TREND MICRO

Le spécialiste de la lutte contre les codes malicieux

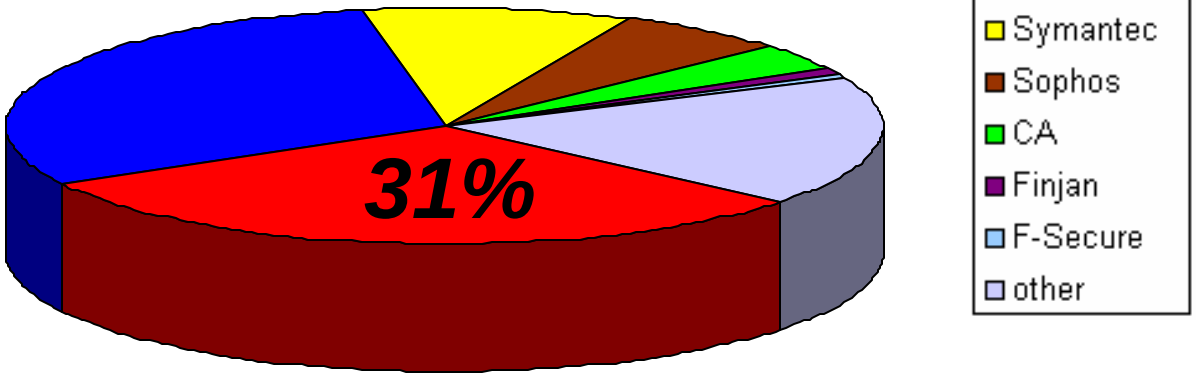
Pierre MORENO
Responsable Partenaire
Trend Micro France

Agenda

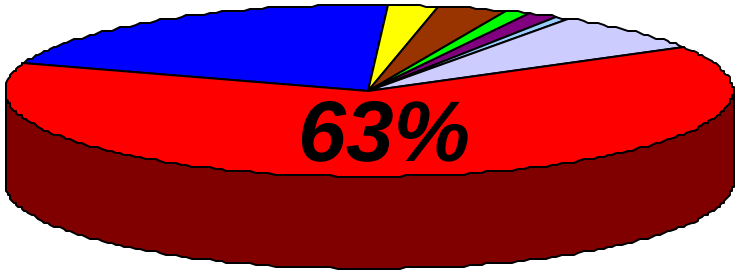
- Trend Micro : Votre fournisseur spécialiste de l ’antivirus
- Contre quoi luttons-nous ? Panorama de quelques attaques remarquables
- Les produits Trend Micro au service de la lutte
- Les services associés : l ’organisation des laboratoires

