



SecureWave

Corporate Presentation

OSSIR

11 octobre 2005

Version 3.3



SecureWave® Corporate Overview



SecureWave

Corporate Overview

3

SecureWave®: Safeguarding Tomorrow™



Financials – Founded in 2000. Privately held, venture backed, profitable and growing at 100%+ per year for three consecutive years

Customers – ~1,000,000 licenses sold across over 700+ enterprise customers.

Leadership – Recognized by the market as an innovator and leader in the security market

Future – The leader in policy-based threat prevention solutions for PCs and Servers



SecureWave

SecureWave Customers

Government, Financial, Health Care, Manufacturing, and IT



EXPERIENCE. RESULTS.



Australian Federal Police



Zentrale Polizeitechnische Dienste
Nordrhein-Westfalen



SecureWave

SecureWave Value Proposition

5

What Do We Do?

SecureWave's Sanctuary™ platform provides policy-based threat prevention solutions for Global 2000 Enterprises

Who are our Customers?

~ 1,000,000 enterprise workers in 700+ accounts rely on our security solutions

Our Product Portfolio

The Sanctuary™ platform secures Personal Computers, Servers, and Terminal Servers against tomorrow's malware today at the point of execution and prevents unauthorized device usage

What Makes Us Unique?

Sanctuary™ shifts customers away from reactive security models through a positive policy-based application and device control model



SecureWave

Sanctuary™ Platform: PC Solutions

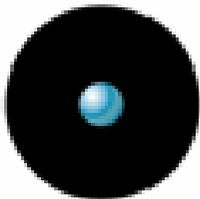
6



SecureWave
Sanctuary™
Custom Edition

Sanctuary™ Custom Edition

Enforces a granular policy over user/user groups and their use of specific applications to match complex and distributed enterprise environments.



SecureWave
Sanctuary™
Device Control

Sanctuary™ Device Control

Establishes and enforces granular policy about which devices can be used by whom, as well as how and when they can be used.



SecureWave
Sanctuary™
Application Control
Custom Edition





SecureWave

Exécutions de logiciels

8

Applications

Autorisées

- > Systèmes d'exploitation
- > Logiciels-métier que l'utilisateur peut accéder

Malware

Connu

- > Virus, vers, chevaux de Troie
- > Logiciels d'intrusion

Non-autorisées – Non-désirées

- > Jeux, Sharewares
- > Logiciels piratés
- > Logiciels que l'utilisateur ne doit pas accéder

Inconnu

- > Virus, vers, chevaux de Troie
- > Logiciels d'intrusion



SecureWave

Approche Liste Noire

9

Applications

Autorisées

- > Systèmes d'exploitation
- > Logiciels-métier que l'utilisateur peut accéder

Malware

Connu

- > Virus, vers, chevaux de Troie
- > Logiciels d'intrusion

RISQUE

Non-autorisées – Non-désirées

- > Jeux, Sharewares
- > Logiciels piratés
- > Logiciels que l'utilisateur ne doit pas accéder

Inconnu

- > Virus, vers, chevaux de Troie
- > Logiciels d'intrusion

Sanctuary™
Application Control
Custom Edition



SecureWave

Approche Liste Blanche

10

Gestion de ce qui est connu et permis

uniquement

Applications

Malware

Autorisées

- > Systèmes d'exploitation
- > Logiciels-métier que l'utilisateur peut accéder

Connu

- > Virus, vers, chevaux de Troie
- > Logiciels d'intrusion

**Non-autorisées –
Non-désirées**

- > Jeux, Sharewares
- > Logiciels piratés
- > Logiciels que l'utilisateur ne doit pas accéder

Inconnu

- > Virus, vers, chevaux de Troie
- > Logiciels d'intrusion



SecureWave

Sun HealthCare Group Inc.

11

Sun HealthCare Group Inc.

- > Actif dans le monde de la santé
- > env. 10.000 lits
- > 15.740 employés

Opération

- > Recherche sur Google (barre d'outil)
- > Lien
- > Code nuisible activé

Conséquences

- > PC infecté
- > PC envoie 30.000 8 bit packets par seconde
- > 3 jours d'impact négatif sur le réseau
- > Firewall ne fonctionne plus
- > Aucune trace



SecureWave

Sun HealthCare Group Inc.

16.02.2005 "Marketplace" *Wall Street Journal*

Microsoft Makes Push for Security

Antivirus Software to Come By Year End, New Version Of Browser Will Arrive Soon

By ROBERT A. GUTH
And DAVID BANK

SAN FRANCISCO—Microsoft Corp. Chairman Bill Gates said the software maker soon would release the first major overhaul of its Internet browser in four years, and outlined a broad strategy of investments and technologies aimed at answering mounting criticism that Microsoft's products are rife with security flaws.

At a computer-security conference here, Mr. Gates said Microsoft by year end will offer antivirus software for consumers. Also available will be software for fighting "spyware" that can surreptitiously steal information from computer users.

Overall, "I'm very optimistic," Mr. Gates said, that "we will solve the security problem."

Mr. Gates's comments are a sign of a shift in Microsoft's strategy, instead of relying on acquisitions to protect users of its products. Microsoft has acquired three technology companies in the last two years, rolling the \$10 billion security-software industry.

The speech was short on details about one of the most widely anticipated pieces of Microsoft's strategy, the antivirus software, which some industry executives had expected in the first part of

this year. Still, Microsoft said that by year end, it would ship a "broad consumer offering" that would include antivirus software. Mr. Gates didn't say whether Microsoft would sell the program, give it away, or include it with other Microsoft offerings.

"That's later than we thought," said John Thompson, chairman of Symantec Corp., the leading maker of antivirus software that could lose sales because of the Microsoft move. Mr. Thompson said the later arrival suggests "that this is not a problem that's easily solved."

While Mr. Gates said Microsoft wouldn't charge for the spyware product, other Microsoft executives said



Thompson said he expects spyware programs to become part of broader antivirus packages.

Microsoft's plans to ship a new version of its browser, called Internet Explorer, come as millions of computer users have defected to Firefox, a free browser that has been less affected by viruses, spyware and other attacks. The rise of Firefox, which is made by a non-profit group called the Mozilla Foundation, helped to pressure Microsoft last year to refocus on making Internet Explorer more secure.

The new browser, Internet Explorer 7.0, will be available early this summer in a test version and will include "new levels of security," Mr. Gates said, including features for fighting spyware and identity-theft scams called phishing. He said the enhanced browser will be built

"A single [infected] machine took our network to its knees," says Zachary Grant, a senior network engineer at Sun HealthCare. Mr. Grant said he tested the Firefox browser, and it wasn't susceptible. Mr. Grant said he was able to fix the problem with software from SecureWave SA, a start-up based in Luxembourg.

else can play."

Symantec's Mr. Thompson said he isn't worried about a Microsoft spyware offering, because antispyware programs aren't big moneymakers. Instead, Mr.

HealthCare. Mr. Grant said he tested the Firefox browser, and it wasn't susceptible. Mr. Grant said he was able to fix the problem with software from SecureWave SA, a start-up based in Luxembourg.

Sanctuary™
Application Control
Custom Edition



SecureWave

0, 1, 2, 3, Go



Utilisateur individuel



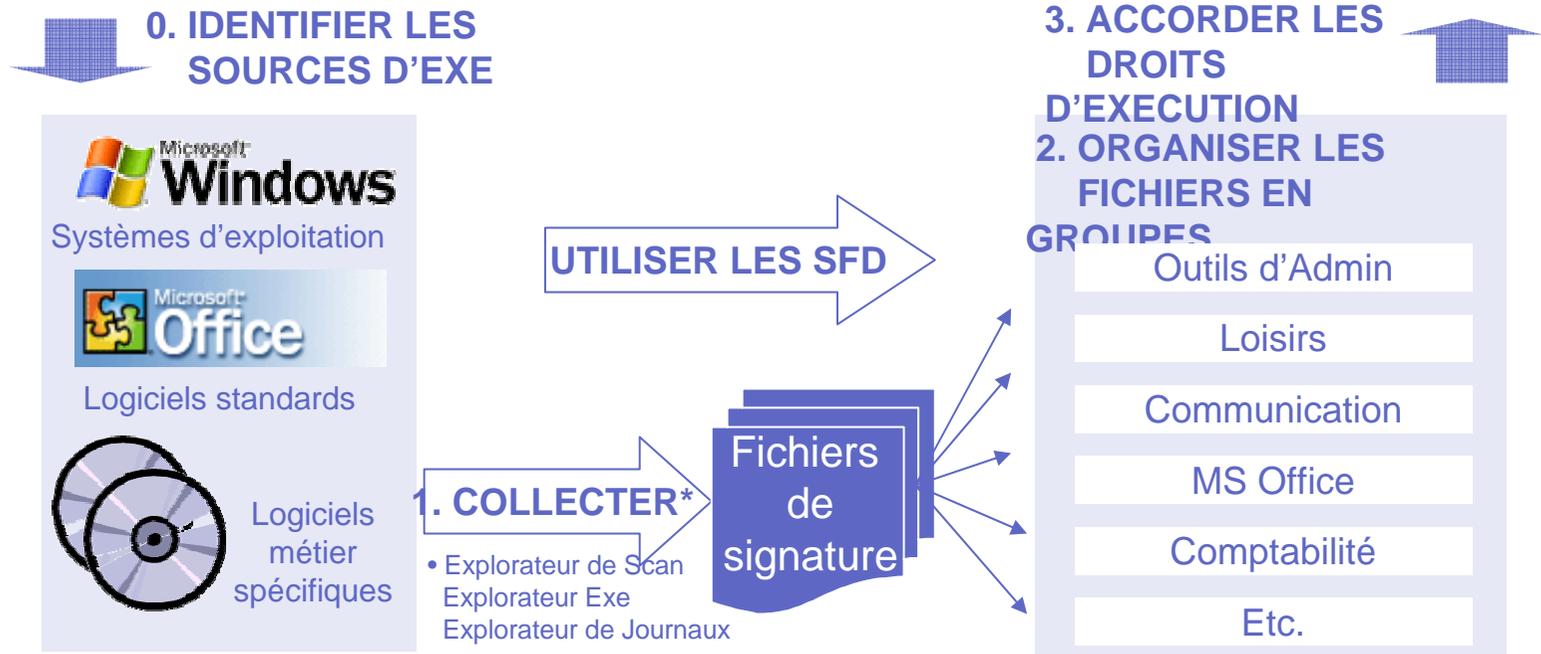
Groupes d'utilisateurs

- Comptabilité
- Force de Vente
- Informatique
- Help desk
- Utilisateurs du Dépt. A
- Personnel externe, Etc.



