StormShield - Version 4.0

SkyRecon®
Intelligent Client Security

Presentation OSSIR 10 juillet 2006

SkyRecon Systems - éditeur de StormShield

- Editeur de Logiciels Français
  - De grands groupes parmi les investisseurs: DGA, la CDC, Thales, AVIVA, EADS…
  - Présence européenne
- Parrainé par Microsoft
  - Parrainage technologique et commercial
- Éditeur actif dans la communauté logicielle
  - Membre de la SecureIT Aliance
  - Membre de la « European Software Association »
  - Membre de l'AFDEL
- Forts partenaires Européens
  - Partenariat stratégique avec NEC dans 40 Pays
  - Alcatel, Microsoft
- Lauréat de nombreux prix
  - Red Herring 100 Europe
  - IE Club
  - Start West

Ils ont choisi StormShield...

Industrie

SITA SUEZ
apave
Atys
ALCAN
PERENCO
IBIDEN
HENRY SCHEIN®
wheelabrator
SBM

Banque / Finance

PACIFICA
GMF
Groupama
AVIVA
Boursorama
Votre partenaire pour investir
GROUPE MORNAY

Administration / Éducation

Conseil Général des Vosges
OGC
Office of Government Commerce
Aube
Conseil Général
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
ACMS
Pour la santé au travail
iéseg
SCHOOL OF MANAGEMENT
CHAMBRE DE COMMERCE ET D'INDUSTRIE DE BREST
ileDeFrance

Services / Commerce

Impress
NESS
vivarte
promod
Gide Loyrette Nouel
AEGIS MEDIA
CINEBANK
VIDEO 24H/24
TROYES HABITAT
NAFNAF
SHOP
ORSID

Qu'en pensent-ils ?

- Microsoft

  « La technologie de protection d'avant-garde de SkyRecon pour les environnements Windows a retenu toute notre attention »

- Frost & Sullivan

  « Frost & Sullivan believes that SkyRecon Systems is an ideal partner to help organizations achieve the desired level of security and protection at the endpoint»