Un fournisseur solide aux parts de marché éloquentes

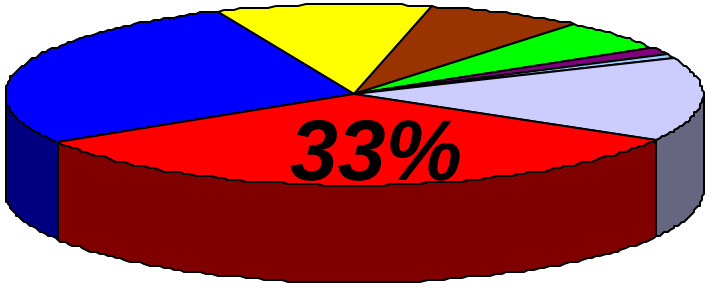
Messageries



Passerelle internet



Tous serveurs

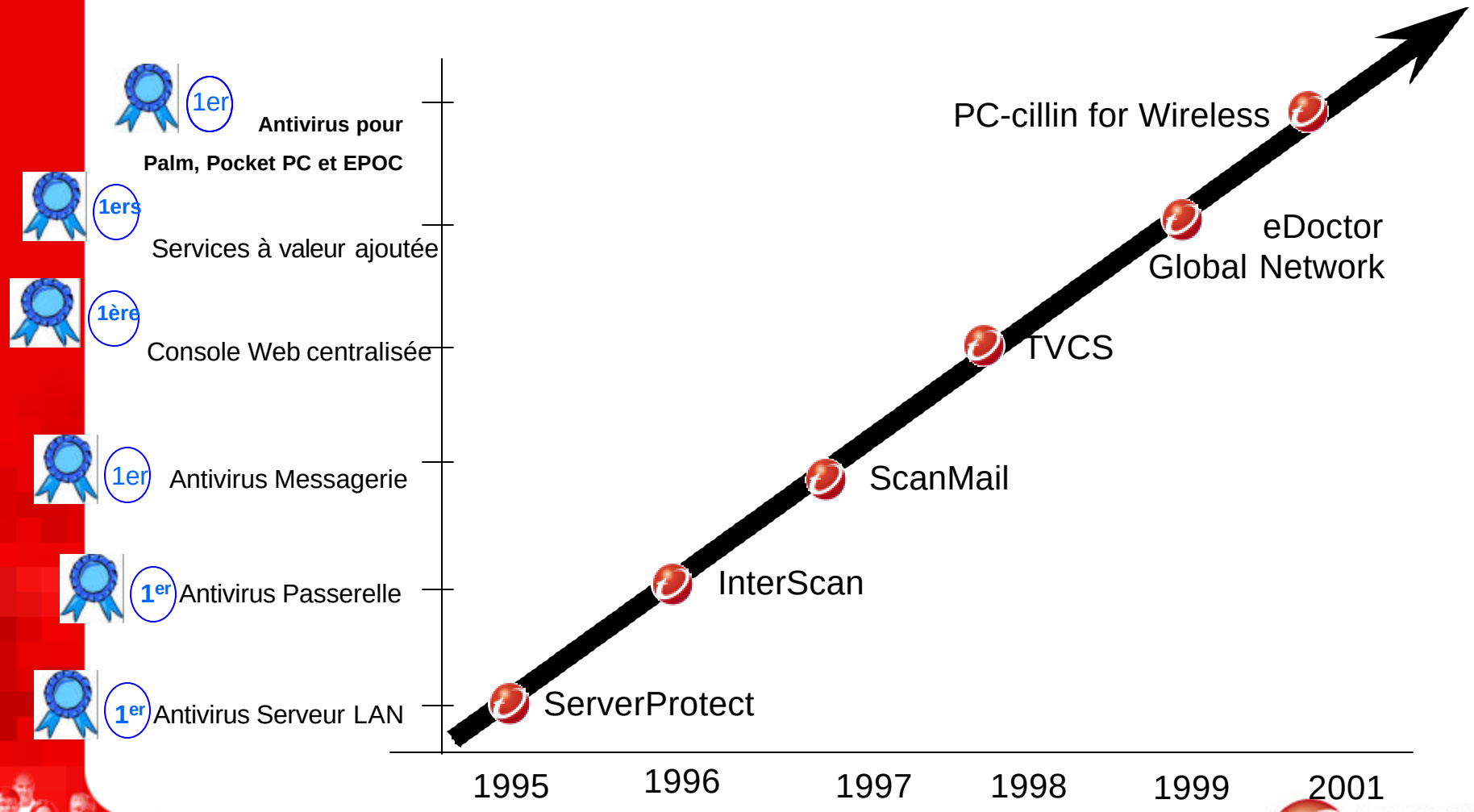


Source: IDC, Juillet 2001

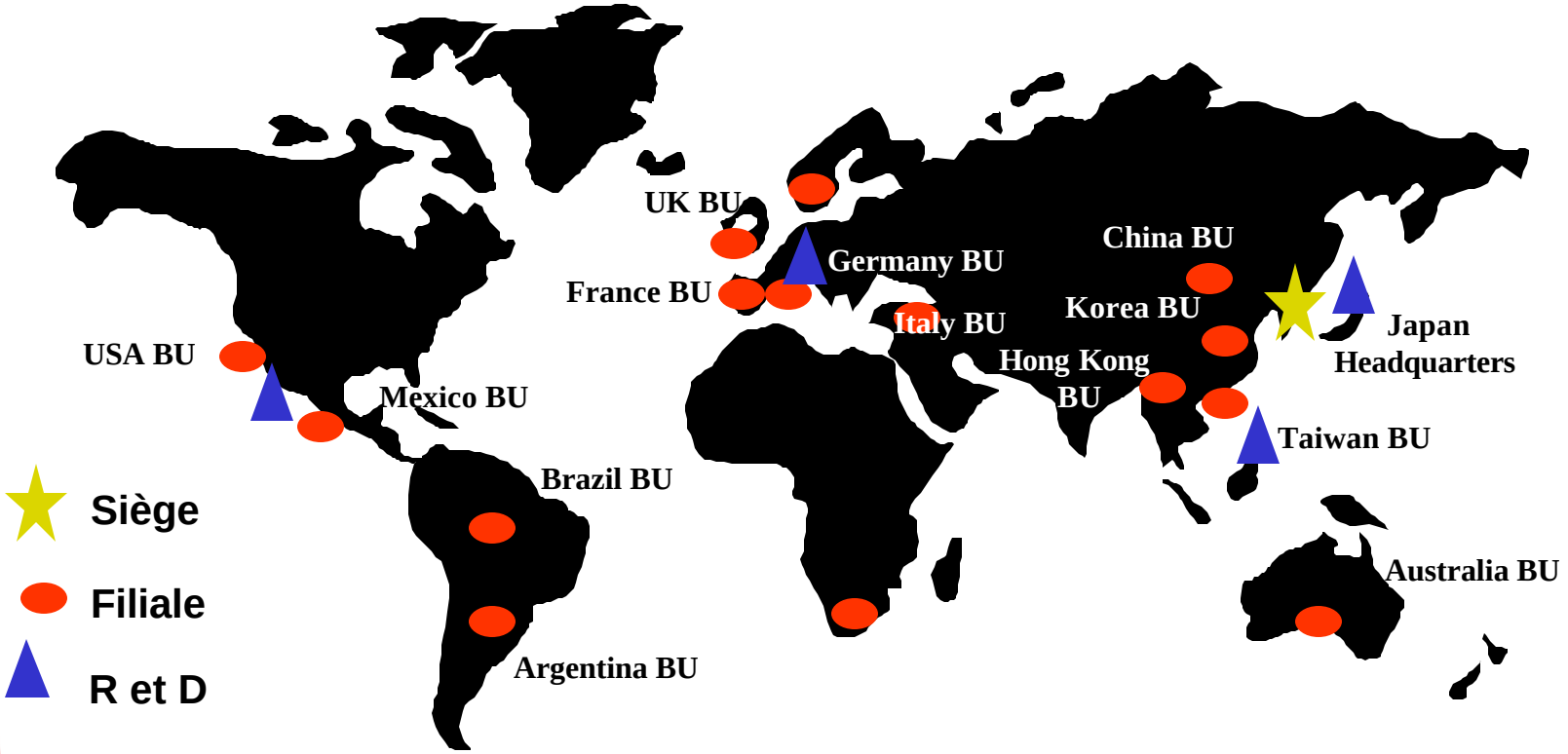
"Antivirus Software: A Segmentation of the Market"