Active Directory

Les utilisateurs ne peuvent dorénavant exécuter que les applications / fichiers executables permis



**Sanctuary™
Application Control
Custom Edition**



SecureWave

Fonctionnement du Produit

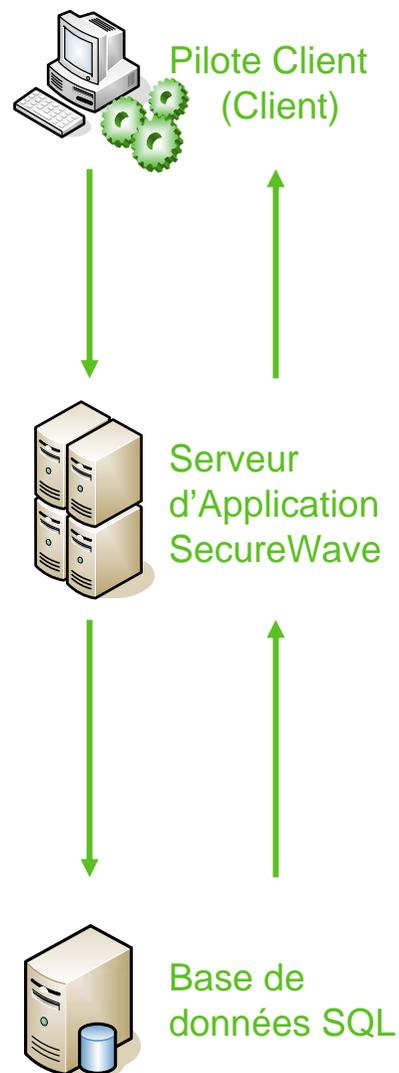
14

1. L'utilisateur s'identifie (logon).

2. Le client Sanctuary demande la vérification de, ou met à jour, la liste des fichiers que l'utilisateur est autorisé à exécuter.

3. Le serveur d'Application SecureWave transmet la requête à la base de données.*

* Le service de cache permet de réduire les accès à la base de données



6. La liste est sauvegardée localement. Chaque tentative d'exécution sera vérifiée localement pour autorisation et inscrite dans les logs.

5. Le serveur d'Application SecureWave signe la liste par clé cryptographique et la transmet au client.

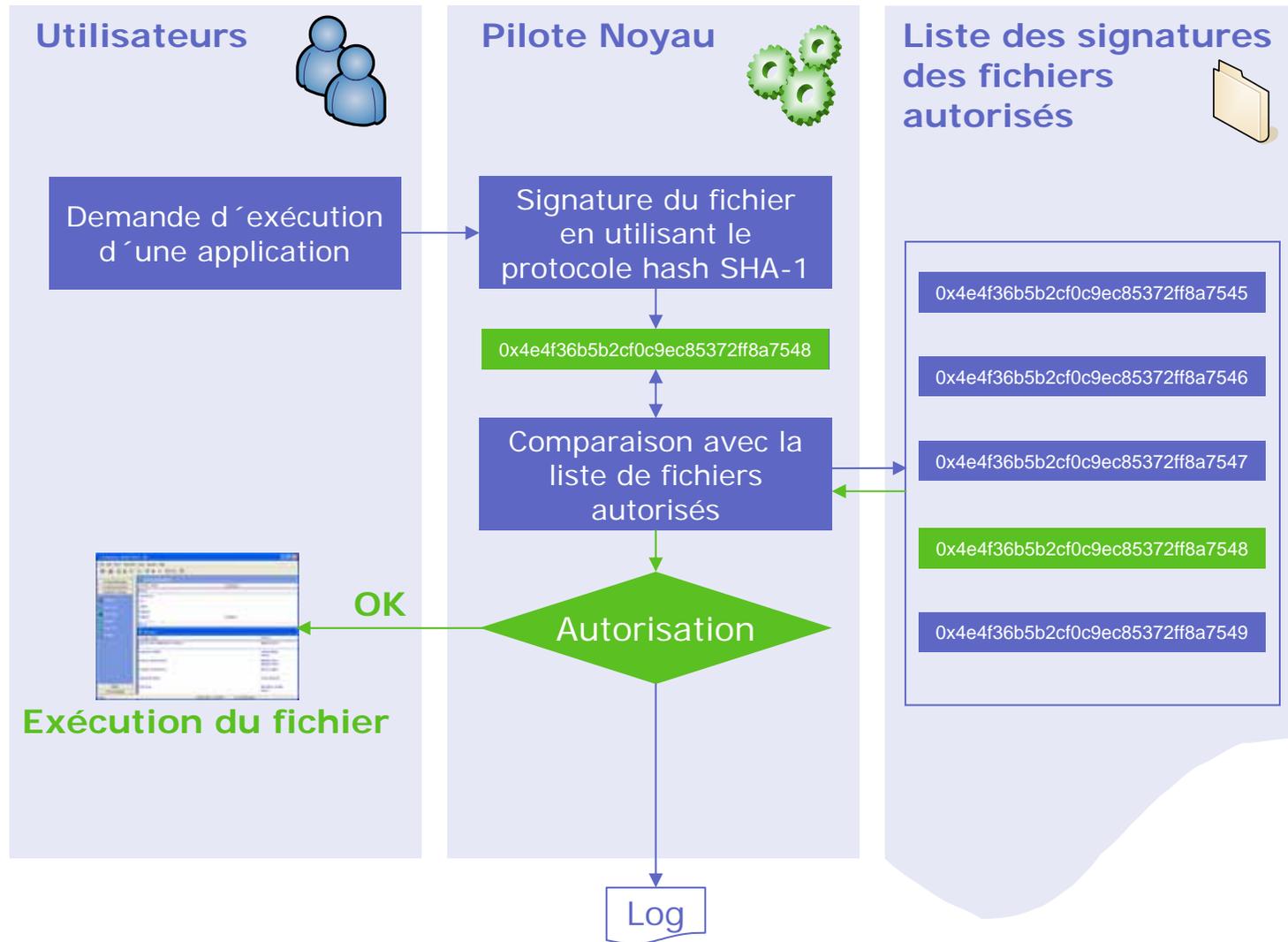
4. Une liste des fichiers autorisés est renvoyée en fonction du profil de l'utilisateur (droits d'autorisation).