- Secure Computing Magazine

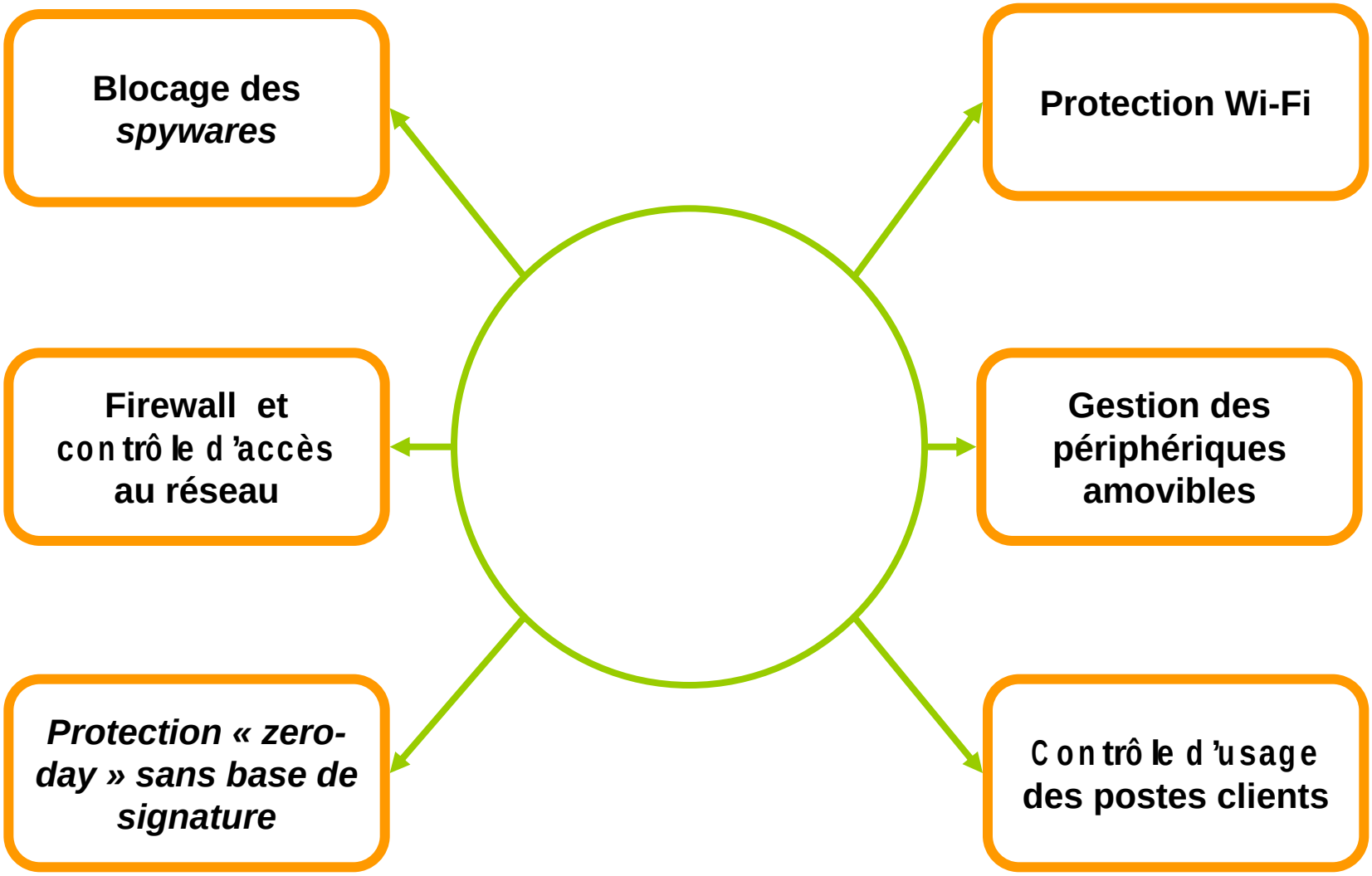
  « StormShield provides excellent and detailed protection for your PCs and Notebooks »

- Network Computing

  « StormShield allows network managers to create fine-grained security