TREND MICRO
your Internet VirusWall®

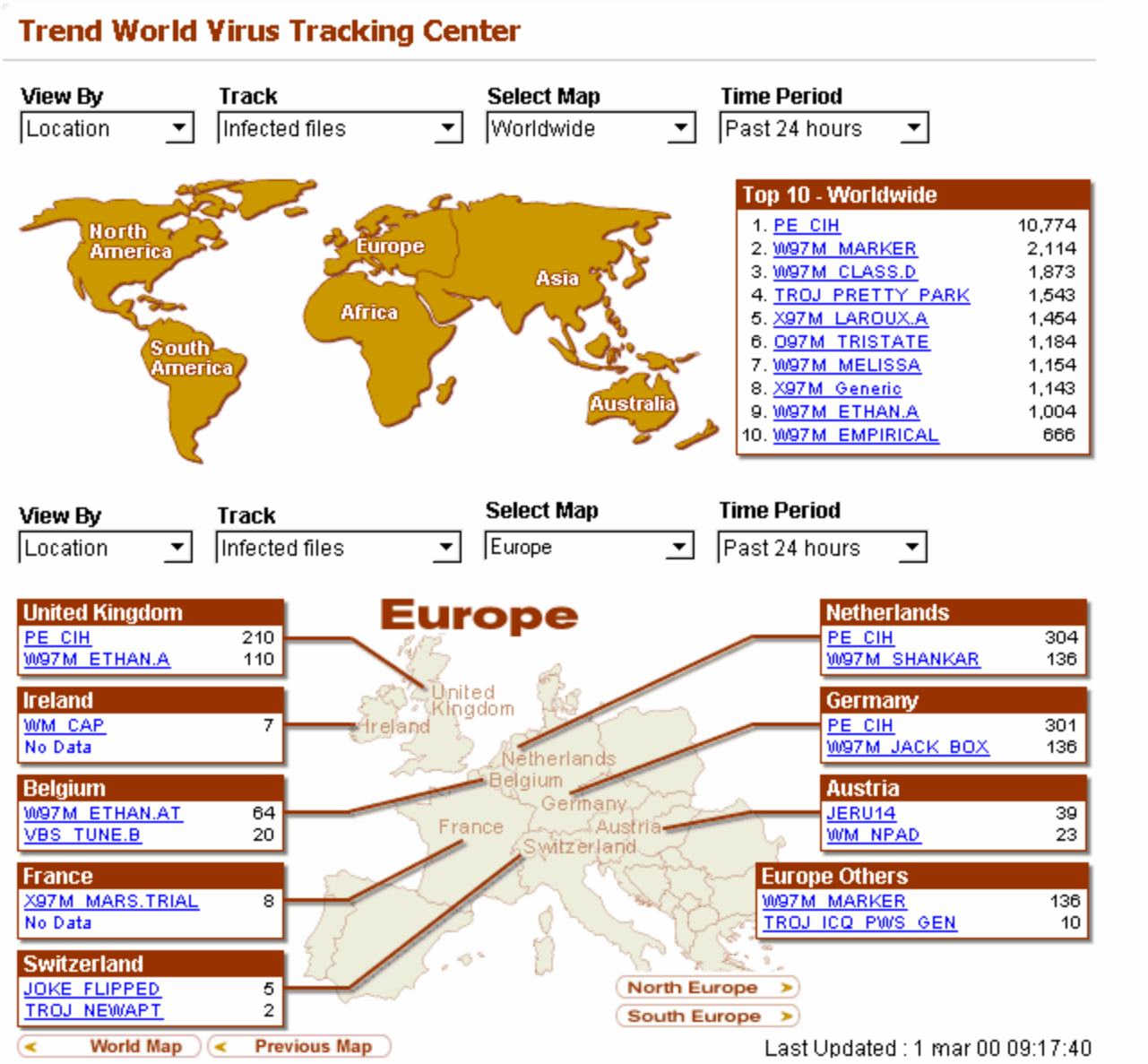
Toujours une technologie d'avance



Trend Micro : 1400 personnes au service de la lutte contre les codes malicieux



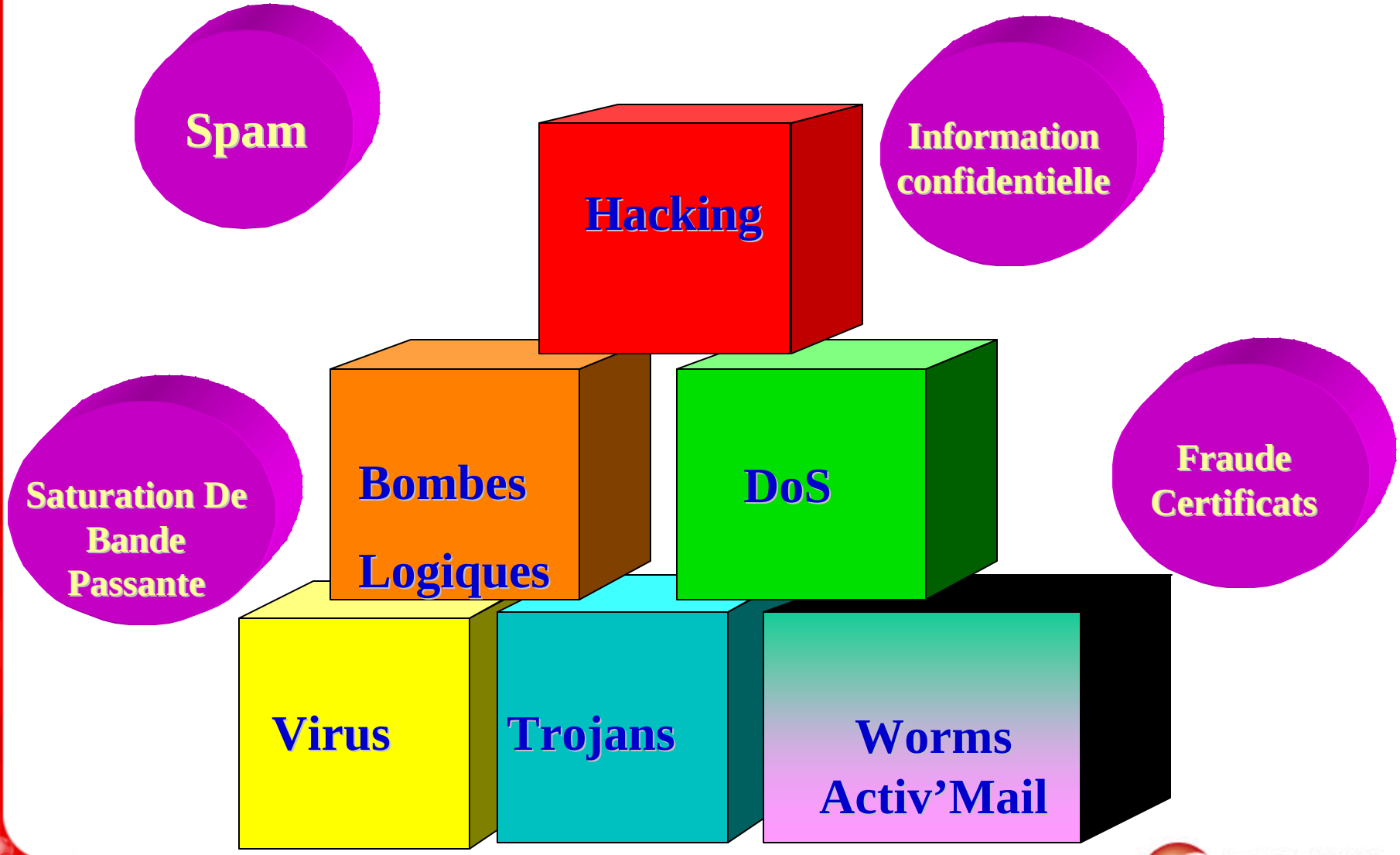
Suivi en temps réel des contaminations dans le monde



Votre besoin d ’informations

- Quelles sont les menaces les plus répandues ?
- Que risque-t-on à être mal protégé ?
- La réponse : des produits et des services adaptés à la mouvance du phénomène viral.

Les types de menaces dans les contenus



Contre quoi luttons-nous ?

Les évolutions des technologies virales

- ***VBS_KAKWORM*** **: premier virus à propagation lente via signature HTML**

- **4 mai 2000 :** ***I LOVEYOU*** **: premier virus en visual basic script à technologie Activ 'Mail à envahir la planète.**

- **28 août 2000 :** ***TROJ_MTX*** **: anti anti-virus !**

- **30 novembre 2000 :** ***TROJ_SHOCKWAVE*****, premier ver utilisant la technologie shockwave**

  - ***NOTA : Les mass 'mailers et spammers deviennent un fléau sur les intranets***

Contre quoi luttons-nous ?

Eté 2001 : SIRCAM, l ’imposteur

- **Sircam s ’est propagé. Il utilise des technologies d ’usurpations :**

  - *Usurpation de codes* : il remplace le contenu d ’un fichier existant par son propre code

  - *Usurpation d ’identité du fichier* : il ajoute une extension .LNK, .EXE, .COM, .BAT ou .PIF à l ’extension originale du fichier après avoir remplacé le code original par son propre code.

  - *Usurpation d ’identité et de contenu* : il se fait passer pour un utilisateur connu en usurpant son identité, et envoie un mail dont le contenu est de type professionnel :

    Hi! How are you?
    I send you this file in order to have your advice
    See you later. Thanks

CodeRed : l ’infiltration furtive

- **CodeRed a été lancé pour *déstabiliser les serveurs Web IIS*, et prouver au monde que toute attaque est possible quelle que soit la technologie de propagation.**

- **Cela nous permet de constater un autre type de spam, beaucoup plus furtif et rapide qu ’avec des technologies de spam par courrier électronique car *les serveurs WEB sont connectés au Net 24h/24*, alors que le courrier électronique doit être lu et exécuté par l ’utilisateur.**

NIMDA : Attaque sur tous les fronts, le 18 septembre 2001

PE_NIMDA ver utilisant 3 technologies de propagations conjointes :

1/ Utilisation du *mail* pour se propager

2/ Propagation au niveau *réseau LAN*

Recherche les unités de Disques locaux et Réseaux partagés pour y déposer son code dans les répertoires.