Sanctuary™
Application Control
Custom Edition



SecureWave

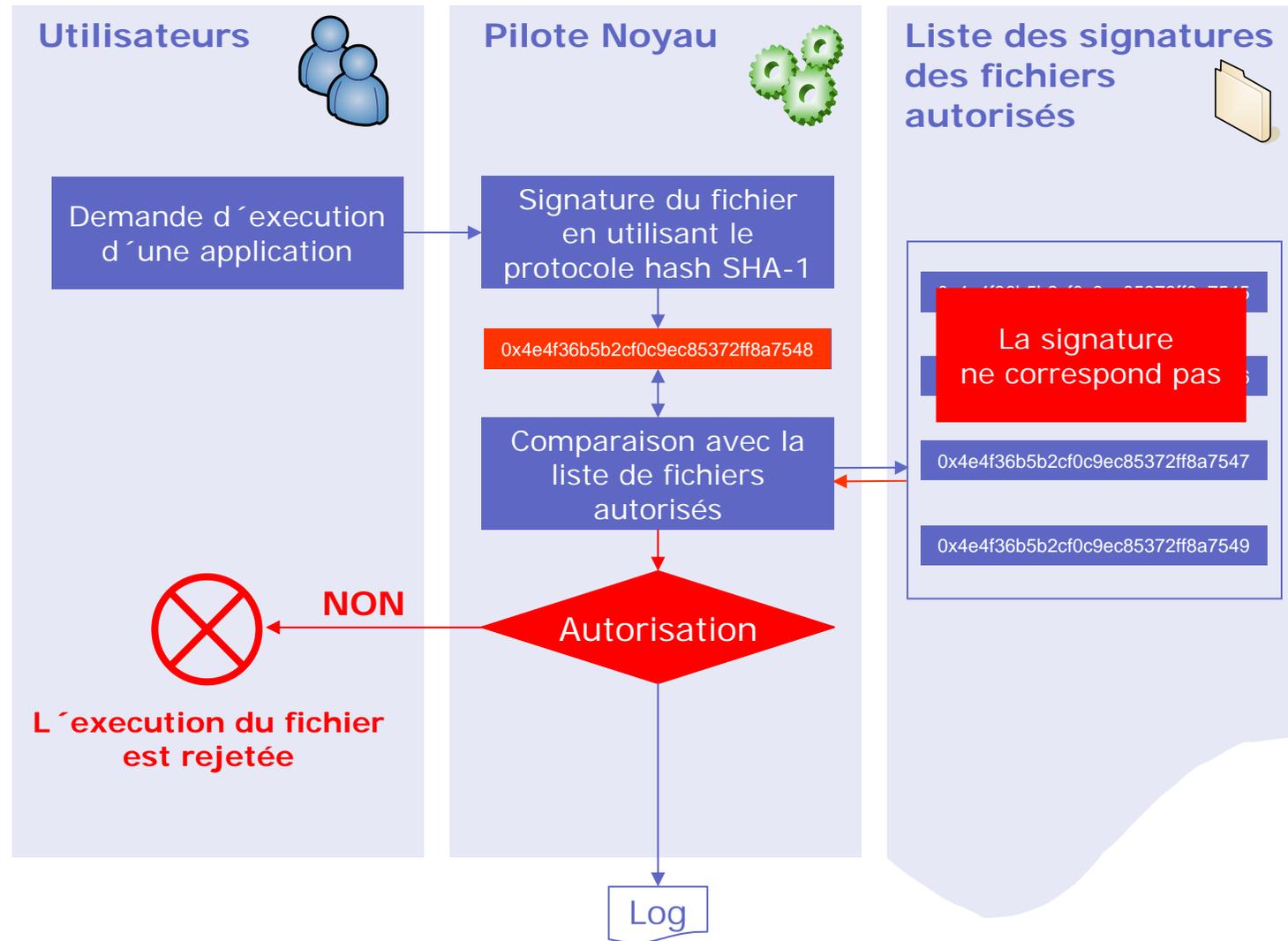
Exécution authentifiée





SecureWave

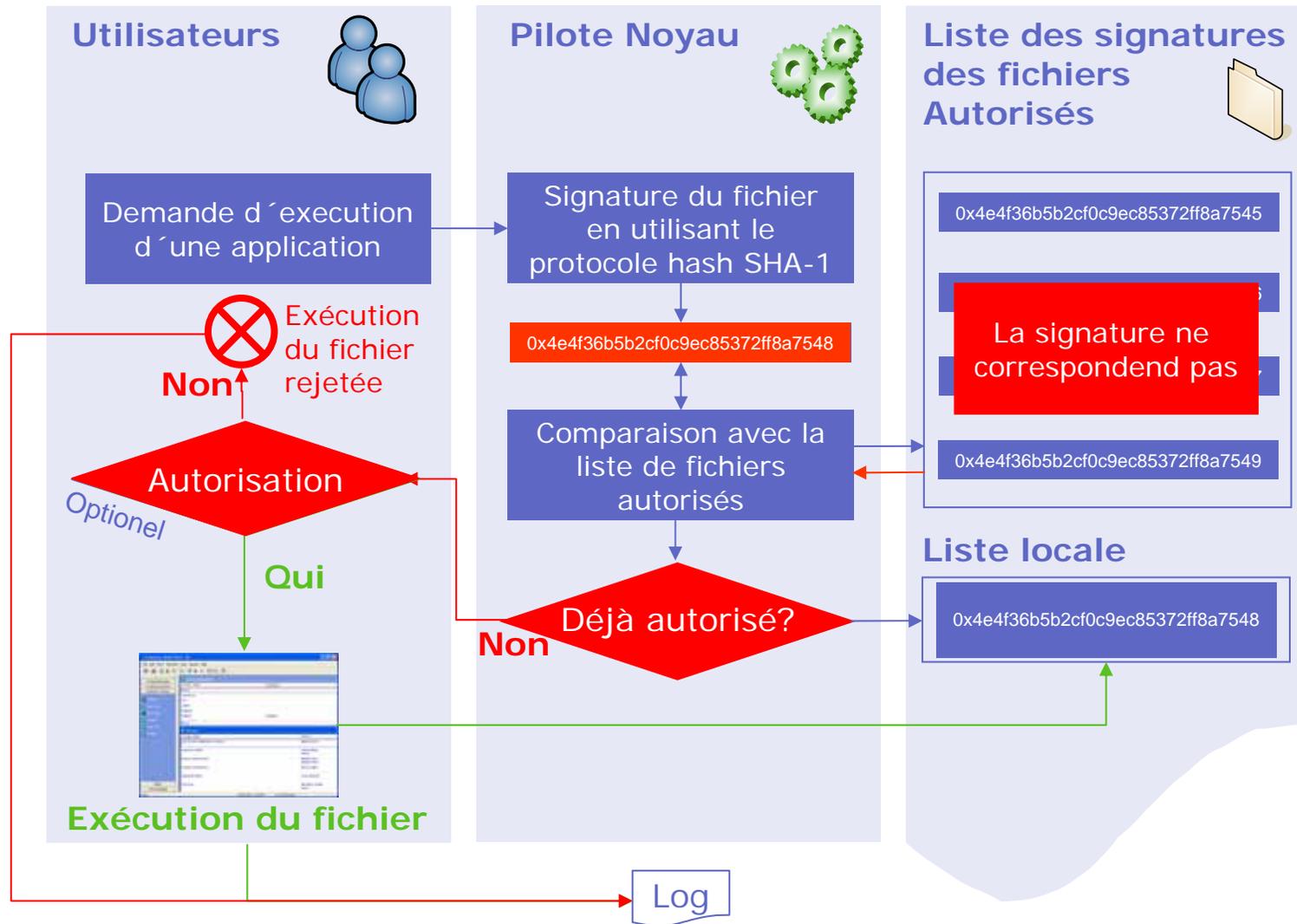
Exécution authentifiée





SecureWave

Exécution authentifiée

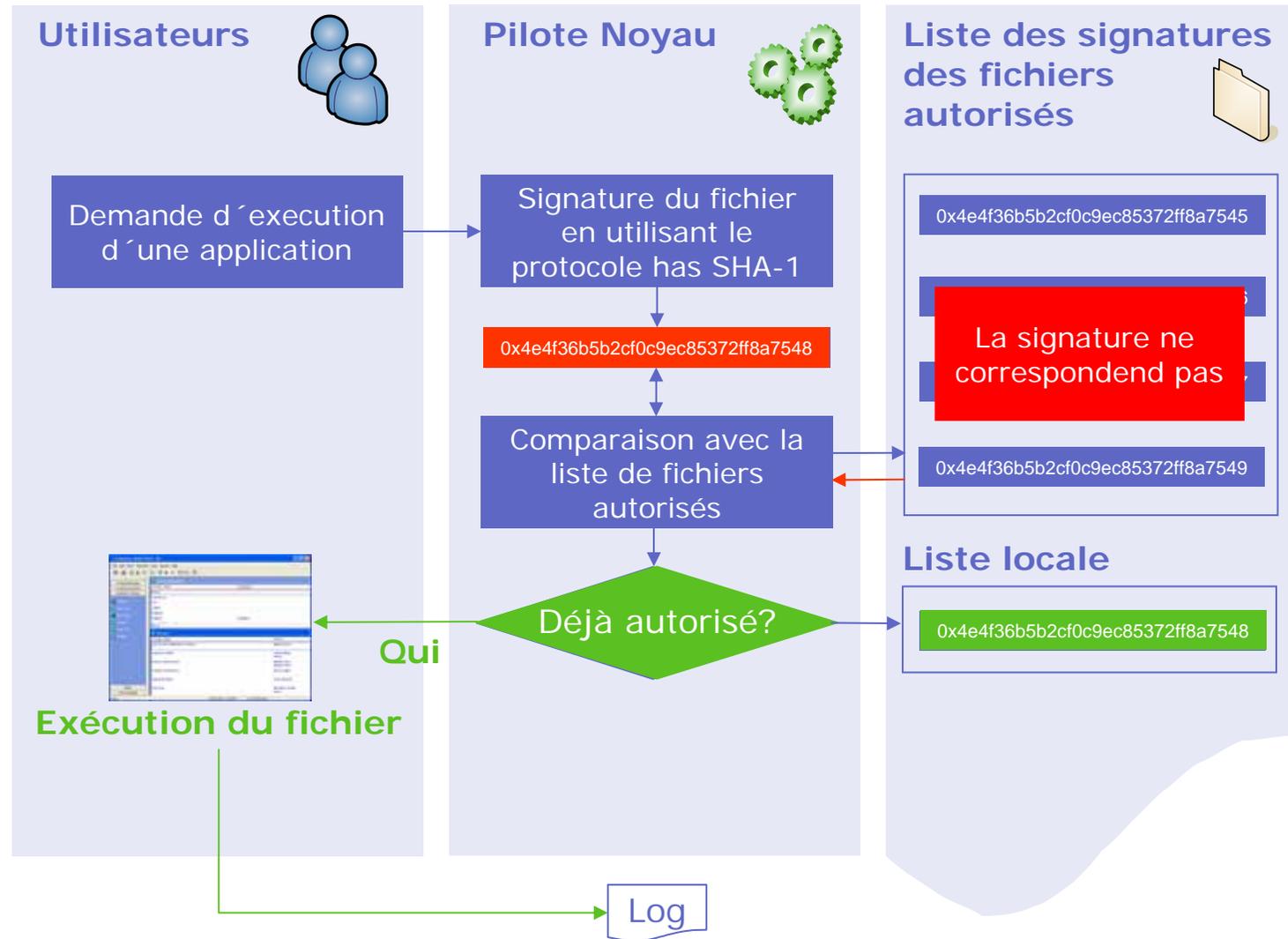


Sanctuary™
Application Control
Custom Edition



SecureWave

Authenticated Execution



Sanctuary™
Application Control
Custom Edition



SecureWave

Sanctuary Application Control Custom

19

Edition

Caractéristiques principales (1/2)

