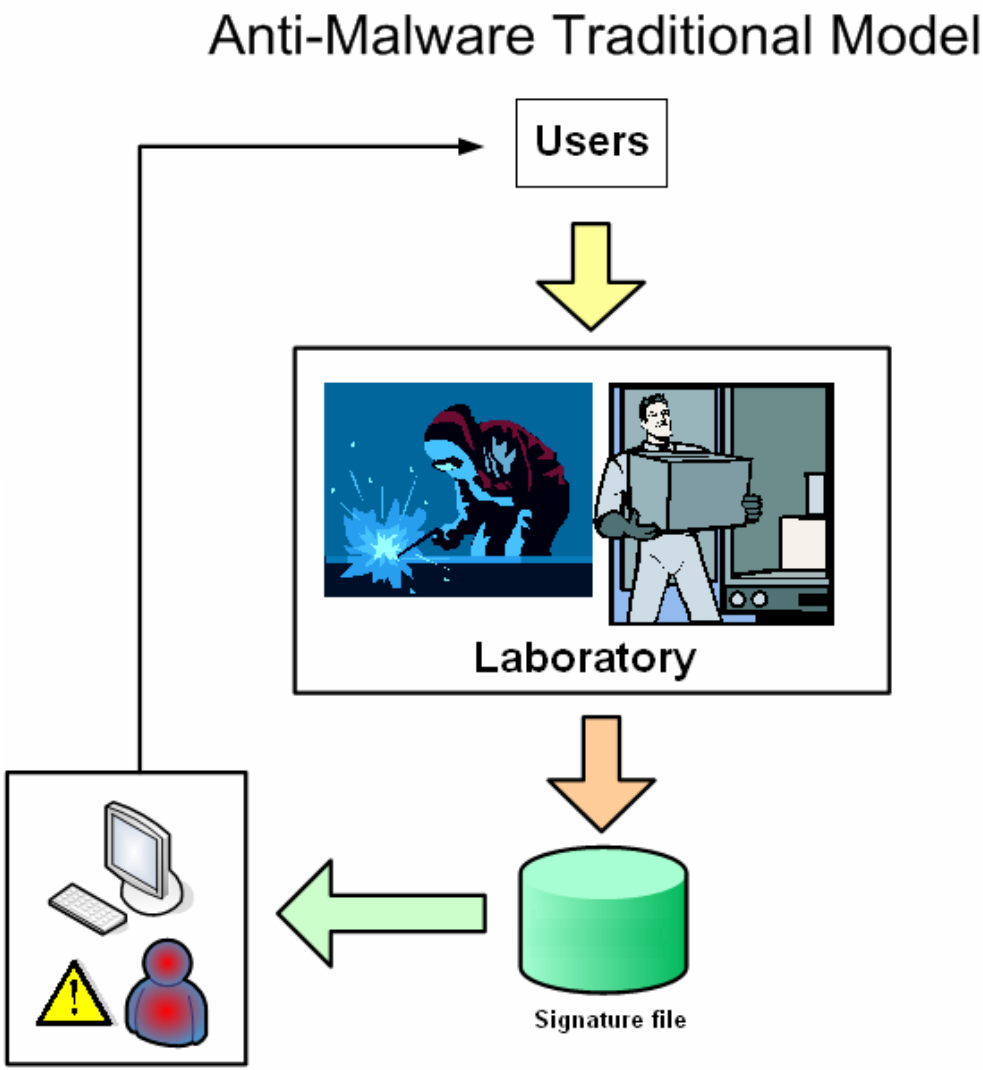
Création importante de codes silencieux

Il n'y a plus d'alerte ni d'épidémie

Les utilisateurs ne savent pas qu'ils ne sont pas Correctement protégés



Un modèle traditionnel dépassé



1. Les laboratoires sont principalement fournit en souches par leurs clients et d'autres sources

2. Les souches sont analysées manuellement par les laboratoires et les signatures mettent énormément de temps a être produites. Tous les laboratoires ont un stock de virus sans signature par manque de temps