Crée un partage pour « tout le monde » à l'insu de l'utilisateur

3/ Utilisation d 'une *faille de pénétration des serveurs IIS* en y déposant un fichier prêt à être téléchargé par l'internaute

sous forme de fichier README.EML, s'exécutant ainsi via son Outlook.

Des dégâts difficiles à évaluer

- **CodeRed : 2.6 Milliards de $***
  - Nettoyage des serveurs infectés
  - Interruption des services de commerce électronique
- **Nimda : 700 Millions de $***
  - Mêmes effets **PLUS**
    - Nettoyage des SITES infectés
    - Nettoyage des serveurs de fichiers
- **Et des nuisances non chiffrables**
  - Perte de productivité
  - Problème d'image des entreprises qui ne peuvent plus communiquer.

Source Computer Economics

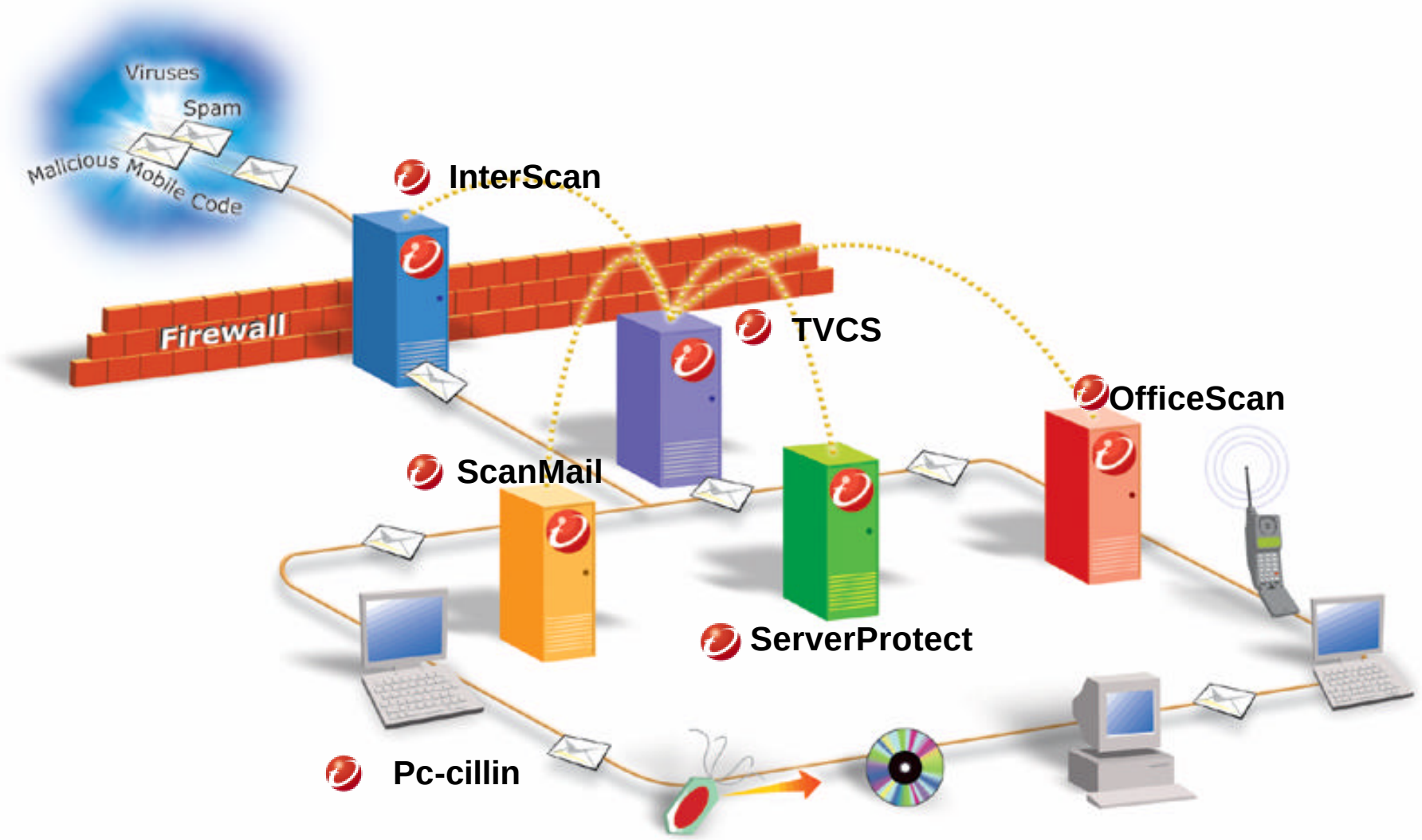
L ’idéal en cas d ’alerte virale

- **Business as usual !**
  - Ne pas avoir à fermer ses serveurs internet et messagerie
  - Avoir le bon outil pour bloquer les mails suspects (si reconnaissables !!)

  - ***Axes de développement de Trend Micro***

    Augmenter la proactivité en déclenchant automatiquement des procédures de blocage de la contamination.

La gamme Trend Micro
Protection de tous les accès à l ’information



Comment se protéger efficacement avec Trend ?

- Une protection virale intégrée à l'architecture du système d'information
- Le poste de travail ne doit pas être la première ligne de défense (ni la seule !)
- Une protection centralisée à laquelle les utilisateurs n'ont pas accès.
- Déploiements et mises à jour automatiques

- Et...

Et les nouveaux environnements

- Les environnements portables :
  - **Palm, EPOC et Pocket PC sont concernés par les virus.**
  - **Même si les virus ne sont pas natifs, ils peuvent transiter par ces environnements dès lors qu'ils possèdent des capacités de stockage suffisantes.**
  - **La réponse : PC Cillin pour le sans-fil (wireless) qui est toujours gratuit.**

Les niveaux de protection

⇨ ***PME/PMI et grandes entreprises***

⇨ ***Internet***

⇨InterScan VirusWall - NT et Win 2000, Solaris, HP-UX, Linux

⇨Trafics : SMTP, HTTP & FTP

⇨ ***Serveurs de fichiers***

⇨ServerProtect NT, Win 2000 et NetWare

⇨ ***Stations de travail en réseau***

⇨OfficeScan Corporate => Windows 95/98, NT, Millenium et 2000

⇨ ***Console globale de Management***

⇨Trend Virus Control System ***(TVCS)***

⇨***Grandes entreprises***

⇨ ***Messageries propriétaires***

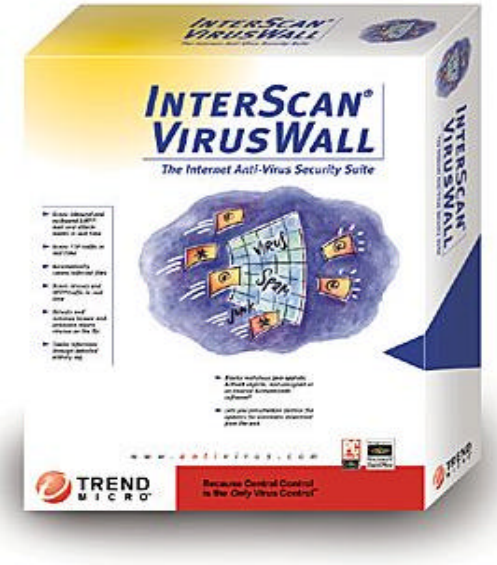
⇨ScanMail Exchange - NT et Win 2000

⇨ScanMail Notes/Domino - NT, Solaris, AIX, AS/400, S/390

TREND MICRO
your Internet VirusWall©

InterScan VirusWall
Protection de la passerelle Internet

- Scanne au niveau de la passerelle,
  les flux en temps réel HTTP, FTP, E-mail/SMTP
- Configurable à distance via un navigateur
- Le programme de contrôle est entièrement au format HTML
- Mise à jour automatique via
  Internet
- Notifications (alertes)
  des administrateurs,
  émetteurs et destinataires
- Journaux d ’évènements précis
  (alertes, tâches, actions….)