Liste blanche

- > Uniquement les fichiers explicitement autorisés peuvent être exécutés, et par défaut tout le reste est “rejeté”
- > Aucun besoin de services de souscription pour mise à jour (de type définitions AV)
- > Besoin de mettre à jour la liste des fichiers autorisés lorsqu’un nouveau logiciel est déployé

Souplesse et capacités de personnalisation

- > Accorde des droits d’accès à des utilisateurs ou groupes d’utilisateurs spécifiques
- > Accorde l’accès à des exécutables “à la volée”, sans redémarrer ou sans se reconnecter
- > Une large gamme d’outils d’administration dont un wizard sont fournis pour faciliter l’autorisation d’applications

Mises à jour des droits d’accès

- > Les mises à jour de la liste des signatures des fichiers autorisés sont effectuées à chaque connexion
- > Possibilité d’implémenter des droits d’accès “à la volée” (sans nouvelle identification)

Protection d’ordinateur distant/déconnecté

- > Une copie locale de la dernière liste de signatures est conservée sur le PC déconnecté ou sur le portable, permettant une protection permanente. Les mises à jour (si nécessaires) seront effectuées lorsque l’ordinateur se reconnectera au réseau

Capacités de logs et d’audit

- > Toutes les demandes d’exécution de fichiers autorisés ou non-autorisés peuvent être notées
- > Audit complet de toutes les actions Administrateur

**Sanctuary™
Application Control
Custom Edition**



SecureWave

Sanctuary Application Control Custom

20

Edition

Caractéristiques principales (2/2)

Protection contre les scripts

- > Sanctuary™ Application Control Custom Edition peut contrôler l'exécution de VBScript, Microsoft Office VBA et JavaScript

Mode bloquant vs. Mode non-bloquant

- > Le mode bloquant ou non-bloquant détermine si le Client Sanctuary™ Application Control Custom Edition doit bloquer l'exécution ou pas d'un exécutable non-autorisé (Mode bloquant est le mode par défaut)
- > Le groupe Administrateurs est configuré automatiquement en Mode non-bloquant pour simplifier la phase d'implémentation

Evolutivité

- > L'utilisation d'une architecture 3-tier (Serveur d'application, Base de données, Client) permet une souplesse de déploiement et une évolutivité pour l'entreprise

Supporte domaine NT/Active Directory et délégation de droits

- > Peut utiliser un domaine Active Directory existant afin d'appliquer les permissions
- > Incorporation automatique de la délégation des droits d'administration des Unités d'Organisation de Active Directory (Active Directory Organizational Units)

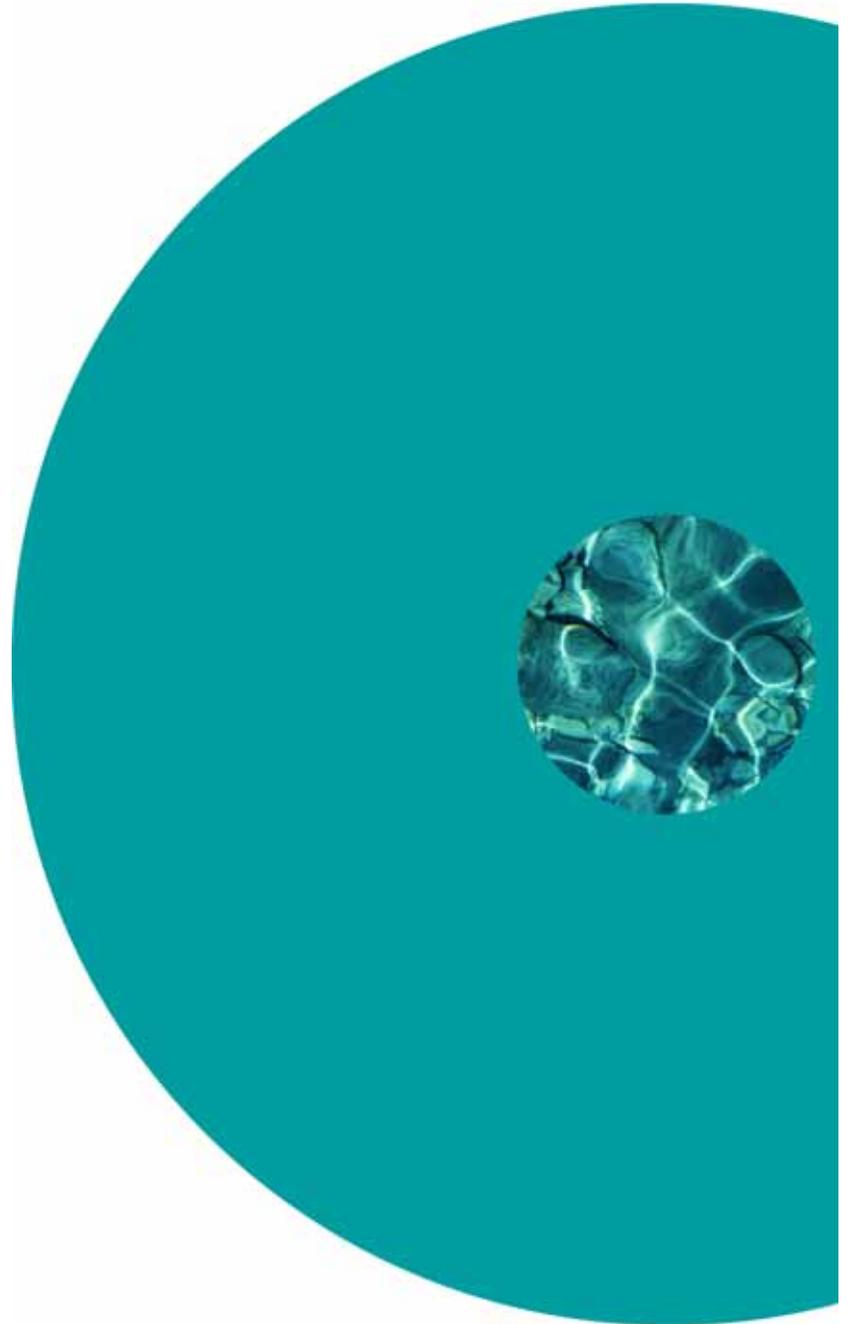
Installation à distance

- > L'installation peut être réalisée à l'aide de n'importe quel outil de déploiement utilisant le Setup MSI (par ex.: Microsoft Systems Management, Group Policies, WinInstall, etc.)

**Sanctuary™
Application Control
Custom Edition**



SecureWave
Sanctuary™
Device Control





SecureWave

Le problème

22

Nouvelle technologie

- > Plug & play
- > Sans fil

D'après Samsung, le marché mondial des clés mémoire représente 2,5 milliards de dollars par an.



SecureWave

Le problème

23

Nouveau comportement

- > Partage et portabilité des données



Les clés mémoire USB deviennent omniprésentes : 85 % des travailleurs les utilisent pour transférer des données entre le bureau et la maison, ce qui augmente le risque d'infection par des logiciels malveillants.



SecureWave

Le problème

24

Nouvelles menaces

- > Conformités réglementaires
 - > Risque pour la vie privée

- > Brèches de confidentialité des données d'entreprise
 - > Pertes concurrentielles

80 % des responsables informatiques récemment interrogés reconnaissent que les périphériques multimédia amovibles (telles les clés mémoire USB) représentent une sérieuse menace à l'encontre de la sécurité.

60 % avouent ne pas pouvoir surveiller l'utilisation de ces périphériques...



SecureWave

Le saviez-vous ?

25



Si un lecteur flash USB est entre de mauvaises mains, votre pare-feu devient inutile !



SecureWave

Le saviez-vous ?

26



**Un iPod = 60 Go = 300 secondes =
5 minutes pour copier 1 500 000
pages Microsoft Word**



SecureWave

Le saviez-vous ?

27



Bien sûr, ceux-là, vous les auriez remarqués...



SecureWave

Le saviez-vous ?

28



...mais celui-ci ?

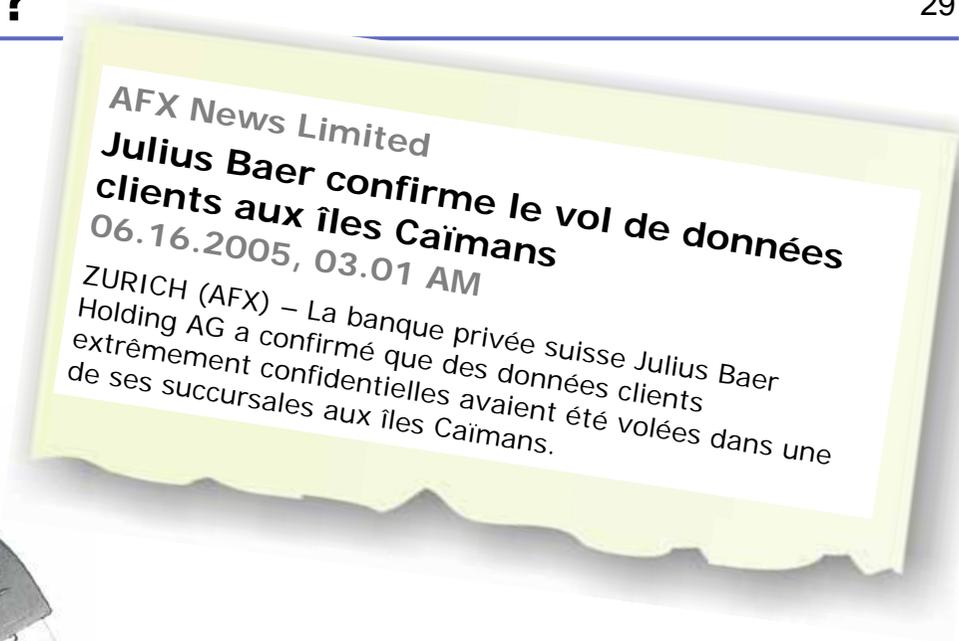
(clé mémoire 512 Mo)



SecureWave

Le saviez-vous ?