solution that offers detailed control over the activities of all network users »

- Validé par des organismes indépendants
  - CERT IST
  - Veritest
  - Alcatel

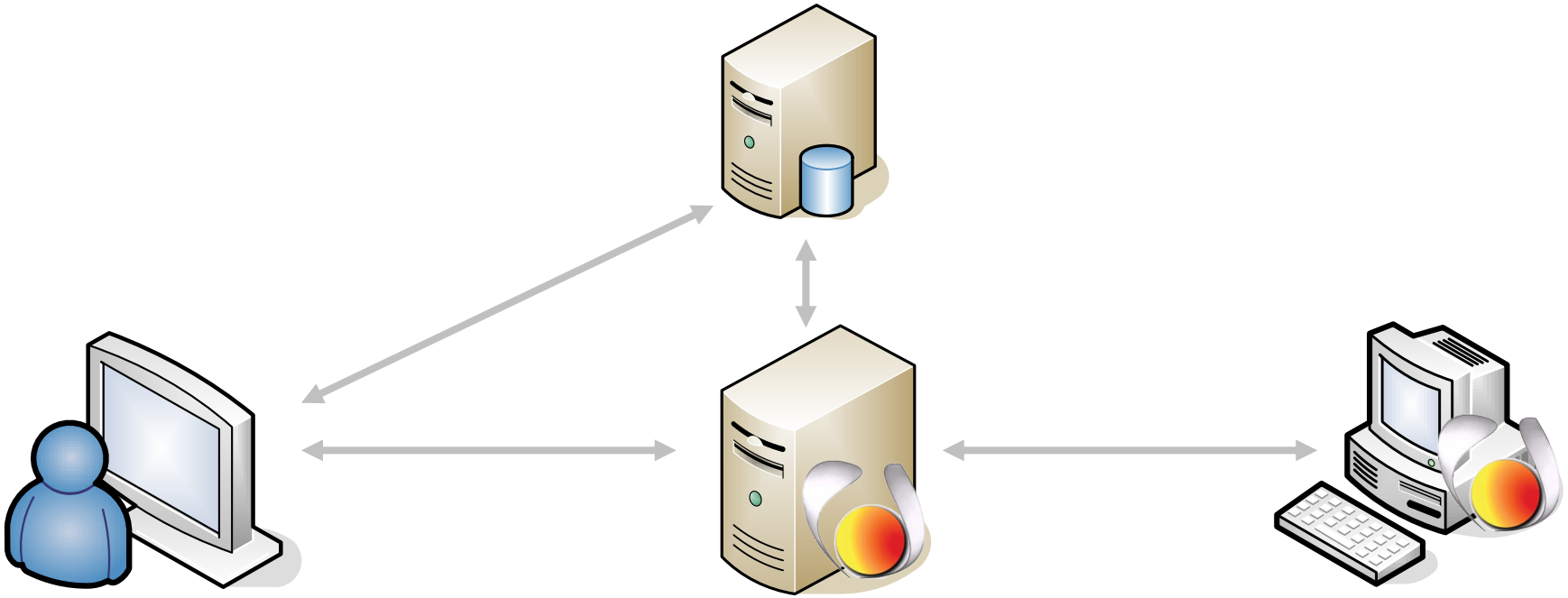
StormShield : Les principales fonctionnalités



