



Utimaco

The Data Security Company

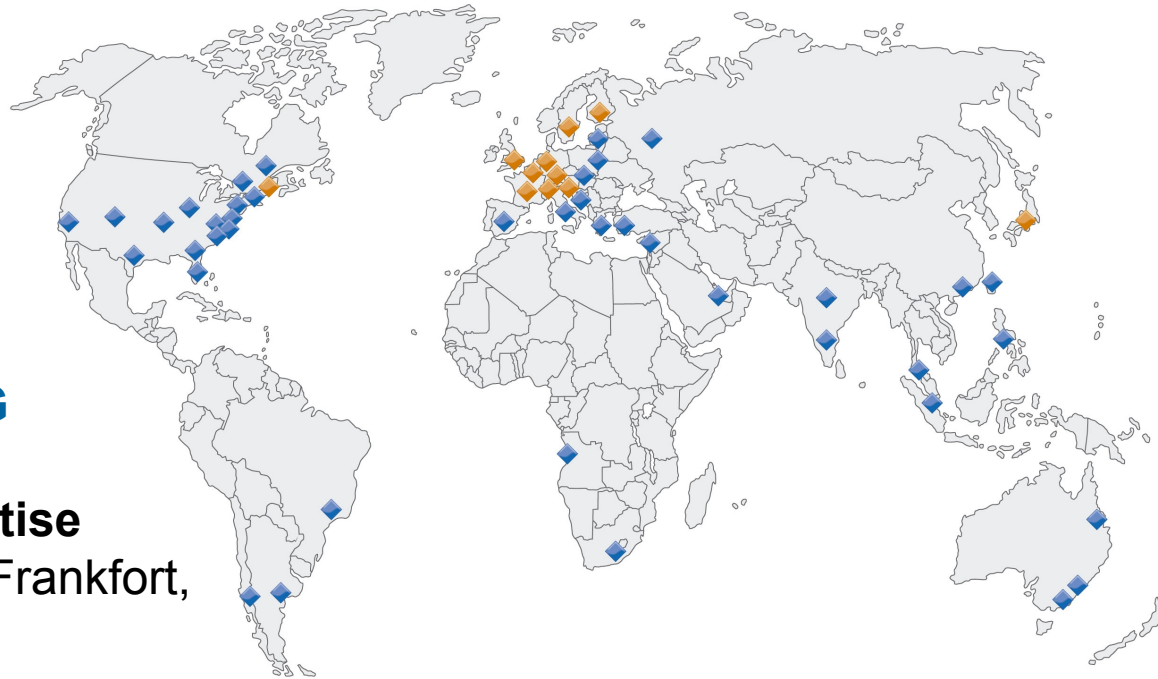
Olivier Perroquin

Le 10 décembre 2007

utimaco[®]
s a f e w a r e

A propos d'Utimaco

Aperçu de la société

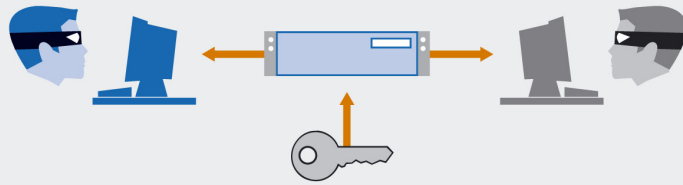


Utimaco Safeware AG

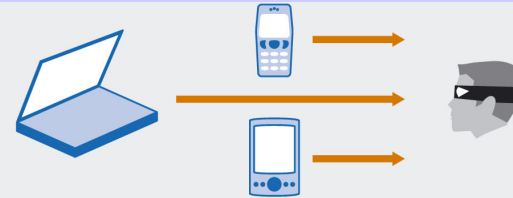
- ▶ Créé en 1983
- ▶ **25 années d'expertise**
- ▶ Entreprise cotée à Frankfort,
- ▶ Siège à Oberusal
- ▶ 300 employées
- ▶ 15 filiales et un fort réseau de partenaires
- ▶ € 50 million de CA 2006/2007
- ▶ € 11 millions résultat net 2006/2007
- ▶ 5 millions de licences / 5000 clients
- ▶ **Spécialisée dans la sécurité des données**

Les menaces sur les d'informations

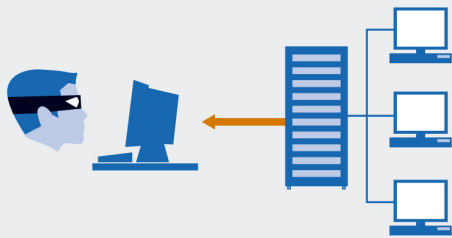
6. Vol des clés



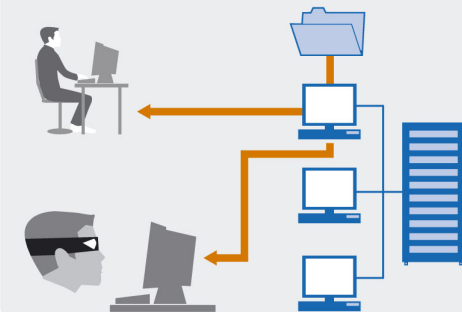
1. Perte ou vol de terminaux



5. Accès illicites sur les serveurs



2. Infogérance non sécurisée



4. Vol des média amovibles

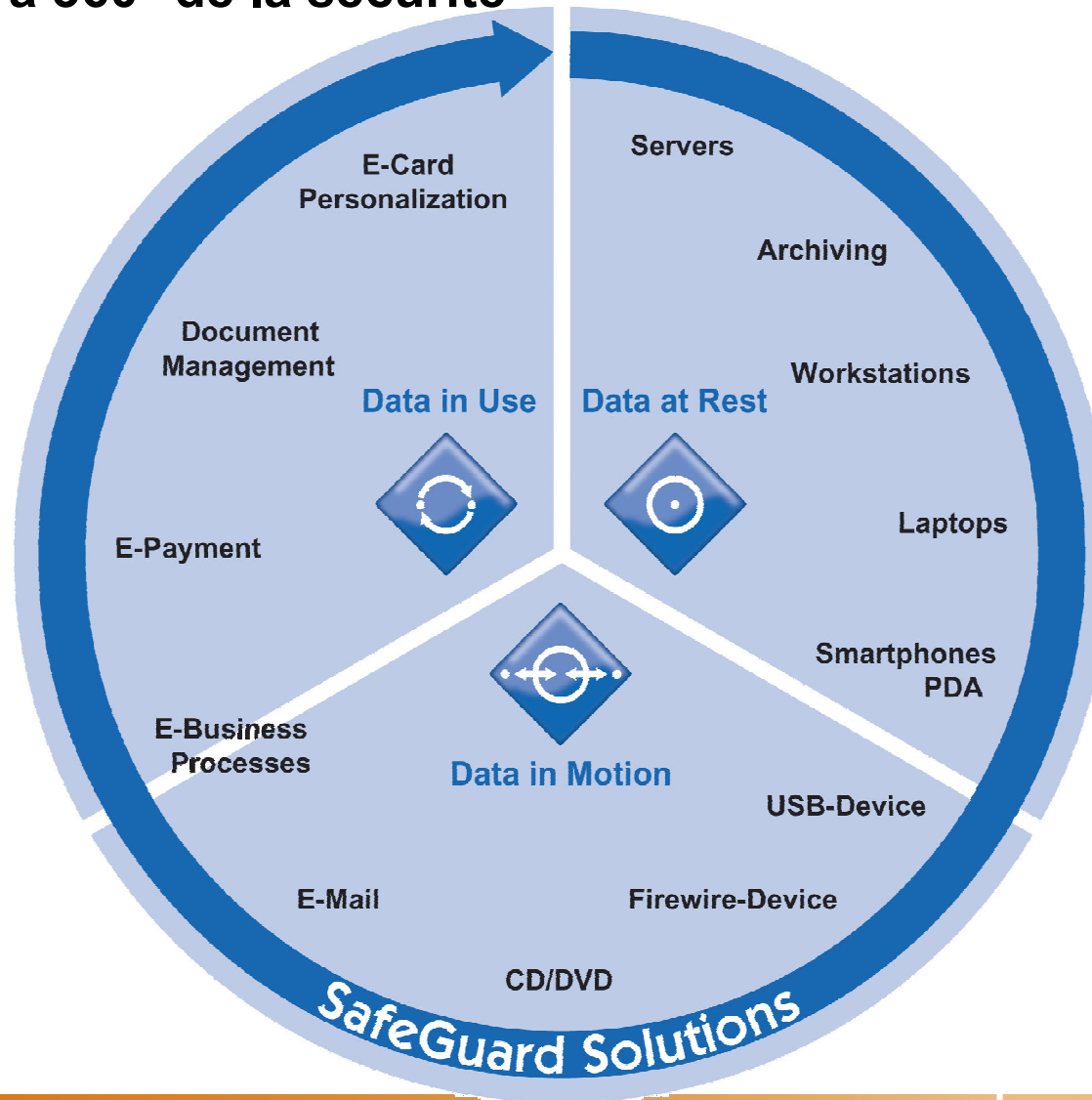


3. Interception des e-mails



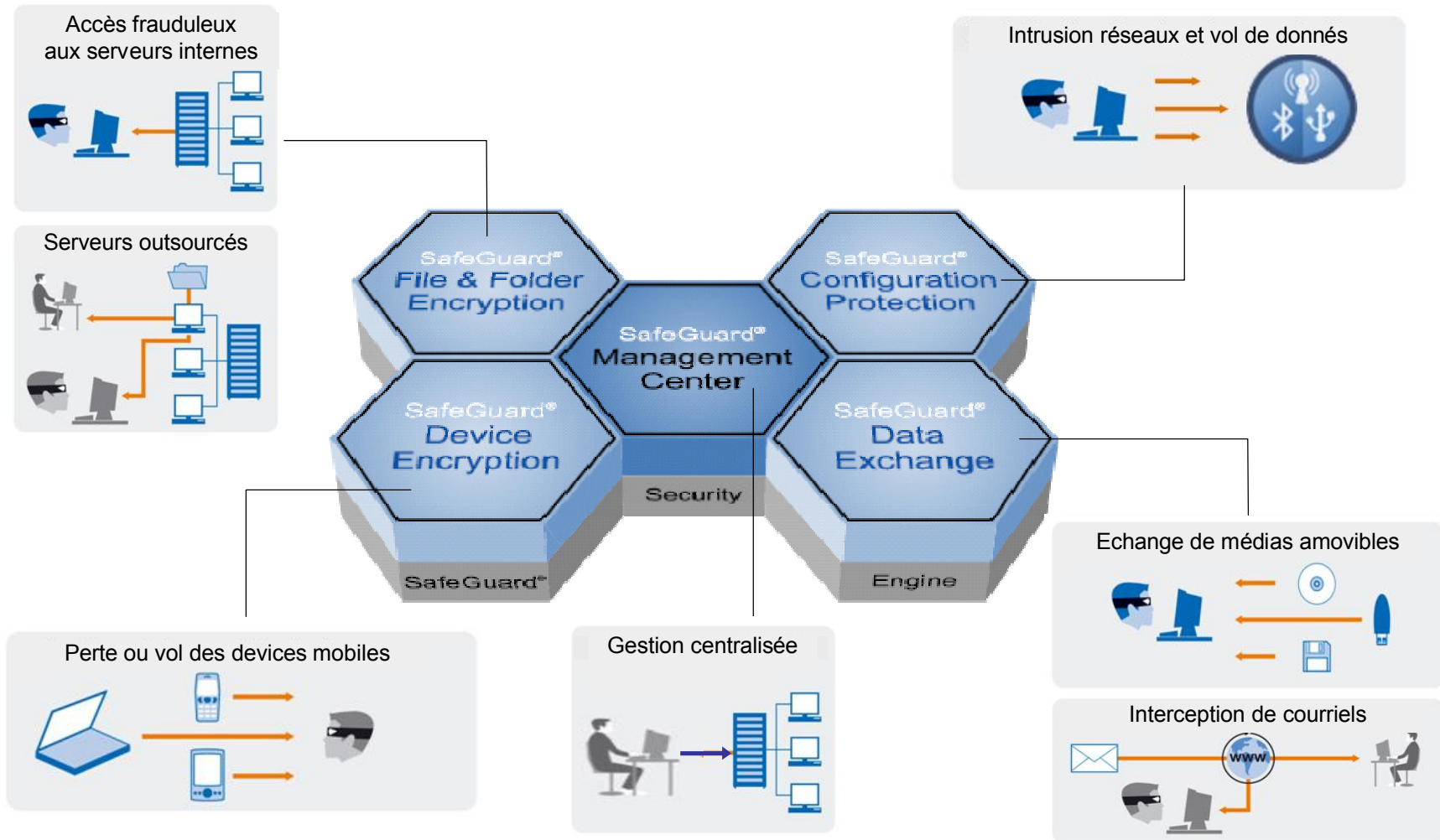
Solutions SafeGuard

Approche à 360° de la sécurité



SafeGuard Enterprise

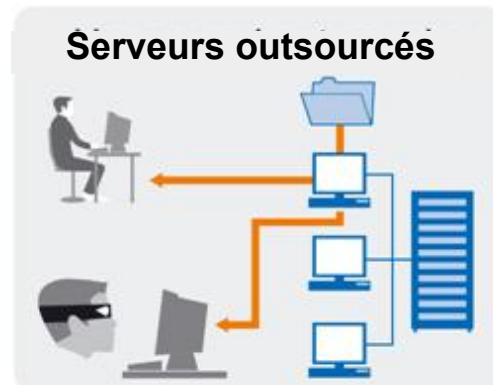
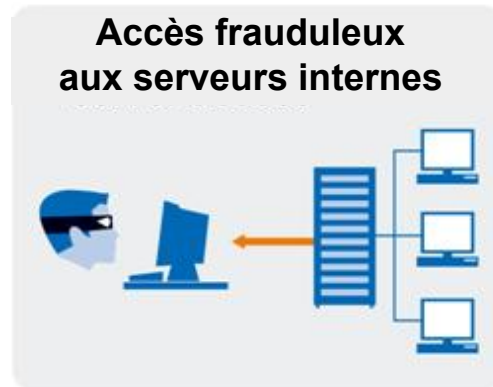
New Generation Data Security Suite