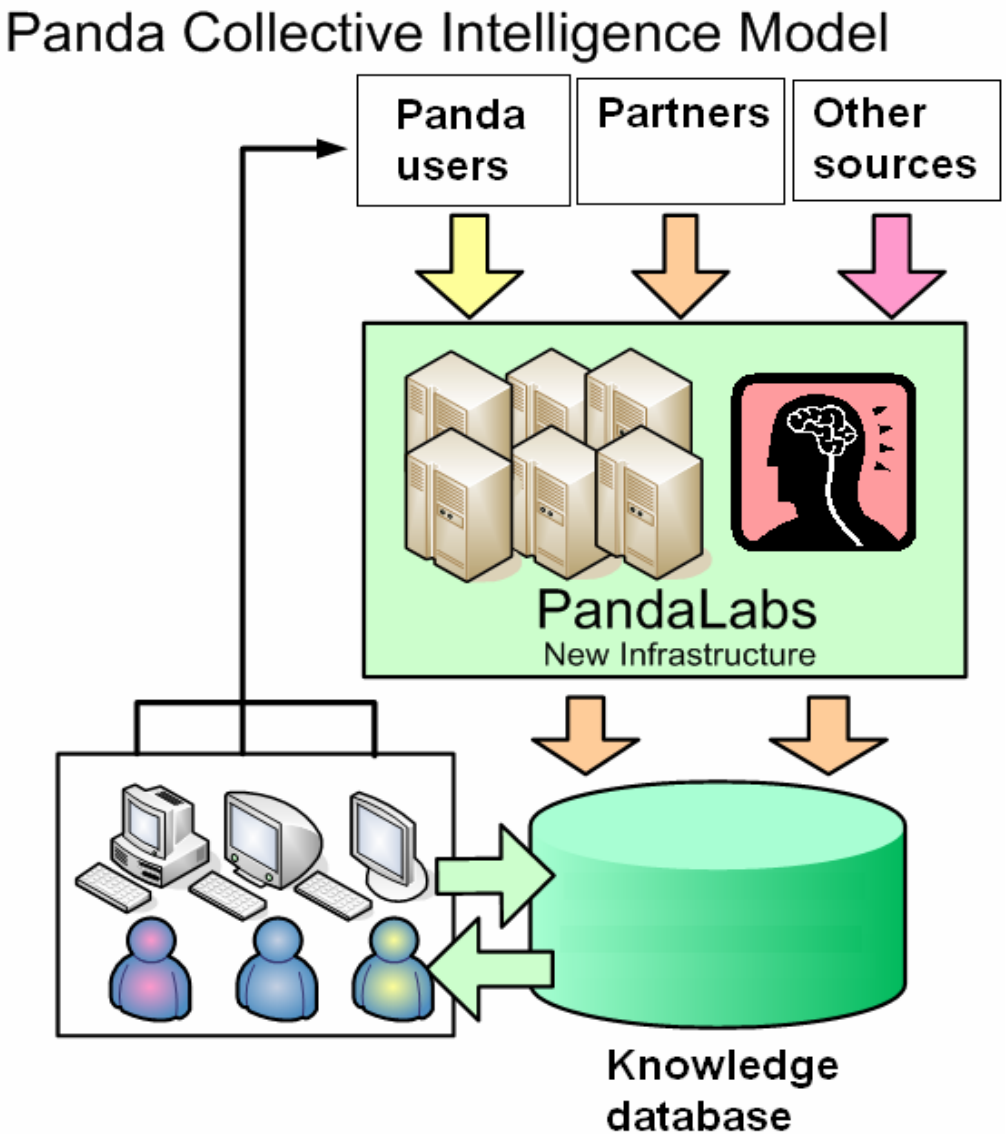
3. Les fichiers de signature délivrés au client sont par conséquent limités et les protections inadaptées à la menace du moment. Cela signifie que les clients ne sont pas bien protégés