Composants StormShield

- Stockage des évènements

Base de données StormShield



SkyRecon Management Console

- Description du parc
- Définition des politiques
- Administration des composants
- Monitoring et reporting

Serveur StormShield

- Distribution des configurations
- Consolidation et stockage des événements
- Clustering et load-balancing

Agent StormShield

- Import et application de la configuration
- Défense automatique
- Envoi des logs et alertes

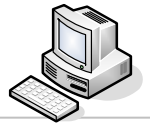
Composants logiciels

Console d'administration

- Configuration des politiques de sécurité et du comportement des agents
- Définition des critères de mise en conformité
- Configuration et gestion des composants StormShield
- Administration des utilisateurs et de l'architecture StormShield

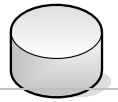
Serveur StormShield

- Mise à disposition des politiques (modes push)
- Récupération des évènements depuis les agents et envoi vers la base de données
- Tolérance de panne et répartition de charge avec un serveur esclave



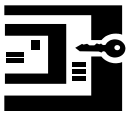
Agent StormShield

- Composant assurant que les politiques du postes sont bien appliquées
- Réception des politiques (mode pull)
- Envoi des évènements (logs)



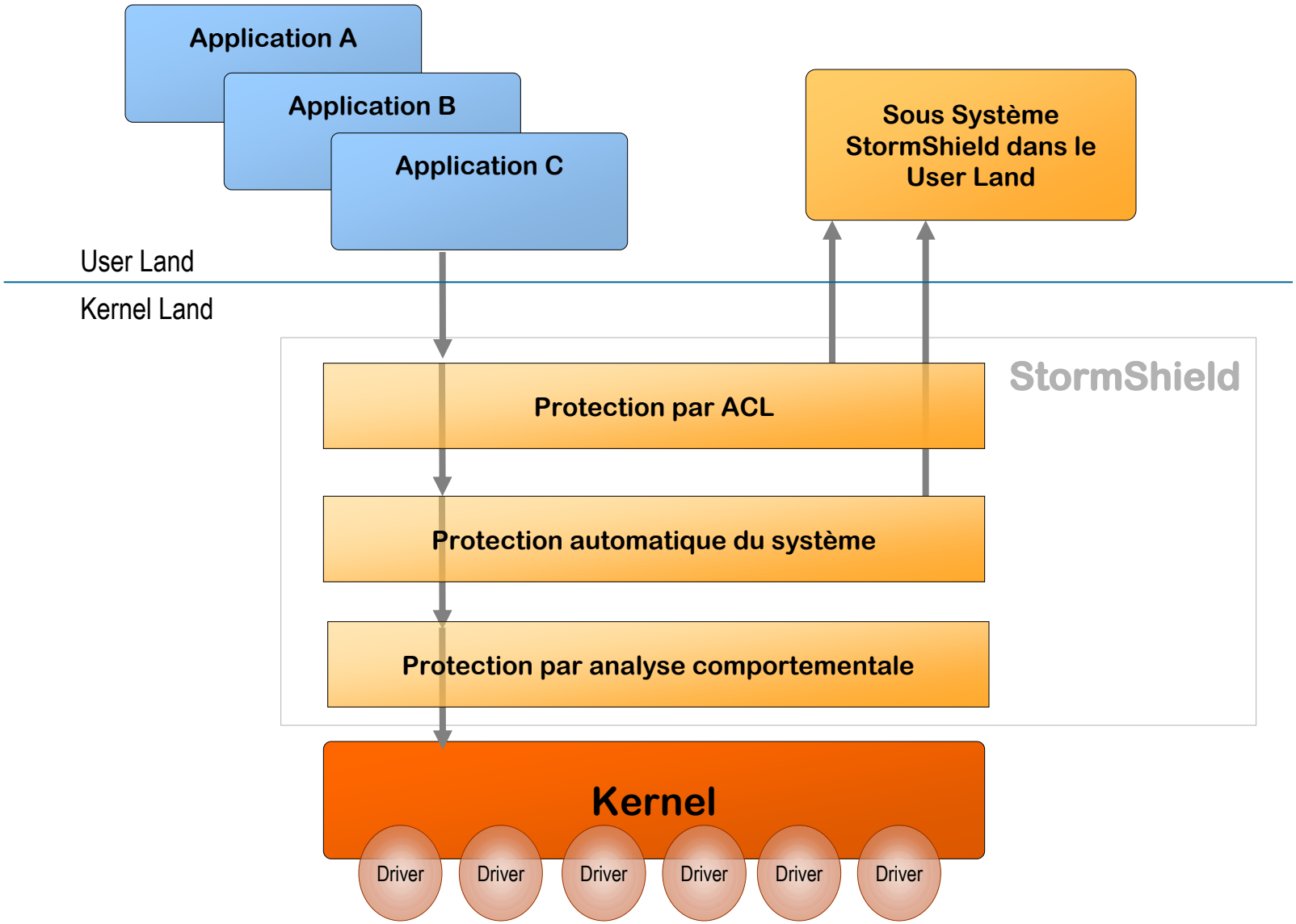
Base de données

- Stockage des configurations et des politiques
- Informations sur les utilisateurs de StormShield
- Stockage des évènements des agents reçus par le serveur