La protection globale de vos données

Partage sécurisé des données

En internes ou externalisée

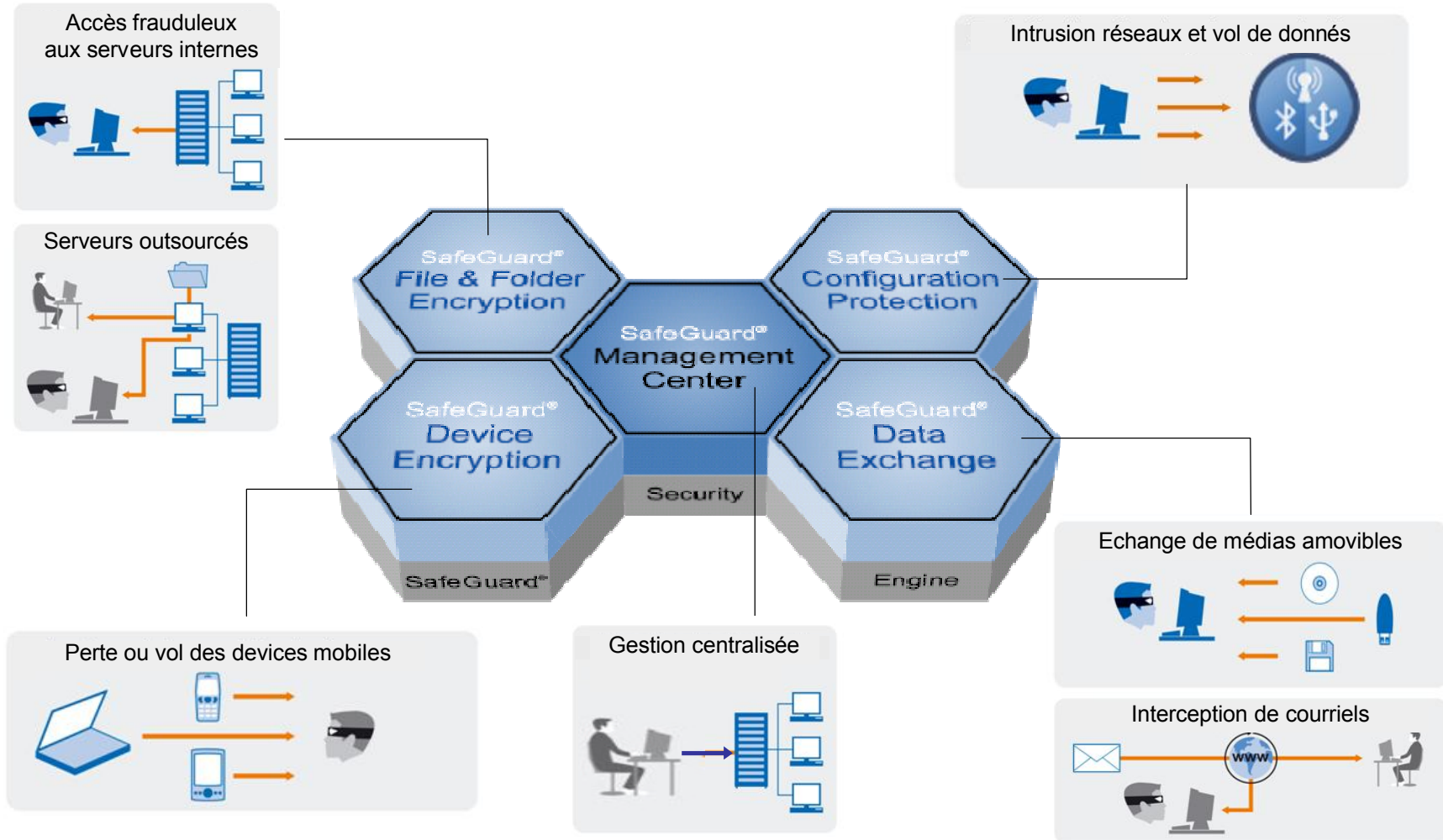


► SafeGuard LanCrypt

- ◆ Chiffrement des données
 - Chiffrement fort (IDEA,AES,3DES)
 - Chiffrement partagés ou personnel
 - Chiffrement selon un profil défini
 - Règles
 - Clés
- ◆ Authentification forte de l'utilisateur
 - Par certificat (logiciel ou puce crypto)
 - L'accès au trousseau de clés
 - L'application des règles de déchiffrement / chiffrement
 - Transparent pour l'utilisateur
- ◆ Division des rôles d'administration réseau vs sécurité
 - Hiérarchie des rôles

SafeGuard Enterprise

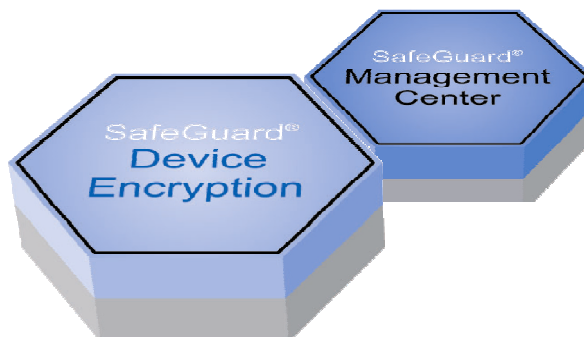
New Generation Data Security Suite



La protection globale de vos données

Protection contre le vol ou la perte

Ordinateurs Portables et de bureau



► SafeGuard Device Encryption /Easy

- ◆ Chiffrement global des disques durs:
 - Chiffrement secteurs
 - Chiffrement fichiers
 - Chiffrement du boot
- ◆ Authentification avant boot et après hibernation ou veille
 - Authentification Windows
 - Authentification forte avec token
 - Authentification forte avec certificats/token
 - Authentification forte biométrique (Lenovo)
- ◆ Recouvrement
 - Authentification par Challenge/Réponse
 - Recouvrement de clés

SafeGuard Enterprise

Démarrage du poste

1. L'utilisateur démarre son poste
2. Le BIOS devient actif
3. La POA s'affiche
4. L'utilisateur s'authentifie ...
 - ⇒ Par User ID & password
 - ⇒ Par credentials sur token
 - ⇒ Par certificat sur token
5. Windows est lancé depuis la partition chiffrée
6. Logon Windows automatique ou manuel



SafeGuard Enterprise

Déblocage du poste



► Recouvrement des clés

◆ Clés de chiffrements

- Générées sur le serveur
- Générées sur le poste
- Synchronisées client/serveur
- Toutes archivées sur le serveur

◆ Officier de recouvrement

- Opération mono/multi officiers
- Attribue la clé à recouvrir à un autre trousseau
- S'authentifie au trousseau
- Déchiffre les données puisque détient la clé

► Accès au poste

◆ Mot de passe avant boot oublié

- Authentification par Challenge/Réponse
- Possibilité de réafficher le mot de passe
- Force le changement du mot de passe
- Fonctionne aussi en mode déconnecté

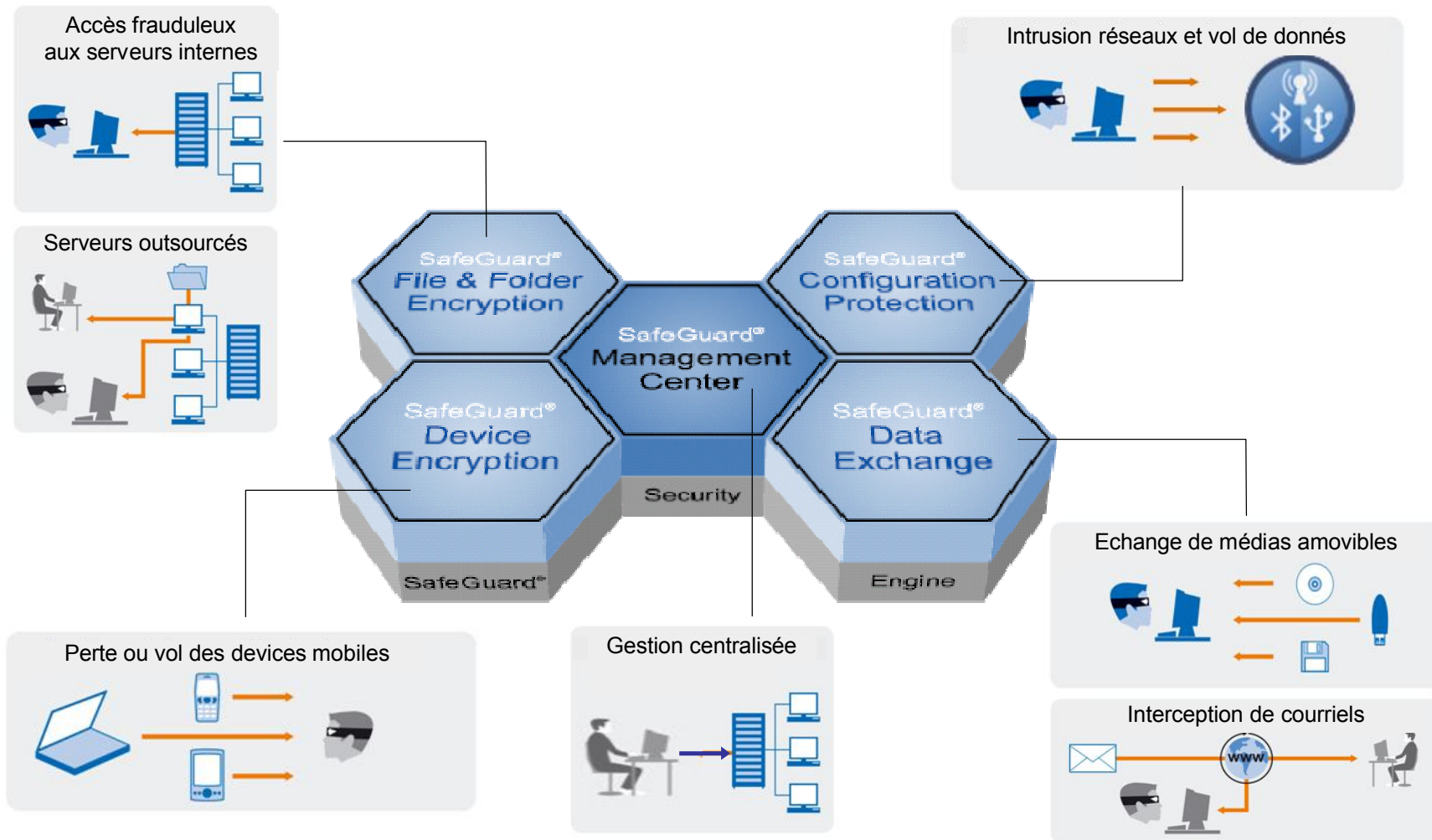
POA et Logon : plusieurs modes ...