Panda Software propose un nouveau modèle de production automatique de signatures

Panda Collective Intelligence

« PCI »

Nouveau modèle PANDA PCI



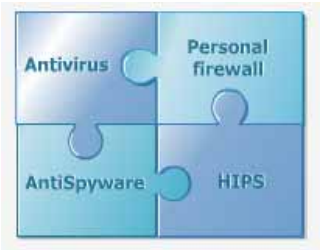
1. **Collecte de données en provenance de la communauté.** Ce système centralisé récupère et stocke les programmes suspects, les traces de fichiers, et les nouveaux exemplaires de malwares etc. Ces données proviennent des utilisateurs Panda, des autres acteurs de la sécurité. **Cette large capacité de collecte permet d'avoir une vision très large de la menace active sur Internet.**

2. **Traitement automatisé**. Un système automatique analyse et classe plusieurs centaines d'exemplaires uniques de code malicieux chaque jour. Pour ce faire, **un système expert** corrèle les données collectées à la base étendue de malwares connus de PandaLabs. Le système donne instantanément un statuts (malware ou goodware) au fichier reçu. Ce moyen permet à PandaLabs de réduire au maximum l'intervention manuelle

3. **Mise à jour de la base de connaissance**. La base est mise à disposition des utilisateurs au travers des services Internet de Panda Software ou par la distribution de la base Virale

Nouveau modèle PANDA PCI

Panda propose un nouveau modèle de sécurité:



+

panda MalwareRadar

Un système PIPS sur chaque PC		Un service d'audits préventifs et curatifs périodique sur l'ensemble du réseau
Une détection traditionnelle	+	Nouvelle approche: **Collective Intelligence**
Une protection permanente	+	Analyse et désinfection à la demande **"on-demand"**
Une décision en temps réel	+	Pas besoin de prendre une décision en temps réel Une analyse étendue des postes en réseau **en utilisant les paramètres heuristiques plus sensible.**
Local: un abonnement au mise à jour quotidienne	+	**Un service en ligne : nécessite aucune installation** **MalwareRadar bénéficie des dernières mise à jour en toute transparence**
Solution comportementale	+	**Détection des malwares indétectable par un PIPS (comme les malwares cachés, les attaques ciblées etc.)**
Problèmes opérationnels possibles de mises à jour, installations, etc.	+	Détection de vulnérabilités –Vérification du statuts de protection –Détection des vulnérabilités relatives aux malwares

Les deux solutions doivent fonctionner en coordination constante pour une amélioration continue des processus de protection.

Agenda

Qui est Panda Software?

Un nouveau modèle de sécurité

Malware Radar

- Définition & caractéristiques
- Résultats obtenus dans les compagnies pilotes
- Fonctionnement
- Bénéfices clients

Final release versions of Malware Radar

MalwareRadar?

C'est un système automatique d'audits préventifs et curatifs de l'ensemble du réseau.

- A la demande
- Il peut fonctionner en local ou à distance
- Il ne demande aucune installation locale et ne nécessite aucune désinstallation de la protection courante

- Il a été conçu pour chercher et trouver:
  1. **Tout type de malwares sur le réseau**
     - **Malwares non détectés par les solutions traditionnelles** (les menaces critiques ou les attaques ciblées) les malwares actifs ou latents connus et inconnus
     - **Rootkit connus ou inconnus** (Hidden drivers, processus, modules, files, registry entries, SDT et IDT modifications, EAT et IRP hooks, Non standard INT2E et SYSENTER…)
  2. **État de la protection**
     - **Protection:** Vérification du statut de la protection
     - **Vulnérabilité critique:** Vérification des vulnérabilités exploitées par les malwares (trou de sécurité)

- **Et permet une désinfection du réseau (désinfection à la demande)**

Software as a service

Panda MalwareRadar bénéficie du concept Software as a Service (SaaS)