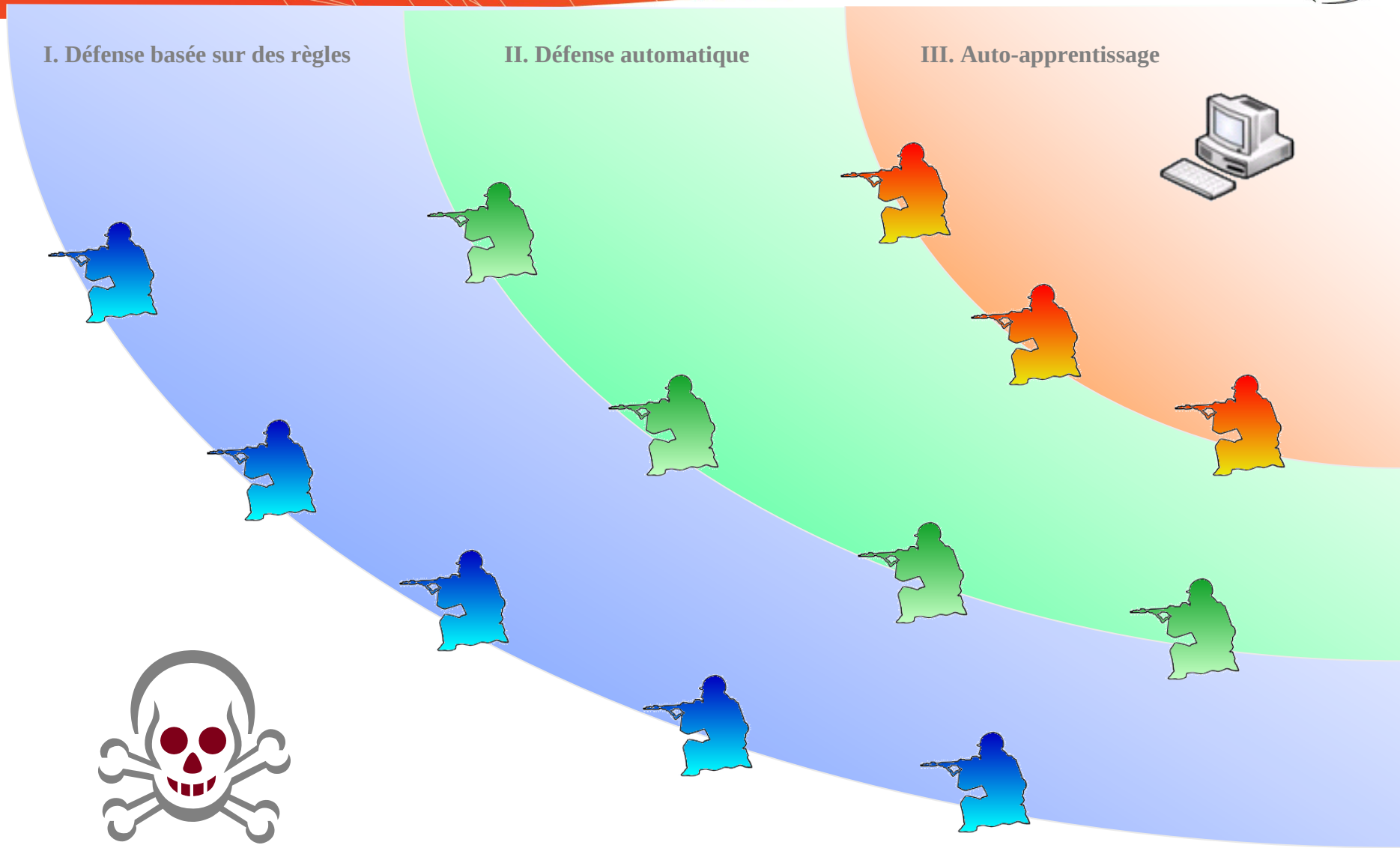


Communications cryptées en SSL v3 (certificats x509)

Une technologie unique



Sécurité globale avec 3 Lignes de Défense



Couche 1 : Créer une politique d'usage

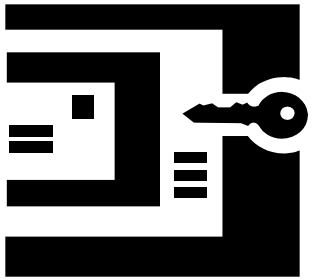
Quelques exemples de politiques d'usage

- Bloquer les outils d'IM : MSN, Yahoo, Skype…
- Filtrage de paquets et de ports
- Empêcher le transfert de fichiers en IM
- Bloquer la désinstallation/désactivation de l'antivirus
- Interdire le changement des paramètres réseau du PC
- Forcer le PC à utiliser son VPN pour aller sur le web
- N'autoriser que certaines applications ou certains fichiers à fonctionner sur le PC
- …etc

Couche 2 : la défense automatique

Quelques exemples de défense automatique

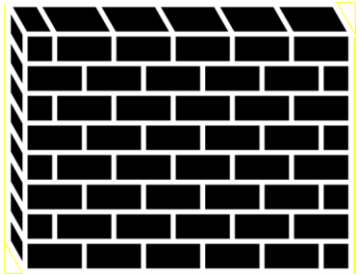
- Blocage proactif des attaques « memory overflow »
- Reboot intempestif des PC
- Saturation du processeur
- Détection et blocage des supports amovibles
- Détection et blocage des injections de process
- Détection et blocage des élévations de privilèges
- …etc