- ▶ Username et Password
- ▶ Non-crypto Token (contenant les secrets)
- ▶ Crypto Token sans Kerberos (certificate au POA, username /password au WinLogon)
- ▶ Crypto Token avec Kerberos



SafeGuard Enterprise

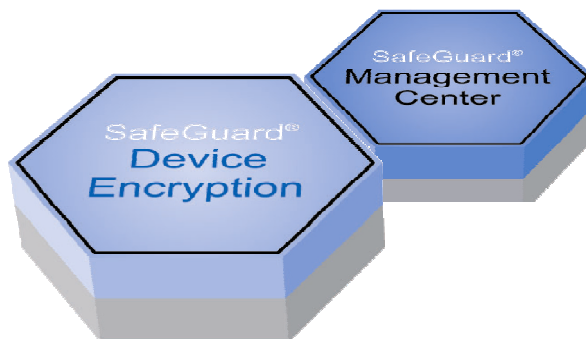
New Generation Data Security Suite



La protection globale de vos données

Protection contre le vol ou la perte

Assistants Personnel

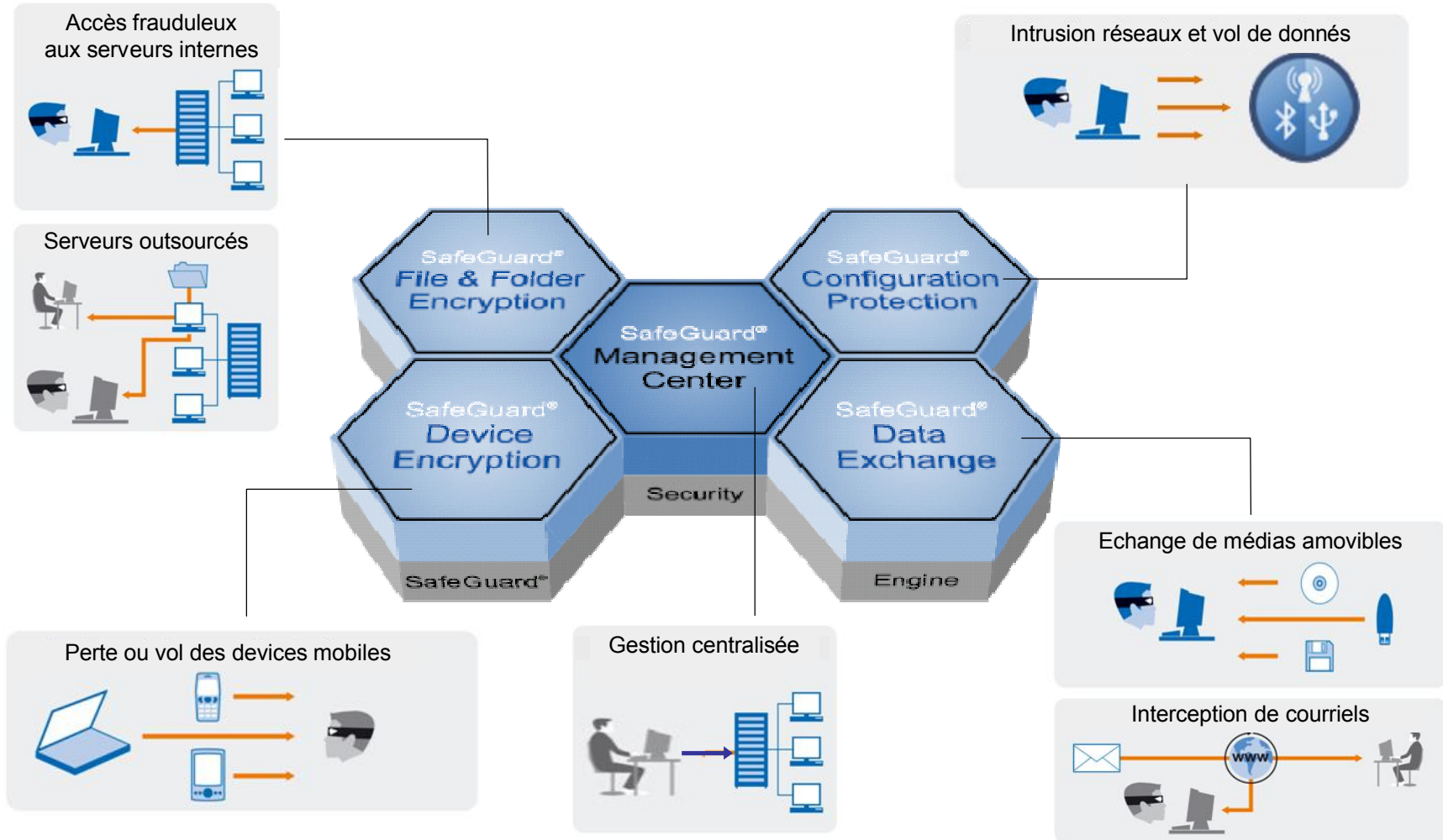


▶ SafeGuard PDA

- ◆ Chiffrement des données
 - Données PIM (tâches, agenda, mails, contacts)
 - Chiffrement des pièces jointes des mails
 - Module de chiffrement embarqué : PrivateCrypto PrivateDisk
- ◆ Authentification renforcée
 - Signature biométrique
 - Numérique, symbolique ou mot de passe
 - Fingerprint ou X509
- ◆ Windows Mobile, Palm, Symbian

SafeGuard Enterprise

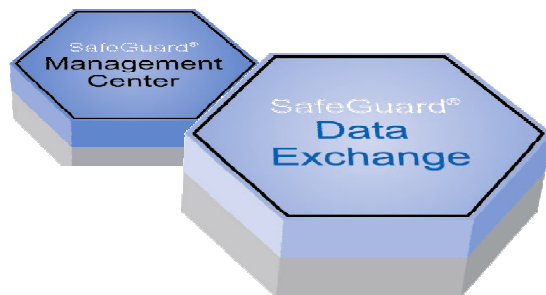
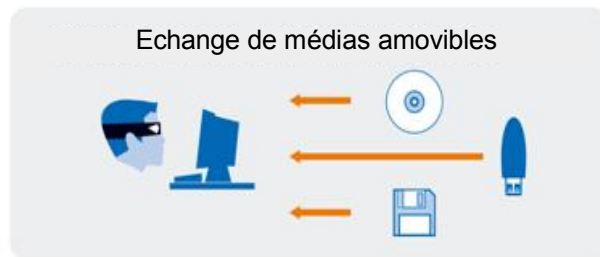
New Generation Data Security Suite



La protection globale de vos données

Echanges sécurisés des données

Supports amovibles



▶ SafeGuard Removable Media

◆ Chiffrement des données

- Chiffrement fort (AES) des fichiers / volume
- Chiffrement partagés ou personnel
 - Certificats (groupe ou utilisateur)
 - Pass-phrase
- Application d'une politique en toute transparence pour l'utilisateur
 - Chiffrement des données existantes
 - Autorisation d'accès aux fichiers non chiffrés
 - Chiffrement des nouveaux fichiers

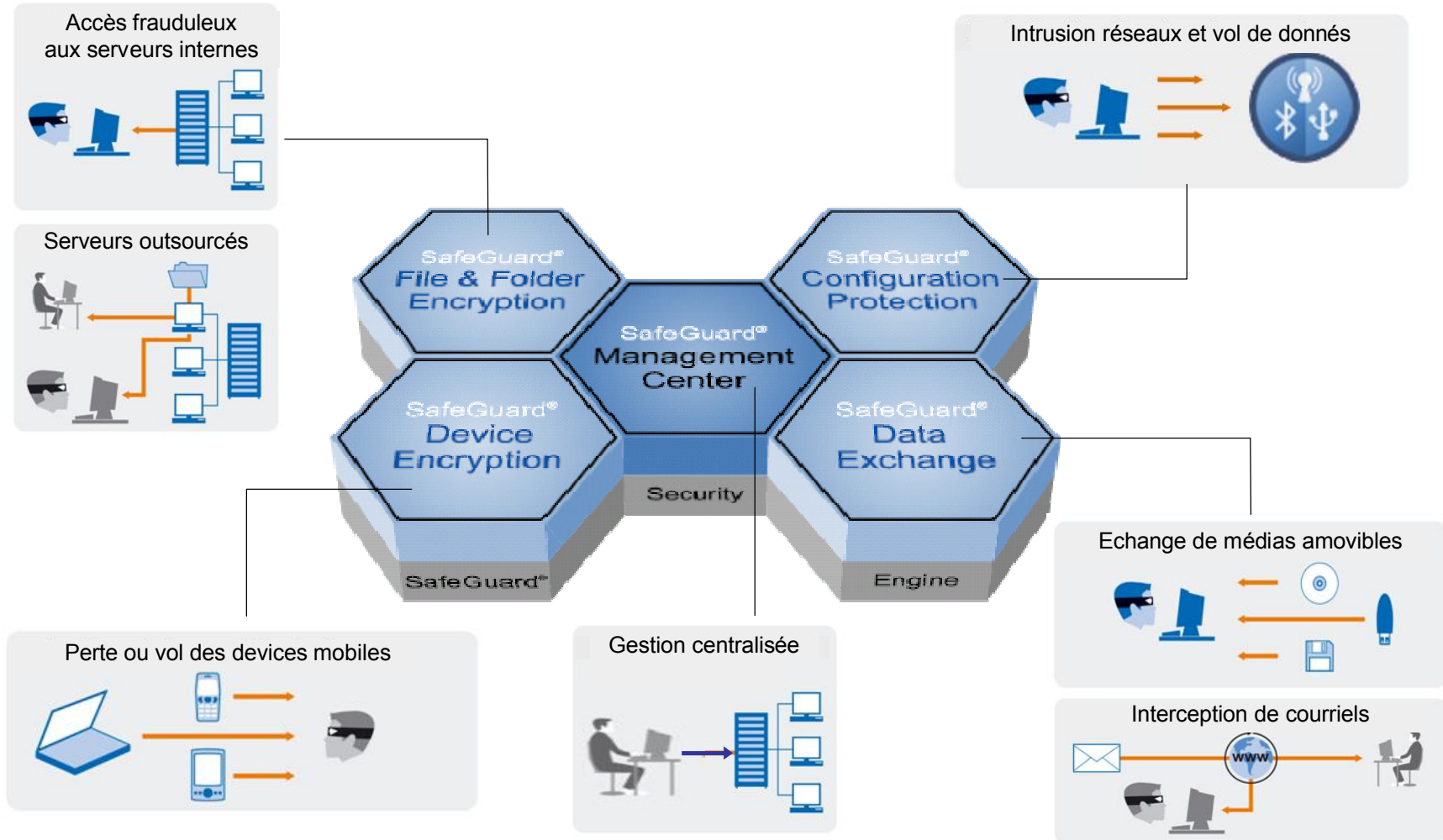
◆ Déchiffrement

- Sur le poste des utilisateurs Safeguard
- Poste banalisé (SG Portable.Exe)