29



AFX News Limited
**Julius Baer confirme le vol de données
clients aux îles Caimans**
06.16.2005, 03.01 AM

ZURICH (AFX) – La banque privée suisse Julius Baer Holding AG a confirmé que des données clients extrêmement confidentielles avaient été volées dans une de ses succursales aux îles Caimans.

Il faut très peu de temps pour voler des données

(clé mémoire 1 024 Mo)



SecureWave

Si vous utilisez Windows XP...

30



- > Si vous utilisez Windows XP, il y a 95 % de chances pour que vous n'ayez même pas besoin d'installer un pilote pour utiliser ces périphériques de grande capacité !
- > Vous n'avez pas besoin d'être administrateur pour installer ces périphériques USB et FireWire !
- > Vous ne pouvez pas gérer les périphériques WiFi, Bluetooth, USB et FireWire via des règles de groupe !



SecureWave

Les faits...

31

- > 80 % des brèches de sécurité sont provoquées par des personnes internes...
- > Les clés mémoire sont faciles à égarer.
- > Des périphériques externes peuvent être utilisés pour voler des données.
- > Tout aussi important : le risque d'introduire du code malveillant dans le réseau d'entreprise.
- > La sécurité des fichiers du système d'exploitation Windows peut être menacée par un bug du protocole FireWire.



SecureWave

Conséquences du vol et de la perte de données

32

For sale:

Memory stick plus cancer patient records

By [John Leyden](#)

Posted: 13/03/2003 at 17:32 GMT Source: www.TheRegister.com

Health bosses in Lancashire are facing awkward questions after confidential medical records of 13 cancer patients found their way onto a portable memory stick, which was repackaged and sold as new to a Crewe estate agent.

Investigations into the leak of the medical records of 13 patients are continuing, the *Bolton Evening News* reported yesterday. Meanwhile hospital chiefs are trying to restore confidence by vowing to take steps to make sure that such a serious security breach can never happen again.

Graham Fullarton, the Royal Bolton Hospital's data protection manager, told the paper that there would be a "full review" of hospital procedures, which will likely result in a ban on portable storage devices.

"Using memory sticks is unusual and unorthodox. We don't want people to cart information like this around," he said. "We are treating this with the utmost gravity. It is a serious incident. There has to be additional security put in place to make sure this situation is not repeated.

Police involvement in the incident is dependent on the results of the hospital's own internal investigation. An early picture of what happened and when has emerged, but there are still plenty of blanks in the story to fill in.

It seems medical records of patients (dating back to 1999) were copied from a hospital PC onto a portable memory stick. We don't know who did this. How this stick was subsequently obtained by a unnamed Crewe reseller, who sold it (as a new, blank stick) to estate agent Dawn Rozzell for £30, also remains unclear.

In any case when Ms Rozzell connected the stick to her PC she had quite a surprise - it contained "the dates of birth, home addresses, telephone numbers, family medical histories and GP details" of 13 cancer patients, the *Bolton Evening News* reports.

Hospital bosses have promised to contact affected patients, once their identities are confirmed. ®



SecureWave

Le défi

33

Nous pouvons nous attendre à ce que l'utilisation de nouveaux périphériques s'intensifie

- > Prix, forme, fonctionnalité
- > Nouveaux moyens de travailler

Nous ne pouvons pas stopper leur adoption

- > Non qu'il faille essayer

Nous devons mettre en vigueur des règles pour permettre une utilisation sûre de ces périphériques

- > Contrôles granulaires permettant aux utilisateurs de faire leur travail tout en garantissant des comportements adéquats.
- > Restrictives mais flexibles



SecureWave

Accorder des droits



Utilisateur isolé

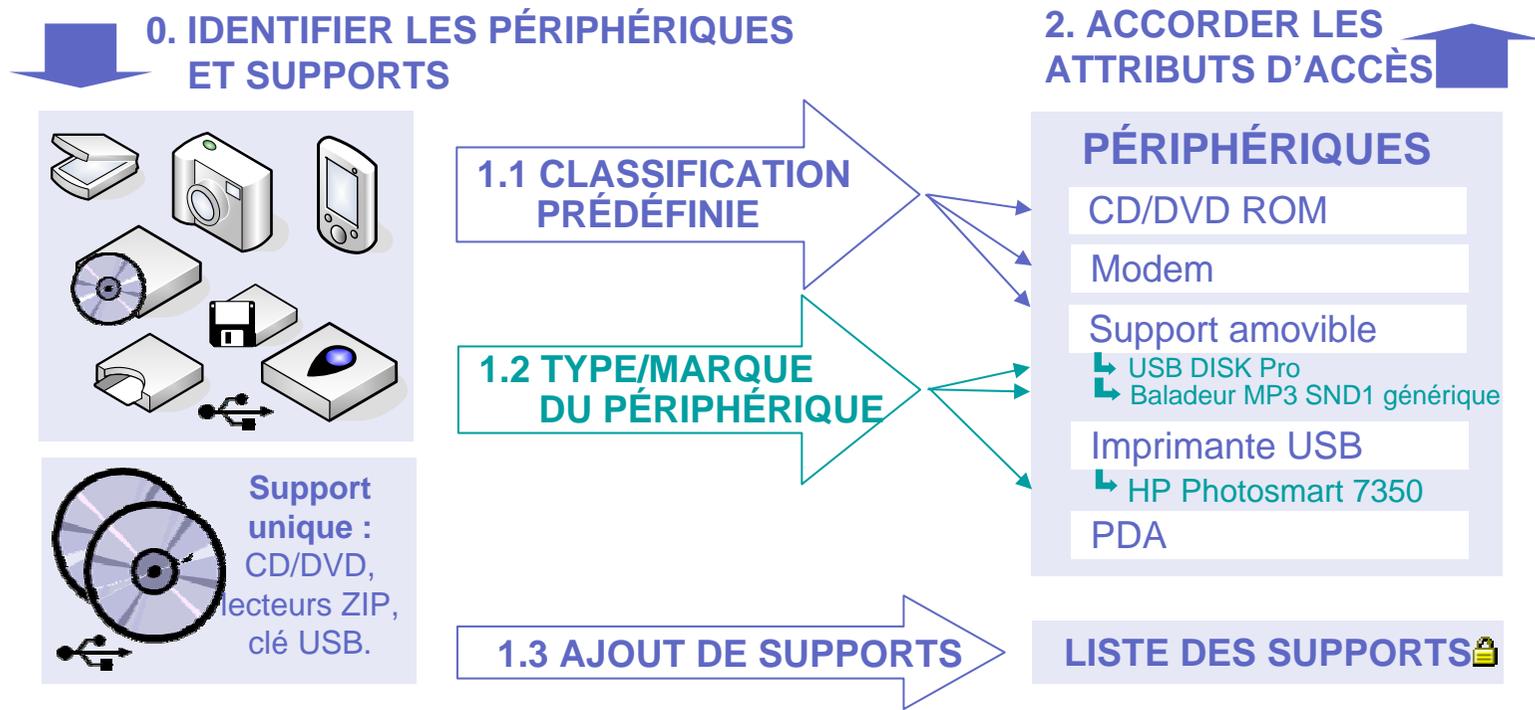


Groupe d'utilisateurs

- Comptabilité
- Commerciaux
- Admin. réseau
- Équipe du support
- Utilisateurs entité A
- Pers. extérieures, etc.



Les utilisateurs ne peuvent désormais accéder qu'aux périphériques et supports autorisés en fonction des droits accordés (lecture/écriture)