Couche 3 : l'auto-apprentissage

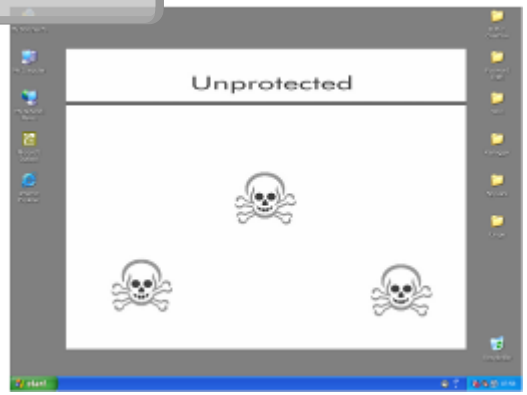
Objectif : Contrer les menaces inconnues et protéger contre les vulnérabilités des applications

- Période et cycles d'exécution à définir par l'administrateur
- Apprentissage du fonctionnement des applications
- Détecte les comportements anormaux
- …etc



Démonstration de StormShield

Non protégé



Protégé

- **Attaque virale**
- **Attaque par faille logicielle**
- **Prise de contrôle à distance**
- **Vol de mot de passe par faille logicielle**
- **Vol d'information par keylogging**
- **Installation de spyware**

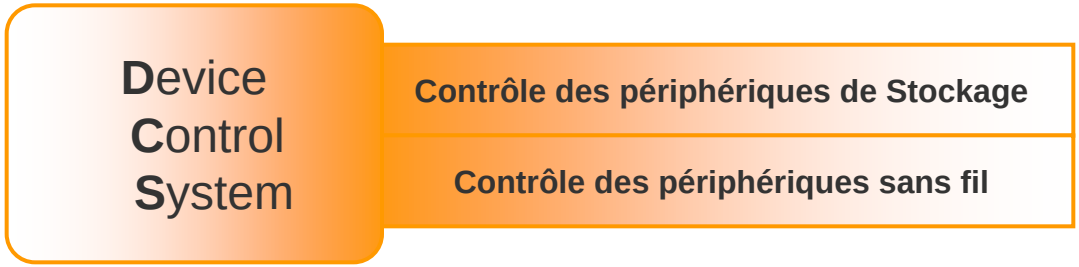
L'offre StormShield

SkyRecon®
Intelligent Client Security

EndPoint Security Agent

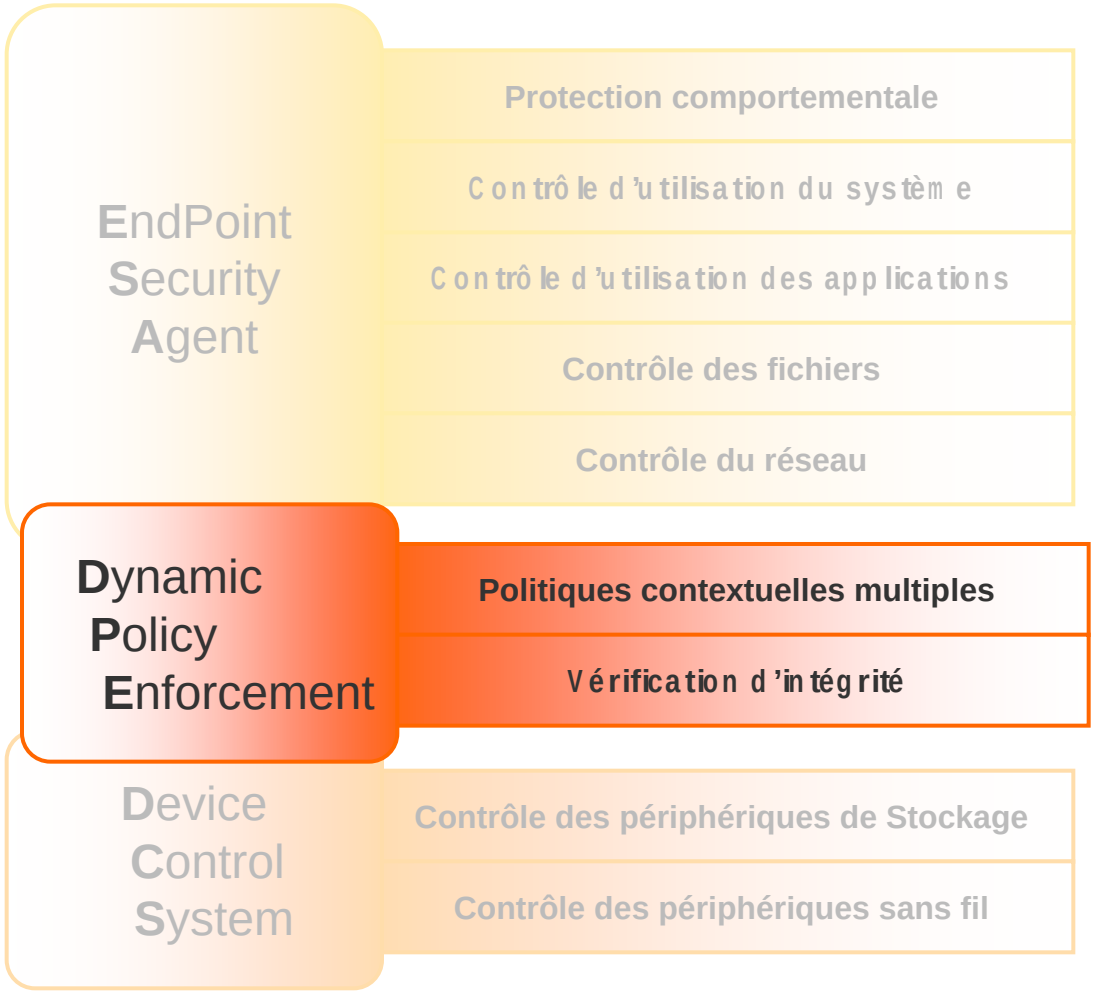
- Protection comportementale
  - Apprentissage
  - Protections automatiques
- Utilisation du système
  - Panneaux de contrôle
  - Base de registre
  - Fichiers systèmes
- Utilisation des applications
  - Installation d'applications
  - Utilisation d'applications
  - Restrictions des ressources par application
- Contrôle des fichiers
  - Droits d'accès sur les extensions
- Contrôle du réseau
  - Firewall Stateful NDIS
  - Filtrage multi-niveau