◆ Support des disques optiques

SafeGuard Enterprise

New Generation Data Security Suite



La protection globale de vos données

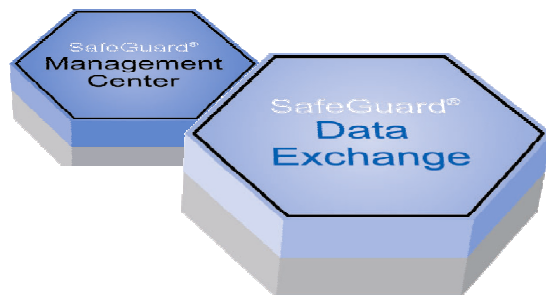
Echanges sécurisés des données

Courriers électroniques



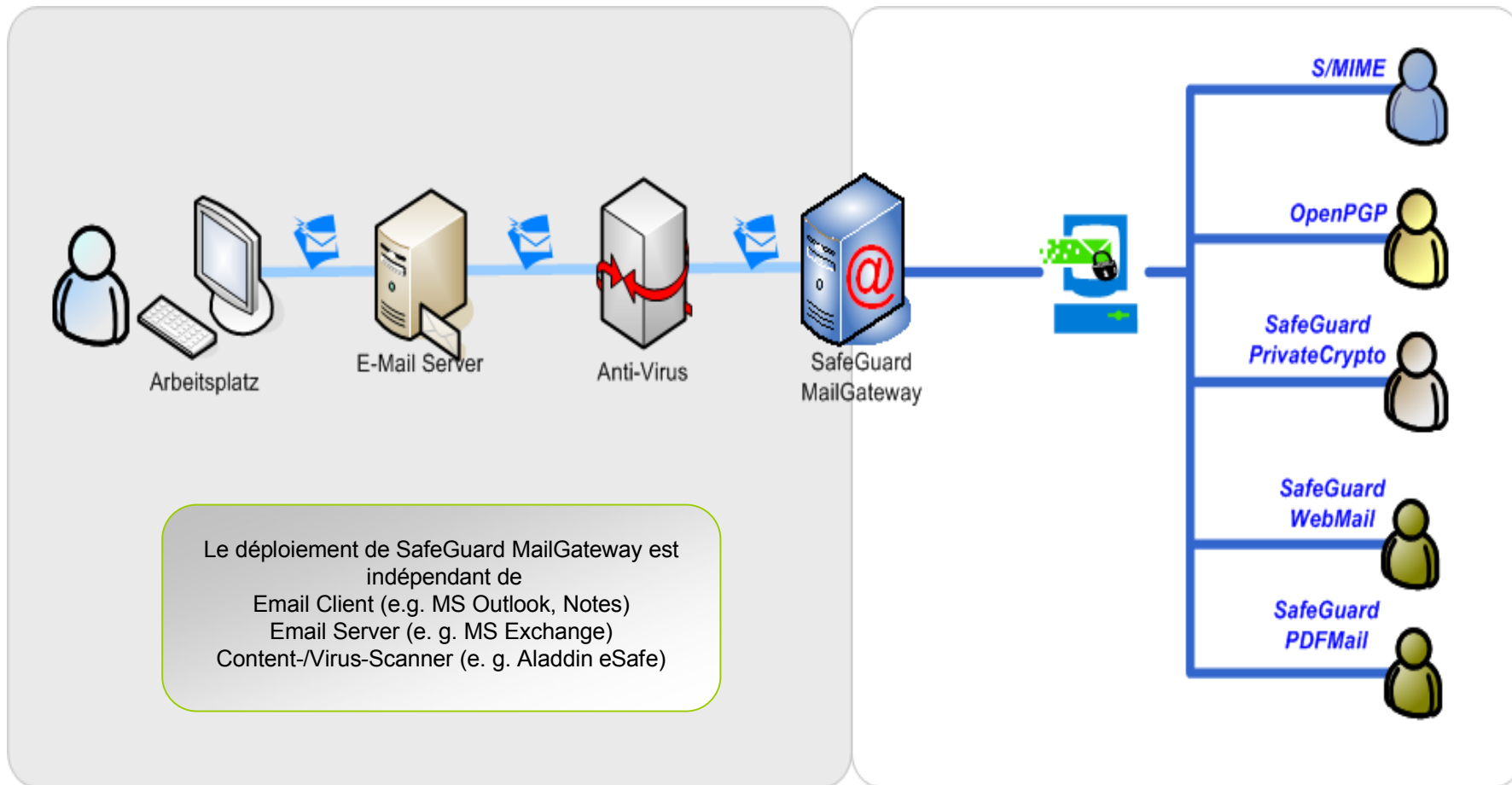
► SafeGuard Secure Mail Gateway

- ◆ Appliance proxy SMTP
- ◆ Chiffrement des mails
 - S/Mime
 - PGP
 - Private Crypto
 - PDF chiffrés
 - Web mail SSL
- ◆ Référenciel de certificats



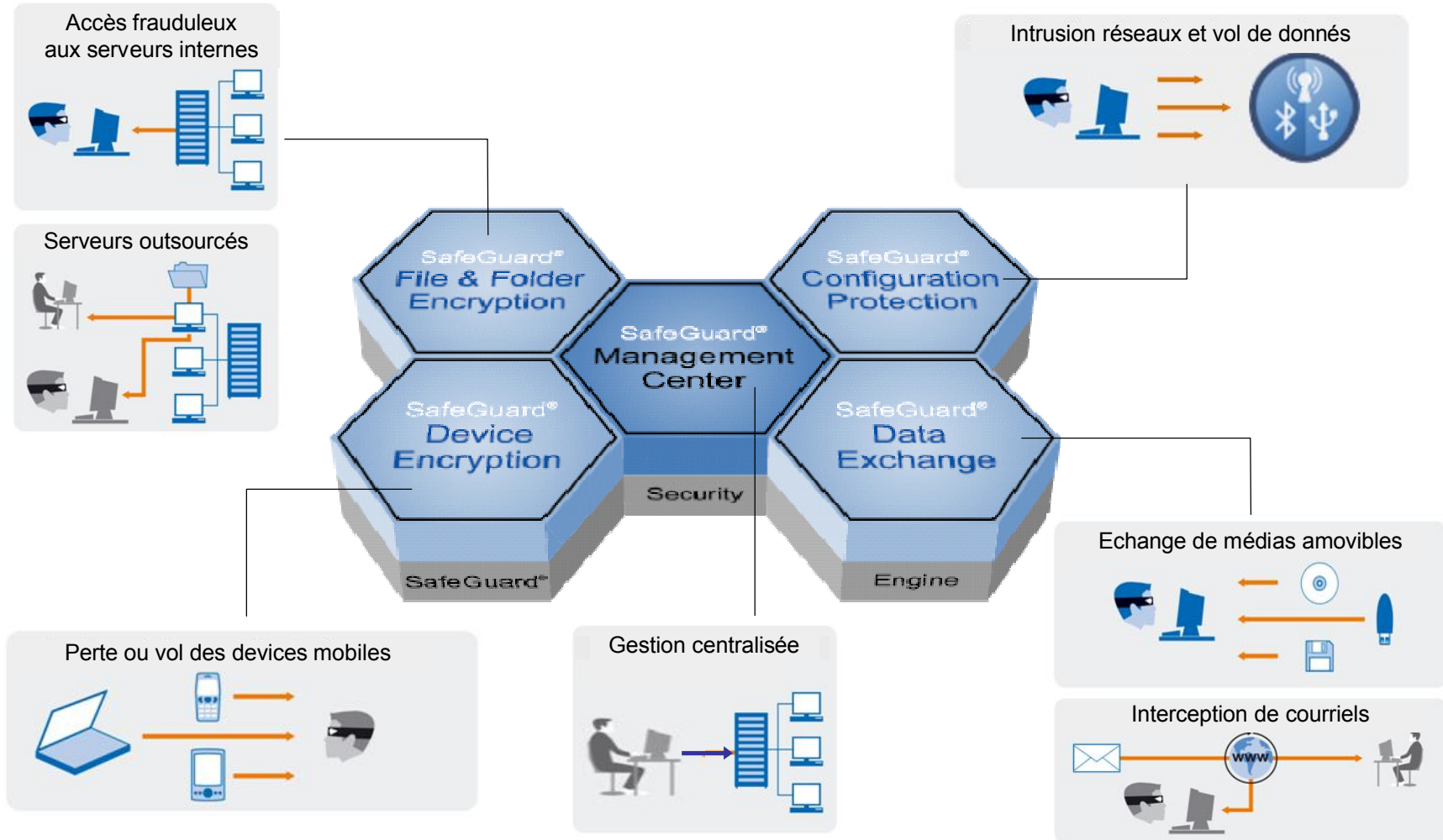
Echanges sécurisés des données

Courriers électroniques



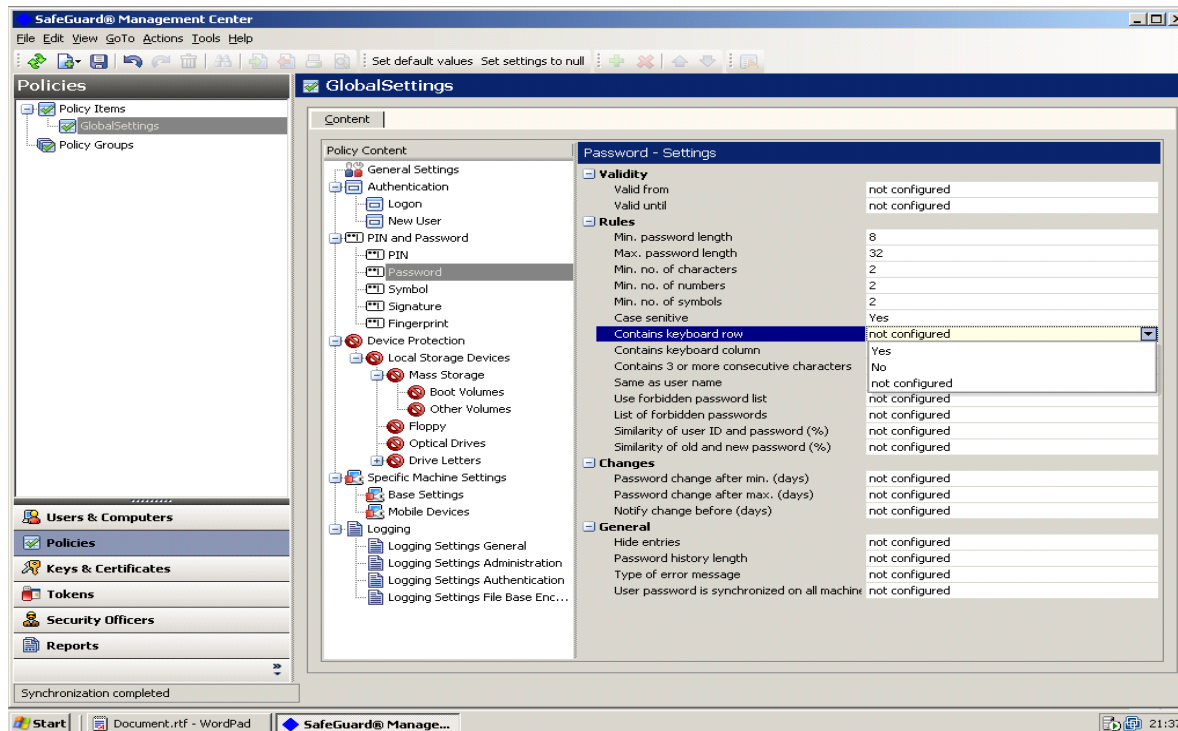
SafeGuard Enterprise

New Generation Data Security Suite

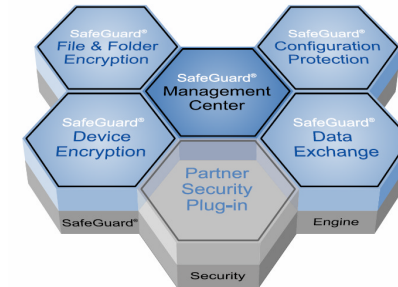


La protection globale de vos données

SafeGuard Management Center



SafeGuard® Enterprise



Points forts:

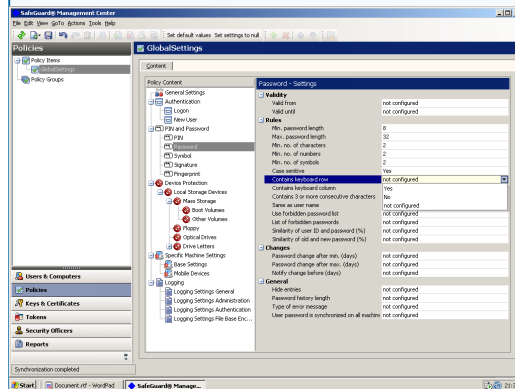
- Définition de la politique de sécurité uniforme pour toutes les plateformes
- Reporting et audit

Confortable, optimise le coût, administration centrale pour forcer la politique de sécurité

SafeGuard Management Center

Highlights

- Puissante administration, cross-plateforme
- Support Active Directory
- Reporting complet et conviviale



- ▶ Console centrale de management
 - ◆ Gestion avancée des clés, incl. Support des certificats et recouvrement
 - ◆ Officiers de sécurité (rôles, hiérarchique)
 - ◆ Evolutif
- ▶ Administration centralisée des politiques
 - ◆ Définition hiérarchique des politiques (héritage des politiques, calcul RSOP)
 - ◆ Politiques pour groupes d'utilisateurs et/ou de machines
 - ◆ Distribution automatisée des politiques multiplateformes (SOAP)
- ▶ Support des infrastructures existantes
 - ◆ Active Directory
 - ◆ PKI
- ▶ Reporting et monitoring Centralisé