TREND MICRO
your Internet VirusWall

InterScan VirusWall : Les Atouts

- **Protège entièrement le réseau de l'entreprise en amont**
  - Transparent pour les utilisateurs
  - Facilité de MAJ/d'Administration
- **Protège les stations clientes du LAN en éradiquant les virus des connexions internet**

- **Multi-plates-formes**
  - UNIX: Solaris, HP-UX, SCO UNIX, Linux...
  - Windows NT/2000
- **Les supports de compressions**
  - Nombreuses technologies de compression supportées
  - Niveaux de compressions multiples et récursives

Et des plug'ins spécifiques……..

TREND MICRO
your Internet VirusWall©

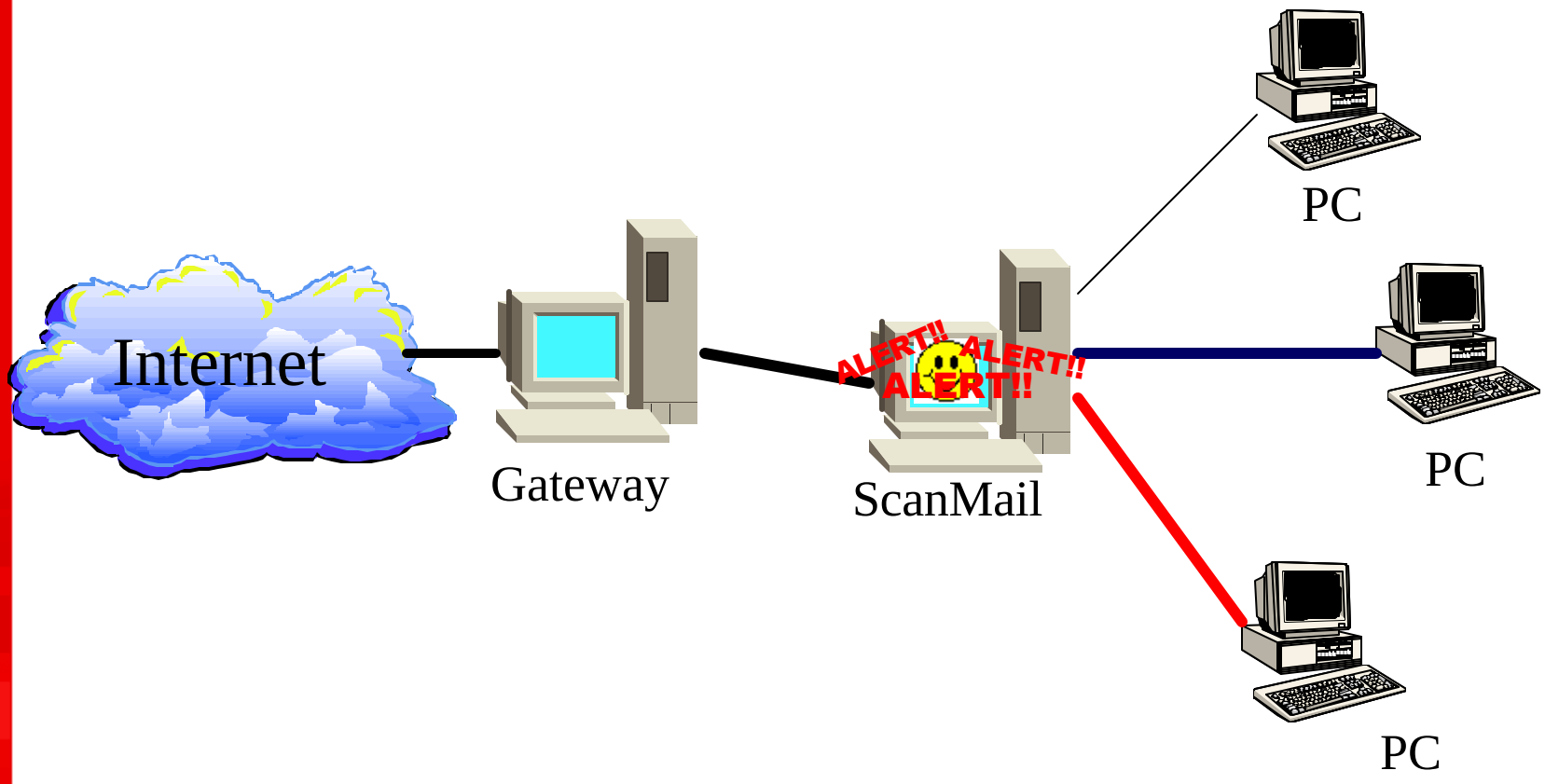
InterScan eManager

- Plug-in d' InterScan VirusWall
- Stoppe les mails de spam à la passerelle internet
- Stoppe les fichiers par nom, par extension (liste paramètrable)
- Administration des emails
- Disponible pour Solaris, HP-UX, Win NT, Win2k, Linux (RedHat, SuSe...)
- eManager disponible pour ScanMail Exchange

InterScan AppletTrap

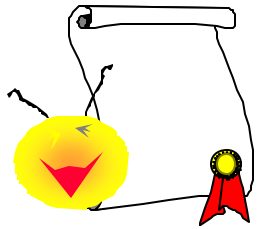
- Contrôle les Active-X et les Applets Java en les certifiant.
- Administration centralisée, aucune installation sur le client requise.
- Disponible sur Win NT, Win 2000, Unix et Solaris