- **Ne requière aucun matériel spécifique**
- **Ne requière aucun logiciel spécifique, un navigateur web suffit**
- **Les mises à jour sont immédiatement disponibles**
  - L'utilisateur bénéficie des dernières technologies et des derniers fichiers de signatures
  - Plus de soucis d'up-grade
- **Toute l'intelligence et les applications sont chez Panda Software**
  - Réduction des coûts pour le client

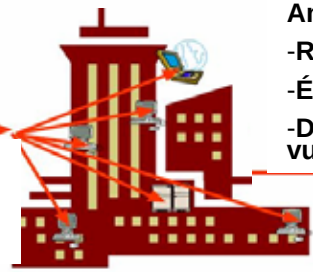
REAL results of the betas

Et toutes les entreprises pensent qu'elles sont bien protégées !!

Fonctionnement de MalwareRadar

Sélection des machines à analyser

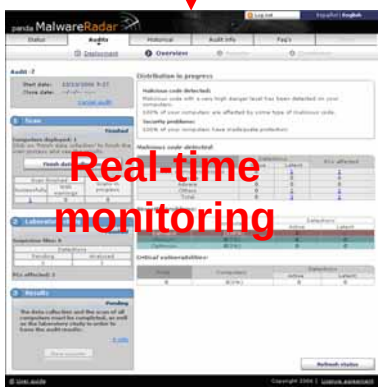
Distribution d'un agent (sans installation)



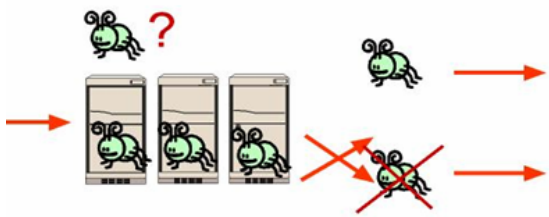
Analyse:
-Recherche des malwares
-Évaluation des protections
-Détections des vulnérabilités

Login
Password

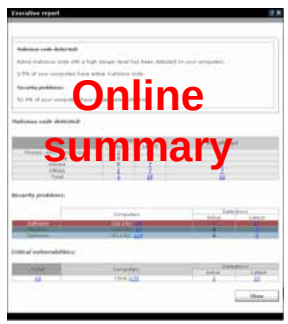
Enregistrement



Envoi des fichiers suspects chez Panda Labs



Génération d'un rapport détaillé et propose une désinfection des malwares détectés