SG Management Center

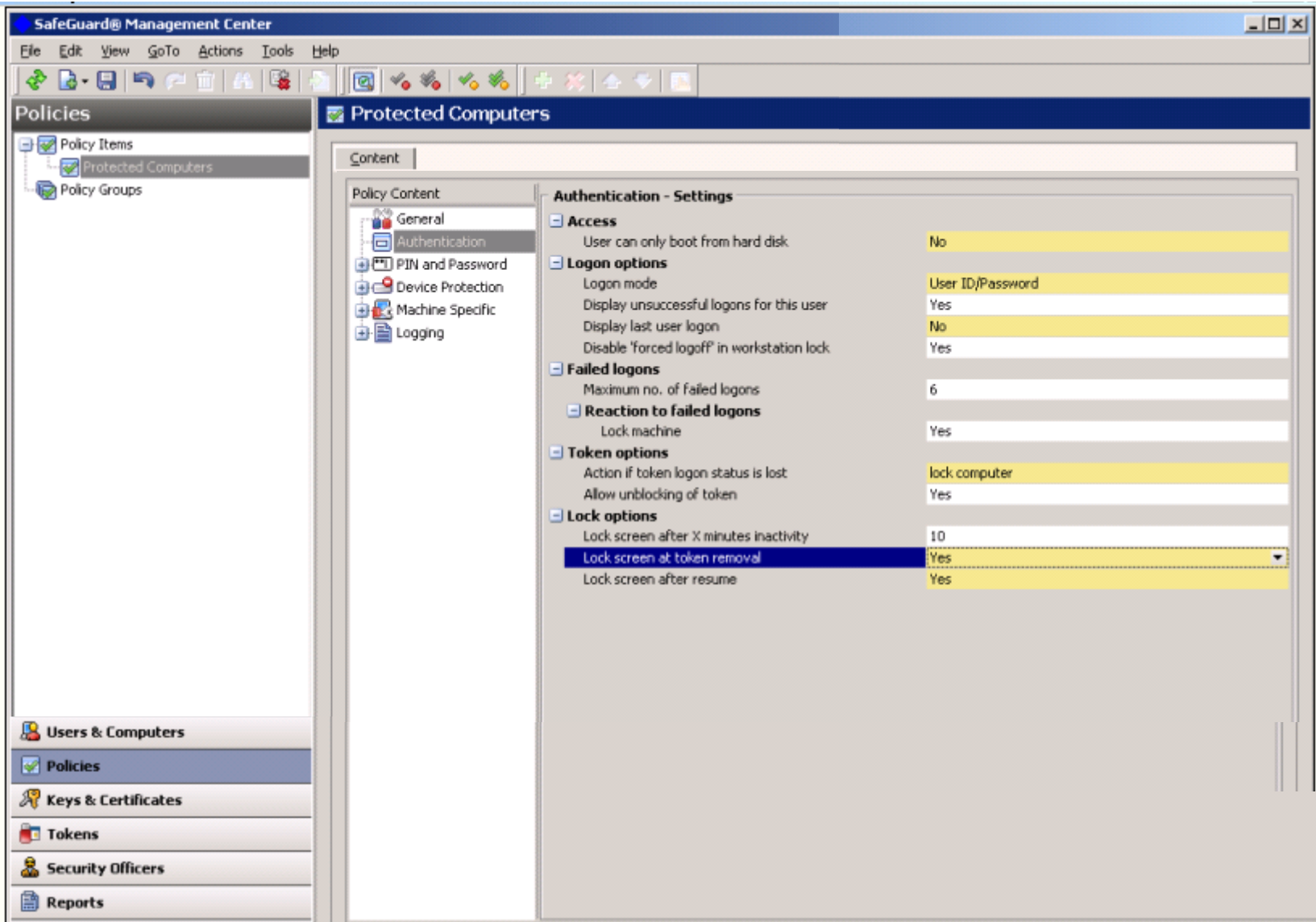
P

The screenshot displays the 'SafeGuard@ Management Center' application window. The interface is divided into several sections:

- Left Panel (Policies):** A tree view showing 'Policy Items' (Protected Computers, Policy Groups) and a bottom navigation bar with 'Users & Computers', 'Policies', 'Keys & Certificates', 'Tokens', 'Security Officers', and 'Reports'.
- Top Panel (Protected Computers):** A tabbed interface with a 'Content' tab selected.
- Policy Content:** A tree view on the left of the main pane showing categories like 'General', 'Authentication', 'PIN and Password', 'Device Protection', 'Local Storage D...', 'Mass Storage', 'Boot Vol...', 'Other V...', 'Floppy', 'Optical Drives', 'Drive Letters', 'Machine Specific', and 'Logging'.
- General - Settings:** A list of configuration options on the right, including:
 - Power On Authentication (POA):** Enable Power On Authentication (Yes), Number of auto logons (0, 10), Access denied if no connection to server (days) (0=no check), Only current POA user can logon (Yes), Only assigned user can logon (No), Creation of new users allowed for (Owner).
 - Display options:** Display machine identification (Yes), Display legal notice (Yes), Legal notice, Display additional information (File ID), Show for (sec.) (5).
 - Cryptographic basic infrastructure framework settings:** Windows cryptographic toolkits (not configured), Additional windows toolkit (not configured), POA cryptographic toolkits (SafeGuard Cryptograp...), Additional POA toolkit (not configured), Advanced framework settings (not configured).
 - Cryptographic toolkit settings - SafeGuard:** Advanced settings (not configured).
 - Cryptographic toolkit settings - Certicom:** Advanced settings (not configured).
 - Cryptographic toolkit settings - MS Crypto API:** MS Crypto API Default CSP (not configured), MS Crypto API Token CSP (not configured), Strong private key protection (not configured), Advanced settings (not configured).
 - Cryptographic toolkit settings - AET:** Advanced settings (not configured).
 - Token support settings PKCS#11 settings module 1:** Windows name (not configured), POA name (not configured), Secure communication (Yes), Advanced settings (not configured).

SG Management Center

P



The screenshot shows the 'Protected Computers' configuration window in the SafeGuard Management Center. The left sidebar contains a tree view with 'Protected Computers' selected. The main area is titled 'Protected Computers' and shows 'Authentication - Settings'.

| Setting | Value |
|---|------------------|
| Access | |
| User can only boot from hard disk | No |
| Logon options | |
| Logon mode | User ID/Password |
| Display unsuccessful logons for this user | Yes |
| Display last user logon | No |
| Disable 'forced logoff' in workstation lock | Yes |
| Failed logons | |
| Maximum no. of failed logons | 6 |
| Reaction to failed logons | |
| Lock machine | Yes |
| Token options | |
| Action if token logon status is lost | lock computer |
| Allow unblocking of token | Yes |
| Lock options | |
| Lock screen after X minutes inactivity | 10 |
| Lock screen at token removal | Yes |
| Lock screen after resume | Yes |

SG Management Center

C SafeGuard® Management Center

File Edit View GoTo Actions Tools Help

Machine: Desktop3 Calculate

| Policy Name | Assigned to object | Object path | In... |
|------------------------|--------------------|---|-------|
| Global Security Policy | UTIMACO.COM | DC=Utlimaco,DC=com | 1 |
| FBEUsingGroupKeyBoard | UTIMACO.COM | DC=Utlimaco,DC=com | 2 |
| UserCanSelectKeyforFBE | Finance | OU=Finance,OU=Headquarter,DC=Utlimac... | 3 |

Policy Content

- General
- Authentication
- PIN and Password
- Device Protection
 - Local Storage D...
 - Mass Storage
 - Floppy
 - Optical Drives
 - Drive Letters
- Machine Specific
- Logging

Optical Drives - Settings

| Setting | Value |
|---|--------------------|
| Media encryption mode | File based |
| Common settings | |
| Algorithm to be used for encryption | AES256 |
| Key to be used for encryption | All keys in key... |
| CPU minimum value (%) | not configured |
| CPU maximum value (%) | not configured |
| File based settings | |
| Initial encryption of all files | Yes |
| User can cancel initial encryption | not configured |
| User is allowed to access unencrypted files | No |
| User can decrypt files | Yes |

Available Computers

- Root [Filter is active]
 - .Unknown Computers
 - UTIMACO.COM
 - Headquarter
 - Development
 - Finance
 - Desktop3
 - Desktop4
 - Management
 - Marketing
 - Production Site
 - Desktop6
 - Desktop7

Socle de sécurité

Key Advantages

- Architecture moderne et éprouvée
- Compatibilité Cross-plateforme
- Rajout de nombreuses cartes prévu

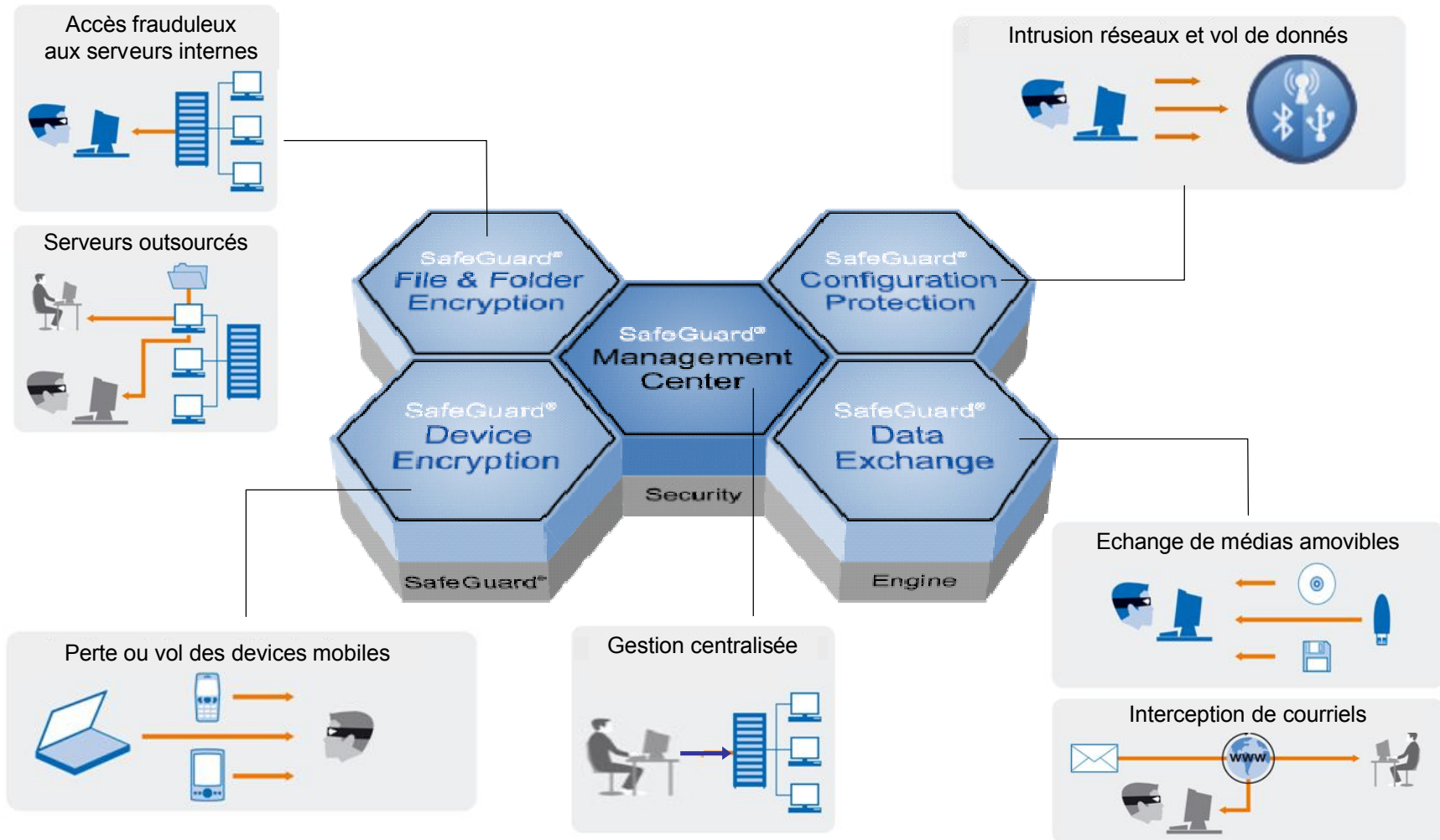


- ▶ Socle cryptographique de sécurité
 - ◆ Interfaces standards évolutives pour ajout de nouveaux algorithmes
 - ◆ Support intégré des certificats X.509
- ▶ Support de HW intégré (cartes à puce, tokens, TPM, etc.)
 - ◆ Support cartes Java: Gemalto, G+D, Oberthur, Orga, IBM, ...
 - ◆ Support cartes ISO: Gemalto, Siemens, G+D, ...
 - ◆ USB tokens: Aladdin, RSA, ActivIdentity
 - ◆ Lecteurs de cartes: Omnikey, SCM, Gemalto, Kobil, ...