La contamination du serveur de messagerie



Les sources de contamination dans la messagerie Exchange

Par l'eMail

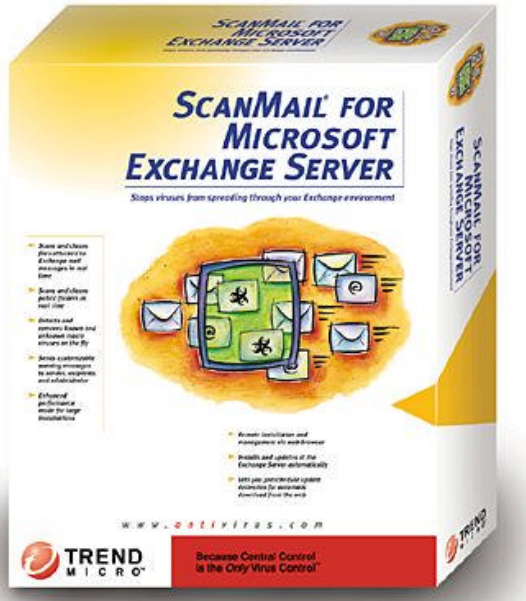


Par les dossiers partagés

Exchange

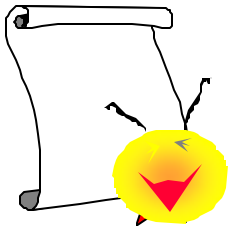
ScanMail Exchange - Fonctionnalités

- **Analyse en temps réel des messages**
- **Analyse des boîtes aux lettres (y compris cachées) & répertoires publics**
- **Fonctionne sur le serveur Exchange**
- **Analyse des répertoires publics**
  - Répertoires sélectionnés
  - Analyse manuelle
  - Analyse pré-programmée
  - En temps réel
- **Disponible pour NT, Win2K**
- **Services packs Exchange supportés**

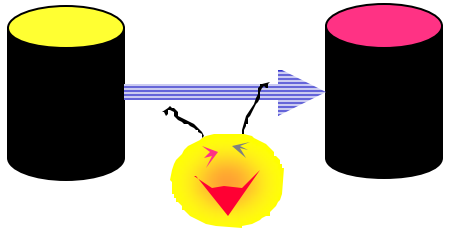


Les sources de contamination dans la messagerie Notes/Domino

Par l'eMail



Par les documents partagés de la Base Notes

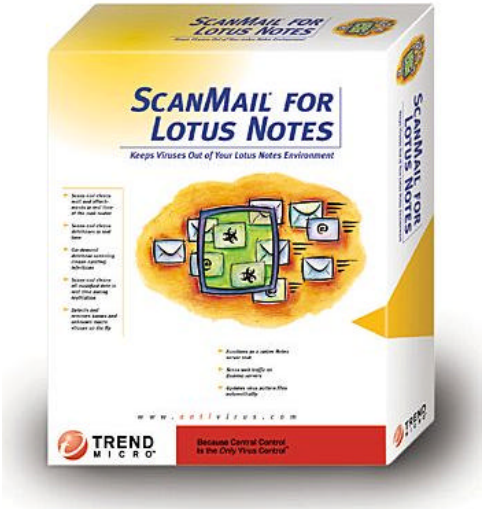


Par la Replication

Lotus Notes

ScanMail Notes - Fonctionnalités

- Architecture native à Notes/Domino
- Interface Web (Domino) ou native Notes
- Analyse en temps réel
- Management remote / mises à jour au travers de la Réplication Notes
- Analyse toutes les bases et applications Notes/Domino



Plates-formes supportées : NT, Solaris, AIX, S/390 et AS/400

Protection des serveurs de fichiers ServerProtect

ServerProtect permet aux administrateurs réseau :

- De gérer leur protection virale sur de multiples serveurs et domaines Windows NT, Windows 2000 et Novell et ce, à partir d'une seule console de management.

- D 'administrer avec cette console les serveurs d'un même domaine et générer des rapports d'incidents viraux de tous les serveurs.

- D 'éviter tout risque lié aux connexions réseau ou aux opérations de maintenance effectués par des intervenants extérieurs sur les serveurs

Protection des Stations OfficeScan Corporate

- Profil idéal d'une protection virale ?
  - Pouvoir administrer, déployer et mettre à jour les solutions de sécurité à partir d'une seule interface pour plusieurs administrateurs.
  - Pouvoir contrôler les utilisateurs sur les options de configuration et de désinstallation.
- OfficeScan **permet cette approche en combinant une solution de sécurité hébergée par le poste de travail et une solution complète de maintien et de déploiement hébergée par un serveur**.

TREND OFFICESCAN CORPORATE EDITION

Workstation Status

Total number of clients : 21
Total number of infected clients : 8

Top Ten Infected Clients

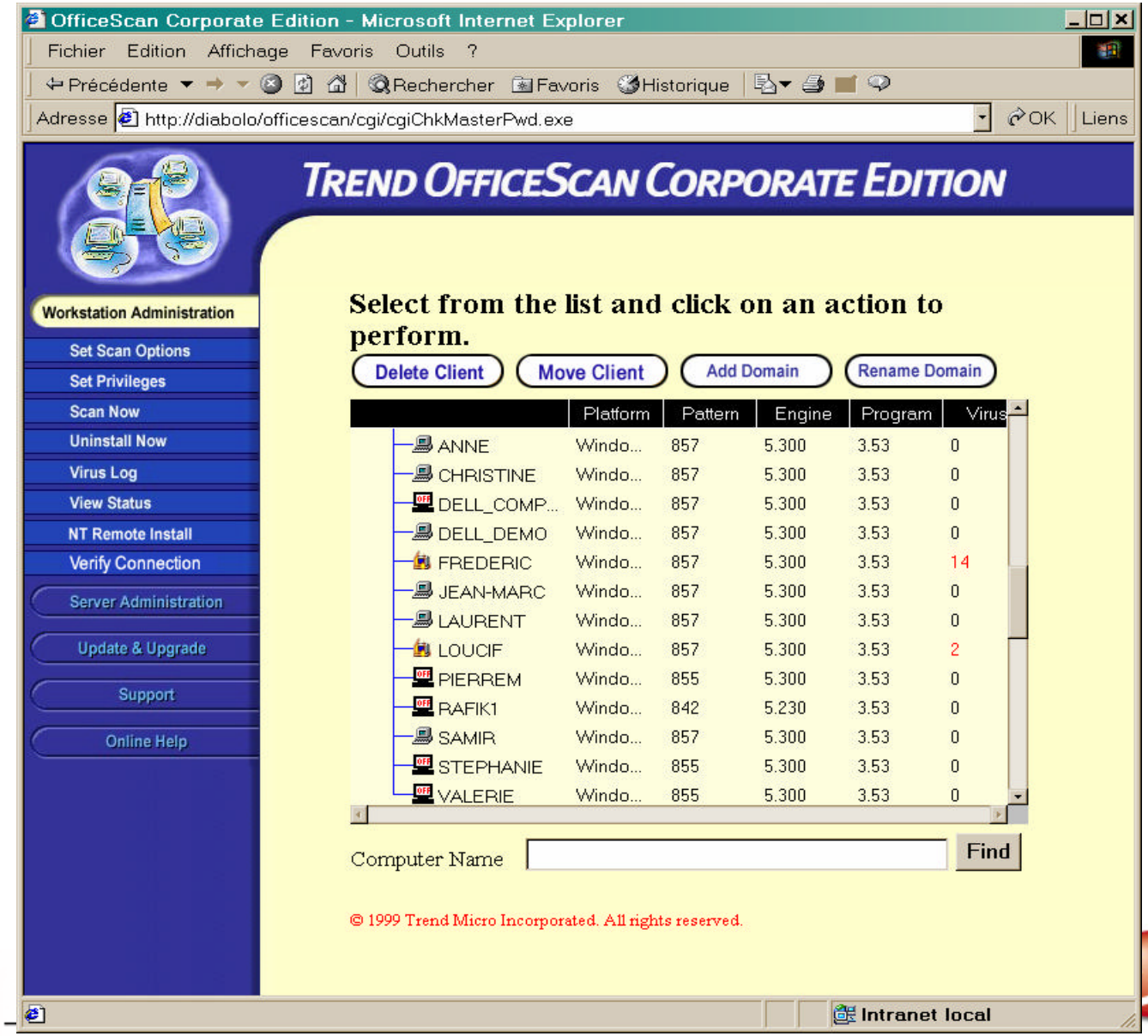
NEUBAUER	88	40.0%
PLATZ14	87	39.5%
ACER-CLIENT-NT	35	15.9%
DELL-MOBIL	3	1.4%
PLATZ010	2	0.9%
PLATZ011	2	0.9%
PLATZ012	2	0.9%
VAIO_FABIAN	1	0.5%