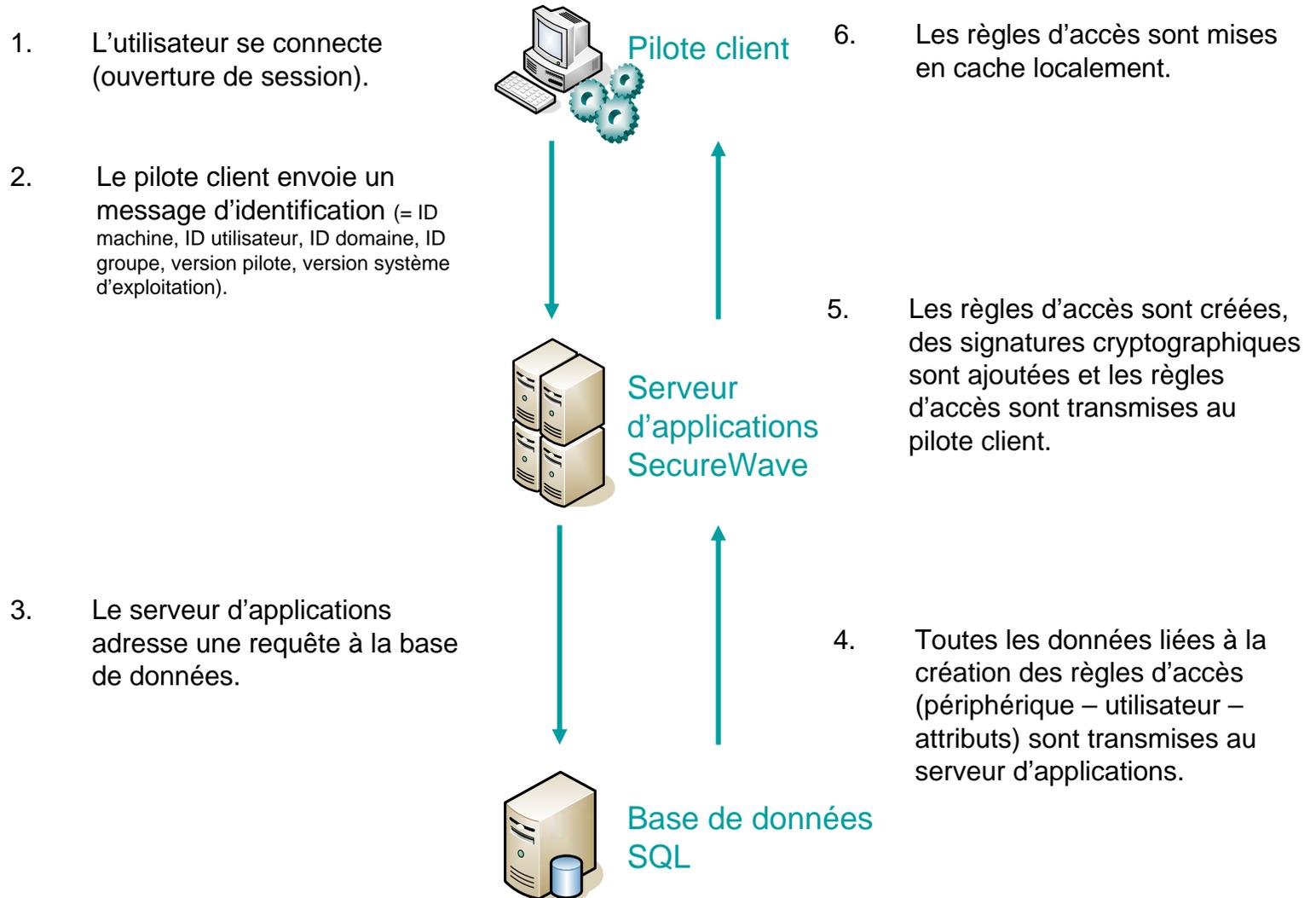




SecureWave

Fonctionnement du produit

35

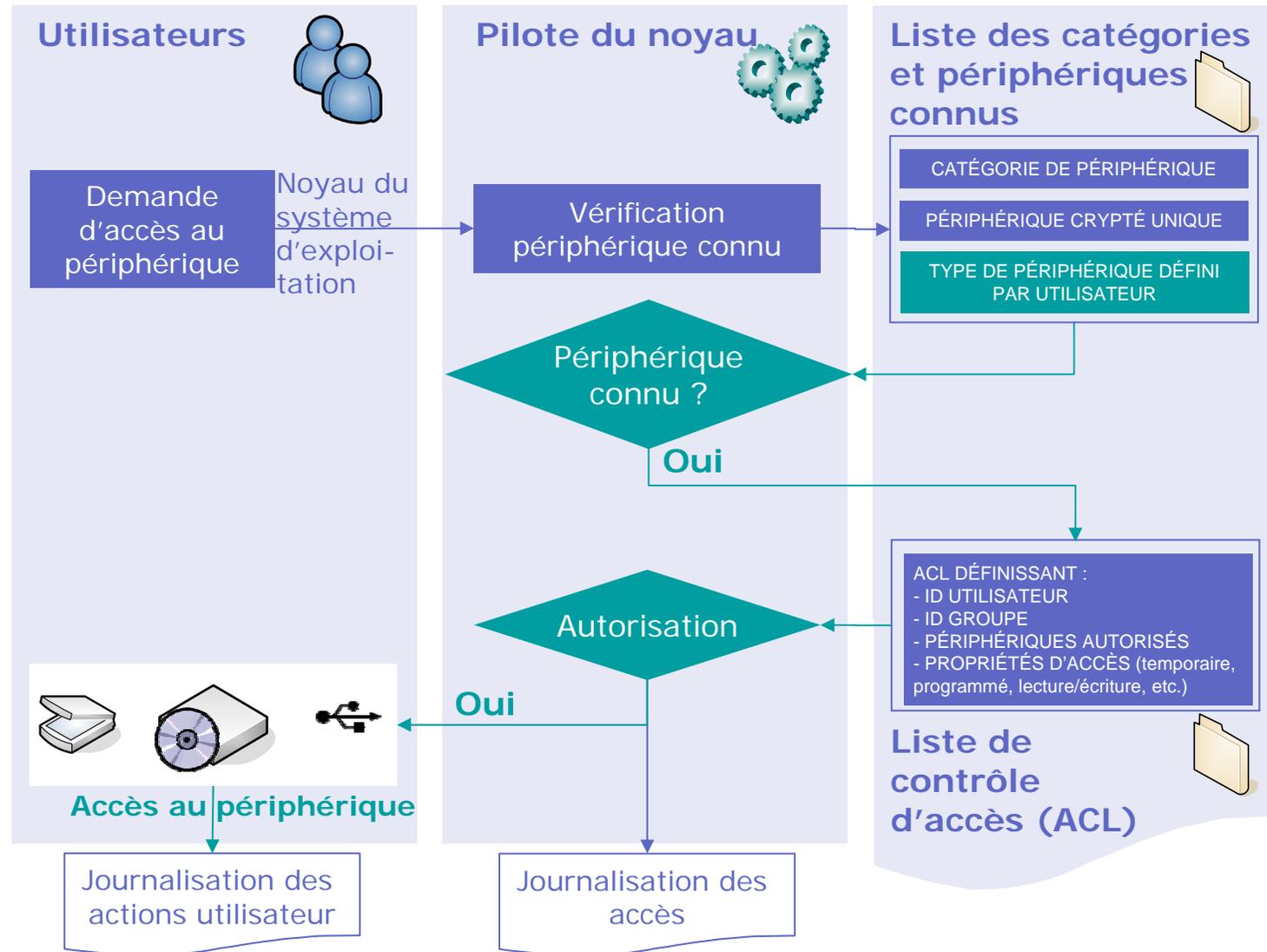




SecureWave

Contrôle de l'accès aux périphériques gérés

36



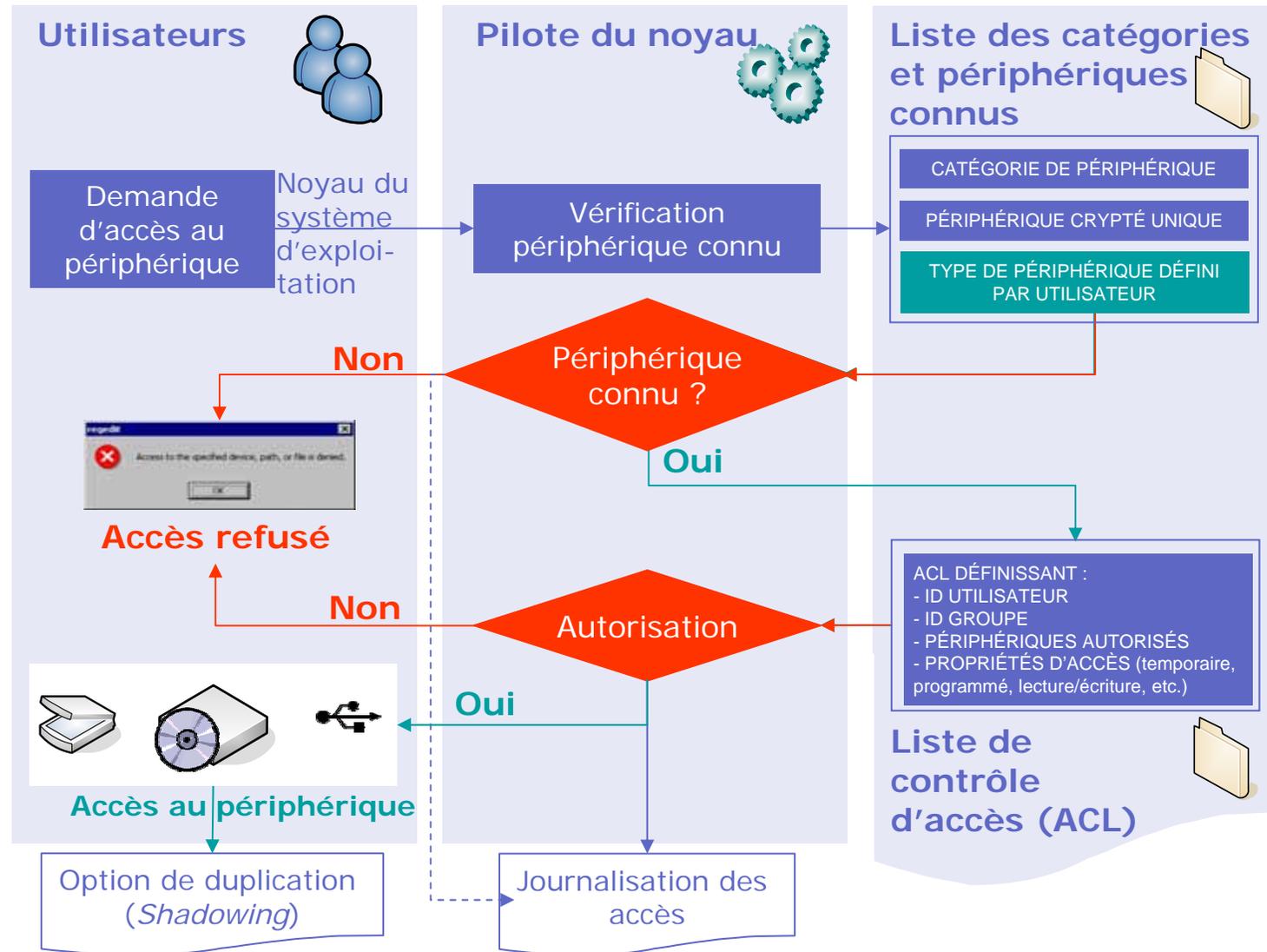
Sanctuary™
Device Control



SecureWave

Contrôle de l'accès aux périphériques gérés

37



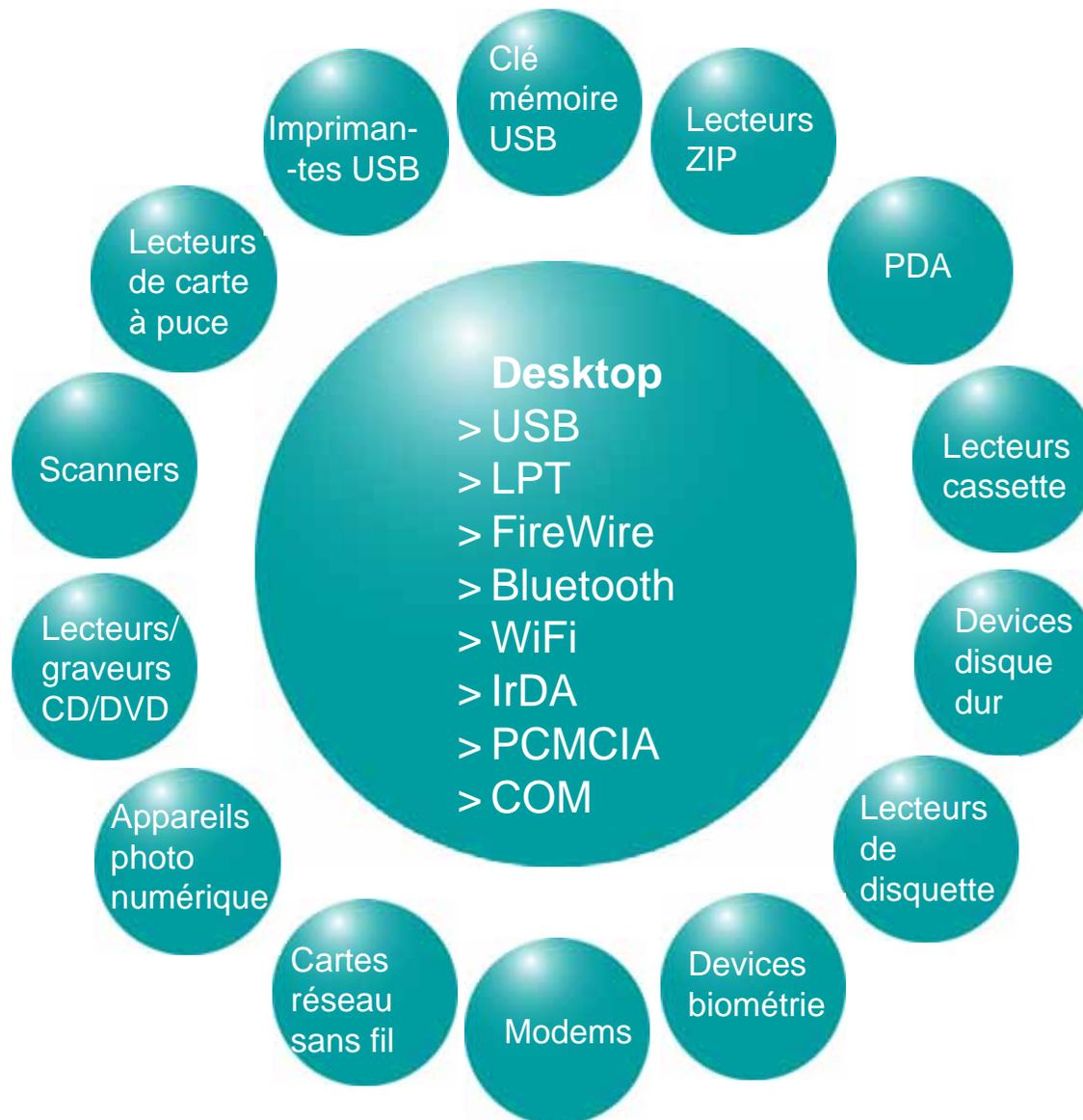
Sanctuary™
Device Control



SecureWave

Sanctuary Device Control

38



Sanctuary™
Device Control



SecureWave

Sanctuary Device Control

39

Caractéristiques principales (1/3)

Permissions basées sur les ACL (Access Control List)

- > Permissions par utilisateur et par groupe d'utilisateurs
- > Permissions spécifiques à une machine également possible

Liste blanche des devices/équipements

- > Evite l'installation de devices non-connus
- > Possibilité d'autoriser uniquement des types de device dans une catégorie
- > Peut identifier un device spécifique de manière unique

Accès programmé et temporaire aux devices

- > Accès en lecture et/ou en écriture
- > Accès programmé pour une durée prédéfinie
- > Accès temporaire

Identification et autorisation ponctuelle de périphériques amovibles spécifiques

- > Crée des collections de DVD/CD-ROM et en accorde l'accès aux utilisateurs ou groupes d'utilisateurs
- > Crée des listes de médias spécifiques amovibles avec un ID unique et en accorde l'accès aux utilisateurs
- > Autorise n'importe quel média amovible à n'importe quel utilisateur utilisant une technologie d'encryption

Sanctuary™
Device Control



SecureWave

Sanctuary Device Control

40

Caractéristiques principales (2/3)

Devices Plug and Play : support du Hot Plug

- > Détection des devices Plug and Play “à la volée”
- > Application des ACL en temps réel

Capacité d’audit et de “shadowing”

- > Possibilité de noter toutes les données copiées vers des devices externes ou des ports spécifiques
- > Une copie des données envoyées vers un équipement d’E/S peut être effectuée et gardée (en temps réel ou avec un délai)
- > Possibilités de rapports (sur les ACL, collection de devices, etc.)

Mises à jour des droits d’accès

- > Les mises à jour des droits d’accès sont effectuées à chaque connexion
- > Possibilité d’implémenter des droits d’accès à la volée (sans nouvelle identification)

Protection d’ordinateur distant/déconnecté

- > Une copie locale de la dernière liste de permissions d’accès aux devices est conservée sur le PC déconnecté ou sur le portable, permettant une protection totale lors d’une déconnexion. Les mises à jour (si nécessaires) seront effectuées lorsque l’ordinateur se reconnectera au réseau



SecureWave

Sanctuary Device Control

41

Caractéristiques principales (3/3)

Restriction du volume de données copiées

- > Possibilité de restreindre la quantité de données copiées depuis le PC (ou depuis le réseau) vers un device externe (Média amovible et disquettes)

Evolutivité

- > L'utilisation d'une architecture 3-tier (Serveur d'application, Base de données, Client) permet une souplesse de déploiement et une évolutivité pour l'entreprise