SafeGuard Enterprise

New Generation Data Security Suite



La protection globale de vos données

Contrôle des postes

▶ Visibilité – SafeGuard PortAuditor



- ♦ Repérer les devices connectés et les réseaux Wifi de chaque poste
- ♦ Identifier les vulnérabilités des postes de travail

| Category | Total | Connected |
|--------------------------|-------|-----------|
| Total Computers | 17 | 2 |
| Account Computers | 2 | 2 |
| Successfully Audited | 2 | 2 |
| Protected by Software | 0 | 0 |
| USB Devices | 183 | 1 |
| IEEE1394a Devices | 5 | 0 |
| Firewire Devices | 0 | 0 |
| Internal Storage Devices | 0 | 0 |
| WiFi Networks | 0 | 0 |
| Storage Devices | 68 | 0 |
| Communication Adapters | 7 | 0 |

| Computer | Name | Connection Type | Device Type | Manufacturer / Model | Serial No. | Vendor | Model |
|----------|----------|-----------------|-------------|-----------------------------|------------------|--------|-------|
| 1 | SAF02200 | USB | Device | USB Device Interface Device | 0000000000000000 | MSI | MSI |
| 1 | SAF02200 | USB | Storage | PCCEM0000000000000000 | 0000000000000000 | UMC | AC66 |
| 1 | SAF02200 | USB | Storage | PCCEM0000000000000000 | 0000000000000000 | UMC | 9550 |
| 1 | SAF02200 | USB | Storage | PCCEM0000000000000000 | 0000000000000000 | UMC | 9550 |

▶ Contrôle – SafeGuard PortProtector



- ♦ Contrôler quels ports et périphériques sont utilisés, par quelle population, et à quel moment
- ♦ Eviter la fuite d'information et les intrusions via les postes
- ♦ Renforce les politiques de sécurité applicables sur les ports physiques et sans fil ainsi que les médias amovibles
- ♦ Permet une conformité avec les législations et réglementations en vigueur

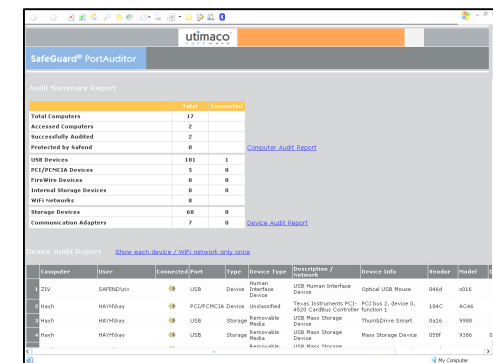
| Policy | Device Type | Action | Log Alert |
|--------------------------------|-------------|-----------------------|--------------------------|
| Device Control | USB | Define Device Control | <input type="checkbox"/> |
| | Firewire | Define Device Control | <input type="checkbox"/> |
| Storage Control | Storage | Define Device Control | <input type="checkbox"/> |
| | Network | Define Device Control | <input type="checkbox"/> |
| WiFi Control | WiFi | Define Device Control | <input type="checkbox"/> |
| | Serial | Define Device Control | <input type="checkbox"/> |
| Network Control | Bluetooth | Define Device Control | <input type="checkbox"/> |
| | WiFi | Define Device Control | <input type="checkbox"/> |
| Auto-Installed Network Bridges | WiFi | Define Device Control | <input type="checkbox"/> |
| | Bluetooth | Define Device Control | <input type="checkbox"/> |
| Hybrid Network Bridges | WiFi | Define Device Control | <input type="checkbox"/> |
| | Bluetooth | Define Device Control | <input type="checkbox"/> |



SafeGuard® PortAuditor



- ▶ Identifier et manager les vulnérabilités des postes
 - ◆ Identifie tous les dispositifs USB, FireWire, PCMCIA et WiFi
 - ◆ Fournit la liste des dispositifs connectés ou ayant été connectés
 - ◆ Présente le résultat en quelques minutes dans une interface simple et performante
 - ◆ Compatible avec les outils d'administration ou de gestion des réseaux existants.
 - ◆ Intuitif, sans installation de client, facile à utiliser

Audit Summary Report

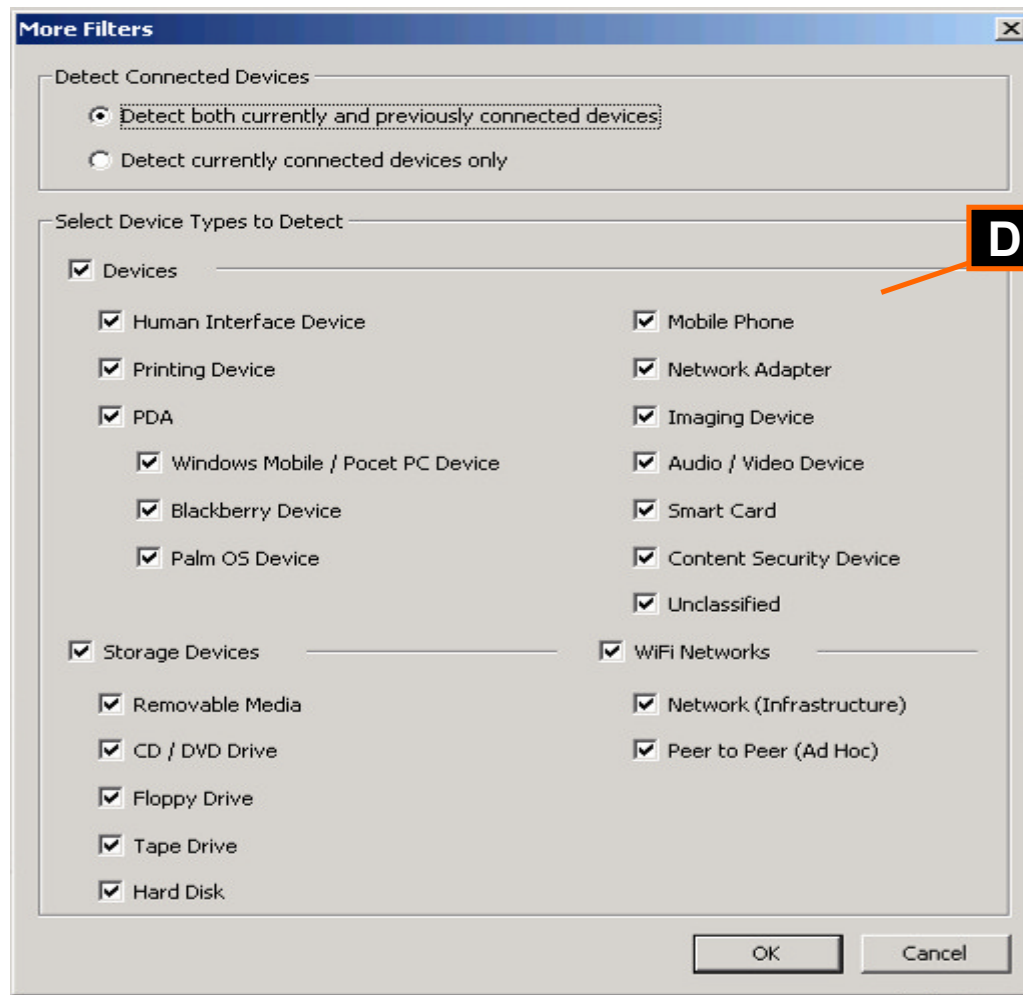
| | Total | Connected |
|--------------------------|-------|-----------|
| Total Computers | 17 | |
| Accessed Computers | 2 | |
| Successfully Audited | 2 | |
| Restricted by Software | 0 | |
| USB Devices | 101 | 1 |
| PC/PCMCIA Devices | 5 | 0 |
| FireWire Devices | 0 | 0 |
| Internal Storage Devices | 0 | 0 |
| WiFi Networks | 0 | 0 |
| Storage Devices | 60 | 0 |
| Communication Adapters | 7 | 0 |

[Computer Audit Report](#)

Device Audit Report [Show each device / WiFi network only once](#)

| Computer | User | Connected/Port | Type | Device Type | Description / Interface | Device Info | Vendor | Model |
|----------|---------|----------------|-----------|-------------|---------------------------------------|------------------------|--------|-------|
| EVU | SAFEDGU | 08 | USB | Device | USB Human Interface Device | epson USB Mouse | 0465 | 0514 |
| Hash | HAYHOU | 08 | PC/PCMCIA | Device | Texas Instruments PCI-1020-2-Device 0 | ESAC | AC04 | |
| Hash | HAYHOU | 08 | USB | Storage | ATI Cariboo Controller Function 1 | USB Mass Storage | 0435 | 3100 |
| Hash | HAYHOU | 08 | USB | Storage | SanDisk | ThumbDrive Smart Drive | 0435 | 3100 |
| ... | ... | ... | ... | ... | ... | ... | ... | ... |

1b. Précisions éventuelles du spectre



Dispositifs à détecter

2. Rapport d'audit



Résumé de Connexion

| | Total | Connected |
|---------------------------------|-------|-----------|
| Total Computers | 17 | |
| Accessed Computers | 2 | |
| Successfully Audited | 2 | |
| Protected by Safend | 0 | |
| USB Devices | 101 | 1 |
| PCI/PCMCIA Devices | 5 | 0 |
| FireWire Devices | 0 | 0 |
| Internal Storage Devices | 0 | 0 |
| WiFi Networks | 8 | |
| Storage Devices | 60 | 0 |
| Communication Adapters | 7 | 0 |

[Computer Audit Report](#)

[Device Audit Report](#)

Détail des dispositifs

| | Computer | User | Connected | Port | Type | Device Type | Description / Network | Device Info | Vendor | Model |
|---|----------|------------|-----------|------------|---------|------------------------|---|---------------------------------|--------|-------|
| 1 | ZIV | SAFEND\ziv | | USB | Device | Human Interface Device | USB Human Interface Device | Optical USB Mouse | 046d | c016 |
| 2 | Hayh | HAYH\hay | | PCI/PCMCIA | Device | Unclassified | Texas Instruments PCI-4520 CardBus Controller | PCI bus 2, device 0, function 1 | 104C | AC46 |
| 3 | Hayh | HAYH\hay | | USB | Storage | Removable Media | USB Mass Storage Device | ThumbDrive Smart | 0a16 | 9988 |
| 4 | Hayh | HAYH\hay | | USB | Storage | Removable Media | USB Mass Storage Device | Mass Storage Device | 058f | 9386 |

3. Rapport d'audit détaillé

Historique

Temps réel

“ Liste Blanche ”

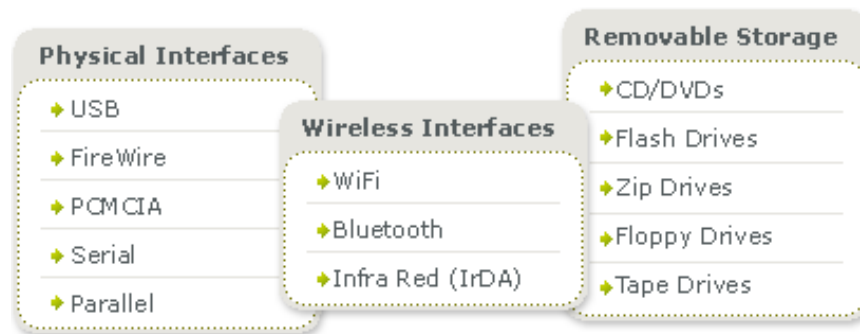
Device Audit Report

| | Computer | User | State | Port | Type | Description | Device In | Vendor | Model | Distinct ID |
|----|----------|-----------|-------|------|---------|-----------------------------------|---|--------|-------|------------------|
| 1 | local | DOR\dor s | | USB | Adapter | ATMEL USB FastVNET (AR) | USB Device | 03eb | 7603 | |
| 2 | local | DOR\dor s | | USB | Storage | Hewlett-Packard Digital Camera | hp photosmart 735 | 03f0 | 4002 | |
| 3 | local | DOR\dor s | | USB | Device | USB Printing Support | Deskjet 6500 | 03f0 | 8204 | MY4893R19D040J |
| 4 | local | DOR\dor s | | USB | Device | USB Printing Support | Deskjet 6500 | 03f0 | 8204 | MY4893R19D040J-F |
| 5 | local | DOR\dor s | | USB | Device | USB Device | USB Device | 040a | 0002 | |
| 6 | local | DOR\dor s | | USB | Device | Microsoft USB Wheel Mouse Optical | Microsoft 3-Button Mouse with IntelliEye (TM) | 045e | 0040 | |
| 7 | local | DOR\dor s | | USB | Device | USB Human Interface Device | USB-PS/2 Optical Mouse | 046d | c03d | |
| 8 | local | DOR\dor s | | USB | Device | USB Human Interface Device | USB-PS/2 Optical Mouse | 046d | c03d | |
| 9 | local | DOR\dor s | | USB | Device | USB Human Interface Device | Combo Mouse | 04b4 | aef8 | |
| 10 | local | DOR\dor s | | USB | Device | USB Human Interface Device | USB Wheel Mouse | 04fc | 0003 | |
| 11 | local | DOR\dor s | | USB | Device | eToken R2 (2.4.4.x) | eToken R2 2442 | 0529 | 0422 | |
| 12 | local | DOR\dor s | | USB | Storage | USB Mass Storage Device | Mass Storage Device | 058f | 9380 | |
| 13 | local | DOR\dor s | | USB | Storage | USB Mass Storage Device | Mass Storage Device | 058f | 9382 | |