See Infected Client | Reset all virus count

Top Ten Viruses Found

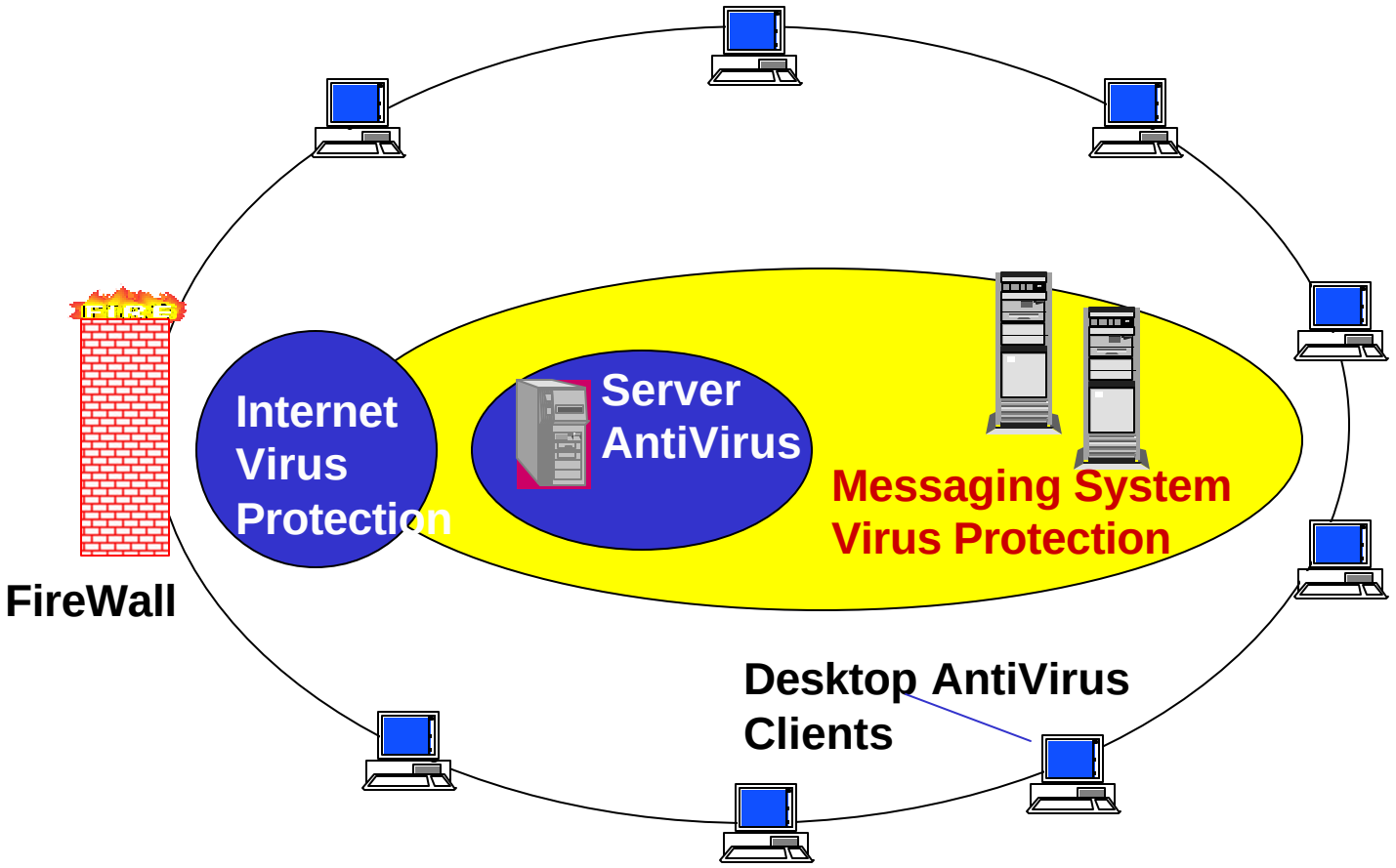
Eicar_test_file	41	13.1%
NE_TEST_VIRUS	33	10.5%
PE_TEST_VIRUS	31	9.9%
JAVA_TEST_VIRUS	24	7.7%

Protection des stations : La visibilité ?