- > Evolutivité et Redondance sont possibles grâce au load-balancing

Supporte domaine NT/Active Directory

- > Peut utiliser un domaine Active Directory existant afin d'appliquer les permissions
- > Incorporation automatique de la délégation des droits d'administration des Unités d'Organisation de Active Directory (Active Directory Organizational Units)

Installation à distance

- > L'installation peut être réalisée à l'aide de n'importe quel outil de déploiement utilisant le Setup MSI (par ex.: Microsoft Systems Management, Group Policies, WinInstall, etc.)

Sanctuary™
Device Control



SecureWave

Attributs d'accès

42

Accès en lecture et/ou écriture

Accès programmé

Du lundi au vendredi, de 08h00 à 18h00

Accès temporaire

Pour les quinze prochaines minutes ou pour deux jours à compter de lundi

Accès en ligne/hors ligne

Gestion par quotas des données copiées

Par exemple, limiter les données copiées à 100 Mo par jour

Duplication des données (*Shadowing*)

Enregistre une copie complète de toutes les données écrites sur un périphérique externe



SecureWave

Des attributs peuvent être alloués à...

43

Une catégorie de périphériques complète

- > Imprimantes USB
- > Lecteur CD/DVD

Une sous-catégorie de périphériques

- > Imprimante USB HP7575
- > CD/DVD NECND 3520A...

Un périphérique crypté unique

Un CD/DVD unique

Des groupes de

- > Périphériques et/ou supports uniques
- > Catégories ou sous-catégories de périphériques



SecureWave

Et donner accès à...

44

- Un compte d'utilisateur local ou de groupe local
- Un utilisateur ou un groupe Active Directory
- Un domaine Active Directory
- Une machine
- Un groupe de machines créé dans SDC



Caractéristiques de sécurité

45

Technologie du pilote du noyau

- > Invisible aux utilisateurs et aux pirates (pas de processus dans le gestionnaire des tâches)
- > Pas de diminution des performances sur le client
- > Aucune possibilité de conflit avec d'autres logiciels de sécurité

Cryptage de périphériques uniques avec AES

- > Clé AES 256 bits = indéchiffrable
- > Cryptage SDC = rapide et transparent au sein du réseau
- > Outil de décryptage autonome pour un accès facile en dehors du réseau
- > Certificat numérique géré par le service MS CA
- > Mesures de sécurité supplémentaires comme l'application de mots de passe renforcés et le refus de toute utilisation externe

Validation du trafic client/serveur via un mécanisme de clés privées/publiques (SHA-1)

- > Impossible de falsifier l'un ou l'autre des trois niveaux
- > Les clés sont créées avec un générateur de paires de clés et facilement déployées

Application des règles selon que l'utilisateur est à l'intérieur ou à l'extérieur du réseau

Audit et journalisation détaillés



SecureWave

Audit et journalisation

46

Sanctuary Device Control permet d'effectuer un audit et une journalisation détaillés, grâce à ses capacités intégrées de filtre, d'export et de recherche

Utilisateur

Journalisation des actions positives et négatives

- 1) Conserve la trace des accès refusés, des nouveaux périphériques insérés, des accès autorisés, etc.