SafeGuard® PortProtector



- ▶ Eviter la fuite d'information et les intrusions via les postes
 - ◆ Détecte et limite l'usage des dispositifs périphériques
 - ◆ Applique des politiques fines sur les connexions physiques, sans fil et de dispositifs de stockages par une analyse bas niveau et temps des ports
 - ◆ Impossible à contourner, désactiver ou désinstaller
 - ◆ Management centralisé et intégration transparente à Active Directory
 - ◆ Permet une conformité réglementaire par ses logs, alertes et rapports
 - ◆ Facile à utiliser et à étendre sur un large périmètre



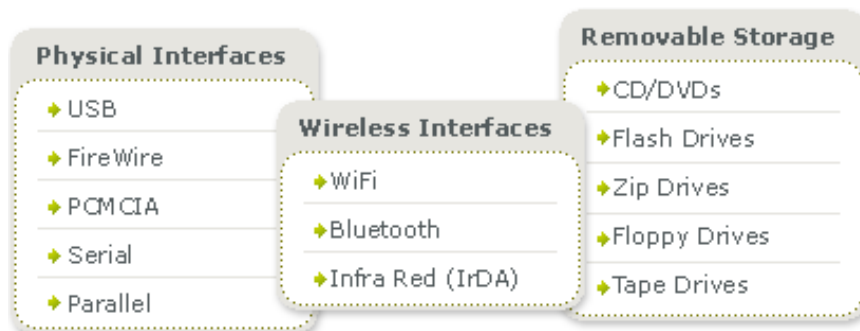
SafeGuard® PortProtector

Fonctionnalités



- ▶ Contrôle des Ports, Périphériques & Stockage
 - ◆ Accepte, bloque ou restreint l'utilisation des ports de certains ou tous les ordinateurs du parc
 - ◆ Identification et acceptation des périphériques

- ▶ Contrôle du Wifi
 - ◆ Par adresse MAC, SSID ou niveau de sécurité du réseau

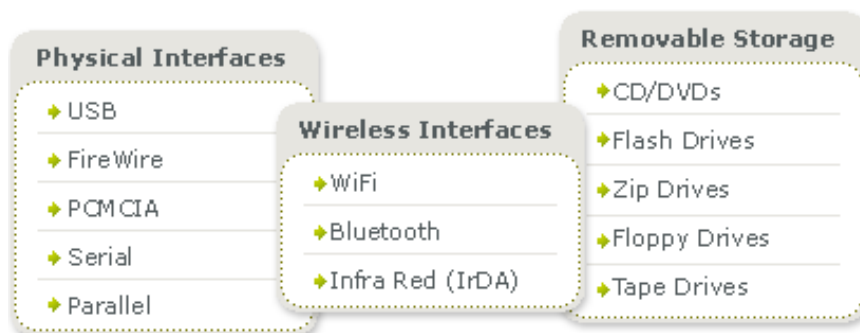


SafeGuard® PortProtector

Security Features



- ▶ Interdit le pontage de réseaux
 - ◆ Permet aux administrateurs de contrôler et de prévenir de l'utilisation simultanée de protocoles réseaux différents
- ▶ Contrôle des clés U3 & Autorun
 - ◆ Réduit l'usage des disques USB U3 à celui d'une simple clé USB lorsque connecté à un poste de l'organisation
 - ◆ Empêche l'utilisation de Keyloggers USB & PS/2



SafeGuard® PortProtector

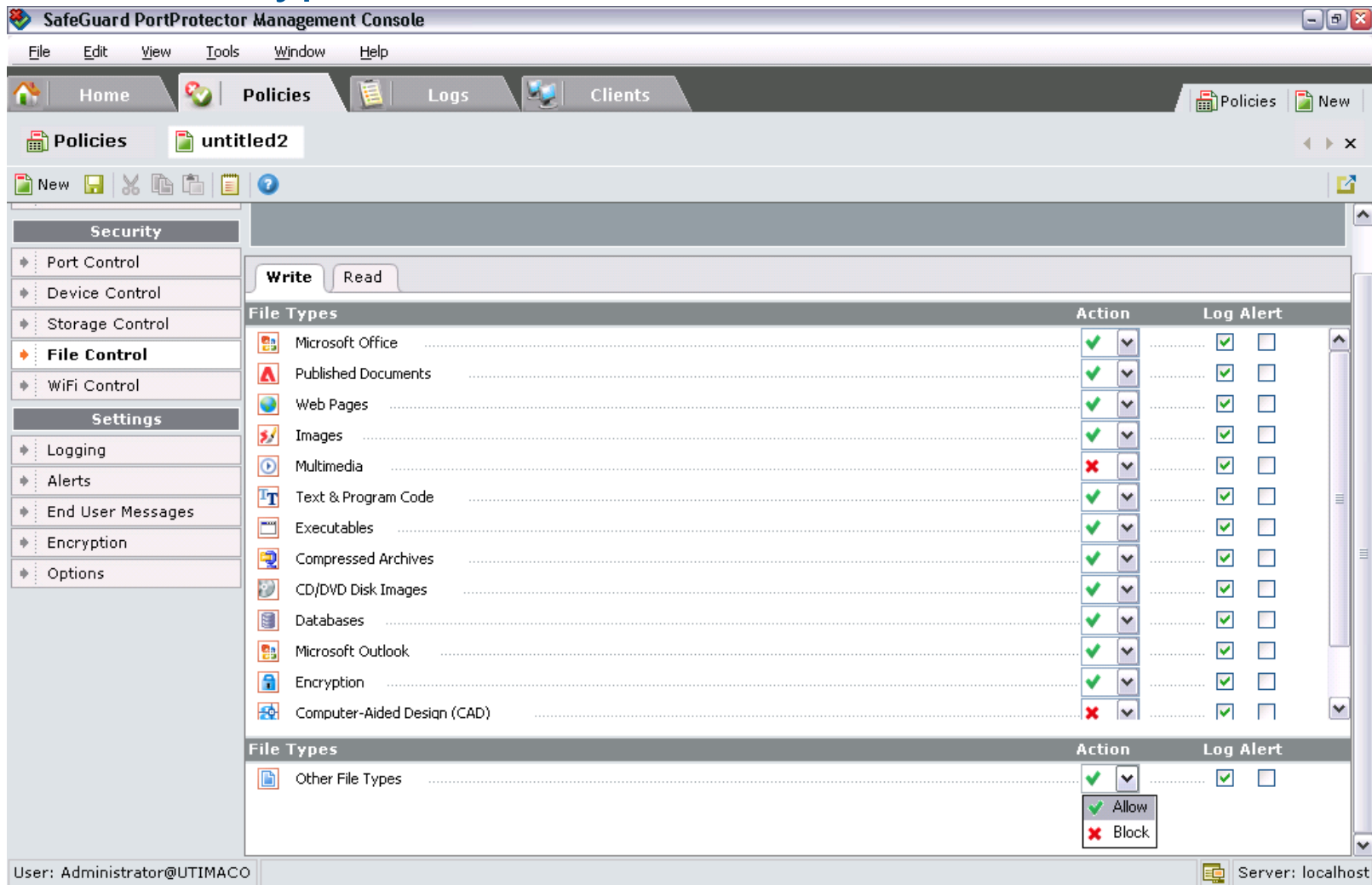
Contrôle du type de fichier

- ▶ Evite
 - ◆ Fuite d'information (Write)
 - ◆ Virus/Malware (Read)
 - ◆ Contenu inapproprié (Read)
- ▶ Classification par type de header
 - ◆ Pas par extension
 - ◆ 250 types de fichiers
 - ◆ 14 catégories
- ▶ Politique
 - ◆ White/Black List
 - ◆ Read/Write
- ▶ Log et Alertes par type de fichiers

| Category | Sample Extensions |
|--------------------------------|----------------------------------|
| Published Documents | PDF, PS |
| Images | JPG, JPES,GIF,BMP |
| Web Pages | HTML, HTM,MHT,HLP,CHM |
| Microsoft Office | DOC, DOCX, PPT, PPTX, XLS |
| Text & Program Code | TXT, CPP, C, H, GCC, JAVA |
| Multimedia | WAV, WMA, MP3, MPG, AVI |
| Compressed Archives | ZIP, ARJ, RAR, GZIP, JAR, CAB |
| CD/DVD Image Files | ISO, NRG |
| Executables | EXE, DLL, COM, OCX, SYS |
| PGP Encryption | PGP |
| Computer Aided Design (CAD) | DWG, DXF |
| Microsoft Outlook | PST, DBX |
| Databases | MDB, ACCDB |
| FrameMaker | MIF, BOOK, FM |

SafeGuard® PortProtector

Contrôle du type de fichier



The screenshot displays the 'SafeGuard PortProtector Management Console' interface. The 'Policies' tab is active, showing a configuration for 'untitled2'. The 'File Control' section is expanded, and the 'Write' tab is selected. A table lists various file types with their corresponding actions and log alert settings.

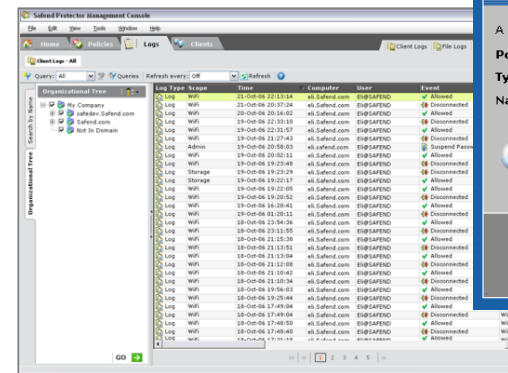
| File Types | Action | Log Alert |
|-----------------------------|--------------------|---|
| Microsoft Office | ✓ | ✓ |
| Published Documents | ✓ | ✓ |
| Web Pages | ✓ | ✓ |
| Images | ✓ | ✓ |
| Multimedia | ✗ | ✓ |
| Text & Program Code | ✓ | ✓ |
| Executables | ✓ | ✓ |
| Compressed Archives | ✓ | ✓ |
| CD/DVD Disk Images | ✓ | ✓ |
| Databases | ✓ | ✓ |
| Microsoft Outlook | ✓ | ✓ |
| Encryption | ✓ | ✓ |
| Computer-Aided Design (CAD) | ✗ | ✓ |
| Other File Types | ✓ Allow ✗ Block | <input checked="" type="checkbox"/> Log <input type="checkbox"/> Alert |

User: Administrator@UTIMACO Server: localhost

SafeGuard® PortProtector

Suivi de l'usage hors-ligne des médias de stockage

- ▶ Visibilité étendue au delà des frontières de l'entreprise
- ▶ Suivi des transferts de fichiers de/vers
 - ◆ Audit de l'utilisation légitime des données de l'entreprise
- ▶ Politique
 - ◆ Configuration globale - Read/Write
- ▶ Logs
 - ◆ Collectées à chaque connexion au réseau
 - ◆ Disponible dans les fichiers logs

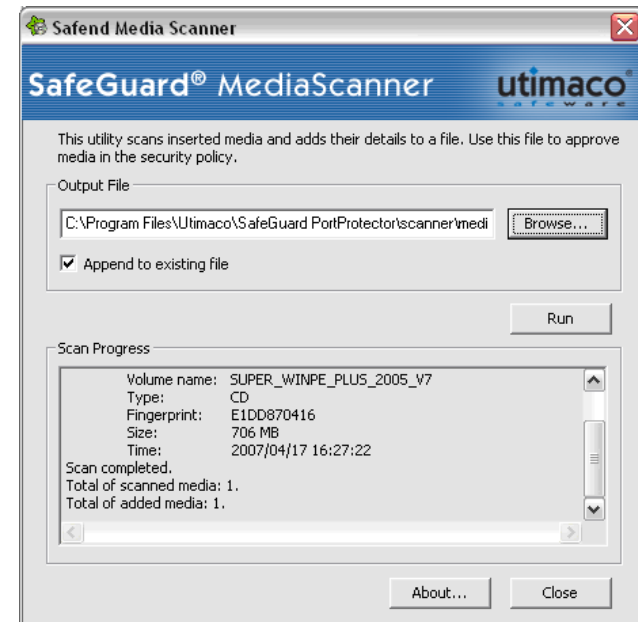


SafeGuard® PortProtector

Liste blanche de CD/DVD



- ▶ Permet la définition de listes de CD/DVD approuvés
 - ◆ CD d'installation de logiciels
 - ◆ Contenus approuvés
 - ◆ CD garantis sans virus
- ▶ Empreinte unique de CD/DVD
 - ◆ Identifie les données de chaque CD
 - ◆ Toute modification révoque l'empreinte
- ▶ Utilitaire de scan de médias
- ▶ Politique
 - ◆ Etend les listes blanches des devices
 - ◆ Exclusion automatique du contrôle sur type de fichiers