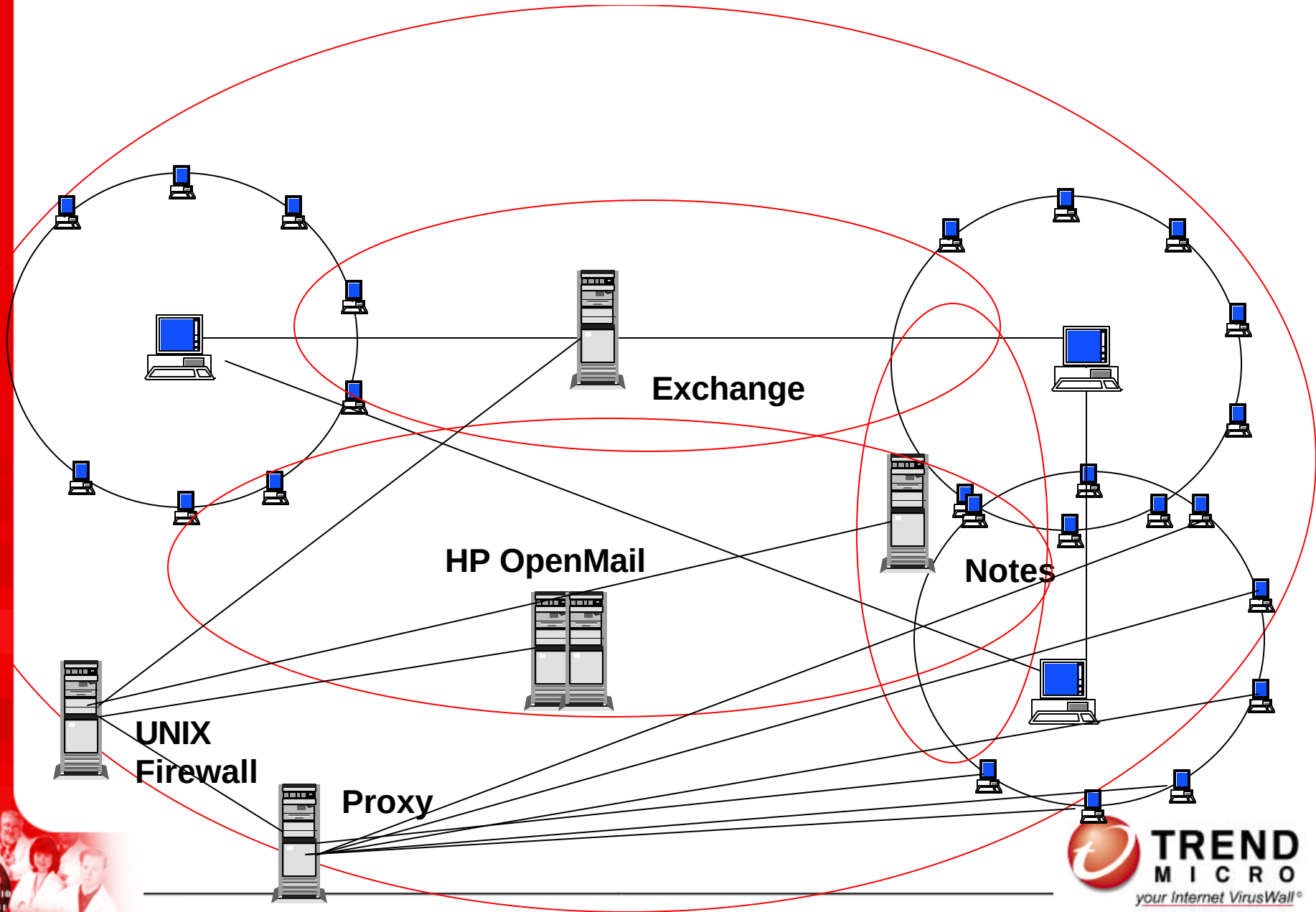


TREND MICRO
your Internet VirusWall

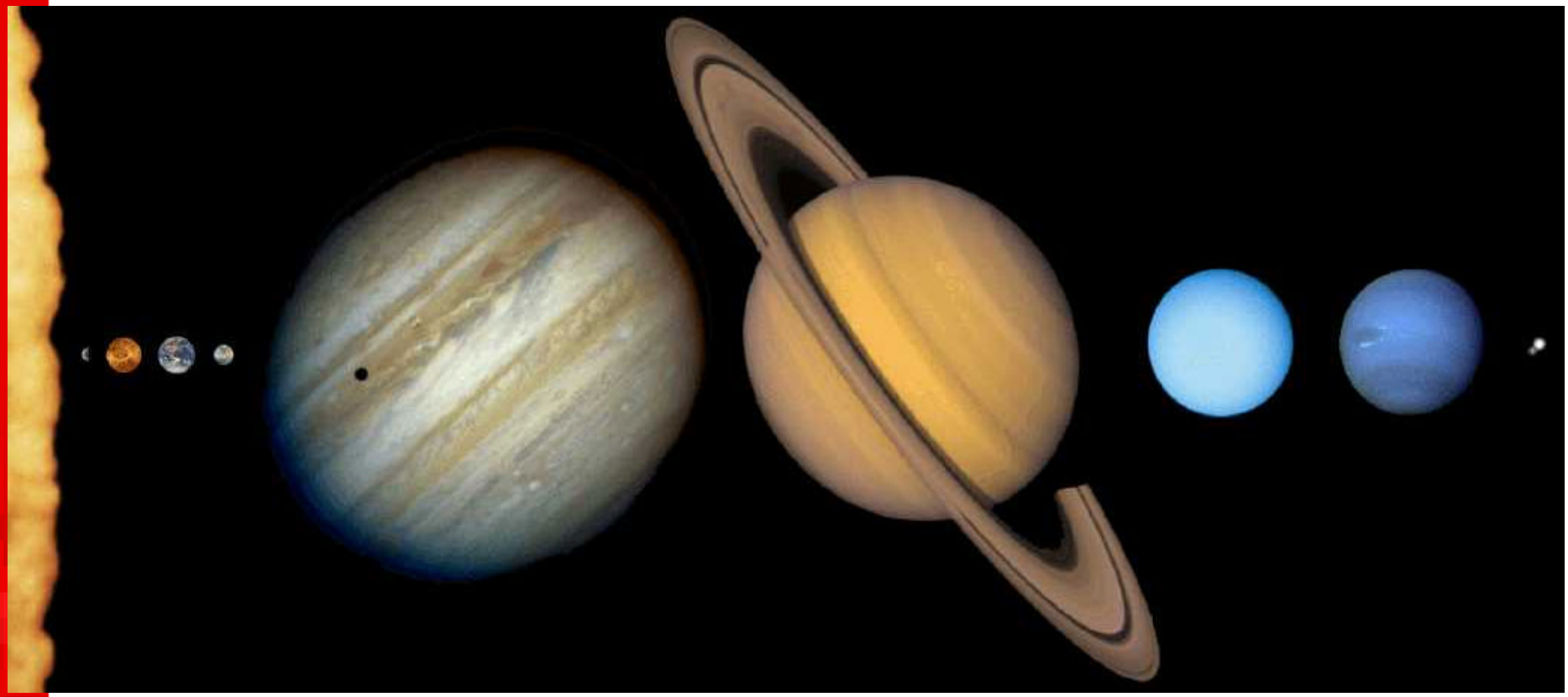
Dans le meilleur des mondes...



Le réseau dans la réalité . . .



Trend Virus Control System



La console web universelle et intégrée pour la protection virale

Pourquoi une console de management centralisée ?

- **Un seul outil pour manager**
  - les différents niveaux de protection virale
  - les différentes plates-formes antivirus
  - l'activité virale dans le réseau - log
  - Le déploiement, la mise à jour
- **Un système doté d'une architecture novatrice utilisant les avantages des dernières technologies informatiques en matière réseau**

Votre besoin une veille permanente

- Système de pré-alerte Information labo
- Système de pré-défense eManager
- Antidote ultra-rapide

Vous avez un doute sur un fichier ?

N ’hésitez pas à tester le support !

TREND MICRO
your Internet VirusWall©

En résumé, les qualités d'une bonne protection virale

- **Les Logiciels**
  - ⇨ Une gamme complète => Protection totale
    - ⇨ Plate-formes : NT/2000, Solaris, Linux,
    - ⇨ SMTP, Notes / Domino, Exchange, ...
  - ⇨ Taux de détection / éradication élevés (Certification ICSA)
  - ⇨ Déploiement / Mises à jour simples et automatisés
- **Le Management de la solution**
  - ⇨ Solutions cohérentes, efficaces, et harmonieuses
  - ⇨ Vision globale de l'activité virale dans l'Entreprise
- **Les Services**
  - ⇨ Réactivité des Laboratoires, Alertes virales, ...
  - ⇨ Antidote sur mesure - Bombes logiques, Chevaux Troie
  - ⇨ Veille technologique
  - ⇨ *Formations aux produits et aux technologies*

Trend Micro

- **Vous apporte :**
  - La sécurité du choix
  - Des services totalement spécialisés
  - Une gamme couvrant l ’ensemble des besoins en protection virale des entreprises
  - Une expertise sans cesse enrichie

Vous avez des questions ?

A nous de vous apporter les réponses !