Duplication (*Shadowing*) de toutes les données copiées

- 2) Premier niveau : affiche des informations comme nom du fichier, type, taille, date de création, emplacement, nom de l'auteur, etc.
- 3) Second niveau : conserve une copie complète de toutes les données écrites sur un périphérique externe.

Administrateur

Audit de TOUTES les actions administratives

- > Garde la trace de toutes les modifications de règles apportées par les

© 2004 SecureWave Administrateurs de SDC (date, responsable, nature)



SecureWave

Gestion facile

47

Facilité d'utilisation

- > Groupes à tous les niveaux
- > Glisser-déposer disponible
- > Sélections multiples
- > Changement de nom et commentaire des périphériques/catégories

Interface client multilingue

- > La langue de l'interface cliente change en fonction des paramètres régionaux

La notification de l'utilisateur peut être activée/désactivée

Transmission en temps réel des règles d'accès

Import et export des règles d'accès

- > Pour l'archivage ou la mise à jour des PC hors ligne.

Détection à distance des nouveaux périphériques



SecureWave

Gestion facile

48

Rôles administratifs pour une gestion granulaire

- > Définir des paramètres d'accès permanents
- > Définir des paramètres d'accès en fonction de l'heure (par exemple, HELPDESK)
- > Ajouter/créer des périphériques/sous-catégories de périphériques spécifiques
- > Ajouter des périphériques et des supports CD/DVD spécifiques
- > Consulter les journaux d'audit administratifs (par exemple, AUDITOR)
- > Consulter les journaux d'accès des utilisateurs
- > Consulter les fichiers dupliqués (les fichiers de données copiés)



SecureWave

Déploiement facile

49

Installation silencieuse et sans surveillance du package MSI via

- > Le propre outil de déploiement de SDC
 - > Simple et rapide
 - > Informations supplémentaires telles que le statut du client, le système d'exploitation utilisé et le service pack
- > Tout outil de déploiement compatible MSI comme
 - > MS SMS
 - > NetInstall
 - > ZenWorks...
- > Règles de groupe
- > Fichier/script par lots

SecureWave Market Validation



SecureWave

Clients

51

Plus de 700 Clients dont :

- > Barclays Bank, PLC
- > McLaren International
- > Le Groupe Goldman Sachs
- > Norwich Union
- > MDR (Radio/tv allemande)
- > Le siège de l'OTAN
- > Daimler Chrysler, AG
- > Ministère de la Justice, Allemagne
- > Mercedes Benz, USA
- > Administration Fédérale de l'Aviation, USA
- > National Geospatial-Intelligence Agency (NGA) – anciennement National Imagery and Mapping Agency (NIMA)
- > Zuger Kantonalbank (Suisse)



SecureWave

Clients

52

Militaire & Police

- > UK MoD
- > Allied Air Forces North HQ
- > Police Fédérale d'Australie
- > CEA France
- > Cheshire Police
- > Marine Nationale, France
- > Hampshire Police
- > Landeskriminalant
- > Metropolitan Police Service London (Scotland Yard)
- > 2nd Signals Brigade
- > Norfolk Police
- > Penitentiary Complex Schevingen
- > Police Information Technology organization
- > Submarine Warfare Systems Center
- > US National Imagery Mapping Agency
- > US Navy (Norfolk & Portsmouth Naval Shipyards)

Services

- > Anglian Water
- > Gratte Brothers Limited
- > Jersey Electric Company
- > KZV Thuringen
- > MDR (Mitteldeutscher Rundfunk)
- > MMI
- > Sedibex
- > SES (Société Européenne de Satellites) - Astra
- > Soluciones Digitales
- > Transcanada Pipeline Ltd
- > Lazard Studi & Ricerche Srl



SecureWave

Clients

53

Gouvernement

- > AOK Sachsen
- > Ministère de la justice Allemand
- > Bundes und Wertpapier Aufsicht
- > Administration Fédérale de l'Aviation
- > Finanzdepartment Basel Stadt
- > Government Communications Bureau
- > Government Communications HQ (UK)
- > Hampshire County Library
- > Hessische Statistische Landesamt
- > Mairie d'Eaubonne
- > Narodni Bezpecnostni urad
- > Opac de l'Indre
- > Rechenzentrum der Hamburger Staatstheater
- > Stadt Gevelsberg
- > Stadt Wedel
- > Stadtverwaltung Schwedt
- > Stadtwerke Dusseldorf AG
- > UK Hydrographic Office
- > US Department of State S/S-IRM
- > Hampshire Constabulary



SecureWave

Clients

54

Institutions financières

- > AMEV Computer Centrum NV
- > Anker Bank
- > Banca del Gottardo Lugano
- > Bance del Salento
- > Banca di Roma International SA
- > Banca Intesa International
- > Banca Popolare di Novara
- > Banca Sella SpA
- > Banque Colbert
- > Banque Continentale du Luxembourg
- > Banque du Gothard
- > Banque et Caisse d'Epargne de l'Etat (Luxembourg)
- > Banque Ferrier Lullin
- > Banque Générale du Luxembourg
- > Banque LB Lux SA
- > Banque Pictet
- > Banque Privée Edmond de Rothschild
- > Banque Puilaetco
- > Barclays Bank Plc.
- > BBVA Privanza Bank
- > BSI SA
- > Comdirect bank AG
- > Commerzbank
- > Crédit Europeen Luxembourg – Data Services
- > Crédit Lyonnais Luxembourg
- > Crédit Lyonnais Switzerland
- > Crédit Mutuel Agricole du Cantal
- > Cregem International Bank
- > Deutsche Bank Bauspar AG
- > DG Bank Luxembourg



SecureWave

Clients

55

Institutions financières

- > East West United Bank SA
- > Egg Plc
- > F.Van Lanschot Bankiers Lux.
- > Fidelity Investments
- > Fideuram Bank
- > Fortis Bank (Nederland) NV
- > Fortis IT
- > Grant Thornton Fiduciaire
- > Goldman Sachs
- > Hauck & Aufhaeuser Banquiers Luxembourg SA
- > HSBC Trinckaus Burckardt
- > Investment Bank Luxembourg
- > Kreissparkasse Gross-Gerau
- > LGT Bank AG
- > Lloyds TSB Bank Plc
- > National Bank of Hungary
- > Natexis Banque Populaire
- > Nomura Bank Luxembourg SA
- > Norwich Union
- > Petercam Luxembourg
- > Rabobank
- > Robeco Bank Luxembourg
- > AG Rolo Banca
- > RZB Oesterreich AG
- > Société Hospitalière d'Assurances Mutuelles
- > Sogenal (Société Générale)
- > Sparkasse Erfurt
- > Sparkasse Knittelfeld
- > Sparkasse Krefeld
- > Swiss Life Luxembourg SA
- > Union Bank of Norway International
- > W.H. Ireland Limited
- > Zuger Kantonalbank



SecureWave

Clients

56

Santé

- > Clinique Romande de Réadaptation
- > Horst Schmidt Kliniken GmbH
- > Klinikum Mannheim GmbH
- > Landesversicherungsanstalt Ofr. Und Mfr.
- > Qinetiq Ltd
- > Shields Health Care Group

Industrie

- > Airbus PLC
- > Authentic Food Company
- > Boyne Smelters Ltd
- > Brake France Services
- > Cicafil SA
- > CIERMA Ascenseurs SA
- > Daimler Chrysler AG
- > Elsa Estavayer le lait
- > Hengst Filterwerke
- > Kuhn GmbH
- > Mitsubishi Motors
- > MTU – Daimler Chrysler Aerospace
- > Naval Reactors
- > SEF FmbH
- > Silvelox Spa
- > Mc Laren International

**De facto
le leader de
la
prévention
contre
l'Intrusion**



SecureWave

Résumé des avantages

57

- > Prévention des risques (par opposition à la détection) quelle que soit la source (interne / externe)
- > Les défenses des PC et serveurs sont renforcées
- > Evolutivité (du petit au grand réseau)
- > Réduction du support et de la maintenance des logiciels et des matériels en améliorant la stabilité de l'environnement des PC et des serveurs
- > ROI immédiat – TCO réduit
 - > Coûts de support réduits sans changement majeur
 - > Moins d'interventions de la part du support informatique
 - > Plus grande stabilité des PC et des serveurs





SecureWave

Analyst Validation

58

Gartner

“SecureWave offers a host-based security solution, where administrators can create rules on the use of PCs to control applications and devices. This allows only authorized devices to be used and bars access to unauthorized ones.”

Ruggero Contu
Gartner Research



“Hurwitz & Associates believes SecureWave has taken a highly intelligent and common sense approach to making the enterprise more secure and done the Industry a great service by simplifying the IT Security buy.”

Robin Bloor
Research Director
Hurwitz & Associates



“Sanctuary™ is a clean, simple way to address multiple threats on the endpoint. It doesn't attempt to “overdo” its welcome on the system by infiltrating every aspect of the system's configuration. Instead, it focuses in that area that is most important – memory and executables.

Pete Lindstrom
Research Director
Spire Security



SecureWave

Strategic Technology Partners

Technology Partners



"Companies in all fields can easily administer and centrally manage their endpoint security solutions with SecureWave's Sanctuary™ suite."

"SecureWave and Network Access Protection will improve overall network security by decreasing the risk of virus attacks and malware introduced to an organization's network, as well as the possibility of data theft associated with mobile devices."

**Steve Anderson, Director
Windows Server Group
Microsoft**



SecureWave

SecureWave® Industry Awards

60





SecureWave

Merci de votre attention

Michel Lacoste
Director, Southern Europe
Mobile +33 607 884 176