SafeGuard® PortProtector:

Caractéristiques du Management

- ▶ Console de management intuitive
 - ◆ Permet une gestion unifiée des politiques, logs et clients
- ▶ Logs et rapports
 - ◆ Visualisation et analyse des log collectées
 - ◆ Génération de rapport personnalisés
- ▶ Gestion des clients
 - ◆ Permet de gérer et de suivre le statut des clients
- ▶ Synchronisation Active Directory ou Novell eDirectory
 - ◆ Application des politiques sur les unités organisationnelles déjà établies
- ▶ Alertes en temps-réel
 - ◆ Destination au choix
- ▶ Suspension du client
 - ◆ Suspension temporaire du client sans désinstallation



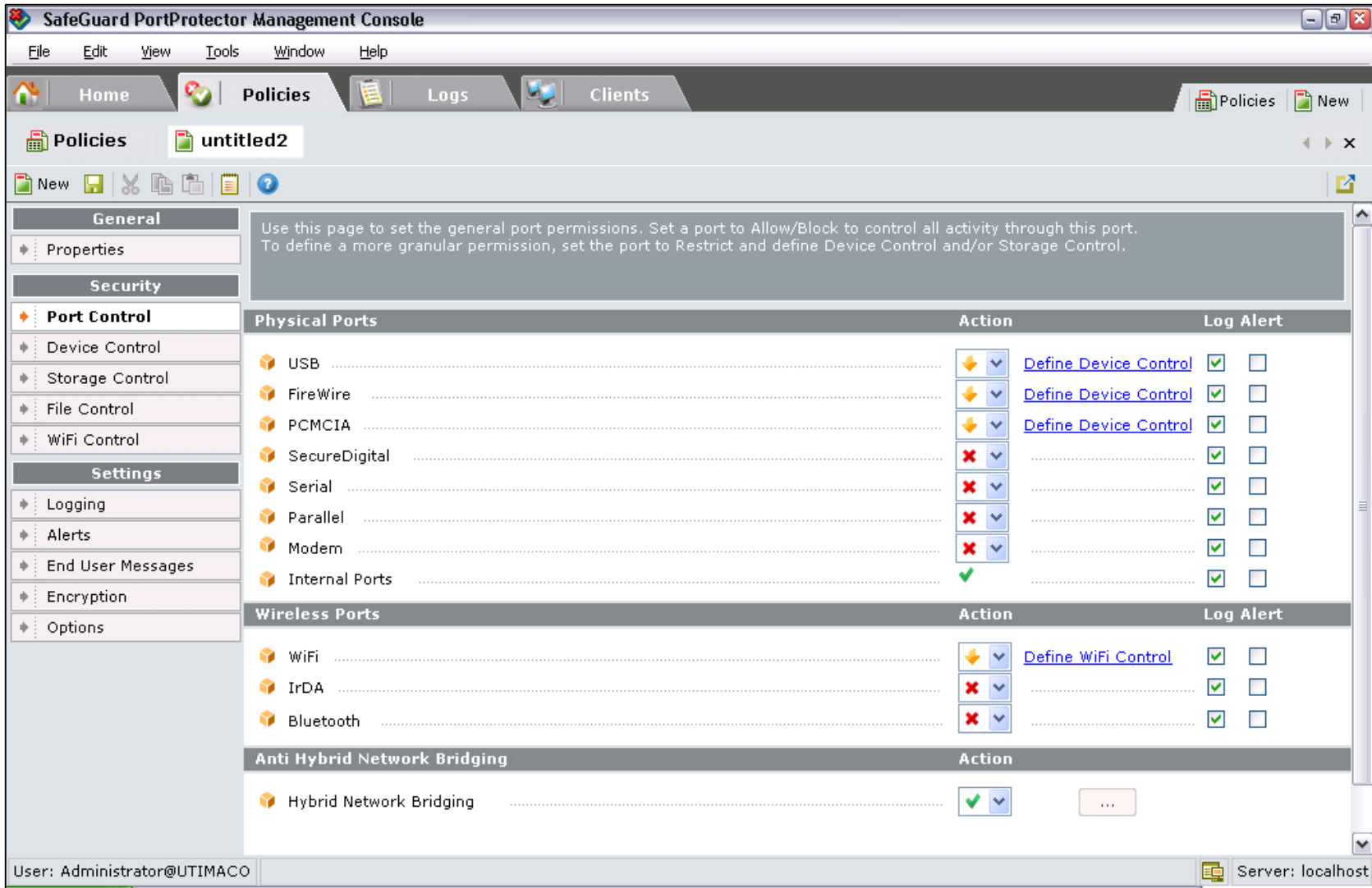
SafeGuard® PortProtector

Une solution unique

- ▶ Politiques flexibles et fortes
 - ◆ Politiques applicable selon domaines, groupes, ordinateurs ou utilisateurs
 - ◆ Logs temps réel (chiffrés) et alertes en cas d'infraction aux politiques
- ▶ Granulaire
 - ◆ Détecte et restreint tout device et port
- ▶ Gestion intuitive
 - ◆ Intégration transparente avec l'AD et autres outils de gestion du réseau
- ▶ Dynamique & souple
 - ◆ Bloque les Keyloggers & Autorun
 - ◆ Permet un contrôle profond du WiFi
- ▶ Sécurisée
 - ◆ Contrôle bas niveau de l'activité
 - ◆ Fortes mesures anti-altération
 - ◆ Déploiement silencieux



SafeGuard® PortProtector en Action



The screenshot displays the 'SafeGuard PortProtector Management Console' window. The interface includes a menu bar (File, Edit, View, Tools, Window, Help) and a navigation pane with tabs for Home, Policies, Logs, and Clients. The 'Policies' tab is active, showing a document titled 'untitled2'. A left-hand sidebar contains sections for General, Security, Port Control, Device Control, Storage Control, File Control, WiFi Control, Settings, Logging, Alerts, End User Messages, Encryption, and Options. The main content area is titled 'Use this page to set the general port permissions...' and contains three tables for configuring port permissions.

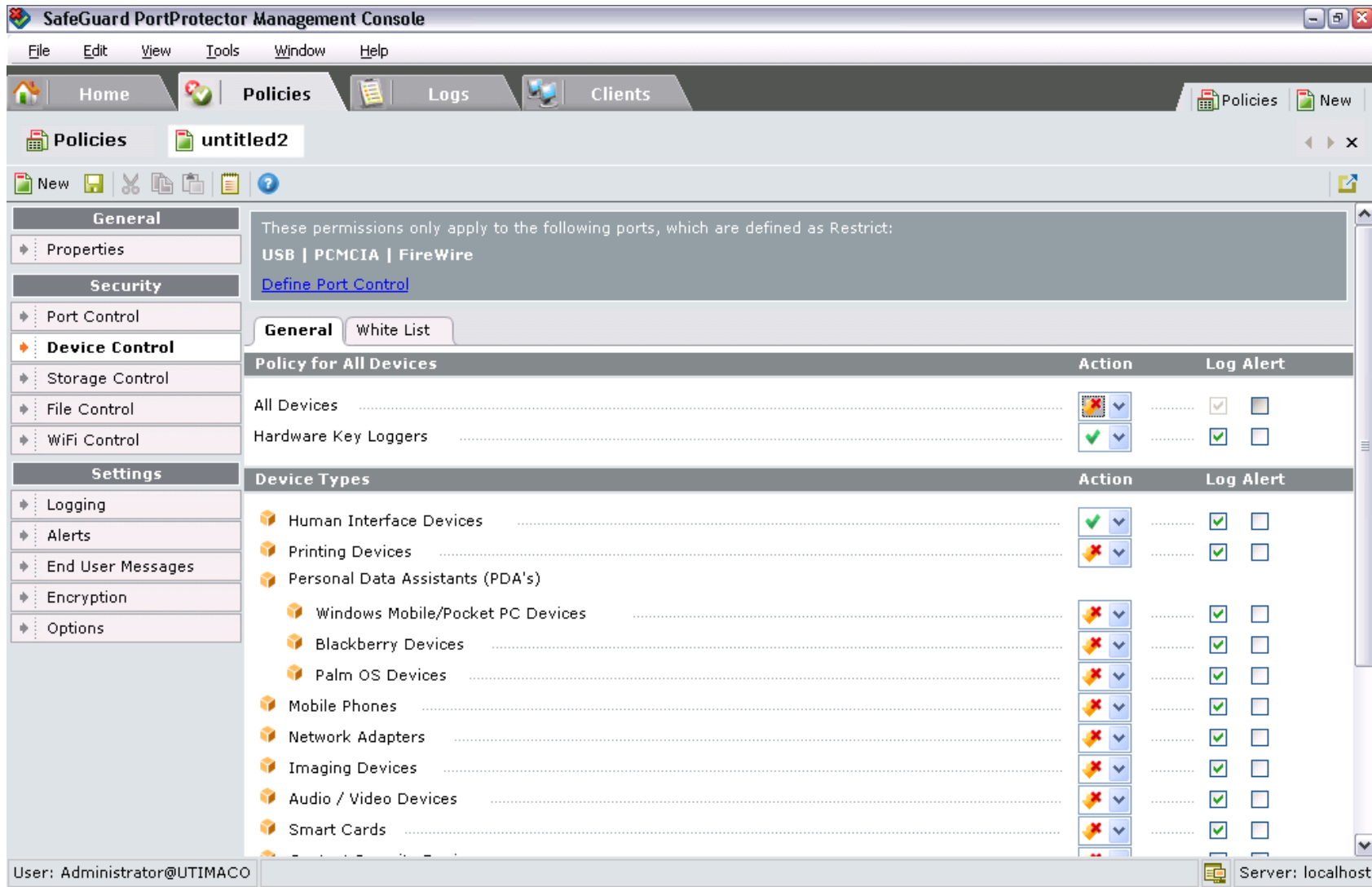
| Physical Ports | Action | Log Alert |
|----------------|-----------------------|--|
| USB | Define Device Control | <input checked="" type="checkbox"/> <input type="checkbox"/> |
| FireWire | Define Device Control | <input checked="" type="checkbox"/> <input type="checkbox"/> |
| PCMCIA | Define Device Control | <input checked="" type="checkbox"/> <input type="checkbox"/> |
| SecureDigital | | <input checked="" type="checkbox"/> <input type="checkbox"/> |
| Serial | | <input checked="" type="checkbox"/> <input type="checkbox"/> |
| Parallel | | <input checked="" type="checkbox"/> <input type="checkbox"/> |
| Modem | | <input checked="" type="checkbox"/> <input type="checkbox"/> |
| Internal Ports | | <input checked="" type="checkbox"/> <input type="checkbox"/> |

| Wireless Ports | Action | Log Alert |
|----------------|---------------------|--|
| WiFi | Define WiFi Control | <input checked="" type="checkbox"/> <input type="checkbox"/> |
| IrDA | | <input checked="" type="checkbox"/> <input type="checkbox"/> |
| Bluetooth | | <input checked="" type="checkbox"/> <input type="checkbox"/> |

| Anti Hybrid Network Bridging | Action |
|------------------------------|--|
| Hybrid Network Bridging | <input checked="" type="checkbox"/> <input type="checkbox"/> ... |

User: Administrator@UTIMACO Server: localhost

SafeGuard® PortProtector en Action



The screenshot displays the 'SafeGuard PortProtector Management Console' interface. The main window shows the 'Policies' tab with a policy named 'untitled2'. The left sidebar contains a navigation tree with sections: General, Security, and Settings. Under 'Security', 'Device Control' is expanded, showing sub-items like Port Control, Storage Control, File Control, and WiFi Control. The main content area shows the configuration for 'Device Control' under a 'White List' tab. It includes a table for 'Policy for All Devices' and a table for 'Device Types'.

Policy for All Devices

| Policy | Action | Log | Alert |
|----------------------|--------|-------------------------------------|--------------------------|
| All Devices | | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Hardware Key Loggers | | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

Device Types

| Device Type | Action | Log | Alert |
|----------------------------------|--------|-------------------------------------|--------------------------|
| Human Interface Devices | | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Printing Devices | | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Personal Data Assistants (PDA's) | | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Windows Mobile/Pocket PC Devices | | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Blackberry Devices | | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Palm OS Devices | | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Mobile Phones | | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Network Adapters | | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Imaging Devices | | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Audio / Video Devices | | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Smart Cards | | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

At the bottom of the console, the user is identified as 'Administrator@UTIMACO' and the server as 'localhost'.