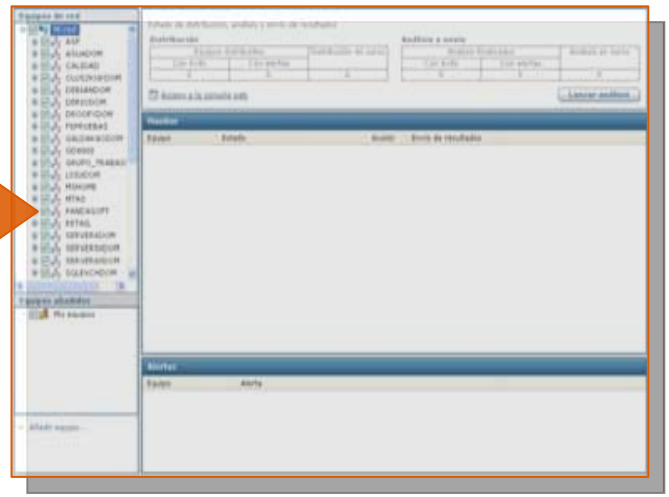


Reports et désinfection

Fonctionnement de MalwareRadar

1. Distribution d'un client exécutable

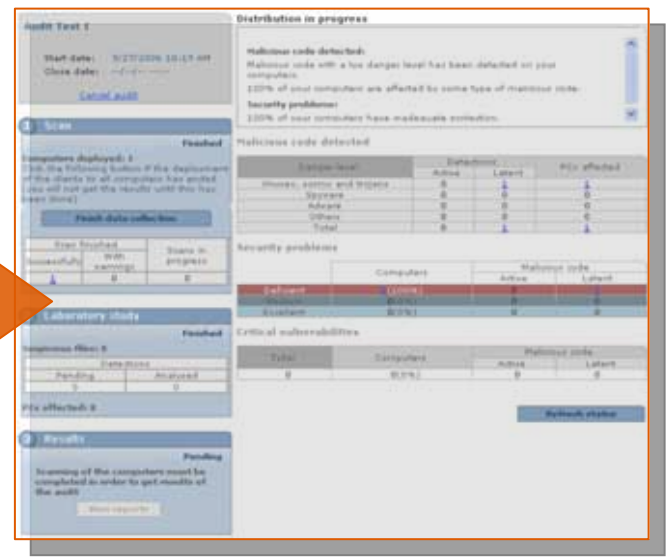
- Utilisation des méthodes de distribution standard (login scripts, SMS, Tivoli, etc.)
- Ou utilisation de l'outil de distribution de MalwareRadar



Analyse du réseau (Workstations / File Servers)

Types	Analyses	Objectifs
Rapide (5 to 10 min. not including distribution)	**Éléments critiques du système: mémoire, répertoires principaux, base de registre, processus actifs**	**Détection de tous les malwares actifs présents sur le réseau**
Complète (approx. 2h not including distribution)	**Tous les disques durs**	**Détection de tous les malwares latents et actifs**

- Console centrale en ligne pour visualiser les processus en cours
- Désinstallation automatique des clients
- Transparence total pour les utilisateurs du réseau
  - Les utilisateurs ne savent que leur Pc est analysé



Fonctionnement Malware Radar

3. Délivrables pour le client :

- Rapports en ligne
- Formats pdf exportables xml

Rapport Executif Executive report	• Situation du réseau et niveau de risque • Statistiques • PCs les plus infectés • Recommandations 
Rapport Technique Technical report	Détail de chaque PC: • Malwares détectés, description, effets, localisations • Niveau de sécurité: – Statut de la protection – Description des vulnérabilités 
Rapport de désinfection	Malwares neutralisés, emplacement et le résultat du nettoyage

Bénéfices client

- ✓Avoir rapidement un statut
- ✓Permet d’avoir un second avis
- ✓MalwareRadar offre une solution de reprise d’activité lors d’épidémies
- ✓Connaître le niveau de sécurité du parc
- ✓Connaître les actions à prendre pour mettre à niveau la sécurité du parc
- ✓Pas d’installation de résident

Agenda

- Qui est Panda Software?
- Un nouveau modèle de sécurité
- Malware Radar
  - Définition & caractéristiques
  - Résultats obtenus dans les compagnies pilotes
  - Fonctionnement
  - Bénéfices clients
- Final release versions of Malware Radar

Final release versions

TYPE	ONE-RUN AUDIT		SUBSCRIPTION
	Without cleaning	With cleaning	
Quick/Full scan	✓	✓	✓
Online summary	✓	✓	✓
Executive and technical reports	✓	✓	✓
Cleaning	✗ Option to buy later	✓	✓
Price depends on	No. of licenses		No. of licenses and time
Telephone and email support	Up to 1 month after the end of the audit		For 1, 2 or 3 years.
Uses	One use only		Unlimited number of audits for 1, 2 or 3 years and for the number of licenses contracted for a fixed group of PCs

QUESTIONS ?

http://www.malwareradar.com

Vos interlocuteurs Panda Software France:

Laurent GIORGETTI
Business Development Manager PSF
lgiorgetti@pandasoftware.com.fr
+33 1 30 06 38 80

Wilfried TRAIN Technical Manager PSF
wtrain@pandasoftware.com.fr
+33 1 30 06 16 61


panda
MalwareRadar