  - IDS embarqué
  - Contrôle d'intégrité des trames

Device Control System



- Périphériques de stockage
  - USB
  - Firewire
- Gestion des exceptions
  - Par type de périphérique
- Pas de blocage du port physique
  - Possibilité de connecter d'autres types de périphériques (souris, clavier, imprimante…)
- Gestion des Graveurs de CD
- Gestion du Bluetooth
- Gestion du Wi-Fi
  - Contrôle du mode ad-hoc
  - Contrôle des points d'accès autorisés
  - Contrôle des méthodes de cryptage et d'authentification

Dynamic Policy Enforcement



- Politiques contextuelles

  En fonction de critères tels que:
  - Adresse IP allouée
  - Passerelle par défaut
  - Serveur DNS
  - Contexte DNS
  - …

- Vérification d'intégrité
  - Services
    - Anti-Virus
    - Windows Update
    - …
  - Fichiers
    - Signatures
    - Patches
    - …
  - Base de registre
    - Configurations

- Remédiation
  - Lancement de batch
  - Lancement de service
  - Application de politique restrictives

EndPoint Security Suite

EndPoint
Security
Agent

Dynamic
Policy
Enforcement

Device
Control
System

EndPoint
Security
Suite

La suite complète, regroupant tous les modules de StormShield

Merci !

SkyRecon®
Intelligent Client Security